# VERİ GİZLİLİĞİ POLİTİKASI BAĞLAMINDA SOSYAL MEDYA PLATFORMLARININ İNCELENMESİ

**Sema Bulat Demir[1], Ayten Övür .[2]**

[1] *Sema BULAT DEMİR, (Turkey)*

[2] *Ayten ÖVÜR, (Turkey)*

*e-mail: semabulat@aydin.edu.tr*

*aytenövür@aydin.edu.tr*

## Öz

Günümüzde internet kullanıcıları tarafından sosyal medya platformları sıklıkla kullanılmaktadır. Bu platformlara üyelik oluşturulurken veri gizliliği politikasının kullanıcı tarafından onaylanması gerekmektedir. Veri gizliliği politikalarının dikkatli bir şekilde incelemeden onay verildiği göz önünde bulundurulduğunda kullanıcı açısından birçok sorun ortaya çıkabilmektedir. Veri politikasına onay verilmesiyle kullanıcıların platformlardaki her aktivitesinin gözetlenmesi, güvenlik, kişisel verilerin korunması, kullanıcı verilerinin ticari amaçlı üçüncü sahışlarla paylaşımı gibi başlıca sorunlar ortaya çıkabilmektedir. Bu noktada sosyal medya platformlarının veri gizliliği politikalarını detaylı bir şekilde incelemek önem arz etmektedir. Bu doğrultuda çalışma kapsamında 30 Ocak 2021 tarihinde Google Play Store platformunun haberleşme kategorisindeki ücretsiz en popüler ilk beş uygulamanın veri gizliliği politikaları incelenmiştir. Bu uygulamaların veri gizliliği politikaları içerik analizi tekniğiyle analiz edilmiştir. Böylece en çok kullanılan bu uygulamaların kullanıcıdan sağladığı izinli ya da izinsiz veri türleri ve bu verilerin kullanım alanları ortaya çıkarılmaya çalışılmıştır.

***Anahtar Kelimeler:*** *Veri Gizliliği Politikası, Sosyal Medya, Veri Madenciliği, Kişisel Verilerin Korunması Kanunu, Gözetim.*

## Giriş

Günümüzde sosyal medya platformlarının toplumun büyük bir bölümü tarafından aktif bir biçimde kullanıldığı bilinmektedir. Sosyal medya platformlarının sunduğu iletişim kurma, haberleşme, eğlenme, gündemi takip etme, görüş bildirme gibi birçok hizmet kullanıcının sosyal medya kullanım motivasyonlarını oluşturmaktadır. Kullanıcıya sağlanan bu ücretsiz hizmetlere karşılık kullanıcının da birtakım verilerini kendi rızası ile platformlara sunması gerekmektedir. Böylece kullanıcı ve sosyal medya platformları arasında sürekli devam süren bir veri alış-verişi söz konusu olmaktadır. İki taraf arasında gerçekleşen bu veri alış-verişi kullanıcının platformlara üyelik oluşturmasıyla başlamaktadır. Üyelik işlemleri sırasında her platformun kendine ait olan *veri gizliliği politikası*nın kabul edilmesi gerekmektedir.

Türkiye'de dijital ortamlarda kullanıcının kişisel veri güvenliğinin korunması ve olası ihlalleri engellemek amacıyla 07.04.2016 tarihli ve 29677 sayılı Resmi Gazete'de *Kişisel Verilerin Korunması Kanunu* (URL-1) adıyla yürürlüğe giren kısaca KVKK bulunmaktadır. KVKK'nın kapsamı *"Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."* şeklinde belirtilmiştir. Amacı ise *"kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."*. Kişisel veriler, kanunun beşinci maddesinde *"ilgili kişinin açık rızası olmaksızın işlenemez."* şeklinde belirtilmiştir.

Günümüzde kullanıcıların platformlara üyelik oluştururken veri gizliliği politikalarını dikkatli bir şekilde incelemeden onay verdiği göz önüne alındığında, bu durumun kullanıcıların birtakım problemlerle karşılaşabileceğini göstermektedir. Oluşabilecek bu problemler arasında, kullanıcıların platformdaki her aktivitesinin gözetlenmesi, güvenlik, gizlilik, kişisel verilerin korunmaması, kullanıcı verilerinin ticari amaçlarla üçüncü sahışlarla paylaşımı

DOI NO: 10.17932/CTC.2021/ctc21.034

yer almaktadır. Bu noktada sosyal medya platformlarının veri gizliliği politikalarının onaylanması ile kullanıcının ne tür verilerinin toplandığı ve hangi amaçlar doğrultusunda bu verilerin kullanıldığının incelenmesi önem arz etmektedir. Bu kapsamda çalışmada 30 Ocak 2021 tarihinde Google Play Store platformunun haberleşme kategorisinde yer alan ücretsiz en popüler ilk beş uygulamanın veri gizliliği politikaları incelenmiştir.

## Endüstri 4.0

Endüstri 4.0, bir ürünün üretiminin, kullanımının, dağıtımının, tamirinin ve geri dönüşümünün insan katkısı olmadan tam otomatik bir biçimde internet üzerinden değişik teknolojilerin entegre edilerek yapılması demektir. Endüstri 4.0, ekonomik büyüme vaat eden bir ideolojidir. Nesnelerin interneti, büyük veri, bulut bilişimi, sosyal medya, çipler, sensörler, yapay zeka ve robotbilimin yaygınlaştırılması ve bu teknoloji kombinasyonları ile fiziki malların üretimi, dağıtımı ve kullanımının yayılmasını sağlayan bir konsepttir (Fuchs, 2020: 70).

Endüstri 4.0 birçok çağdaş otomasyon sistemini, üretim teknolojilerini ve veri alışverişlerini içeren kollektif bir terimi ifade etmektedir. Endüstri 4.0'ın ayırt edici en önemli unsurları üç başlıkta toplanmaktadır: Hız: Yeni dönemdeki endüstriyel gelişmeler çok büyük hızla ilerlemektedir. Yeni bir teknolojik gelişmeye çok sık rastlanmakta, yeni teknolojik gelişmeler, daha yenilerinin önünü açmaktadır. Genişlik ve Derinlik: Yeni dönemdeki gelişmeler dijital devrim üzerine gelişmektedir. Ancak bu hızlı gelişme sadece üretim yapısını değil iş dünyasında, toplumda ve bireyin yaşam koşullarında derin değişikliklere neden olmaktadır. Sistem Etkisi: Yeni dönem, şirketlerin, sektörlerin ama aynı zamanda ülkelerin yapısını (sistemlerini) değiştirmekte ve sistemlerin bütünsel dönüşümünü içermektedir (Özsoylu, 2017: 46).

İnovasyon, dijital teknoloji ve bilişim tabanlı bu yeni üretim modeli, üretim süreçlerinin her aşamasını değiştirmekte ve makinelerin birbirleriyle haberleştiği yeni bir üretim sistemi, internet aracılığıyla işgücü ve hatta makineler arası iletişimin yaşandığı ve robotların aktif olarak üretim sürecinin en önemli aktörleri haline geldiği yeni bir üretim düzenidir (Büyükuslu, 2017: 77). Nesnelerin internetinin, bütünleşik bir küresel ağ üzerinde her şeyi herkes ile birbirine bağlayacağı ön görülmektedir. İnsanlar, makineler, üretim hatları, lojistik ağları, doğal kaynaklar, tüketim alışkanlıkları, geri dönüşüm süreçleri sosyal ve ekonomik hayatın her noktası sensörler ve yazılımlar aracılığıyla nesnelerin interneti platformunu oluşturmaktadır. Bu yolla büyük veri tüm düğümleriyle -evler, işletmeler, taşıtlar- gerçek zamanlı olarak birbirine bağlanmaktadır. (Rifkin, 2015: 20). Bu gelişmeler karşısındaysa beyinlerimiz teknolojiye uyum sağlamak için değişip evrimleşeceği düşünülmektedir. Ancak insan zekası artacak mı yoksa yapay zekanın gölgesinde kalarak gerileyecek mi, tarihsel süreç içerisinde ortaya çıkacaktır (Greengard, 2017: 157).

İnternet üre-tüketici metasının sömürülmesini kapitalizmin bir aşaması olarak gören Fuch'a göre, bu aşamada oyun ve emek arasındaki sınırlar bulanıklaşmakta ve oyun emeğinin sömürülmesi yeni bir ilke haline gelmektedir. Sömürü eğlence gibi hissettirme eğilimindedir ve serbest zamanın bir parçası haline gelmiştir (Fuchs, 2014: 168).

Couldry ve Mejias'a göre, veri sömürgeciliği, 21. yüzyıla özgü yeni bir sömürgecilik biçimidir. İnsanların veriler aracılığıyla sömürülmesini normalleştiren, yeni bir veri sömürgeciliği biçimi olarak gören Couldry ve Mejias, bu durumun kapitalizmin yeni bir aşamasının yolunu açtığını söylemektedir. Büyük verinin işlenmesini kapitalizmin yeni bir aşaması olarak, zamanla veri sömürgeciliğinin günümüzde öngörülemeyen ve insan yaşamının veri üzerinden düzenlenmesinin merkezi olacağı yeni bir kapitalizm biçiminin ön koşullarını ortaya çıkaracağı düşünülmektedir (Couldry ve Mejias, 2020: 15-16).

## Veri Madenciliği

Günümüzde dünyayı tehdit eden en önemli konulardan birisi *siber saldırı* ve bundan korunmak için *siber güvenlik*tir. Bu anlamda, veri madenciliğini siber saldırının daha soft bir versiyonu olarak da gören teorisyenler bulunmaktadır. Veri madenciliğinin çok net olarak kullanıldığı üç mecra şunlardır; 1) Arama motorları (Google, Yandex vs.), 2) Kredi kartları, 3) Bilgisayarlar, internet, akıllı telefonlar, uygulamalar (Bedava görüşme ve mesajlaşma yaptığımızı sandığımız aplikasyonlar, Whatsapp, FaceTime vs.dir) (Büyükuslu, 2017: 134).

Veri madenciliği, çeşitli bilgi parçaları arasında ilişkiler kurulması demektir. Özellikle yeni medya ortamlarında kullanıcıların verilerinin işlenmesi ve ortamda bırakılan dijital izler üzerinden yapılan veri eşleştirmesi ile kullanıcılara yönelik profil bilgileri çıkarılmaktadır. Böylece şirketler ürünlerini daha iyi pazarlayabilmek için kullanıcıların kişisel bilgilerini toplayıp, onları belli özelliklerine göre sınıflandırmaktadır (Binark ve Bayraktutan: 2013: 74).

DOI NO: 10.17932/CTC.2021/ctc21.034

Veri madenciliği, kişisel verilerin doğrudan ya da aynen madencilikte olduğu gibi kazıyarak bilgi ve veri toplamak suretiyle başta reklam sektörü ve pazarlama stratejisi olarak kullanılmak üzere yapılan veri analizleri sonucunda tüketici davranışlarının manipülasyonunu, diğer bir ifadeyle tüketici eğilimlerini yönlendirmeyi ve etkilemeyi amaçlamaktadır. Bu veri toplama işleminin yani veri madenciliğinin kişisel yaşama dair bilgilere, kişinin özel alanına girmesi sebebiyle etik boyutu çokça tartışma konusudur. Kişisel bilgilerin ya da verilerin mahremiyetine saldırı, kişisel özgürlük alanlarına müdahale veya kurumsal firmalar arasındaki ticari ilişkilerde elde edilen bilgilerin haksız rekabet unsuru olarak kullanılması durumunda konu kişisel özgürlüğe müdahalenin ötesinde kamusal alan ve özel sektör arasındaki ilişkiler bakımından da oldukça sıkıntılı sonuçlar doğurabilmektedir (Büyükuslu, 2017: 133).

İnternet ve sosyal medyanın kimin kontrolünde ya da sahipliğinde olduğuna yönelik mülkiyet ilişkileri de kullanıcılar açısından risk yaratmaktadır. Örneğin Twitter ve facebook gibi sosyal ağlar bir yandan bireye kendini ifade etme özgürlüğü verirken diğer yandan onun tüm kişisel bilgilerinin fikirlerinin kayıt altına alındığı bir fişleme mekanizması olarak karşısına çıkabilmektedir (Sayımer, 2014: 17). Telif hakkı ve diğer entelektüel mülkiyet hakları nosyonu da, dijital medyanın yükselişiyle tehdit altında kalmıştır (Pavlik, 2013: 216).

Her dönemde gözetim ve denetim araçları farklı amaçlar için kullanılmıştır. Tarih boyunca hükümetler kimi zaman bilgiyi koruma ve saklama amacıyla; kimi zaman da bilgiyi baskı unsuru olarak kullanmışlardır (Yılmaz, 2020: 238). Özel hayat ve kişisel bilgilerle ilgili bir kavram olan mahremiyet bir insan hakkıdır. Kişisel bilgiyi kontrol etmek, kişilerin ilişkilerini ve bu ilişki bünyesinde kendilerine nasıl davranılacağını kontrol etmek demektir. Kişilerin kendileri hakkındaki bilgiyi kontrol etmeleri özerkliklerinin önemli bir unsurudur (Dedeoğlu, 2016: 71).

## Gözetim Toplumu

Yeni medyanın hayatlarımıza girmesiyle birlikte gözetim farklı bir boyut kazanmıştır. Artık herkes hem gözetleyen hem de gözetlenen olarak daha aktif bir durumdadır. Sosyal medya ile birlikte kişisel tercihler, yaşam tarzı kültür, zevkler, inançlar, manevi dünya, politik görüşler, ideolojiler vb. her şey gözetlenebilir ve bilinebilir hale gelmiştir.

Dijital yerliler hayatlarında bilgiye ulaşma, ders çalışma, haberleşme ve eğlence gibi her türlü faaliyetlerini dijital medya araçlarını kullanarak sürdürmektedir. Dijital yerliler karşılaştıkları her sorunun cevabını arama motorlarında, sosyal medyada ya da çevrim içi tartışma forumlarında aramaktadır (Kürkçü, 2016: 199). Bu durum arkalarında büyük miktarda dijital ayak izi bırakmalarına neden olmaktadır.

Gözetim toplumu bireylerin yeni medyayı kullanarak ve bu sistemlerle gözetleyen ve gözetlenen olma durumlarıyla oluşan toplum yaklaşımıdır (Yengin, 2014: 183). Günümüzde gözetim ve gözetlemek, hem kolaylaşmış hem de normalleşmiştir. Bir zamanlar mobese kameralarına karşı çıkan bireyler zamanla azalmış, bunların bir şekilde faydalı ve gerekli olduğu fikri toplum geneline yerleşmiştir. Panoptikon artık toplumun tamamını kapsayan bir kavram haline gelmiştir.

Panoptikonun amacı gözetim ve disiplini sağlamaktır. Jeremy Bentham'ın Panoptikonu Yunanca Pan ve Optikon kelimelerinden türetilen "her yeri gören yer" anlamına gelmektedir. Bentham'a göre Panoptikon ya da gözetim –evi – merkezi bir gözetleme kulesi etrafında çok sayıda hücreden oluşan ve bir gardiyanın aynı anda çok sayıda mahkumu görebildiği ve denetleyebildiği dairesel büyük bir yapıdır. Hücrelere bir miktar ışık verilerek izlenen mahkumlar, gardiyanları ve kameraları göremese de izlendiğini ve gözetlendiğini bildiğinden huzursuz hissetmekte, kurallara uymak için hareketlerine ve davranışlarına dikkat etmektedir (Akt. Yılmaz, 2020: 241).

Foucault'un "Hapishanenin doğuşu" çalışmasındaki yaklaşımda hapishanede bulunan herkes kontrol edilmekte ve gözetlenmektedir. Ancak gözetleyen ve kontrol eden birey tarafından kesinlikle görülememektedir. İşte bu noktada bireyler; dijital kimlikleriyle kendi temsil ettiği sanal dünyada kolaylıkla görünmekte ve gözetlenmektedir. Bu bağlamda birey aslında tam olarak şeffaf bir hapishanede yaşamaktadır ancak içinde yaşadığı durumun farkında değildir (Yengin, 2014: 178). Öte yandan bunun gönüllü bir hapis durumu olduğunu söylemek de mümkündür. Dış dünyanın gerçekleri ile mücadele etmekte zorlananların hapishaneye geri dönmesindeki gibi kendilerini sanal bir kutunun içine hapsetmektedirler.

Sosyal medyanın kontrolü, geleneksel medyaya göre daha zordur. Sosyal medya hizmetleri veren şirketlerin çoğunlukla ABD hukukuna tabi olması ve veri paylaşımı konusunda katı bir tutum takınmaları hükümetlerin denetimlerini zorlaştırmaktadır (Özutku vd., 2014: 97). Yeni medya ortamında etik kurallara bireylerin uyması için genel iletişim atmosferinin ve iktidar sahiplerinin de benzer konularda etik davranmayı bir ilke olarak benimsemeleri gerekmektedir (Binark ve Bayraktutan: 2013).

DOI NO: 10.17932/CTC.2021/ctc21.034

## Araştırmanın Yöntemi

Çalışmada, araştırmanın gerçekleştirildiği tarih olan 30.01.2021'de Google Play Store'un verilerine göre, "Haberleşme Kategorisinde", "Ücretsiz En Popüler Uygulamalar" alanında yer alan ilk beş uygulama seçilmiştir. Bu uygulamalar ilgili tarihte sırasıyla; BİP-Mesajlaşma, Kaliteli Görüntülü Arama, Telegram, WhatsApp Messenger, Discord-Talk, Video Chat & Hang Out with Friends, Signal-Gizli Mesajlaşma uygulamalarıdır. Çalışma kapsamındaki bu uygulamaların veri gizliliği politikaları karşılaştırılarak içerik analizi yöntemiyle incelenmiştir. Uygulamaların veri gizliliği politikaları incelenirken araştırmanın yapıldığı tarihteki son güncellenen veri politikaları dikkate alınmıştır.

## Bulgular

Araştırma kapsamında bu uygulamalarda üyelik oluşturulması için gereken kullanıcı bilgileri, uygulamayı temel düzeyde kullanma ve uygulamaların kendine has bazı özelliklerinden yararlanabilmek için kullanıcı tarafından sağlanan erişim izinleri ve uygulamaların veri politikaları karşılaştırmalı bir şekilde analiz edilmiştir.

***Tablo 1: Uygulamaların Özellikleri***

|  |  |  |  |  |
|---|---|---|---|---|
| ***BİP*** | ***Telegram*** | ***WhatsApp*** | ***Discord*** | ***Signal*** |
| Mesajlaşma, Kaliteli Görüntülü Arama | Telegram | WhatsApp Messenger | Talk,Video Chat & Hang Out with Friends | Gizli Mesajlaşma |
| 2013 | 2013 | 2010 | 2015 | 2018 |
| BİP A.Ş. | Telegram FZ-LLC | WhatsApp LLC | Discord Inc. | Signal Vakfı |
| 50 Milyon + Kullanıcı | 500 Milyon + Kullanıcı | 2 Milyar + Kullanıcı | 100 Milyon + Kullanıcı | 50 Milyon + Kullanıcı |

BİP - Mesajlaşma, Kaliteli Görüntülü Arama uygulaması 2013 yılında BİP A.Ş. tarafından **Türkiye'de** kurulmuştur. Uygulamanın 50 milyon üzerinde kullanıcısı bulunmaktadır. Telegram uygulaması 2013 yılında Telegram FZ-LLC tarafından kurulmuştur. Uygulamanın 500 milyon üzerinde kullanıcısı bulunmaktadır. WhatsApp Messenger uygulaması araştırma kapsamındaki uygulamalar arasında en erken kurulan ve en fazla kullanıcısı olan uygulamadır. Uygulama 2010 yılında WhatsApp LLC tarafından yayınlanmıştır. Uygulamanın bugüne kadar 2 milyarın üzerinde kullanıcısı bulunmaktadır. Discord Talk,Video Chat & Hang Out with Friends uygulaması 2015 yılında Discord Inc. tarafından yayınlanmıştır. Dünya genelinde 100 milyonun üzerinde kullanıcısı olan uygulama ekran paylaşımı özelliğiyle genellikle dijital oyun oynayan kullanıcılar tarafından tercih edilmektedir. Signal Gizli Mesajlaşma uygulaması diğer uygulamalardan farklı olarak bir vakıf olan Signal Vakfı tarafından kurulmuştur. 2018 yılında kullanıma sunulan uygulamanın günümüzde 50 milyonun üzerinde kullanıcısı bulunmaktadır.

Aşağıda yer alan Tablo 2'de araştırma kapsamında yer alan uygulamaların akıllı telefonlara indirildikten sonra üyelik işlemlerinin gerçekleştirilmesi aşamasında yer alan kullanıcı bilgilerini içermektedir.

**Tablo 2:Üyelik Oluşturulurken Gerekli Kullanıcı Bilgileri**

| HESAP OLUŞTURULURKEN GEREKEN KULLANICI BİLGİLERİ | BİP | TELEGRAM | WHATSAPP | DİSCORD | SİGNAL |
|---|---|---|---|---|---|
| Telefon Numarası | √ | √ | √ | √ | √ |
| E-mail | - | - | - | √ | - |
| Ülke | - | √ | √ | - | √ |
| Profil Fotoğrafı | √ | √ | √ | √ | √ |
| Kullanıcı Adı | √ | √ | √ | √ | √ |
| Doğum Tarihi | - | - | - | √ | - |

DOI NO: 10.17932/CTC.2021/ctc21.034

Tablo 2'ye göre, BİP uygulamasının üyelik işlemlerinde profil oluşturulması için kullanıcıdan telefon numarası, kullanıcı fotoğrafı ve kullanıcı adı bilgileri istenmektedir. Telegram uygulamasının üyelik aşamasında ülke bilgisi, telefon numarası, profil oluşturulması için kullanıcı fotoğrafı ve kullanıcı adı bilgilerinin girilmesi gerekmektedir. WhatsApp uygulamasında Telegram ile aynı şekilde ülke bilgisi, telefon numarası, profil oluşturulması için kullanıcı fotoğrafı ve kullanıcı adı bilgileri istenmektedir. Discord uygulamasında, kullanıcıdan, diğer uygulamalardan farklı olarak ek bilgiler de istenmektedir. Discord uygulamasında istenen kullanıcı bilgileri şunlardır; telefon numarası ya da e-mail adresi, kullanıcı adı, fotoğraf ve doğum tarihi bilgileri. Signal uygulamasında ise diğer uygulamalardaki gibi kullanıcının telefon numarası, ülke bilgisi, profil oluşturulması için kullanıcı fotoğrafı ve kullanıcı adı bilgilerinin yer alması gerekmektedir. Tablo 2'de yer alan bilgiler doğrultusunda genel anlamda tüm uygulamalarda üyelik oluşturulması için kullanıcıdan istenen ortak bilgiler; telefon numarası, kullanıcı adı ve profil fotoğrafıdır. Yalnızca Discord uygulaması ek olarak doğum tarihi bilgisi, telefon numarası ya da e-mail bilgisi seçeneğini sunması ve ülke bilgisinin belirtilmemesi bakımından diğer uygulamaların üyelik aşamalarında istenen kullanıcı bilgilerinden farklı olduğu görülmüştür.

***Tablo 3: Kullanıcı Tarafından Sağlanan İzinler***

| KULLANICI TARAFINDAN SAĞLANAN İZİNLER | BİP | TELEG-RAM | WHATSAPP | DİS-CORD | SİGNAL |
|---|---|---|---|---|---|
| Arama Yapma ve Aramaları Yönetme İzni | √ | √ | √ | - | √ |
| Rehbere Erişim İzni | √ | √ | √ | √ | √ |
| Fotoğraf, Medya ve Dosyalara Erişim İzni | √ | √ | √ | √ | √ |
| Kameraya Erişim İzni | √ | √ | √ | √ | √ |
| Mikrofon Erişim İzni | √ | √ | √ | √ | √ |
| Konuma Erişim İzni | √ | √ | √ | - | √ |
| Arama Geçmişine Erişim İzni | √ | √ | √ | - | - |
| SMS Gönderme ve Görüntüleme İzni | √ | - | √ | - | √ |
| Takvime Erişim İzni | - | - | - | - | √ |

Tablo 3'te yer alan bilgiler kullanıcının uygulama üyelik işlemlerini tamamladıktan sonra uygulamaların bazı özelliklerinin kullanılabilmesi için kullanıcının isteğe bağlı olarak verdiği erişim izinlerini kapsamaktadır. Buna göre, BİP uygulamasının kullanılabilmesi için kullanıcıdan şu bilgilere erişim izni talep edilmektedir; arama yapma ve aramaları yönetme izni, uygulamayı kullanan diğer kullanıcıları görebilmek için rehberdeki kişilere erişim izni, fotoğraf, medya ve diğer dosyalara erişim izni (depolama), fotoğraf ve video çekme izni (kamera), ses kaydetme izni (mikrofon), konuma erişim izni, arama geçmişine erişim izni ve SMS mesajları gönderme ve görüntüleme izni. Ayrıca uygulamada mesajların farklı dillere çevrimini sağlamaya yarayan çeviri özelliği bulunmaktadır. Bu özelliğin kullanılabilmesi için uygulamaya çeviri izni verilmesi gerekmektedir. Diğer taraftan uygulamada bir başka özellik ise uygulama içi para transferi ve ödemelerin yapılabilmesidir. Bu özellik için ise sisteme sanal bir kart ya da kredi kartı bilgilerinin tanımlanması gerekmektedir. BİP, yalnızca takvime erişim izni talep etmemektedir.

Telegram uygulamasının kullanılabilmesi için uygulama tarafından şu izinler istenmektedir; arama yapma ve aramaları yönetme izni, uygulamayı kullanan diğer kullanıcıları görebilmek için rehberdeki kişilere erişim izni, fotoğraf medya ve diğer dosyalara erişim izni (depolama), fotoğraf ve video çekme izni (kamera), ses kaydetme izni (mikrofon), yakınımdaki kullanıcıları görebilme özelliği için konuma erişim izni ve arama geçmişine erişim izni. Telegram, SMS gönderme ve görüntüleme izni ile takvime erişim izni talep etmemektedir.

WhatsApp uygulaması tarafından kullanıcıdan, arama yapma ve aramaları yönetme izni, uygulamayı kullanan diğer kullanıcıları görebilmek için rehberdeki kişilere erişim izni, fotoğraf, medya ve diğer dosyalara erişim izni (depolama), fotoğraf ve video çekme izni (kamera), ses kaydetme izni (mikrofon), konuma erişim izni, arama geçmişine erişim izni ve SMS mesajları gönderme ve görüntüleme izinleri istenmektedir. WhatsApp uygulamasının temelde BİP uygulaması ile aynı izinleri istediği görülmektedir. Ancak WhatsApp'ta, BİP uygulamasında olduğu gibi uygulama içi para transferi ve ödeme işlemlerinin yapıldığı özellik olmadığından kredi kartı bilgilerinin tanımlandığı bir alan uygulamada yer almamaktadır. Ayrıca WhatsApp, takvime erişim izni de istememektedir.

Discord uygulaması hem ara yüzü ve kullanım olanakları açısından hem de uygulamanın kullanılabilmesi için talep edilen izinler açısından diğer uygulamalardan farklıdır. Discord tarafından kullanıcıdan yalnızca dört izin talep edilmektedir; uygulamayı kullanan diğer kullanıcıları görebilmek için rehberdeki kişilere erişim izni, fotoğraf medya ve dosyalara erişim izni (depolama), fotoğraf veya video çekmek için kamera izni ve mikrofona erişim izni. Discord'da diğer uygulamaların aksine kullanıcıdan arama yapma ve aramaları yönetme izni, konuma erişim izni, arama geçmişine erişim izni, SMS mesajı gönderme ve görüntüleme izni ve takvime erişim izinleri istenmemektedir.

DOI NO: 10.17932/CTC.2021/ctc21.034

Signal uygulamasında ise temel olarak uygulamanın ve bazı özelliklerinin kullanılabilmesi için arama yapma ve aramaları yönetme izni, rehberdeki kişilere erişim izni, fotoğraf, medya ve dosyalara erişim izni (depolama), kameraya erişim izni, mikrofon erişim izni, konuma erişim izni, SMS mesajı gönderme ve görüntüleme izni, takvime erişim izinlerinin verilmesi gerekmektedir. Diğer uygulamalardan farklı olarak Signal tarafından arama geçmişine erişim izni talep edilmemektedir. Bununla birlikte sadece Signal uygulaması kullanıcıdan takvime erişim izni istemektedir.

**Tablo 4: Veri Politikasına Göre Kullanıcıdan Toplanan Veriler**

| VERİ POLİTİKASINA GÖRE KULLANICIDAN TOPLANAN VERİLER | BİP | TELEGRAM | WHATSAPP | DİSCORD | SİGNAL |
|---|---|---|---|---|---|
| Temel Hesap Verileri | √ | √ | √ | √ | - |
| Sohbet Verileri | - | √ | - | √ | - |
| Çerezler Aracılığıyla Sağlanan Veriler | √ | √ | √ | √ | - |
| Finansal Veriler | - | - | √ | √ | - |
| Kullanıcının Uygulamayı Kullanımı Hakkındaki Veriler | √ | √ | √ | √ | - |
| Kullanıcının Cihaz Bilgileri | √ | √ | √ | √ | - |

Yukarıda Tablo 4'te araştırma kapsamındaki uygulamaların veri gizliliği politikalarına göre toplanan kullanıcı bilgileri yer almaktadır. Buna göre uygulamaların veri politikalarına göre kullanıcıdan topladığı veriler; temel hesap verileri, sohbet verileri, çerezler aracılığıyla toplanan veriler, finansal veriler, kullanıcının uygulamayı kullanımı hakkındaki veriler ve kullanıcının cihaz bilgileri olmak üzere altı kategoriye ayrılarak analiz edilmiştir.

BİP uygulamasının son güncellenen 14.01.2021 tarihli veri politikası incelendiğinde uygulama tarafından kullanıcının temel hesap verilerine erişildiği açık bir şekilde belirtilmiştir. BİP uygulamasının kullanıcıdan topladığı temel hesap verileri; telefon numarası, kullanıcı adı (rumuz), avatar, GSM operatörü, hesabı güvenli tutmak için kullanılan şifreler, profil fotoğrafı, durum bilgisi, engellenen numaralar ve uygulama aracılığıyla yapılan anketlerin sonuçlarına ilişkin verileri kapsamaktadır.

BİP uygulamasının veri politikasında en önemli maddelerden biri kullanıcının sohbet içeriğine erişim sağlanmaması ve hiçbir şekilde depolanmamasıdır. Veri politikasında da açık bir şekilde belirtilmiştir: *"BiP, Uygulama üzerinden kurulan iletişiminizin içeriğiyle ilgili herhangi bir veri toplamaz"* (URL-2).

Diğer taraftan BİP Web uygulamasında çerezler (cookies) politikası bulunmaktadır. Kullanıcı tarafından çerezler kabul edildiğinde analitik/performans çerezler ve fonksiyonel çerezler olmak üzere uygulamanın kullandığı iki tür çerez bulunmaktadır. Bu çerezler veri politikasında şu şekilde açıklanmıştır: *"Analitik/Performans Çerezleri: İnternet sitemizi geliştirmemize hizmet eden çerezlerdir. Bu tür çerezler, ziyaretçilerin siteyi kullanımı hakkında bilgi edinmek ve internet sitesinin sorunsuz çalışıp çalışmadığının kontrolü ve varsa hataların tespiti için kullanılmaktadır. Fonksiyonel Çerezler: İnternet sitemizi ziyaret eden kullanıcıların tercihlerini hatırlamamıza olanak sağlayan çerezlerdir. Örneğin, ziyaretçinin dil veya font tercihlerinin saklanmasını sağlar"* (URL-2). BİP uygulaması veri gizliliği politikasında çerezler, genel anlamda kullanıcı deneyimini iyileştirme ve internet sitesine ziyaretler ile ilgili yapılan verileri saklamak amacıyla kullanıldığı belirtilmiştir.

BİP uygulamasının veri politikasında ödeme, fatura, vergi vb. finansal kayıtların toplandığını içeren herhangi bir açıklama yer almamaktadır. Ancak uygulamanın içerisinde ödeme ayarları sekmesinde kullanıcı tarafından kredi kartı bilgilerinin kayıt edilebileceği bir alan bulunmaktadır. Bu özellik uygulama içi satın alma işleminin yapılabilmesi için kullanılmaktadır. BİP uygulamasının veri politikasında kullanıcının finansal kayıtlarına ilişkin verilerin toplanması ile ilgili belirsizlik ve bir açıklamanın yer almaması veri politikası açısından dikkat çekicidir.

Diğer taraftan BİP uygulaması kullanıcının kullanım verilerine de erişmektedir. Veri gizliliği politikasında kullanım verilerini ilişkin toplanılan veriler; *"cihazınızdan teknik ekipmanlar yoluyla toplanan teknik veriler, (içeriği hakkında hiçbir bilgi toplamaksızın) gönderilmiş iletilerin türü (yazılı mesaj, video vb.), aktif kullanılan zamanlar, kullanılan hizmetlerin türü, Uygulama ara yüzüne ilişkin kullanım alışkanlıkları, Uygulamaya en son giriş yapılan tarih, Uygulamanın kullanımı sırasında meydana gelen hatalar ve hataya ilişkin bilgiler, İletişim türü (BiP Çağrıları, anlık mesajlar vb.), iletişimin süresi, tarihi ve tarafları, iletişim kurulan kişiler ile ilgili veriler"* (URL-2) şeklinde belirtilmiştir. BİP uygulaması kullanım verilerini toplama amaçlarını ise kullanım ve favoriler maddesi altında açıklamıştır: *"Bu Kişisel Veriler iş geliştirme, doğrudan veya dolaylı pazarlama (uygulama içerisindeki müşteri kampanyaları, reklam, hizmet ve fonksiyonların müşterilere tavsiye edilmesi, reklamların sunulması), profilleme (reklamların tercihlerinize göre sunulması, müşterilerin konum, operatör, kullanım süresi, uygulamada kalma süresi ve işlevlerine göre sınıflandırılması), denetim ve kontrol, risk yönetimi, şirket içi değerlendirme, hizmet kalitesinin ölçümü ve geliştirilmesi, iletişim, şikâyet yönetim süreçlerinin icrası, operasyonel faaliyetlerin*

DOI NO: 10.17932/CTC.2021/ctc21.034

*icrası ve geliştirilmesi, (aşağıda daha ayrıntılı olarak belirtildiği üzere) Microsoft ve Google tarafından sağlanan çeviri hizmetinin sunulması, hata/arıza bildirimleri ve kullanım alışkanlıklarına dayalı hizmet kalitesinin iyileştirilmesi gibi amaçlar doğrultusunda işlenmektedir"* (URL-2). Bu durum BİP uygulaması tarafından kullanıcının uygulama kullanım verilerinin reklam ve pazarlama amaçlı kullanılabildiğini göstermektedir. Bu bağlamda, BİP uygulamasının, araştırma kapsamındaki diğer uygulamalar ile karşılaştırıldığında, kullanıcının kullanım verilerinin toplanma amaçları açısından farklılık gösterdiği tespit edilmiştir.

BİP uygulamasının veri gizliliği politikasında kullanıcının cihaz bilgilerine de erişildiği belirtilmiştir. Bu bilgiler, *"cihaz modeli, cihazın işletim sistemi, tercih edilen telefon dili, kullanıcıların hangi operatörü kullandığına ilişkin bilgiler, ülke bilgilerine ilişkin veriler"* (URL-2) şeklinde açıklanmıştır.

Araştırma kapsamındaki diğer uygulama olan Telegram'ın 25 Mart 2019 tarihli veri politikası incelendiğinde kullanıcının hesap verilerinin toplandığı belirtilmiştir*: "Telegram bir iletişim hizmetidir. Bir Telegram hesabı oluşturmak için cep telefonu numaranızı ve temel hesap verilerinizi (profil adı, profil resmi ve bilgileri içerebilir) sağlarsınız. Kişilerinizin ve diğer kişilerin size ulaşmasını ve kim olduğunuzu tanımasını kolaylaştırmak için, Telegram'da* seçtiğiniz ekran adı, profil resimleriniz ve *kullanıcı adınız* (bir tane ayarlamayı seçtiyseniz) her zaman herkese açıktır. Gerçek adınızı, cinsiyetinizi, yaşınızı veya neyi sevdiğinizi bilmek istemiyoruz." (URL-3). Veri gizliliği politikasındaki bu madde Tablo 2'de yer alan kullanıcının yalnızca üyelik oluşturulurken kullanıcının uygulamaya sağladığı verilerin Telegram tarafından toplandığını göstermektedir.

Telegram uygulamasında mesajlaşma, bulut sohbetler ve gizli sohbetler olmak üzere ikiye ayrılmaktadır. Uygulama kullanıcının bulut sohbetlerini Hollanda'da bulunan sunucularda yedeklemektedir: *"Telegram bir bulut hizmetidir. Bulut sohbetlerinizdeki* mesajları, fotoğrafları, videoları ve belgeleri sunucularımızda *saklıyoruz, böylece verilerinize herhangi bir cihazınızdan üçüncü taraf yedeklemelerine güvenmek zorunda kalmadan istediğiniz zaman erişebilirsiniz. Tüm veriler büyük ölçüde şifrelenmiş olarak depolanır ve her durumda şifreleme anahtarları, farklı yetki alanlarındaki birkaç başka veri merkezinde depolanır. Bu şekilde yerel mühendisler veya fiziksel saldırganlar kullanıcı verilerine erişemez."* (URL-3). Telegram'ın veri politikasına göre, gizli sohbet seçeneği kullanıldığında ise gizli sohbetin içeriğinin hiçbir şekilde sunucularda saklanmadığı belirtilmiştir. Ancak bunun için kullanıcının gizli sohbet seçeneğini kullanması gerekmektedir. Aksi takdirde kullanıcı sohbetleri sunucularda saklanmaktadır.

Diğer taraftan Telegram uygulaması, içerisinde bulunan hizmetlerin kullanılması ve özelleştirilmesi açısından çerezleri kullanmaktadır. Çerezlerin reklam yapmak için kullanılmadığı da ayrıca veri politikasında belirtilmiştir. Bununla birlikte Telegram'ın web tarayıcısı aracılığıyla kullanılmasını sağlayan Telegram Web özelliği bulunmaktadır. Bu özelliği kullanabilmek için çerezlerin aktif hale getirilmesi gerekmektedir: *"Kullandığımız çerezler, Hizmetlerimizi web üzerinde işletmek ve sağlamak için olanlardır. Profil oluşturmak veya reklam yapmak için çerez kullanmayız. Kullandığımız çerezler, Hizmetlerimizi sunmamıza ve özelleştirmemize olanak tanıyan ve bunu yaparken size gelişmiş bir kullanıcı deneyimi sağlayan küçük metin dosyalarıdır. Tarayıcınız, kabul edip etmeme ve nasıl kaldırılacağı dahil olmak üzere bu tanımlama bilgilerini kontrol etmenize izin vermelidir. Çerezleri web tarayıcınızla engellemeyi seçebilirsiniz, ancak bu çerezleri devre dışı bırakırsanız, Telegram Web'de oturum açamazsınız."* (URL-3). Bu durumda reklam amaçlı kullanılmadığı belirtilmesine rağmen kullanıcı tarafından çerezler aktif hale getirilmediğinde Telegram Web'ın kullanımı da mümkün olmamaktadır.

Veri politikasında Telegram tarafından kullanıcının kredi kartı bilgileri gibi finansal kayıtlarına erişim sağlanmadığı da açıkça belirtilmiştir*: "Bir satın alma işlemi yaparken, kredi kartı bilgilerinizi, ödemeyi işleyecek ödeme sağlayıcısı tarafından sağlanan bir forma girersiniz ve bu bilgiler doğrudan ödeme sağlayıcısının sunucusuna gider. Kredi kartı bilgileriniz asla Telegram'ın sunucularına ulaşmaz. Kredi kartı bilgilerinize erişmiyoruz ve saklamıyoruz."* (URL-3).

Telegram tarafından kullanıcının uygulamayı kullanım verilerinin toplandığı da belirtilmiştir. Veri politikasında cihazlar arası işlevselliği sağlamak ve kullanıcıya yararlı özellikler sunmak amacıyla kullanıcının uygulamayı kullanım verilerinin toplandığı şu şekilde belirtilmiştir: *"Yararlı özellikler oluşturmak için Telegram'ı nasıl kullandığınıza ilişkin bazı toplu verileri kullanabiliriz. Örneğin, Ara menüsünü açtığınızda, Telegram mesaj gönderme olasılığınız daha yüksek olan kişileri ekranın üst kısmındaki bir kutuda görüntüler. Bunu yapmak için, hangi kişilere sık mesaj gönderdiğini gösteren bir derecelendirme hesaplarız."* (URL-3).

Telegram'ın veri gizliliği politikasında yer alan diğer önemli bir madde ise kullanılan cihaza ilişkin verilerdir. Telegram tarafından kullanıcının kullandığı cihaza ve özelliklerine ilişkin verilerin toplandığı açık bir şekilde belirtilmemiştir. Ancak veri politikasında yer alan kişisel verilerin işlenmesi başlığının emniyet ve güvenlik maddesinde kullanılan cihazlara ilişkin bilgilerin gerekli durumlarda toplanabileceği belirtilmiştir: *"Hesabınızın güvenliğini artırmak ve ayrıca spam, kötüye kullanım ve Hizmet Şartlarımızın diğer ihlallerini önlemek için IP adresiniz, kullandığınız cihazlar ve Telegram uygulamaları, kullanıcı adı değişiklikleri geçmişi gibi meta verileri toplayabiliriz. Eğer toplanırsa, bu üst veriler en fazla 12 ay saklanabilir."* (URL-3). Bu durum emniyet ve güvenlik ihlallerine karşı Telegram'ın kullanıcının cihaz bilgilerine eriştiğini göstermektedir.

DOI NO: 10.17932/CTC.2021/ctc21.034

Araştırılan diğer uygulama WhatsApp'ın, 4 Ocak 2021 tarihli son güncellenen veri gizliliği politikası incelendiğinde, diğer uygulamalarda olduğu gibi kullanıcının temel hesap verilerinin toplandığı görülmüştür. WhatsApp'ın topladığı hesap temel verilerini *"WhatsApp hesabı oluşturmak için cep telefonu numaranızı ve tercih ettiğiniz bir profil adı dahil olmak üzere temel bilgilerinizi sağlamanız gerekir. Bize bu bilgileri sağlamazsanız Hizmetlerimizi kullanmak için hesap oluşturamazsınız. Hesabınıza bir profil resmi ve "hakkımda" kısmındaki bilgiler gibi başka bilgiler ekleyebilirsiniz."* (URL-4) şeklinde açıklamıştır.

WhatsApp uygulamasının kullanıcıdan toplamadığı tek veri ise sohbettir. Kullanıcının mesajlarını uygulama sunucularında saklanmadığı açık bir şekilde veri politikasında ifade edilmiştir. *"Hizmetlerimizi size sunmak üzere izlediğimiz olağan iş akışında mesajlarınızı saklamayız. Bunun yerine, mesajlarınız cihazınızda saklanır ve genellikle sunucularımızda saklanmaz. Mesajlarınız, teslim edildikten sonra sunucularımızdan silinir."* (URL-4). Uygulama veri politikasında yalnızca mesajın diğer kullanıcıya teslim edilemediği durumlarda mesajı kullanıcıya teslim edebilmek amacıyla en fazla 30 gün boyunca sunucularda şifrelenmiş bir şekilde saklandığını da belirtilmiştir. Bununla birlikte bir kullanıcı aynı medyadan tekrar ilettiği durumlarda da mesajın şifreli bir şekilde sunucularda saklandığı belirtilmiştir. Aksi herhangi bir durumda WhatsApp uygulaması kullanıcının verilerini sunucularda saklamamaktadır.

WhatsApp uygulamasının da web tarayıcısında açılmasını sağlayan WhatsApp Web özelliği bulunmaktadır. Web özelliği olan diğer uygulamalar gibi WhatsApp uygulaması da çerezleri kullanmaktadır. Veri politikasında WhatsApp'ın çerezleri kullanma amacı şu şekilde belirtilmiştir: *"WhatsApp'ı web, masaüstü ve diğer web tabanlı Servislerimizde sunmak, deneyimlerinizi geliştirmek, Servislerimizin nasıl kullanıldığını anlamak ve Servislerimizi tercihlerinize göre geliştirmek için; hangi Sıkça Sorulan Sorular (SSS) makalemizin popüler olduğunu anlamak ve size Servislerimizle ilgili daha doğru içerikleri göstermek için; dil tercihiniz ve size özel geliştirmeler yapmak amacıyla seçimlerinizi hatırlamak için; ve İnternet sitemizdeki Sıkça Sorulan Sorular (SSS) makalelerini popülerliklerine göre sıralamak, web tabanlı Servislerimizin mobil ve masaüstü kullanıcılarını karşılaştırmak ve anlamak, veya belirli internet sayfalarımızın popülerliğini ve etkinliğini anlamak için."* (URL-4).

WhatsApp'ın kullanıcıdan otomatik olarak topladığı diğer bir veri, finansal kayıtlardır. Uygulamanın topladığı finansal kayıtlar şöyledir; *"Ödeme hizmetlerimizi kullanmanız ya da satın alma veya diğer finansal işlemler için sunulan Hizmetlerimizi kullanmanız halinde, ödeme hesabı ve işlem bilgileri dahil olmak üzere hakkınızdaki ek bilgileri işleriz. Ödeme hesabı ve işlem bilgileri, işlemi tamamlamak için gerekli olan bilgileri içerir (örneğin, ödeme yönteminizle ilgili bilgiler, gönderim ayrıntıları ve işlem tutarı)"* (URL-4). Buradan yola çıkarak kullanıcı tarafından ödeme işlemi yapıldığında satın alma geçmişi de dahil olmak üzere ödeme ayrıntılarıyla ilgili her veri WhatsApp tarafından toplandığını ortaya çıkarmaktadır.

WhatsApp uygulamasının topladığı veriler arasında diğer önemli nokta, kullanım verileridir. Veri gizliliği politikasında kullanıcının kullanım verilerinin neleri kapsadığı otomatik toplanan veriler başlığı altında ayrıntılı bir şekilde açıklanmıştır: *"Hizmetlerimizde gerçekleştirdiğiniz işlemler hakkında bilgiler (örneğin, hizmetle ilgili, tanılama amaçlı veya performansla ilgili bilgiler) toplarız. Bu bilgiler; işlemlerinizle ilgili bilgileri (Hizmetlerimizi nasıl kullandığınız, Hizmetlerdeki ayarlarınız, Hizmetlerimizi kullanarak başkalarıyla nasıl etkileşim kurduğunuz (işletmelerle kurduğunuz etkileşimler dahil), işlem ve etkileşimlerinizin zamanı, sıklığı ve süresi dahil), günlük dosyalarını, tanılama, çökme, web sitesi ve performans günlüklerini ve raporlarını kapsar. Bu bilgiler arasında Hizmetlerimizi kullanmak üzere ne zaman kaydolduğunuz ve mesajlaşma, arama, durum, gruplar (grup adı, grup resmi, grup açıklaması dahil), ödemeler veya işletme özellikleri gibi kullandığınız özellikler, profil fotoğrafı, "hakkımda" kısmındaki bilgiler, çevrimiçi olup olmadığınız; Hizmetlerimizi en son ne zaman kullandığınız ("son görülme" bilginiz) ve "hakkımda" kısmındaki bilgileri en son ne zaman güncellediğiniz de yer almaktadır."* (URL-4).

WhatsApp uygulamasının otomatik olarak topladığı son veri ise cihaz bilgisi ve bağlantılardır. *"Hizmetlerimizi yüklediğinizde, kullandığınızda veya Hizmetlerimize eriştiğinizde, cihaza ve bağlantıya özgü bilgiler toplarız. Bu bilgiler arasında donanım modeli, işletim sistemi bilgileri, pil seviyesi, sinyal gücü, uygulama sürümü, tarayıcı bilgileri, mobil şebeke, bağlantı bilgileri (telefon numarası, mobil iletişim operatörü veya İnternet servis sağlayıcısı dahil), dil ve saat dilimi, IP adresi, cihaz işlem bilgileri ve tanımlayıcılar (aynı cihaz veya hesapla ilişkili Facebook Şirketi Ürünlerine* özgü tanımlayıcılar dahil) gibi bilgil*er bulunmaktadır."* (URL-4). Burada diğer uygulamalardan farklı olarak WhatsApp uygulamasının -Facebook Şirketi Ürünlerine özgü tanımlayıcılar"- ifadesini kullanması önemli bir noktadır. WhatsApp, Facebook Şirketi'ne bağlı ürünlerden biridir: *"Facebook Ürünleri; WhatsApp, Oculus Ürünleri (bir Oculus hesabı kullanıldığında) ve CrowdTangle'a ait web siteleri, ürünler veya uygulamalar da dahil olmak üzere hepsi birbirinden farklı ve bağımsız hizmet koşullarına ve gizlilik ilkelerine tabi olan ve Facebook Şirketleri* (Facebook *Payments Inc, Facebook Payments International Limited, Onavo, Facebook Technologies, LLC ve Facebook Technologies Ireland Limited, WhatsApp Inc. ve WhatsApp Ireland Limited, CrowdTangle) tarafından sağlanan diğer ürünler ile birlikte Facebook Şirketi Ürünleri'ni*

DOI NO: 10.17932/CTC.2021/ctc21.034

*oluşturur."* (URL-4). WhatsApp uygulaması da Facebook Şirketi ürünlerinden biri olması sebebiyle yukarıda yer alan ürün ve şirketlerde, aynı cihaz üzerinden erişim ya da ilişkili hesap kullanıldığı durumlarda bu verileri otomatik olarak toplayabilmektedir.

Araştırma kapsamındaki uygulamalardan biri olan Discord uygulamasının son güncellenen 23 Haziran 2020 tarihli veri gizliliği politikası incelenmiştir. Tablo 3'e bakıldığında Discord uygulaması tarafından kullanıcının tabloda yer alan bütün kategorilerdeki verilerin toplandığı görülmektedir. Discord tarafından toplanan bu veriler Amerika'da bir sunucuda saklanmaktadır. Bu veriler arasından en başta hesap bilgileri gelmektedir. Uygulamanın veri politikasında hesap bilgileri, kullanıcının sağladığı veriler başlığı altında uygulamaya kaydolurken kullanıcı adı, e-posta adresi vb. (Tablo 2) toplanan tüm veriler olarak belirtilmiştir. Discord uygulamasının kullanıcının kişisel verilerini toplaması bir başka önemli noktadır. Bazı kişisel veriler uygulamaya hesap oluşturulurken (Tablo2) uygulama tarafından talep edilmektedir. Discord uygulaması ise bu veriler ile sınırla kalmayarak *"müşterilerimizin demografik istatistikleri, ilgi alanları ve davranışları"* (URL-5) ile ilgili verileri de toplamaktadır. Bunun yanında veri politikasında, bu veriler araştırma yapma, bağlı kuruluşlar, temsilciler ve iş ortaklarıyla ve yasal amaçlarla üçüncü taraflarla da paylaşılabileceği açık bir şekilde ifade edilmiştir.

Discord uygulaması kullanıcının sohbet verilerini de toplamaktadır. *"sohbet özelliği yoluyla gönderdiğiniz herhangi bir mesaj, görüntü, geçici VOIP verisi (yalnızca haberleşme teslimini etkinleştirmek için) ya da herhangi bir içerik yer alabilir."* (URL-5). Veri politikasında sohbet verilerinin kullanıcının sağlamış olduğu veriler olarak belirtilmesi önemli bir noktadır.

Discord uygulamasının kullanıcıdan topladığı diğer veri, çerezlerdir. Uygulama, Tablo3'te yer alan diğer uygulamalar gibi çerezleri kullanmaktadır. Uygulama tarafından bu çerezleri kullanma amaçları ise şu şekildedir: *"Hangi hesaptan oturum açtığınız ve bildirim ayarlarınız gibi yerel bilgisayar ayarlarınızı takip etmek için çerezler ve benzer teknolojilerden faydalanmaktayız. Çerezler; sitelerin ya da hizmetlerin tarayıcınız ya da cihazınızda açtığı ve bir sonraki ziyaretlerinizde okunabilen veri parçalarıdır. Hizmet'e yeni özellikler eklendikçe ek verileri korumak için çerez kullanımımızı genişletebiliriz. Ayrıca, web işaretçisi ve tek piksel gif'ler gibi teknolojileri sistem tarafından gönderilen açık tarifeler gibi günlük verileri kaydetmede kullanıyoruz."* (URL-5). Discord tarafından çerezler kullanılarak hem kullanıcının yerel ayarlarına ve günlük verilerine erişim sağlanmakta, hem de uygulamadaki üçüncü taraf web sitesi (Google Analytics vb.) araçları gibi ek hizmetler ve teknolojilerin kullanımı sağlanmaktadır.

Discord uygulaması Amerika'daki sunucularında kullanıcının finansal verilerini de toplamaktadır. Veri gizliliği politikasında açık bir şekilde belirtilmese de bilgilerinizin tarafımızdan açıklanması başlığı altında yer alan temsilciler, danışmanlar ve ilgili üçüncü taraflar maddesi altındaki *"birçok işte olduğu gibi, zaman zaman biz de işle ilgili belirli görevleri yerine getirmesi için başka şirketleri ya da bireyleri görevlendiriyoruz. Bu görevlere örnek olarak posta bilgileri, veri tabanlarının sürdürülmesi ve ödemelerin işlenmesi verilebilir."* (URL-5) şeklindeki geçen cümleler kullanıcının finansal kayıtların toplandığını göstermektedir. Diğer taraftan veri politikasında Kaliforniya'da ikamet eden kullanıcıların gizlilik hakları başlığında ise uygulama tarafından satın alma geçmişi, ödeme bilgilerinin toplandığı açıkça belirtilmiştir. *"(...) ticari bilgiler (varsa Discord'dan satın aldıklarınızın kaydı); finansal veriler (Discord'dan herhangi bir şey satın aldıysanız ödeme bilgileri) (...)"* (URL-5).

Discord tarafından kullanım bilgileri de sunucularda toplandığı veri gizliliği politikasında belirtilmiştir. Kullanım bilgilerinin toplandığı net bir şekilde açıklanmadığı görülmüştür. Ancak veri politikasında sağladığınız bilgiler maddesinde *"Söz konusu bilgileri kendi isteğinizle sağladığınızda sizden bilgi toplarız: ör. Hizmetlere erişim sağlamak üzere kaydolduğunuzda ya da belli başlı Hizmetleri kullandığınızda. Topladığımız bilgiler arasında, bunlarla sınırlı olmamak kaydıyla, kullanıcı adı, e-posta adresi ve sohbet özelliği yoluyla gönderdiğiniz herhangi bir mesaj, görüntü, geçici VOIP verisi (yalnızca haberleşme teslimini etkinleştirmek için) ya da herhangi bir içerik yer alabilir."* (URL-5) cümlelerinden anlaşılabileceği gibi kullanım verilerinin kullanıcının sağladığı veriler çerçevesinde değerlendirilerek toplandığı anlaşılabilmektedir.

Discord tarafından veri politikasında kullanıcının cihaz bilgisi ve bağlantılar ile ilgili verilerinin toplandığı ifade edilmiştir. Bu verileri otomatik olarak topladığımız veriler başlığı altında *"...IP adresi, cihaz kimlik bilgisi ve Hizmetler içerisindeki faaliyetleriniz gibi birtakım bilgileri alır ve depolarız.(...)"* (URL-5) şeklinde belirtilmiştir.

Araştırma kapsamındaki son uygulama ise Signal'dir. Signal uygulamasının 25 Mayıs 2018'de güncellenen en son veri politikası incelenmiştir. *"Signal, hassas bilgileri asla toplamayacak veya saklamayacak şekilde tasarlanmıştır. Signal mesajlarına ve çağrılarına biz veya diğer üçüncü şahıslar tarafından erişilemez çünkü bunlar her zaman uçtan uca şifrelenmiş, özel ve güvenlidir."* (URL-6) Bu bağlamda Signal'in, araştırılan diğer uygulamalar arasında kullanıcıdan en az veri topladığı tespit edilmiştir.

Signal uygulaması kullanıcı hesap oluşturabilmesi için bazı bilgiler (Tablo2) talep etmektedir. Ancak veri politikasında kullanıcının hesap bilgilerinin toplanmadığı açık bir şekilde ifade edilmiştir. *"Bir Signal hesabı oluşturduğunuzda bir telefon numarası kaydedersiniz. Telefon numaraları, Hizmetlerimizi size ve diğer Signal kullanıcılarına sağlamak için kullanılır. Hesabınıza isteğe bağlı olarak profil adı ve profil resmi gibi başka bilgiler*

DOI NO: 10.17932/CTC.2021/ctc21.034

*de ekleyebilirsiniz. Bu bilgiler uçtan uca şifrelenmiştir . ”* (URL-6).

Signal uygulaması kullanıcın sohbet verilerini de toplamamaktadır. “*Signal mesajlarınızın veya aramalarınızın şifresini çözemez veya içeriğine erişemez. Signal, geçici olarak çevrimdışı olan cihazlara (örneğin, pili bitmiş bir telefon) teslim edilmek üzere sunucularında uçtan uca şifrelenmiş mesajları sıraya koyar. Mesaj geçmişiniz kendi cihazlarınızda saklanır.”* (URL-6). Bu durum uygulamanın koşulsuz şartsız hiçbir şekilde kullanıcının sohbet verilerine hem erişmediğini hem de toplamadığını göstermektedir. Diğer taraftan Signal, mesajlara erişim sağlamadığı için cihazın ya da hesabının güvenliğinden kullanıcıyı sorumlu tutmaktadır.

Signal uygulamasının veri gizliliği politikasında çerezler ile ilgili bir bilgi bulunmamaktadır. Signal üçüncü taraf sağlayıcıları da yalnızca doğrulama kodu gönderme ve destek hizmeti vermek amacıyla kullanmaktadır. Bunlara ek olarak Signal’in veri politikasında kullanıcının finansal kayıtları, kullanım verileri, cihaz bilgisi ve bağlantılar, kişisel verilere ilişkin bir bilgi de bulunmamaktadır. *“Signal kişisel verilerinizi veya içeriğinizi hiçbir şekilde satmaz, kiralamaz veya bunlardan para kazanmaz.”* (URL-6). Veri politikasındaki bu cümle Signal’in kullanıcı verilerini ticari amaçlı kullanmadığını da göstermektedir.

## Uygulamalar Tarafından Toplanan Verilerin Kullanımları

Yukarıda veri politikaları incelenen her uygulama kullanıcının birtakım verilerini talep etmektedir. Bu verilerin kullanım amaçları her uygulamaya göre değişebilmektedir. BİP uygulaması tarafından toplanan verilerin kullanım amaçları, hizmetlerin sağlanması, reklam ve sponsorlu içeriklerin sunumu, emniyet ve güvenlik, hizmet kalitesinin geliştirimi başlıkları altında toplanabilmektedir. Telegram, reklam ve sponsorlu içeriklerin sunumu dışında hizmetlerin sağlanması, emniyet ve güvenlik, hizmet kalitesinin geliştirimi amaçları doğrultusunda verileri kullanmaktadır. WhatsApp ve Discord uygulamalarının, hizmetlerin sağlanması, reklam ve sponsorlu içeriklerin sunumu, emniyet ve güvenlik, hizmet kalitesinin geliştirimi olmak üzere tüm başlıklar verileri kullanma amaçlarını oluşturmaktadır. Signal’de ise yalnızca hizmetlerin sağlanması, emniyet ve güvenlik açılarından kullanıcı verilerinin kullanılabileceği tespit edilmiştir.

## Toplanan Verilerin Paylaşımı

Veri gizliliği politikasına göre BİP uygulaması tarafından toplanan veriler, *“hizmetin işlevselliği ve kendi tercihleri doğrultusunda ve yürürlükteki yasalar tarafından izin verildiği ölçüde diğer kullanıcılarla etkileşime girebilme”* (URL-2) amacıyla diğer kullanıcılar ile paylaşılmaktadır. Kamu yararı adına gerekli durumlarda hukuk ve emniyet teşkilatı ile *“yasal bir yükümlülük dâhilinde kişisel verileri sunmakla yükümlü olduğu ve gerek kendi haklarını, mülkiyetini veya güvenliğini gerekse üçüncü kişilerin haklarını, mülkiyetini veya güvenliğini korumak amacıyla yetkili mercilerle”* (URL-2) paylaşılabileceği belirtilmiştir. Bununla birlikte kullanıcı verileri, üçüncü şahıslara “*uygulamanın kullanıcıları hakkında toplulaştırılmış istatistiksel veriler ve analizler”* (URL-2) sağlayabilmek amacıyla paylaşıldığı görülmüştür. Uygulamanın çeviri özelliği kullanıldığında ise Microsoft veya Google üçüncü taraf hizmet sağlayıcısıyla paylaşılabileceği belirtilmiştir.

Telegram uygulaması kullanıcı verilerini etkileşim kurabilmek adına diğer kullanıcılarla paylaşmaktadır. *“(...) diğer Telegram kullanıcıları ile iletişim kurmayı seçerek, kişisel verilerinizi sizin adınıza bu Gizlilik Politikasına uygun olarak bu kullanıcılara aktarmamız için bize talimat verdiğinizi unutmayın.”* (URL-3). Diğer taraftan Telegram uygulamasının kullanıcı verilerini ortakları ile paylaşabileceği açıkça belirtilmiştir; *“*(1) *İngiliz Virgin Adaları›nda bulunan ana şirketimiz Telegram Group Inc; ve* (2) *Hizmetlerimizi sağlamaya, iyileştirmeye ve desteklemeye yardımcı olmak için Dubai’de bulunan bir grup üyesi olan Telegram FZ-LLC.”*Telegram kamu yararı adına da kullanıcının kişisel verilerini paylaşabileceği *“terör zanlısı olduğunuzu doğrulayan bir mahkeme emri varsa, IP adresinizi ve telefon numaranızı ilgili makamlara ifşa edebiliriz.”* (URL-3) şeklinde belirtilmiştir. Bugüne kadar böyle bir paylaşımın yapılmadığına ilişkin bilgiye de veri politikasından ulaşılabilmektedir.

WhatsApp uygulamasının veri politikasında iletişim hizmetini sağlamak amacıyla diğer kullanıcılar ile hesaba ilişkin bilgileri içeren kullanıcı verilerinin paylaşıldığı belirtilmiştir. Bununla birlikte WhatsApp İşletme hesaplarına kullanıcı hizmet kullanımlarıyla ilgili ölçüm sağlamak amacıyla da kullanıcı verilerini paylaşılabilmektedir. WhatsApp uygulaması bir sosyal medya platformu olan Facebook ile birlikte çalışmaktadır. Veri politikasında *üçüncü taraf hizmet sağlayıcıları* başlığı altında Facebook şirketleriyle paylaşılan veriler şu şekilde açıklanmıştır. *“Hizmetlerimizi yürütmemize, sağlamamıza, iyileştirmemize, anlamamıza, özelleştirmemize, desteklememize ve pazarlamamıza yardımcı olmaları için üçüncü taraf hizmet sağlayıcılarıyla ve diğer Facebook Şirketleriyle çalışırız. Teknik altyapı, teslimat ve diğer sistemleri sağlamak, hizmetlerimizi pazarlamak, anket ve araştırma yaptırmak, kullanıcıların ve başkalarının güvenliğini, emniyetini ve bütünlüğünü korumak ve müşteri hizmetlerine yardımcı olmak gibi Hizmetlerimizi desteklemek için bu şirketlerle birlikte çalışırız.”* (URL-4). WhatsApp uygulaması üçüncü taraf hizmet sağlayıcılarıyla da kullanıcı verilerini paylaşmaktadır. “(…) *iCloud veya Google Drive gibi, hizmetlerimize entegre olan bir veri yedekleme hizmeti kullanırsanız bu hizmetler WhatsApp mesajlarınız gibi kendileriyle paylaştığınız bilgilere sahip olur. Üçüncü taraf bir platformdan içerik oynatmak için uygulama içi oynatıcıyı kullandığınızda olduğu gibi, Hizmetlerimiz aracılığıyla bağlantılı bir üçüncü taraf hizmeti veya başka*

DOI NO: 10.17932/CTC.2021/ctc21.034

*bir Facebook Şirketi Ürünü ile etkileşimde bulunursanız IP adresiniz ve bir WhatsApp kullanıcısı olduğunuz gibi sizinle ilgili bilgiler, bu tür üçüncü taraflara veya Facebook Şirketi Ürününe sunulabilir."* (URL-4).

Discord uygulamasının veri politikasında kullanıcı verilerini ortaklar ile paylaşılabileceği belirtilmiştir. Ortaklar kategorisinde işle ilgili nakiller, ilgili şirketler başlıkları dahil edilmiştir. İşle ilgili nakiller; *"işimizi geliştirdikçe, işletmeler ya da mal varlıkları satıp alabiliriz. Şirkete ilişkin bir satış, birleşme, yeniden yapılanma, iflas, tasfiye ya da benzer bir durumda, sizin bilgileriniz nakledilen mal varlıklarının bir parçası olabilir.", ilgili şirketler ise "gizlilik politikasına uygun amaçlarla ilgili şirketlerimizle de bilgilerinizi paylaşabiliriz."* (URL-5) şeklinde açıklanmıştır. Bununla birlikte Discord uygulamasının veri politikasında kullanıcı bilgilerinin paylaşılabildiği başka alan *developers'dır.* Developers; *"Yazılım Geliştirme Kitimizi (SDK) ya da Uygulama Programlama Ara yüzümüzü (API) kullanan geliştiriciler mesaj içeriği, mesaj meta verileri ve ses meta verileri dâhil olmak üzere son kullanıcılarının bilgilerine erişim sağlayacaktır. Geliştiriciler bu bilgileri yalnızca uygulamalarında ve/ veya hizmetlerinde SDK/API işlevselliği sağlamak için kullanmalıdır."* (URL-5) şeklinde belirtilmiştir. Yalnızca uygulamayı geliştirme amacıyla olsa dahi SDK ve API'nın kullanıcı mesaj içeriğine erişim sağlaması oldukça önemli bir noktadır. Diğer taraftan Discord uygulamasında temsilciler, danışmanlar ve ilgili üçüncü taraflar ile uygulama içi birtakım hizmetlerin kullanımı, sürdürülmesi ve işlenmesi kullanıcı verilerinin paylaşılabileceği belirtilmiştir. Discord uygulaması tarafından diğer uygulamalarda olduğu gibi kamu yararı amacıyla da kullanıcı bilgilerinin gerekli durumlarda paylaşabileceği ifade edilmiştir.

Signal uygulamasının ise veri politikasında kullanıcı verilerinin *üçüncü şahıslar* başlığı altında şu şekilde paylaşıldığı belirtilmiştir; *"Hizmetlerimizden bazılarını sağlamak için üçüncü taraflarla birlikte çalışıyoruz. Örneğin, üçüncü taraf sağlayıcılarımız, hizmetlerimiz için kaydolduğunuzda telefon numaranıza bir doğrulama kodu gönderir. Bu sağlayıcılar, bu bilgileri korumakla yükümlüdürler. Hizmetlerimizle bağlantılı olarak YouTube, Spotify, Giphy, vb. gibi diğer üçüncü taraf hizmetlerini kullanıyorsanız, bu hizmetleri kullanımınızı Hizmetlerin Şartları ve Gizlilik Politikaları yönetir."* (URL-6). Diğer taraftan incelenen diğer uygulamalardaki gibi veri politikasında kamu yararı doğrultusunda kullanıcı verilerinin yasaların uygun gördüğü gerekli durumlarda paylaşılabileceği açıklanmıştır.

## Sonuç

Araştırmanın çıkış noktasını oluşturan temel problem araştırma kapsamındaki uygulamaların veri gizliliği politikalarının incelenmesidir. Kullanıcıların, üyelik işlemiyle birlikte uygulamalar tarafından sunulan veri politikası sözleşmesini kabul etmesi gerekmektedir. Çalışmada uygulamaların veri politikaları içerik analizi tekniğiyle incelenerek kullanıcıların hangi kişisel bilgilerinin toplandığı ve hangi amaçlar doğrultusunda depolandığı ya da kullanıldığı tespit edilmeye çalışılmıştır. Böylece üyelik işlemi gerçekleştirilirken veri gizliliği politikalarının dikkatli bir şekilde incelenmesine dair bilinçli kullanıcı oluşturulmasına yönelik katkı sağlanmaya çalışılmıştır.

Araştırmadan elde edilen bulgular doğrultusunda üyelik işlemleri sırasında, BİP telefon numarası, profil fotoğrafı ve kullanıcı adı bilgisi; Telegram ülke bilgisi, telefon numarası, profil fotoğrafı ve kullanıcı adı bilgisi; WhatsApp ülke bilgisi, telefon numarası, profil fotoğrafı ve kullanıcı adı bilgisi; Discord telefon numarası ya da e-mail adresi, kullanıcı adı, profil fotoğrafı ve doğum tarihi bilgisi; Signal telefon numarası, ülke bilgisi, profil fotoğrafı ve kullanıcı adı bilgilerinin belirtilmesi gerekmektedir. Diğer uygulamalardan farklı olarak Discord tarafından bu verilere ek olarak kullanıcının doğum tarihi bilgisinin de istenmesi, aynı zamanda kullanıcıya telefon numarası ya da e-mail seçeneği sunmasıyla birlikte ülke bilgisinin de gerekli olmadığı tespit edilmiştir. Ancak genel anlamda araştırma kapsamındaki tüm uygulamalarda üyelik oluşturulması için benzer kullanıcı bilgilerinin belirtilmesi gerektiği görülmüştür.

Uygulamalarda telefon görüşmesi yapma, fotoğraf ve video paylaşabilme gibi bazı temel özelliklerinin kullanılabilmesi için kullanıcı tarafından isteğe bağlı olarak erişim izinleri verilmesi gerekmektedir. Bunlar kullanıcı tarafından sağlanan veriler başlığı altında değerlendirilmiştir. Buna göre BİP uygulamasında arama yapma ve aramaları yönetme izni, rehberdeki kişilere erişim izni, fotoğraf, medya ve diğer dosyalara erişim izni (depolama), fotoğraf ve video çekme izni (kamera), ses kaydetme izni (mikrofon), konuma erişim izni, arama geçmişine erişim izni ve SMS mesajları gönderme ve görüntüleme izinlerinin verilmesi gerektiği belirlenmiştir. Bu izinler arasında BİP uygulamasında sadece takvime erişim izni gerekmediği de görülmüştür. Telegram uygulamasında kullanıcının arama yapma ve aramaları yönetme izni, rehberdeki kişilere erişim izni, fotoğraf medya ve diğer dosyalara erişim izni (depolama), fotoğraf ve video çekme izni (kamera), ses kaydetme izni (mikrofon), yakınımdaki kullanıcıları görebilme özelliği için konuma erişim izni ve arama geçmişine erişim izinlerini vermesi gerektiği tespit edilmiştir. Telegram bu erişim izinlerinden SMS gönderme ve görüntüleme izni ile takvime erişim izni talep etmediği görülmüştür. WhatsApp uygulamasında arama yapma ve aramaları yönetme izni, rehberdeki kişilere erişim izni, fotoğraf, medya ve diğer dosyalara erişim izni (depolama), fotoğraf ve video çekme izni (kamera), ses kaydetme izni (mikrofon), konuma erişim izni, arama geçmişine erişim izni ve SMS mesajları gönderme ve görüntülemeye erişime açılması gerektiği belirlenmiştir. WhatsApp uygulaması da takvime erişim izni istememektedir. Discord uygulaması ise oyun oynayan kullanıcılar için tasarlanması nedeniyle diğer uygulamalardan kullanım alanı açısından farklıdır. Uygulamanın kullanılabilmesi için kullanıcının yalnızca dört

DOI NO: 10.17932/CTC.2021/ctc21.034

izni onaylaması gerekmektedir. Bu izinler rehberdeki kişilere erişim izni, fotoğraf medya ve dosyalara erişim izni (depolama), fotoğraf veya video çekmek için kamera izni ve mikrofona erişim izinleridir. Discord uygulamasında diğer uygulamalardan farklı olarak arama yapma ve aramaları yönetme izni, konuma erişim izni, arama geçmişine erişim izni, SMS mesajı gönderme ve görüntüleme izni ve takvime erişim izinlerinin istenmediği görülmüştür. Signal uygulamasında arama yapma ve aramaları yönetme izni, rehberdeki kişilere erişim izni, fotoğraf, medya ve dosyalara erişim izni (depolama), kameraya erişim izni, mikrofon erişim izni, konuma erişim izni, SMS mesajı gönderme ve görüntüleme izni, takvime erişim izinlerinin verilmesi gerektiği belirlenmiştir. Signal uygulaması, bu uygulamalar arasında takvime erişim izni isteyen tek uygulamadır. Bununla birlikte Signal uygulaması tarafından arama geçmişine erişim izni talep edilmediği tespit edilmiştir.

Araştırmanın yapıldığı tarih aralığında uygulamaların en son güncellenen veri politikalarına bakılmıştır. Bu doğrultuda BİP uygulamasının 14.01.2021 tarihli son güncellenen veri politikası incelenmiştir. Uygulamanın veri politikasında kullanıcının temel hesap verilerine, kullanıcının uygulamayı kullanım verilerine, kullanıcının cihaz bilgilerine erişim sağlandığı belirtilmiştir.

BİP uygulamasının veri politikasında kullanıcının sohbet içeriğine erişim sağlanmadığı ve hiçbir şekilde depolanmadığı bilgisi yer almaktadır. Diğer taraftan BİP Web uygulamasında çerezler kullanılmaktadır. BİP uygulamasının veri politikasında çerezlerin genel anlamda kullanıcı deneyimini iyileştirme ve internet sitesine ziyaretler ile ilgili yapılan verileri saklamak amacıyla kullanıldığı belirtilmiştir. Bununla birlikte uygulamanın veri politikasında finansal kayıtların toplandığını içeren herhangi bir açıklama yer almadığı görülmüştür. Ancak uygulamanın içerisinde ödeme ayarları sekmesinde kullanıcı tarafından kredi kartı bilgilerinin kayıt edilebileceği bir alan bulunmaktadır. Bu özellik uygulama içi satın alma işleminin yapılabilmesi için kullanılmaktadır. BİP uygulamasının veri politikasında kullanıcının finansal kayıtlara ilişkin verilerin toplanması ile ilgili belirsizlik ve bir açıklamanın yer almaması veri politikası açısından dikkat çekicidir.

Telegram'ın veri politikasında kullanıcı tarafından sağlanan ve üyelik oluşturulurken elde edilen hesap verilerinin toplandığı belirtilmiştir. Telegram uygulamasında mesajlaşma bulut sohbetler ve gizli sohbetler olmak üzere ikiye ayrılmaktadır. Kullanıcının bulut sohbetlerini Hollanda'da bulunan sunuculara yedeklendiği bilgisi yer almaktadır. Gizli sohbet seçeneğinde ise sohbetin içeriğinin hiçbir şekilde sunucularda saklanmadığı belirtilmiştir. Ancak bunun için kullanıcının gizli sohbet seçeneğini kullanması gerekmektedir. Aksi takdirde kullanıcı sohbetleri sunucularda saklandığı görülmüştür. Diğer taraftan Telegram uygulaması, içerisinde bulunan hizmetlerin kullanılması ve özelleştirilmesi açısından çerezleri kullanmaktadır. Çerezlerin reklam yapmak için kullanılmadığı da ayrıca veri politikasında belirtilmiştir. Veri politikasında Telegram tarafından kullanıcının kredi kartı bilgileri gibi finansal kayıtlarına erişim sağlanmadığı da açıkça belirtilmiştir. Telegram tarafından kullanıcının uygulamayı kullanım verilerinin toplandığı da belirtilmiştir. Telegram, kullanıcının kullandığı cihaza ve özelliklerine ilişkin verilerin toplandığı açık bir şekilde belirtilmemiştir. Ancak veri politikasında yer alan kişisel verilerin işlenmesi başlığının emniyet ve güvenlik maddesinde kullanılan cihazlara ilişkin bilgilerin gerekli durumlarda toplanabileceği yer almaktadır.

Araştırılan diğer uygulama WhatsApp'ın 4 Ocak 2021 tarihli son güncellenen veri politikası incelendiğinde diğer uygulamalarda olduğu gibi kullanıcının temel hesap verilerinin toplandığı görülmüştür. Uygulamasının sohbet içeriğine erişim sağlamamakta ve kullanıcının mesajlarını depolanmadığı açık bir şekilde veri politikasında ifade edilmiştir. WhatsApp uygulamasının da web tarayıcısında açılmasını sağlayan WhatsApp Web özelliği bulunmaktadır. Web özelliği olan diğer uygulamalar gibi WhatsApp uygulaması da çerezleri kullanmaktadır. WhatsApp'ın kullanıcıdan otomatik olarak topladığı diğer bir veri, finansal kayıtlardır. Kullanıcı tarafından ödeme işlemi yapıldığında satın alma geçmişi de dahil olmak üzere ödeme yapıldığında ödeme ayrıntılarıyla ilgili her veri WhatsApp tarafından toplandığı tespit edilmiştir. Uygulama, otomatik olarak kullanıcının uygulamayı kullanım ve cihaz bilgisi verilerini de depolamaktadır. WhatsApp uygulaması, Facebook Şirket'i ürünlerinden biri olması sebebiyle, aynı cihaz üzerinden erişim ya da ilişkili hesap kullanıldığı durumlarda bu verileri otomatik olarak toplayabilmektedir.

Araştırma kapsamındaki uygulamalardan biri olan Discord uygulamasının son güncellenen 23 Haziran 2020 tarihli veri politikası incelenmiştir. Uygulama diğer uygulamalarda olduğu gibi kullanıcı hesap verilerini toplandığı görülmektedir. Bunun yanında diğer uygulamalardan farklı olarak Discord uygulaması kullanıcının ilgi alanları, davranışları, demografik verilerini de Amerika'daki sunucularda depolamaktadır. Diğer taraftan uygulama kullanıcının sohbet verilerini de toplamaktadır. Veri politikasında sohbet verilerinin kullanıcının sağlamış olduğu veriler olarak belirtilmesi diğer bir önemli bir noktadır. Discord uygulamasının kullanıcıdan topladığı diğer veri, çerezlerdir. Discord tarafından çerezler kullanılarak hem kullanıcının yerel ayarlarına ve günlük verilerine erişim sağlanmakta, hem de uygulamadaki üçüncü taraf web sitesi (Google Analytics vb.) araçları gibi ek hizmetler ve teknolojilerin kullanımı sağlandığı görülmüştür. Discord uygulamasının kullanıcının finansal verilerini de topladığı tespit edilmiştir. Bununla birlikte uygulama veri gizliliği politikasında kullanıcının cihaz bilgisi ve bağlantılar ile ilgili verilerinin toplandığı belirtilmiştir.

DOI NO: 10.17932/CTC.2021/ctc21.034

Araştırma kapsamındaki diğer uygulama ise Signal'dir. Signal uygulamasının 25 Mayıs 2018'de güncellenen en son veri gizliliği politikası incelenmiştir. Signal, uygulamasının araştırılan diğer uygulamalar arasında kullanıcıdan en az veri topladığı tespit edilmiştir. Signal uygulaması kullanının hesap oluşturabilmesi için bazı bilgiler talep etmektedir. Ancak veri politikasında kullanıcının hesap bilgilerinin toplanmadığı açık bir şekilde ifade edilmiştir. Ayrıca uygulama tarafından kullanıcın sohbet verilerinin de depolanmadığı görülmüştür. Diğer taraftan mesajlara erişim sağlanmadığı için cihazın ya da Signal hesabının güvenliğinden kullanıcı sorumlu tutulmaktadır. Signal uygulamasının veri gizliliği politikasında çerezler ile ilgili bir bilgi bulunmamaktadır. Signal üçüncü taraf sağlayıcıları da yalnızca doğrulama kodu gönderme ve destek hizmeti vermek amacıyla kullanmaktadır. Bunlara ek olarak Signal'in veri politikasında kullanıcının finansal kayıtları, kullanım verileri, cihaz bilgisi ve bağlantılar, kişisel verilere ilişkin bir bilgi de bulunmamaktadır. Signal uygulamasının diğer uygulamalardan daha az kullanıcı verisini talep ettiği görülmüştür.

Tüm bunlar değerlendirildiğinde Signal uygulaması haricinde diğer tüm platformların kullanıcı verilerini daha fazla oranda talep ettikleri görülmüştür. Bu veriler arasında yer alan kullanıcının uygulamayı kullanım verileri çeşitli ortaklar ve grup şirketleri ile paylaşıldığı tespit edilmiştir. Bu noktada kullanıcının bu verileri profillenerek kullanıcıya özel reklam ve pazarlama yapılmasıyla sonuçlanmaktadır. Bununla birlikte genel anlamda bu uygulamalar, arayüzü geliştirme ve daha fazla kitle tarafından tercih edilme amacıyla da bu verileri kullanabilmektedir. Önemli olan bir diğer nokta ise kullanıcının sohbet içeriğidir. BİP, WhatsApp ve Signal uygulamaları kullanıcının sohbet verilerine erişim sağlamadığı görülmüştür. Telegram ise gizli sohbet özelliği kullanılmadıkça ve Discord uygulaması da genel anlamda tüm sohbet verilerini depolamaktadır. Bir vakıf tarafından kurulan Signal uygulamasının genel anlamda gizlilik üzerine kurulu yapısı itibariyle araştırma kapsamındaki diğer tüm uygulamaların tersine kullanıcının üyelik bilgileri dışında kullanıcının kim olduğu, davranışları, eğilimleri, kullanım verilerini içeren veriler de dahil olmak üzere hiçbir bilgiyi depolamadığı görülmüştür. Sonuç olarak akıllı telefonlara çeşitli uygulamalar indirilirken, uygulamaların kullanıcının ne tür verilerini işlediğine dair tek açıklama olan veri politikalarının kullanıcı tarafından dikkatlice incelenmesi önem arz ettiği görülmüştür.

## Referanslar

[1]Binark, M. ve Bayraktutan G. (2013). *Yeni Medya ve Etik*. 1. Basım. İstanbul: Kalkedon Yayınları.

[2]Büyükuslu, A. R. (2017). *Dijital Kapitalizm.* 1. Basım. İstanbul: Der Yayınları.

[3]Couldry, N. ve Mejias, U. A. (2020). *Veri Sömürgeciliği: Büyük Verinin Modern Özne il İlişkisini Yeniden Düşünmek*. (Çev. Esra Cizmeci Ümit). Yeni Medya Kuramları II (içinde). Editör: Filiz Aydoğan. İstanbul: Der Yayınları.

[4]Dedeoğlu, G. (2016). Teknoloji, İletişim, Yeni Medya ve Etik. 1. Basım. İstanbul: Sentez Yayıncılık.

[5]Fuchs, C. (2020). *Endüstri 4.0: Dijital Alman İdeolojisi*. (Çev. Çağla Çavuşoğlu). Yeni Medya Kuramları II (içinde). Editör: Filiz Aydoğan. İstanbul: Der Yayınları.

[6]Fuchs C. (2016). Sosyal Medya: Eleştirel Bir Giriş.1. Basım. İ. Kalaycı ve D. Saraçoğlu (çev.). Ankara: NotaBene Yayınları.

[7]Greengard, S. (2017). *Nesnelerin İnterneti*. (Çev. Müge Çavdar). MIT Essentials. İstanbul: Optimist Yayınları.

[8]Kürkçü, D. D (2016). Yeni Medya ve Gençlik. Birinci Baskı. İstanbul: Kriter Yayınevi.

[9]Özsoylu, A. F. (2017). *Endüstri 4.0.* Çukurova Üniversitesi İİBF Dergisi. Cilt:21. Sayı:1. Haziran 2017. ss.41-64

[10]Özutku, F. vd. (2014). *Sosyal Medya'nın ABC'si*. İstanbul: Alfa Yaynları.

[11]Pavlik, J. V (2013). Yeni Medya ve Gazetecilik.1. Basım. M. Demir, B. Kalsın (çev.). Ankara: Phoenix Yayınevi.

[12]Rifkin, J. (2015). *Nesnelerin İnterneti ve İşbirliği Çağı*. (Çev. Levent Göktem). İstanbul: Optimist Yayınları

[13]Sayımer, İ. (2014). Yeni Medya Araştırmaları Kavramlar, Uygulamalar, Tartışmalar. 1. Basım. İstanbul: Literatürk Academia Yayınları.

[14]Yengin, D (2014). *Yeni Medya ve Dokunmatik Top*lum. 2. Basım. İstanbul: Derin Yayınları.

[15]Yılmaz. S. (2020). *Bir Gönüllü İfşa Aracı Olarak Panoptikon*. Korona Günlerinde Dijital Toplum (içinde). Editör: Ayten Övür. İstanbul: Der Yayınları.

DOI NO: 10.17932/CTC.2021/ctc21.034

## Elektronik Kaynaklar

URL-1 https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 (Erişim Tarihi: 16.09.2020)

URL-2 https://bip.com/tr/gizlilik-politikasi/#BiPGIZLILIKPOLITIKASI (Erişim Tarihi: 30.01.2021)

URL-3 https://telegram.org/privacy (Erişim Tarihi: 31.01.2021)

URL-4 https://www.whatsapp.com/legal/updates/privacy-policy/?lang=tr (Erişim Tarihi: 31.01.2021)

URL-5 https://discord.com/privacy (Erişim Tarihi: 30.01.2021)

URL-6 https://signal.org/legal/ (Erişim Tarihi: 31.01.2021)

DOI NO: 10.17932/CTC.2021/ctc21.034