T.C.

ÜSKÜDAR ÜNİVERSİTESİ

SOSYAL BİLİMLERİ ENSTİTÜSÜ

YENİ MEDYA VE GAZETECİLİK ANABİLİM DALI

YENİ MEDYA VE GAZETECİLİK PROGRAMI

SOSYAL MEDYA PLATFORMLARINDA VERİ GİZLİLİĞİ POLİTİKALARI

Sadık Ahmet ÇAVUŞOĞLU

YÜKSEK LİSANS

TEZİ

Danışman: Doç. Dr. Gül Esra ATALAY

İstanbul – 2020

T.C.
ÜSKÜDAR ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ
YENİ MEDYA VE GAZETECİLİK ANABİLİM DALI
YENİ MEDYA VE GAZETECİLİK PROGRAMI

SOSYAL MEDYA PLATFORMLARINDA VERİ GİZLİLİĞİ POLİTİKALARI

Sadık Ahmet ÇAVUŞOĞLU
184105010

YÜKSEK LİSANS
TEZİ

Danışman: Doç. Dr. Gül Esra ATALAY

İstanbul – 2020

ÖNSÖZ

Bu çalışma, günümüzde aktif olarak kullanılan Facebook, Whatsapp, Twitter, Youtube gibi sosyal medya platformlarının veri gizliliği sözleşmelerini açıklayabilmek amacıyla ortaya koyulmuştur. Yüksek lisans araştırması olarak hazırlanan çalışma, sosyal medya kullanıcılarının kişisel verilerinin korunması ve gizliliği gibi konuların önemine dikkat çekmektedir. Bu çalışma, Üsküdar Üniversitesi Sosyal Bilimler Enstitüsü Yeni Medya ve Gazetecilik Ana Bilim Dalı bünyesinde gerçekleştirilmiştir.

Çalışma dört bölümden oluşmaktadır. Birinci bölümde iletişimin tarihsel gelişimi, büyük veri, veri gizliliği gibi kavramların açıklamalarına yer verilmiştir. İkinci bölümde Amerika Birleşik Devletleri, Almanya ve Türkiye'nin veri gizliliği tarihi ve günümüzde uygulanan veri gizliliği politikaları incelenmiştir. Üçüncü bölümde Facebook, Whatsapp, Twitter ve Youtube gibi sosyal medya platformlarının gizlilik sözleşmeleri incelenmiş ve karşılaştırılmıştır. Aynı zamanda yaşanan veri gizliliği ihlallerinin yanında kullanıcıların veri gizliliklerini koruma yolları gibi konulara açıklık getirilmiştir.

Yüksek lisans öğrenimim amacıyla beni kabul eden **Üsküdar Üniversitesi**'ne, akademik bilgi ve tecrübesiyle araştırmama katkı sağlayan danışmanım **Doç Dr. Gül Esra ATALAY**'a teşekkürlerimi sunarım.

Sosyal Medya Platformlarında Veri Gizliliği Politikaları

Sadık Ahmet Çavuşoğlu

ÖZET

Günümüzde sosyal medya platformlarının gelişmesi kullanıcıların bu platformlarda daha fazla zaman geçirmesini sağlamıştır. Bu durum sebebiyle kullanıcılar, sosyal medya platformlarında kişisel veri olarak adlandırılan özel bilgilerini diğer kullanıcılarla paylaşmaya başlamıştır. Aynı zamanda kullanıcıların platformlar üzerindeki faaliyetleri, düşünce ve ilgi alanları gibi bilgiler devletler ve ticari kuruluşlar tarafından kolayca ulaşılabilir ve işlenebilir hale gelmiştir. Kullanıcılardan toplanan veriler bir araya geldiğinde büyük veri (big data) şeklinde adlandırılan bir yığın haline gelmektedir. Bu verilerin işlenmesi ve anlamlandırılması sonucu, ticari kuruluşların bu veriler üzerinden kazanç sağlaması durumu ortaya çıkmaktadır. Sosyal medya platformları, kullanıcılara hizmetlerini sunmadan önce gizlilik sözleşmeleri imzalatmaktadır. Bu tez çalışmasında sosyal medya platformlarının gizlilik sözleşmeleri döküman incelemesi yöntemiyle ele alınmaktadır. Araştırmanın sonucunda kişisel verilerin gizliliğinin, kullanıcıların medya okuryazarlık seviyesine, verilerini teslim etme konusundaki tutumlarına, devletlerin ve ticari kuruluşların güvenlik protokollerine uymasına göre değiştiği, kişisel verilerin gizli kalmasında da en önemli rolün kullanıcılarda olduğu görülmüştür.

Anahtar Kelimeler: Büyük Veri, Veri Gizliliği, Gizlilik İhlali

Data Privacy Policies of Social Media Platforms

Sadık Ahmet Çavuşoğlu

SUMMARY

At the present time, the development of social media platforms allowed users to spend more time thereon. Because of this, users started to share their personal data with other users on these social media platforms. At the same time, information regarding users' activities and their thoughts and interests on these social media platforms can be easily accessed and processed governments and institutions. When the collected data merges, such data becomes a stack called big data. As a result of interpretation and process of this data, institutions make profit out of such data. Social media platforms which are part of new media, execute confidentiality agreements prior they engage service relation with their users. In this thesis, confidentiality agreements of the social media platforms be addressed with the document review method. Accordingly, it is observed that confidentiality of the personal data varies in accordance with users' media literacy, their attitudes towards sharing their data and states and institutions compliance with such confidentiality agreements. Also, it was seen that the most important role in keeping the personal data confidential is rested with users.

Keywords: Big Data, Data Privacy, Breach of Confidentiality

İÇİNDEKİLER

GİRİŞ

İletişim, insanların geçmiş dönemlerden bugüne bulundukları toplumlarda fikir ve düşüncelerini aktarması, ikna etmesi üzerine kurulmuş bir sistemdir. Öyle ki milattan önceki yıllarda yaşayan avcı toplayıcı insanlar, konuşarak ifade ettikleri fikir ve düşüncelerini mağara duvarlarına resmederek nesilden nesile aktarılmasını sağlanmışlardır. İlerleyen yıllarda yazının bulunmasıyla toplumların görsel olarak ifade ettiği düşüncelerin yazıya aktarılması anlatılmak istenen düşüncenin detaylandırılmasını sağlamıştır. Yazı, sadece toplumsal iletişimi değil aynı zamanda gündelik hayatta ürünlerin sınıflandırılmasını, matematiksel hesaplamalar gibi günümüzde kullandığımız sistemlerin de temellerini atmıştır.

1450 yılında Avrupa'da matbaanın bulunması ile iletişimin sadece bir bölge ile sınırlı kalmayıp dünyadaki birçok bölgeye ulaşması sağlanmıştır. Özellikle 1455'te Guterberg'in matbaa ile bastığı ilk eser olan İncil, Hristiyanlığın yayılmasında ve kiliselerin fikir ve düşüncelerini aktarmasına öncülük etmiştir. Yıllar geçtikçe basım tekniklerinin gelişmesi gazetelerin ortaya çıkmasını sağlamıştır. Gazeteler toplum içerisindeki çeşitli olayları okuyucuları ile paylaşmanın yanında kitleleri belirli düşenlere ikna etmek için de kullanılmıştır.

Elektriğin keşfi ve gündelik hayatta kullanılmaya başlanması iletişim araçlarının gazetede olduğu gibi tek yönlüden çift yönlü iletişime geçişini sağlamıştır. 1843 yılında ABD'de Baltimore-Washington arasına bakır kablolar ile oluşturulmuş telgraf hattı mesajların çift yönlü olarak iletilmesine olanak tanımıştır. Telgraf hatlarında bakır tellerin kullanılması bugünkü teknolojik cihazlara öncülük edecektir. Öyle ki 1969'lu yıllarda bilgisayar teknolojilerinin gelişmesi ve internet kavramının başladığı yıldır. ABD'nin askeri amaçlarla geliştirdiği ARPANET (The Advanced Research Projects Agency Network) temelde farklı konumlardaki bilgisayarların birbirlerine bağlanmasıyla gerçek zamanlı iletişimin başlamasını sağlamış, daha sonra alınan kararla da internet halkın kullanımına açılarak küresel anlamda medya tüketim alışkanlıklarının değişimine yol açmıştır.

Web 1.0 ile başlayan internet süreci başlangıçta tek taraflı iletişim modeli olsa da Web 2.0'la birlikte içerik oluşturucular ve içeriği tüketenlerin eş zamanlı olarak etkileşime geçtiği, fikir ve düşüncelerini paylaştığı bir medya mecrasına dönüşmüştür.

Medya kavramı daha çok gazete, radyo veya televizyon gibi medya mecralarını ifade etmektedir. İletişim teknolojilerindeki gelişmelerle birlikte medya kavramı da değişime uğramış ve yeni medya kavramı literatüre girmiştir. İçerik üretiminin sadece medya mensuplarının tekelinde olduğu bir dönemden, kullanıcıların da içerik ürettiği bir döneme girilmiştir.

Yeni medya platformlarının gelişmesi ve kullanıcıların bu platformlardaki faaliyetleri kullanıcı verilerinin satılması veya çalınması gibi bazı olumsuz durumların ortaya çıkmasına sebebiyle devletler sosyal medya platformu sahiplerine ve kullanıcılara çeşitli sorumluluklar yüklemiştir. Verilerin gizliliği, kişinin kendisine özel, kişiyi tanımlayan ve paylaşılmaması gereken bilgilerdir. Dolayısıyla ülkelerin veri gizliliği politikalarına baktığımızda sadece günümüzde değil geçmişte de çeşitli kanunlar çıkarılmıştır. Örneğin internetin kurucu ülkesi olan ABD'de 1975 yılında gizlilik yasası yürürlüğe girmiş ve 1978'de bazı mali evraklara olan erişimlere düzenleme getirilmiştir. Bilgisayarın insan hayatına girmeye başlamasıyla 1986'da elektronik haberleşme yasasında düzenlemeye gidilmiştir. Günümüzde Amerika'nın devlet çapında uyguladığı merkezi bir yasanın yanında eyaletlerin de bu yasaya bağlı olarak farklı veri gizliliği politikaları mevcuttur. Almanya'da ise 1977 yılında Federal Veri Gizliliği kanunu kabul edilmiş ve ilerleyen zamanda 1986 ve 1988 yıllarında iki kez yenilenmiştir. Günümüzde ise Avrupa Veri Koruma Kanunu ile veri gizliliğinde bir standarda ulaşmıştır. Türkiye'de ise veri gizliliği, 1841'de Osmanlı Devleti zamanında kurulmuş ve Cumhuriyet Döneminde de devlete bağlı olarak faaliyetlerine devam eden PTT (Posta, Telefon, Telgraf) tarafından 1950 yılında kişilerin göndermiş olduğu postaların yetkili personel tarafından kesinlikli açılmaması üzerine bir kanun yayımlanmasıyla başlamaktadır. 1973 yılında kanun metni içerisinde personel kavramı geniş bir ifade ile yeninden düzenlenerek postanın gizliliğinin arttırılması amaçlanmıştır. Türkiye'de elektronik anlamda veri gizliliği, Avrupa'daki veri gizliliği kanunlarının standartlarına göre hazırlanan ve 24.03.2016 yılında kabul edilen 6698 sayılı "Kişisel Verilerin Korunması Kanunu" ile mümkün olmuştur.

Devletlerin olumsuz durumlara karşı belirlemiş olduğu veri gizliliği kanunlarına ticari kuruluşların uyma zorunluluğu bulunmaktadır. Örneğin İngiltere'de bulunan Facebook sunucuları çeşitli birçok kişinin verisini içerdiğinden fiziksel olarak güvenliklerinin yanı sıra teknolojik olarak da korunması amaçlanmıştır. Bu amaç

doğrultusunda hazırlanan GPDR (Avrupa Veri Koruma Kanunu) ticari kuruluşların kullanıcılardan veri talep etmeleri ve bu verileri kullanma, üçüncü kişiler ile paylaşımı söz konusu ise kullanıcıların onayının alınması gerektiğini belirtmiştir. Aynı zamanda alınan verilerin teknolojik standartlar düzeyinde korunması zorunlu tutulmuş ve kullanıcının şahsi verilerinin silinmesi yönünde bir talepte bulunması durumunda da ticari kuruluşlarda bulunan kişisel verilerin en kısa sürede temizlenmesi şartı getirilmiştir.

Yeni medya ortamlarının gelişmesi ve kullanıcıların içerik üretici bir konuma gelmesi büyük miktarda verinin üretilmesini sağlamıştır. Ancak çok fazla veri olması bir anlam ifade etmemekte üstelik gürültü (noise) oluşturmaktaydı. Web 3.0 teknolojisiyle birlikte içerikler insan kontrolünden yazılım kontrolüne geçmiş, nitelendirilen ve işlenen verilerin daha değerli olduğu da firmaların gözünden kaçmamıştır. Bir kullanıcının sosyal medyada ürettiği ve tükettiği içerikler ile bakış açısı, zevkleri ve satın alma alışkanlıkları veri analiziyle kolaylıkla ortaya çıkarılabilmektedir. Bu nitelemeler kişilerin gizli kalması gereken verileridir. Ancak hemen hemen tüm sosyal medya platformları kullanıcıların verilerini yasal yollarla işleyebilmektedir. Örneğin bir kullanıcı Facebook'a üye olmak istiyorsa belirli kişisel bilgi alanlarını doldurduktan sonra firmanın gizlilik sözleşmesini onaylamak zorundadır. Onaylamadığı taktirde kullanıcı hizmeti kullanamamaktadır. Kullanıcı sözleşmesi incelendiğinde kullanıcının üretmiş olduğu içeriğin yanında kullanıcıdan bağımsız olarak cihaz bilgileri, medya platformu içerisinde incelediği tüm verileri topladığı ve işlediği görülmektedir. Milyonlarca Facebook kullanıcısı olduğu bilindiğinden firmanın elinde değerli bir verinin olduğu söylenebilir. Daha da önemlisi bu verilerin farklı amaçlar doğrultusunda kullanılması söz konusu olabilmektedir. Yakın zamanda yaşanan Cambridge Analytica skandalı buna güzel bir örnek oluşturmaktadır. Skandalın patlak vermesiyle ortaya çıkan olayda Facebook kullanıcı verilerinin Amerika Başkanlık seçiminde seçmelerin tercihlerini belirleme ve yönlendirilmesinde kullanıldığı iddia edilmiş, bu iddiaları araştıran ABD Federal Ticaret Komisyonu Facebook'a 5 milyar dolar ceza kesmiştir. Yaşanan bu olayla kişisel veri gizliliği konusunun önemi bir kez daha gözler önüne serilmiştir.

Bu çalışmada, günümüz yeni medya mecralarında sıklıkla ihlallerin yaşandığı veri gizliliği konusunun Amerika, Almanya ve Türkiye gibi ülkelerde nasıl geliştiği, bu ülkelerdeki yasalaştırılmış olan veri gizliği kanunlarının nasıl uygulandığı, sosyal medya platformları kullanıcı sözleşmelerinden hangi verileri talep ettiği ve hangi şartlarda

verileri kullanacağı araştırılmıştır. Tez çalışmasında betimsel araştırma yöntemlerinden olan doküman incelemesi çalışması uygulanmıştır. Araştırma şu sorulara cevap aramayı amaçlamaktadır:

- Sosyal medya platformlarının gizlilik sözleşmeleri hangi şartları içermektedir?
- Sosyal medya platformları tarafından toplanan veriler hangi amaçlar için kullanılmaktadır?
- Türkiye'deki veri koruma kanunları ve uygulamaları nelerdir?

Araştırmada veri gizliliği kanunlarının Türkiye'de nasıl uygulandığı, ABD ve Almanya gibi ülkelerde veri gizliliği uygulamalarının nasıl olduğu, sosyal medya platformlarının belirlemiş olduğu gizlilik sözleşmeleri aracıyla kullanıcıların hangi bilgileri topladıkları, verilerin hangi amaçlar doğrultusunda kullanılmakta olduğu, kişisel verilerin satılması veya veri güvenliği açıkları sebebiyle çalınması gibi konulara yer verilmiştir.

BİRİNCİ BÖLÜM: KAVRAMLAR

1.1.Yeni Medya Kavramı ve Tarihsel Gelişimi

İletişim, geçmiş dönemlerden itibaren insanların fikir ve düşünlerini paylaşılmasında önemli yere sahiptir. M.Ö. 25000 yıllarında avcılık ve toplayıcılık dönemlerindeki ilk insanlar birbirleri ile iletişimi doğal zeminler üzerine çeşitli resimler veya heykeller yaparak sağlamaktadır. Böylelikle fikir ve düşünceler sadece o dönemki toplumda kalmayıp gelecek nesillere de aktarılabilmiştir. Öyle ki bugün halen Lascoux[1] ve Altamira[2] mağaralarında ilk duvar resimleri mevcuttur (Bulat, 2007). M.Ö. 3100 yıllarından itibaren insanlar arasında yazının gelişmesi iletişim kavramına farklı bir boyut kazandırmıştır. Matbaanın bulunması geçmişte elle yazılarak sınırlı sayıda çoğaltılabilen kitapların ucuz ve hızlı bir şekilde çoğaltılabilmesine aynı zamanda gazete benzeri materyallerin yayımlanmasına imkân sağlamıştır. Böylelikle fikir ve düşünceler daha fazla kitle ile paylaşılmıştır. Örneğin 1455 yılında Gutenberg tarafından basılan ilk eser İncil'dir (Küçükcan, 2006: 160). Bu durum iletişimin temellerinden olan ikna kavramını güçlenmesine ve kitap, gazete gibi yayımların bir ikna aracı olarak kullanılmasına sebep olmuştur.

Kuramsal olarak bakıldığında iletişim, gönderen ve alıcı olarak basit bir şekilde tanımlanabilir. Bu konu üzerine araştırma yapan Lasswell, iletişim kuramının bu kadar basit olarak kalmayacağını söylemiş ve iletişimi *"kim, kime, neyi, hangi kanalla, ne şekilde söylüyor?"* şeklinde tanımlamıştır. Lasswell, propaganda üzerine yaptığı çalışmalarda kitle iletişim araçlarının başka işlevlerini de bulur. Konu ile ilgili sistematik sınıflandırma yapan Lasswell kitle iletişim araçlarının temelde 3 unsurunun olduğunu belirler (Güngör, 2018: 88):

- Çevrenin gözetilmesi,
- Toplumun parçaları arasında bütünlük sağlanması,
- Kuşaklar arası kültür aktarımının gerçekleşmesi şeklindedir.

Lasswell'in kuramına karşılık olarak iletişim kuramları üzerinde araştırma yapan Westley ve Maclean'nin kitle iletişim modelinde iletişimi karşılıklı bir süreç olarak tanımlar ve iletişimde geri bildirim öğesinin olduğunu savunur (Güngör, 2018: 68).

[1] Lascaux mağarası, Fransa'nın güneybatısında yer alan Montignac Köyü yakınlarında bulunmaktadır.
[2] Altamira mağarası, İspanya'nın kuzey kesiminde Santillana Del Mar yakınlarında bulunmaktadır.

Çünkü gerek kişi gerekse kitle ile yapılan iletişimlerde, iletişimin doğru ve amaca uygun şekilde anlaşıldığından emin olmak için geri bildirim önemli bir noktadır. Örneğin bir siyasetçi çeşitli araçlar ile yaptığı propaganda sonrasında kitlesinden destek görebiliyorsa iletişimini doğru yönetmiş ve amaca uygun hareket etmiştir. Aksi taktirde gürültü unsuru sebebiyle iletişim kesintiye uğramıştır.

İletişim bu noktaya kadar sadece kağıt üzerinde kalan veya söz ile ifade edilebilen bir araç olmaktadır. Teknolojinin gelişmesi iletişim araçlarının seyrini değiştirecektir. Artık iletişim çift yönlü ve karşılıklı olarak kullanılabilen bir araç haline gelecektir. Bu temeller ilk olarak telgrafın icadı ve kullanılması ile sağlamıştır. Samuel Morse tarafından icat edilen telgraf, Amerikan Kongresini o kadar etkilemiştir ki 1843 yılında Washington Baltimore Maryland arasına bakır kablo ile telgraf hattı çekilmesi için 30.000 dolar[3] fon sağlanmıştır (A History of Telegraphy, 2014). O dönem telgraf sinyallerinin iletilmesi için döşenen bakır kabloların kullanılması bugünkü teknoloji donanımların temelini oluşturacaktır. Telgraf hattının kurulması sonrasında ilk iletilen mesaj "Tanrı ne yaptı?" sözü olacaktır (Czitrom, 1982). Sonrasında telefonun icadı telgrafın kullanımını ortadan kalkacaktır.

İlerleyen zamanlarda teknoloji yatırımlarını arttıran Amerika bir adım daha ileri giderek iletişim araçlarının tasarlanmasına öncülük etmiştir. 1969 yılında Amerika bilgisayar teknolojisini geliştirmek ve askeri araştırmalar yapmak amacıyla ARPANET internet ağını oluşturmuştur. (Çağıltay, 2009) Sonrasında bu teknolojinin kamuya açılmasıyla internet evlere girmeye başlamış teknolojik ürünlerdeki fiyat düşüşü ile kişisel bilgisayarların kullanımı artmıştır. Bu gelişim 2000'li yıllara kadar sürmüş, 2000'li yılların sonrasında ise radyo dalgaları üzerinden sağlanan veri akışı gelişen teknoloji ile sürekli artmıştır. Bu artış, sadece sabit mekanlardan sağlanabilen internet erişimini evlerden dışarıya çıkarak taşınabilir hale getirmiştir. Yine bu dönem içerisinde internetin yaygınlaşması, bant genişliklerinin artması, donanımların daha da küçülerek işlevsellik sağlaması gibi özellikler günümüz teknolojilerini bir arada kullanmamamıza imkân sağladı. İletişim teknolojilerindeki gelişmeler ve internetin yaygınlaşması Web 1.0 dönemini bir kenara bırakmamıza ve kullanıcıların da içerik ürettiği Web 2.0 dönemine

[3] Samuel Morse 1843 yılında Amerikan Kongresinden aldığı 30.000 Dolarlık fon bugünün değeriyle 1,039,414.86 Milyon Dolara eşittir (*$30,000 in 1843 - 2020, Inflation Calculator*, 2020).

geçişimizi hızlandırmış böylece web kaynaklı araçlar ile daha fazla iş birliği içerisinde kalmamızı sağlamıştır (Kesim & Ağaoğlu, 2007).

Web 2.0, 2004 yılında sosyal medyanın kapılarını açan Facebook ile tam anlamıyla kullanılmaya başlamıştır (*Facebook Newsroom*, 2019). Facebook, yaşadığımız gerçek hayatın yanında bir de sanal bir hayat ortamı oluşturdu. Böylece gerçek hayatta arkadaşlarınızla kurmuş olduğumuz etkileşim bu tür platformlarda da gerçekleşir hale geldi. Sonrasında çıkan Twitter, Instagram gibi platformalar da bu alanı genişletmiştir. İletişim teknolojilerinin yoğun kullanımıyla birlikte hedef kitle hakkında daha fazla bilgiye sahip olunabildiği görülmüş aynı zamanda elde edilen bilgiler sayesinde onların ikna süreçlerinin de kısaldığı tespit edilmiştir. Bu nedenle kişi veya ticari kuruluşlarda harekete geçmeden önce hedef kitle ile ilgili birçok bilgiyi toplamak istemişlerdir. Zaman içerisinde hedef kitlenin yaptığı tüm faaliyetler büyük bir veri oluşturmasına neden olmuş, bu verilerin hızlı bir biçimde işlenmesi gerektiği ancak bunun da sistem tarafından öğrenilerek gerçekleştirilebileceği görülmüştür. Semantik yani öğrenebilir bir yapıda olan Web 3.0 teknolojileri de işte burada devreye girmektedir. Günümüzde arama motorları çok daha fazla bilgiyi indeksleyebiliyor ve hedeflenen bilgiler üretebiliyor, kullanıcılar da sosyal medya uygulamaları aracılıyla arkadaşları ve işletmelerle daha sık bir şekilde bağlantı kuruyorlar. Ortaya çıkan bu bilgi yığınlarından faydalı bilgiler elde isteği verileri daha fazla kaydetme, saklama ve sınıflandırma yeteneği olan Web 3.0'ı daha kesin ve yararlı hale getiriyor (Nath & Iswary, 2015: 2). Dolayısıyla pazarlamacılar hedef kitlesine elde ettikleri veriler sayesinde reklam veya ürün ile ilgili kişisel deneyimler sunabilmektedir. Bu durumu kitle iletişim araçları kullanarak hedef kitleye gönderilen mesajın doğrudan etki ettiği düşünülen "Sihirli Mermi Kuramı" ile açıklayabiliriz. Mesaj iletildikten sonra kitlenin davranışlarını etkilemektedir (Yaylagül, 2010: 46). Web 1.0 ve Web 2.0 arasındaki temel fark, içerik üreticileri ile tüketicilerin tek bir kullanıcı olabilmesidir. Web 2.0 ve Web 3.0 arasındaki farkın çok büyük olmadığı görülmektedir (Choudhury, 2014: 4):

Web 1.0	Web 2.0	Web 3.0
1996 - 2004	2004 - 2016	2016…
Hypertext bağlantı verilen web siteleri	Sosyal Web	Semantik Web
Sadece Okunabilir Web	Okunabilir ve Yazılabilir Web	Yürütülebilir, Öğrenebilir Web
Milyonlarca Kullanıcı	Milyarlarca Kullanıcı	Trilyonlarca Kullanıcı
Kendine Ait Ekosistem	Katılımlı ve Etkileşimli	Kendini Öğrenmeye Dayalı
Tek Yönlü	Çift Yönlü	Çoklu Kullanıcılı Sanal Ortam
Kurumlar İçerik Yayımlar	Kullanıcılar İçerik Yayımlar	İnsanlar Diğer İnsanlarla Etkileşime Girdiği Bir Uygulama Yayımlar
Sabit İçerik	Dinamik İçerik	Yapay Zeka, 3D, Web Öğrenme
Kişisel Sayfalar	Blog ve Sosyal İçerik	Sınırsız İçerik
Mesaj Listeleri	Topluluk Forumları	Semantik Forumlar
Arkadaş Listesi	Sosyal Ağ Bağlantıları	Semantik Sosyal Ağ Bilgileri

Tablo1: Web 1.0, Web 2.0 ve Web 3.0 Karşılaştırması

Yakın gelecekte göreceğimiz Web 3.0 teknolojisiyle yapay zekanın yükselişini, internet üzerindeki bilgileri semiyotik olarak öğrenmesi sonucunda akıllanan sistemleri ve sonuçta insan ve yapay zekanın etkileşimini göreceğiz (“Web 4.0: The Ultra Intelligent Electronic Agent is Coming”, 2013). Telekomünikasyonun gelişimindeki ilerleme ile insan beyni kadar güçlü Web 4.0 üzerinden kontrol edilecek ara yüzlere sahip olunacak. Böylece makineler web içeriğini analiz etmede akıllıca davranacak, web sitelerini hızlı ve kaliteli bir şekilde yükleyecek ve daha fazla komut istemiyle ara yüzlerde ilk önce neyin çalışacağına karar verecektir (Choudhury, 2014: 5).

1.2. Yeni Medya ve Veri Gizliliği İlişkisi

Teknolojinin günümüzdeki gelişimi nedeniyle hızlı bir değişim süreci sonrasında olguların ve sınırların ortadan kalktığı aynı zamanda anlamlandırmadaki değişimler küreselleşme dediğimiz kavramı oluşturmuştur (Işık, 2004: 2). Küreselleşme ile bir daha hiç çıkılmamak üzere yeni medya ortamlarına girildiği görülmektedir (Akgül & Akdağ, 2017: 211). Baudrillard'ın[4] "*artık toplumsallaşmayı belirleyen şey kuramsal sınırlar değil, haber miktarıyla iletişim araçlarının karşısında geçirilen saatlerdir. Ancak bu yanlış bir düşüncedir. Çünkü haber kitlenin enerjisini yok etmek yerine, her zaman için giderek büyüyen bir kitle yaratmaktadır*" sözü yeni medyanın geri dönülmez bir nokta olduğunu desteklemektedir (Baudrillard, 1991). Yeni medya kitlelerin içerisinde içerik üretebildiği ve aynı zamanda içeriği tüketebildiği bir alan yaratmıştır. Bu alan zaman, mekan farkının bulunmadığı, yazınsal ve görsel öğelerin analiz edilmesi ile bireylerin tutum ve davranışlarını yeniden tasarlamaya yönelten bir medya hizmeti olduğu belirtilmektedir (Yanik, 2016: 903). Yeni medyanın temelde 3 ana özelliğini şu şekilde sıralamak mümkündür (Aydoğan & Kırık, 2012: 60):

- **Etkileşim (Interaction):** İletişim esnasında gönderici ile alıcı arasında etkileşime ihtiyaç duyulmaktadır. Böylelikle her iki taraf birbirinden etkilenmektedir.
- **Kitlesizleştirme (Demassification):** Yeni medya içerisinde çok sayıdaki bireye kişisel mesajlar ile iletişime geçilebilmesini sağlamak için toplumdaki bireylerin kitlesizleştirilmesi gerekmektedir.
- **Eşzamansızlık (Asekron):** Yeni teknoloji altyapıları ile bireylere istediği zaman mesaj alma ve gönderme işlemi imkanını sağlamıştır.

Yeni medya günümüzde toplumların hayatlarının içerisine o kadar girmiştir ki artık toplum bunu bir yaşam biçimi olarak görmektedir. Kişiler, sosyal medya platformları aracılıyla tanıdığı veya tanımadığı birçok kişiyle iletişim kurabilmekte ve

[4] Baudrillard, günümüz dünyasının teknoloji ile hızla dönüşümünden ve bu dönüşümün postmodern batı dünyasına eleştiriler yaparak analizler ortaya koymuştur. Baudrillard'ın değindiği önemli noktalardan biri toplumun gerçeklik algısını yitirmesidir.

etkileşime geçilebilmektedir. Manuel Castells[5] bu durumu iletişimin gücü adlı kitabında, "*ağlar yirmi birinci yüzyılın toplumlarının her türlü temel yaşam biçimi oluşturur. Fritjof Capra'nın[6] yazdığı gibi ağ tüm yaşam için ortak bir kalıptır. Yaşamı nerede görürsek görelim ağları görüyoruz*" şeklinde ifade etmiştir (Castells, 2009: 21). Ağlar toplumun içerisine yerleşmiş bir yaşam biçimi halindedir. Ayrıca bu ağ arasında herhangi bir siyasi veya bölgesel sınır bulunmadığından Marshall McLuhan'ın belirttiği küresel köy ifadesi, ağ toplumlarındaki kitlelerin kolaylıkla etkileşime geçebileceğini destekler niteliktedir. McLuhan, yeni elektronik medyanın yardımıyla taşınan mesajlar, kişileri etkilemese de küresel köyü oluşturacağını savunuyor. Çünkü medyanın mesaj olduğunu iddia ederek medya insanların birlikteliğini, eylemlerinin ölçeğini, şekillendireceğini ve kontrol edeceğini belirtmiştir (Georgiadou, 1995: 13). Küresel köy dünya üzerindeki sınırları ortadan kaldırarak herkesin etkileşime geçmesini ve kullanıcıların sadece içeriği tüketen değil aynı zamanda içerik üreten olması web üzerindeki verilerin büyümesine sebep olmuştur. MarTech verilerine göre internetin 2017'deki toplam büyüklüğü 2.7 Zettabayte'tır. 2020 yılına gelindiğinde ise bu oran 44 Zettabayt'a[7] kadar çıkması bekleniyor (*How Much Data On The Internet*, 2019). Bu oranların artması üretilen içeriklerin türlerinin belirlenmesi ve analiz edilmesini gerektirmektedir. Büyük veri şeklinde ifade edilen bu kavram geleneksel işleme tekniklerinin çalışmadığı yapısal ve yapılandırılmamış büyük karmaşık veri kümelerini ifade eder (Taylor, 2016: 1). Ancak bu veri yığını içerisinde sadece sistemsel veriler bulunmamakta, bunun yanında kişisel veriler dediğimiz özgeçmiş bilgileri, sağlık bilgileri gibi kişiye ait olan bilgiler yer almaktadır. Bu verileri kullanıcılardan alan ticari kuruluşlar, verilerin güvenli bir şekilde saklanması ve verilen önem düzeyine göre üçüncü kişiler ile paylaşılması konusunda sınırlanmaktadırlar. Özellikle 2017'de Avrupa Birliği bu konu üzerinde odaklanarak, veri gizliliği politikalarına aykırı durumlarda Mayıs 2018'de yürürlüğe giren veri koruma yönetmeliği (GDPR) çok önemli cezalar verme potansiyeli nedeniyle dikkat çekmektedir. Cezalar, 20 Milyon Euro ve firmaların cirolarının yüzde 4'üne varan ödemelerle

[5] Manuel Castells, teknolojinin gelişmesiyle oluşan sosyal ağların toplumları birbirine bağlayarak kitlesel hareketlerin toplumları daha hızlı etkilediğini belirtmiştir. Castells buna bağlı olarak iktidar ve iktidar karşıtlığı kavramlarını ele almıştır.

[6] Fritijof Capra, yüksek enerji fiziği konusunda çalışmalar yapmış, çalışmalarını teorik fiziğin felsefi etkilerini irdelen Capra, *Fiziğin Tao*'su adlı kitabında bu çalışmasını yayımlamıştır.

[7] Zettabayte çok sayıda bulunan verilerin birim katıdır. Örneğin 1 Zettabyte'ın Gigabayt oranına ulaşmak için 1024Byte⁴ ile çarpılması gerekmektedir. Bk. Tablo 4

sonuçlanabilmektedir (Raul, 2017: 1). Ticari kuruluşların kullanıcılardan topladıkları verileri saklamakla yükümlü olduğu kadar kullanıcılar üzerinde de birer sorumluluk vardır. Çünkü ticari kuruluşlar bu verileri kullanıcıların rıza göstermesi sonrasında elde etmektedir. Türkiye kişisel verilerin korunması kanununda, kişi belirli bir konuya ilişkin verilerinin, konuyla ilgili yeterli bilgi almak kaydıyla verilerin işlenmesine özgür iradesi ile onay vermesidir (*Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular*, 2018: 23). İşte burada önemli nokta, kullanıcıların onay verme sürecidir. En az üzerinde durulan bu husus, medya tüketiminde kritik öneme sahiptir. Yeni medyanın özellikleri hakkında, kullanıcıların kritik birer sorumlu haline getirilmesi gerektiği savunulmaktadır. Daha da önemlisi kullanıcıların medyayı tüketirken kritik önem taşıyan medya yetkinliğinin geliştirilmesi şarttır (Wu, 2011: 86).

1.3. Büyük Veri Kavramı

Web 2.0 teknolojisinin hayatımıza girmesi, internet ortamına birçok verinin yüklenmesi ve tutulması zaman geçtikçe veri boyutlarını arttırmıştır. Veri tabanlarındaki yazılımlar ile bu verilerin yönetilemeyecek kadar büyük boyutlarda olması büyük veriyi tanımlayabilir (Kiliç, Atalay, & Yurtsever, 2019: 296). Büyük veri kaynaklarına iklimlendirme sensörleri, sosyal medya sayfaları, dijital ortamdaki fotoğraflar, videolar, bankalar üzerinde tutulan müşteri işlemleri, cep telefonlarından gönderilen gps sinyalleri örnek olarak verilebilmektedir (Çakirel, 2016: 54).

Büyük veri tanımlarının çoğu, depolama alanlarındaki verilerin boyutlarına odaklanır. Boyut önemlidir ancak verilerin çeşitliliği ve veri hızı gibi diğer önemli nitelikleri de vardır. Büyük verinin temelde, hacim, çeşitlilik ve hız faktörlerinin bir arada bulundurularak değerlendirilmesi gerekmektedir (Russom, 2011: 6).

Büyük veride hacim, verilerin depolandığı platformlardaki boyutu yani hacmini ifade eder. Bu büyük boyutlu veriler terabaytlarla ölçülen boyutlarda olabilir. Ancak ilerleyen zamanda depolanan bu verilerin boyutlarının artacağı düşünülüyor. Cisco küresel internet trafiği üzerinde yayımlamış olduğu çalışmada şu sonuçlar dikkat çekmektedir (“Cisco Visual Networking Index: Forecast and Trends, 2017–2022”, 2019: 5):

Yıllar	Küresel İnternet Trafiği
1992	Günde 100 GB
1997	Saatte 100 GB
2002	Saniyede 100 GB
2007	Saniyede 2 TB
2017	Saniyede 46,6 TB
2022	Saniyede 150,7 TB

Tablo 2: Yıllara Göre Küresel İnternet Trafiği ("Cisco Visual Networking Index: Forecast and Trends, 2017–2022", 2019)

Cisco'nu yapmış olduğu çalışmada küresel internet trafiği 2007'den 2017'ye 44.6 TB'lık bir artış görülmüştür. Bununla beraber 2022 yılında beklenen veri akışı saniye 150 TB'ları bulan veri yığınları öngörülmektedir.

Boyut	Sembol	Byte Boyutu[8]
Byte	B	1 Bytes
Kilobyte	KB	1 000 Bytes
Megabyte	MB	1 000 000 Bytes
Gigabyte	GB	1 000 000 000 Bytes
Terabyte	TB	1 000 000 000 000 Bytes
Petabyte	PB	1 000 000 000 000 000 Bytes
Exabyte	EB	1 000 000 000 000 000 000 Bytes
Zetabyte	ZB	1 000 000 000 000 000 000 000 Bytes
Yottabyte	YB	1 000 000 000 000 000 000 000 000 Bytes
Brontobyte	BB	1 000 000 000 000 000 000 000 000 000 Bytes
Geopbyte	GB	1 000 000 000 000 000 000 000 000 000 000 Bytes

Tablo 3: Dosya Boyutu Birim Tablosu

Büyük veride çeşitlilik, veri içerisindeki çeşitli kaynakları tanımlamaktadır. Verilerin çoğu gün içerisindeki web hareketleri kaynaklıdır. Bu veriler ticari kuruluşlar

[8] Tablo 3'te yer alan birimlerin byte boyutları 1024'ün katları şeklinde artmaktadır. Örneğin 1 Megabyte boyutunun Byte cinsinden gerçek değeri 1.048.576 Byte (1024x1024) şeklindedir. Tablo daha iyi anlaşılması için rakamlar yuvarlanmış şekilde yazılmıştır.

için yeni değildir ancak bu verilerin analiz edilmesi ve etkin bir şekilde kullanılması ticari kuruluşlar için daha karmaşıktır (Russom, 2011: 7).

Büyük veride hız, verilerin platformlar arasındaki iletişim süresini ifade eder. Günümüzde veri üretim oranının yüksek olması, internet ortamında hızlı aktarılmasını gerektirmektedir.

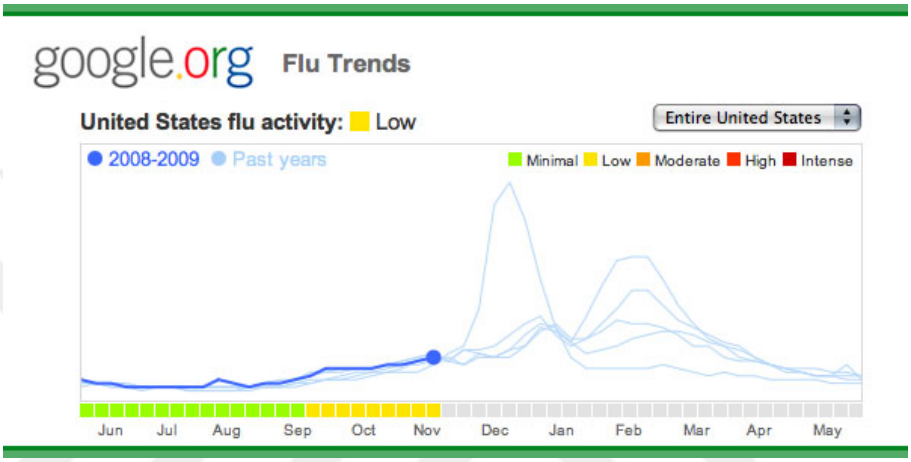
Büyük veri kavramı ortaya atıldığında 3V kavramları ile açıklanırken sonrasında bu kavramlara iki unsur daha eklenmiştir. Bunlar, verilerin doğrulanması ve verilerin analiz edildikten sonra değerlendirilmesidir. Veri doğrulama iki farklı anlama sahiptir. İlki verileri oluşturan kaynağın doğruluğunu ifade ederken, ikincisi ise analiz edilen verilerin hedef kitleye uygunluğu ile ilgilidir (Kiliç, Atalay, & Yurtsever, 2019: 296). Diğer unsur olan verinin değeri, maddi anlamdaki durumunu ifade eder. Verinin maddi olarak kabul edilmesi süreci, 2012 yılında Davos'da yapılan Dünya Ekonomik Forumu'nda bugün kullanılan altın ve para gibi maddi değerlerine ek olarak yeni ekonomik değer adı altında "veri" kavramından bahsedilmiştir (Korcan; Arslantekin, 2016: 21).

Hacim (Volume)	**Çeşitlilik (Variety)**	**Hız (Velocity)**	**Doğrululuk (Veracity)**	**Değer (Value)**
Terabytes	Yapılandırılmış Veri	Veri Yığını	Verinin Güvenilirliği	İstatistiksel
Kayıtlar	Yapılandırılmamış Veri	Yakın Zaman Verisi	Verinin Gerçekliği	Olaylar
İşlemler	Yarı Yapılandırılmış Veri	Gerçek Zaman Verisi	Verini Kaynağı	Verinin Bağlantıları
Tablolar ve Dosyalar	Yukarıdakilerden Tümü	Verilerin Akışı	Hesap Verebilirlik	Verinin Kurumsallığı

Tablo 4: Büyük Veride 5V Unsurları

Büyük verinin kullanım alanlarında ticari kuruluşlar müşterilerinin satın alma faaliyetleri, satın alma davranışları, kişisel veriler gibi özellikleri analiz edebilmektedir. Devletler tarafından bakıldığında ise örneğin sağlık alanındaki harcamalarını daha doğru saptayabilir ve kaynak israfı yapılmadan daha tutarlı bir hedef belirlenebilir. Sağlık verilerini depolayarak yılda hastanelere kaç hastanın başvurduğu, bu hastanelerde kaç kişiye ameliyat yapıldığı, aynı zamanda ne kadar ilaç tüketildiği gibi bilgiler edinilmiş olacaktır (Altınbas, 2018: 218).

Büyük verinin örneklerinden olan ve Google tarafından geliştirilen *Google Flu Trends*, Google üzerinden gelen arama verileri ile enfekte aktivitesini gözlemlemek için kullanıldı (Wilson, 2009: 1). Google elinde bulunan hastalık verilerini ABD Hastalık Kontrol Merkezi (CDC) ile iş birliği yaparak karşılaştırdı. Böylelikle Google, arama motorundan gelen verileri anlık olarak incelemiş ve hastalık arama oranlarında bir artış gözlemlendiğinde hastalık kontrol merkezinden gelen veriler ile karşılaştırılarak doğruluğu teyit edilmiştir (Google.org, 2009).



Şekil 1: Google Hastalık Trendleri, ABD'de Hastalanma Verileri[9]

Şekil 1'deki grafikte ABD 2008-2009 yılları arasındaki hastalık arama verileri görülmektedir. Verilerde geçmiş yıllara ait analizlerde bulunmaktadır. Böylelikle hastalıkların hangi dönemlerde artacağı veya azalacağı ön görülebilmektedir. Google hastalık trend sistemini 2014 yılına kadar devam etmesine rağmen çeşitli nedenler dolayısıyla proje durdurulmuştur ("Google Flu Trends", 2019).

Büyük verinin işlenmesine örnek olacak bir diğer araştırma geliştirme projelerinden olan Google'ın Picasa programında uyguladığı ve şirket gizlilik politikasında *"Kullanıcılar fotoğraflarını Google'ın ilk fotoğraf uygulaması olan Picasa'da nasıl düzenlediklerini anlamamız, Google Fotoğrafları tasarlayıp kullanmamıza yardımcı oldu"* ifadelerine yer verilmiştir (*Google Gizlilik Politikası*, 2019: 4).

[9] Google Flu Trends Bk: *http://blog.fabric.ch/index.php?/archives/297-Google-Flu-Trends-Tracking-Flu-across-the-U.S..html*

Büyük veri özellikle internet üzerindeki içeriklerin artması ve bununla beraber gelen internet trafik oranlarının artışı platformlar arasındaki veri transferlerinin daha hızlı olmasını zorunlu kılmıştır. Ancak bu hız verilerin birer yığın halinde birikmesine, analiz edilmemesine yol açmaktadır. Google, Amazon, Microsoft gibi teknolojiye ve yapay zekaya yatırım yapan kuruluşlar elde ettikleri verileri milyonlarca değişken ile sınıflandırmaktadır. Özellikle gelecekte bu firmaların sahip olacağı semantik web sonrasında Web 4.0 ile veriler analiz edilirken daha veriler sistemlere ulaşmadan yapay zekâ, gelecek olan verilerin içeriklerini veya oranlarını tahmin edecek, sonrasında gelen gerçek veriler ile karşılaştırılarak doğruluklarını ve tutarlılıklarını analiz edilecek. Bu sistemin benzerini hastalık trendlerinde kullanan Google, anlık olarak elde ettiği arama verilerini, merkezi sağlık raporları ile karşılaştırarak sistemin tutarlılıklarını geliştirmiştir.

Web 4.0 teknolojisi büyük veri kavramını daha da üst seviyeye çıkaracağı muhtemeldir. Bunun nedeni artık kullanıcılar ürettiği içerikler değil, aynı zamanda yapay zekanın ürettiği içerikler de görülecektir. Bunun yanında yapay zekâ büyük veriden destek alarak tartışmalara katılabilecektir.[10] Bu da yapay zeka ile büyük veri entegrasyonun sağlanmasıyla olacaktır.

2.3.1. ULAKBİM Türkiye Ağ İstatistiği Örneği

Büyük veri kavramı, sadece binlerce müşterisi olan ticari k elde ettiği verileri değil bunun yanında dünyada bu verilerin bir noktadan diğer bir noktaya aktarılmasını da kapsamaktadır. Türkiye İstatistik Kurumunun yapmış olduğu cinsiyete ve yaşlara göre internet kullanım oranlarına bakıldığında özellikle 25-34 yaş grubunun yüzde 91,7'si internete ulaşmaktadır (*Türkiye İstatistik Kurumu*, 2020). Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) tarafından 2019 yılında hazırlanan Toplam Küresel İnternet Geçişi raporunda, alınan ve gönderilen veri boyutunun 94.09 Petabyte olduğu görülmektedir. 2019 yılının ortalama alınan ve gönderilen veri boyutu 6.28 Petabyte şeklindedir. 2020 yılı içerisinde Ocak ayından 8.68 Petabyte ve Şubat ayından 8.22 Petabyte değerleri görülmüştür (*ULAKNET Uç İstatistikleri*, 2020).

[10] IBM'in tarafından geliştirilmiş olan yapay zeka, karşısında bir insan ile şehirlerde bulunan güvenlik kameralarının kişilerin gizliliğini engellemesi konusunda tartışma yapabilmektedir. Bk. https://youtu.be/ZIY1uSxL-qQ

	Alınan	Gönderilen	Toplam
Ocak	5.45 PB	1.52 PB	6.97 PB
Şubat	5.66 PB	1.46 PB	7.12 PB
Mart	7.6 PB	1.72 PB	9.31 PB
Nisan	7.2 PB	1.71 PB	8.91 PB
Mayıs	7.73 PB	1.82 PB	9.55 PB
Haziran	4.23 PB	1.13 PB	5.36 PB
Temmuz	4.56 PB	1.24 PB	5.81 PB
Ağustos	3.41 PB	1.02 PB	4.43 PB
Eylül	4.99 PB	1.43 PB	6.41 PB
Ekim	7.98 PB	1.81 PB	9.8 PB
Kasım	7.5 PB	1.8 PB	9.3 PB
Aralık	9.1 PB	2.01 PB	11.12 PB
Yıl Toplam (PB)	75.41 PB	18.69 PB	94.09 PB
Yıl Toplam (GB)	75.410.000 GB	18.690.000 GB	94.090.000 GB[11]

Tablo 5: ULAKNET Toplam Küresel İnternet Geçişi İstatistiği

Büyük veri kavramının ülkemizdeki veri alışverişi istatistiklerine bakıldığında devasa boyutlarda olduğu görülmektedir. Büyük veri kavramını bugün ülkemiz için baktığımızda 9.3 Petabyte olarak görebiliriz. Ancak gelecek yıllarda artacağı tahmin edilen veri hacmi ile büyük veri kavramı Petabyte boyutlarını da geçip Exabyte boyutlarında olabilir. Önemli olacak konu büyük verinin hacminin yanında bu verinin Google Flu Trends'teki gibi verimliliği arttıracak şekillerde işlenebilmesidir.

[11] 2019 yılında alınan ve gönderilen toplam veri boyutu 94.090.000 Gigabyte boyutundadır. Bu oranı 32GB'lık USB Bellekler ile karşılamak için toplam 2.940.312 adet belleğe ihtiyaç duyulmaktadır.

İKİNCİ BÖLÜM: ÜLKELERDEKİ VERİ GİZLİLİĞİ POLİTİKALARI

2.1. ABD Veri Gizliliği Politikaları

Amerika Birleşik Devletleri'nde, veri gizliliği konusunda ilk adım ABD Başkanı Lyndon B. Johnson tarafında 1966 yılında bilgi özgürlüğü yasasının (FOIA[12]) onaylamasıyla başlamıştır. Yasa yürürlüğe girdikten 1 yıl sonra uygulamaya koyulmuştur. Yasada devlet ve mahkeme kendi alanındaki dosyalara erişim haklarına sahip olmasına rağmen adli dosyalar ve hükümet dosyaları bu yasa kapsamına girmemektedir (Martin, 2019). 12 Ağustos 1974 yılında dönemin Amerikan Başkanı Gerald Ford, Amerikan halkının gizlilik haklarına olan güçlü inancı dolayısıyla kongrede şu sözleri ifade etmiştir: "*Yasa dışı gizlice dinlemeler, hatalar veya ihlaller olmayacaktır. Hem hükümet hem de özel faaliyetlerde yasadışı gizlilik ihlalini önlemek için sert yasalar için çalışılacaktır"*. Başkan Ford'un kongrede ifade ettiği bu sözler sonrasında, 31 Aralık 1974 tarihinde Gizlilik Yasasını imzalayarak yasayı onaylar. Gizlilik yasası, bireylere bazı haklar tanımıştır (*1974 Privacy Act*, 2019):

- Varlığı gizli tutulan federal hükümetlerin kişisel kayıt tutma sistemleri bulunmayacaktır.
- Federal hükümet kişisel bilgi bulunması gereken durumlarda sadece gerekli bilgileri toplayacaktır.
- Bireyler, kendileri hakkında hangi bilgilerin tutulduğu konusunda, bilgileri görme ve doğruluğunu sorgulama imkanına sahip olacaktır.
- Bir amaç için toplanan bilgiler, bireyin rızası olmadan başka bir amaçla kullanılamaz.

1974 tarihinde çıkarılan Federal Gizlilik Yasası zamanında yenilikçi ve etkili olmasına rağmen, Amerika Birleşik Devletleri diğer ülkelerle tamamen karşılaştırılabilir bir veri koruma ajansına sahip değildir (Flaherty, 1989: 305). Çünkü Gerald Ford'un çıkarmış olduğu yasalar bürokrasiye karşı çıkanlar sebebiyle bir gizlilik koruma komisyonu oluşturmadı (Flaherty, 1989: 306). Bir gizlilik komisyonu kurmanın başlıca nedenlerinden biri mevcut veriyi, devlet veri bankalarının ve kişisel bilgi sistemlerinin

[12] FOIA (Freedom of Information Act) açılımına sahip olan yasa, Federal Özgürlük Yasası olarak da tanımlanmaktadır.

kurulmasının denetlenmesi ve kişisel gizlilik ihlallerinin incelenmesi için idari süreci oluşturmaktadır (Flaherty, 1989: 311).

1966	Bilgi Özgürlüğü Yasası kabul edildi.
1970	Adil Kredi Raporlama Yasası yürürlüğe girdi
Temmuz 1973	Sağlık, Eğitim ve Refah Bakanlığı, Sekreterin Otomatik Kişisel Veri Sistemleri Danışma Komitesi raporunda "Kayıtlar, Bilgisayarlar ve Vatandaşların Hakları" konusunu yayınladı.
1974	Bilgi Edinme Özgürlüğü Yasasında yapılan önemli değişiklikler. Aile Eğitim Hakları ve Gizlilik Yasası, hükümetin kişisel eğitim kayıtlarına erişimini düzenler ve öğrencilere kendi kayıtlarına erişim izni verir.
1 Mayıs 1974	Senatör Samuel J. Ervin, bir Federal Gizlilik Kurulu oluşturmak için 3418'i tanıttı.
31 Aralık 1974	Başkan Gerald Ford, Gizlilik Yasasını imzaladı.
8 Nisan 1975	Savunma Bakanlığı, Savunma Gizlilik Kurulunu oluşturdu.
Temmuz 1975	Yönetim ve Bütçe Dairesi, Gizlilik Yasası'nın uygulanmasına ilişkin kılavuz ilkeler yayınlar.
27 Eylül 1975	Gizlilik Yasası yürürlüğe girer.
1976	Vergi Reformu Yasası, devletin vergi bilgilerinin başka amaçlarla kullanımını kısıtlar.
Ocak 1977	Başkan Carter, Beyaz Saray Telekomünikasyon Politikası Ofisinin sorumluluklarını Ulusal Telekomünikasyon ve Bilgiye devretti
Temmuz 1977	Gizlilik Koruma Çalışma Komisyonu Raporu oluşturuldu.
Kasım 1978	Mali Gizlilik Kanunu, bireysel mali kayıtlara federal erişimi düzenler.
2 Nisan 1979	Başkan Jimmy Carter, tıbbi, araştırma ve mali kayıtlar ile haber medyası notları ve materyalleri hakkında gizlilik mevzuatı önerir.
18 Nisan 1979	Yönetim ve Bütçe Ofisi, eşleşen programların yürütülmesi için kurallar yayınlar.

1980	Evrak Azaltma Yasası, hükümetin kişisel bilgi toplamasını azaltmaya çalışıyor. Gizlilik Koruma Yasası, devlet dairelerinin haber aramalarını denetlemek için tasarlanmıştır.
Ocak 1980	Yönetim ve Bütçe Ofisi, Bilgi ve Düzenleme İşleri Ofisini oluşturur.
1982	Borç Toplama Yasası, federal hükümetin kötü borçlarla ilgili kişisel bilgileri kredi kuruluşlarına salıvermesini düzenler.
14 Mayıs 1982	Yönetim ve Bütçe Ofisi sayıları bilgisayar eşleştirme programlarını yürütmek için ek kılavuzları gözden geçirdi.
15-16 Aralık 1982	Senatör William S. Cohen bilgisayar eşleşmesi üzerine yapılan duruşmalara başkanlık ediyor.
7-8 Haziran 1983	Kongre Üyesi Glenn English, Gizlilik Yasası hakkındaki ilk gözetim oturumuna başkanlık ediyor.
1984	Kablolu İletişim Politikası Yasası, abonelerin kablolu televizyona karşı gizliliğini korumak için önlemler içerir.
1985	Yönetim ve Bütçe Ofisi, "Federal Bilgi Kaynaklarının Yönetimi" konulu A-130 sayılı Genelge'yi yayınladı.
1986	Teknoloji Değerlendirme Ofisi, "Elektronik Kayıt Sistemleri ve Bireysel Gizlilik" üzerine bir rapor yayınlar. Elektronik Haberleşme Gizlilik Yasası, belirli elektronik haberleşmelerin ele geçirilmesini yasaklar ve bu tür haberleşmelerin ele geçirilmesini ve kullanımını Jaw uygulama amaçları için düzenler.
16 Eylül 1986	Senatör William S. Cohen bilgisayar eşleşmesi üzerine duruşmalara başkanlık ediyor.
1987	1987 tarihli Bilgisayar Güvenliği Yasası, federal bilgisayar sistemlerinde hassas kişisel bilgilerin güvenliğini korumayı amaçlamaktadır.
23 Haziran 1987	Temsilciler Meclisi bilgisayar eşleştirme mevzuatı hakkında duruşma yapar.

1988	Video Gizlilik Koruması Yasası, video kaset kiralama mağazalarının sahip olduğu bireysel borçluların kayıtlarını korur.
18 Ekim 1988	Bilgisayar Eşleşmesini kontrol etmek için Bilgisayar Eşleştirme ve Gizlilik Koruma Yasası kabul edildi.

Tablo 1: Amerika Birleşik Devletleri Federal Veri Koruma Mevzuatı Kronolojisi (Flaherty, 1989)

Gizlilik ile ilgili çalışmalar dönemin teknolojilerine göre düzenlenmiştir. Örneğin 1984 yılında kablolu iletişim yasası çıkartılmıştır. Bireyler bu yasa ile kablolu televizyon sahibi olmak için hizmet sağlayıcılarına verdikleri kişisel bilgilerinin korunması amaçlanmıştır. 1987 tarihinde çıkarılan Bilgisayar Güvenliği Yasası, bilgisayar sistemlerinde hassas verilere karşı koruma sağlamayı amaçlamıştır. Bu yasa ticari kuruluşlara bazı zorunluluklar getirmiştir (Glickman, 1988);

- Her ticari kuruluş bilgisayar sistemlerinin yönetimi, kullanımı veya işletimi ile ilgili tüm çalışanlara büro tarafından geliştirilen yönergeler uyarınca bilgisayar güvenliği alanında zorunlu eğitimlerin verilmesi gerekmektedir.
- Her ticari kuruluş bir bilgisayar sistemi ile hassas bilgilerin güvenliği ve gizliliği için bir plan oluşturması gerekmektedir.

Amerika Birleşik Devletleri'nde, ülkenin büyüklüğü ve kapsamına göre halkın gözetimi sorunları karşılaştırılabilir. Yönetim ve Bütçe Ofisi, ABD'de bulunan Federal Hükümetin en büyük tek üretici, tüketici olduğundan bilgi gizliliğine uymadığını belirtmektedir. Bunun en temel nedeni federal hükümetin en büyük bilgisayar ve bilgi teknoloji üreticisi olmasıdır. Hükümetin gözetimini sınırlandırmak için veri korumanın uygulanması ve bunun için hangi yöntemin benimsenmesi gerektiğini belirlemek zor bir iştir (Flaherty, 1989: 314). Bu gibi durumlardan dolayı ABD içerisinde her eyalet ana kurallara bağlı kalarak kendi gizlilik yasalarını oluşturmuştur (*Data Security Laws | State Government*, 2020).

- *Alabama Eyaleti**;*** Eyalet içerisindeki belediye veya belediyelere bağlı olan kuruluşların kişilerden aldığı hassas ve tanımlayıcı bilgilerin kanunlarda belirtildiği şekilde yeterli güvenlik önemlerini almasını ve korumasını sağlamaktadır (*Data Security Laws | State Government*, 2020).

- *Arizona Eyaleti;* Devlet kurumu veya devlet bütçesiyle kurulmuş kurumların eyalet çapında bir bilgi güvenliği ve gizlilik ofisi kurması gerekmektedir. Ofisin, eyalette bilgi teknolojisi güvenliği için stratejik planlama ve koordinasyon hizmeti vermesi sağlanır. Aynı zamanda ofisin, bilgi teknolojisi güvenliği için operasyonel sorumluluğu sürdürmesi gerekmektedir. Güvenlik ofisinin tüm bu faaliyetleri yürütebilmesi için bir bilgi merkezi güvenliği yetkilisi atamalıdır. Yetkili, güvenlik ve gizlilik uyumunu incelemesi, ortaya çıkabilecek olan güvenlik risklerin tespit edilmesi ve azaltılmasını standartlara uygun bir şekilde sağlaması gerekmektedir (*Data Security Laws | State Government*, 2020).

- *Kaliforniya Eyaleti;* Tüm devlet kurumlarının kritik altyapı bilgilerini güvence altına almak ve siber güvenlik stratejisi standartlarını uygulaması ve geliştirilmesi için Siber Güvenlik Merkezi kurulur. Yıllık olarak bir güvenlik değerlendirmesi yapılarak tüzükte belirtildiği şekilde Bilgi Güvenliği Dairesi Başkanlığı tarafından geliştirilen bilgi güvenliği programına uyulmaktadır. Merkez, siber olaylara müdahale ekibini oluşturur ve tüm devlet departmanlarının belirtilen kurallara uymalarını ve çalışanların bilgi güvenliği konusundaki farkındalıklarının arttırılması amaçlanmaktadır (*Data Security Laws | State Government*, 2020).

- *Kolorado Eyaleti;* Siber güvenlik kapsamını devlet kurumları, yüksek öğretim kurumları (üniversiteler) ve genel kurumlar şeklinde belirlemiştir. Eyalet Siber Güvenlik Konseyi kurar ve eyalet güvenliği ve siber güvenlikle ilgili görevlerin koordinasyonunu sağlar. Ayrıca konsey, kamu kurumlarının veri sistemleri üzerinde sağlanan güvenliğin benimsenmesi ve uygulanmasının yararları konusunda değerlendirmeye teşvik eder. Kamu ve yüksek öğretim kurumları bilgi güvenliği politikalarını, bilgi güvenliği yetkisi tarafından geliştirilen standartlaştırılmış kılavuzları kullanarak bir bilgi güvenliği planı geliştirmesi gerekmektedir. Eyalet bilgi güvenliği yetkilisinin görevlerini şu şekilde açıklamaktadır;
    - Kurumlar için bilgi güvenliği politikaları, standartları ve yönergeleri geliştirmek ve güncellemek,

- Bilgi güvenliği kanunu gereğince, devlet kurumların geliştirdiği bilgi güvenliği planlarının politikalara, standartlara ve yönergelere dahil edilerek uyulmasını sağlamak,
- Kurallara uyumluluğu ve düzenlemeleri sağlamak için kamu kurumlarından doğrudan yapılan bilgi güvenliği denetimlerini değerlendirmektir (*Data Security Laws | State Government,* 2020).

- *Connecticut Eyaleti;* Başta devlet kurumları ve devletin çeşitli hizmetleri gerçekleştirmesi için sözleşme yaptığı yüklenici firmaların bu yasaya bağlı olduğu belirtilmektedir. Connecticut yasasında, gizli bilgilerin korunması için kapsamlı bir veri güvenlik programı uygulaması ve sürdürmesi gerekmektedir. Ayrıca Politika ve Yönetim Ofisi mevcut yasaların yanında ilave güvenlik önlemleri talep edebilmektedir (*Data Security Laws | State Government,* 2020).

- *Florida Eyaleti;* Veri gizliliği yasası, devlet kurumlarının her üç yılda bir kapsamlı bir risk değerlendirmesi yapması, bir olay müdahale ekibi oluşturmak ve raporlama sürecini sağlamak, güvenlik ve siber güvenlik bilincini sağlamak üzere, devletin Bilgi Teknolojisi Güvenlik Standartları ve Devlet Teknoloji Ajansının belirlediği şekilde süreçlere uyulması ve tüm devlet kurumu çalışanlarına eğitim verilmesi gerekmektedir (*Data Security Laws | State Government,* 2020).

- *Georgia Eyaleti;* Georgia Teknoloji Otoritesine göre eyalet içerisindeki tüm ticari kuruluşların teknoloji güvenlik standartlarını ve hizmetlerini oluşturmak ve teknoloji denetimlerinin yapılması gerekmektedir (*Data Security Laws | State Government,* 2020).

- *Idaho Eyaleti;* Devlet kurumları kapsamında, valiliğin bulunduğu merkezde bilgi teknoloji ofisi kurulur. Eyalet içerisindeki tüm bilgi teknolojisi hizmetlerini ve siber güvenlik politikaları denetlemek için Bilgi Teknolojisi Hizmetleri yöneticilerini tayin eder. Riskleri azaltmak ve devlet çalışanlarının zorunlu eğitiminde siber güvenlik politikaları, bilgi güvenliği ihtiyaçları ve güvenlik açığı taramaları gibi uygulamalar içermektedir (*Data Security Laws | State Government,* 2020).

- *Illinois Eyaleti;* Eyalet içerisinde stratejik planlamayı kolaylaştırmak ve koordinasyonu sağlaması amacıyla Bilgi Güvenliği Ofisi kurmaktadır. Ticari kuruluşlar riskleri belirlenmesi için yapılan değerlendirme sonrasında eyalet çapında bilgi güvenliği

farkındalığı "eğitim programlarının koordine edilmesi gibi statüde ayrıntılı olarak belirtilen hizmetleri sunmaktadır. Siber güvenlik denetimi özellikle büyük miktarda kişisel bilgi içeren ticari kuruluşlara odaklanarak siber güvenlik uygulamalarının gözden geçirilmesi sağlanmaktadır (*Data Security Laws | State Government*, 2020).

- *Indiana Eyaleti;* Devlet kurumları, teknoloji ofisinin belirlediği kurallara uyması gerekmektedir:
    - Teknoloji ofisi projelerin güvenliğini, personel ve harcamalarını gözden geçirecektir.
    - Bilgi teknolojisinin devlet yönetimlerinde etkin ve güvenli kullanılması için politikalar, prosedürler ve kılavuzların geliştirilmesini sürdürülecektir.
    - Ofis, devlet kurumları personeli için bilgi teknolojisi yönergeleri hakkında tavsiyelerde bulunacaktır.
    - Talep üzerine devlet kurumları içindeki bilgi teknolojisi faaliyetlerinin periyodik olarak yönetim incelemeleri yapılmaktadır (*Data Security Laws | State Government*, 2020).

- *Kansas Eyaleti;* Bölge içerisindeki yönetim şubesi kurumları, bilgi güvenliği programlarının yürürlükte olmasını sağlamak için yürütme organı başkanlarının görev almasını, tespit edilen tehditlerden veri ve bilgi teknolojisi kaynaklarına yönelik tehditlerin azaltılması, ortadan kaldırılması veya kurtarılması için güvenlik politikaları, standartlar ve uygun maliyetli önlemlerin uygulanması; veri ve bilgi teknolojisi sistemlerini ve hizmetlerini tedarik etmek için teklif özellikleri için ticari kuruluşun talebindeki siber güvenlik gerekliliklerini Bilgi Güvenliği Merkezine 16 Ekim tarihine kadar siber güvenlik değerlendirme raporunu sunması gerekmektedir (*Data Security Laws | State Government*, 2020).

- *Kentucky Eyaleti;* Bölge içerisindeki devlet kurumları ve devlet kurumları olmayan üçüncü kurumlar, kişisel bilgilerin tutulduğu şekil ne olursa olsun, kişisel bilgileri koruyan veya başka şekilde elinde tutan bir kuruluş veya bağlı olmayan üçüncü taraf güvenlik önlemlerine karşı koruma sağlamak için uygun düzeltici önlemlerin alınması da dahil olmak üzere güvenlik prosedürlerini ve uygulamalarını uygulamalı, sürdürmeli ve güncellemelidir. Eyalet hükümeti yürütme organının örgütsel birimleri

tarafından kurulan ve uygulanan makul güvenliği, ihlal soruşturması prosedürleri ve uygulamaları, Ortak Zenginlik Ofisi tarafından oluşturulan ilgili işletme politikalarına uygun olmalıdır. Eyalet hükümeti yürütme organının örgütsel birimleri tarafından kurulan ve uygulanan standart güvenliği, ihlal soruşturması prosedürleri ve uygulamaları Milletler Topluluğu Teknoloji Ofisi tarafından oluşturulan işletme politikalarına uygun olmalıdır (*Data Security Laws | State Government,* 2020).

- *Maryland Eyaleti;* veri güvenliği yasasının kapsamını şu şekilde belirlemiştir:
    - Devlet kurumu olan yüksek öğretim kurumu, ilçe, belediye,
    - Bölgesel, iki şehirli veya çok ülkeli ticari kuruluşlar,
    - İlçe eğitim kurulu, kamu kuruluşu, otorite veya devletin diğer herhangi bir siyasi alt kurumu.

Ticari kuruluşlar, toplandığı kişisel bilgilerin ve faaliyetlerinin niteliğine uygun bir yazılı bilgi güvenliği politikası ve uygun güvenlik prosedürlerini uygulamalı ve sürdürmelidir. Yazılı sözleşme veya anlaşma yoluyla üçüncü tarafların, bağlı olmayan üçüncü taraflara açıklanan kişisel bilgilerin niteliğine uygun güvenlik prosedürleri ve uygulamaları gerçekleştirmelerini ve sürdürmelerini istenmektedir (*Data Security Laws | State Government,* 2020).

- *Massachusetts Eyaleti;* Veri güvenliği yasasını, kamu kuruluşları içerisinde yer alan yasama organı, adli şube, genel avukat, devlet sekreteri, devlet saymanı ve devlet denetçisi olarak belirlemektedir. Milletvekili kullanıcıların kişisel bilgilerini kendi bölümlerini korumak için tasarlanmış kural ve düzenlemeleri kabul etmesi ve kendi bölümleri tarafından sağlanan hizmetlerin boyutunu, kapsamını ve türünü, buradaki kaynak miktarını, depolanan verilerin miktarını ve hem tüketici hem de çalışan bilgilerinin gizliliğe olan ihtiyacı dolayısıyla dikkate almalıdır (*Data Security Laws | State Government,* 2020).

- *Minnesota Eyaleti;* Eyalet içerisindeki yüksek öğretim kurumu, eyalet kolejleri ve üniversiteleri dahil olmak üzere devlet yönetiminin yürütme organındaki devlet kurumlarını kapsaması şeklinde tanımlanmaktadır. Eyalet Baş Bilgi Görevlisi, internete bağlı devlet kurumlarının ağlardaki veri ve sistemlerini korumak için gerekli standartları

oluşturması ve yürütmesi amacıyla donanım ve yazılım desteğini sağlar (*Data Security Laws | State Government,* 2020).

- *Montana Eyaleti***;** Veri güvenliği yasasının kapsamını kişisel bilgileri tutan her devlet kurumu olarak belirlemiştir. Eyalet, devlet kurumunun federal ya da eyalet hukuku kapsamındaki görevlerini yerine getirmek için gerekli olan kişisel bilgilerin kullanılmasına izin verirken, kişisel bilgileri korumak için tüzükte belirtildiği gibi prosedürler geliştirilmelidir (*Data Security Laws | State Government,* 2020).

- *New York Eyaleti;* Devlet kurumlarının koordinasyonu, yönetimi, güvenliği, gizliliği, programın etkinliğini, satın almayı ve teknolojinin yayılmasını geliştirmek için yapılan politikalar, planlar ve programlar geliştirmeleri konusunda danışmanlık yardımında bulunulması bilgi teknolojileri ofisi tarafından sağlanır. Ayrıca yasa ofise, teknoloji incelemeleri yapma, teknolojiye ilişkin yönetimin etkinliğini arttırmaya yönelik önerileri verme ve eyalet kurumları tarafından teknoloji satın alımlarının gözden geçirmesi ve koordine edilmesi ve gerektiğinde aşağıdaki unsurları gözden geçirme yetkisi verir:

  - Ülke çapında stratejik teknoloji planı ile kurum teknolojisi planının tutarlılığını değerlendirmek,
  - Eyalet çapında teknoloji standartları ve bilgi gizliliğinin korunması; gizli kayıtların güvenliği, kamuya açık bilgilerin doğru bir şekilde dağıtılması şeklindedir.

Bilgi Ofisi, eyalet devleti ağlarının ve coğrafi bilgi sistemlerinin güvenliği ile ilgili eyalet çapında politikalar, standartlar, programlar ve hizmetler dahil olmak üzere, tercih edilen teknoloji standartları ve güvenliği de dahil olmak üzere ülke çapında teknoloji politikaları oluşturma yetkisi verir. Ayrıca, güvenlik açıklarının tanımlanması ve azaltılması, siber olayları caydırmak ve bunlara müdahale etmek ve devlet içinde siber güvenlik bilincini teşvik etmek amacıyla bunlarla devlet hükümetinin siber güvenlik altyapısının korunmasını sağlar (*Data Security Laws | State Government,* 2020).

- *Kuzey Carolina Eyaleti;* Devlet kurumlarında bulunan Baş Bilgi Sorumlusu, iletişim ve şifreleme teknolojileri dahil olmak üzere, devletin dağıtılmış bilgi teknolojisi varlıklarının işlevselliğini, güvenliğini ve birlikte çalışabilirliğini en üst düzeye çıkarmak

için bilgi teknolojisi güvenliği için ülke çapında bir standartlar kümesi oluşturacaktır. Eyalet Baş Bilgi Sorumlusu, yıllık olarak güvenlik standartlarını gözden geçirip yenileyecektir. Bu işlevin bir parçası olarak bilgi sorumlusu, bu standartların ve uygulamaların eyalet çapında güvenlik ve şifreleme gereksinimlerini karşılayıp karşılamadığını belirlemek için çeşitli devlet kurumları arasında yürürlükte olan güvenlik standartlarını ve uygulamalarını periyodik olarak gözden geçirir. Bilgi sorumlusu, bu madde uyarınca kabul edilen güvenlik standartlarına uymayan herhangi bir eyalet kurumunun bilgi teknolojisi güvenliğini sağlama sorumluluğunu doğrudan üstlenebilir (*Data Security Laws | State Government*, 2020).

- *Ohio Eyaleti;* Ohio eyalet içerisindeki devlet kurumları tarafından tutulan ve imha edilen kişisel bilgilerin güvenliği için politikalar ve prosedürlerin Baş Bilgi Görevlisi tarafından oluşturulur. Oluşturulan politikalar ve prosedürlerin uygulanması baş bilgi görevlisinin sorumluluğu altındadır. Ayrıca bilgi görevlisi kurumların bilişim teknolojisi güvenlik stratejilerini planlama ve gözden geçirme konusunda yardımcı olmaktadır (*Data Security Laws | State Government*, 2020).

- *Oklahoma Eyaleti;* Veri gizliliği politikası bilgi teknolojilerini kullanan tüm devlet kurumları şeklinde kapsamını belirlemiştir. Bilgi sistemiyle ilişkili güvenlik açıklarını belirlemek için yıllık bilgi güvenliği risk değerlendirmesi yapılır. Nihai bilgi güvenliği risk değerlendirme raporu, değerlendirilen her devlet kurumu için bilgi güvenliği açıklarını tespit etmeli, önceliklendirmeli ve belgelemelidir. Bu alt bölümün gerekliliklerine uyulmaması, BT için ödenecek desteğin kurumdan geri alınmasına neden olabilir. Devlet kurumları ya Bilgi Servisleri Bölümü tarafından oluşturulan standart güvenlik risk değerlendirmesini ya da ISO / IEC 17799[13] standartlarını karşılayan ve Ulusal Standartlar ve Teknoloji Özel Yayın 800-30 (NIST SP800-30) Enstitüsünü kullanarak üçüncü taraf risk değerlendirmesini kullanırlar. Bilgi Hizmetleri Bölümü tarafından işleme alınır ve onaylanır (*Data Security Laws | State Government*, 2020).

- *Oregon Eyaleti;* Veri gizliliği kapsamını devlet kurumları şeklinde belirleyerek İdari Hizmetler Bölümünün aldığı kararlara bağlı olarak;

[13] ISO/IEC 17799: 2005, bir organizasyonda bilgi güvenliği yönetimini başlatmak, uygulamak, sürdürmek ve iyileştirmek için kılavuz ilkeler belirlenmiştir.

- Kurumlar tarafından işletilen bilgi sistemlerinin güvenliğini gözden geçirmek ve doğrulamak;
- Güvenlik tehditlerini tanımlamak ve bunlara tepki vermek için durum ağı trafiğini izlemek;
- Bilgi sistemlerinin saldırı, bozulma veya bilgi sistemlerinin kullanılabilirliğini, bütünlüğünü veya gizliliğini tehdit eden diğer herhangi bir olayı veya bilgi sistemlerinde saklanan bilgileri tehdit etmek amacıyla duyarlılığını değerlendirmek ve bunlara cevap vermek amacıyla kurum bilgi sistemlerinin güvenlik açığı değerlendirmeleri yapılmalıdır (*Data Security Laws | State Government*, 2020).

- *Güney Carolina Eyaleti;* Veri gizliliği politikasını devlet kurumları çerçevesinde sınırlandırmıştır ve İdare Bakanlığı tarafından geliştirilen siber güvenlik politikalarını, kurallarını ve standartlarını uygulanmalıdır. Bakanlık, uygunluğu izlemek için gerektiğinde devlet kurumları hakkında denetimler yapabilir. Talep üzerine, yüksek öğrenim sağlayan kamu kurumları, teknik kolejler, siyasi alt bölümler ve yarı-devlet kurumlarının siber güvenlik politikaları ve yönergelerinin yanında standartlarının kurum tarafından karşılandığını İdare Bakanlığına göstermesi gerekmektedir. Eyalet veri gizliliği politikalarına yargı ve yasama kurumlarını dahil etmemiştir (*Data Security Laws | State Government*, 2020).

- *Texas Eyaleti;* Devlet kurumları tarafından toplanan bilgilerin kontrolünü ve güvenliğini geliştirmek için eyalet çapında bir veri koordinatörünün istihdam edilmesini sağlar. Bilgi güvenliğini artırmak için bilgi yönetimi ve analizini geliştirmek üzere devlet kurumları arasında en iyi uygulamaları geliştirmek ve uygulamak için eyalet çapında veri koordinatörünü gerektirir (*Data Security Laws | State Government*, 2020).

- *Utah Eyaleti;* Mevcut devlet yönetimi veri güvenliği politikalarını gözden geçirecek, devam eden riskleri değerlendirecek, yeni ve yerel riskleri yerel kurumlara bildirecek, veri ihlali uygulamalarını koordine edecek, devlet hükümeti için en iyi uygulama önerileri geliştirecek bir veri güvenliği yönetim konseyi oluşturur. Her devlet kurumu için bir baş bilgi güvenliği görevlisinin işe alınması ve eğitilmesi sağlanır (*Data Security Laws | State Government*, 2020).

- *Vermount Eyaleti;* Dijital Hizmetler Kurumlarına, eyalet hükümeti dahilindeki siber güvenlik hizmetleri sunma yetkisi verir ve Genel Kurul'a BT ve siber güvenlik hakkında stratejik bir plan hazırlaması gerekir. Kurumların BT ve siber güvenlik politikaları geliştirmesini ve bazı yeni BT projeleri için bir güvenlik değerlendirmesi yapması gerekmektedir (*Data Security Laws | State Government,* 2020).

- *Virginia Eyaleti;* Her ticari kurum ve departman tuttukları elektronik verilerin korunmasından sorumludur ve kanun maddesi 2.2.2009'da belirtilen şekilde, toplumun bilgi teknolojisi güvenliği ve risk yönetimi programının gerekliliklerine uymalı ve bilinen tüm olayları rapor etmelidir. Bilgi Güvenliği Ofisi, güvenlik risklerini değerlendirmek, uygun güvenlik önlemlerini belirlemek ve devlet elektronik bilgilerin güvenlik denetimlerini gerçekleştirmek için politikalar, prosedürler ve standartların geliştirilmesini sağlar. Bu tür politikalar, prosedürler ve standartlar, toplumun yürütme, yasama ve yargı organları ile bağımsız kurum ve yüksek öğrenim kurumlarına uygulanacaktır. Bilgi Güvenliği Ofisi, güvenlik denetimlerinin kapsamını ve bu güvenlik denetimlerinin sıklığını ele alan politikalar, prosedürler ve standartlar da geliştirmelidir. Ek olarak, Bilgi Güvenliği Ofisi her yürütme organı şubesinin yıllık siber güvenlik politikalarını kapsamlı olarak gözden geçirmektedir (*Data Security Laws | State Government,* 2020).

- *Washington Eyaleti;* Teknoloji Hizmetleri Kurumu, devletin bilgi teknolojisi sistemleri ve altyapısında işlem gören, depolanan veya işlenen bilgilerin gizliliğini, kullanılabilirliğini ve bütünlüğünü sağlamak için güvenlik standartları ve politikaları oluşturması gerekmektedir. Ayrıca, güvenlik olaylarını algılamak, raporlamak ve yanıt vermek için bir işlem uygulanmasını sağlar. Teknoloji Hizmetleri Kurumu Başkanı, eyalet baş bilgi güvenliği görevlisi atayacaktır. Her devlet kurumu, yüksek öğrenim kurumu, yasama organı ve yargının, ofisin güvenlik standartlarına ve politikalarına bağlı bir bilgi teknolojisi güvenlik programı geliştirmesini gerektirir. Her devlet kurumundan programını yıllık olarak gözden geçirmesini ve güncellemesini ve programın ofisin güvenlik standartlarına ve politikalarına uygun olduğunu ofise onaylatması gerekir. Devlet kurumlarının en az üç yılda bir bağımsız uyum denetimi yaptırması gerekir (*Data Security Laws | State Government,* 2020).

- *Batı Virginia;* Baş Bilgi Sorumlusu, bilgi sistemleri, veri ve iletişim altyapılarını korumak için uygulamaların benimsenmesini tanımlayan ve gerektiren politikalar,

prosedürler, standartlar ve yasal kurallar geliştirmeye yetkilidir. Devlet veri tabanlarının ve veri iletişiminin korunmasına ilişkin tüm yürütme organlarının yıllık güvenlik denetimlerini sağlar (*Data Security Laws | State Government,* 2020).

- *Wyoming Eyaleti;* Her kurumun veri toplama, erişim, güvenlik ve kullanımı ile ilgili bir politika benimsemesini, uygulamasını ve sürdürmesini gerekmektedir. Politika, asgari olarak, geçerli federal ve eyalet yasalarına uygun olarak, devlet başkanı bilgi subayı tarafından belirlenen standartlara uymalı ve aşağıdakileri içermelidir:

  - Bir kurum tarafından istenen, toplanan veya saklanan tüm verilerin bir envanteri ve açıklaması,
  - Verilere erişmek için yetkilendirme ve doğrulama mekanizmaları,
  - Çalışan eğitimi ve veri şifreleme dahil, idari, fiziksel ve mantıksal güvenlik önlemleri,
  - Gizlilik ve güvenlik uygunluk standartları,
  - İhlal bildirimi ve azaltma prosedürleri dahil olmak üzere veri güvenliği olaylarının tanımlanması ve bunlara müdahale edilmesi için işlemler,
  - Mevcut yasaya göre, verilerin imhası ve iletişimi için işlemler gerekmektedir (*Data Security Laws | State Government,* 2020).

2.1.1 ABD Veri Gizliliği Politikalarının Değerlendirilmesi

ABD veri güvenliği konusunda uyguladığı yasalara bakıldığında, ülkenin yönetim şekli gereği her eyaletin temelde aynı fakat uygulamada farklı yollar izlediği görülmektedir. 29 eyaletin veri gizliliği konusunda bulunduğu eyaleti kapsayacak şekilde bir Bilgi Güvenliği Ofisi oluşturduğu görülmektedir. Devlet tarafından oluşturulan bu kurum, eyalet içerisindeki diğer ticari kuruluşların veri güvenliği konusundaki uygulamalarını denetleme ve belirli ilkeler doğrultusunda ticari kuruluşların veri güvenliği kavramını benimsemesi rolünü üstlenmektedir. Denetlemelerin yapılması sonucunda ticari kuruluşların veri güvenliği uygulamaları, verilerin saklandığı sistemler, altyapı gibi teknik ihtiyaçlar raporlanarak belirlenir. Bunun yanında sistemleri kullanan kullanıcıların veri güvenliğine karşı eğitim programlarının belirlenmesi de söz konusudur. Örneğin California ve Batı Virginia eyaletleri her yıl düzenli olarak altyapı sistemlerinin denetlenerek örnek olay çalışmalarının yapılması gerektiğini belirtilmektedir. Washington eyaleti yıllık olarak yapılan denetlemelerin yanı sıra üç

yılda bir bağımsız denetçi tarafından denetlenmesi gerektiğini belirtmektedir. Yine benzer zaman aralığına sahip Florida eyaleti, üç yılda bir ticari kuruluşların detaylı incelenmesi gerektiğinden bahsetmektedir. Oklahoma eyaleti veri güvenliği konusunda diğer eyaletlerden farklı olarak uluslararası bir standart olan ISO 17799'u benimsemiştir. Eyalet içerisindeki ticari kuruluşların uluslararası standartlara sahip olabilmesi için bazı ilkelere sahip olması gerekmektedir (*ISO/IEC 17799*, 2005):

- Güvenlik politikası,
- Varlık yönetimi,
- İnsan kaynaklarının güvenliği,
- Fiziksel ve çevresel güvenlik,
- İletişim ve operasyon güvenliği,
- Bilgi sistemlerinin edinimi, geliştirilmesi ve bakımı,
- Bilgi güvenliği olay yönetimi şeklinde belirlenmiştir.

ISO 17799'da belirtilen ilkelerde sadece sayısal anlamda bir veri güvenliğinden bahsedilmediği görülmektedir. Verilerin depolandığı sunucuların fiziksel güvenlikleri de büyük önem taşımaktadır. Bu ilkelere uygulayan kurumlar sadece eyalet çapında değil aynı zamanda uluslararası bir standarda sahip olmaktadır.

2.2. Almanya Veri Gizliliği Politikaları

Günümüz Avrupa'sında yürürlükte olan kişisel verilerin korunması kanunu, iletişim araçlarının bu kadar gelişmediği ve sadece telgraf, mektup gibi iletişim araçlarının mevcut olduğu dönemlere dayanır. Özellikle 1892 yıllarında Bismark Anayasasında temel hak ve özgürlüklere ilişkin madde bulunmamaktadır.

İlk olarak gizliliğin korunması kavramı, 1950 yılında kabul edilen ve 1953 yılında yürürlüğe giren Avrupa İnsan Hakları Sözleşmesinde, özel hayatın korunması ve gizliliği 8'inci madde de "*herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkında sahiptir*" şeklinde ifade edilmiştir. Maddenin ikinci bölümde ise *"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"* şeklinde açıklanarak gizliliği yalnızca yasa ile

belirlenmiş tedbirler doğrultusunda incelenebileceği belirtilmiştir (Avrupa İnsan Hakları Sözleşmesi, 1950: 11). Avrupa İnsan Hakları Sözleşmesi, özel hayatın korunması ve gizliliğine yönelik ihlallere karşı kişilere güvence sağlamaktadır (Şen, 1993: 141).

1970	Hessen eyaleti bir veri koruması kabul eder.
1973	Federal İçişleri Bakanlığı, Federal Meclis'e veri korumaya ilişkin bir taslak yasa tasarısı sunmaktadır.
1975	Spiros Simitis, Hessen eyaleti için Veri Koruma Başkanı oldu.
27 Ocak 1977	Federal Veri Koruma Yasası (BDSG) yürürlüğe girdi.
1978	Hans Peter Bull federal Veri Koruması Başkanı oldu.
1979	Heinrich Weyer, Kuzey Ren-Vestfalya eyaleti için Veri Koruma Başkanı oldu (Eylül 1987'ye kadar).
1 Ekim 1982	Hristiyan bir Demokrat olan Helmut Kohl, Sosyal Demokrat Helmut Schmidt'in yerine şansölye olarak yer alıyor.
1983	Reinhold Baumann federal Veri Koruma Komiseri oldu.
6 Mart 1983	Hristiyan Demokrat parti ve Özgür Demokrat parti koalisyon hükümetinin kurulması.
15 Aralık 1983	Federal Anayasa Mahkemesinin nüfus sayımı davasındaki kararı, bilgi edinme konusunda kendi kendini belirleme konusunda anayasal bir haktır.
11 Kasım 1986	Hesse, Veri Koruma Yasasını revize etti.
1988	Kuzey Ren-Vestfalya Veri Koruma Yasasını revize etti. Alfred Einwag federal Veri Koruma Başkanı oldu.

Tablo 2:Batı Almanya Veri Koruma Mevzuatı Kronolojisi (Flaherty, 1989)

Batı Almanya, kapsamlı veri koruma mevzuatı getiren tek federal hükümet sistemidir. 1970 yılında Hessen eyaleti, kamu idaresindeki otomatik veri işlemenin sosyal sonuçlarıyla ilgili endişelere yanıt olarak genel bir veri koruma yasası çıkartılan ilk yargı alanıydı. Çünkü kamu sektöründeki kişisel bilgilerin yüzde 80 ile 90'ı devlet düzeyinde

tutulmaktadır (Flaherty, 1989: 22). Kişisel veri ve bilgisayar tartışmaları 1960'lı yılların sonlarına doğru başlamış olmasına rağmen federal bir kanunun çıkması on yılı bulmuştur. İçişleri Bakanlığı federal meclise veri korumaya ilişkin yasa tasarını 1973 yılında sunmuştur. Ancak 1970 yıllarda Batı Almanya'daki siyasi partiler arasında veri koruması konusunda büyük bir görüş ayrılığı bulunmamaktadır (Flaherty, 1989: 24). Özellikle ABD Gizlilik Yasası üzerindeki tartışmalar Batı Almanya'dakilere kıyasla küçük kalmaktadır.

İlk Federal Komisyon Üyesi olan Profesör Hans Peter Bull, veri koruması tartışmaların sonucunda kabul edilen yeni kuralların, yönetimin uygulamada tereddüt edeceğini şu şekilde belirtmiştir (Flaherty, 1989: 24): *"Bağımsız bir dış denetim oluşturmanın temel nedenlerinde biri, insanların veri ihlalleri konusundaki şikayetlerini ele alabilmeleri için özel bir merkezin gerekli olacağı ve yöneticilerin idare ile bağlantısı olmayan güvenilir kişilerin olması gerekecektir."* Diğer ülkelerde uygulanan bağımsız denetim merkezleri, örnekleri sebebiyle Bull'un fikrini güçlü bir şekilde desteklemektedir. 1975'te Hessen'in Veri Koruma Başkanı olan Frankfurt Üniversitesinde Profesör olan Spires Simitis de Bull'un düşüncelerine yakın fikirlere sahipti.

1976 yılında yapılan bir ankette kamuoyu, kişisel verilerin kamu tarafından olmasa da özel sektör tarafından kötüye kullanılmasından çok fazla korktuğunu belirtmiştir. Bull, yaşamlarını tüm kişilik özelliklerini gizli olarak geçirmek isteyen bireyler için gizlilik korumasının yasanın merkezinde olacağını ifade etmiştir (Flaherty, 1989: 34): *"Federal Koruma Kanunu verileri korumak için bir yasa değildir. Aksine amacı vatandaşı korumaktır. Bu gerçekler yasaların başlıklarında yeterince açık değildir. Anayasada öngörüldüğü gibi bireyin kişiliği konusu ne zaman ihlal edilir? sorusunun cevabı genel düzenlemeler ile gelemez. Bu tür ihlaller her zaman bireyin özel koşullarına bağlı olmalıdır. Bu gerçeklere göre Alman yasa koyucular, kişilerin kişilikleri ile ilgili bireysel haklarını korumaya karar verdiler."*

1978'den beri Batı Almanya'da temel veri koruma yasaları çerçevesi oluşturulmuş ve veri koruma çalışmaları daha rutin hale gelmiştir. Hem federal hem de eyalet seviyesindeki uygulamaların ilk on yılı başarılı olmuştur. 1986 yılında Hessen'in

veri koruma yasası ilk yürürlüğe koyulduğu tarihten 18 yıl sonra yenilenmiştir. 1988 Kuzey Ren Vestfalya'da 10 yıl sonra veri koruma kanunu yenilemiştir.

1988'den günümüze kadar geçen süreçte özellikle internet teknolojinin gelişmesi dünyada bilginin sınırlarını ortadan kaldırmış ve veri güvenliği konusunda daha fazla tedbirlerin alınmasına yol açmıştır. 2016 yılında Avrupa Birliği veri gizliliği yasası, veriyi toplayanlar ve işleyenlere yönelik sorumluluk yükleyen veri güvenliği yönetmeliğini hazırlamış ve kamuya sunmuştur. 2016 yayımlanan veri güvenliği yönetmeliğinde bazı önemli tanımlara yer verilmektedir (General Data Protection Regulation, 2016: 2):

- Kişisel veri: *"Tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir (veri sahibi); tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir"*,
- İşletme Faaliyeti: *"otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisidir"*,
- Kişisel Veri İhlali: *"iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlalidir"*,
- Genetik Veri: *"bir gerçek kişinin fizyoloji veya sağlığı ile ilgili eşsiz bilgiler sağlayan ve özellikle söz konusu gerçek kişiden alınan bir biyolojik numunenin analizinden kaynaklanan ve söz konusu kişinin kalıtım yoluyla alınan veya kazanılan özelliklerine ilişkin kişisel verilerdir"*,
- Biyometrik Veri: *"yüz görüntüleri verileri gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel verilerdir"*

- Sağlık Verileri: *"sağlık hizmetlerinin sağlanması da dahil olmak üzere bir gerçek kişinin sağlık durumuyla ilgili bilgilerin açıklandığı, söz konusu gerçek kişinin fiziksel veya ruhsal sağlığına ilişkin kişisel verilerdir"* şeklinde açıklanmaktadır.

Avrupa Birliğinin veri güvenliği ve gizliliği ile ilgili yapmış olduğu tanımlara bakıldığında, veri kavramında kişiyi veya kişileri ilgilendiren birçok unsuru barındırmaktadır. Kişinin kimlik bilgileriyle birlikte sağlık verileri gibi spesifik bilgileri de ihtiva etmektedir. Tanımda yer verilen işletme faaliyeti, veri işleyen olarak ifade edilmektedir. Başka bir deyişle veri üzerinde toplama, analiz ve hatta verilerin silinmesi sürecine kadarki tüm faaliyetleri sürdüren olarak tanımlanmaktadır.

Yönetmeliğin kişisel verilerin işlenmesine ilişkin ilkeler bölümünde, kişisel verilerin hukuka uygun, adil ve şeffaf olarak işlenmesi gerektiği, bunun yanında verileri toplamada veya işlemede yetkisiz kişilerin eline geçmesini önlemek amacıyla güvenliğin sağlanması gerektiğinden bahsedilmektedir. Ayrıca kişi verilerinin işlenmesine rıza göstermelidir. Rıza gösteren veri sahibi rızasından geri dönebilmektedir (General Data Protection Regulation, 2016: 6).

Günümüzde yeni medya ortamlarını sadece yetişkinler değil çocuk yaşlardaki bireyler de kullanmaktadır. Yönetmeliğin sekizinci maddesinde çocuk yaşlardaki bireylere ait kişisel verilerin işlenebilmesi için on altı yaş şartı getirilmiştir. Bu yaştan daha küçük olması halinde çocuk üzerinde velayeti bulunan kişi verilerin işlenmesi için onay verebilmektedir. Ek olarak Avrupa Birliği üye devletleri bu yönetmelik maddesinde belirtilen on altı yaş sınırını en az on üç yaşa kadar düşürebilme esnekliği tanınmıştır (General Data Protection Regulation, 2016: 8).

Özel kategori veri sınıfına giren ırk, etnik köken, siyasi görüşler, dini ve felsefi bilgiler ile kişinin biyometrik ve sağlık verilerinin işlenmesi yasaktır. Ancak bir kişi bu verilerinin işlenmesine rıza göstermesi halinde veya kişinin hukuki olarak rıza gösteremeyecek durumlardan birinin oluşması halinde verinin işlenmesine onay verilir (General Data Protection Regulation, 2016: 9).

Kişinin rızası doğrultusunda ticari kuruluşlara vermiş olduğu verilerin içeriği, kişinin kendisini doğru şekilde yansıtmadığını düşünüyor ise kişi, kendisi ile ilgili olan verinin içeriğinin düzeltilmesi için talepte bulunabilmektedir. Diğer yandan kişi, ticari

kuruluştan kişisel verilerinin silinmesi talebinde de bulunabilmektedir. Ticari kuruluş, veri sahibinin bu talebi üzerine herhangi bir gecikmeye yer vermeden silmekle yükümlüdür (General Data Protection Regulation, 2016: 15).

Ticari kuruluşların veri sahiplerinden topladıkları verileri başka kurumlara aktarabilme hakkına sahiptir. Ancak verilerin aktarılma süreci sonrasında veri sahiplerinin hakları ve özgürlükleri olumsuz yönde etkilenemez (General Data Protection Regulation, 2016: 17).

Veri sahibinden toplanan tüm bu veriler veri sorumluları ve veri işleyenlerin elinde olduğundan, herhangi bir gizlilik ihlaline karşı denetlenmesi gerektiğinden yönetmelik, kontrolörlere sorumluluk yüklemiştir (General Data Protection Regulation, 2016: 21): *"işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, işleme faaliyetinin bu Tüzük uyarınca gerçekleştirilmesini sağlamak ve bu şekilde gerçekleştirildiğini gösterebilmek için uygun teknik ve düzenlemeye ilişkin tedbirler uygular. Bu tedbirler gözden geçirilir ve gerektiğinde, güncellenir."*

Yönetmelik, ticari kuruluşlara verilerin korunmasına ilişkin sorumluluk yüklerken bir yandan verilerin gizliliği konusunda kısıtlamalara gitmiştir. Devletlerin milli güvenlik, savunma, kamu güvenliği gibi konular söz konusu olduğunda bu bilgiler devlet kurumları tarafından talep edilebilmektedir. Ancak yönetmelik bu durumun hukuki süreçlere zarar vermeyecek şekilde uygulanması gerektiğini belirtmiştir (General Data Protection Regulation, 2016: 20).

Verilerin güvenliği her ne kadar kontrolörler tarafından denetlense de her zaman veri gizliliğinin ihlal edilebilme ihtimali bulunmaktadır. Dolayısıyla bir veri ihlalinde, özellikle kişisel haklar ve özgürlükler açısından verilerin ihlal edilmesi sebebiyle veri sahibine gecikme olmaksızın bilgi verilmelidir. Verilen bilgi sonucunda veri sahibi, veriyi depolamak veya güvenliğini sağlamakla yükümlü olan ticari kuruma, yönetmeliğin 79. maddesine göre yetkili merciler ile mahkemelere şikâyette bulunabilir ve tazminat hakkını kullanabilmektedir (General Data Protection Regulation, 2016: 41).

2.3. Türkiye Veri Gizliliği Politikaları

Günümüzde veri gizliliği politikaları çalışmalarında medya platformlarını da kapsayan düzenlemeler yapılmaktadır. Veri gizliliği kavramı sadece sayısal ortamı değil tüm yazılı basılı ortamı da kapsamaktadır. Çünkü iletişim teknolojilerindeki gelişmelerin ilk dönemlerinde içerikler yazılı basılı ortamlarda iletilmekteydi.

Posta Nezareti 23 Ekim 1840 yılından İstanbul'un Eminönü semtindeki Yeni Cami avlusunda bulunan Cizyehane dairesinde Postahane-i Amire olarak açılmıştır. İlk posta teşkilatının bu mevkide kurulmasının sebebi İstanbul'un tam ortasında yer aldığından hem kara hem de deniz postaları için ideal bir konumda olmasıdır (Yurtoğlu, 2016). 1939 yılında ise PTT adını alarak ulaştırma bakanlığına bağlanmıştır (*PTT Hakkında*, 2019).

Günümüzdeki gibi veri gizliliği politikalarına sahip olunmayan dönemlerde, özellikle PTT gibi devlet kurumları mektup gibi içeriğin gizli tutulmasına yönelik tedbirler alınmıştır. Örneğin 1950 yılında çıkarılan 7451 sayılı posta kanununda, posta gizliliği başlığındaki 16'ıncı maddesinde: *"Kendilerine posta servisinde bir iş verilmiş olanların, belli kişilerin posta münasebetlerini açığa vurmaları, kapalı mektupları açmaları, içlerinde ne olduğunu araştırmaları veya haberleşme kağıtlarındaki yazılar hakkında üçüncü kişilere bilgi vermeleri veyahut herhangi birinin bunları yapmasına meydan bırakmaları yasaktır."* şeklinde belirtilerek verilerinin korunması amaçlanmıştır (Posta Kanunu, 1950: 4). 1973 yılında geldiğimizde devlet, 1950 yılında çıkarılmış olan posta kanunu referans alınarak içerisindeki maddelerin açıklamalarını genişletilmiştir. 1973 yılında çıkarılan 14505 sayılı posta kanunda, posta gizliliği ve bunu gözetleyecek olanlar başlığı altında 8'inci maddede: *"Kendilerine posta servisinde bir iş verilmiş olanların, belli kişilerin posta ilişkilerini açığa vurmaları, kapalı mektupları açmaları, içlerinde ne bulunduğunu araştırmaları veya haberleşme kağıtlarındaki yazılar hakkında üçüncü kişilere bilgi vermeleri yahut herhangi birine bunları yapmaya imkan bırakmaları yasaktır.*

1- Aşağıda belirtilenler kendilerine posta servisinde iş verilmiş sayılırlar:

a) Her derecedeki PTT personeli;

b) Posta acentaları ve posta pulu satıcıları;

c) Yurtdışından gelen postaların açılışında hazır bulunan ve gümrüklü posta gönderilerinin muayenesini yapan gümrük memurları;

d) PTT'nin diğer idare ve taşıma ortaklıklarıyla posta işlerinin görülmesi konusunda yaptığı sözleşme şartlarına göre bunların posta hizmeti ile görevlendirdiği personeli;

e) PTT'nin posta taşıma müteahhitleri ve bunların vekilleri veya mutemet olarak gösterdikleri adamları ile posta taşıyan araçların sürücü, şoför ve kaptanları;

f) Yetkili PTT personelinin izni ile veya izni olmaksızın Tüzüğün 7'inci maddesi gereğince postaya yardım edenlerin bütünü.

2- Gönderici ile alıcıdan ve bunların tayin ettikleri vekillerinden başkaları üçüncü kişi sayılır." şeklinde belirtilmiştir (Posta Kanunu, 1973: 3). Maddede verilen posta içeriğinin gizliliği hakkındaki tanımda, bahsedilen iş verilmiş olanlar ve üçüncü kişiler alt maddeler halinde belirtilerek, maddenin bahsetmiş olduğu kapsam açıklamıştır. Görüldüğü gibi teknolojinin günümüzdeki kadar gelişmemesine rağmen, veri kavramının o dönemlerde de kişisel veri olarak karşımıza çıkmasının yanında, bu verilerin korunması konusuna da özen gösterilmiştir.

Teknolojinin insan hayatına girmesi ve yeni medya ortamlarının artması, kişisel verilerin birçok ortamda paylaşılmasını beraberinde getirmiştir. Örneğin internet üzerinden verilen bir sipariş sırasında kredi kartı ve kimlik numarası gibi bilgiler alınmaktadır. Bu veriler, geçmiş dönemlerde olduğu gibi devlet kurumları ile sınırlı kalmayıp ticari kuruluşlar tarafından da toplanır hale gelmiştir. Dolayısıyla bu kadar verinin çeşitli kurumlarca toplanması toplum içerisinde, "veriler gerçekten gizli kalıyor mu?" sorusunu ortaya çıkarmaktadır. Veri gizliliği politikalarının günümüz dinamiklerine karşı yetersiz kalması sebebiyle 2016 yılında "Kişisel Verileri Koruma Kurumu Başkanlığı" kurulmuş ve aynı yıl 6698 sayılı kişisel verilerin korunması kanunu çıkarılmıştır. Kanun veri sorumlusu, veri işleyen ve verilerin yurt dışına aktarılması kavramlarını getirmiştir. Kişisel verileri korunması kanunu (KVKK), veri sorumlusunu, *"Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder"* şeklinde tanımlamıştır (*Veri Sorumlusu ve Veri İşleyen*, 2018: 2). Tanımdan veri sorumlusunun gerçek veya tüzel kişi olabileceği ve hukuki açıdan bir farklılığın olmadığı

anlaşılmaktadır. Veri sorumluları şu konularda karar alabilmektedir (*Veri Sorumlusu ve Veri İşleyen*, 2018: 4):

- Kişisel verilerin alınması ve nasıl alınacağı,
- Alınan verilerin türleri,
- Verilerin hangi amaçla kullanılacağını,
- Kimlerin kişisel verilerini alabileceğini,
- Verilerin kimler ile paylaşılıp, paylaşılmayacağına karar vermek,
- Verilerin saklanma süresine karar verebilmektedir.

Veri sorumlularına bağlı olarak çalışan veri işleyenleri de kişisel verilerin korunması kanunu şu şekilde açıklamaktadır: *"Veri işleyen ise, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişiler"* olarak tanımlamaktadır (*Veri Sorumlusu ve Veri İşleyen*, 2018: 2).

Kişisel verileri koruma kanunun 5'inci maddesinde: *"Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez."* ifadesiyle veri işleme usulü açıklanmıştır. Bu ifadeyle kanun maddesi, kişinin verileri işlenmeden önce rızasının gerektiğini belirtmiştir. Ancak 5'inci maddenin 2. fıkrasında (Kişisel Verilerin Korunması Kanunu, 2016: 2): *Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:*

a) Kanunlarda açıkça öngörülmesi.

b) 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.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

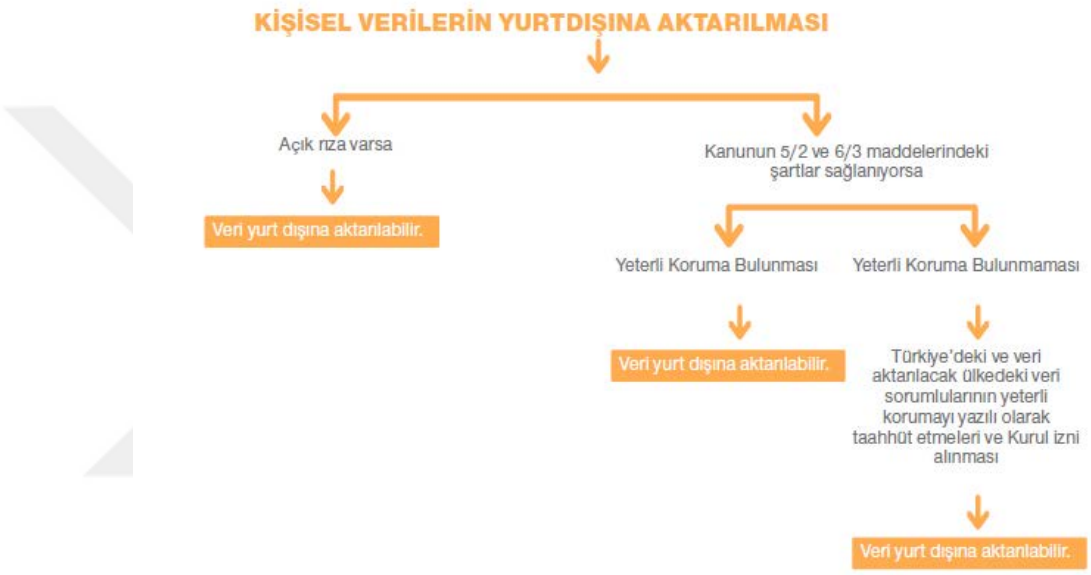
ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" durumlarında

verilerin işlenmesi için kişinin açık rızasına gerek duyulmamaktadır. Yukarıda belirtilen hallerde kişinin rızasının alınmasına gerek duyulmadan verilerin işlenmesi, verilerin yurt dışına aktarılması sürecinde de yer almaktadır. Ancak kanun, kişisel veriler yurtdışına aktarılmadan önce verilerin aktarılacağı noktanın korunacağı konusunda garanti istemektedir. Aksi taktirde veri sorumlularının verileri aktarmadan önce verilerin korunacağı konusunda taahhüt vermeleri ve KVKK kurulundan izin alması gerekmektedir.



Şekil 2: Verilerin Yurtdışına Aktarılması Süreci

2.3.1 İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun Değişikliği Teklifi

4 Nisan 2007 tarihinde, 5651 sayılı *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi"* yasasıyla internet ortamındaki içeriklerin devlet tarafından denetlenmesini sağlamıştır. 21 Temmuz 2020 tarihinde TBMM Kanunlar ve Kararlar Başkanlığı aracılıyla 5651 sayılı kanuna değişiklik teklifi getirilmiştir. Kanun değişikliği teklifine gerekçelerine bakıldığında, kişilerin sosyal ağlara ilgilerinin artması sebebiyle sosyal ağ sağlayıcılarının bu veriler üzerinden milyarlarca dolar gelir elde etmektedir. Ancak sosyal ağ sağlayıcıları yüksek gelir elde etmelerine rağmen kişilik haklarının

korunması konusunda gerekli önlemleri alamadıkları ve devletlerin haklı taleplerine direnç göstermeleri kanun değişikliği teklifinin verilmesinin başlıca nedeni olarak görülmektedir. İnternetin geniş ve anonim ortamı sebebiyle kişilerin fikir ve düşüncelerine, dinlerine veya milletlerine sahte hesaplar yoluyla hakaret etmesine imkân vermektedir. Belirtilen sebeplerden dolayı Almanya ve Fransa gibi ülkelerde yasalaşmış olan internet kanunları kaynak olarak gösterilmiştir. Değişiklik teklifinde kişilik haklarının ve özel hayatın gizliliğinin korunmasının yanı sıra ihlal durumlarında devlet ve temsilcisi aracılıyla etkili bir mekanizma kurulması amaçlanmaktadır. (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi, 2020).

Madde 1'de sosyal ağ sağlayıcıları kanunda yeniden tanımlanmıştır. Düzenlemeye göre *"kullanıcıların internet ortamında sosyal etkileşim amacıyla metin, görüntü, ses, konum gibi içeriklerin oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek veya tüzel kişiler"* şeklinde tanımlama yapılmıştır. (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi, 2020).

Madde 2'de devletin muhataplarına (erişim sağlayıcı, sosyal ağ sağlayıcı veya temsilci) yapacağı bildirimlerin nasıl iletileceği konusunda bir düzenleme yapılmıştır. Özellikle eposta benzeri yöntemlerin yaygın olması sebebiyle dijital iletişim yöntemleri ile bildirim yapılmaktadır. Ancak 2014 yılında dijital iletişim yönteminin geçerli bir bildirim olmadığına ilişkin yapılan itiraz danıştay tarafından incelenerek internet ortamına yönelik *"özel bildirim usulü tebligat"* şeklinde bildirimleri yapılacağı kabul edilmiştir. Yeni düzenlemeyle yurt dışında bulunan servis sağlayıcılarına yurt dışına özgü bir biçimde bildirim sağlanabilmesi için devlet kurumu tarafından üçüncü fıkrada belirtilen usullere göre bildirim yapılacağı belirtilmiştir (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi, 2020).

Madde 3'te kanun maddesinde belirtilen yer sağlayıcıların yükümlülüklerine yerine getirmediği taktirde haklarında on bin Türk Lirası ile yüz bin Türk Lirası arasında

idari para cezası uygulanması öngörülmüştür. Yeni düzenlemeyle ceza miktarı bir milyon Türk Lirası ile on milyon Türk Lirasına yükseltilmiştir. (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi, 2020).

Madde 4'te 5651 sayılı kanunun 8'inci maddesinde, internet ortamında yer alan çocukların cinsel istismarı, fuhuş, kumar ve uyuşturucu kullanımının kolaylaştırılması gibi yayınlarla ilgili mücadele edilebilmesi amacıyla erişim engeli kararı uygulanabilmektedir. Düzenleme teklifiyle erişim engelleme işlemlerinin içerik sağlayıcılara bırakılmıştır. (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi, 2020).

Madde 5'te ifade ve haber alma özgürlüğünün güvence altına alınması amacıyla içeriğin çıkarılması hususunda karar verme imkânı bulunmaktadır. Ayrıca yetkili makamlarca engelleme kararına rağmen arama motorları içerisinde kişiye ait olan içerikler bulunmaktadır. Düzenlemeyle hem içeriğin kaldırılması hem de kişiye ait olan içeriğin arama motorları ile ilişkilendirilmemesi kararı verilebilmektedir (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi, 2020).

Madde 6'da devletin yetkili mercileri ile sosyal medya sağlayıcıları arasında etkin bir mekanizma sağlanabilmesi amacıyla sosyal medya sağlayıcıları Türkiye'de en az bir kişiyi temsilci olarak belirleyecektir. Belirlenen temsilci gerçek kişi ise Türk vatandaşı olmak zorundadır. Temsilci olarak belirlenen kişinin bilgilerinin yetkili mercilere bildirilmesi gerekmektedir. Bildirimde bulunmayan sosyal medya sağlayıcıları hakkında çeşitli cezalar uygulanır (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi, 2020):

- Yetkili merci tarafından uyarı yapılır ve otuz gün içerisinde bildirim işlemi gerçekleşmediği taktirde on milyon Türk Lirası idari para cezası verilmektedir.
- Ceza sonrasında otuz gün içerisinde bildirimde bulunmayan sosyal medya sağlayıcısına otuz milyon Türk Lirası para cezasına verilmektedir.

- İkinci kez verilmiş olan para cezasından sonra otuz gün içerisinde bildirim işlemini yerine getirmeyen sosyal medya sağlayıcılarına reklam verme, sözleşme ve para transferi kısıtlamaları getirilmektedir.
- Kısıtlamalar sonrasında üç ay içerisinde bildirimde bulunmaya sosyal medya sağlayıcılarının internet bant genişliklerinin yüzde elli oranında azaltılması için yetkili merci tarafından Sulh Ceza Hakimliğine başvurulabilir. Başvurunun kabulü halinde otuz gün içerisinde sosyal medya sağlayıcı tarafından bildirim yapılmadığı taktirde Sulh Ceza Hakimliğine internet bant genişliğinin yüzde doksanına kadar kısıtlanması konusunda başvuru yapılabilmektedir.

Yukarıdaki cezai işlemlerden herhangi birinin uygulanması sonrasında temsilci bildirimini yapılması halinde idari para cezasının dörtte biri tahsil edilir ve sosyal medya sağlayıcıda bulunan reklam, sözleşme ve para transfer yasağı ve trafik bant genişliği kısıtlamaları sona erdirilmektedir (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi, 2020).

Sosyal medya sağlayıcıları kişilerden gelen başvuruları en geç 48 saat içerisinde cevaplamakla yükümlüdür. Temsilci kişiye olumsuz cevap verdiği taktirde gerekçesini belirtmekle yükümlüdür. Yükümlülüklerini yerine getirme sosyal ağ sağlayıcısına beş milyon Türk Lirası idari para cezası verilmektedir (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi, 2020).

Türkiye'de günlük erişimi bir milyondan fazla olan sosyal ağ sağlayıcıları altı ayda bir istatistik ve kategorik bilgiler içeren raporları yetkili mercilere ulaştırması gerekmektedir. Ayrıca bir milyondan fazla erişimi olan sosyal medya sağlayıcıları Türkiye'deki kullanıcıların verilerinin Türkiye'deki sunucularda barındırılması yönünde belirtilmiştir. Bu yükümlülüklerin yerine getirmeyen sosyal ağ sağlayıcısına on milyon Türk Lirası idari para cezası verilmektedir (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi, 2020).

Ek olarak hukuka aykırı olarak belirlenen içeriğin kaldırılması yönünde sosyal ağ sağlayıcılarına bildirimde bulunulmasına rağmen 24 saat içerisinde kaldırılmayan veya

engellenmeyen içeriklerden doğan zararlar sosyal ağ sağlayıcı tarafından tazmin edilmektedir. Bir yıl içerisinde yeniden ihlal yapan sosyal medya sağlayıcısının cezasını bir kat arttırılması şeklinde karar verilmektedir. (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi, 2020).

İnternet ortamında yapılan yayınların düzenlenmesine ilişkin yapılan kanun teklifi incelendiğinde, sosyal medya platformların farklı ülkelerde bulunması sebebiyle yaşanan kişilik ihlalleri sonucunda devletin yaptırımları kısıtlanmaktadır. Bu sebeple kanun teklifi Türkiye'de bir milyondan fazla kullanıcısı olan platformların Türkiye içerisinde temsilcilik açmasını zorunlu kılmaktadır. Ayrıca temsilci olarak belirlenen kişi, gerçek kişi sıfatını taşıyorsa Türk vatandaşı olması zorunludur. Temsilcilik açmayan platformlara kanunda belirtildiği gibi belirli aşamalarda cezalar kesilecektir. Eğer sosyal medya sağlayıcı bir temsilci görevlendirilmiş ve yetkili makamlara bildirim sağlanmış ise platformun faaliyetleri boyunca kişilerden gelen şikayetleri en geç 48 saat içerisinde olumlu veya olumsuz şekilde yanıtlamak zorundadır. Bununla beraber yürürlükte olan kanunda mahkeme tarafından engelleme kararı erişim sağlayıcı tarafından uygulanırken yeni değişiklik teklifi ile bildirim yapıldıktan sonra 24 saat içerisinde temsilci tarafından içeriğin kaldırılması şeklinde düzenlenmiştir. Ayrıca temsilci altı ayda bir olmak üzere Türkçe raporlar hazırlayacak ve yetkili mercilere teslim edecektir. Kanunla ilgili nitel değerlendirme tartışma ve sonuç kısmında yapılmıştır.

ÜÇÜNCÜ BÖLÜM: SOSYAL MEDYA PLATFORMLARININ GİZLİLİK POLİTİKALARININ İNCELENMESİ

3.1. Araştırma Yöntemi

Bu tez çalışmasında sosyal medya platformlarının sahip olduğu gizlilik sözleşmeleri, betimsel araştırma yönetmelerinden olan doküman inceleme yöntemiyle incelenmiştir. Doküman incelemesi nitel bir çalışma yöntemi olması dolayısıyla elde edilen veriler yorumlanacaktır. Dokümanlarda yazı temelli kaynaklar kullanılacaktır. Sosyal medya platformlarının resmi internet sitelerinde paylaşmış olduğu gizlilik politikaları birincil kaynak olarak kullanılacaktır. Türkiye uygulamakta olduğu veri gizliliği politikaları hem birincil kaynak olan devlet kaynakları olarak belirlenmiştir. Çalışmanın örnekleminde Facebook, Whatsapp, Twitter ve Youtube gibi platformların gizlilik sözleşmeleri şeklinde belirlenmiştir. Çalışma güncel tarihli gizlilik sözleşmelerinin incelenmesiyle sınırlandırılmıştır:

- Facebook 19 Nisan 2018,
- Whatsapp 25 Ağustos 2016 ve Ocak 2020,
- Twitter 25 Mayıs 2018,
- Youtube 22 Ocak 2019 tarihli gizlilik sözleşmeleri ele alınmıştır.

Tezin amaçları şu şekilde belirlenmiştir:

- Sosyal medya platformlarının gizlilik sözleşmeleri hangi şartları içermektedir?
- Sosyal medya platformları tarafından toplanan veriler hangi amaçlar için kullanılmaktadır?
- Türkiye'deki veri koruma kanunları ve uygulamaları nelerdir?

Çalışmada elde edilen sonuçlar doğrultusunda sözleşmelerin hangi verileri hangi amaçla topladıklarının yanında bu verilerin kullanıcılar tarafındaki öneminin neler olduğu ve Türkiye'nin uygulamakta olduğu veri gizliliği politikalarının diğer devletlere göre hangi aşamada olduğu şeklinde cevaplar yorumlanacaktır.

3.2. Facebook ve Instagram Gizlilik Sözleşmesi

Facebook şirketi 2004 yılında kurulduğunda tek bir isim hakkına sahip iken bugün firmanın sahip olduğu birçok alt marka mevcuttur. Bunlar Instagram, Messanger,

Whatsapp gibi milyonlarca kişinin kullandığı markalardır. Yeni medya platformlarının topladıkları veri hakkında ayrıntılı bilgi büyük veri başlığı içerisinde verilmişti. Facebook gibi ticari firmaların faaliyetlerini devam ettirebilmesi için kanunlara uyma zorunluğu yanında kazanç da sağlaması gerekmektedir. Bunu da ücretsiz olarak sunduğu sosyal medya hizmetinden topladığı verileri çalışma ortaklarıyla paylaşarak ve aldığı reklamlar vasıtasıyla sağlamaktadır.

Son güncellenme tarihi 19 Nisan 2018 olan Facebook veri gizliliği sözleşmesinin maddeleri baz alınarak kişisel veri gizliliği incelenmiştir (*Facebook Veri İlkesi*, 2018).

Facebook ve Instagram aynı firma tarafından yönetildiğinden her iki markanın veri gizlilik politikaları aynıdır. Facebook veri ilkesi sözleşmesinin "Ne tür bilgiler topluyoruz" maddesinin ilk cümlesinde Facebook ürünlerinin sunulması için kullanıcıların verilerinin işlenmesi gerektiğinden bahsetmektedir. Özellikle Facebook kullanılırken bir resmin çekildiği tarih, bulunulan konum bilgisi gibi ögelerin mevcut olan kaynaklarının tanımlanmasını sağlayan meta verilerden aşağıdakileri kaydedilmektedir (Küçük & Al, 2001);

- Paylaşılan içerikler,
- Kullanıcıların mesajlaşma geçmişi,
- Kişiler, sayfalar ve paylaşımda kullanılan etiketler,
- Kullanıcının rehber paylaşımları,
- Kullanıcının çekilen fotoğrafları sonrasında kullanılmak için kaydedilmektedir.

Facebook yukarıda sayılan tüm kaydedilen verilerin firma tarafından kullanılacağını belirtirken, bunun yanında, verilerin kullanıcının arkadaş veya takipçi kitlesiyle paylaşma kararını kullanıcıya bırakmaktadır. Özellikle dini inanç, siyasi görüşler, etnik köken gibi konuların kitle ile paylaşımı yine kullanıcı tarafından belirlenmektedir. Facebook üzerinden yapılacak finansal işlemde şirket şu bilgilerin alınacağını belirtmiştir:

- Kredi kartı veya banka kartı numarası,
- Ödeme bilgileri
- Kimlik doğrulama bilgileri ve
- İletişim bilgilerini, verilerin toplanması kapsamına almaktadır.

Facebook'un kullanım platformları sadece web ortamında sınırlı değildir. Akıllı telefonlar, akıllı televizyonlar, bilgisayarlar, tabletler yani hemen hemen tüm platformlarda mevcuttur. Facebook tüm bu cihazlardaki verilerin toplanıp hepsinin birbiri ile karşılaştırılıp analiz edileceğini belirtmiştir. Cihaz bilgilerinin toplanmasında şu noktalar ön plana çıkmaktadır;

- İşletim sistemi,
- Donanım ve yazılım sürümleri,
- Pil seviyesi,
- Wifi, bluetooth sinyal güçleri, bağlantı hızları ve çevredeki diğer cihazların sinyalleri,
- Kullanılan internet tarayıcısı türü,
- Cihaz içerisindeki uygulamalar, dosya adları ve türleri,
- GPS konumu,
- Mobil operatör, internet servis sağlayıcısı ve ip adresleri[14]
- Cep telefonu numarası gibi birçok veri Facebook tarafından toplanmaktadır.

Facebook son kullanıcıların yanında diğer şirketler ile çalışma ortaklığı yapmaktadır. Bu ortaklar, Facebook'un oluşturduğu API'ler[15] ve SDK'leri[16] kullanarak yazımlardan gelen veriler, sadece çalışma ortakları değil Facebook tarafından da depolanmaktadır. Facebook, üçüncü kişilerin verileri kullanımında "Üçüncü Taraf Hizmete Uygulanan Koşul ve İlkelere" tabi olacağını belirtmiştir. Ek olarak kullanıcılar Facebook verilerini üçüncü kişilere paylaşılması konusunda karar verebilecektir. Facebook veri gizliliği politikasının üçüncü kişilere entegrasyonu başlığı altında, *"Kötüye kullanımın önüne geçmek için geliştiricilerin veri erişimini daha da sınırlandırıyoruz. Örneğin; son 3 ayda uygulamasını kullanmadığınız geliştiricilerin, Facebook ve*

[14] IP adresi, açılımı (Internet Protocol) olan ve anlamı itibariyle, internete bağlanabilen tüm cihazların belirli protokollerde belirli bir adrese sahip olması gerekmektedir. IP adresleri IP versiyon 4 (IPv4) veya yeni nesil IP versiyon 6 (IPv6) şeklinde tanımlanabilir. İkisi arasındaki temel fark IPv4'te 4 milyar kadar sisteme tanımlanabilirken IPv6 ise 340 trilyon sisteme tanımlama yapabilir. Türkiye ve Dünya'nın birçok yerinde IPv4 kullanılmaktadır.

[15] API (Application Programming Interface) şeklinde açılımı olan ve bir uygulamanın sahip olduğu yetenekleri başka bir uygulamanın kullanabilmesidir. Örneğin Google Haritaları bir havayolu firması alarak, uygulamayı kendi uçuş rotalarını göstermek için kullanabilir.

[16] SDK (Software Development Kit) açılımına sahip olan sistem, geliştiricilerin uygulama oluşturmak için kullandıkları araç setidir. SDK'ler içerisinde API'leri kapsamaktadır ve bu kitler hepsi bir arada olduğundan uygulama geliştiricisine kolaylık sağlamaktadır.

Instagram verilerinize erişimi kaldırıyoruz" şeklinde bilgi verilmektedir (*Facebook Veri İlkesi*, 2018). Facebook verilerin paylaşılması konusunda sadece geliştiriciler değil devletin kolluk kuvvetleri ile de çalışacağını belirtmiştir. Çalışma, arama izni, mahkeme emri gibi talepleri yerine getirmek amacıyla veri paylaşımı politikasının uygulanacağını belirtmiştir. Dünya genelinde veri kullanımı konusunda standart sözleşme hükümlerine uyulduğunu belirtmektedir. Verilerin ABD ve diğer ülkelere aktarımı konusunda da kullanıcılardan izin aldıkları belirtilmektedir.

Facebook bu verileri sadece üçüncü kişilerin kullanımı için sunmamaktadır. Şirket içerideki araştırma ve geliştirme faaliyetleri içinde bu verileri kullanmaktadır. Örneğin konum verileri depolayan Facebook kullanıcının yakınındaki aktiviteler için uyarabilmektedir. Ayrıca kullanıcının eylemleri sonucunda oluşan verilerden ilgi alanlarını belirleyip kişiselleştirilmiş reklamlar da sunabilmektedir.

Facebook gizlilik sözleşmesi genel olarak değerlendirildiğinde kullanıcıların gerçek anlamda birçok verisinin alındığı gözlemlenmektedir. Özellikle bu verilerin kendi kullanımı dışında üçüncü şahıslar ile de paylaşması hususu dikkat edilmesi noktalardan biridir. Facebook gizlilik sözleşmesinin de *"Hiçbir bilginizi kimseye satmıyoruz ve asla satmayacağız"* şeklinde ifade edilmektedir. Buna rağmen Facebook'un 50 milyon kullanıcının verilerini Cambridge Analytica'ya satması şirketin veri gizliliği konusundaki tutumunu göstermiştir (Hansen, 2018).

3.3. Whatsapp Gizlilik Sözleşmesi

Whatsapp, daha önce Yahoo şirketinde yirmi yıl çalışan Jan Koum ve Biran Acton tarafından 2009 yılında piyasaya çıkarılmıştır. Whatsapp markasının doğuşu, "What's Up" ifadesi üzerinde yapılan kelime oyunu ile ortaya çıkmıştır. İlk zamanlarda sadece sms gibi mesajlaşma uygulaması iken bugün sesli ve görüntülü sohbetin yanında, dosya gönderimlerini de destekleyen bir platform haline gelen Whatsapp, 2014 yılında Facebook tarafından satın alınmış olup aynı adla faaliyetlerine devam etmektedir (*WhatsApp Hakkında*, 2019).

Çalışmada 25 Ağustos 2016 tarihinde Whatsapp'ın güncellemiş olduğu gizlilik sözleşmesi esas alınarak inceleme yapılmıştır (*WhatsApp Legal Info*, 2016).

Whatsapp gizlilik sözleşmesinde, ilk maddeden itibaren kullanıcıların gizliliğine saygı duyulacağını ve bu konunun şirket politikası haline getirilmesi "Gizliliğe saygı, DNA'mıza kodlanmıştır" şeklinde ifade edilmiştir. Whatsapp, platformun gerekliliği sebebiyle kullanıcıların cep telefonu numarası, kullanıcının adres defteri olmak üzere iki temel kaynağa ihtiyaç duymaktadır. Eğer isterse kullanıcı, profil resmi, durum mesajı gibi eklemeler de yapabildiği sözleşmede belirtilmiştir. Whatsapp kullanıcıları uygulama içerisinde çeşitli faaliyetlerde bulunmaktadır. Sözleşmede de belirtildiği gibi bazı veriler şirket tarafından toplanmaktadır;

- Günlük dosyaları, tanılamalar, kilitlenme raporları,
- Kullanıcının durum bilgisi, kullanıcının çevrimiçi olup olmadığı, hangi zamanlarda çevrimiçi olduğu bilgisi,
- Whatsapp kullanılan cihazın modeli, işletim sistemi, tarayıcı bilgisi,
- IP adresi, telefon numarası, mobil ağ bilgisi,
- Ek olarak Whatsapp Web kullanımının sağlanması için gerekli olan çerezlerin sistemlere eklenmesi sonrasında bu gibi bilgilerin toplandığı belirtilmiştir.

Whatsapp üçüncü kişiler ile veri paylaşımı konusunda gizlilik sözleşmesinde, Whatsapp hizmetlerinin devam edilebilmesi için ticari kuruluşlar ile çalıştığını belirtmiştir. Örneğin uygulama marketleri (Google Play ve AppStore), altyapı, harita (Google Haritalar), ödemeler, araştırma geliştirme çalışmaları, pazarlama faaliyetleri gibi uygulamalarda veriler paylaşılmaktadır. Ek olarak Whatsapp, Facebook şirketi olması dolayısıyla elde ettiği verileri Facebook ile paylaşabileceğini belirtmiştir.

Kullanıcı bilgileri işlenmesine rağmen Whatsapp, kullanıcılarına banner[17] diye ifade edilen reklamları uygulamasında kullanmamaktadır. Whatsapp uygulama içerisindeki konuşma verilerinin hangi sistemlerde bulundurulduğunu belirtmiştir. Sözleşmeye göre iki kullanıcı birbiri ile görüşme sırasında gönderdikleri içerikler cihazlarına ulaştıkları anda Whatsapp sunucularından bu içeriğin silindiği belirtilmektedir. Bir kullanıcının diğer bir kullanıcıya gönderdiği içeriğin ulaşmaması durumunda, Whatsapp sunucuları bu içerik karşı tarafın cihazına ulaşıncaya kadar 30 güne kadar saklamaktadır. Buradan

[17] İngilizce karşılığı afiş olan "banner" kavramı, genellikle yeni medya ortamlarında reklam ve pazarlama amacıyla kullanılmaktadır. İnternet sayfalarının veya uygulamaların boyutlarına göre şekillendirilebilmekte ve tıklama başına ücretlendirme yapılmaktadır.

anlaşılacağı üzere Whatsapp içerikleri çoğunlukla kullanıcıların cihazlarında depolanmaktadır. Veriler cihazlarda Whatsapp'ın 2 Nisan 2016 tarihinde aktif ettiği uçtan uca şifreleme yani kriptolama[18] ile depolamayı güvence altına almaktadır. Verilerin kullanıcıların cihazlarında depolanması, Whatsapp'ın kullanıcı verilerini yedeklemediği anlamına gelmemektedir. Bu durumu da gizlilik sözleşmesinin bilgileri yönetme başlığı altında belirtilen, kullanıcı Whatsapp hesabını silme talimatı verdiğinde, merkez sunuculardan hızlı bir şekilde silineceğidir. Ancak verilerin diğer sunuculardan da tamamen silinmesinin zaman alacağı Whatsapp tarafından da belirtilmiştir.

3.3.1. Ocak 2020 Gizlilik Sözleşmesi Güncellemesi

Ocak 2020 tarihinde Whatsapp, 2016 yılından itibaren kullanıcılarına sunduğu gizlilik sözleşmesinde bazı güncellemeler yapmıştır. Whatsapp, altı ana başlık altında sözleşmesini güncellemiştir (*WhatsApp Yasal Bilgiler*, 2020).

- Whatsapp ilk olarak 2016 yılındaki gizlilik sözleşmesi daha anlaşılır hale getirildiğini ve Whatsapp Web ve Arama işlevlerine yeni özellikler eklediği belirtilmiştir.
- 2014 yılından Facebook tarafından Whatsapp'ın alınması sonrasında kullanıcı verilerinin Facebook ile paylaşılması konusunda reklam, gereksiz mesajların engellenmesi ve ürün önerilerini yapmak amacıyla kullanılacağı belirtilmiştir. Ancak kullanıcılar arasındaki mesajların şifreleme yöntemi ile saklandığı ve hem firma hem de üçüncü kişiler ile paylaşılmayacağı belirtilmiştir.
- Whatsapp kullanıcıların mesajlaşmaların güvenliği şifreleme yöntemi ile sağlandığı belirtilmiştir. Kullanıcı mesajlaşmalarının saklanmadığı sözleşme içerisinde belirtilmiştir.[19]
- İkinci madde de Whatsapp'ın Facebook'a katılmasıyla reklam için çeşitli bilgilerin kullanılacağı belirtilmiştir. Bu durum kullanıcıların özelliklerine göre kişiselleştirilmiş reklamlar üretmek amacıyla bu bilgileri kullanmasıdır. Ancak

[18] Kriptolama, dijital ortamdaki verilerin depolanması veya bir noktadan diğer noktaya aktarılması sırasında verilerin üçüncü kişiler tarafından müdahalesini engelleyen güvenlik sistemidir. DES (Data Encrytion Standart), AES (Advanced Encrytion Standart) gibi şifreleme protokolleri bulunmaktadır.

[19] Whatsapp kullanıcılarının oluşturduğu mesajları yine kullanıcıların cihazları içerisine kaydetmesi şeklinde depolanmaktadır. Veri kaybını önlemek amacıyla da Android cihazlarda "Google Drive", Apple cihazlarda ise "ICloud" bulut disklerine yüklenmektedir.

Whatsapp uygulamalarında herhangi bir tanıtım, öneri gibi reklam araçları kullanmadığı belirtilmiştir.

- Whatsapp dünya çapından kullanılan bir uygulamadır. Dolayısıyla bugün iletişim uygulaması kavramından ayrılıp daha çok iletişim aracı haline gelmiştir. Dolayısıyla Whatsapp iki kişinin farklı yerlerde iletişime geçmesi için kullandığı bir aracın ötesinde firmaların ürün siparişi aldıkları, havayollarının müşterilerine uçakları ile alakalı bilgilendirme yapması, ödeme sonrası fatura gönderilmesi gibi çeşitli uygulama alanları mevcuttur.[20] Whatsapp sözleşmesinde bu gibi kullanımları onayladığı ve tercihe göre kullanılabileceği belirtilmiştir.
- Son olarak sözleşme içerisinde, yapılan güncellemenin kullanıcılar tarafından kabul etmeme seçeneklerinin bulunduğunu ve seçim yapmak için sözleşme çıkış tarihi itibarıyla 30 günlerinin olduğu belirtilmiştir.

3.4. Twitter Gizlilik Sözleşmesi

Twitter Amerika Birleşik Devletleri, California'da 3 Mart 2006 tarihinde Jack Dorsey tarafından kurulmuştur. Twitter'ın ilk tweet'i olan ve Jack Dorsey tarafından "Just setting up my twitter" paylaşımı ile dünyaya açılmıştır (*Twitter Kuruluş Tarihi,* 2006). Bugün de Twitter'a ilk defa kayıt yaptırdığınızda varsayılan olarak "Şu an Twitter'ımı ayarlıyorum" paylaşımının hikayesi Jack Dorsey'in attığı ilk tweet'e dayanmaktadır.

Çalışmada Twitter'ın 25 Mayıs 2018 tarihinde güncellemiş olduğu gizlilik bildirimi esas alınarak kullanıcıların verilerinin nasıl alındığı ve nasıl kullanıldığı konuları araştırılmıştır (*Twitter Privacy Policy,* 2018).

Twitter gizlilik politikasında ilk olarak platformun nasıl kullanılabileceği konusunda kullanıcılara bilgi vermektedir. Örneğin bir kullanıcı Twitter hesabını kişisel tercihine bağlı olarak gerçek ismi veya takma ad (Nickname[21]) şeklinde kullanabilmektedir. Kullanıcılar Twitter ara yüzünde oturumlarına giriş yapılmamış dahi olsa, şirket ziyaret edilen sayfa, cihaz türü gibi bilgileri kaydetmektedir.

[20] Whatsapp, son kullanıcıya hitap eden bir uygulamadır. Firmanın sonradan çıkarmış olduğu Whatsapp Business, önceki uygulamanın mantığında çalışan sadece firmalara için özelleştirilmiş bir arayüze sahiptir. Ayrıca Bkn: *https://www.whatsapp.com/business/*

[21] Nikname kavramı, internet ortamında faaliyet gösteren kullanıcıların gerçek isimlerini yerine takma ad kullanmaları durumudur. Takma ad ile kullanıcıların internet ortamındaki faaliyetleri anonim olabilmektedir.

Twitter gizlilik politikasının şirket ile paylaşılan bilgiler başlığı altında ilk olarak kullanıcıların genel hesap bilgileri yer almaktadır. Twitter, kullanıcıların açmış oldukları hesapta eposta adresleri, telefon numaraları gibi bilgilerden yararlanmaktadır. Buna ek olarak Twitter ek bilgiler başlığı altında belirttiği gibi kullanıcıların şu bilgilerini incelemektedir:

- Zaman dilimi, kullanıcının konuştuğu dil,
- Satın alma faaliyetleri esnasında kullanılan kredi kartı veya banka kartı numarası, son kullanma tarihi, CVV[22] kodu,
- IP adresi, konum bilgisi
- Mobil operatör adı, işletim sistemi adı, tarayıcı türü,
- Twitter üzerinden yönlendirildiğiniz ve ziyaret ettiğiniz sayfalar gibi bileşenler toplanmaktadır.

Twitter, toplanan bu verilerin nasıl kullanıldığı konusuna gizlilik sözleşmesinde şu şekilde yer vermektedir; Toplanan veriler kullanıcıların platform üzerindeki deneyimlerini arttırarak kişiye özel reklam faaliyetlerinde, Twitter içerisinde bulunan sayfaların kişinin ilgi alanlarına göre önerilmesi şeklinde kullanılacağı belirtilmiştir. Twitter, özellikle Google Analitics gibi ortaklarına kendi kullanımı için verileri işletebilmektedir. Eğer Twitter şirketinde iflas, birleşme, satın alma, yeniden düzenleme gibi işletmeler için hukuki sonuç doğuran faaliyetlerde bulunulduğunda veriler bu işlemin bir parçası olarak aktarılabilir veya satılabilir.

Twitter, onaylattığı sözleşmeyle kullanıcılara bazı sorumluluklar ve haklar tanımıştır. Örneğin kullanıcı, Twitter platformu üzerinden yapacağı bir paylaşımın sorumluluğunun kişiye ait olduğu ve paylaşılan bu içeriklerin kamuya açık olarak paylaşılacağından dikkatli olunması konusunda uyarılmaktadır. Bir başka konu da profil bilgilerinin paylaşılması hususundadır. Kamuya açık bir platform olması sebebiyle profil bilgilerinin kitle ile paylaşılması kararını kullanıcıya bırakmıştır. Özellikle telefon numarası, din, ırk, siyasi düşünce gibi değerlerin paylaşımı kararı kullanıcılara aittir. Kullanıcı Twitter'da tutulan kişisel verisinin değiştirilmesi veya silinmesi talebinde bulunabilir. Her iki durum için Twitter şirketine başvuru yapılmasının yeterli olacağı

[22] Kredi kartlarında bulunan CVV (Card Validation Value), özellikle internet üzerinden satın almalar sırasında, satıcının kredi kartının kullanıcıya ait olup olmadığını kontrol eden güvenlik kodu sistemidir.

belirtilmiştir. Silme talebinde bulunan kullanıcının otuz güne kadar bu talebinden vazgeçilebileceğini, otuz gün sonrasında ise verilerinin tamamen silineceği bilgisi verilmektedir. Twitter, bunlara ek olarak kullanıcıların günlük verilerinin kopyalarını en fazla 18 ay süresinde tutulduğunun bilgisini de vermektedir.

3.5. Youtube Gizlilik Sözleşmesi

Youtube bugün dünyanın en büyük video içerik platformlarından biridir. Özellikle Google, Youtube'u 2006 yılında 1,5 Milyar Dolara satın almasından bugüne kadar ki geçen sürede hızlı bir ivme kazanarak 1 Milyar kullanıcıya ve günlük 1 Milyar saat izlenme süresine sahip olmuştur ("Press—YouTube"). Google müşterilerine tüm markaları (Gmail, Youtube, Google Home, Chrome, Chrome OS, Google Play, Google Ads) ile hitap ettiğinden oluşturulmuş olan gizlilik politikaları tüm ürünleri kapsamaktadır.

Çalışmada Youtube'un 25 Mayıs 2018 tarihinden itibaren geçerli olan hizmet politikası, veri işleme politikası şartları ("Hizmet Koşulları—Youtube") ve 22 Ocak 2019 tarihinde geçerli olan Google veri gizliliği politikaları ele alınmıştır.

Youtube hizmet sözleşmesi ilk olarak, kullanıcı hesaplarının güvende tutulması amacıyla hesap bilgilerinin üçüncü kişilerle paylaşılmaması, bir kullanıcı şahsi hesabında şüpheli aktiviteler fark ettiğinde firmanın bilgilendirilmesi gerektiğini belirtmektedir. Youtube'un hesap güvenliği konusunda kullanıcıları uyarmalarının en temel nedeni, sözleşmenin Youtube hesapları başlığı altında yer alan 4.3 maddesinde; kullanıcılar hesapları içerisindeki tüm aktivitelerden sadece kendisi değil aynı zamanda üçüncü kişiler de sorumludur. Yani kullanıcının Youtube ortamına yüklediği videonun içeriğinin ve yüklenip yayımlanmasının sorumluluğu sözleşmenin içerik başlığı altında tamamen kullanıcıya bırakılmıştır. Ek olarak Youtube, kullanıcının kendisine ait olmayan Youtube Video Oynatıcı, reklamlar, sponsorluklar gibi unsurların kullanıcılar tarafından ticari amaçlarla satılamayacağını açıkça belirtmiştir.

Youtube ile kullanıcılar arasındaki sözleşmede İngiliz Hukuku esasları uygulanmaktadır. Faaliyetler esnasında meydana gelebilecek uyuşmazlıklarda İngiliz Mahkemelerinin görevlendirileceği bilgisi verilmektedir. Ancak Youtube dünyanın birçok ülkesinde kullanıldığı için sözleşmenin 7. madde 6. fıkrasında Youtube içerisine

yüklenecek materyallerin ikamet edilen ülkenin kanunlarına da uygun olması gerektiğini belirtmektedir.

Youtube veri koruma mevzuatı (GDPR)[23] kapsamında müşterilerin kişisel verilerini işlemektedir. Google, müşteri verilerinin farklı bir şekilde işlenmesi gerektirmediği sürece verilerin farklı yerlere aktırılması konusunda AB ve AB ülkeleri mevzuatlarına uygun davranacağını belirtmiştir.

Youtube bir Google hizmeti olduğundan kullanıcıların etkinlikleri sırasında hangi verileri topladığına ilişkin veriler, gizlilik sözleşmesinin topladığımız bilgiler başlığı altında verilmektedir:

- Web tarayıcı (browser), cihaz türü ve ayarları,
- İşletim sistemi,
- Telefon numarası, mobil ağ ile bağlı baz istasyonu ve kablosuz ağ bilgileri,
- GPS, IP adresi, bluetooth ve cihazın içerisindeki sensör verileri gibi donanım bileşenlerinden gelen veriler toplanmaktadır.

Yukarıda belirtilen toplanan verilerin yanında kullanıcıların Youtube gibi uygulamaların içerisindeki aktivite verileri de alınmaktır:

- Youtube ve Chrome üzerinden aranan terimler,
- Youtube üzerinden izlediğiniz videolar,
- Kullanıcının içerik ile reklam görüntüleme etkileşimleri[24]
- Kullanıcının vermiş olduğu sesli komutlar
- Satın alma etkinlikleri gibi verilerin Google tarafında toplanacağı ifade edilmektedir.

Google toplamakta olduğu tüm verileri şekil 3'te görüldüğü üzere dünyanın farklı noktalarında bulunan sunucu ağı ile birbirine aktarmaktadır. Bu aktarma sürecinde Avrupa Veri Yönetmeliğinin dikkate alındığı ve işlemlerin yönetmeliğe uygun bir şekilde yapıldığı belirtilmiştir.

[23] GDPR, açılımı "Genaral Data Protection Regulation" olup, Avrupa Veri Yönetmeliğini ifade etmektedir.
[24] Örneğin kullanıcı Youtube üzerinden bir video izleme sırasında giren reklamı, Youtube'ın belirlediği 5 saniye içerisinde geçiyor mu yoksa izlemeye devam mı ediyor? Kullanıcı bir reklamı izliyor ise o reklamın konusu kullanıcının ilgisini çekiyor mu gibi etkileşimleri ifade etmektedir.

Şekil 3: Google Sunucu Merkezleri

Google gizlilik sözleşmesinde, Youtube gibi hizmetlerini kullanan kullanıcılarına, kullandıkları hizmetten vazgeçmesi halinde verilerinin silinmesine imkân verir. Eğer kullanıcı verilerinin silinmesi için bir talepte bulunursa, kötü amaçlı kullanıma karşı silme işlemi Google tarafından bir süre bekletilir ve bu süre içerisinde kullanıcıya bilgilendirme yapılıp onayı istenir. Onay sonrasında Google sunucularına, kullanıcının verilerinin silinmesi talimatı verilir. Google, birçok sunucu merkezinde yedeklenmiş veriler bulunduğundan silinme sürecinin zaman alacağını belirtmektedir.

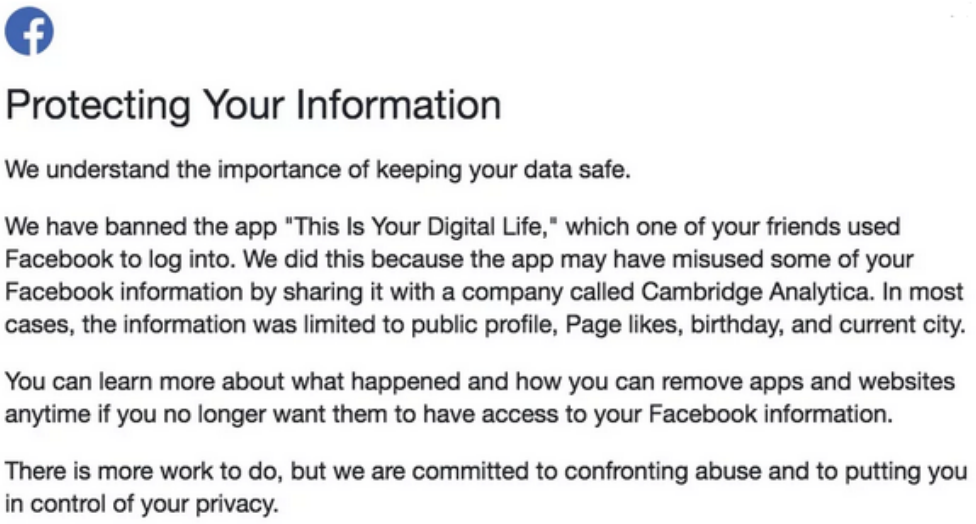
Diğer bir gizlilik önlemi olarak Google, sunucu merkezlerinin fiziki güvenliğinin sağlanması yanında veri işleme politikasında belirttiği gibi sunucu merkezinde kullanılan bir diskin bozulması veya devre dışı bırakılması durumunda diskin geri dönüşüm merkezine gönderilemeden önce "Devre Dışı Bırakılmış Disk" ve "Veri İmha Kılavuzuna" göre fiziki olarak imha edildiğini ancak bu işlemden sonra geri dönüşüme gönderildiği ve bunun Google tarafından bir politika haline getirildiği belirtilmiştir.

3.6. Cambridge Analytica ve Veri Gizliliği İhlalleri

Facebook ilk ortaya çıkışından bu yana kullanıcıların kendi bilgileriyle oluşturdukları profiller üzerinden birbirleri ile etkileşime geçmesi şeklinde planlanmış bir sosyal yapıya sahiptir. Dolayısıyla kullanıcıların içerikleri zaman içerinde kendi fikir ve düşüncelerini oluşturduğu bir profil ortaya çıkmaktadır. Facebook kullanıcı kitlesi göz önüne alındığında bu büyüklükteki verilerin işlenmesi reklam ve pazarlama sektörlerinin gerçek hedef kitlelerine ulaşmasını sağlamaktadır.

Bu durumun benzerini Cambridge Analytica olayında görmekteyiz. 2014 yılında Amerikalı seçmenlerin psikolojik profillerinin siyasi kampanyalarda kullanımı amacıyla on milyonlarca verinin Amerika Birleşik Devletleri başkan adaylarından Donald Trump'un seçim ekibi ve Cambridge Analytica firmasına satılması gündeme geldi (Confessore, 2018). Hatta o dönem Cambridge Analytica çalışanlarından olan Christopher Wylie: "Milyonlarca insanın profilini işleyebilmek için Facebook'tan yararlandık. Onlar hakkında edindiğimiz bilgiler ile hedeflerimiz doğrultusunda modeller inşa ettik" açıklamasında bulunmuştur (Cadwalladr & Graham-Harrison, 2018). Ayrıca verilerin Aleksander Kogan tarafından "This Is Your Digital Life" adlı uygulaması aracılığı ile Global Science Research ve Cambridge Analytica iş birliği sayesinde yüz binlerce kullanıcıya kişilik testi yapılması için ödeme yapıldığı kabul edilmiştir. Uygulamadaki test katılımcıları Facebook arkadaşlarının bilgilerini toplaması sonucunda büyük ve güçlü bir veri havuzuna sahip olmuştur (Cadwalladr & Graham-Harrison, 2018).

"This is Your Digital Life" uygulaması Facebook üzerinde çalışan ve kişilere çeşitli sorular yönelterek kişilerin cevaplarına göre düşünce haritası oluşturan bir uygulamadır. Kişiler uygulamaya girmeden önce Facebook profil bilgilerinden olan beğenilen sayfalar, doğum tarihi ve bulunduğu şehir gibi bilgileri istemektedir (*Did Facebook Warn You That a Friend Used the "This Is Your Digital Life" App?*, 2018).



Protecting Your Information

We understand the importance of keeping your data safe.

We have banned the app "This Is Your Digital Life," which one of your friends used Facebook to log into. We did this because the app may have misused some of your Facebook information by sharing it with a company called Cambridge Analytica. In most cases, the information was limited to public profile, Page likes, birthday, and current city.

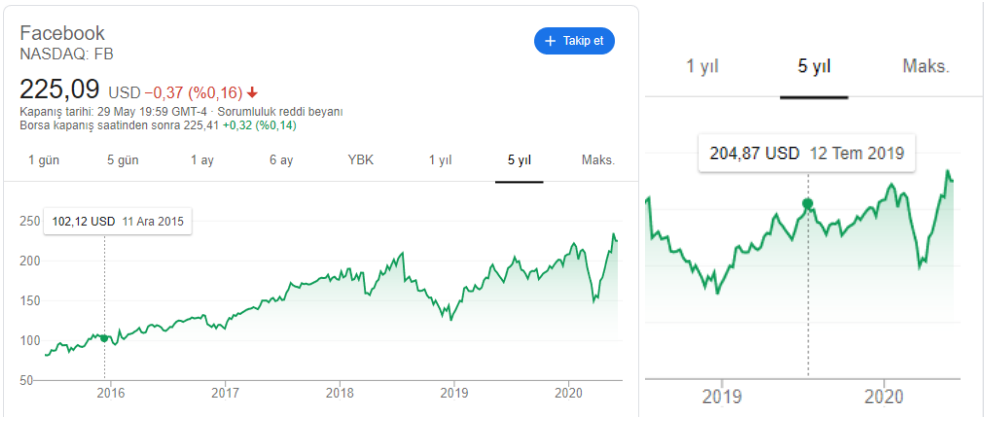
You can learn more about what happened and how you can remove apps and websites anytime if you no longer want them to have access to your Facebook information.

There is more work to do, but we are committed to confronting abuse and to putting you in control of your privacy.

Şekil 4: This is Your Digital Life uygulamasının talep ettiği bilgiler için Facebook'un kullanıcılara göstermiş olduğu uyarı yazısı.

Amerika Başkanlık Seçimi için yapılan bu veri toplama yöntemleri ile kullanıcıların bir haritası çıkartılmıştır. Örneğin bugün anketlerde yapılan katıyorum, kararsızım veya katılmıyorum seçenekleri gibi kullanıcıların başkan adaylarından olan Donald Trump'a yönelik seçmenlerin ilgisi ölçülmüştür. Ölçümler sayesinde seçmeler belirli sınıflara ayırılarak seçim kampanyasının en doğru şekilde planlanması hedeflenmiştir.

Verilerin çeşitli amaçlar için Facebook'tan toplanması kamuoyu tarafında büyük tepki çekmiştir. Nitekim ABD Federal Ticaret Komisyonu, Cambridge Analytica'nın Facebook'ta bulunan kullanıcı verilerini uygunsuz olarak elde ettiği konusunda araştırma yapmıştır. Şirket herhangi bir usulsüzlük olmadığı ve herhangi bir şekilde verilerin 2016 yılındaki ABD başkanlık seçiminde kullanılmadığını belirtmiştir. Ancak Aleksander Kogan, Cambridge Analytica ile verilerin paylaşması sonucunda ticari sözleşmesinde bulunan şartları ihlal etmiş bulunmaktaydı. Dolayısıyla yapılan soruşturmaların ardından Cambridge Analytica kapatılmış oldu. Facebook bu süreçte kullanıcıları tarafından büyük tepki çektiği söylenebilir. Süreç esnasında "deletefacebook" etiketiyle birçok paylaşım yapılmış ve Facebook hisselerinde düşüş gözlemlenmiştir. Facebook'a yapılan soruşturma sonucunda 5 Milyar Dolar para cezası kesilmiştir ("'Facebook'a Cambridge Analytica skandalı nedeniyle 5 milyar dolar ceza kesilecek'", 2019). Verilen bu cezanın ardından ABD borsalarında işlem gören Facebook hisseleri ilginç bir şekilde yükselişe geçti. Bunda soruşturma sürecinin kapanması ve Facebook'un belirtilen rakamları 2019 birinci çeyrek bilançosunda belirtmesinin yatırımcılar üzerindeki olumlu etkisi oldu (*Hisseleri yüzde 2'ye yakın yükseldi - Habertürk*, 2019). Bu olayın The Guardian tarafından detaylı bir şekilde açıklandığı ve dünyada oldukça ses getirdiği 11 Aralık 2015 tarihinde Facebook hisseleri yaklaşık 102 dolar civarında olmasına karşın cezanın açıklandığı gün (12 Temmuz 2019) yaklaşık 205 dolardı (Davies, 2015).



Şekil 5: Intervesting.com, 12 Temmuz 2019 – Facebook Hisse Değeri Grafiği

Sadece Cambrige Analytica gibi kullanıcı verilerinin satın alınması yoluyla veri ihlali yapılmamaktadır. Aynı zamanda verilerin depolama merkezlerinden çalınması da söz konusudur. Türkiye'de yaşanan kredi kartı bilgilerinin çalınması bu duruma örnek olabilmektedir. Özellikle Türkiye'de internet üzerinden yapılan alışverişlerin toplam alışverişe oranı 2017 yılında %4,1 iken 2018 yılında %5,8'e yükselmiştir. Perakendecilik sektöründe çok kanallı perakendenin katkısı 10,7 Milyar TL iken sadece online alışverişlerin perakendeye katkısı 20,8 Milyar TL'dir (*E-Ticaretin Gelişimi, Sınırların Aşılması ve Yeni Normlar 2019*, 2019). Rakamlar incelendiğinde her yıl kullanıcıların internet üzerinden yaptığı alışverişlerin sayısının arttığı, bu artış nedeniyle de kredi kartı gibi değerli olan verilerin sanal ortama aktarıldığı görülmektedir.

Türkiye'de yaşanan kredi kartı verilerinin çalındığına ilişkin haberlerin yayılması sonucunda verilerin bankalar ya da sanal mağazalar tarafından paylaşılması şüphelerini doğurmuştur. Konuyla ilgili Türkiye'deki resmi makamları bilgilendiren Singapur merkezli Group ID şirketi, 28 Ekim - 27 Kasım tarihleri arasında 460.000'den fazla kredi kartı bilgisinin Deep Web'de bulunan Joker's Stash mağazasında satışa çıkarıldığını duyurmuştur (*Huge set of Turkish banks' cards on sale on dark net marketplace*, 2019). Ticari kuruluşa ait web sayfasında çalınan verilerin 4 parti olarak satışa konulduğu ve her bir kart bilgisi için 1 Dolar ile 3 Dolar arasında bir ücretle satışa çıkarıldığı belirtilmiştir. Group ID'ye göre dünyada Hindistan'dan sonra ikinci büyük kredi kartı satışı olduğunu açıklamıştır (*Türk kullanıcılara ait kredi kartları 1 dolara satılıyor!*, 2019). Group ID Siper Suçları Araştırma Birimi Başkanı Dmitry Shestakov'un yapmış olduğu açıklamada,

kimlik avı, kötü amaçlı yazılımların artan etkinlikleri nedeniyle tüm kredi kartlarının çevrimiçi olarak ele geçirilebileceğini belirtmiştir. Kredi kartı bilgilerinin paylaşıldığı veri tabanından şu bilgilerin paylaşıldığını belirtmiştir:

- Kart numarası,
- Son kullanma tarihi,
- CVV/CVC güvenlik numarası,
- Kart sahibinin adı,
- E-Posta adresi,
- Telefon numarası,
- Kredi kartı üzerinde bulunan manyetik şerit içerisindeki bilgiler olarak açıklamıştır.

Ayrıca Shestakov, satışı yapılan verilerin kaynağının bilinmediği ve konuyla ilgili Türk makamlarını bilgilendirdiklerini böylelikle riskleri azaltarak önlemleri arttırabileceklerini belirtmiştir (*Huge set of Turkish banks' cards on sale on dark net marketplace*, 2019).

Konuyla ilgili Türkiye'de Bankalararası Kart Merkezinin yaptığı açıklamada, kredi kartı bilgilerinin çalınmasıyla ilgili haberlerin tüm kuruluşlarca takip edildiği, kredi kartlarının uluslararası standartlarda korunduğunu ve bu gibi sahtekarlık durumlarının oluşmaması için kredi kartı bilgilerini korumaya özen gösterdikleri belirtilmiştir (*Kamuoyu Bilgilendirmesi , BKM,* 2019).

Verilerin çalınmasına ilişkin haberin duyulduğu tarihten günümüze kadar geçen zaman içerisinde Türkiye'deki resmi makamlar tarafından kredi kartı verilerinin hangi kaynaklar tarafından çalındığı, kaç kullanıcının kredi kartı verisi çalındığı ve bankalar tarafından hangi koruma yöntemleri uygulandığına ilişkin herhangi bir açıklama yapılmamıştır.

Bir başka veri gizliliği ihlali örneği olan Mastercard, Almanya'daki kullanıcıların kredi kartı verilerinin çalındığını duyurmuştur. Firma kullanıcılarının bağlılığını ve hizmetlerini geliştirmek amacıyla "Priceless (Paha Biçilmez)" adında bir kampanya başlatmıştır. Kampanyada amaç kullanıcı şartlarında belirtildiği gibi, Mastercard sahiplerine deneyimler, teklifler ve içerik sunmaktır (*Priceless Cities*, 2020).

Verilerin sadece üçüncü şahıslarla paylaşılmamasının veri gizliğini sağlayamayacağı aynı zamanda toplanan verilerin uygun standartlarda güvenli bir şekilde saklanması gerektirdiği veri gizliliği kanunları bölümünde açıklanmıştı. Mastercard olayında kullanıcı verileri yasal olmayan yollarda üçüncü şahıslar tarafından çalınmıştır. Dolayısıyla Cambridge Analytica'da olduğu gibi firmaların bilgisi dahilinde gerçekleşen bir durum söz konusu değildir.

Verilerin açığa çıkması Mastercard'ın kampanyayı uyguladığı ülkelerden olan Almanya'da gerçekleşmiştir. Ayrıca çalınan verilerin sadece Almanya'da yaşayan ve kampanyaya katılan kullanıcılara ait olduğu belirlenmiştir. Verilerin belirli bir süre çevrimiçi olarak yayımlandığı Belçika Veri Koruma Kurumu tarafından teyit edilmiştir (*Data leak affects Mastercard,* 2019). Yaklaşık 90 bin kullanıcıya ait çeşitli bilgilerin ele geçirildiği belirtilmiştir:

- İsimler ve ünvanlar,
- Telefon numaraları,
- Kısmi kredi kartı verileri,
- IP Adresleri gibi kişisel verilerin ortaya çıktığı belirtilmiştir (*Mastercard Priceless Specials,* 2019).

Veri ihlali sonrasında Mastercard'ın yaptığı açıklamada, kampanyanın içerisindeki bilgilerin çalınması durumunu onaylamıştır. Konu ile ilgili kampanyanın ve kullanıcıların kredi kartlarının askıya alınması şeklinde önlem alınmıştır (*Data leak affects Mastercard*, 2019).

3.7. Yeni Medya Platformlarında Gizliliği Korumak

Yeni medya platformlarında kullanıcıların kişisel bilgileri bir diğer ifadeyle özel bilgileri barındırılmaktadır. Özel hayatın bir parçası olan gizli alan kişilerin fikir ve düşüncelerin olduğu bölgedir. Bu bilgilerin üçüncü kimseler tarafından ele geçirilmesi kişilerin özel hayatlarına müdahale etme durumunu ortaya çıkarmaktadır. Hangi yöntemlerle olursa olsun kişilerin gizli alanlarına girilmesi özel hayatın gizliliğinin ihlali anlamına gelir (Çelik, 2017).

Türkiye'de 1982 Anayasasının Özel Hayatın Gizliliği başlığı altında verilen 20'inci maddede "*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme*

hakkında sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." şeklinde ifade edilmiştir. İfade edilen maddenin 2010 yılındaki ek fıkrasında "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkında sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişim, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmayacağını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir…"* şeklinde ifade edilmiştir (Türkiye Cumhuriyeti Anayasası, 1982). Kanunda da ifade edildiği gibi kişi paylaşmış olduğu veriler ile ilgili durumu sorgulama hakkına sahiptir. Ayrıca ticari kuruluşların veriyi işleyebilmek için veri sahiplerinden onay alması şartı da eklenerek veri gizliliği güvence altına alınmıştır.

Devletlerin kullanıcıları korumak üzere hazırlamış olduğu yasalar kullanıcıların veri gizliliğini kısmen koruyabilmektedir. Bunun en temel nedeni firmaların ürün ve hizmetleri için kullanıcılara gizlilik sözleşmesi imzalatmasıdır. Böylelikle firmalar veri alışverişini yasal yollardan gerçekleştirebilmektedir. Dolayısıyla kullanıcılar verilerini paylaşmadan önce firmaların hangi verilerini talep ettiği ve hangi amaçlarla kullanılacağını incelemesi gerekmektedir. Ancak gizlilik sadece bir web sitesinin kullanıcıdan isteği verilerle sınırlı olmadığı ve akıllı telefonlar gibi internete ulaşabilen cihazların da ciddi bir veri alışverişi olduğu görülmektedir.

Kaspersky'ın Dijital Gizliliği Korumak adlı araştırmasında kullanıcıların yeni medya ortamlarında veri gizliliği konusunda almış olduğu önlemleri araştırmıştır. Çalışmanın bazı önemli sonuçları bulunmaktadır:

- Kullanıcıların %34'ü özel bilgilerine erişim izini vermediği halde bilgilerine erişildiği olaylarla karşılaşmıştır. Özellikle bu durum 25-34 yaşları arasında %39 seviyesindedir.
- Kullanıcıların %82'si kamuya açık olan veya sosyal medyadaki bilgilerini kaldırmaya çalışmıştır.
- İnsanların önemli bir kısmı internette gezinirken %43'ü siber suçlular, %41'i ziyaret ettikleri web siteleri, %37'si ortak kullanılan cihazlar için ek gizlilik önemleri almaktadır.

- Kullanıcıların %22'si bilgisayar, tablet veya akıllı telefonlarındaki tarayıcıların şifrelerini kaydetmesine izin vermektedir. Bu gizlilik ihlalleri için önemli bir sorundur.
- Kullanıcıların %54'ü şifrelerinin internet ortamına sızdırılmış olup olmadığı nasıl kontrol edeceğini bilmemektedir.
- Kullanıcıların %21'i mobil cihazlardaki uygulamaların topladığı verilerle ilgili endişe taşımaktadır.
- Kullanıcıların %53'ü cihazlarının hoparlörleri üzerinden dinlemeleri engellemek için önlem almıştır. Ayrıca kullanıcıların %47'si gizliliklerini korumak için web kameraları üzerine bant yapıştırmak, %35'i özel bir kamera koruma etiketi ve yine %35'i cihaz yönetiminden kamerayı devre dışı bırakmıştır.

Kaspersky'ın yapmış olduğu araştırmada kullanıcıların büyük bir bölümü veri gizliliği konusunda çeşitli önlemler almaya çalışmıştır. Özellikle firmaların gün geçtikçe artan veri hacimleri düşünüldüğünde veri gizliliği önemli bir unsur haline gelmektedir. Ancak kullanıcılar verilerin gizlenmesini tamamen sağlayamasa da önemli ölçüde bilgilerinin alınmasını engelleyebilir.

- Aileniz, yakın veya iş arkadaşlarıyla hesap bilgilerinin veya şifrelerin asla paylaşılmaması,
- Kullanmakta olduğunuz sosyal medya platformları veya cihazlar içerisindeki uygulamaların üçüncü kişiler ile veri paylaşmasını engellemek için uygulama izinlerinin kapatılması gerekmektedir (*Defending Digital Privacy,* 2020).
- Kullanmakta olduğunuz hesapların mutlaka güçlü bir şekilde şifrelendirilmesi gerekmektedir. Güçlü şifreler genellikle en az 8 karakterden oluşmalıdır. Şifre içerisinde rakam ve özel karakterler içermesi ve büyük-küçük harf olması şifrenin kırılma olasılığını büyük oranda azaltacaktır (*Güçlü Parola Oluşturma,* 2020). Şifrelerinizin çalınıp çalınmadığını öğrenmek için Firefox Monitor[25] gibi veri ihlallerini yayımlayan sayfalarda taratılması ve olumsuz sonuçlar çıktığı taktirde

[25] Firefox Monitor, dünyadaki internet sitelerinde yaşanan veri gizliliği ihlali olaylarını kaydeden ve kullanıcıların eposta adreslerini taratması şeklinde kontrol edebileceği bir platformdur. Bk. *https://monitor.firefox.com*

şifrelerin yenilenmesi ve iki aşamalı doğrulama[26] gibi sistemlerin aktif hale getirilmesi gerekmektedir.

- Sanal mağazalardan alışveriş yapılması esnasında mağazanın güvenli olduğunun teyit edilmesi gerekmektedir. Özellikle alışverişlerin güvenli bağlantı protokolü olan "HTTPS" olmasına dikkat edilmesi gerekmektedir. Ödemeleri kredi kartı yerine sanal kartla yapılması ve 3d Secure ile iki aşamalı doğrulama yapılması önerilmektedir. Ayrıca sanal mağazalara kredi kartı bilgilerinin kaydedilmemesine dikkat edilmelidir (*E-Ticaret ve E-Ticarette Dikkat Edilmesi Gerekenler*, 2017).

Kullanıcılar belirli korunma yöntemleriyle verilerin güvende kalmasını sağlayabilmektedir. Ancak tam anlamıyla veri gizliliği söz konusu değildir. Bunun en temel sebebi kullanıcılar internet üzerinden ziyaret etmiş oldukları sayfalara kullanıcı izlerini bırakmaktadır. Önemli olan bu bilgilerin mümkün olduğunca anonim hale gelmesi kullanıcıların verini gizleme konusunda yardımcı olabilmektedir.

3.8. Sosyal Medya Platformlarının Gizlilik Sözleşmelerinin Karşılaştırılması

Yeni medya platformlarını kullanabilmek için kullanıcılar, söz konusu platformların sosyal medya gizlilik sözleşmelerini onaylamak zorundadır. Sözleşmeler şirketlerin gizlilik politikalarına göre değişiklik göstermektedir. Gizlilik sözleşmelerindeki temel amaç, kullanıcıların kişisel ve cihaz bilgilerinin toplanması ve işlenmesi şeklindedir.

Facebook, Whatsapp, Twitter ve Youtube gibi platformların veri gizliliği sözleşmelerinde, veri şifreleme yöntemleri, veri depolama merkezleri, toplanan kişisel bilgiler, toplanan cihaz bilgileri, verilerin üçüncü kişiler ile paylaşılması ve verilerin silinmesi gibi unsurlar dikkate alınarak karşılaştırılmıştır.

[26] İki aşamalı doğrulama sistemleri kullanıcı hesabına giriş yaptığı sırada kullanıcını eposta adresine veya telefon numarasına rasgele güvenlik kodu gönderilmesi ve bu kodu girilmesiyle oluşturulmuş bir onaylama sistemidir.

	Facebook	Whatsapp	Twitter	Youtube
Veri Şifreleme Yöntemi	128 Bit-TLS 1.3	128 Bit-TLS 1.3	128 Bit-TLS 1.2	128 Bit-TLS 1.3
Veri Depolama Merkezleri	USA-Oregon, USA- K.Karolina, USA-Pennsylvania, İsveç-Lulea	USA-Oregon (Facebook), Google Drive, Apple Icloud	USA-Utah, USA-Virginia (NTT Data Center), USA-Kaliforniya (Raging Wire Enterprice Inc.)	USA (13 Lokasyon), Şili- Quilicura, İrlanda-Dublin, Danimarka-Frederika, Belçika- St.Ghislain, Singapore, Hollanda-Eemshaven, Firlandia-Hamina, Tayvan-Changhua
Toplanan Kişisel Bilgiler	Paylaşılan İçerikler, Mesajlaşma Geçmişi, Kullanılan Etiketler, Rehber Paylaşımları, Çekilen Fotoğraflar	Kullanıcı Durum ve Çevrimiçi Bilgisi, Telefon Rehberi, Profil Resmi	Paylaşılan İçerikler, Ziyaret Edilen Sayfalar, İlgi Alanları	Youtube ve Chrome üzerinden aranan terimler, İzlenen Videolar, Kullanıcının içerik ve reklam etkileşimleri, sesli komutlar, satın alma etkinlikleri
Toplanan Cihaz Bilgileri	İşletim Sistemi Sürümü, Tarayıcı Bilgileri, Pil Seviyesi, GPS-Wifi-Bluetooth ve Baz İstasyonu Sinyal Verileri, Cihazın Telefon Numarası	İşletim Sistemi Sürümü, Tarayıcı Bilgileri, GPS-Wifi ve Baz İstasyonu Sinyal Verileri, Cihazın Telefon Numarası	İşletim Sistemi Sürümü, Tarayıcı Bilgileri, GPS-Wifi-Bluetooth ve Baz İstasyonu Sinyal Verileri	İşletim Sistemi Sürümü, Tarayıcı Bilgileri, Wifi, Bluetooth ve Baz İstasyonu Sinyal Verileri, Cihazın Telefon Numarası ve Donanım Sensör Verileri
Verilerin Üçüncü Kişiler ile Paylaşılması	API ve SDK Geliştiricileri İçin Veriler Paylaşılabilir.	Facebook Reklamları	Google Analitics	API ve SDK Geliştiricileri İçin Veriler Paylaşılabilir.
Kullanıcı Talebi İle Verilerin Silinme Süresi	90 Gün	30-90 Gün	30 Gün	60 Gün

Tablo 3: Veri Gizliliği Sözleşmelerinin Karşılaştırılması

Platformların veri şifreleme yöntemleri karşılaştırıldığında, Facebook, Whatsapp, Youtube gibi platformların TLS 1.3 standartında şifreleme yapmaktadır. Ancak Twitter daha eski bir sistem olan TLS 1.2 standarttı kullanmaktadır. TLS (Transport Layer Security) ilk olarak 1999 yılında ortaya çıkmıştır. İnternet sunucusu ile başka cihazlar arasındaki veri alışverişinin şifrelenmesini sağlayan bir güvenlik protokolüdür. TLS protokolü SSL'le (Secure Sockets Layer) göre daha yeni ve daha güvenli algoritmalar desteklemektedir. TLS 1.3 ile 1.2 arasındaki farklar veri güvenliği açısından incelendiğinde, TLS 1.2'nin 2008 yılında geliştirildiği için eski şifreleme algoritmaları

(SHA-1, RC4, DES, 3DES, AES-CBC, MD5) barındırmaktadır. TLS 1.3 sürümü ile eski algoritmalar kaldırıldığından veri güvenliği arttırılmıştır. (*TLS 1.3 Nedir ve Nasıl Çalışır?*, 2018). Ayrıca 2018 yılından itibaren Google Arama Motoru, TLS veya SSL yöntemleri ile şifrelenmeyen internet sayfalarını "Güvenli Değil" şeklinde işaretlemektedir (Loiselle, 2018). Bu durum sosyal medya platformlarının ve diğer internet sayfalarının şifreleme standartlarını kullanmasındaki sebeplerden biri olabilmektir.

Veri depolama merkezleri açısında platformlar karşılaştırıldığında, Facebook ve Google gibi uluslararası şirketlerin birçok konumda sunucu merkezinin olduğu görülmüştür. Dolayısıyla diğer karşılaştırma unsuru olan verilerin silinme sürelerinin 30 veya 90 güne kadar belirlenmesi temel nedeni, farklı merkezlerdeki sunucuların yoğunluk durumuna göre farklı zamanda silme işlemlerinin yapılmasıdır. Whatsapp veri depolaması konusunda Facebook, Google veya Youtube gibi firmalardan farklı bir farklı bir anlayışa sahiptir. Whatsapp bünyesinde bulunan sunucular sadece kullanıcıların profil bilgilerini kaydetmek amacıyla kullanmaktadır. Diğer kullanıcı aktivitelerinden olan mesajlaşma, resim, video, belge gibi paylaşımları kullanıcıların cihazları üzerinde depolamaktadır. Ayrıca verilerin kaybolmasını önlemek amacıyla Google Drive veya Apple ICloud gibi bulut depolama hizmetlerine yedeklenmesi söz konusudur. Kullanıcı bir içerik gönderdiğinde diğer kullanıcının cihazına ulaştığı süre boyunca sunucuda saklamaktadır. İçerik karşı tarafa ulaştığı taktirde sunucudan anlık olarak silinmektedir.

Kişisel bilgilerin toplanması konusunda sosyal medya platformları karşılaştırıldığında, kullanıcıların platform içerisindeki faaliyetleri izlenmektedir. Örneğin paylaşılan, beğenilen, etiketlenen içeriklerin türü, konusu gibi unsurlar kullanıcı ile eşleştirilmektedir. Böylelikle kullanıcının ilgi alanları, hobileri belirlenerek içeriğin kişileştirilmesi sağlanmaktadır. Youtube kullanıcıların izlemiş olduğu videoları ve reklamları izleme süresine göre analiz etmektedir. Facebook ve Twitter, Youtube'ta olduğu gibi kullanıcıların paylaşımlarına göre ilgi alanlarını analiz etmektedir. Whatsapp sadece profil verilerini sunucularında sakladığından içeriğin kişileştirilmesi söz konusu değildir.

Gizlilik sözleşmeleri incelenen Facebook, Whatsapp, Twitter ve Google gibi platformlar karşılaştırıldığında, cihaz bilgileri detaylı bir şekilde toplaması söz

konusudur. Cihaz verilerinin toplanması sosyal medya platformlarının birçok cihazda uyumlu bir şekilde çalışmasını sağlamaktadır. Platform geliştiricileri kullanıcının karşılaşmış olduğu güvenlik, hata gibi sorunlarda cihazdan gelen verileri dikkate almaktadır. Dolayısıyla cihaz içerisindeki işletim sistemi bilgisi, pil durumu, wifi veya bluetooth bağlantıları gibi birçok cihaz verisinin alınması, verilen hizmetin kalitesinin artmasına, aynı zamanda kullanılan cihaz modellerine göre sürüm geliştirmeleri planlanarak şirket içerisindeki kaynakların doğru yönetilmesi sağlamaktadır.

Verilerin üçüncü kişiler ile paylaşılması veri gizliliğinin en önemli konularından biridir. Çünkü üçüncü kişiler ile paylaşılan veriler hem kişisel veriler hem de cihaz verileridir. Örneğin bir API geliştiricisi, API'nin kullanım durumuna bağlı olarak kullanıcıların yaş ortalaması, ilgi alanları veya kullanılan cihaz sürümü gibi bilgileri temin edebilmektedir. Buradaki önemli unsur geliştiricinin topladığı veriler birçok kullanıcıdan gelen ve işlenmiş verilerdir. Dolayısıyla bu veriler şirketin gizlilik sözleşmesine bağlı olarak kişiler anonimleştirilmiş veya gerçek kişi olarak üçüncü kişilere aktarılmış olabilir. Facebook ve Youtube gibi şirketler genellikle verilerin API geliştiricileri ile paylaşılacağını belirtmiştir. Twitter gibi şirketler daha çok kullanım istatistiği analizi için kullanılan uygulamalar ile verileri paylşamaktadır. Whatsapp bir Facebook kuruluşu olduğundan daha çok reklam verisinin paylaşılması üzerine odaklanmaktadır.

TARTIŞMA VE SONUÇ

Çeşitli devletlerin ve sosyal medya platformlarının veri gizliliği politikalarının ve sözleşmelerinin incelendiği bu çalışma, verinin önemini ortaya koymaktadır. Web 2.0 ile internet sitelerinin etkileşimli olması kullanıcıların içerik üreticisi durumuna gelmesini sağlamıştır. Özellikle sosyal medya mecralarının ortaya çıkması ve akıllı telefonların yaygınlaşması kullanıcıların daha fazla içerik üretmesine ve tüketmesine imkân sağlamış, bunun sonucunda da büyük veriler oluşmaya başlamıştır. Yeni medya platformlarının kullanıcı odaklı hale gelmesi, ticari kuruluşların kullanıcılar ile ilgili daha fazla veri toplanmasına neden olmuştur. Ticari kuruluşların gizlilik sözleşmelerinde uyguladıkları politikalara bakıldığında, hizmetlerinin devam edebilmesi amacıyla kullanıcıların kişisel bilgilerini talep ettiği ve bu bilgileri analiz edip değerlendirdiği görülmüştür. Bu uygulamanın bir diğer tanımı kontroldür. Ayrıca şirketler için bu tanım iki anlama gelmektedir. İlk olarak bir bilginin var olup olmadığı hakkında kontrol etmek, ikincisi ise bu bilgileri çeşitli amaçlarla üçüncü kişiler ile paylaşmak anlamındaki yönetmektir (Sütçü, 2012: 77). Kendi başına sadece bir yığın olan veriler işlendiği zaman bir anlam ve değer kazanmaktadır. Verinin işlenmesindeki temel unsur kullanıcının sürekli izlenmesi şeklindedir. Ticari kuruluşlar elde ettikleri işlenmiş veriler ile Facebook, Twitter, Instagram veya Youtube gibi ücretsiz hizmetlerini sunabilmektedir. Uygulanan veri politikalarının sonucunda ortaya çıkan durum "Bir ürün ücretsiz ise ürün sizsiniz" cümlesiyle açıklanabilir. Bir hizmeti kullanmak için kullanıcılar para yerine verilerini ticari kuruluş ile paylaşıyorsa o ürünün ücretsiz olmadığı söylenebilir. Çünkü verilen hizmetin karşılığında kullanıcılar kişisel verilerini şirketlere vermektedir.

Devletlerin veri gizliliği uygulamalarında, ticari kuruluşların kullanıcılar açısından olumsuz durumlara sebep olmamaları için çeşitli veri gizliliği kanunları uyguladığı görülmüştür. Bilgisayar teknolojilerin başladığı Amerika, veri gizliliği yasalarının çıkmasında öncülük eden ülke olduğu ve ABD Başkanı Lyndon B. Johnson'ın 1966 yılında imzaladığı bilgi özgürlüğü yasası ile veri gizliliği kanunlarının başlangıcı olduğu görülmüştür. 1974 yılında Gerald Ford, gizlilik yasalarının daha sert olması amacıyla çalışmalar başlatılmış ve gizlilik yasası yenilenmiştir ve Ford'un imzalamış olduğu yasa ile kullanıcılar hangi bilgilerinin tutulduğunu öğrenmek, bilgilerini görmek veya doğruluğunu sorgulayabilmek gibi haklara sahip olduğu görülmüştür. 1988 yılında

çıkarılan bilgisayar güvenliği yasası ile hassas verilerin tutulduğu merkezlerin koruması amaçlanmıştır. Verilerin korunması ve belirli standartların sağlanması amacıyla ABD içerisindeki her bir eyalette bilgi güvenliği ofisi kurulması, ülke içerisindeki ortak kanunlardan biridir. Oklahoma Eyaleti bilgi güvenliği yönetimini başlatmak, uygulamak, sürdürmek ve iyileştirmek amacıyla eyalet içerisindeki ticari kuruluşların ISO / IEO 17799 standartlarını karşılayan bilgi sistemleri kullanmasının zorunda olduğu görülmüştür. Oklahoma gibi eyaletler ISO standartlarına göre verilerini korumaya alması, standartların uluslararası düzeye çıkmasını sağlamıştır. California ve Batı Virginia eyaletleri, her yıl veri güvenliği konusunda karşılaşılabilecek sorunlara karşı ticari kuruluşlar, örnek olay çalışma yapmaktadır. Washington eyaleti, yetkililer araçlıyla yılda bir kez ve üç yılda bir kez şeklinde bağımsız denetçiler tarafından ticari kuruluşların denetlenmesi öngörülmüştür. Benzer bir şekilde Florida eyaleti ticari kuruluşların üç yılda bir denetlenmesi kararlaştırılmıştır. ABD'yi kapsayan genel veri koruma yasasının yanında eyaletlerin standartlaştırılmamış veri gizliliği politikaları uygulaması, bazı eyaletlerde veri korumasının güçlü bazı bölgelerde zayıf kalmasına neden olmuştur. Bu durum verilerin çalınması veya verilerin ihlal edilmesi gibi sorunlara yol açabilmektedir.

Veri gizliliği politikalarında Almanya ABD'ye benzer bir şekilde eyaletlerden oluşan bir yapıya sahiptir ve veri gizliliği yasaları 1970 yılında Hesen Eyaleti tarafından kabul edilen ve 1977 yılında yürürlüğe giren veri koruması yasası ile başlamaktadır. 1983 yılında Almanya'da yaşayan kişilerin bilgi edinmesinin anayasal bir hak olduğu belirtildiği görülmüştür. 1988 yılına yasa yenilenmiş ve Almanya'nın Avrupa Birliği üye ülkesi olması dolayısıyla 2016 yılında birlik içerisinde çıkarılan veri gizliliği yasasına bağlanmıştır. Veri gizliliği yasasına göre, kişisel veri olarak tanımlanan ırk, etnik köken, siyasi görüş, dini ve felsefi bilgiler, biyometrik veriler ve sağlık verileri kişilerin izni olmadan kullanılması yasaklanmıştır. Ayrıca kişiler bilgilerini talep etme, doğruluğunu sorgulama ve bilgilerinin silinmesi talebinde bulunabilmektedir. Ancak istisnai olarak devletlerin milli güvenlik veya kamu güvenliği durumlarında hukuki süreçlere zarar vermeyecek şekilde kişilerin verilerini ticari kuruluşlardan talep edebileceği görülmüştür. Yasada kişilerin ticari kuruluşlara karşı korunması amaçlanırken güvenlik protokolleri gerekçesiyle devletlerin kişilerin verilere ulaşması istisnaya tabidir. Avrupa Birliği üye ülkelerinin uymakla yükümlü olduğu veri gizliliği yasasında bazı istisnalar

bulunmaktadır. Örneğin uluslararası bir ticari kuruluşun veri ihlali yapması durumunda kuruluşun veri merkezi Fransa'da ise o ülke içerisinde yasal işlemler yapılabilmektedir.

Türkiye'de veri gizliliğinin korunması amacıyla yasaların geç yürürlüğe girdiği söylenebilir. Bir devlet kurumu olan PTT, kişilerin verilerini gizli tutmak amacıyla bazı yasal düzenlemeler yapmıştır. 1950'de çıkarılmış olan posta kanunu, kişilerin postalarının içeriği, mektupların açılması ve üçüncü kişilere verilmesinin engellenmesi gibi durumlar 7451 sayılı kanunda belirtilmiştir. 1973 yılında kanun yenilenerek posta sorumlusu kavramı genişletilmiş detaylı açıklanmıştır. Türkiye'de 2016 yılında Kişisel Verilerin Korunması Kanunu ile veri gizliliği konusunda önlemler alınmıştır. Kanunun içeriğinin Avrupa Birliği veri gizliliği yasasının içeriğine benzer olduğu görülmektedir. Her kanunda da kişisel verilerin işlenmesi ve üçüncü kişilerle paylaşılması açık rızaya tabi olması, verilerin veri sorumluları tarafından güvence altına alınması, bilgi edinme hakkı gibi unsurlar bulunmaktadır. Türkiye'de bireyler yaşamış oldukları kişisel veri ihlali durumlarında Kişisel Verileri Koruma Kurumu[27] ile iletişime geçebilir ve yasal haklarını kullanabilirler.

Türkiye 2007 yılında internet ortamında yayınlanan içeriklere yönelik yasa ile internet içerisinde bulunan içeriklerin yetkili merciler tarafından denetlenmesi ve erişim sağlayıcılar aracılıyla erişimin engellenmesi sağlanmıştır. 21 Temmuz 2020 tarihinde 2007 yılında çıkarılmış olan kanuna bazı düzenlemeler getirilmiştir. Teklif Türkiye'de bir milyondan fazla kullanıcısı bulunan sosyal medya sağlayıcılarının Türkiye'de temsilci bulundurmasını zorunlu hale getirmiştir. Böylelikle devletin yetkili mercileri yaşanan bir kişilik ihlal durumunda içeriğin kaldırılması için temsilciye bildirimde bulunulabilecektir. Temsilci gelen bildirim üzerinde 24 saat içerisinde içeriğin kaldırılmasını sağlayacak ayrıca kullanıcılarından gelen talepleri de en geç 48 saat içerisinde olumlu veya olumsuz şekilde cevaplandırılacaktır. 2.3.1. başlığında kanun içerikleri incelediğinde, evrensel olan sosyal medya platformlarının yerelleştirilme çabası olarak görülebilmektedir. Özellikle kanun maddesinde belirtildiği gibi kişilik ihlalleri durumlarında devletler karşılarında bir muhatap bulamadıklarından yaptırımları etkisiz kalmaktadır. Sosyal medya sağlayıcılarına getirilen temsilci bulundurma zorunluluğu ile devletin yaptırımları güçlenecektir. Bu açıdan bakıldığında herhangi bir ihlal yaşanması

[27] Kişisel Verileri Koruma Kurumu "sikayet.kvkk.gov.tr" adresi üzerinde şikayet taleplerini almaktadır.

durumunda artık bir yaptırım olacağından olumlu olarak görülebilmektedir. Ancak içeriklerin mahkeme kararları ile kaldırılması internetin olumsuz içeriklerin olmadığı tertemiz bir yapıya dönüşmesine yol açabilmektedir. Dolayısıyla burada devlet tarafından bir denge belirlenmesi gerekmektedir. Kanunda belirtildiği gibi gerçek ihlal durumlarında içeriğin kaldırılması doğru ancak kaldırma işlemlerinin tüm internet içeriklerine uygulanması ifade ve haber alma özgürlüğü açısından olumsuz durumlara yol açacaktır.

Devletler belirli kanun ve düzenlemeler ile kişisel verilerin güvence altına alınmasını sağlamışlardır. Kanunlarda belirtilen verilerin işlenmesi için kullanıcıların onayı gerekmektedir. Dolayısıyla ticari kuruluşlar imzalattıkları sözleşmeler ile verilerin işlemesini yasal hale getirmektedir. Araştırmada incelenen Facebook, Twitter, Instagram, Youtube, Whatsapp gibi sosyal medya platformlarının kullanıcılarından aldığı veriler gizlilik sözleşmelerinde açık şekilde belirtilmiştir. Örneğin kullanıcıların platform içerisindeki paylaşımlarının yanı sıra akıllı telefonlarının işletim sistemi, donanım özellikleri, pil seviyesi, cihaz içerisindeki dosyalar, ip adresleri gibi kullanıcıyı tanımlayan bilgilere ulaşılmaktadır. Aynı zamanda toplanan verilerin çalışma ortakları ve üçüncü kişilerle de paylaşıldığı da görülmektedir. Sözleşme içerisinde kullanıcılar Avrupa Birliği gizlilik sözleşmesinde olduğu gibi kullanıcı verileri, verilerin doğruluğunu ve tüm bilgilerinin silinmesini talep edebilmektedir. Ayrıca bilgilerin tüm sunuculardan silinmesi işleminin 30 gün içerisinde başlatılacağı bilgisi sözleşmede yer almaktadır.

Devletlerin oluşturmuş olduğu yasalar her zaman veri korunmasını sağlayamamaktadır. 2014 yılında Facebook ve Cambridge Analytica şirketleri kullanıcı verilerin yasal olmayan yollarla nasıl işlediğine dair örnek gösterilebilir. Cambrige Analytica, yaklaşan ABD Başkanlık Seçimleri için Amerikalı seçmenlerin olduğu profillerin bulunduğu aktivite verilerini Facebook tarafından talep etmiş ve çeşitli algoritmalar ile kimlerin hangi adaylara sempati duyduğu konusunda fikir edinilmiş ve seçim kampanyası ortaya çıkan analizlere göre planlanmıştır. Olayın ortaya çıkması sonucunda Facebook'a para cezası kesilmiş ve Cambridge Analytica kapatılmıştır. Türkiye'de yaşanmış olan kredi kartı bilgisinin çalınması olayı, Singapur'lu bir siber güvenlik şirketi tarafından tespit edilmiş ve 460 bin verinin Deep Web'te yayınladığını ortaya çıkarmıştır. Veri ihlalinin sanal mağazaların alışveriş sırasında kullanıcıların kredi kartı bilgilerini kaydetmesi sebebiyle olduğu tahmin edilmektedir. Konuyla ilgili Türkiye de resmi bir açıklama yapılmadığı görülmüştür. Mastercard'ın Almanya'da gerçekleşen

kullanıcı verilerinin çalınması durumunda yaklaşık 90 bin kullanıcının isim, telefon numarası, kredi kartı bilgisi gibi verilerin çalındığı tespit edilmiştir. Firma veri ihlali sonrasında tüm kullanıcıların kredi kartlarını dondurmuş ve internet sayfalarını kapattığı görülmüştür. Veri ihlali örneklerine de bakıldığında kişisel veriler internet ortamlarında ticari kuruluşlar tarafından ihlal edileceği gibi üçüncü kişilerin veri merkezlerine girmesi şeklinde de yapılabilmektedir. Bu durumlar göz önüne alındığında merkezlerin Oklahoma Eyaletinde olduğu gibi verilerin ISO standartlarında korunması veri merkezleri ve ticari kuruluşlara katkı sağlayacaktır. Ancak veri ihlallerinin önlenmesi sadece yasalar veya ticari kuruluşların alacağı önlemlerle değil aynı zamanda kullanıcıların medya etiği ve medya okuryazarlığı alanlarında bilinç kazanmasıyla mümkündür. Veri gizliliği ile ilgili Kaspersky'ın 2020 yılında yapmış olduğu araştırmada kullanıcıların yüzde 47'sinin internet üzerinde anonim kalmaya çalışması, kullanıcıların gizlilikle ilgili endişelerinin olduğunu görülmektedir.

Çalışmada *"Sosyal medya platformlarının gizlilik sözleşmeleri hangi şartları içermektedir?"* ve *"Sosyal medya platformlarında toplanan veriler hangi amaçlar için kullanılmaktadır?"* sorularına bakıldığında, sosyal medya platformlarının kullanıcı verilerinin analiz edilmesi üzerine kurulu bir sistem olduğu görülmektedir. Bunun sebebi platformların ücretsiz olarak kullanıcılara sunulmasıdır. Platformlar gizlilik sözleşmeleri ile kullanıcıların verilerinin toplaması ve işlenmesi onayı alınmaktadır. Böylelikle devletlerin belirlemiş olduğu yasal sınırlar şirketler tarafından aşılmaktadır. Facebook, Whatsapp, Twitter ve Youtube gibi platformların gizlilik sözleşmeleri incelediğinde tüm platformların kullanıcı verilerini topladığı görülmüştür. Ayrıca platformun üçüncü kişilerle (Çalışma ortakları, Api geliştiricileri vb.) verileri paylaşması gibi durumların olduğu da görülmüştür. Platformların toplamış olduğu kişiler veriler incelediğinde yaş, cinsiyet, ilgi alanları ve hobiler gibi bilgilerin yanında kullanıcıların platform içerisindeki aktiviteleri ön plana çıkmaktadır. Kullanıcının paylaştığı içerikler, beğendiği veya etiketlediği sayfalar, izlediği videolar, sayfada gösterilen hangi reklamın ilgisini çektiği gibi detaylı bilgiler işlenmektedir. Elde edilen veriler ile reklam gibi içerikleri kişiselleştirerek kullanıcıların satın alma alışkanlıklarında olumlu yönde etkileme yaşanabilir. Geçtiğimiz yıllarda Cambrige Analytica'nın ABD başkanlık seçimi için kullanıcıların verilerini toplayarak çeşitli analizler yapmıştır. Bu şekilde seçim kampanyası daha iyi yönetilmiştir. Platformlar sadece kişisel veri değil aynı zamanda

kullanıcıların cihaz verilerini toplamaktadır. Böylelikle platformlar sundukları hizmeti geliştirmektedir. Sonuç olarak platformlar topladıkları veriler ile kullanıcıların bilgileri ve faaliyetlerini analiz edip değerli birer veri haline getirmeyi amaçlamaktadır ve gizlilik sözleşmelerinde bu durum açıkça belirtilmiştir. Bu şekilde platformların ücretsiz olarak elde ettiği veriler ile şirketler mali kazanç sağlamaktadır.

Çalışmanın diğer bir sorusu olan "Türkiye'deki veri koruma kanunları ve uygulamaları nelerdir?" sorusuna baktığımızda, Türkiye'nin veri gizliliği konusundaki gelişimini posta dağıtımı sürecinde gönderileri içeriklerinin gizli kalması amacıyla çeşitli kanunlar çıkarılmıştır. Ancak bilgisayar teknolojilerinin veri gizliliği konusu ABD ve Almanya gibi ülkelerden geri kaldığı görülmektedir. Bilgisayar teknolojilerinin Amerika'da gelişmesi ve gündelik hayatta bilgisayar kullanımının artması veri gizliliği kavramlarını gündeme getirmiştir. Bunun üzerine Amerika çeşitli yasalar ile kişilerin veri gizliliklerini güvence altına almıştır. Özellikle Avrupa'ya da bilgisayar ve internet teknolojilerinin gelmesiyle veri gizliliği konusunda farkındalıklar oluşmaya başlamış ve Almanya'nın Hesen eyaletinde ilk veri gizliliği kanunu çıkarılmıştır. Veri gizliliği konuları bu iki ülkede günümüze kadar gelişmesine rağmen Türkiye'de 2016 yılına kadar herhangi bir gelişme yaşanmamıştır. 2016'da Avrupa Birliği veri gizliliği kanunları çıkarmıştır ve Türkiye bu kanunları KVKK adıyla ülkesinde yürürlüğe sokmuştur. Bu tarih itibarıyla Türkiye'deki veri gizliliği kanunları Avrupa standartlarına ulaşmıştır. Buradaki önemli nokta ülkelerdeki veri gizliliği kanunlarının uygulanması amacıyla devletlerin şirketleri denetlemesidir.

Kullanıcıların verilerini teslim etmeden önce ticari kuruluşların sözleşmelerini iyice okumaları ve hangi verilerin ticari kuruluş tarafından alınacağını anlamaları önem arz etmektedir. Veri ihlali örneklerine bakıldığında verilerin gizliliğin ihlalinin önlenmesi büyük orada kullanıcıların tutumlarına bağlıdır ve bölüm 3.7'de bahsedilen verileri koruma yollarıyla kullanıcıların karşılaştıkları veri ihlallerini en aza indirebilecekleri fakat verilerini tamamen gizli tutmalarının pek mümkün olmadığı sonucuna varılmıştır.

KAYNAKÇA

″1974 Privacy Act: Ford Library Museum″. 9 Ekim 2019 tarihinde https://www.fordlibrarymuseum.gov/library/document/factbook/privacy.htm adresinden erişildi.

"Cisco Visual Networking Index: Forecast and Trends, 2017–2022". Cisco White Papers. 22 Eylül 2019 tarihinde, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc532256790 adresinden erişildi.

"Data Leak Affects Mastercard". Decisionmarketing. 11 Mayıs 2020 tarihinde, https://www.decisionmarketing.co.uk/news/not-quite-so-pricelepp.-data-leak-affects-mastercard adresinden erişildi.

"Data Security Laws: State Government". National Conference Of State Legislatures. 22 Şubat 2020 tarihinde, https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx adresinden erişildi.

"Defending Digital Privacy: Taking Personal Protection To The Next Level". Kaspersky. 2 Haziran 2020 tarihinde, https://www.kaspersky.com/blog/global-privacy-report-2020/ adresinden erişildi.

"E-Ticaret ve E-Ticarette Dikkat Edilmesi Gerekenler". Güvenli Web. 5 Haziran 2020 tarihinde, https://www.guvenliweb.org.tr/blog/e-ticaret-ve-e-ticarette-dikkat-edilmesi-gerekenler adresinden erişildi.

"Facebook Newsroom". Facebook. 30 Ekim 2019 tarihinde, https://newsroom.fb.com/company-info/ adresinden erişildi.

"Facebook Veri İlkesi". Facebook. 30 Ekim 2019 tarihinde, https://www.facebook.com/privacy/explanation adresinden erişildi.

"General Data Protection Regulation (GDPR)". 14 Nisan 2020 tarihinde, https://gdpr-info.eu/ adresinden erişildi.

"Google Flu Trends". Google. 23 Ağustos 2019 tarihinde, https://www.google.org/flutrends/about/ adresinden erişildi.

"Güçlü Parola Oluşturma". Tübitak. 7 Mayıs 2020 tarihinde, http://www.bilgimikoruyorum.org.tr/?b222_guclu_parola_olusturma adresinden erişildi.

"Hizmet Koşulları-Youtube". Youtube. 28 Ağustos 2019 tarihinde, https://www.youtube.com/static?gl=TR&template=terms adresinden erişildi.

"How Much Data On The Internet". Sharpcorner. 29 Kasım 2019 tarihinde, https://www.c-sharpcorner.com/article/how-much-data-is-on-the-internet/ adresinden erişildi.

"Huge Set Of Turkish Banks Cards On Sale On Dark Net Marketplace". Group IB. 7 Haziran 2020 tarihinde, https://www.group-ib.com/media/turkish-banks-cards/adresinden erişildi.

"ISO/IEC 17799:2005". ISO. 5 Haziran 2019 tarihinde, http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/96/39612.html adresinden erişildi.

"Kamuoyu Bilgilendirmesi". BKM. 10 Haziran 2020 tarihinde, https://bkm.com.tr/kamuoyu-bilgilendirmesi/ adresinden erişildi.

"Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular". Kişisel Verilerin Korunması Kanunu. 12 Kasım 2019 tarihinde, https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular adresinden erişildi.

"Mastercard Pricelepp. Specials ". Firefox Monitor. 5 Mayıs 2020 tarihinde, https://monitor.firefox.com adresinden erişildi.

"Press Youtube ". Youtube. 28 Ağustos 2019 tarihinde, https://www.youtube.com/intl/en-GB/yt/about/press/ adresinden erişildi.

"Priceless Cities". Mastercard. 7 Haziran 2020 tarihinde, https://www.priceless.com/terms/tr_TR adresinden erişildi.

"PTT Hakkında". 6 Eylül 2019 tarihinde, https://www.ptt.gov.tr/Sayfalar/Kurumsal/Hakkimizda.aspx adresinden erişildi.

"Son Üç Ay İçinde Bireylerin Yaş Grubuna Ve Cinsiyetine Göre Bilgisayar Ve İnternet Kullanım Oranları 2004-2019". Türkiye İstatistik Kurumu. 2 Haziran 2020 tarihinde, www.tuik.gov.tr/PreIstatistikTablo.do?istab_id=2603 adresinden erişildi.

"TDK Zorbalık". Türk Dil Kurumu. 22 Ocak 2019 tarihinde, http://www.tdk.gov.tr/index.php?option=com_gts&kelime=ZORBA adresinden erişildi.

"TLS 1.3 Nedir ve Nasıl Çalışır?". Medianova 29 Kasım 2019 tarihinde, https://www.medianova.com/tr-blog/2018/11/29/tls-1-3-nedir-nasil-calisir adresinden erişildi.

"Twitter Kuruluş Tarihi". Twitter. 3 Mart 2020 tarihinde, https://twitter.com/jack/status/20 adresinden erişildi.

"Twitter Privacy Policy". Twitter. 13 Eylül 2019 tarihinde, https://cdn.cms-twdigitalapp.ets.com/content/dam/legal-twitter/site-app.ets/privacy-page-gdpr/pdfs/PP_Q22018_April_EN.pdf adresinden erişildi.

"ULAKNET Uç İstatistikleri". Tübitak. 23 Mayıs 2020 tarihinde, https://stat.ulakbim.gov.tr/ulaknet/omurga_details.php?name=toplam-internet&type=bps&dev=anauc&place=omurga&details=yes adresinden erişildi.

"Veri Sorumlusu ve Veri İşleyen". Kişisel Verileri Koruma Kurumu. 17 Eylül 2019 tarihinde, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf adresinden erişildi.

"WhatsApp Hakkında". WhatsApp. 16 Ocak 2020 tarihinde, https://www.whatsapp.com/about/ adresinden erişildi.

"WhatsApp Legal Info". WhatsApp. 16 Ocak 2020 tarihinde, https://www.whatsapp.com/legal/#privacy-policy adresinden erişildi.

"WhatsApp Yasal Bilgiler". WhatsApp. 13 Mayıs 2020 tarihinde, https://www.whatsapp.com/legal/#key-updates adresinden erişildi.

“Inflation Calculator" 18 Haziran 2020 tarihinde https://www.officialdata.org/us/inflation/1843?amount=30000 adresinden erişildi.

Akgül, M., ve Akdağ, M. (2017). Türkiye'de Yeni Medya Eğitimi Üzerine Niceliksel Bir Betimleme. Erciyes Üniversitesi İletişim Dergisi, 5(1), pp. 210-220.

Altınbaş.A. (2018). Sağlıkta Büyük Verinin Önemi. Ortadoğu Tıp Dergisi. 10(2), pp. 216-219.

Avrupa İnsan Hakları Sözleşmesi, (2010). Erişim adresi: https://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf

Aydoğan, F., & Kırık, A. M. (2012). Alternatif Medya Olarak Yeni Medya. Akdeniz Üniversitesi İletişim Dergisi 18, pp. 58-60.

Baudrillard, J. Sepp.iz yığınların gölgesinde ya da toplumsalın sonu. Ayrıntı, İstanbul, 1991.

Bulat, M. (2007). Form ve Kompozisyon. Atatürk Üniversitesi Sanat Dergisi, 12, pp. 73-78.

Cadwalladr, C. ve Graham-Harrison, E. (17 Mart 2018). Revealed: 50 million Facebook Profiles Harvested For Cambridge Analytica In Major Data Breach. The Guardian. 20 Nisan 2020 tarihinde, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election adresinden erişildi.

Castells, M. Communication Power. Oxford University Prepp.. Great Britain, 2009.

Choudhury, N. (2014). World Wide Web and Its Journey from Web 1.0 to Web 4.0. International Journal Of Computer Science Technologies, *5(6)*, 8096-8100.

Confepp.ore, N. (4 Nisan 2018). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. The New York Times. 5 Mayıs 2020 tarihinde, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html adresinden erişildi.

Çakirel, Y. (2016). İşletmelerde Büyük Veri. Kırklareli Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi. 5(1), pp. 52-62

ÇeliK, A. G. Y. (2017). Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı. Türkiye Adalet Akademisi Dergisi. 32, pp. 387-406.

Davies, H. (11 Aralık 2015). Ted Cruz Campaign Using Firm That Harvested Data On Millions Of Unwitting Facebook Users. The Guardian. 5 Mayıs 2020 tarihinde, https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data adresinden erişildi.

Deniz, Y. (2012). Yeni Medya Ve. Sütçü, C. (Yay. Haz.) Sosyal Medyaya Girmeden Önce Bilinmesi Gerekenler. Anahtar Kitaplar.

E-Ticaretin Gelişimi, Sınırların Aşılması ve Yeni Normlar 2019. Deloitte Digital. İstanbul, 2019. Erişim adresi: https://www.eticaretraporu.org/wp-content/uploads/2019/05/DD-TUSIAD-ETicaret-Raporu-2019.pdf

Facebook'a Cambridge Analytica skandalı nedeniyle 5 milyar dolar ceza kesilecek. (13 Temmuz 2019). BBC News Türkçe. 6 Mayıs 2020 tarihinde, https://www.bbc.com/turkce/haberler-dunya-48974921 adresinden erişildi.

Flaherty, D. H. Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States. The University Of North Carolina Prepp.. London, 1989.

Fowler, J. ve Rood, E. (2013) Web 4.0 The Ultra Intelligent Electronic Agent is Coming. Bigthink. Erişim adresi: https://bigthink.com/big-think-tv/web-40-the-ultra-intelligent-electronic-agent-is-coming

Georgiadou, E. (1995). Marshall McLuhan's 'global village' and the Internet. University Of Kent At Canterbury. Erişim adresi: https://doi.org/10.13140/rg.2.1.1490.1282

Glickman, D. (1 Ağustos 1988). H.R.145 - 100th Congrepp.: Computer Security Act of 1987. 12 Ağustos 2020 tarihinde, https://www.congress.gov/bill/100th-congrepp./house-bill/145 adresinden erişildi.

Güngör, N. İletişim Kuram ve Yaklaşımlar. Siyasal Kitabevi. Ankara, 2018.

Hansen, L. (20 Mart 2018). 5 Soruda Facebook Veri Skandalı. 6 Mayıs 2020 tarihinde, https://www.dw.com/tr/5-soruda-facebook-veri-skandal%C4%B1/a-43055462 adresinden erişildi.

Harley, O. (13 Nisan 2018) Did Facebook Warn You That a Friend Used The This Is Your Digital Life App? Here's What That Means. HelloGiggles. 5 Mayıs 2020 tarihinde, https://hellogiggles.com/news/facebook-this-is-your-digital-life-app/ adresinden erişildi.

Hisseleri Yüzde 2'Ye Yakın Yükseldi. (15 Temmuz 2019) Habertürk. 5 Haziran 2020 tarihinde, https://www.haberturk.com/facebook-5-milyar-dolar-ceza-yedi-ucusa-gecti-2504467-teknoloji adresinden erişildi.

Işık, M. Küreselleşme ve Medya Sistemleri Üzerine Etkileri. Işık M. (Yay.Haz.). Medyada Yeni Yaklaşımlar. Eğitim Kitabevi. İstanbul, 2004

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun Teklifi (21 Temmuz 2020) (Sayı: 2/3050). https://www2.tbmm.gov.tr/d27/2/2-3050.pdf

Kesim, E. ve Ağaoğlu, E. (2007). A Paradigm Shift in Distance Education: Web 2.0 and Social Software. Turkish Online Journal of Distance Education, 8(3), pp. 66-75.

Kiliç, H., Atalay, E. ve Yurtsever, A. E. (2019). Büyük Veri (BigData) Ve Müşteri İişkileri Yönetimi (CRM) İşbirliğinin Pazarlama İletişimi Stratejilerindeki Rolü: Büyük Ölçekli Özel Bir Banka Örneği. Stratejik ve Sosyal Araştırmalar Dergisi, *3*(2), 289-310.

Kişisel Verilerin Korunması Kanunu. (24 Ocak 2016). (Sayı: 29677) Erişim adresi: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

Korcan Arslantekin, D. (2016). Büyük veri: Önemi, yapısı ve günümüzdeki durum. Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi, *56*(1), 15-36.

Küçük, M. E. ve Al, U. (2001). Metadara Kavramı. Bilgi Dünyası Dergisi, 2(2), pp. 169-187.
Küçükcan, B. (2006). Dünden Bugüne Matbaanın Serüveni. Türk Kütüphaneciler Derneği İstanbul Şubesi. pp. 158-172

Loiselle, S. (6 Eylül 2018). SSL nedir, ne işe yarar? 7 Haziran 2020 tarihinde, https://tr.godaddy.com/blog/pp.l-nedir-ne-ise-yarar/ adresinden erişildi.

Martin, S. (2019). Freedom of Information Act 1966. Encyclopedia Britannica. 25 Kasım 2019 tarihinde, https://www.britannica.com/topic/Freedom-of-Information-Act adresinden erişildi.

Nath, K. ve Iswary, R. (2015). What Comes after Web 3.0? Web 4.0 and the Future. International Conference on Computing and Communication Systems. Erişim adresi: https://www.researchgate.net/publication/281455061_What_Comes_after_Web_30_Web_40_and_the_Future

Özel Hayatın Gizliliği Ve Korunması (18 Ekim 1982) (Sayı: 17863). https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf

Posta Kanunu. (12 Nisan 1973). (Sayı:1909). Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin/2.5.76156.pdf

Posta Kanunu. (2 Mart 1950). (Sayı:7451). Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.3.5584.pdf

Raul, A. C. The Privacy Data Protection And Cybersecurity Law Review. Law Business Research Ltd. United Kingdom, 2015

Russom, P. Big Data Analytics. TDWI Research, 2011

Şen, E. (1993). Avrupa İnsan Hakları ve Ana Hürriyetlerine Dair Sözleşme'de Özel Hayatın Gizliliği ve Korunması Hakkı ve Türk Hukuku. İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, (3-4-5), 141.

Taylor, K. (2016). Big Data: Understanding Big Data. Aston University. Erişim adresi: https://www.researchgate.net/publication/291229189_Big_Data_Understanding_Big_Data

Türk Kullanıcılara Ait Kredi Kartları 1 Dolara Satılıyor (12 Aralık 2019). Habertürk. Erişim adresi: https://www.haberturk.com/son-dakika-turkiye-deki-kart-bilgileri-calindi-1-dolara-satisa-cikti-haberler-2548631-teknoloji

Wilson, N. (2009). Interpreting “Google Flu Trends ” data for pandemic H1N1 influenza: The New Zealand experience. EuroSurveillance. Erişim adresi: https://www.eurosurveillance.org/content/10.2807/ese.14.44.19386-en#html_fulltext

Wu, C. J. (2011). Unpacking New Media Literacy. Systemics, Cybernetics And Informatics. *9*(2), 84.

Yanik, A. (2016). Yeni Medya Nedir Ne Değildir. Journal of International Social Research, *9*(45), 898-898.

Yaylagül, L. Kitle iletişim kuramları: Egemen ve eleştirel yaklaşımlar. Dipnot Yayınlar. İstanbul, 2010

Yurtoğlu, N. (2016). Haberleşme Sektörünün Önemli Bir Teşekkülü: Milli Mücadele Döneminden 1960 Yılına Türkiye'de Posta, Telgraf ve Telefon (PTT) Teşkilatı *1920-1960*. Kastamonu Üniversitesi. Erişim adresi: https://www.researchgate.net/publication/322314663_Haberlesme_Sektorunun_Onemli_Bir_Tesekkulu_Milli_Mucadele_Doneminden_1960_Yilina_Turkiye%27de_Posta_Telgraf_ve_Telefon_PTT_Teskilati_1920-1960.

Zeiger. R. (2009). Google Flu Trends Overview [VIDEO]. Erişim adresi: https://www.youtube.com/watch?v=6111nS66Dpk

ÖZGEÇMİŞ

SADIK AHMET ÇAVUŞOĞLU

sacavus@gmail.com | +905303102012

-

Deneyim

- ***İstanbul 29 Mayıs Üniversitesi | Kütüphaneci***
  Kasım 2019 – Halen
- ***Freelancer***
  Ağustos 2019 - Halen
- ***AjansPress | Operasyon Çağrı Merkezi Süpervizörü***
  Mart 2018 – Mart 2019
- ***AjansPress | Stajyer***
  Şubat 2018 – Mart 2018
- ***Nişantaşı Üniversitesi | Asistan Öğrenci***
  Temmuz 2017 – Ağustos 2017
- ***Nişantaşı Üniversitesi | Akademik Asistan Öğrenci***
  Temmuz 2016 – Mart 2017

Eğitim

- ***Üsküdar Üniversitesi | Yüksek Lisans***
  Yeni Medya ve Gazetecilik Tezli Yüksek Lisans
  2018 – 2020
- ***Anadolu Üniversitesi | Lisans***
  Kamu Yönetimi
  2014 – 2020
- ***Nişantaşı Üniversitesi | Lisans***
  Halkla İlişkiler ve Reklamcılık
  2014 – 2018

Sertifikalar

- ***Uygulamalı Beyaz Şapkalı Hacker Kursu***
  BUSİBER Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi
  Eylül 2018

Yetenekler

- *Adobe Photoshop*
- *Adobe After Effect*
- *Adobe Premier Pro*
- *Wordpress*
- *Microsoft Office 365*
- *Windows Server 2012 – 2019*
- *Veri Yedekleme Sistemleri*
- *DSpace Kurumsal Arşiv*
- *YORDAM Kütüphane Otomasyon Sistemi*
- *UDOO CRM Sistemi*