

WHATSAPP GÜVENLİK DEĞİŞİKLİĞİ NE ANLAMA GELİYOR? VERİLERİMİZ PAYLAŞILACAK MI?

Murat Volkan Dülger*

Giriş

4 Ocak 2021 sabahı uyanıp cep telefonlarımızı elimize aldığımızda “WhatsApp” tarafından telefonlarımızda sözleşme değişikliğine gidileceğine ilişkin bir uyarı ile karşılaştık. Sözleşmedeki “Gizlilik İlkesi” gereğince onay vermemiz halinde verilerimizin Facebook ve bağlı şirketleri ile paylaşılacağı, onay vermememiz halinde ise bu uygulamayı belirtilen tarihten sonra kullanamayacağımızı öğrendik. Ülkesinin ordusunun kozmik odasına girilmesiyle bu kadar ilgilenmeyen ve tedirgin olmayan insanlarımız, ne kadar derin sırlar saklıyorlarsa bu değişiklikten çok tedirgin oldular ve her yerde bu konuyu konuşmaya başladılar. Sonuçta WhatsApp’ın veri paylaşma ilişkin sözleşme değişikliği bir anda ülkemizin gündeminin baş köşesine oturdu.

WhatsApp’ın yapmaya çalıştığı (ya da daha doğru bir deyişle dayattığı) sözleşme değişikliği nedeniyle haklı olarak korkuya kapılan ve çeken pek çok kullanıcı bir anda Telegram, Signal veya BİP gibi mesajlaşma platformlarına geçiş yapmaya başladı. Tabi bir yandan hepimizin aklında ardı arkası kesilmeyen sorular oluştu; zira bu süreçte WhatsApp uygulaması iş yaşamımızdan özel yaşamımıza kadar hayatımızın her alanına çoktan girmişti. Bu değişiklik öylesine önemsendi ki ülkemizde, Twitter üzerinden “*WhatsApp Siliyoruz*” hashtagi ile uygulamaya karşı boykotlar ve toplu eleştiriler başladı.

Aslında bu bir bakımdan oldukça iyi bir gelişme oldu. Böylelikle toplumun büyük bir çoğunluğu son derece önemli olan kişisel veri güvenliği konusunda farkındalık edindi, hatta aydınlanma yaşadı. Bunu da bu sürecin önemli bir yanı ve kazanımı olarak dikkate almalıyız.

İşte bu yazımda kullanıcıların verilerin paylaşılması noktasında bu derece radikal bir farkındalık yaşamasına neden olan mobil uygulamaları, bunların kişisel verilerin güvenliğe yaklaşımlarını ve konunun hukuki boyutunu değerlendirmeye çalışacağım.

* Doç. Dr., İstanbul Aydın Üniversitesi Hukuk Fakültesi Ceza Hukuku, Ceza Muhakemesi Hukuku ve Bilişim Hukuku öğretim üyesi / Avukat, volkan.dulger@dulger.av.tr, ORCID: 0000-0003-4034-5436.

I. WhatsApp'ın Gelişme Süreci ve Bugünü

Öncelikle tartışılan sözleşme değişikliğiyle ne olacağını bir cümleyle ortaya koyalım: WhatsApp tarafından 8 Şubat 2021 tarihinde yürürlüğe konulacak “Gizlilik İlkelerine” göre kullanıcılar tarafından onay verilmesi halinde kullanıcıların “bazı” verileri Facebook ve Facebook bünyesinde bulunan diğer şirketler ile paylaşılacak. Bu ilkelere onay vermeyen kullanıcılar ise 8 Şubat 2021 tarihi itibarıyla WhatsApp uygulamasını kullanamayacaklar.

WhatsApp, akıllı telefonlar için geliştirilen ve platformlar arası çalışma özelliğine sahip anlık mesajlaşma, arama ve haberleşme hizmeti sunan; bugün itibarıyla aylık iki milyar kullanıcısı olan dünyanın en yaygın mesajlaşma uygulamasıdır. 2009 yılında Kaliforniya’da kurulan “WhatsApp”, kurulduğu günden itibaren hem uygulamayı hem de gizlilik politikalarını geliştirdi. WhatsApp uygulamasına 2010 yılında ilk olarak grup sohbeti özellikleri eklendi. Böylece kullanıcıların ikili iletişimlerinin yanı sıra iki veya daha fazla kişiden oluşan sohbet odaları oluşturmalarına imkân sağlanmış oldu. WhatsApp, 2012 yılının Ağustos ayında getirdiği güncelleme ile kullanıcılar tarafından yapılacak olan görüşmelerin IOS ve Android işletim sistemleri üzerinden şifreleneceğini duyurdu. 2013 Ağustos ayında WhatsApp sesli mesajlaşmayı tanıttı. 19 Kasım 2014 tarihinde ise WhatsApp uygulamasının Facebook Inc. şirketine satılması ile bu uygulama için yeni bir dönem başlamış oldu.

Aynı yıl Kasım ayında WhatsApp, mesajları alıcılar tarafından okunduğunda gönderenleri uyaran, “okundu bilgisi” şeklinde anılan ve “iki mavi tik” şeklinde görünen özelliğini sundu. Bir hafta içinde WhatsApp, kullanıcıların bu özelliği devre dışı bırakmasına olanak tanıyan ek bir güncellemeyi daha uygulamaya ekledi. Mart 2015’te iki hesap arasında sesli arama yapma özelliği eklendi. 24 Şubat 2017 tarihinde WhatsApp daha büyük bir yenilik yaptı: Snapchat isimli uygulama ile kullanmaya alıştığımız “Hikayeler” (Story) özelliğini kullanıma sundu. Bu özellik ile WhatsApp kullanıcılarına filtre ve eklemeler kullanarak 24 saatlik zaman dilimi için görüntülenebilen resim, video, müzik, link ve yazı paylaşımları yapma imkânı tanındı. Ekim 2017’de konum paylaşma özelliği eklendi. Ocak 2018’de ise WhatsApp, küçük işletmelerde kullanım için WhatsApp Business’ı başlattı.

8 Şubat 2021 tarihinde yürürlüğe girecek WhatsApp Gizlilik İlkeleri ile ilgili yapılan açıklamalarda güdülen amaç “İşletmelerin WhatsApp Business üzerinden müşterileriyle iletişime geçmeleri sırasında şeffaflığın sağlanması ve WhatsApp’ın ana şirketi olan Facebook üzerinden güvenli hosting hizmeti almalarına olanak vermek.” şeklinde belirtildi. Yapılacak bu gizlilik güncellemelerinin işletmelerin müşterileriyle olan iletişimlerinde daha fazla güvenilirlik ve şeffaflık sağlanması amacıyla yapıldığı söylene de bunlar, WhatsApp Business kullanmayan kullanıcılar açısından verilerinin Facebook’a aktarımı konusunda endişeler yarattı.

II. Gizlilik Politikası ve Sorunlar

Aslında WhatsApp uygulamasının 2014 yılında Facebook Inc. şirketine satılması sırasında, arka planda pek çok değişiklik gerçekleşti. Şirket tarafından, Facebook’a yapılan satışın ardından yapılan ilk açıklamalarda verilerin gizliliği ve paylaşımı hakkında var olan güvencenin sürdürüleceğine dair açıklamalar yapıldı: *“Gelecekteki ortaklığımızın WhatsApp kullanıcılarının verileri ve gizliliği için ne anlama geleceği hakkında dolaşan birçok yanlış ve dikkatsiz bilgi de var. Gizliliğinize saygı platformumuzda çok önemlidir. WhatsApp’ı sizin hakkınızda olabildiğince az bilgi edinme hedefi etrafında kurduk. Facebook ile ortaklık, değerlerimizi değiştirmek zorunda olduğumuz anlamına gelse, bunu yapmazdık. Bunun yerine, bağımsız ve özerk bir şekilde faaliyete devam etmemize izin verecek bir ortaklık kuruyoruz. Temel değerlerimiz ve inançlarımız değişmeyecek. Temel ilkelerimiz değişmeyecek.”*

Ancak bu açıklamaların aksine 2016 yılında Facebook Inc. ile kullanıcıların kişisel verileri paylaşılmaya başlandı. Facebook ile kullanıcıların kişisel verilerinin paylaşılması sayesinde WhatsApp ile Facebook arasındaki entegrasyonun sağlanması hedeflendi. Bu entegrasyonlar ile kullanıcıların telefon rehberinde bulunan kişilerin WhatsApp kullanıp kullanmadığına ilişkin verilerin işleneceği belirtildi. WhatsApp tarafından 4 Ocak 2021’de yayınlanan ve 8 Şubat 2021’de yürürlüğe girecek olan “Gizlilik Politikası” gereğince ise kullanıcılarının bazı verilerinin Facebook Inc. ile paylaşılmaya başlanacağı ve buna onay vermeyen kullanıcıların WhatsApp uygulamasını kullanmaya devam edemeyecekleri belirtildi.

WhatsApp’da gerçekleşecek bu yeni gizlilik dönemi ile kullanıcılar arasında oluşan kaos ortamı nedeniyle Telegram, Signal hatta Türk yazılımı olan BİP uygulamalarının hızla indirilmeye ve kullanılmaya başladığını gözlemlemekteyiz. Bu noktada WhatsApp uygulaması aktif olarak ayda iki milyardan fazla kişi tarafından kullanırken, Telegram uygulaması 400 milyon ve Signal ise 10-20 milyon kişi tarafından aktif olarak kullanılmaktadır. Kullanıcılar açısından verilerin paylaşılması ve gizlilik yönünden endişelerin artmasıyla bu uygulamaların detaylıca incelenmesi gerekir. Zira bu hızlı geçiş esnasında, diğer uygulamaların güvenlik ve mahremiyet adına neler sundukları tam olarak incelenmemektedir. Dolayısıyla yağmurdan kaçarken doluya tutulmamak için diğer uygulamaların profesyonel düzeyde titizlikle incelenmesi ve mantıklı bir teknik karşılaştırma yapıldıktan sonra karar verilmesi gerekir.

III. Güvenlik ve WhatsApp

WhatsApp, kullanıcılarına sunulan “Gizlilik İlkeleri” uyarınca, uygulama kapsamındaki iletişim içeriklerinde uçtan uca şifreleme yöntemini kullandığını belirtmektedir. Alıcı ve mesajı gönderdiği kişi arasında gerçekleşen mesajlaşmalar, video

görüşmeleri, sesli aramalar, gönderilen görseller vb. uygulama aracılığıyla paylaşılan tüm içerik WhatsApp tarafından şifrelenmektedir. “Uçtan uca şifreleme” (End to End Encryption / E2E) sayesinde mesaj göndericisi ve alıcısı arasındaki mesajları yalnızca iletişimin tarafları görebilmektedir. Şifreleme, her çeşit elektronik verinin (dosya, şifre, imaj) okunamaz bir biçime dönüştürülerek, sadece gerekli koda (şifre anahtarı) sahip olanlarca okunması için geliştirilmiş bir yöntemdir. WhatsApp, uçtan uca şifreleme için “Open Whisper Systems” tarafından geliştirilen “E2E” protokolünü kullanmaktadır.

Belirtmek gerekir ki ülkemizde WhatsApp’ın 8 Şubat tarihinde yürürlüğe girecek olan şartlarını kabul etmeyip günlük iletişimi için Signal uygulamasına geçiş yapan pek çok kullanıcı olmasına rağmen WhatsApp ve Signal uygulamalarında “uçtan uca şifreleme” için aynı protokolün kullanıldığı yaygın şekilde bilinmemektedir.

WhatsApp, kullanıcılar arasındaki haberleşme için E2E şifrelemesini kullansa da Gizlilik İlkelerinde belirtilen yedekleme esasları uyarınca bünyesinde bulunan yedeklemeleri şifrelememektedir. Benzer şekilde alıcı ve gönderici arasında iletişimin taşınmasını sağlayan meta dataları da şifrelememektedir. Meta data (üst veri), kaynak veya verilerin öğelerini belirten bilgiler olarak tanımlanabilir. Meta data ile üçüncü kişilerin mesajların içeriğini görmesine engel olunurken, yetkili kişiler tarafından mesajların kim tarafından, kime, ne zaman ve ne kadar süre ile gönderildiği vb. verilere erişilmesine imkân sağlanır. Uygulamanın güvenlik açısından en problemli noktası meta datalar üzerinde şifreleme bulunmamasıdır. Şifrelenmeyen meta data aracılığıyla erişilen veriler sayesinde, kullanıcıların davranışsal hareketlerinin Facebook tarafından takip edebilmesine olanak sağlanmaktadır. Bu da iyi bir sosyal mühendislik çalışmasıyla aslında belli bir kişi hakkındaki birçok bilginin elde edilebilmesi anlamına gelmektedir. Nitekim NSA gibi istihbarat servislerinin de yaptığı budur. Üzülerek belirtmeliyiz ki kullanıcıların ezici çoğunluğunun gözden kaçırdığı nokta da meta datalardır.

IV. Güvenlik ve Signal

WhatsApp’ın kullandığı uçtan uca şifreleme protokolü aslında Open Whisper Systems tarafından 2013 yılında Signal uygulaması için geliştirilmiş olup; sesli aramalar, anlık mesajlaşmalar ve video konuşmalar için uçtan-uca şifreleme sağlamak üzere kullanılabilen bir şifreleme protokolü olarak tanımlanabilir.

Signal, mesajların ve aramaların şifrelenmesinin yanı sıra meta dataları da şifrelemektedir. Bu, uygulamanın geliştirilmesi ve kullanılması açısından diğer haberleşme uygulamalarına göre daha güvenli bir haberleşme deneyimi sunduğunun göstergesidir.

Signal uygulaması kapsamında yapılan mesajlaşmaları daha güvenli hale getirmek için geliştirilen “Sealed Sender” mekanizması ile gönderici ve alıcı arasında gerçekleştirilen

mesajlaşmanın kimler arasında gerçekleştiğinin anlaşılması mümkün değildir. Sealed Sender mekanizması ile göndericilerin doğrulama yeteneğini ortadan kaldırdığından, kullanıcılar tarafından gönderilen mesajların kim tarafından gönderildiğinin anlaşılması mümkün olamamaktadır. Bunun yanı sıra uygulama kullanıcılara sunduğu gizlilik özellikleri ile mesajları biyometrik veriler veya şifreler ile kitleme imkânı sağlamaktadır.

V. Güvenlik ve Telegram

WhatsApp ve Signal uygulamaları ile karşılaştırıldığı zaman Telegram kullanıcılara mesajları ve diğer verileri şifreleme konusunda uçtan uça şifreleme imkanını sadece “gizli sohbetler” ile sağlamaktadır. Gizli sohbetlerin uygulanması ise pratikte pek mümkün değildir. Uçtan uça şifrelenmeyen normal sohbetlerden gönderilen mesajların kullanıcının cihazında şifrelenmesi ve şifreli mesajların daha sonra Telegram sunucularında çözülmesi anlaşılmalıdır. Bu noktada uygulamanın mesajlarınıza erişmesi mümkün olmakla beraber Telegram Gizlilik Politikasında *“mesajları saklama ve şifre çözme anahtarlarını kullanarak verilere erişmek için ülkelerden gelecek bir mahkeme kararı olması gerektiği”* belirtilmektedir.

Telegram tarafından gizli sohbet mesajlarında uçtan uça şifreleme için Telegram tarafından geliştirilen şifreleme protokolü olan “MT Protokolü” kullanılmaktadır. Kullanıcılar tarafından gerçekleştirilen sesli ve görüntülü aramalar kullanıcıların şifrelemeyi doğrulamaları için aradaki şifreleme anahtarları dört karakterden oluşan emojilerle simgelenmektedir. Öte yandan uygulama üzerinden oluşturulan grup sohbetlerinin şifrelenmesi mümkün olmamaktadır.

Telegram’ın mesajlaşma anlamında kullanıcılara sunduğu imkanlardan biri de “sürekli mesaj / kendi kendini imha eden mesajlar” özelliğidir. Bu sayede alıcı ve gönderici arasında gerçekleştirilen mesajlaşma sırasında istenmeyen mesajların cihazdan silinmesine olanak tanınmaktadır.

VI. Güvenlik ve BİP

Yabancı kaynaklı haberleşme uygulamalarının aksine ülkemizde geliştirilen BİP uygulaması son günlerde bir alternatif olarak gündeme gelmiştir. BİP uygulaması Turkcell tarafından IOS ve Android kullanıcıları için geliştirilen tüm operatörlere ait kullanıcıların ücretsiz olarak kullanabileceği bir uygulamadır. Uygulamada; kaybolan mesaj, caps yaratma, herkesle iletişim kurabilme, grup mesajlaşma ve konum paylaşma, oyunlar, para transferi gibi özellikler bulunmaktadır.

Diğer uygulamalarla karşılaştırıldığında BİP’in uçtan uça şifreleme protokolü kullanmadığı görülmektedir. Bu noktada BİP tarafından paylaşılan “BİP Gizlilik Politikası” incelendiğinde *“Kişisel Veriler Kiminle Paylaşıyor?”* başlığı altında *“Yasal yükümlülükler*

doğrultusunda adli makamlar, düzenleyici kurumlar ve diğer taraflar ile paylaşılmaktadır. BİP 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 paylaşabilir.” ifadesi yer almaktadır.

Bu noktada BİP uçtan uca şifreleme protokolü kullanmadığı için yasal yükümlülüklerin söz konusu olması halinde uygulamayı kullanan kullanıcılara ait mesaj içerikleri kolluk, istihbarat örgütü, savcılık ve mahkemelerle paylaşabilecektir.

VII. WhatsApp Hangi Verileri Neden Topluyor?

Haberleşme platformları tarafından kullanıcılara sunulan “Gizlilik Politikaları” incelendiği zaman, kişilerin verilerinin hangi amaçla ve kimlerle paylaşıldığı görülmektedir. WhatsApp tarafından yapılan Gizlilik İlkeleri’ndeki güncellemeye göre “*Hesap Bilgileri, Bağlantılar, Durum Bilgisi, İşlem ve Ödeme Bilgileri, Mesajlar, Müşteri Desteği ve Diğer İşlemlere*” ilişkin veriler kişilerin paylaşımına onay vermesi halinde toplanacaktır. Eski düzenlemeden farklı olarak yeni Gizlilik İlkeleri’nin içerisinde bu veriler içinden “*Hesap Bilgileri ile İşlem ve Ödeme Bilgileri*” yer almaktadır. WhatsApp tarafından otomatik olarak toplanan bilgiler ise “*Kullanım ve Kayıt Bilgileri, Cihaz ve Bağlantı Bilgileri, Konum Bilgileri ve Çerezler*” olarak belirtilmiştir. Kullanıcılara ait otomatik toplanan verilerin ve kullanıcıların WhatsApp kullanmayı tercih etmeleriyle paylaşmayı kabul ettikleri verileri Facebook ve Facebook Inc. bünyesinde bulunan şirketlerle paylaşılması hususu, 2016 senesindeki kullanımdan farklı olarak kullanıcıların seçimine bırakılmamaktadır.

Gizlilik İlkeleri konusunda bu verilerin ne şekilde kullanılacağı “*hizmetlerimizin ve Facebook Şirket Ürünleri dahil bu şirketlerin sunduğu olanakların yürütülmesi, sunulması, iyileştirilmesi, anlaşılması, özelleştirilmesi, desteklenmesi ve pazarlanması amacıyla bu şirketlerden aldığımız bilgileri kullanabiliriz ve bu şirketler de bizim onlarla paylaştığımız bilgileri kullanabilirler.*” şeklinde açıklanmıştır. Kullanıcılar tarafından sağlanan ve otomatik olarak toplanan verilerin ilkelerde belirtildiği üzere “*Hizmetler, Emniyet, Güvenlik ve Bütünlük ve Kurumsal Etkileşimler*” için kullanılması mevcut Gizlilik İlkeleri açısından da geçerlidir.

WhatsApp tarafından 20 Temmuz 2020 itibariyle güncellenen WhatsApp Gizlilik İlkesi ile 8 Şubat 2021 tarihinde yürürlüğe girecek uygulama arasında Facebook ve Facebook’a bağlı şirketlerle paylaşımın zorunlu olması hususu dışında esasen çok fazla fark bulunmamaktadır.

Halihazırdaki WhatsApp kullanımında da kullanıcılara ait kişisel veriler, gerekli görülmesi halinde yabancı devletler ve güvenlik sebepleriyle istihbari faaliyetler kapsamında paylaşılabilir.

Amerika Birleşik Devletleri (ABD) Kongresi, 23 Mart 2018 tarihinde CLOUD Yasasını (Clarifying Lawful Overseas Use of Data) geçirerek iletişim ve bulut hizmeti sağlayıcılarının sunucularında depolanan verilere yönelik ABD kolluk kuvvetlerinin talepleri için geçerli olan yasal çerçeveyi güncellemiştir. CLOUD Yasası, ABD kolluk kuvvetlerinin ABD ve denizaşırı ülkelerde depolanan verilerle ilgili talepte bulunmasına yönelik sınırlı bir mekanizma sunmaktadır. CLOUD Yasası ABD yasalarında yapılan, ABD kolluk kuvvetlerinin taleplerinin coğrafi kapsamı konusundaki sınırları belirleyen ve hizmet sağlayıcıların başka ülkelerin yasaları veya ulusal çıkarıyla çatışan istekleri reddetmesi için yeni çözüm önerileri sunan bir yasa olarak gündeme gelmiştir. Bu yasa, bulut hizmet sağlayıcılarına başka bir ülkenin yasaları veya ulusal çıkarlarıyla çatışması halinde talebi reddetme imkânı sunmaktadır. CLOUD Yasası uyarınca WhatsApp, hesapları ve hareketleri ile şüpheli davranışlarda bulunan veya WhatsApp koşullarını ihlal eden kullanıcıları incelemek için “Emniyet, Güvenlik ve Bütünlük” ilkesi kapsamında kişisel verileri paylaşabilmektedir. Bu noktada WhatsApp uygulamasının yanı sıra Signal uygulaması da ABD merkezli olması nedeniyle “*Emniyet, Güvenlik ve Bütünlük*” ilkesi kapsamında kullanıcıların verilerini CLOUD Yasası uyarınca ülkelerin mevzuatları aksini emretse dahi ABD ile paylaşabilecektir.

VIII. Verilerin Bulut Ortamında Toplanması

Kullanıcılar tarafından haberleşme uygulamalarını kullanırken dikkat edilmesi gereken noktalar arasında paylaşma ve depolama seçenekleri de yer almaktadır. Bu bağlamda WhatsApp üzerinden kullanıcılar her türlü dosyayı (görüntü, ses, video vb.) paylaşabilmektedir. Ancak kullanıcılar tarafından gönderilen fotoğraflar, sesler ve video dosyaları için sınır 16 MB iken belgeler için bu sınır 100 MB’dir. WhatsApp kullanıcıları dosyalarını Android için Google Drive; IOS için ise iCloud uygulamaları üzerinden saklayabilmektedirler.

WhatsApp Gizlilik İlkelerinin güncellenmiş versiyonunda “*Sizin Sağladığımız Bilgiler – Mesajlar*” başlığında belirtildiği üzere kullanıcılar tarafından gönderilen mesajların olağan iş akışı kapsamında saklanmayacağı belirtilmiştir. Kullanıcıların gönderdikleri ve aldıkları mesajlar kendi cihazlarında saklanmakla beraber mesajlar teslim edildikten sonra WhatsApp sunucuları üzerinden silinmektedir. WhatsApp tarafından oluşturulan senaryolarda hangi durumlar için mesajların saklanmaya devam edeceği belirtilmiştir. Bu haller:

- *Teslim Edilmeyen Mesajlar:* Gönderdiğiniz bir mesaj alıcının çevrimdışı olması gibi bir sebepten ötürü hemen teslim edilemezse mesaj en fazla otuz gün boyunca sunucularda şifrelenmiş şekilde saklanır ve bu süre içinde mesajı teslim etmeye çalışılır ancak otuz günden sonra hâlâ teslim edilmemişse bu mesajı sunucular üzerinden silinmektedir.

- *Medya İletme*: Bir kullanıcı bir mesaj içinde medya ilettiğinde, aynı medyanın tekrar iletildiği durumlarda daha verimli şekilde teslim edilmesini sağlamak için bu medyayı şifrelenmiş şekilde geçici olarak sunucularında saklamaktadırlar.

Ülkemizde yaygın ve hatalı olarak inanılan WhatsApp'ın 8 Şubat 2021 itibariyle kullanıcıların mesajlarının hepsine erişebileceği ve bunları tek tek okuyabileceği bilgisi yukarıda anlatılan gerekçelerle mümkün değildir.

WhatsApp ile diğer haberleşme uygulamaları olan Telegram ve Signal'ın bulut (cloud) üzerinden yaptıkları depolama faaliyetlerini karşılaştırmak gerekirse, Telegram üzerinden kullanıcıların gönderdikleri ve aldıkları tüm mesajlar Telegram'ın kendi bulut sunucularında depolanmakta, Signal uygulamasında ise bulut ortamı bulunmayıp veriler yerel (local) olarak saklanmaktadır.

IX. Avrupa Birliği ve WhatsApp Kullanımı

WhatsApp'ın, 8 Şubat 2021 tarihinde yürürlüğe girecek “Gizlilik İlkeleri” ile uygulamaya koyacağı Facebook ve Facebook bünyesinde bulunan şirketlerle yapılacak veri paylaşımı politikası, GDPR'ın kişisel veri koruma düzenlemelerine tabi olan Avrupa Ekonomik Alanının (EEA) parçası olan Avrupa Birliği ülkeleri için geçerli olmayacaktır.

Bu noktada Avrupa Birliği ile ABD arasındaki veri aktarımı konusunda AB Adalet Divanı (ABAD) tarafından, *Facebook Ireland Limited v. Maximillian Schrems (Dava C-311/18, Schrems II)* davasında 16 Temmuz 2020 tarihli karara değinmek gerekir. ABAD kararında, kişisel verilerin AB – ABD arasındaki aktarımını ve bunun koşullarını incelemiştir. ABAD, Avrupa Komisyonu tarafından kişisel verilerin AB dışında kurulan veri sorumlularına aktarılması için düzenlenen Standart Sözleşme Maddelerinin (*Standard Contractual Clauses, SSC*) geçerli olduğuna karar verirken, AB ile ABD arasındaki Gizlilik Kalkanı'nın (*Privacy Shield*) AB dışı veri aktarımlarında uygulanamayacağına karar vermiştir. ABAD, Schrems II kararında, Standart Sözleşme Maddelerine dayalı olarak AB'den veri aktarılan ve AB üyesi olmayan veri sorumlularının, AB'deki veri aktaranlara Standart Sözleşme Maddelerine uyup uymayacağı konusunda bilgi vermeleri gerektiğini değerlendirmiştir. AB üyesi olmayan veri alıcıları Standart Sözleşme Maddelerine uymaması ve “yeterli düzeyde koruma” sağlayacak ek güvenceler olmaması durumunda AB merkezli veri aktaranı veri sorumlusu bu faaliyeti askıya almak ve / veya sona erdirmek zorundadır.

ABAD kararında ayrıca AB-ABD Gizlilik Kalkanı çerçevesinin geçerliliğini incelemiştir. ABAD, Gizlilik Kalkanı'nın geçersiz olduğuna karar verirken, ABD'ye aktarılan verilerin ABD kamu yetkilileri tarafından erişilmesiyle ilgili olarak; ABD kamu kurumlarınca uygulanan gözetim programlarının ABD vatandaşı olmayan kişiler açısından herhangi bir güvence sağlamadığını, yabancılara ilişkin istihbari faaliyetin de gerçekleştirilebileceğini ve

herhangi bir kısıtlama öngörülmediğini değerlendirerek, AB hukuku uyarınca yeterli korumayı sağlayamayacağına, AB düzeninde öngörülen koruma ile eşdeğer bir koruma seviyesinin bulunmadığına ve Avrupa Birliği Temel Haklar Bildirgesi'ni ihlal ettiğine karar vermiştir.

Mahkeme, SCC'lerin kullanımını desteklerken, SCC'lerin korumayı sağlayamadığı durumlarda (kolluk kuvvetlerine erişim içerenler gibi) “diğer hükümler ve ek güvenceler” kullanımını öngören GDPR'daki düzenlemelerin esas alınması gerektiğine işaret etmiştir. Bu noktada Scherms II kararı, ABD ve Avrupa Birliği bünyesinde bulunan devletler arasındaki veri aktarımı açısından yeni bir döneme girildiğinin göstergesidir.

WhatsApp tarafından yürürlüğe konulacak yeni Gizlilik İlkeleri'nin Avrupa Birliği ve Avrupa Ekonomik Alanının (EEA) parçası olan Avrupa Birliği ülkeleri için geçerli olmayışı Birlik kapsamında etkili olarak uygulanan GDPR ve Birlik bünyesinde bulunan veri koruma otoritelerinin bireylerin mahremiyetini korumaya yönelik istikrarlı karar ve uygulamalarının sonucudur.

X. Türkiye’de Durum Nedir?

WhatsApp tarafından Gizlilik İlkelerinin güncellenmesi, bilişim sektörü ve kişisel verilerin korunması hukuku ile ilgilenen pek çok kişi tarafından beklenen bir gelişmeydi. Bunun gerçekleşmesi üzerine verilen tepki, ülkemizde gerek toplum gerekse şirketler açısından veri koruma hukukunun öneminin hala tam anlamıyla kavranamadığını göstermektedir.

Öncelikle ifade etmeliyiz ki bu bir kişisel veri işleme sorunudur ve Türkiye’deki kullanıcılar açısından “ülkesellik ilkesi” gereğince KVKK’nın uygulanması gerekir. O halde WhatsApp’ın sunucuları yurt dışında bulunduğu için bu durum KVKK m. 9’un uygulanmasını gerektiren bir yurt dışına aktarımdır. Özellikle kurumsal kullanıcılar tarafından bu husus dikkate alınmalı ve KVKK m. 9’un, m. 5 ve 6’ya yaptığı atıf gereğince tüm kullanıcılardan tek tek açık rıza alınması mümkün değilse bu kullanımdan kaçınılmalıdır. Sonuç olarak yurt dışına aktarım söz konusu olduğu için bu üç madde birlikte değerlendirilerek bir karara varılmalıdır.

Öte yandan WhatsApp, söz konusu değişiklikle kullanıcılarını aydınlatmaktadır. Ancak hizmeti sunmak için açık rıza şartını öne sürdüğünden KVK Kurul’unun da çok sayıda kararında belirttiği üzere bu, KVKK m. 3 ve m. 12/1-a’ya açıkça aykırı bir durumdur. Bir ön şart şeklinde, veri ilgisinden adeta dayatma şeklinde alınan rızanın hukuken bir geçerliliği bulunmamaktadır. WhatsApp’ın bu değişiklikten vazgeçmemesi halinde, bu şirkete KVKK m. 18 gereğince idari para cezası uygulanmalıdır. Ancak cezanın verilmesiyle, bu cezanın infaz

edilebilirliđi birbirine karıştırılmamalıdır. İnfazda güçlük yaşanacağı ihtimali, kanunun ihlal edildiđi gerçeđini ve bu konuda bir karar verilmesi gerekliliđini ortadan kaldırmamaktadır.

Bu bağlamda Rekabet Kurulu'nun 11.01.2021 tarihli ve 21-02/25-M sayılı kararıyla, WhatsApp kullanıcılarına getirilen veri paylaşma zorunluluđu hakkında Facebook Inc., Facebook Ireland Ltd., Whats App Inc. ve Whats App LLC hakkında 4054 sayılı Rekabetin Korunması Hakkında Kanun'un 6. maddesinin ihlal edilip edilmediđi hakkında re'sen soruşturma açılmıştır. Kurul tarafından yapılan açıklamada uygulamamanın soruşturma sonucunda alınacak nihai karara kadar ciddi ve telafi olunmayacak zararlar doğurma ihtimalini haiz olduđundan 4054 sayılı Kanun'un 9. maddesi çerçevesinde geçici tedbirler alınması ve bu kapsamda Facebook'un Türkiye'de kullanıcıların verilerini 8 Şubat 2021 tarihinden itibaren başka hizmetler için kullanılmasına yönelik getirdiđi koşulları durdurması ve bu koşulları kabul eden veya bilgilendirmeyi alarak kabul etmeyen tüm kullanıcılara Facebook'un veri paylaşımını içeren yeni koşulları durdurduđunu anılan tarihe kadar bildirmesi gerektiđine karar vermiştir.

Konu hakkında Rekabet Kurulu'nun karar vermesi kullanıcıların verdikleri tepkiler ve yanlış anlaşılmanın önüne geçilmesi açısından isabetlidir. Ancak asıl olarak konunun ilgisi KVK Kurulu tarafından konuya ilişkin bir açıklama yapılması gerekir. Zira KVK m. 22/1-c'de belirtildiđi üzere Kurulun görev ve yetkileri *"Şikayet üzerine veya ihlal iddiasını öğrenmesi üzerine re'sen görev alanına giren konularda kişisel verilerin kanuna uygun olarak işlenmediđini incelemek ve gerektiğinde bu konuda geçici önlemler almak."* olarak tanımlanmıştır.

Nitekim Kurul, 12.01.2021 tarihinde yapmış olduđu kamuoyu duyurusunda WhatsApp Gizlilik İlkeleri ve Facebook Şirketlerine veri aktarımı hakkında resen soruşturma başlattıđını duyurmuştur. Kurul söz konusu açıklamasında, yapılan ön deđerlendirme sonucunda řu hususlara işaret edilmesi gerektiđini belirtmiştir:

- Kurul ilk olarak; WhatsApp'm, kullanıcılardan kişisel verilerinin işlenmesine ve yurtdışındaki kişilere veri aktarılması için rıza alınması işleminde ayrıştırmaya gitmediđini; bu durumun açık rızanın unsurlarından "özgür iradeyle açıklanması" açısından bir ihlal oluşturup oluşturmadıđının incelenmesi gerektiđini, zira veri ilgisinin verisinin işlenmesine rıza gösterirken aynı anda verisinin yurt dışına aktarımı için rıza vermek istemeyebileceđini, oysa söz konusu deđişiklik ile bu iki hususunun birlikte düzenlendiđini ve veri ilgililerinin buna zorlanmasının söz konusu olup olmadıđının incelenmesinin gerektiđini belirtmiştir.
- İkinci olarak Kurul, yurtdışında bulunan başka bir şirkete aktarım yapılmak şartıyla uygulamanın kullanılmasına izin verilmesinin Kanunun 4. maddesinde sayılan ilkelerden "hukuka ve dürüstlük kurallarına uygun olma", "belirli, açık ve meşru

amaçlar için işlenme” ve “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkeleri açısından bir ihlale sebebiyet verip vermediğinin araştırılması gerektiğini ifade etmiştir.

- Kurul üçüncü olarak; sunulan hizmetin açık rıza şartına bağlanmış olmasının verilen açık rızayı sakatlayabileceğini bu durumun da kişisel verilerin hukuka aykırı işlenmesi sonucunu doğurabileceğini, dolayısıyla Whatsapp tarafından yapılan güncelleme ile verilen hizmetin “rıza şartına bağlanması” durumunun ortaya çıkıp çıkmadığının incelenmesi gerektiğine işaret etmiştir.
- Kurul son olarak, WhatsApp tarafından yurtdışında yerleşik veri sorumlularına yapılacak aktarımın KVKK m. 9’a aykırı olup olmadığının incelenmesi gerektiğini belirtmiştir.

Görüleceği üzere, Kurul, toplumda konuyla ilgili oluşan rahatsızlığı dikkate almış ve resen soruşturma başlatmıştır. Ayrıca yukarıda bizim de yapmış olduğumuz tespitler çerçevesinde, Kişisel Verilerin Korunması hukuku bakımından yerinde olarak verilerin işlenmesi ve aktarılması temelli bir yaklaşım göstermiş ve soruşturmanın doğrultusunu da açıklayarak şeffaflık adına bu konuda doğru ve örnek bir yaklaşım sergilemiştir.

Ben belirtilen bu hususların birçoğu açısından ihlal kararı verilebileceğini düşünüyorum. Ancak bir yönüyle büyük bir balon olarak gelişen bu olayın toplumumuzda “kişisel verilerin korunması”na ilişkin farkındalığın artması bakımından olumlu bir gelişme olarak belirdiğini de belirtmeliyim.