ISSN: 1304-4796
Manisa Celal Bayar Üniversitesi Sosyal Bilimler Dergisi
Manisa Celal Bayar University Journal of Social Sciences
2022; 20 (2); 149-168

Sosyal Ağ Platformlarının Bilgi Politikalarına İlişkin Gizlilik Algısı: Kullanıcı Bilgi Davranışının Değerlendirilmesi

Türkay Henkoğlu[a, b],

Özet

Günümüzde sosyal ağ uygulamalarının temel unsurları arasında yer alan mesajlaşma yazılımlarının kişisel ve kurumsal kullanımı yaşamsal bir zorunluluk haline gelmiştir. Bu durum, yaygın olarak kullanılan mesajlaşma uygulamalarında, ilgili şirketlerin tamamen kendi stratejilere uygun güvenlik politikalarını uygulama isteğini arttırmaktadır. Bilgi güvenliği politikalarındaki bu tür değişiklikler, bireysel ve kurumsal gizliliğe yönelik endişeleri arttırmakta ve buna bağlı olarak kullanıcılar değişikliklere karşı tepki oluşturarak farklı uygulamalara yönelmektedirler. Bu çalışmada, dünyada ve Türkiye'de en fazla kullanıcısı olan WhatsApp uygulaması üzerinden inceleme yapılmış ve kullanıcıların mesajlaşma uygulamalarında gizliliğe yönelik olarak dikkat etmeleri gereken hususlar ortaya konulmuştur. Çalışmada WhatsApp tarafından yapılmak istenen değişikliklerin etkileri, kişisel verilerin korunması ve bilgi güvenliğinin sağlanmasına yönelik iki farklı yaklaşımla değerlendirilmiştir. Bu kapsamda bilgi güvenliği algısına bağlı olarak kullanıcıların sergiledikleri bilgi davranışının, sosyal ağ platformlarının içerdiği potansiyel risk ve tehditlerle bağdaşmadığı görülmüştür. Çalışma sonucunda, mesajlaşma uygulamaları üzerindeki risk ve tehditlere karşı kişisel ve kurumsal verilerin korunmasına ilişkin alınabilecek önlemler ve tercihler sunulmuştur.

Anahtar Kelimeler

Sosyal ağ platformları
Bilgi güvenliği ve gizlilik
WhatsApp
Bilgi davranışı

Makale Hakkında

Geliş Tarihi: 08.01.2022
Kabul Tarihi: 21.06.2022
Doi: 10.18026/cbayarsos.1055166

Privacy Perception of Social Network Platforms Regarding the Information Policies: Evaluation of User Information Behavior

Abstract

Today personal and corporate use of messaging applications, which are among the basic elements of social networking platforms, has become a vital necessity. This situation has increased the desire of relevant organizations to implement security policies on widely used messaging applications, which are completely suitable for their own strategies. Such changes in information security policies increase concerns about individual and corporate privacy, and as a result of this situation, users turn to different applications as a reaction to these changes. In this study, the WhatsApp application, which has the most users both in the world and in Turkey, was examined and the privacy issues that users should pay attention to in messaging applications were revealed. In the study, the effects of changes planned to be made by WhatsApp were evaluated with two different approaches to protecting personal data and ensuring information security. In this context, it was found that the information behaviors of users related to the perception of information security are not compatible with the potential risks and threats. At the end of the study, measures and preferences that can be taken to protect data against the risks and threats of messaging applications are presented.

Keywords

Social networking platforms
Information security and privacy
WhatsApp
Information behavior

About Article

Received: 08.01.2022
Accepted: 21.06.2022
Doi: 10.18026/cbayarsos.1055166

[a] İletişim Yazarı: turkay.henkoglu@adu.edu.tr
[b] Doktor Öğretim Üyesi, Aydın Adnan Menderes Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, ORCID ID: 0000-0002-0567-5408

Giriş

Bireylerin bilgi kazanımlarında, iletişimi sürdürmelerinde, oluşturulan gruplar ile sosyal kazanım elde etmelerinde ve bir arada kalabilmelerinde sosyal medya uygulamaları önemli bir rol oynamaktadır (Elciyar ve Küçük, 2020, s. 207). Kullanıcı dostu olması ve tüm kullanıcılar tarafından bireysel olarak da kullanılıyor olması nedeniyle, kurum ve kuruluşlar da son yıllarda yoğun bir şekilde sosyal medya platformlarında oluşturdukları arayüz ile kullanıcılarına ulaşmaya çalışmaktadırlar (Kwayu ve diğerleri, 2021; Şengöz ve Eroğlu, 2017). Ancak kurum ve kuruluşların faaliyet gösterdiği alana ya da sunduğu hizmete bağlı olarak, saklanan verilerin yeri, süresi ve saklanma koşulları önemli bir hukuksal soruna dönüşebilmektedir (Filerskeepers, 2021). Kurumsal yapılarda iki temel risk öne çıkmaktadır. Birincisi, elde edilen verilerden büyük veriye ulaşılması ve ilgili kurum ya da gruba ilişkin bilgi davranışlarının ortaya konulmasıdır. Kurum bazında elde edilen bilgilerin analiziyle, bu kurumların stratejilerine yönelik bilgilere ulaşılabileceği gibi, işleyiş üzerinde olumsuz etki yaratacak koşulların oluşturulması da mümkün olabilmektedir. İkinci önemli risk ise kullanılan altyapı ve kurumsal bilişim sistemlerine yönelik hukuka aykırı erişimlerdir. Bu tür erişimlerle çoğunlukla kişisel veriler hedef alınmakla birlikte, sistemi engelleme ya da sistem üzerinde bulunan bilgilere zarar verilmesi amacıyla girişimde bulunma da risk olarak görülebilmektedir.

Sosyal medya risklerinin kişisel verilerin korunmasına yönelik olarak değerlendirilmesinde üç önemli yaklaşım bulunmaktadır. Bunlar; bireysel riskler, kurumsal riskler ve toplumsal risklerdir. Bireysel riskler; kullanıcı bilgi davranışının tespiti, kişisel verilerin elde edilmesi ve kişiye özel ürünlerin sunulmasıdır. Kurumsal riskler; kurumsal verilerin elde edilmesi, kurumun prestijinin kaybolması ve/veya rekabet koşullarının değiştirilmesidir. Toplumsal riskler ise algı yönetiminin yapılması ve toplumsal hareketliliğe neden olabilecek zeminin oluşturulmasıdır.

Winter'ın (1997) sosyal medya platformlarının henüz yaygın olarak kullanılmadığı yıllarda gizlilik için yapmış olduğu tanım, WhatsApp vb. sosyal medya platformlarındaki risklere yaklaşım konusunda bugün de önemli bir bakış açısı sunmaktadır. Winter gizliliği, "kullanıcıların kendilerine ait kişisel bilgilerin ne zaman, nasıl ve ne kadarının başkalarının erişimine açılacağına karar vermeleri" olarak tanımlamaktadır. Buna göre mahremiyetin sağlanmasına yönelik risk ve tehditler sosyal medya platformları tarafından oluşturulabileceği gibi, bu platformları kullanan kullanıcıların da zafiyetlerin oluşumunda önemli etkilerinin olabileceği görülmektedir. Durgin'in (2007, s. 14) de ifade ettiği gibi, kullanılan bir sistem üzerinde bilgi güvenliğinin sağlanmasına ilişkin sahip olunabilecek en yüksek değer, risk unsurları arasındaki en zayıf noktanın sahip olduğu değerle eşit seviyededir. Organizasyonlar açısından bakıldığında, en sık gözden kaçırılan ve zafiyetlere neden olan unsurun organizasyon içindeki kişiler olduğu görülmektedir (Durgin, 2007, s. 5).

Sosyal ağ platformlarının gizlilik politikaları üzerinde yapmış oldukları değişiklikler, kullanıcılarda oluşan gizlilik algısını ve bu platformlar arasındaki kullanım tercihlerini değiştirmektedir. WhatsApp tarafından duyurulan yeni gizlilik sözleşmesinde verilerin Facebook ile paylaşılacağı bilgisine yer verilmesi üzerine kullanıcıların tepki göstererek diğer alternatif özel mesajlaşma platformlarıyla ilgilenmeye başlamaları bu algının sonucunda ortaya çıkan bir bilgi davranışıdır. Gizlilik algısına bağlı olarak kullanıcıların yöneldiği bazı mesajlaşma uygulamaları, kapasiteleri yetersiz olduğu için altyapılarını güçlendirmek ve yeni sunucuları hizmete sunmak zorunda kalmışlardır (Doffman, 2021b). Bu durum, gizlilik

politikalarına ilişkin kullanıcı bilgi davranışının etkilerinin sadece bireylerin gizliliği ile sınırlı olmadığını, tercih edilen platformların geleceği üzerinde de etkili olabileceğini göstermektedir.

Çalışmanın Önemi

Amerika Birleşik Devletleri (ABD), Çin, Hindistan, İngiltere ve Almanya'daki yaşayan bireylerin katıldığı anketler üzerinden elde edilen verilere göre, sağlık bilgileri, iletişim bilgileri, kimlik bilgileri ve banka kartı bilgilerinin korunması için daha fazla ödeme yaptıkları ve kişisel verilerin güvenli olarak işlenmesi konusunda en az sosyal medya şirketleri ve sosyal medya platformlarına güvendikleri görülmektedir (Morey ve diğerleri, 2015, s. 6, 9). Bireylerin hassasiyet gösterdiği sosyal medya platformları arasında iki milyarın üzerinde aktif kullanıcı sayısıyla üçüncü sırada olan (Statista, 2021) ve dünyanın en büyük özel mesajlaşma aracı (Doffman, 2021b) olarak kullanılan WhatsApp, aynı zamanda dünya genelinde en fazla kullanıcıya sahip sosyal medya platformu olan Facebook bünyesinde yer almaktadır. Global Web Index'in Sosyal Medya Kullanıcı Eğilimleri Raporuna göre, 16-64 yaş arası internet kullanıcı oranları üzerinden değerlendirildiğinde, Türkiye WhatsApp kullanımı konusunda %88 oran ile dünyada sekizinci sırada bulunmaktadır (Rollason, 2021). Kullanım oranına bağlı olarak, WhatsApp aracılığıyla iletişim ve tanımlanan grup paylaşımları üzerinden bilgilenme süreçlerinin bireyler için gereksinimin de ötesinde zaman zaman zorunluluğa dönüştüğü görülmektedir. Bu nedenle çalışmada, WhatsApp örneği üzerinden veri koruma ve bilgi güvenliği kapsamında değerlendirme yapılması ve mevcut koşulların ortaya konulması hedeflenmektedir.

Çalışma kapsamında WhatsApp tarafından uzun süredir sözleşme üzerinde yapılmak istenen değişikliklerin hukuksal koşulları ve bilgi güvenliği riskleri iki farklı yaklaşımla değerlendirilmekte ve göz önünde bulundurulması gereken bilgi güvenliği unsurlarına dikkat çekilmektedir. Bununla beraber, kişisel hakların veri koruma kurulu ve/veya komiserliği gibi veri koruma otoriteleri tarafından savunulması, bireylerin değişikliklere tepki göstererek alternatif platformlara yönelmeleri ve WhatsApp'ın tek taraflı değişikliklerden geri adım atması süreci değerlendirilmiş ve kullanıcı bilgi davranışının sonuçları tartışılmıştır. Çalışmanın mevcut hukuksal koşullara dikkat çekilerek ve bilgi güvenliğine yönelik mevcut durumu açıklayan yaklaşımlar ortaya konularak şekillendirilmesinin, kullanıcıların daha büyük zafiyetlere neden olabilecek görece kişisel verilerin güvenliğini tehdit etme potansiyeli yüksek unsurlara odaklanmalarına katkı sağlayacağı düşünülmektedir.

Çalışmanın Amacı ve Araştırma Soruları

Sosyal ağ platformlarının en önemli bileşenlerinden biri olan mesajlaşma uygulamalarının tümünün, bilgi güvenliği risk ve tehditlerine yönelik zafiyetlerinin bulunduğu açıktır (Clarke ve Ali, 2017). Ancak bunların içinde en fazla kullanıcı sayısına sahip WhatsApp, kullanıcı gizliliğinin sağlanmasına ilişkin tartışmaların odağında yer almaktadır. Bu nedenle çalışmada mevcut durumu saptamaya ve koşulların olduğu gibi ortaya konulmasına yönelik betimleme yöntemi (Kaptan, 1995, s. 59) kullanılarak WhatsApp örneği üzerinden inceleme yapılmıştır. Bu kapsamda WhatsApp kullanıcı sözleşmeleri içinde beyan edilen güvenlik uygulamaları, bilgi güvenliği ve kişisel verilerin korunmasına yönelik yaklaşımlar ve WhatsApp uygulamasının diğer uygulamalardan ayrılan yönleri araştırılmıştır. Elde edilen veriler ışığında, WhatsApp ve yaygın olarak kullanılan diğer sosyal ağ uygulamaları tarafından toplanan kişisel veri miktarına ilişkin kıyaslamalı örnekler sunularak, kullanıcıların risk

algısının zafiyet oluşturma potansiyeli yüksek risk ve tehditlerle ne kadar tutarlı olduğunun ortaya konulması amaçlanmıştır. Aynı zamanda kullanıcıların odaklanması gereken zafiyet oluşturma potansiyeli yüksek risk ve tehditlere dikkat çekilerek, çalışmanın kullanıcı farkındalığına katkı sağlanması hedeflenmiştir.

Çalışmanın amacı doğrultusunda aşağıda yer alan araştırma sorularına yanıt aranmıştır;

a. Sosyal ağ uygulamaları ne tür verileri, hangi amaçla ve nasıl işlemektedir?
b. Sosyal ağ kullanıcılarının kişisel verilerinin korunmasına yönelik literatürde genel yaklaşım nasıldır?
c. Sosyal ağ kullanıcıların gizliliğinin korunmasına yönelik olarak AB ve Türkiye'deki veri koruma otoritelerinin değerlendirmeleri ve uygulamaları nelerdir?
d. WhatsApp tarafından kullanıcılara sunulan sözleşmelerde, kullanıcı gizliliğinin sağlanmasına yönelik hangi taahhütleri içermektedir?
e. WhatsApp vb. uygulamaların diğer sosyal medya platformlarıyla daha fazla veri paylaşma istekleri ve buna yönelik sözleşme tasarıları bilgi güvenliği ve hukuksal açıdan ne tür sorunlar içermektedir?
f. Mesajlaşma yazılımlarında öne çıkan uçtan uca kriptolama uygulaması kullanıcı gizliliğinin sağlanması için yeterli midir?

Kişisel Verilerin Korunmasına Yönelik Yaklaşım

Sosyal ağlar ve bulut alanlarının kullanımına yönelik teknolojik gelişmeler, bilginin elde edilmesi, işlenmesi ve saklanmasına yönelik değişimi de beraberinde getirmiştir. Bu yeni teknolojiler, kişisel verilerin hukuka aykırı olarak elde edilmesini, transferini ve kullanımını kolaylaştırmaktadır. Çoğu ücretsiz olan sosyal ağ uygulamalarının hizmet bedelinin ödenmesi, kullanıcılar farkında olmasa da kişisel veriler kullanılarak yapılmaktadır (Stepanova ve Feldmann, 2020). Kişisel verilerin korunmasına yönelik güncel hukuksal düzenlemelerin ve uluslararası sözleşmelerin yanı sıra, veri sahiplerinin de verilerinin korunması konusunda almaları gereken bazı sorumluluklar bulunmaktadır. Verilerin işlenmesi, transferi ve kullanımına yönelik izin ve onayın verilmesi konusunda kullanıcıların bilinçli olmaları gerekmektedir (Akıncı, 2017, s. 19).

Temel olarak kurum ve kuruluşların e-posta gönderimleri için de merkezi yurt dışında bulunan hizmet sağlayıcılarını kullandıkları bilinmektedir (Henkoğlu, 2017, s. 161). Birçok sosyal paylaşım sitesinin sözleşmesinde belirtildiği gibi, bu tür hizmet sağlayıcılar da sunmuş oldukları ücretsiz hizmetin karşılığında elde etmiş olduğu kişisel verileri nasıl kullanacaklarını belirtmektedirler (Google, 2021b; Microsoft, 2021; Yahoo, 2021; Yandex, 2021). Bu sözleşme metinlerinde yer alan taahhütlerin benzer nitelikte olması, kişisel verilerin korunmasına yönelik olarak evrensel ilkelerin (OECD, 2013) benimsenmiş olduğunu göstermektedir. Bazı hizmet sağlayıcıların (Google, 2021a), bu ilkeleri maddeler halinde açıklayarak kullanıcılara sundukları görülmektedir. Ancak sunucuları yurt dışında olan hizmet sağlayıcıların, bu ilke ve taahhütleri yazılı olarak sunmasının da yeterli olmadığı görülmektedir. Kurumlarda gizlilik içeren kurumsal haberleşme ve belge paylaşım kanalı olarak WhatsApp gibi mesajlaşma uygulamalarının kullanılması, 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi ile bağdaşmamaktadır (CBDDO, 2020, s.211-214; 2019/12 Sayılı

Genelge, 2019). Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin (CBDDO) hazırladığı Bilgi ve İletişim Güvenliği Rehberinde (2020, s.161), sunucuları yurt dışında bulunan WhatsApp gibi mesajlaşma uygulamaları yerine, ihtiyaç duyulan güvenlik gereksinimlerinin karşılanması durumunda sunucuları yurt içinde bulunan mesajlaşma uygulamalarının kullanılması teşvik edilmektedir.

Avrupa Birliği (AB) veri koruma tüzüğü ve buna bağlı uygulamaların katı bir şekilde uygulanması nedeniyle, AB sınırları içindeki kullanıcılara daha uygun koşulları içeren sözleşmeler sunulmaktadır (O'Flaherty, 2021). Zira bu konuya ilişkin olarak AB veri koruma mevzuatında belirtilen yüksek ceza oranlarının ilgili hizmet sağlayıcılara birçok kez uygulandığı görülmektedir (Satariano, 2019). 11 Mayıs 2021 tarihinde Hamburg Veri Koruma ve Bilgi Özgürlüğü Komiserliği'nin (HmbBfDI) WhatsApp kullanıcı verilerinin Facebook tarafından kendi amaçları için daha fazla işlenmesini yasaklayan (Schemm, 2021) bir karar alması, AB içinde veri koruma konusundaki hassasiyeti ortaya koyan bir örnek olarak dikkat çekmektedir. HmbBfDI tarafından alınan kararın arka planında, WhatsApp'ın 15 Mayıs 2021 tarihinden itibaren geçerli olacak yeni gizlilik politikasında, kullanıcılardan Facebook ile veri paylaşmak için kapsamlı yetki vermelerinin talep edilmesi bulunmaktadır. HmbBfDI basın bülteninde bu kararın üç ay süreyle uygulanmasını GDPR'nin aciliyet prosedürü uyarınca istediğini ve bu kararın aynı zamanda Avrupa düzeyinde bağlayıcı bir karar oluşması için Avrupa Veri Koruma Kurulu'na (European Data Protection Board-EDPB) gönderileceğini belirtmektedir. Bültende, WhatsApp gizlilik sözleşmesindeki güncellemelerin hukuka uygunluğuna ilişkin bazı dikkat çekici değerlendirmeler şunlardır (Schemm, 2021);

a. Veri sahiplerinin hak ve özgürlüğü karşısında, WhatsApp kullanıcılarının kişisel verilerinin Facebook tarafından kendi amaçları için işlenmesinin bir yasal dayanağı bulunmamaktadır.
b. Gizlilik politikasının Avrupa ve uluslararası sürümleri ayırt edilememekle birlikte, veri aktarımlarına ilişkin hükümler dağınık olarak verildiği için anlaşılır değildir.
c. Gizlilik politikasının içeriğinde yanıltıcı ve çelişkili ifadeler bulunduğu için, onaylamanın kullanıcılar için doğurabileceği sonuçlar açık değildir.
d. WhatsApp, yeni hükümlerin kabul edilmesi koşuluyla hizmete ilişkin işlevlerin sürekli kullanımına izin vereceğini belirtmektedir. Bu onayın, bilgilendirilmeye dayalı ve özgür iradeyle açıklanan rıza ile kullanıcı tarafından verilmediği görülmektedir. Özellikle küçük yaştaki kullanıcılar için bu durumun daha belirgin olduğu görülmektedir. Bu nedenle, alınan rıza ile veri koruma mevzuatı çerçevesinde yasal dayanak oluşturulması mümkün değildir.
e. Kapsamlı veri aktarımı için şeffaf olmayan koşullarla yapılmak istenen veri işleme faaliyetlerinin GDPR'ye uygun değildir.
f. Kullanıcı güveninden yoksun verilere dayalı iş modelleri uzun vadede başarılı olamayacağı için rıza mekanizmasının tüm dünyada yeniden değerlendirilmesi gerekmektedir.
g. WhatsApp tarafından oluşturulan yeni sözleşme, Cambridge Analytica skandalında (Zialcita, 2019) olduğu gibi, temel hak ve özgürlüğe yönelik yeni ihlallerin oluşmasına imkân sağlamaktadır.

WhatsApp'ın yeni gizlilik sözleşmesinde kişisel hak ihlaline neden olabilecek veri paylaşımını içeren kullanım koşullarının, Türkiye'de de veri koruma otoriteleri tarafından zaman geçmeksizin incelemeye alındığı görülmektedir. WhatsApp tarafından güncellenen gizlilik ilkesinin kullanıcılar tarafından onaylanmasının istenmesi üzerine, 11 Ocak 2021 tarihinde Rekabet Kurumu tarafından geçici tedbir kararının alındığı bildirilmiştir. Veri koruma otoritelerinin başlattığı soruşturmaların ve kullanıcıların alternatif platform arayışlarının etkisiyle, WhatsApp önce planlanan güncellemenin tüm dünyada 15 Mayıs 2021 tarihinden itibaren geçerli olacağını duyurmuş, daha sonra da bu sözleşmenin Türkiye'deki hiçbir kullanıcı için yürürlüğe girmeyeceğini Rekabet Kurumu'na bildirmiştir (Rekabet Kurumu, 2021).

Sosyal medya hizmetleri sunan tüm yurtdışı kaynaklı şirketlerin bir veri ihlali olması durumunda aynı tutumu göstermeyeceği açıktır. Örneğin ABD mevzuatı gereğince, bir veri tabanından herhangi bir nedenle kişisel veri ihlali olması halinde, ilgili veri sorumlusunun en kısa sürede kamuoyunu ve veri sahibini bilgilendirmesi gerekmektedir. Bu sayede ilgili veri sahipleri, hukuka aykırı olarak ele geçirilen kişisel verilerine (kredi kartı bilgileri vb.) yönelik tedbirleri alabilmekte ve olası zararların önüne geçilebilmektedir. Merkezi Türkiye dışında bulunan tüm hizmet sağlayıcıların Türkiye'deki kullanıcılarına yönelik olarak benzer bir bildirim taahhüdü bulunmamaktadır. WhatsApp hizmet koşullarına (2021b) ilişkin ihtilafların çözümü konusunda, Kaliforniya Eyaleti yasalarının geçerli olacağı ve münhasıran ABD Kaliforniya Kuzey Bölgesi Bölge Mahkemesi ya da Kaliforniya San Mateo County'de bulunan bir eyalet mahkemesinin yetkili olarak kabul edileceği belirtilmektedir. Bununla beraber, eğer WhatsApp tarafından uygun görülürse ihtilafın çözümü için kullanıcının ikamet ettiği ülkede yargı yetkisine sahip olan bir yetkili mahkemenin de kabul edilebileceği ifade edilmektedir. Türkiye'de bulunan bir kullanıcının, ihtilaf durumunda Kaliforniya Eyaleti yasalarına tabi olarak ABD'de bulunan bir mahkemede bu ihtilafın çözümü için çaba harcaması, oldukça zorlu bir süreci işaret etmektedir.

WhatsApp tarafından hizmet performansını arttırma amacıyla otomatik olarak elde edilen kullanım bilgileri, genel konumun tahmini amacıyla işlenen IP adresi bilgisi ve hizmetlerin özelleştirilmesi amacıyla kullanılan çerezler, kişisel verilerin korunması açısından sorunlu olarak ifade edilebilecek işlemlerdir. Kanaatimizce bir kullanıcının WhatsApp ile konum bilgisini paylaşmak istememesi nedeniyle ilgili servisi kapatması, IP adresi vb. veriler kullanılarak genel konum bilgilerine ulaşılmasına da rızasının olmadığı anlamına gelmektedir. Nitekim bir IP adresinin kişi ile ilişkilendirilerek ve ilgili kullanıcının genel konum bilgisi olarak işlenmesi, veri koruma hukuku (KVKK, 2016) açısından da irdelenmesi gereken bir durumdur. Benzer şekilde WhatsApp gizlilik politikasında (2021a), cep telefonu üzerinde kayıtlı kullanıcı bilgilerinin, başkaları tarafından sağlanması halinde işleyebileceğini belirtilmektedir. WhatsApp tarafından bu bilgiyi sağlayan üçüncü tarafın yasal olarak ilgili kullanıcının bilgilerini toplama, kullanma ve paylaşma hakkına sahip olması şart koşulmuş olsa da pratikte bunun kontrol ve denetiminin mümkün olmadığı bilinmektedir. WhatsApp tarafından belirtildiği gibi, bilgiyi sağlayan üçüncü tarafın gerekli hukuksal koşulları sağlayarak bu bilgileri WhatsApp ile paylaştığı göz önüne alındığında ise, ilgili kişinin bilgisi dahilinde olmasa dahi veri koruma hukukuna aykırı olarak bilgi toplanmadığı sonucuna ulaşılmaktadır.

WhatsApp vb. uygulamaların sunucuları üzerinde (geçici olarak da olsa) saklanan bilgiler arasında, kişiler arasında yapılan yazılı, sesli ve/veya görüntü görüşmelerin ve gönderilen

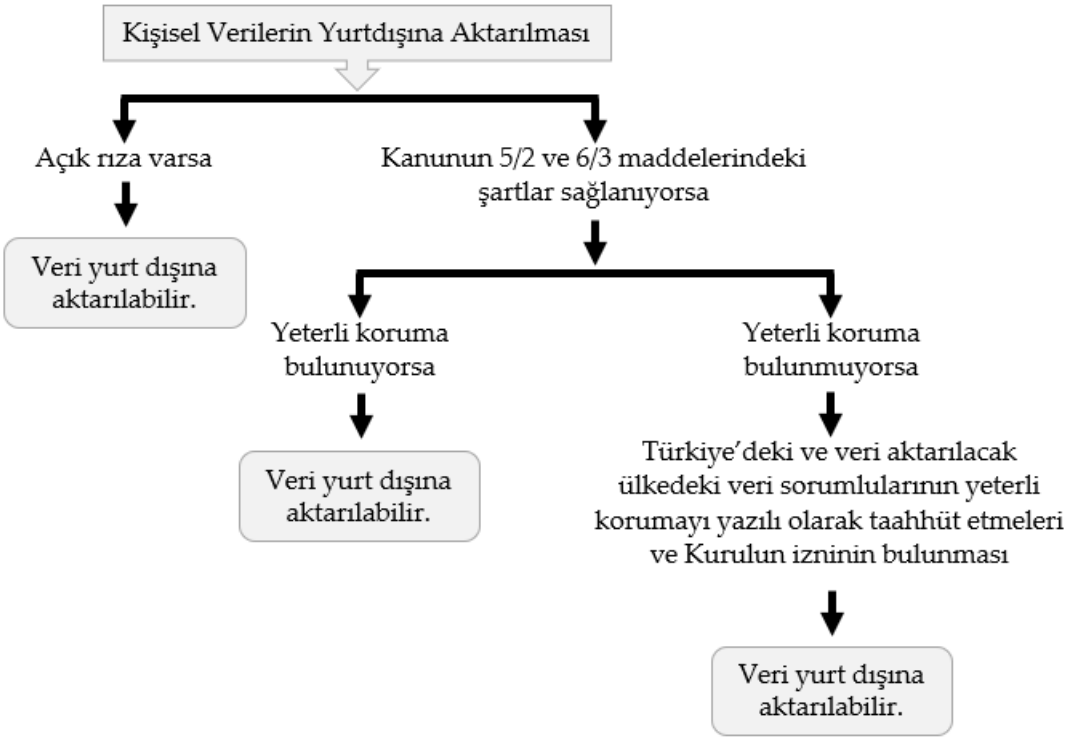
dosyaların bulunabileceği açıktır. Bu tür iletişim bilgileri de gizlilik açısından önemli riskler barındırmaktadır. Görüşmenin ilgili tarafları ya da üçüncü taraflarca sağlanan bu bilgilere ilişkin hukuksal sorumluluklar, Türk Ceza Kanunu'nun (TCK) (2004) dokuzuncu bölümünde 132 ila 140. Maddeleri arasında düzenlenmiş olan "özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altındaki düzenlenmeler kapsamında değerlendirilmektedir. Bu durumda, WhatsApp sunucuları üzerinde geçici olarak saklanan bilgilerin güvenliğine yönelik riskler bulunurken, esasen bu risklerin oluşumu öncesinde hukuken suç olarak tanımlanmış bir eylemin gerçekleşmiş olabileceği göz ardı edilmemelidir. Benzer şekilde, haber kanalı vb. üçüncü taraf hizmeti içinden bilgi paylaşımı amacıyla WhatsApp bağlantısının kullanılması durumunda da üçüncü taraf hizmetinin sunulduğu platformun gizlilik sözleşmesi dikkate alınmalıdır.

WhatsApp gizlilik ilkeleri içinde, verilerin AB Hukukuna uygun olarak işlendiği belirtilmektedir. Bilginin saklanmasına yönelik işlemlerin de aynı hukuksal dayanaklara bağlı olarak yapıldığı ifade edilmektedir. Bununla beraber, kullanıcıların bilgilerinin işlenmesine yönelik itiraz edebilecekleri ve bazı kullanım kısıtlamalarını ya da engellemeleri yapabilecekleri seçenekler sunulmaktadır. Saklanan bilgilere hukuksal çerçevede erişim sağlanması ve paylaşım yapılmasına ilişkin gerekçeler ise örnekler verilerek açıklanmaktadır (WhatsApp LLC, 2021a);

WhatsApp, Facebook'un küresel altyapısını ve veri merkezlerini kullanmaktadır. Bu kapsamda küresel faaliyetlerine ilişkin olarak, gizlilik ilkeleri çerçevesinde dahili olarak Facebook ve harici olarak diğer ortaklarıyla bilgileri paylaştığını belirtmektedir. Bununla beraber, gizlilik ilkesinde açıklanan amaçlar doğrultusunda bu bilgilerin ABD ve/veya diğer ülkelere transfer edileceğini, bu ülkelerde saklanacağını ve işleneceğini açıklamaktadır. Facebook tarafından yapılan açıklamalarda ise buna ilâve olarak, AB veri koruma kurumlarıyla daha önce yapılan görüşmeler çerçevesinde WhatsApp bilgilerinin AB'de doğrudan reklam amacıyla kullanılmadığı vurgulanmaktadır. Bu açıklama, AB için bir muafiyet uygulandığını göstermektedir. Buna göre AB'deki kullanıcıların WhatsApp'ı kullanmaya devam etmek için şartları kabul etmeleri zorunlu tutulurken, veri gizliliği koşullarında herhangi bir değişiklik olmayacağı anlaşılmaktadır (Holroyd, 2021). Avrupa Komisyonu (2019) da internet kullanıcılarında farkındalık oluşturmak amacıyla konuya ilişkin olarak sosyal medya ve mesajlaşma platformlarında sanal kimliğin korunmasına yönelik bilgilendirmeler yapmaktadır.

WhatsApp tarafından bazı hizmetlerin sunulabilmesi için gerekli olduğu öne sürülen bilgi transfer işlemlerinin hukuksal dayanağının Avrupa Komisyonu tarafından onaylanan sözleşme olduğu belirtilmektedir (WhatsApp LLC, 2021a). Ancak Avrupa Komisyonu (2021) tarafından yeterli koruma seviyesinin bulunması gerekçesiyle alınan uygunluk/yeterlilik kararlarının Türkiye sınırları içindeki kullanıcılar için bağlayıcılığının olmadığı açıktır. Şekil 1 üzerinde görüldüğü gibi kişisel verilerin yurt dışına aktarılabilmesi için, KVKK'nın (2016) 9. Maddesi gereğince ilgili kişinin açık rızasının bulunması, KVK Kurulu tarafından ilan edilen yeterli korumaya sahip güvenli ülkelerden biri olması ya da Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yazılı olarak taahhüt etmiş olduğu koruma ile birlikte KVK Kurulu izninin bulunması gerekmektedir. ABD ve/veya diğer ülkelerle Türkiye'nin taraf olduğu bir sözleşmenin bulunmadığı da göz önüne alındığında, Türkiye'de bulunan kullanıcıların verilerinin yurtdışına aktarımı için açık rızasının bulunması önem taşımaktadır. Bu açık rıza, WhatsApp'ın işlemesine izin verilen verinin kapsamının, sınırlarının, işlenme

şeklinin ve süresinin belirlemesini de sağlamaktadır. WhatsApp kullanıcıları, kişisel verilerinin geleceğini belirleme hakkı kapsamında vermiş oldukları açık rızayı istedikleri zaman geri alabilmelidirler (KVK Kurumu, 2020).



Şekil 1. Kişisel Verilerin Yurtdışına Aktarılması (KVK Kurulu, 2018)

Bilgi Güvenliğinin Sağlanmasına Yönelik Yaklaşım

Türk hukuk mevzuatında verilerin güvenli bir şekilde saklanması ve/veya hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için teknik ve idari tedbirlerin alınmasına ilişkin politikaların geliştirileceği ve bu konuya ilişkin önlemlerin veri sorumlusu tarafından alınacağı belirtilmektedir (KVK Kurulu, 2017; KVKK, 2016). Ancak bu konuda hangi standartların, hangi koşullarda ve nasıl uygulanacağına yönelik özel bir düzenleme bulunmadığı gibi, kurum ve kuruluşlarda bilgi güvenliğinin sağlanmasına yönelik olarak belirli standartlar çerçevesinde hazırlanmış bir bilgi güvenliği politikasının oluşturulma zorunluluğu da bulunmamaktadır. Bu nedenle, özellikle kurumsal düzeyde bilgi ve iletişim araçları topyekûn değiştirilmediği sürece, güvenlik önlemi olarak bir sosyal medya platformundan diğerine geçilmesi bilgi güvenliği açısından önemli bir kazanım sağlamamaktadır.

WhatsApp gizlilik ilkelerinin (2021a) güncellenmesi ile birlikte, gizliliğin korunmasına yönelik endişe ve tartışmaların arttığı görülmektedir. Ancak kullanıcıların çok büyük bir bölümünün takip etmiş olduğu medya yayın organları üzerinden yapılan bu tartışmaların odağında, verilerin kontrolsüz bir şekilde WhatsApp tarafından servis edileceği endişesi bulunmaktadır. Buna karşın WhatsApp tarafından yayınlanan bilgilendirme mesajında (WhatsApp LLC., 2021), uçtan uca yapılan görüşme içeriğinin gizliliğinin korunmasına yönelik herhangi bir değişiklik olmayacağı ve mevcut güvenlik düzeyinden ödün verilmeyeceği belirtilerek, bu çerçevede benimsenen ilkeler ve verilen güvenceler

açıklanmaktadır. Verilen güvencelerin bilgi güvenliğinin sağlanmasına yönelik işlemleri içerdiği görülmektedir. Bu önlemlerin, aynı zamanda kişisel verilerin korunmasına yönelik katkı sağlayacağı ve hatta kişisel verilerin korunması için gerekli temel işlemler olduğu açıktır. Bununla beraber, kişisel verilerin korunmasına yönelik bu taahhütleri sunan WhatsApp'ın, gerekli teknik önlemleri alabilme imkân ve kabiliyetine sahip olmasının da kullanıcılar tarafından dikkate alınması önem taşımaktadır. Diğer taraftan, her ne kadar WhatsApp güvenlik maliyetini arttıran uçtan uca kriptolama özelliğiyle merkezi yurt dışında bulunan ve dünya genelinde çok sayıda kullanıcısı olan rakiplerine karşı daha avantajlı görünse de günümüzde uçtan uca kriptolama özelliğinin iletişim güvenliği tercihi açısından temel şartlardan biri olduğu göz ardı edilmemelidir. CBDDO'nun (2020, s.162) "Bilgi ve İletişim Güvenliği Rehberinde" belirtilen genel güvenlik önlemleri arasında, mesajlaşma uygulamalarından gönderilen tüm mesajlar ve uygulama kullanılarak yapılan tüm sesli ve görüntülü aramalar için uçtan uca kriptolamanın kullanılması önerilmektedir.

Kişiselleştirme konusunda yapılan çalışmalar (Wattal ve diğerleri, 2009), bazı şirketlerin daha fazla kullanıcıya ulaşabilme ve kullanıcılara daha yakın olabilme amacıyla kişiselleştirme araçlarını kullandıklarını göstermektedir. Çevrimiçi uygulamalarda gazetelerin genel bir ön sayfa yerine kullanıcılarına doğrudan ilgilendikleri haber konularına yönelik içeriği sunmaları, bu konuda yıllardır uygulanan kişiselleştirme örneklerinden biridir (Wattal ve diğerleri, 2009). WhatsApp, öncelikli olarak spam, tehditler, kötüye kullanım veya ihlal faaliyetleriyle mücadele için Facebook Şirketleri ile bilgi alışverişinde bulunduğunu belirtmekle birlikte, hizmetlerin geliştirilmesi ve özelleştirme amacıyla da bilgi paylaşımı yapıldığının ve bunun içinde sistemlerin güvenliğini sağlama hedefinin de olduğunun altı çizilmektedir. Bu amaçla WhatsApp tarafından otomatik olarak elde edilen ve kullanıcıları endişelendiren bilgiler arasında, hizmet performansını arttırmaya yönelik kullanım bilgileri, genel konumun tahmini amacıyla IP adresi bilgisi ve hizmetlerin özelleştirilmesi amacıyla kullanılan çerezler ile elde edilen bilgiler yer almaktadır. Kullanıcıların konum bilgilerini başkaları ile paylaşabilmelerini sağlayan hizmetlerin sunulabilmesi ise kullanıcıların bu verileri sağlaması ile mümkün olabilmektedir (WhatsApp LLC, 2021a).

WhatsApp, sunucularında herhangi bir mesaj saklama işlemi yapmadığını, bunun yerine mesajların kullanıcı telefonunda saklandığını belirtmektedir (WhatsApp LLC, 2021a). Bununla beraber, 30 gün boyunca teslim edilemeyen mesajların ve mesaj ile gönderilen medyanın tekrar gönderilme işlemlerinde hız kazandırılması amacıyla geçici olarak sunucularda tutulduğu bilinmektedir. Bu durum merkezi veri depolama ortamı olarak WhatsApp sunucuları üzerinde geçici süreyle tutulduğu ifade edilen bilgiler için risk oluşturmaktadır. Ancak kullanıcılar için daha büyük bilgi güvenliği riski barındıran ortamın, kullanıcı telefonunun veri depolama ortamı olduğu aşikârdır. Ayrıca kullanıcı telefonu kaynaklı bilgi güvenliği zafiyetlerinin oluşması halinde hem telefon üzerinde tutulan bilgilere hem de telefon üzerinden elde edilen diğer uygulamalara ilişkin kullanıcı adı ve şifreleri ile kullanıcının erişim sağladığı tüm merkezi veri depolama ortamlarına erişim sağlanması mümkün olabilmektedir (Henkoğlu, 2018, s. 25).

Bilginin korunmaya değer temel karakteristik özelliklerinden biri de erişilebilirliktir (Henkoğlu, 2015). Kullanıcıların ihtiyacı olan bilgiye erişim yetkisi dahilinde istediği zaman ulaşabilmesi ve kullanabilmesi, bilgi güvenliği çerçevesinde sağlanması beklenen asgari koşullar olarak görülmektedir (Peltier ve Peltier, 2007, s. 89-90). Ancak WhatsApp hizmet koşullarında (2021b), bakım ve onarım gibi gerekçelerle hizmetlerde kesinti olabileceği gibi,

WhatsApp tarafından istenildiğinde tamamen durdurulabileceği belirtilmektedir. Hangi koşullarda hizmetin tamamen durdurulmasına yönelik kararın alınabileceğinin açık olarak belirtilmemesi, kullanıcıların ihtiyaç duyduğu bilgi ve sunulan hizmete istediği zaman erişim sağlayabilmesi açısından düşündürücüdür.

WhatsApp bilgi güvenliğinin sağlanması amacıyla, maliyeti daha yüksek olan uçtan uca şifreli iletişimi kullanmaktadır. Ücretsiz olarak hizmet sunan bu tür platformların faaliyetlerine devam edebilmesi reklam gelirleriyle mümkün olabilmektedir. Bu reklamların kişiselleştirilmiş olması ve reklam veren şirketlerle kullanıcılar arasında köprü olması da reklamlarla ilgili hedefler içinde yer almaktadır. Sosyal medya platformlarının birçoğunun, kullanıcıların kişisel verilerini reklamcılık ve web sitesi yönetimi amacıyla topladığı ve kullandığı bilinmektedir (Atamaniuk, 2021; Doffman, 2021a). Kullanıcılar her ne kadar haberleşme içeriğinin açığa çıkması konusunda endişelenseler de iş modeli reklamcılığa dayalı olan Facebook ile WhatsApp verilerinin paylaşımına ilişkin tartışmaların odağında, reklamlara ilişkin politikaların hayata geçirilmesi amacıyla mesaj içeriğinin kullanılması bulunmaktadır. Kullanım amacından bağımsız olarak, Facebook'un isminin önceki yıllarda veri paylaşım skandallarıyla birlikte gündeme taşınmış olması, WhatsApp bilgilerinin Facebook ile paylaşımı konusunda kullanıcılarda endişe oluşturabilmektedir (Hinds ve diğerleri, 2020). AB bu konuya ilişkin olarak Genel Veri Koruma Tüzüğü (GDPR) çerçevesinde WhatsApp Ireland Limited ile görüşmeler yaparak, bu tür reklam amaçlı veri paylaşımlarının yapılmamasını sağlamıştır.

Şirketlerin sadece hizmetin sürekliliği için gerekli olan bilgileri toplaması, saklaması ve bilgi paylaşımına ilişkin şeffaf tutumu, kullanıcıların uygulama tercihini doğrudan ve olumlu yönde etkileyen unsurlardır. Morey ve diğerleri (2015, s. 6) tarafından yapılan bir araştırma, katılımcıların %97'sinin bu konuda kamu kurumlarına dahi güvenmediklerini ve bu verilerin kötüye kullanılmasından endişe duyduklarını göstermektedir. Çalışmada ayrıca, gizliliklerini korumak amacıyla katılımcıların yaklaşık %76'sının şirketlerle bilgi paylaşımında isteksiz davrandığı vurgulanmaktadır. Kullanıcıların, bu hususlara ilişkin bilgi güvenliği önlemlerini dikkate alarak alternatif mesajlaşma uygulamalarına yöneldikleri görülmektedir. Tablo 1'de, WhatsApp ile birlikte merkezi yurt dışında bulunan ve dünyada en fazla kullanıcısı olan diğer iki özel mesajlaşma platformunun uygulama özellikleri bu çerçevede kıyaslanarak verilmiştir.

Tablo 1. WhatsApp, Signal ve Telegram Uygulama Özelliklerinin Karşılaştırılması

	WhatsApp	**Signal**	**Telegram**
Uçtan uca kriptolama	Var	Var	Sadece gizli mesajlar
Belirli süre sonunda mesajların kaybolması/silinmesi	Evet	Evet	Evet (Gizli mesajlar)
Mesajların yedeklenmesi	Google/iCloud üzerinde	Sadece cihaz üzerinde	Telegram bulut sunucularında (Gizli mesajlar yedeklenmez)
Grup mesajlarının güvenliği	Evet, Uçtan uca kriptolama	Evet, Uçtan uca kriptolama	Hayır
Ekran kilidi	Evet	Evet	Evet

Reklam	Hayır	Hayır	Hayır
Çift doğrulama	Evet	Evet	Evet
Konum bilgilerinin elde edilmesi	Evet	Hayır	Hayır
Cihaz kimliğinin elde edilmesi	Evet	Hayır	Hayır

Tablo 1'de görüldüğü gibi, WhatsApp uçtan uca şifreleme yöntemini, kullanıcı mesajlarına erişimi engelleyecek şekilde her sohbet için uygulamaktadır. Bu nedenle WhatsApp, güvenli mesajlaşma uygulamalarından biri olarak öne çıkmaktadır. Kullanıcıların daha güvenilir olduğunu düşündükleri için tercih ettiği platformlardan biri olan Telegram'da ise uçtan uca şifreleme yöntemi, kullanıcıların her bir kişi için aktif olarak seçmesi gereken "gizli sohbetler" için etkinleştirilmektedir (Holroyd, 2021). Signal ise WhatsApp gibi uçtan uca şifreleme yöntemini kullanmanın yanı sıra, mesajları bulut üzerinde yedeklemediği için bulut ortamına ilişkin riskleri (Henkoğlu ve Külcü, 2013, s. 68) ortadan kaldırmaktadır. Bununla beraber mesajın meta verilerini de şifrelediği için, gönderilen ya da alınan mesajın yerinin ve saatinin izlenememesini sağlamaktadır. Gizlilik odaklı olması ve özel bilgileri analiz etme, paylaşma ya da bunlardan kâr etme arzusu olmaması nedeniyle, WhatsApp'a güveni kaybolan ve alternatif uygulama arayışı içinde olan kullanıcıların Signal'e yönelmelerini sağlayacak önemli gerekçelerin olduğu görülmektedir (O'Flaherty, 2021).

Uçtan uca şifreleme yöntemiyle iki kişi arasındaki iletişimin gizliliği sağlarken, bilgi güvenliği kapsamında mesajların gizliliğinin korunması için sadece bu yöntemin kullanılması yeterli değildir. WhatsApp kullanıcı deneyimindeki "önce gizlilik" yerine "önce kullanılabilirlik" paradigmasının, WhatsApp üzerinden veri elde etmeye yönelik güvenlik boşlukları yarattığı görülmektedir (Wijnberg ve Le-Khac, 2021, s. 8). Mesajların gizliliğinin korunması konusunda dikkate alınması gereken ve bilgi güvenliği zincirinin daha zayıf olduğu düşünülen halkası, iletişim için kullanılan cihazlardır (Doffman, 2021b). Mesajların açık olarak bulunduğu telefon vd. cihaz için kullanıcı tarafından tercih edilen koruma yöntemi cihaz üzerinde bulunan mesajların gizliliğinin korunması için sağlanan en üst güvenlik seviyesini belirlemektedir. Vukadinović (2019, s. 37), özellikle uygulamaların web arayüzü aracılığıyla kullanıldığı bilgisayarlar üzerinden gönderilen tüm mesajların, silinen mesajların 2/3'ünün ve gönderilen tüm resimlerin hem Chrome'da hem de Firefox'ta kurtarılabileceğini göstermektedir.

WhatsApp üzerindeki en önemli gizlilik ve güvenlik uygulaması olarak dikkat çeken uçtan uca kriptolama yöntemi, hedeflenen alıcıların dışındaki bazı kurumlara da açık olduğu gerekçesiyle son yıllarda eleştirilerin odağı haline gelmiştir. 2015 yılında FBI tarafından incelenmek istenen bir iPhone cep telefonuna Apple tarafından da erişim sağlanamaması üzerine, Apple'ın iPhone'ların güvenliğini kasıtlı olarak zayıflatmasının ve IOS üzerinde FBI'ın erişimine olanak sağlayacak bir arka kapı oluşturmasının istendiği bilinmektedir (Evans, 2020). Kolluk kuvvetlerine engel oluşturmaması için açık bırakılan arka kapılar, diğer saldırganlar için de kullanışlı hale gelmektedir. 7 Temmuz 2021 tarihli FBI belgelerinde, WhatsApp, Signal, Telegram, Viber ve WeChat'in aralarında bulunduğu en büyük dokuz mesajlaşma uygulamasındaki yazışmaların yasal yollarla takip edildiği açıklanmaktadır. FBI'ın "Yasal Erişim" belgesinde, WhatsApp kullanıcıları ve faaliyetleri hakkında diğer tüm büyük güvenli mesajlaşma araçlarından daha pratik olarak gerçek zamanlı bilgi

sağlanabileceği belirtilmektedir (Kroll, 2021). Amazon'un kurucusu Jeff Bezos'un telefonuna WhatsApp aracılığıyla gönderilen kötü amaçlı bir video mesajıyla erişilmesi (Shires, 2020, s. 27), kolluk kuvvetlerimin erişimine yönelik açıklardan faydalanıldığı düşüncesini oluşturmakta ve dolaylı olarak kullanıcıların WhatsApp tarafından sağlanan gizlilik uygulamalarına şüpheyle yaklaşmasına neden olmaktadır.

Uygulamalar Üzerinden Elde Edilen Bilginin Miktarina İlişkin Riskler ve Öneriler

WhatsApp kullanıcı sözleşmesi kapsamında elde edilen kişisel verilerin kullanımı ve paylaşımına yönelik endişeler diğer sosyal medya riskleri ile karşılaştırılarak değerlendirildiğinde, mevcut diğer riskleri gölgede bırakan bir algının oluştuğu görülmektedir. Dünya genelinde en fazla kullanım oranına sahip sosyal medya platformlarının topladığı ve kullandığı kişisel verilerin analiz edildiği çalışmalar (Atamaniuk, 2021), WhatsApp'ın %11 oranı ile listenin 45. Sırasında yer aldığını göstermektedir. Bununla beraber WhatsApp'ın, listenin ilk 44 sırasında yer alan diğer uygulamalardan farklı olarak herhangi bir kişisel veri elde etmediği görülmektedir. Listenin ilk sıralarında yer alan Facebook ve Instagram gibi uygulamalar, bir kurumun yasal olarak toplayabileceği verilerin %70'ini işleyerek, bu verilerin kullanımına ilişkin çok daha fazla risk barındırmaktadır.

WhatsApp tarafından kullanılan ve transfer edilen bilgiye ilişkin risklerin kapsamlı olarak değerlendirilebilmesi için, hemen hemen tüm kullanıcıların kullanmakta olduğu uygulamalar tarafından elde edilen bilgilerin neler olduğu ve bu bilgilerin nasıl kullanıldığının da incelenmesi önem taşımaktadır. Bunun için dünya genelinde %92 oranında pazar payına sahip olan Google hizmetlerinin ya da ürünlerinin kullanıcılardan elde ettiği bilgileri ve kullanıcı sözleşmelerinde belirtilen kullanım amaçlarını irdelemenin faydalı olacağı düşünülmektedir (Johnson, 2021). Her geçen gün daha kullanılabilir veriler elde etmek amacıyla ortalama 10 yeni arama kuralı değişikliği yapan Google, kullanıcılarını yakından takip eden şirketlerin başında gelmektedir. Örneğin bir kurumda çalışan kullanıcının Google aramalarının analiziyle, kullanıcının işindeki mutluluğuna yönelik veriler elde edilebilmektedir (Sidell, 2021). Google'ın arama sonuçlarına yönelik değişikliklerle pazardaki rekabetin bozulmasına yol açtığı konusunda somut örnekler bulunduğu ve bu nedenle Türkiye'de de Rekabet Kurulu (2020, 2021) tarafından cezalandırılmasına yönelik kararların alındığı bilinmektedir. Google, kullanıcıların bilgi davranışını izlemek için Gmail ve YouTube etkinliği, konum bilgileri, Google aramaları, çevrimiçi satın almalar vb. etkinlik ya da tercih bilgilerini kullanmaktadır. Çevrimiçi etkileşimde bulunulan hemen her şirkette olduğu gibi, Google da kişiselleştirme amaçlı olarak çevrimiçi alışkanlıkları ve tercihleri incelemek için web izleme teknolojisi kullanmaktadır. Üstelik bu amaca yönelik olarak veri elde edebilmesi için, kullanıcıların gönüllü olarak sunmuş oldukları ya da erişime izin vermiş oldukları bilgiler yeterli olmaktadır. Google, konum belirleme için IP adresi izleme yöntemi kullanılmaktadır. Kişiselleştirilmiş içeriği depolama, sunma ve web sitelerinin önceki ziyaretlere ilişkin bilgileri hatırlamasını sağlayabilmek için ise çerezler kullanılmaktadır (Sidell, 2021).

Google da WhatsApp gibi elde ettiği kişisel verileri, daha iyi hizmetler sunmak, iyileştirmeler yapmak ve kullanıcı deneyimini özelleştirmek için kullandığını belirtmektedir (Google, 2021b). Ancak elde edilen verilerin türleri ve büyüklüğü göz önünde alındığında, kullanıcıların çevrimiçi ortamdaki davranışlarını etkileyebilecek düzeyde ve kullanıcıların endişe duydukları birçok uygulamadan daha büyük boyutta veri toplandığı görülmektedir.

Google tarafından bilginin elde edilmesi için kullanılan ve kullanıcı bilgi davranışını etkileyebilecek yöntemler Şekil 2 üzerinde gösterilmiştir.

Hedeflenmiş Reklamcılık	Elde edilen verilerle ayrıntılı reklam profili oluşturularak, kişisel ihtiyaçlara göre hedeflenmiş reklamların sunulması amacıyla kullanılmaktadır. Genellikle kullanıcının bir ürünü aradığı esnada ilgili ya da tamamlayıcı ürünün de reklamının sunulması, hedeflenmiş reklamcılığın sonucudur.
Konum Takibi	Kullanıcının aramalarıyla ilgili kişiselleştirilmiş öneriler sunmak için konum bilgilerinin kullanılmasıdır. Konum takibi, bilgi aramada ilgililiği arttırmak ve bulunulan konuma bağlı daha kullanılabilir sonuçlar üretmek amacıyla kullanılmaktadır.
Kullanılabilirliğin İyileştirilmesi	Milyarlarca kişinin farklı uygulamalardan elde edilen verilerinin analiz edilerek en iyi sonuçların elde edilmesi amacıyla kullanılmaktadır. Örneğin kullanıcının bulunduğu yoldaki trafik yoğunluğu bilgilerinin doğruluğu, bölgede bulunan diğer kullanıcıların sağladığı veri miktarına bağlı olarak artmaktadır.
Arama Algoritmalarında Değişiklikler	Google, daha iyi bilgi erişim etkinliğinin elde edilebilmesi için arama algoritmaları üzerinde sürekli olarak güncelleme ve değişiklikler yapmaktadır. Arama sonucunda elde edilen sonuçların sıralanması bu iyileştirmelere bağlı olarak değişmektedir. Algoritmalar üzerindeki değişiklikler, yine kullanıcıların yapmış olduğu aramalara bağlı olarak sergilediği bilgi davranışı (tercihleri) analiz edilerek yapılmaktadır.
Trend Belirleme ve Analiz	Arama sorguları izlenerek ve analiz edilerek, elde edilen bilgiler son trendlerin gösterildiği Google web sayfasına aktarılmaktadır.

Şekil 2. Kullanıcı Bilgi Davranışını Etkileyen Yöntemler (Sidell, 2021)

Yukarıda belirtilen yöntemler kullanılarak elde edilen ve kullanıcının bilgi davranışına yönelik çıkarım sağlama amacıyla kullanılan kişisel veriler ise şunlardır (Sidell, 2021);

a. Konuşulan dil,
b. Satın alınan ürün ve harcama bilgileri,
c. Google haritalarından yapılan aramalar ve gidilen yerler,
d. Sık kullanılan ve ziyaret edilen mağazalar,
e. Epostalar, ekleri ve bunlara yönelik olarak yapılan tüm işlemler,
f. Tüm arama bilgileri, video izleme bilgileri ve yapılan yorumlara ilişkin bilgiler,
g. Google Drive'a kaydedilen tüm dosya ve belgeler,
h. Takvim üzerinde kayıtlı tüm bilgiler,
i. Kullanılan uygulamalar ve kullanıma yönelik tarih/saat bilgileri

j. Google Asistanına sorulan sorular,
k. Google haberleri üzerinden okunan makaleler,
l. Görüntülenen ve tıklanan tüm reklamlara ilişkin bilgiler.

WhatsApp tarafından elde edilen bilgilerin niteliği ve miktarı diğer sosyal medya platformları ve hemen her kullanıcının kullanmakta olduğu temel uygulamaların elde ettiği bilgilerin niteliği ve miktarıyla kıyaslanarak değerlendirildiğinde, daha fazla risk ve olası tehdit içermediği görülmektedir. Ancak bununla birlikte, aşağıda sıralanan bazı ayarlarda değişiklik yapılması risklerin azaltılması açısından önem taşımaktadır (Doffman, 2021b).

a. WhatsApp üzerinden gelen kötü amaçlı içerikten korunmak için görüntü vd. eklentilerin otomatik kaydetme seçeneği devre dışı bırakılmalıdır.
b. Kullanıcı hesabının hukuka aykırı olarak ele geçirilerek gönderilen yeni mesajların içeriğine erişim sağlanamaması ve kişilere erişilememesi için, uygulama üzerinde bir kişisel kimlik numarası kullanılmalıdır.
c. Google bulut ortamındaki yedeklere ilişkin güvenlik riskleri bu platforma yönelik olarak ayrıca değerlendirilmeli ve kullanım tercihleri yaparken dikkate alınmalıdır.

Değerlendirme ve Sonuç

WhatsApp vb. mesajlaşma uygulamalarının bilgi güvenliğine yönelik önlemleri, kullanıcılar tarafından genel olarak gizlilik ve kişisel verilerin elde edilmesine yönelik amaçlar çerçevesinde değerlendirilmektedir. Kullanıcı sözleşmelerindeki gizlilik vurgusu, kullanıcıları bu sınırlı çerçevede düşünmeye zorlamaktadır. Ancak bu tür uygulamaların kullanıcı verilerini nasıl işlediği, depoladığı ve kimlerle paylaştığına bağlı olarak, risk ve tehditler daha kapsamlı hale gelmektedir. WhatsApp vb. mesajlaşma uygulamaları üzerinden elde edilen bilgiler, bireyleri ve kurumları itibarsızlaştırmaya ya da hukuka aykırı toplumsal hareketleri oluşturmaya yönelik bir araç olarak kullanılma potansiyeli taşımaktadır. HmbBfDI basın bülteninde, WhatsApp'ın uygulamaya koymak istediği sözleşmenin, Almanya'da yapılacak seçimler için somut tehlike içerdiği vurgulanmaktadır. Bu görüş dikkate alındığında, bu sözleşmenin sadece bireysel ve kurumsal riskleri değil, toplumsal güvenlik risklerini de içerdiği düşünülmektedir. Bu yönüyle, mesajlaşma uygulamalarının içerikleri başta ABD olmak üzere birçok ülke için güvenlik sorunu olarak algılanırken, aynı zamanda kontrol edilebildiği ölçüde etkili bir bilgi kaynağı olarak yararlanılmaktadır. Bu tür mesajlaşma uygulamalarının hangi tehditlere neden olacağı, tamamen kullanıcıların bilgi davranışına bağlı olarak şekillenmektedir.

Sanal kimliğin gizliliğinin korunmasında, ilgili sosyal ağ hizmet sağlayıcılarının veri toplama, saklama, işleme, transfer etme ve imha etme politikalarının her aşaması önemli bir rol oynamaktadır. Bu amaçla hazırlanan veri koruma ilkeleri, kullanıcıların hangi platformları kullanacağına ilişkin tercihleri üzerinde de etkili olabilmektedir. Ancak bununla beraber, benimsenen ilkelerin uygulanması ve taahhütlerin yerine getirilebilmesi için yeterli düzeyde teknik güvenlik önleminin alınması da gerekmektedir. Veri iletişim altyapısının kullanıldığı sosyal platformlar üzerinde verilerin korunması söz konusu olduğunda, siber güvenlik risk ve önlemleri de göz ardı edilmemelidir. Bu kapsamda siber güvenlik zafiyetlerinin en önemli nedenlerinden biri olan insan faktörü göz önüne alınarak, mesajlaşma uygulamalarının kişisel ve kurumsal kullanımına yönelik bilgi güvenliği farkındalığının oluşturulması önem taşımaktadır (Kaur ve diğerleri, 2015, s. 23).

Ücretsiz olarak sunulan sosyal ağ hizmetlerinin bedeli kişisel veriler üzerinden ödenmektedir. Kullanıcıların özellikle hedeflenen reklamcılık ve sanal kimlik üzerinden para kazanılması konusundaki farkındalığının arttırılabilmesi için, KVK Kurulu gibi veri otoriteleri tarafından hazırlanan kullanıcılara yönelik uyarı ve bilgilendirme metinlerinin, kamu spotlarının yanı sıra internet kullanıcılarının yoğun olarak bulunduğu bilgi paylaşım platformları üzerinden görünürlüğü arttırılmalıdır. Avrupa Komisyonu (2019) tarafından hazırlanan bilgilendirme metinlerinde olduğu gibi, kişisel verilerin toplanmasının ve üçüncü şahıslarla paylaşılmasının bazı sosyal medya platformları, e-posta sağlayıcıları, arama motorları ve yazılım sağlayıcıların iş modellerinin büyük bileşenini oluşturduğuna ve topladıkları verilerin onlarla aktif olarak paylaşılanların ötesine geçebileceğine dikkat çekilmelidir. Bununla beraber, e-posta, takvim, aramalar, konum bilgileri, mesajlar ve üyesi olunan grupların takip edilerek, ilgi alanı ve tercihlere göre sanal kimlik haritasının çıkarılabileceği konusunda kullanıcılar uyarılmalıdır. Kullanıcıların WhatsApp tarafından elde edilen ve paylaşılan bilgilerin risklerine odaklanırken, topladığı bilgilerle kullanıcı bilgi davranışına yönelik daha fazla çıkarım sağlayabilen diğer sosyal ağ uygulamalarının risklerini göz ardı etmemeleri önem taşımaktadır.

Hukuksal olarak başvuruların yapılabilmesi ve yanlış uygulamaların durdurulabilmesi açısından merkezi Türkiye'de olan ya da Türkiye'de temsilcisi bulunan hizmet sağlayıcıların tercih edilmesi önem taşımaktadır. Bununla beraber, kullanımı tercih edilen uygulamaların merkezinin bulunduğu ülke ile Türkiye arasındaki uluslararası sözleşme ve iş birliği koşullarına dikkat edilmelidir. Bu konuda AB ve ABD kaynaklı bir hizmet sağlayıcısına karşı en azından kişisel hakların savunulmasına yönelik bir hukuksal zemin bulunmasına karşın, Çin merkezli bir hizmet sağlayıcısına karşı bu tür seçeneklerin bulunmadığı açıktır. Örneğin, kullanıcılardan gelen tepkilerin veri koruma otoriteleri tarafından da incelenmeye alınması sonucunda, WhatsApp'ın mevcut kullanıcılarını kaybetmeyi göze alamadığı ve 15 Mayıs 2021 tarihinden itibaren geçerli olduğunu belirttiği sözleşmeyle geri adım atarak veri paylaşma isteğini rafa kaldırdığı görülmektedir. Bu sonuç, kullanıcı farkındalığının artması ve gösterilen tepkilerin veri koruma otoritelerince desteklenmesi halinde, sözleşme şartlarını kabul etmek zorunda kalan kullanıcıların kişisel hak ve özgürlüğünün ilgili platformlar karşısında korunabileceğini göstermektedir. Başka bir ifadeyle veri korumaya ilişkin kullanıcı farkındalığının artması, kullanıcıların bu platformlardaki gizlilik ilkeleri ve stratejisi üzerinde daha fazla söz sahibi olmasını sağlanabilmektedir.

Kullanıcılar diğer platformlara yönelirken, hassasiyet gösterilen sözleşme maddelerinin diğer platformlarda da olup olmadığına dikkat etmelidir. Kullanıcı sözleşmelerinde bilgi güvenliğinin ve kesintisizliğin sağlanmasına yönelik taahhütlerin bulunmaması, bilgilerin saklandığı/depolandığı ortamlardaki kişisel verilerin teknik yöntemlerle korunamaması ve hukuka aykırı erişimlerle başkaları tarafından erişilebilmesi halinde, bireylere ya da kurumlara yönelik mağduriyetin oluşması mümkündür. Bu nedenle, bilgi güvenliğine yönelik önlemler, bunun için ayrılan bütçe ve alınan önlemlere dayanarak taahhüt edilen koruma düzeyi dikkate alınmalıdır. WhatsApp yerine kullanılması düşünülen alternatif mesajlaşma uygulamalarında bilgi güvenliği açısından göz önünde bulundurulması gereken üç önemli husus bulunmaktadır. Bunlar, uçtan uca veri kriptolama, servis sağlayıcı tarafından saklanan veriler ve bu verilerin paylaşımı konularıdır. Uçtan uca kriptolama ile kullanıcıların haberleşme gizliliği sağlanırken, servis sağlayıcılarda saklanan verilerin de kriptolu olarak saklanması önem taşımaktadır. Servis sağlayıcıların sunucuları ya da bulut hizmet sağlayıcılarda herhangi bir verinin tutulmaması ise bu konuda daha az risk alınarak daha üst

seviyede güvenlik önleminin sağlandığı anlamına gelmektedir. WhatsApp'ın en fazla eleştirildiği konular, saklanan verilerin kriptosuz olarak tutulması ve bu verilerin üçüncü taraflarla paylaşılmasıdır. Bununla beraber, 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi ve CBDDO'nun Bilgi ve İletişim Güvenliği Rehberinde özellikle kurumlar için vurgulandığı gibi, sunucuları yurt dışında bulunan mesajlaşma uygulamalarının yerine, sunucuları yurt içinde bulunan mesajlaşma uygulamalarının kullanılması tercih edilmelidir.

En fazla kullanıcı bilgisi toplayan sosyal medya devi Facebook tarafından satın alınmış olması, WhatsApp'ı veri paylaşımı konusunda zorlamaktadır (Doffman, 2021a). Kişisel verilerin işlenmesine yönelik olarak Facebook'un geçmiş yıllarda ortaya çıkan skandalları, WhatsApp kullanıcı bilgilerinin Facebook ile paylaşılmak istenmesine yönelik endişeleri arttırmaktadır. WhatsApp'ın Facebook ile bilgi paylaşımı kararına bağlı olarak, milyonlarca kullanıcının zaman kaybetmeksizin tepki verdiği ve alternatif uygulamaları kullanmaya başladıkları görülmektedir. Alternatif uygulamaların gizliliğe daha duyarlı olduğu algısının oluştuğu 2020 yılından itibaren, bu uygulamaların kullanıcı sayıları yaklaşık %30 artmıştır (Holroyd, 2021). Bununla birlikte, alternatif uygulamaların kullanım oranındaki artışa bağlı olarak (Ulukan, 2021), kullanıcıların WhatsApp uygulamasını tamamen terk ettiğini ya da kullanıcı sayısında aynı oranda azalma olduğunu söylemek mümkün değildir. Kullanıcıların içinde oldukları grupları topyekûn farklı uygulamalara taşıyamamaları nedeniyle tamamen WhatsApp'ı kullanmayı bırakamadığı ve öncelikli olarak tercih edebilecekleri farklı mesajlaşma platformlarına yöneldikleri görülmektedir. Tepki göstererek alternatif platformlara yönelen kullanıcıların bu platformlara ilişkin bilgi güvenliği koşullarını da dikkate almaları önem taşımaktadır. Zira bir mesajlaşma platformunun kullanıcı bilgilerini farklı sosyal medya uygulamalarıyla paylaşımı, kişisel verilerin korunması açısından güvenli ya da güvensiz olduğuna ilişkin tek değerlendirme kriteri olarak görülmemektedir. Bilgi güvenliğine ilişkin olarak, hangi bilgilerin elde edildiği, bilginin nerede depolandığı, kimlerin erişim sağlayabildiği ve uçtan uca iletişim güvenliğinin de bu kapsamda dikkate alınması önem taşımaktadır.

WhatsApp tarafından otomatik olarak elde edilen IP adresi gibi kişisel verilerin her ne amaçla olursa olsun kullanıcının açık onayı alınmaksızın işlenmesinin KVKK'ya aykırı olduğu değerlendirilmektedir. Bununla beraber, konum bilgilerinin elde edilmesine ve kullanılmasına kullanıcı tarafından izin verilmemesine karşın, IP adresi üzerinden genel konum bilgilerine ulaşılarak belirli amaçlar için kullanılmasının da kullanıcının bilgi ve onayının dışında gerçekleşen bir işlem olduğu düşünülmektedir. Kullanıcılar, verilerin nasıl toplandığı, işlendiği ve kimlerle paylaşıldığı konusunda açık olarak bilgilendirilmeli ve verileri üzerinde kontrol sahibi olmaları sağlanmalıdır.

Kaynakça

2019/12 *Sayılı Genelge. (2019). Bilgi ve iletişim güvenliği tedbirleri.* Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2019/07/20190706-10.pdf

Akıncı, A. N. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi*. K. Bakanlığı. Erişim adresi: http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf

Avrupa Komisyonu. (2019). *Take control of your virtual identity*. Erişim adresi: https://ec.europa.eu/info/sites/default/files/virtual_idenitity_en.pdf

Avrupa Komisyonu. (2021). *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection*. Erişim adresi: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions

CBDDO. (2020). *Bilgi ve iletişim güvenliği rehberi.* Erişim adresi: https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf

Clarke, D. ve Ali, S. T. (2017). End to End Security is Not Enough. F. Stajano, J. Anderson, B. Christianson ve V. Matyáš (Ed.), *Security Protocols 2017. Lecture Notes in Computer Science* (s. 260-267) içinde. Springer. https://doi.org/10.1007/978-3-319-71075-4_29

Doffman, Z. (2021b). *Yes, you can still use WhatsApp - But change these 3 critical settings first*. Erişim adresi: https://t.ly/gRmv

Doffman, Z. (2021a). *Why You Should Quit WhatsApp As Critical New Update Confirmed*. Erişim adresi: https://t.ly/mPOA

Durgin, M. (2007). *Understanding the importance of and implementing internal security measures*. SANS Institute. Erişim adresi: https://t.ly/mlt7

Elciyar, K. ve Küçük, M. (2020). Sosyal ağ kullanımı: Sosyal kazanımlar, kendini gerçekleştirme ve aidiyet. *Akdeniz İletişim Dergisi*(33), 198-210. https://doi.org/10.31123/akil.617079

Evans, D. (2020). *Why the US government is questioning WhatsApp's encryption*. Erişim adresi: https://t.ly/047W

Filerskeepers. (2021). *Solving records retention once and for all: Confidently decide how long you keep your data with our records retention schedules*. Erişim adresi: https://t.ly/oH53

Google. (2021a). *Gizlilik ve güvenlik ilkelerimiz.* Erişim adresi: https://safety.google/intl/tr/principles/

Google. (2021b). *Gizlilik ve şartlar*. Erişim adresi: https://policies.google.com/privacy?hl=tr

Henkoğlu, T. (2015). *Bilgi güvenliği ve kişisel verilerin korunması*. Yetkin Hukuk Yayınları.

Henkoğlu, T. (2017). Hukuksal zorunluluklara bağlı olarak veri korumaya bakış açısındaki değişim. F. Özdemirci ve Z. Akdoğan (Ed.), *Bilgi sistemleri ve bilişim yönetimi: Beklentiler ve yeni yaklaşımlar* (s. 153-173) içinde. Ankara Üniversitesi Basımevi

Henkoğlu, T. (2018). Sanal duvarın arka yüzü: Merkezi veri depolama ortamları ve iletişim teknolojilerinin bilgiye tehdidi. T. Çakmak ve B. Yılmaz (Ed.), *Gerçek ötesi ve bilgi yönetimi* (s. 22-33) içinde. Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü.

Henkoğlu, T. ve Külcü, Ö. (2013). Bilgi erişim platformu olarak bulut bilişim: Riskler ve hukuksal koşullar üzerine bir inceleme *Bilgi Dünyası, 14*(1), 62-86. https://doi.org/10.15612/BD.2013.135

Hinds, J., J.Williams, E. ve N.Joinsona, A. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies, 143*(2020). https://doi.org/10.1016/j.ijhcs.2020.102498

Holroyd, M. (2021). *Turkey investigates WhatsApp and Facebook over data privacy update*. Erişim adresi: https://www.euronews.com/2021/01/11/turkey-investigates-whatsapp-and-facebook-over-data-privacy-update

Johnson, J. (2021). *Global market share of search engines 2010-2021.* Erişim adresi: https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/

Kaptan, S. (1995). *Bilimsel araştırma ve istatistik teknikleri* (10 bs.). Rehber Yayınevi.

Kaur, S., Sharma, S. ve Singh, A. (2015). Cyber security: Attacks, implications and legitimations across the globe. *International Journal of Computer Applications, 114*(6), 21-23. Erişim adresi: https://research.ijcaonline.org/volume114/number6/pxc3901932.pdf

Kroll, A. (2021). *FBI Document Says the Feds Can Get Your WhatsApp Data - in Real Time*. Erişim adresi: https://t.ly/2jN5

KVK Kurulu. (2017). Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi hakkında yönetmelik. Erişim adresi: https://t.ly/Mh9f

KVK Kurulu. (2018). *Kişisel verilerin yurtdışına aktarılması*. Erişim adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/ca163cb6-39ad-4024-870a-8a9508c92387.pdf

KVK Kurumu. (2020). *Açık rıza alırken dikkat edilecek hususlar*. Erişim adresi: https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar

KVKK. (2016). *Kişisel Verilerin Korunması Kanunu*. Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

Kwayu, S., Abubakre, M. ve Lal, B. (2021). The influence of informal social media practices on knowledge sharing and work processes within organizations. *International Journal of Information Management, 58*(2021). https://doi.org/10.1016/j.ijinfomgt.2020.102280

Microsoft. (2021). *Microsoft Gizlilik Bildirimi*. Erişim adresi: https://privacy.microsoft.com/tr-tr/privacystatement

Morey, T., Forbath, T. ve Schoop, A. (2015). *Customer Data: Designing for Transparency and Trust*. Harvard Business Review. Erişim adresi: https://t.ly/nqJ4

O'Flaherty, K. (2021). *Is it time to leave WhatsApp – and is Signal the answer?* Erişim adresi: https://t.ly/qbbv

OECD. (2013). Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. Erişim adresi: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Peltier, T. R. ve Peltier, J. (2007). *Complete guide to CISM certification*. Auerbach Publications.

Rekabet Kurulu. (2020). *Google Reklamcılık ve Pazarlama Ltd. Şti., Google International LLC, Google LLC, Google Ireland Limited ve Alphabet Inc. hakkında yürütülen soruşturmaya ilişkin nihai kararın 4054 sayılı Rekabetin Korunması Hakkında Kanun'un 49. maddesi uyarınca açıklanması*. Erişim adresi: https://www.rekabet.gov.tr/Dosya/nihai-karar-aciklamalari-tefhim-duyurulari/google-adwords-nihai-karar-20201113173238734-pdf

Rekabet Kurulu. (2021). *Google Reklamcılık ve Pazarlama Ltd. Şti., Google International LLC, Google LLC, Google Ireland Limited ve Alphabet Inc. hakkında yürütülen soruşturmaya ilişkin nihai*

kararın 4054 Sayılı Rekabetin Korunması Hakkında Kanun'un 49. Maddesi uyarınca açıklanması. Erişim adresi: https://t.ly/uYvQ

Rekabet Kurumu. (2021). *Facebook- WhatsApp Soruşturması Hakkında Basın Duyurusu*. Erişim adresi: https://www.rekabet.gov.tr/tr/Guncel/facebook-whatsapp-sorusturmasi-hakkinda--7f1270260cbaeb11812e00505694b4c6

Rollason, H. (2021). *What Countries are the Biggest WhatsApp Users?* Erişim adresi: https://www.conversocial.com/blog/what-countries-are-the-biggest-whatsapp-users

Satariano, A. (2019). *Google is fined $57 million under Europe's Data Privacy Law*. Erişim adresi: https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html

Schemm, M. (2021). *Order of the HmbBfDI: Ban of further processing of WhatsApp user data by Facebook*. Erişim adresi: https://t.ly/hnxC

Shires, J. (2020). The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and U.S. Politics. *Texas National Security Review, 3*(4). Erişim adresi: https://t.ly/UcOQ

Sidell, E. P. (2021). *What does Google do with your data?* Erişim adresi: https://t.ly/44zB

Slynchuk, A. (2021). *Which companies might access our personal data the most?* Erişim adresi: https://clario.co/blog/which-company-uses-most-data/

Statista. (2021). *Most popular social networks worldwide as of January 2021, ranked by number of active users*. Erişim adresi: https://t.ly/1LYT

Stepanova, O. ve Feldmann, J. (2020). *The Privacy, Data Protection and Cybersecurity Law Review: Germany*. Erişim adresi: https://t.ly/cEAF

Şengöz, A. ve Eroğlu, E. (2017). Örgütlerde sosyal medya kullanımı: sosyal medya algıları, amaçları ve kullanım alışkanlıkları. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi, 5*(1), 503-524. https://doi.org/10.19145/gumuscomm.288789

TCK. (2004). *Türk Ceza Kanunu*. Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf

Ulukan, G. (2021). *11 günde WhatsApp, Telegram ve BiP'in kullanıcı sayılarının değişimi*. Erişim adresi: https://t.ly/tMKl

Vukadinović, N. V. (2019). *Whatsapp forensics: Locating artifcats in web and desktop clients* Purdue University]. West Lafayette, Indiana. Erişim adresi: http://pstorage-purdue-258596361474.s3.amazonaws.com/14954516/NVillacisVukadinovicWhatsAppThesis.pdf

Wattal, S., Telang, R. ve Mukhopadhyay, T. (2009). Information personalization in a two-dimensional product differentiation model. *Journal of Management Information Systems, 26*(2), 69-95. https://doi.org/10.2753/MIS0742-1222260204

WhatsApp LLC. (2021a). *WhatsApp Privacy Policy*. Erişim adresi: https://t.ly/TRLp

WhatsApp LLC. (2021b). *WhatsApp Terms of Service*. Erişim adresi: https://t.ly/6Bzz

WhatsApp LLC. (2021). *Answering your questions about WhatsApp's Privacy PolicyAnswering your questions about WhatsApp's Privacy Policy*. Erişim adresi: https://t.ly/WI1F

Wijnberg, D. ve Le-Khac, N.-A. (2021). Identifying interception possibilities for WhatsApp communication. *Forensic Science International: Digital Investigation, 38*. https://doi.org/10.1016/j.fsidi.2021.301132

Winter, K. A. (1997). Privacy and the rights and responsibilities of librarians. http://www.cstone.net/~kwinter/articles/ksr4_winter.pdf

Yahoo. (2021). *Yahoo Gizlilik Merkezi*. Erişim adresi: https://t.ly/mGcw

Yandex. (2021). *Gizlilik politikası*. Erişim adresi: https://yandex.com.tr/legal/confidential/

Yargıtay. (2014). *Yargıtay kararı (Esas No: 2014 / 7409, Karar No: 2014 / 24197)*. http://kazanci.com.tr/gunluk/12cd-2014-7409.htm

Zialcita, P. (2019). *Facebook pays $643,000 fine for role in Cambridge Analytica scandal*. Erişim adresi: https://t.ly/q4QB