Kişisel Veriler Evrensel Ölçütlerden Korunmalı...
BİLGİSAYAR MÜHENDİSLERİ ODASI'NDAN ÖZGÜR YAZILIM ÇAĞRISI

Bilgisayar Mühendisleri Odası (BMO), 12 Ocak 2021 tarihinde yaptığı açıklama ile WhatsApp'ın gizlilik politikasına değişikliğine ilişkin yurttaşları uyardı. En çok kullanılan anlık mesajlaşma uygulamalarının teknik olarak kıyaslandığı açıklamada, Kişisel Verilerin Korunması Kanunu'nun AB ülkeleri düzeyinde koruma sağlamadığına dikkat çekildi. "Ağ tarafsızlığı" ilkesi kapsamında mevzuat düzenlemesi yapılması ve koruma politikası geliştirilmesi istenen açıklamada, yurttaşlara "özgür yazılım" kategorisine giren uygulamaları tercih etme çağrısı yapıldı.

WhatsApp'ın kullanıcılara gizlilik politikasını 8 Şubat 2021'den başlayarak değiştireceği bildirimi yaptığını hatırlatıldığı açıklamada, "*WhatsApp uygulamasının sahibi olan Facebook şirketi bu değişikliği şöyle açıklıyor: WhatsApp kullanıcılarından toplanan kişisel veriler, Facebook'a ait diğer uygulamalarda kullanılabilecek ve başka şirketlerle de paylaşılabilecek. Uygulamayı kullanmaya devam etmek isteyen kullanıcılar bu koşulları kabul etmek zorunda bırakılırken değişikliği onaylamayan kullanıcılar 8 Şubat 2021'den sonra uygulamayı kullanamayacaklar*" bilgisini aktardı.

Yurttaşların kaygılarının uygulama silme ve alternatif uygulama arayışına dönüştüğüne vurgu yapılan açıklamada, uygulamalar şöyle kıyaslandı:

WhatsApp

WhatsApp, kullanıcılar arası veri aktarımında (transferinde) uçtan uca şifreleme (E2E) kullandığından söz ederek, bu durumun değişmeyeceğini ve kullanıcıların güvende kalacaklarını açıklamakta; yeni gizlilik politikası sonrasında yalnızca üst verilerin (örneğin: kiminle ne zaman iletişim kurulduğu bilgisi, kullanılan cihaz bilgisi, konum bilgisi, telefon numarası, IP adresi vb.) ortaklarıyla paylaşılacağını, kullanıcıların uygulama içindeki paylaşımlarının şifrelenmiş olarak aktarılmaya devam edeceğini belirtmektedir. Ancak WhatsApp uygulamasının istemci (client) ve sunucu (server) katmanlarındaki kaynak kodlarının tamamı kapalı olduğu için bu iddia bağımsız otoritelerce kesin olarak kanıtlanamamaktadır. İstemciler arası iletişim tümüyle şifrelenmiş olarak gerçekleşse bile istemci düzeyinde gerçekleşen işlemlerin de şirketin kontrolünde olduğu gözden kaçırılmamalıdır. Diğer yandan, WhatsApp uygulamasının sahibi olan Facebook'un geçmişte kullanıcılarından topladığı bilgileri resmi otoritelerle, ABD'de CIA ve NSA gibi istihbarat örgütleriyle paylaştığı çok sayıda habere konu olmuş; dahası, bir önceki ABD seçimlerinde bu bilgilerin başkan adaylarından biri yararına kullanıldığını gösteren "Cambridge Analytica" skandalı unutulmamıştır.

Telegram

Telegram uygulamasında ön tanımlı mesajlaşmada veriler istemciden sunucuya şifrelenmiş olarak iletilmekte ve şifrelenmiş veri sunucuda çözülüp alıcının istemcisine yeniden şifrelenerek gönderilmektedir. Telegram, sunucularında bulunan kullanıcı verilerine erişilmek istendiği takdirde veriye erişim için birçok farklı hukuk sisteminden izin alınması gerektiğini öne sürmektedir. Uygulamada gizli mesajlaşma seçeneği kullanıldığında ise uçtan uca (E2E) şifreleme yapılmakta, yani göndericinin iletisi şifrelenmiş olarak alıcıya iletilmekte ve alıcının uygulamasında çözülmektedir. Telegram'ın özgür yazılım olan mobil, web, masaüstü uygulamalarına karşın tüm iletişimin akışını sağlayan sunucu yazılımları özgür yazılım değildir, yani kaynak kodları kamusal erişime açık değildir. Ayrıca bu uygulamanın da bir şirketin sahipliğinde olması ileride gizlilik politikasını değiştirme riskini taşımaktadır.

Signal

Signal uygulaması, gerek istemci ve sunucu yazılımları düzeyinde özgür yazılım olmasıyla gerekse yazılı, sesli ve görüntülü veri aktarımında uçtan uca (E2E) şifreleme kullanmasıyla kişisel verilerin korunması yönünden daha güvenli bir seçenek olarak görünmektedir. Signal'in, kimin kiminle mesajlaştığı üstverisi (metadata) gibi verileri yalnızca kullanıcı uygulamasında tutması, gizlilik özellikleri için önemli bir avantajdır. Kâr amacı gütmeyen bir vakfın kontrolünde olması nedeniyle de şirketlerin kâr odaklı değişen politikalarının oluşturduğu risklerle karşı karşıya değildir. Özgür

yazılım olması, kamusal erişime açık olan kaynak kodlarının gelecekte de erişilebilir olacağının ve yeni sürümlerinin de aynı özellikleri taşıyacağının güvencesidir. Dolayısıyla saydamlığı ve sürekliliği güvence altındadır.

Güvenlik ve saydamlık konusunda doyurucu açıklamaları bulunmayan, 'yerli' olma iddiasıyla ortaya çıkan ve dünya genelinde olmasa da ülkemizde gündeme gelen 'Bip' ve 'Dedi' gibi bazı uygulamalar, açık kaynak kodlu ya da özgür yazılım olmamaları nedeniyle kullanıcılara güven verememektedir. Ayrıca hiçbir üçüncü tarafla veri paylaşmamak gibi bir taahhütleri de söz konusu değildir."

"Korunması Politikası Eksik"

WhatsApp'ın yeni gizlilik politikasını AB ülkelerinde uygulanmazken Türkiye'de uygulanmaya geçilmesinin çifte standart olarak değerlendirildiği açıklamada, kişisel verilerin korunması açısından AB ülkeleri ile Türkiye arasındaki farklılık şöyle anlatıldı:

"Birçok yurttaşımız şirketin bu tutumunu "çifte standart" olarak değerlendirerek tepkilerini şirkete yöneltmiştir. Oysaki uygulamanın aynı dayatmayı AB üyesi ülkelerde yapmamasının nedeni keyfi bir tercih değil; AB vatandaşlarının kişisel verilerinin, kısaca GDPR (General Data Protection Regulation) olarak bilinen, kişi hak ve özgürlükleri temel alınarak oluşturulan, 1990'lı yıllardan bu yana güncellenerek geliştirilen yasal düzenlemeyle sıkı biçimde korunuyor olmasıdır. Beri yandan ülkemizde 2016'dan bu yana yürürlükte olan Kişisel Verilerin Korunması Kanunu (KVKK), GDPR'nin ilk düzenlemeleri baz alınarak oluşturulduysa da sonrasındaki teknolojik ve hukuksal gelişmeler doğrultusunda gerekli güncellemeler yapılamamıştır. Dolayısıyla KVKK, GDPR'nin AB vatandaşlarına sağladığı koruma düzeyini yurttaşlarımıza sağlamaktan uzaktır."

Ağ Tarafsızlığı Vurgusu ve Öneriler

İletişim ve kişisel verilerin gizliliğinin temel bir hak olmasının yanında bireysel düzeyde toplanan verilerin kitlesel düzeyde işlenerek, gözetim, denetim ve üretim mekanizmalarının kullanılması nedeniyle kamusal bir sorun olduğuna vurgu yapılan açıklamada, TBMM başta olmak üzere ilgili kurumlardan aşağıda sıralanan konularda acilen adım atılması önerildi:

"- Kişisel veriler üzerinden büyük kazançların elde edilmesinin engellenmesi, bu alanda tekelleşmenin önüne geçilmesi için başta KVKK'nin iyileştirilmesi olmak üzere gerekli yasal düzenlemeler yapılmalıdır.

- Kişisel verilerin korunması için yapılacak düzenlemelerde, uygulamalarda ve denetimlerde başta meslek odalarımız olmak üzere konuyla ilgili demokratik kitle örgütleriyle işbirliği yapılmalıdır.

- Milyonlarca yurttaşın verilerini içermesi itibarıyla kamusal varlık olarak değerlendirdiğimiz büyük veri kümelerini işleyen kamu bilişim sistemleri (örneğin: sağlık bilişim sistemleri, UYAP, MERNİS, SEÇSİS), anayasal sorumluluklarından biri kamusal denetim olan meslek odalarımızın bağımsız denetimine açılmalıdır.

Kişisel verilerin gizliliğinin evrensel standartlarda güvence altına alınabilmesinin yolu, İnternet altyapısına ve uygulamalarına 'ağ tarafsızlığı' ilkelerine uygun şekilde yaklaşan, demokratik, özgürlükçü, saydam, hesap verebilirlik ilkelerine uygun bir hukuk devleti olmaktır. Yurttaşlarımız, 'verilerim nereye/kimlere gidiyor', 'başıma bir iş gelecek mi' gibi kaygılar içinde olmadan iletişim kurabilmelidir."

Yurttaşlara Yönelik Öneriler ve Uyarılar

WhatsApp nedeniyle kişisel verilerin işlenmesi konusunda duyarlılık oluşmasının sevindirici olduğuna değinilen açıklamada, "Birçok uygulama hiçbir paylaşım yapılmasa bile kullanıcılarını işaretlemekte; ekranlardaki gezinmeleri, hangi sayfaya ya da paylaşıma ne kadar süre bakıldığını, nelerin beğenilip nelerin hızla geçildiğini, kimlerle etkileşime girildiğini izlemektedir. Söz konusu durum aslında kişisel verilerimizi satan, güvenliğimizi hiçe sayan ve kullanıcıları yalnızca kâr aracı olarak gören uygulamalardan kurtulmak için bir şans oluşturmuştur" ifadelerine yer verildi.

Açıklamada, yurttaşlara aşağıdaki öneriler ve uyarılara yer verildi:

-Aygıtlarınıza kurduğunuz uygulamaların erişmek istediği bilgileri ve izinleri mutlaka kontrol edin; vermek istemediğiniz bilgileri ve izinleri edinmek isteyen uygulamaları kurmaktan kaçının. Halihazırda kurulu olan uygulamalarınıza verilmiş izinleri düzenli aralıklarla gözden geçirin.

-Veri aktarımı sağlayan anlık ileti uygulamaları ve sosyal medya uygulamalarında, gerekli ya da zorunlu olmadıkça kritik kişisel bilgilerinizi (sağlık bilgileri, kredi kartı bilgileri, ev adresi vb.) paylaşmaktan kaçının. Kişisel sır ya da ticari sır olarak değerlendirdiğiniz bilgileri, anlık ileti ve sosyal medya ortamlarında paylaşmaktan kaçının. Bu tür bilgileri paylaşmanızın gerekli olduğu durumlarda ise gereklilik ortadan kalktığında paylaşımınızı silin.

- Çocuklarınızın kullandıkları aygıt ve uygulamaları kontrol ve takip edin, onları kişisel verilerin gizliliğinin önemi konusunda bilgilendirin.

- Özgür yazılımları tercih edin. Gereksinim duyacağınız birçok uygulamanın özgür yazılım olan bir alternatifini bulabilirsiniz. Özgür yazılımlar herkesin katılabildiği saydam bir geliştirme süreciyle, kaynak kodları tüm insanların erişimine açık olarak geliştirilirler; sahipleri ise kişi ya da şirketler değil tüm insanlıktır."