Türkiye Bilişim Derneği

Anlık İleti Hizmetleri Değerlendirme Raporu

3 Şubat 2021, Ankara

Türkiye Bilişim Derneği
Anlık İleti Hizmetleri Değerlendirme Raporu

Yayımcı Adı

TÜRKİYE BİLİŞİM DERNEĞİ
Ceyhun Atuf Kansu Cad., 1246 Sk. No: 4/17 Balgat – ANKARA
Tel: +90 (312) 473 8215 (pbx) Faks: +90 (312) 473 8216
tbd-merkez@tbd.org.tr

Yayın Tarihi

3 Şubat 2021, Ankara

Raporu Hazırlayanlar

Dr. Aydın Kolat	TBD İcra Kurulu Başkanı,	Verisis AŞ, Genel Md.
İ. İlker Tabak	TBD İcra Kurulu Bşk. Yrd.,	TBK Bilişim AŞ, YK Bşk.
Mehmet Ali İnceefe	TBD İcra Kurulu Bşk. Yrd.,	Accert AŞ, Genel Md.

TBD Yayın Numarası : 2021 / 01

ISBN :

Bilişim Teknikbilimini ulusal bir kalkınma aracı olarak kullanacağız…

Aydın KÖKSAL, 1968
TBD Kurucusu ve Onursal Başkanı

İÇİNDEKİLER

TABLOLAR

RAPORA KATKI VERENLER

Bu raporun içeriğinde ve hazırlanmasında katkılarını sunan katılımcılar aşağıda yer almaktadır.

Rahmi Aktepe	TBD Genel Başkanı
Dr. Aydın Kolat	TBD İcra Kurulu Başkanı, Verisis AŞ, Genel Md.
İ. İlker Tabak	TBD İcra Kurulu Bşk. Yrd., TBK Bilişim AŞ, YK Bşk.
Mehmet Ali İnceefe	TBD İcra Kurulu Bşk. Yrd., Accert AŞ, Genel Md.
Av. A. Kemal Kumkumoğlu	Kumkumoğlu Özdoğan Ergün Hukuk Bürosu, Ortak
Prof. Dr. Ali Yazıcı	Atılım Üniversitesi
Alp Köksal	Khan Akademi
Dr. Atilla Aydın	TBD YK Üyesi, TC Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
Dr. Ayşe Kula	Milli Eğitim Bakanlığı
Barış Özel	Bilgisayar Mühendisleri Odası (BMO)
Prof. Dr. Betül Ulukol	Ankara Üniversitesi
Buğra Ayan	Ankara Hacı Bayram Veli Üniv. Öğretim Görevlisi
Av. Burhanettin Al	TBD İcra Kurulu Üyesi, TURKCELL
Dr. Cenk Tezcan	Futuristler Derneği
Av. Ceren Küpeli	Marmara Üniv. Ve Bahçeşehir Üniv. Öğretim Görevlisi
Av. Ceyda Cimilli Akaydın	TBD İstanbul Şb. YK Sayman Üye, Serbest Avukat
Doç. Dr. Cihan Çetinkaya	TBD Adana Şubesi Bşk., Alpaslan Türkeş Bilim ve Teknoloji Üniversitesi
Çağdaş Ergin	Türkiye Bilişim Vakfı (TBV), Genel Sekreter
Demet Kabasakal	TBD İcra Kurulu Üyesi, Bilgi Teknolojileri ve İletişim K.
Deniz Tiryakioğlu	TBD İstanbul Şubesi YK Bşk.
Dilek Şen Karakaya	Sağlık Bakanlığı
Ertan Barut	TBD İcra Kurulu Üyesi, Globalnet Genel Md.
Füsun Sarp Nebil	BT Danışmanı, Teknoloji Gazetecisi
Prof. Dr. Gonca Telli	Maltepe Üniversitesi
Kemal Aydın	TSE Kıdemli Sızma Testi Uzmanı, BTYÖN Danışmanlık
M. Ali Yazıcı	TBD 2. Başkanı, ASELSAN
Av. Mehmet Ali Köksal	Köksal&Partners | KP Veri, Yönetici Ortak
Murat Duran	duSoft Yazılım AŞ, Kurucu Ortak
Dr. Mustafa Özhan Kalaç	Manisa Celal Bayar Üniversitesi
N. Kenan Altınsaat	TBD Ankara Şubesi YK Bşk., Jforce Ankara Bölge Md.
Nihan Tuna	TBD İcra Kurulu Üyesi, EMT Elektronik
Doç. Dr. Özhan Yalçın	Ankara Üniversitesi
Seyit Hasoğlu	TBD Kayseri Şubesi Bşk., Erciyes Üniv. Öğretim Görevlisi
Dr. Şebnem Özdemir	İstinye Üniversitesi
Doç. Dr. Tarkan Gürbüz	ODTÜ
Tolga T. Tuncer	TBD İcra Kurulu Üyesi, Güven Future Genel Md.
Doç. Dr. Tunç Medeni	Yıldırım Beyazıt Üniversitesi
Prof. Dr. Türksel Kaya Bensghir	TBD İcra Kurulu Üyesi, Ankara Hacı Bayram Veli Üniversitesi
Yağmur Fırat	Türkiye Teknoloji Geliştirme Vakfı (TTGV)
Zafer Koçak	TBD İcra Sektör Kurulu, Lotus Danışmanlık

KISALTMALAR

3G	3rd Generation – 3. Nesil
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AEDP	Agencia Española de Protección de Datos (İspanyol Veri Koruma Ajansı)
ATT	Application Tracking Transparency (Uygulama İzleme Şeffaflığı)
BBS	Bulletin Board System (Bilgisayarlı Bilgi Sistemi)
BTİDER	Bilgi Teknolojileri ve İnternet Derneği
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CEO	Chief Executive Officer (İcra Kurulu Başkanı)
CERN	Conseil Européen pour la Recherche Nucléaire (Avrupa Nükleer Araştırma Merkezi)
CNIL	Comission Nationale de Informatique & Libertés (Fransız Veri Koruma Otoritesi)
DDO	Dijital Dönüşüm Ofisi
DPA	Data Protection Authority (Veri Koruma Yetkilisi)
FBI	Federal Bureau of Investigation (Federal Soruşturma Bürosu, ABD)
FTC	Federal Trade Commision (Federal Ticaret Komisyonu, ABD)
Garante	İtalyan Veri Koruma Yetkilisi
GDPR	General Data Protection Regulation (Genel Veri Koruma Yönetmeliği)
GSM	Global System for Mobile Communications (Mobil İletişim için Küresel Sistem)
ICO	Information Commissioner's Office (Birleşik Krallık Bilgi Komiserliği Ofisi)
ICQ	İngilizce "I seek you" (Seni arıyorum) cümlesinin söylenişidir
IGF	Internet Governance Forum (İnternet Yönetişim Forumu)
IRC	Internet Relay Chat (İnternet Aktarmalı Sohbet)
KVKK	Kişisel Verileri Koruma Kanunu / Kurumu / Kurulu
MFA	Multi-Factor Authentication (Çoklu Kimlik Doğrulama)
MiTM	Man in The Middle (Ortadaki Adam Saldırısı)
NSO Group	Mobil cihazlara uzaktan erişim sağlayan siber istihbarat şirketi
RK	Rekabet Kurumu / Kurulu
SMS	Short Message Services (Kısa Mesaj Hizmetleri)
STK	Sivil Toplum Kuruluşu
TBD	Türkiye Bilişim Derneği
TBMM	Türkiye Büyük Millet Meclisi
TBV	Türkiye Bilişim Vakfı
TC CB	Türkiye Cumhuriyeti Cumhurbaşkanlığı
TTGV	Türkiye Teknoloji Gerliştirme Vakfı
Wi-Fi	Wireless Fidelity (Kablosuz Bağlantı Alanı)
WSIS	World Summit on the Information Society (Dünya Bilgi Toplumu Zirvesi)

TÜRKİYE BİLİŞİM DERNEĞİ
1971
.yıl
TEKNOLOJİ ÜRETEN TÜRKİYE

Bilişim Toplumu Yasalarıyla Yönetelim, Yönetilelim

Türkiye Bilişim Derneği

SUNUŞ

Değerli Bilişimciler, Değerli Paydaşlar…

Son birkaç yılda mobil teknoloji ve sosyal medyadaki gelişmeler ile birlikte gerçek zamanlı verinin önemi artmış, veri hacminin yanında çeşitliliği ve veri artış hızı da bu gelişmelerden etkilenmiştir. Akıllı telefonların kullanım oranındaki artış, İnternete 7/24 erişim olanağı sağlamasının yanı sıra WhatsApp ve benzeri çevrim içi mesajlaşma uygulamaları ile anlık mesaj, fotoğraf ve video paylaşımlarını artırmış, kişisel verilerin kullanımı konusunda çeşitli sorunlara da neden olmuştur.

Oysa kişisel veriler özel ve kıymetlidir. Bu verilerin analizi ile veriye dayalı ticari veya toplumsal yönlendirme yapılabilmektedir.

Bu tür platformlar "hedefli reklamcılık" üzerinden gelir elde etme stratejisini kullanmaktadır. Böylece özel şirketler mecranın belirlediği para ölçüsünde reklamlar vererek ulaşmaya çalıştığı hedef kitleye kolaylıkla ulaşabilir. Bizler de, bu farklı mecralarda geçirdiğimiz zaman içerisinde bizim hedeflendiğimiz pek çok reklama maruz kalırız.

Bütün bunları söylerken akıllı telefon ve bilgisayar kullanımının başlı başına bir güvenlik sorunu olduğunu, kişisel bilgilerimizin sadece anlık iletişim uygulamaları yoluyla değil telefonumuza veya bilgisayarımıza indirdiğimiz birçok uygulama yoluyla elde edilebileceğini de hatırlatmak isteriz.

WhatsApp uygulaması üzerinden gündeme böyle bir dijital güvenlik tartışmasının gelmiş olması aslında konunun masaya yatırılması açısından yerinde bir durum olmuştur. Özetle; söz konusu durum aslında tüm aygıt ve uygulamalar için sürdürülmelidir ve kişisel verilerimizi şu ya da bu şekilde kullanan, güvenliğimizi önemsemeyen ve kullanıcıları yalnızca kazanç fırsatı olarak gören uygulamaları daha yakından anlamak anlamak için bir ortam oluşturmuştur.

Gereksinim duyacağımız birçok uygulamanın özgür yazılım olan bir alternatifini bulabiliriz. Özgür yazılımlar herkesin katılabildiği saydam bir geliştirme süreciyle, kaynak kodları tüm insanların erişimine açık olarak geliştirilirler; sahipleri ise kişi ya da şirketler değildir.

Son birkaç yıldır açıkça görülmektedir ki, , dünya genelinde en değerli ve en çok yatırım yapılan şirketler internet, yazılım ve teknoloji şirketleridir. Türkiye'de ise internet ve sosyal medya konusunda yerlilik açısından birçok çaba olmasına karşın, yaygınlaşması bugüne kadar mümkün olamamıştır. Konumunun da etkisiyle Türkiye'nin diğer birçok ülkeye göre küreselleşmeden daha fazla etkilendiği gözlemlenmektedir. Bu alanda birçok girişim bulunan ülkemizde yerli uygulamalara yeterince önem verilmemiş ve bu platformların bilinirliği sağlanamamıştır. 2019 yılında Resmi Gazetede yayımlanan bir genelgede iletişimde ve haberleşmede yerli ve milli platformların tercih edileceği ve kullanımının teşvik edileceği belirtmektedir. Bu ve benzeri durumların aslında yerli ve milli sosyal medya platformlarının kullanımını artıracağı öngörülmektedir.

Şu anda artan dijitalleşme ve sosyal medya kullanımıyla birlikte kullanıcıların veri güvenliği, sosyal medya firmalarının vergi ve diğer yasal yükümlülükler altına alınması ile denetime açık olmaları vb. faktörler de göz önünde bulundurulduğunda; bazı ülkelerin uygulamaya koymaya başladığı şekliyle ülkemizin de yerli ve milli girişimleri desteklemesi önem arz etmektedir.

Piyasada yer alan mal ve hizmetlerin yerli ve milli üretimle elde edilmesi kadar sosyal medya başta olmak üzere tüm dijital platformların yerli ve milli alternatiflerinin geliştirilmesi, desteklenmesi ve piyasaya sunulması ülkemizin ve kullanıcıların siber güvenliği açısından da kaçınılmazdır.

Bu bağlamda sunduğumuz bu çalışma ortaya koyduğu bilgilerle kamuoyuna önemli katkılar sağlayacaktır.

Ayrıca tüm bu değişkenler bağlamında pazarlama faaliyetlerinde sosyal medyanın türü, kullanıcıları, tercih nedenlerine vb. göre planların şekillendirilmesi ve düzenlenmesi noktasında önemli çıktılar ortaya konmuştur.

Bu alanda ortaya konacak destekler yerli ve milli uygulamalar ülkemizin kendi pazarlama faaliyetlerine entegrasyonunu ve kullanımda başarısını olumlu yönde etkileyecektir.

Her şeyden önce, verinin zenginlik olduğunu sürekli hatırlattığımız bu dönemde, veri ve getirdiği tüm katkıların ülke içerisinde kalması ve değerlendirilmesi her türlü özgürlüğümüzün önüne geçecek değerdedir.

Önemli bir referans belgesi olan bu çalışmanın oluşmasında değerli katkı ve emekleriyle yer alan başta Sayın Aydın Kolat olmak üzere tüm TBD İcra Kurulumuza gönülden teşekkürlerimizi sunarım…

Saygılarımla,

Rahmi Aktepe

Türkiye Bilişim Derneği
Genel Başkanı

ÖNSÖZ

WhatsApp'ın 4 Ocak 2021 tarihinde "kullanıcılar ile yeni sözleşme imzalanacağını, bu sözleşmeyi imzalamayan kullanıcıların 8 Şubat 2021 tarihinden itibaren WhatsApp'ı kullanamayacağını" açıklaması ile hem Türkiye'de hem de dünyanın çeşitli ülkelerinde kullanıcılar arasında ciddi bir kaos yaşandı. Bunun sonucunda WhatsApp kullanıcılarının çok irdelemeden, panik halinde benzer uygulamalara geçmeye başlamaları üzerine, TBD olarak anlık ileti hizmetleri hakkında toplumumuzu bilgilendirmek, birey olarak kullanıcılara, karar verici otoritelere ve STK'lara düşen görev ve sorumlulukları tartışmak amacıyla 3 aşamadan oluşan bir dizi çalışma başlattık.

TBD bu konuda hızlı tepki verebilmek için bu çalışmanın ilk adımında kamuoyunun bilgilendirilmesi ve farkındalığının artırılmasına yönelik bu konuların tartışıldığı bir çalıştay düzenlemiştir. 13 Ocak 2021 tarihinde ilgili kurumlar, STK'lar ve basın ile paylaşılan "*WhatsApp tarafından kullanıcılarına gönderilen yeni sözleşme değişikliğine ilişkin Türkiye Bilişim Derneği'nin Değerlendirmeleri*" başlıklı kamuoyu duyurusunu yayımlamıştır. Çalışmanın ikinci aşamasında anlık ileti hizmetleri ile ilgili teknik, idari ve hukuki açılardan ele alınan kapsamlı bir rapor hazırlanması hedefiyle 21 Ocak 2021 tarihinde yeni bir çalıştay gerçekleştirilmiştir. Bu rapor, birinci ve ikinci çalıştaylarımızda tartışılan konular kapsamında ve TBD Merkez İcra Kurulu, TBD İcra Sektör Kurulu, TBD şubeleri ve STK'ların destekleri ile geniş bir katılımla hazırlanmıştır.

Çalışmanın son aşamasında ise, daha uzun soluklu ve daha kapsamlı olarak sadece anlık ileti hizmetleri değil, daha geniş anlamıyla sosyal medya ile ilgili sosyo-kültürel, sosyo-ekonomik, dijital vatandaşlık, etik, psikolojik ve hukuki boyutları da dahil edilerek, hem kullanıcılar, hem yönetici ve karar vericiler açısından farkındalık yaratmaya yönelik çeşitli çalıştaylar gerçekleştirilip raporlar hazırlanması hedeflenmektedir.

TBD, verinin dijital ekonominin gelişiminde en önemli faktörlerden biri olduğu ancak kişisel verilerin korunmasının da mahremiyetin sağlanması için gerekli olduğunu uzun zamandır savunmakta, bununla ilgili çalıştaylar yapmakta ve raporlar hazırlamaktadır. 17 Şubat 2015 tarihinde yayımlanan "Siyasi Partilerden Bilişim Sektörü Beklenti Raporu"nda[1] tüm siyasi partilerimizle kişisel verilerin korunmasıyla ilgili aşağıdaki görüşler paylaşmış ve zaman geçirilmeden önlemlerin alınmasını istemişti.

> *Türkiye'de ilk çalışmaları 1995'te Adalet Bakanlığı bünyesindeki bir komisyon tarafından yapılan ve 2008 yılından beri Türkiye Büyük Millet Meclisi'nde (TBMM) kanunlaşmayı bekleyen Kişisel Verilerin Düzenlenmesi Hakkında Kanun Tasarısı, Ocak 2015'te TBMM'de tartışmaya açıldı.*
>
> *Türkiye'nin Avrupa Birliği nezdinde kişisel veriler konusunda "güvenli olmayan üçüncü ülke" statüsünde bulunması Kişisel Verilerin Düzenlenmesi Hakkında Kanun'un çıkarılmasını daha da önemli hale getirmektedir.*
>
> *Kişisel Verilerin Düzenlenmesi Hakkında tasarının kanunlaşmasıyla "belirli veya kimliği belirlenebilir bir kişiye ilişkin bütün bilgiler" kişisel veri sayılacaktır. Kişisel verilerin "toplanması, elde edilmesi, kaydedilmesi, düzenlenmesi, depolanması, uyarlanması veya değiştirilmesi,*

[1] https://www.tbd.org.tr/tbd-bilisim-sektoru-icin-siyasi-partilerden-beklentiler-raporu/

değerlendirilmesi, kullanılması, açıklanması, aktarılması veya elde edilebilir olması, ayrılması veya birleştirilmesi, dondurulması, silinmesi veya yok edilmesi" gibi işlemlerden herhangi biri kişisel verilerin işlenmesi anlamına gelecektir.

Kişisel verilerin, ister yurt dışında, ister yurt içinde, ister iyi niyetli kullanım için, ister ticari amaçla, ister bir kurumun menfaati için, bireylerin kontrolü dışında ortalara saçılması, kişilerin mahremiyetini ortadan kaldırmaktadır. Hatta kişisel verilerin bir bütün olarak analiziyle ülke güvenliğini ve geleceğini bile tehdit edebilir boyutlara gelebilmektedir. Uygulamanın niteliği gereği uluslar arası iletişimlerin yapılabilmesi de gerektiğinden, anlık ileti uygulamalarında, kişisel verilerimizin ülkemizde saklanması bir yandan güvenlik faktörü olarak görülse de, bunun sağlanması ülkemizdeki teknik, alt yapı, idari ve hukuki açıdan sorunlar oluşturabilmektedir.

Bu raporda TBD'nin 12 Ocak 2021 ve 21 Ocak 2021 tarihlerinde gerçekleştirdiği "Anlık İleti Uygulamaları" çalıştaylarının çıktıları, TBD'nin bu konu ile ilgili geçmişte yayımladığı raporlar ve TBD Merkez İcra Kurulunun daha önce yaptığı çalışmalar esas alınmıştır. Raporda, en çok kullanılan yerli ve yabancı anlık ileti uygulamaları; kullanıcıların hangi kişisel verilerinin toplandığı ve ne şekilde işlenilerek kullanıldığı; nerede ve ne kadar güvenli saklandıkları özetlenmiş, kullanıcıların kendilerine uygun anlık ileti uygulamasını seçmelerine yardımcı olacak "Anlık İleti Seçim Ölçütleri" detaylı olarak anlatılmıştır. WhatsApp'ın sözleşme değişikliği uygulamasını tüm ülkelerde eşit koşullarda uygulamayarak çifte standart yaratması karşısında ülkemizde alınması gereken önlemler de bu raporda değerlendirilmiştir. TBD Merkez İcra Kurulu Başkanı olarak emeği geçen herkese teşekkür ediyor, sonraki çalışmalarımızda da destek vereceklerine inanıyorum.

Dr. Aydın Kolat
TBD Merkez İcra Kurulu Başkanı

TÜRKİYE BİLİŞİM DERNEĞİ
1971
.yıl
TEKNOLOJİ ÜRETEN TÜRKİYE

TÜRKİYE BİLİŞİM DERNEĞİ

ANLIK İLETİ SİSTEMLERİ DEĞERLENDİRME RAPORU

TÜRKİYE BİLİŞİM DERNEĞİ
1971
.yıl
TEKNOLOJİ ÜRETEN TÜRKİYE

1 GİRİŞ

WhatsApp'ın kullanıcılarına gönderilen sözleşme değişikliği ile ilgili olarak sunduğu hizmetten yararlanmaya devam etmek için, yeni sözleşmeye rıza gösterilmesini ve bu şekilde açık rızayı bir hizmet koşulu haline getirmesi ülkemizde ve dünyada özellikle kişisel veriler konusunda ciddi endişelere yol açmıştır. Bu endişeler gerek yerli gerekse de yabancı anlık mesajlaşma uygulamalarının tartışılmasına da neden olmuştur.

WhatsApp'ın Kullanım Koşulları ve Gizlilik Politikası'nda 4 Ocak 2021 tarihinde yaptığı değişiklik ile birlikte ülkemizde kullanılan anlık ileti uygulamalarının teknik ve hukuki açıdan mahremiyete yaklaşımlarının analiz edilmesi gerekliliği doğmuş ve TBD tarafından yapılan kapsamlı bir çalışmanın ilk sonucu olarak 13 Ocak 2021 tarihinde "WhatsApp tarafından kullanıcılarına gönderilen yeni sözleşme değişikliğine ilişkin Türkiye Bilişim Derneği'nin Değerlendirmeleri"[2] adıyla Kamuoyu Bilgilendirmesi yayımlanmıştır.

Diğer yandan Facebook'un 16 Aralık 2020 tarihinde Apple'ın yeni ATT[3] uygulamasını şikayet amacıyla New York Times, Wall Street Journal ve Washington Post gazetelerine verdiği ilan, dikkatleri Facebook'un topladığı kullanıcılara ait kişisel verilere çekmiştir. Buna göre Facebook sadece kullanıcılardan elde ettiği kişisel verilerin yanında, aynı zamanda kullanıcılardan kendi telefonlarında yer alan diğer uygulamalarla ilişkili verileri de "izinsiz olarak" toplamaktadır.[4] WhatsApp'tan aktarılacak kişisel veriler bu nedenle diğer anlık ileti uygulamalarının topladığı verilerden farklıdır.

Bu raporda Türkiye Bilişim Derneği (TBD) olarak, WhatsApp'ı diğer benzer uygulamalarla birlikte ele alarak geniş perspektifte yeni teknolojik gelişmeler çerçevesinde devlet, birey ve STK'ların görev ve sorumlulukları teknik, hukuki, idari ve toplumsal yönden değerlendirilmiştir.

Teknolojideki gelişmelerin çok büyük miktarlarda ve çeşitli formatlardaki verinin toplanıp analiz edilmesine, işlenerek ve yorumlanarak yeni anlamlı bilgilere dönüştürülmesine olanak sağlamasıyla, verinin önemi ve hayatımızı ne ölçüde etkileyebileceği daha iyi anlaşılmıştır.

Bilgisayarlar, akıllı telefonlar, oyun konsolları, giyilebilir cihazlar ve diğer sensörler aracılığıyla, genel olarak yazılımlar, özel olarak da bilgisayar oyunları, sosyal medya uygulamaları, artırılmış gerçeklik ve sanal gerçeklik uygulamaları verilere ulaşmak için araç olarak kullanılmıştır. Hızla yaygınlaşan Apple Siri, Google Asistan, Amazon Alexa gibi asistanlar sürekli şekilde ortamlardaki tüm sesleri ve talimatları toplamaktadır. Facebook, Twitter, YouTube, Instagram, gibi etkileşimli Sosyal Medya platformları veya WhatsApp, Telegram, Signal, BiP, Dedi gibi anlık ileti uygulamaları ise yine bir çok kişisel veriye erişmekte ve ayrıca üst verileri de toplamaktadır. Tüm bu şirket ve platformlar tarafından tüketici alışkanlık ve tercihleri, değişen kullanıcı eğilimleri hakkında veriler toplanıp işlenerek tüketici davranışlarınının kolaylıkla yönlendirildiği gözlenmektedir.

---

[2] https://www.tbd.org.tr/kamuoyu-duyurusu-whatsapp-gundemi/ (13.01.2021)

[3] Application Tracking Transparency - Uygulama İzleme Şeffaflığı

[4] https://turk-internet.com/apple-app-storeun-guncellenen-gizlilik-politikasi-facebookun-hangi-bilgileri-topladigini-gosteriyor/

2 AMAÇ VE KAPSAM

Bu raporun amacı teknik, idari, hukuki ve toplumsal yaklaşımlar ışığında sosyal medya ve anlık ileti uygulamalarını kullananlara, yasa yapıcılara, hukukçulara, karar vericilere, teknik uzmanlara ve bu konuda girişim yapmak isteyen kişi ve kurumlara TBD olarak rehberlik etmektir.

Raporun kapsamında kişisel veriler, anlık ileti uygulamalarının teknik özellikleri, ileti protokolleri, uygulama örnekleri, kişi, kurum ve STK'ların görev ve sorumlulukları ele alınmış olup girişimci ekosistemi açısından uluslararası benzer çözümler değerlendirilmiştir.

Ayrıca, ticari ve kişisel verilere ilişkin ulusal ve uluslararası mevzuat ve uygulamalar açısından değerlendirmelerde bulunulmuştur.

3 ANLIK İLETİ HİZMETLERİNİN KISA ÖYKÜSÜ

Uçtan uca anlık ileti hizmetleri, 1990'ların ilk yarısında karşımıza BBS (Bulletin Board Systems) ve IRC (Internet Relay Chat) olarak çıktı. İkinci yarısında internetin yaygınlaşmasıyla birlikte, kullanıcı dostu metin bazlı ya da ses ileten anlık uygulamalar hızla yaygınlaştı. ICQ, Messanger gibi sadece internet üzerinden ve metin bazı olanlar yanında yine aynı günlerde PalTalk gibi (Skype benzeri) sesli ve metin olarak anlık görüşme yapılan çok sayıda uygulama kullanılmaya başladı.

GSM teknolojisi, mobil haberleşmede kelimenin gerçek anlamıyla bir devrim ve bir patlamaya yol açmıştır. Mobil telefonların yaygınlaşması ve çeşitliliğinin artması fiyatlarında önemli bir düşüşe yol açmıştır. Mobil telefonların gençler tarafından kullanılmaya başlaması ise özellikle mesajlaşma hizmetlerinde çok ciddi biçimde artış getirmiştir.

2006-2007 yıllarında gündeme gelen akıllı telefon (smartphone) kullanımı ve özellikle 2010'lu yıllarda 3G gibi yüksek veri altyapısı sunan mobil şebekeler ile Wi-Fi gibi ev ve iş ortamlarından da kolaylıkla internete erişim olanakları, sadece mobil haberleşmenin değil internet kullanımının da biçimini değiştirmiştir. Akıllı telefonlar basit uygulamalar ile toplumun günlük yaşantısını da değiştirmiş, bu cihazlarda ilk etkin uygulamalardan biri doğal olarak 2011 yılında kullanımının doruğa çıktığı mesajlaşma hizmetleri olmuştur.

Anlık ileti (mobil mesajlaşma) hizmetlerinin aynı dönemlerde oldukça yaygın olarak kullanılmakta olan ve masaüstü/dizüstü bilgisayarlar aracılığıyla erişilen internet tabanlı kişisel sosyal ağlardan (sosyal medya / *personal social networking*) temel farklılıkları vardır. Kişisel sosyal ağlar, kullanıcıların etkileşimde bulunabilecekleri paylaşılan bir sosyal alan içerir. Bu ortamda kişilerin arkadaşları ve aileleri ile fotoğraf, video ve kişisel deneyimlerini paylaşmaları sağlanır. Facebook bu alandaki ilklerden ve en büyük olanıdır. Anlık ileti hizmetleri ise, kullanıcıların kendilerinin iletişim bilgilerine sahip olduğu bir grup kişi ile sınırlı olan bir grup insana ileti göndermelerini ve sesli, görüntülü iletişime geçmesini sağlayan bir hizmet türüdür. Facebook'un kurucusu olan Zuckerberg, 2019 yılındaki bir iletisinde bu ayrımı, Facebook gibi kişisel sosyal ağ sağlayıcılarını "*bir şehir meydanının dijital eşdeğeri*" olarak

nitelendirmiş ve WhatsApp gibi mobil mesajlaşma uygulamalarının sunduğu özel iletişimi "*oturma odasının dijital eşdeğeri*" olarak tanımlamıştır.[5]

Anlık ileti hizmetleri mevcut kısa mesaj hizmetlerinin (*SMS*) yanısıra internet tabanlı daha yetenekli hizmetlere de dönüşmüştür. Öncelikle ilk sağladığı avantaj ücretli olan kısa mesaj hizmetlerinin (SMS) karşısına internet tabanlı ücretsiz bir hizmet sağlamasıdır. Ayrıca standart metin mesajlarının ötesinde fotoğraf, video, görüntü ve ses mesajlarının, üstelik bazı durumlarda mesajların içeriklerinin şifrelenerek de gönderilmesini sağlayıp olağanüstü bir büyüme göstermiştir.

Facebook, bir video paylaşım uygulaması olan Instagram'ı kendisi için tehdit olarak algılayıp benzeri özellikleri taklit etmeye çalıştı; ancak, çok fazla başarı sağlayamayınca bu şirketi satın alma yoluna gitti. Bu satın almanın ardından 2014 yılında "*bir sonraki en büyük tüketici riski*" olarak değerlendirdiği anlık ileti hizmetleri sunan popüler ve yaygın olarak kullanılan WhatsApp'ı da satın aldı.

WhatsApp topladığı kişisel verileri, çeşitli taraflar ile paylaşmaktadır. Ayrıca, "*Facebook şirketler ailesinin bir parçası olan WhatsApp, bu şirketler ailesinden bilgi alır ve bu şirketlerle bilgi paylaşır.*" [6]

Diğer taraftan Facebook da hem kullanıcılarından hem de kullanıcısı olmayanlardan topladığı kişisel verileri diğer Facebook şirketleriyle (*Instagram, WhatsApp ve Messenger dahil*) ve üçüncü taraf iş ortaklarıyla paylaşmaktadır. Kullanıcıların Facebook'ta sakladıkları verileri Facebook kullanan veya Facebook ile entegre olan üçüncü taraf uygulamalar, web siteleri veya diğer hizmetlerle paylaşmalarına da olanak tanır.[7] Bu, kullanıcıların (bilerek veya başka şekilde) yalnızca kendileriyle ilgili olmayan arkadaş listeleri gibi verileri paylaşabileceği anlamına gelmektedir.

4 VERİLERİN ÖNEMİ

Veriler çeşitli kararları almak için dayanak oluşturan insan davranışını çevreleyen değerleri ve bilgileri somut halde ortaya koyan unsurlardır. Toplanan veriler, işletmelerin ya da kurumların ilgili hizmetlerinin sunulmasında, müşteri sadakatinin sağlanmasında, potansiyel müşterilerin daha iyi hedeflenmesinde ve müşterilerin satın alma davranışının temel itici güçlerinin belirlenmesinde etkilidir. Özellikle "Bilgi Çağı"nda oluşacak rekabette bireysel teklifleri yönetebilmek için de bu veriler önemlidir.

2016 ABD Başkanlık seçimleri ile ortaya çıkartılan "Cambridge Analytica" skandalı, bu verilerin sadece reklam sektörü için toplanmayabileceğini de gösterdi. Cambridge Analytica olayı ile başlayan tartışmalar ve geçen yılın seçim kampanyasında Trump'ın "tweet"lerinin engellenmesi sonucunda, ABD siyaseti bu firmaları kontrol altına almaya karar verdi. Avrupa Birliğinin de "Güvenli Liman" ve "Gizlilik Kalkanı" sözleşmelerini iptal etmesi sonrasında, önümüzdeki dönemde "arka kapı" olaylarının ve bu tür gölge profillemenin artacağı anlaşılmaktadır.

Aynı şekilde, Edward Snowden'in ortaya döktüğü kimi bilgiler, son 5-6 yılda ortaya çıkan "arka kapı" olayları, Whatsapp'ı MiTM[8] siber saldırısıyla kıran (hacking) NSO Group'un bunu Facebook'un talebiyle

[5] FTC vs Facebook
[6] https://www.whatsapp.com/legal/privacy-policy
[7] https://www.facebook.com/privacy/explanation
[8] MiTM - Man in The Middle yani ortadaki adam saldırısı

yaptığını açıklaması ya da güvenlik araştırmacılarınca ortaya çıkarılan Gölge Profil[9] türü çalışmalar da, arka planda bu verilerin kapsamlı bir şekilde reklam sektörünün talebinin çok üstünde amaçlarla bir araya getirildiğini göstermektedir.

Bu verilerin kullanımının sadece kullanıcılara uygun reklam gösterimi ile kısıtlı kalmadan ticari ve politik amaçlarla da kullanılma olasılığı ciddi bir tehdit oluşturmaktadır.

4.1 Kişisel Veri

6698 sayılı Kişisel Verileri Koruma Kanunu'nda kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Bir kişinin ismi, soyadı, TC kimlik numarası gibi bilgiler vermeden dahi bu kişinin belirlenebilir kılınmasını sağlayan veriler mevcutsa, bunlar kişisel veri olarak kabul edilmektedir. Kişisel verilerin korunması hakkı, evrensel hukuk bağlamında bireyin temel hak ve özgürlükleri çerçevesinde korunmasında hukuki yarar bulunduğu kabul edilen, ülkemizde de anayasal dayanağı olan bir temel haktır. Yalnızca veri sahibi olan birey, tasarruf hakkı olarak adlandırılan kişisel verileri hakkında özgürce tasarruflarda bulunma imkanına sahiptir. Ülkemizde özel kanun mahiyetindeki KVKK uyarınca da, kişisel verilerin işlenmesine yönelik veri sahiplerinin bilgilendirilmesi, açık rızalarının alınması ve verilerine ilişkin olarak tasarruf haklarının sürekli olarak korunmasının esas alındığını görüyoruz. Dolayısıyla uluslararası hukuka paralel olarak ülkemizde kişisel verilerin korunması, hakkın özünü koruyan birtakım esaslara haizdir. Bireyi doğrudan işaret edebilmesi dolayısıyla hukuken büyük bir öneme sahip olan kişisel veriler, bir arada değerlendirilerek veriye dayalı ticari veya toplumsal yönlendirme yapılabilmesi yönüyle birçok hukuki riski beraberinde getirmektedir.

Bu gerçeklerden hareketle Facebook, Amazon, Apple, Netflix ve Google (FAANG) gibi dijital ekonominin dev firmaları, verileri toplayarak yarattıkları değerle şirketlerinin değerini büyütmüştür. Bu amaçla daha fazla veri toplayan uygulamaları geliştirmiş ya da kendi elindeki veriye değer katacak potansiyeli olan küçük şirketleri satın alarak kendi bünyelerine katmışlardır. Bu şirketler zaman zaman kendisine rakip olabilecek işletmeleri, görece küçük oldukları dönemlerde, satın alıp tehdit olarak gördükleri uygulamayı geliştirmeyi durdurmuşlar ve rakip uygulamanın pazara girmesini ve gelişmesini önlemişlerdir.

Verinin gücünün giderek artması veri gizliliğinin ve güvenliğinin nasıl sağlanacağına ilişkin soruları da beraberinde getirmektedir. Medya kullanımının giderek arttığı ve yaygınlaştığı günümüzde her yaş grubundan milyonlarca kişi kendi istek ve iradeleriyle, üstelik ücretsiz olarak ad, soyad, adres, cinsiyet, doğum tarihi, kimlik numarası, ilgi alanı, arkadaş listesi gibi değerli kişisel verilerinin ne amaçla ve nasıl kullanılabileceğini irdelemeden paylaşmaktadır. Bu noktada, konuya ilişkin durumsal farkındalık büyük bir önem kazanmaktadır.

4.2 Üst Veri (Meta Veri)

Üst veri "veriler ile ilgili veriler" olarak tanımlanmaktadır. Gerçek veriler kadar güçlü ve değerlidir. Kime, ne zaman ve ne sıklıkla mesaj gönderildiği, kim kimi tanıyor ve mesaj gönderiyor gibi veriler kullanıcı kimliğini anlamak ve izlemek için oldukça önemlidir.

[9] https://turk-internet.com/facebook-iliskilerinizi-nasil-biliyor-golge-profil/

"*Facebook'un bilgi madenciliği makinesini yönlendiren bu meta verilerdir. WhatsApp planları konusunda bu kadar gergin olmasının nedeni de budur, çünkü tüm bu kullanıcılar arasında para kazanmayı teşvik eder ve onu diğer platformlarıyla entegre eder*."[10]

4.3 VERİ TOPLAMA

Anlık mesajlaşma ve sosyal medya uygulamaları başta olmak üzere her türlü uygulama tarafından kişilere ait veriler toplanmaktadır.

Bu verilerin toplanma yöntemleri aşağıdaki gibi özetlenebilir:

4.3.1 Beyan edilen veriler

Birey tarafından bilerek ve aktif olarak sağlanan verilerdir. Bu, bir hesap oluşturulduğunda kullanıcı tarafından girilen verilerdir. [11]

4.3.2 Çıkarılan ve gözlemlenen veriler

Hizmet sağlayıcılar ve diğer taraflarca beyan edilen verileri işleyerek oluşturulan verilerdir. Bu veriler, diğer uygulamalardan sızdırılan beyan edilmiş verilerden çekilerek ve bu verileri diğer veri kümeleriyle birleştirilerek ve/veya kullanıcı faaliyetlerine ve davranışına veri analitiği uygulanarak oluşturulmaktadır.

4.3.3 İlgi ve niyet verileri

Yeterince büyük miktarda veri biriktirildikten sonra fark edilebilen verilerdir. Bu büyük veri daha sonra gösterge olarak sıklıkla kullanılan eğilimler veya modeller için analiz edilmektedir.

Anlık mesajlaşma ve sosyal medya uygulamaları bu kapsamda düzinelerce veri toplayabilir:

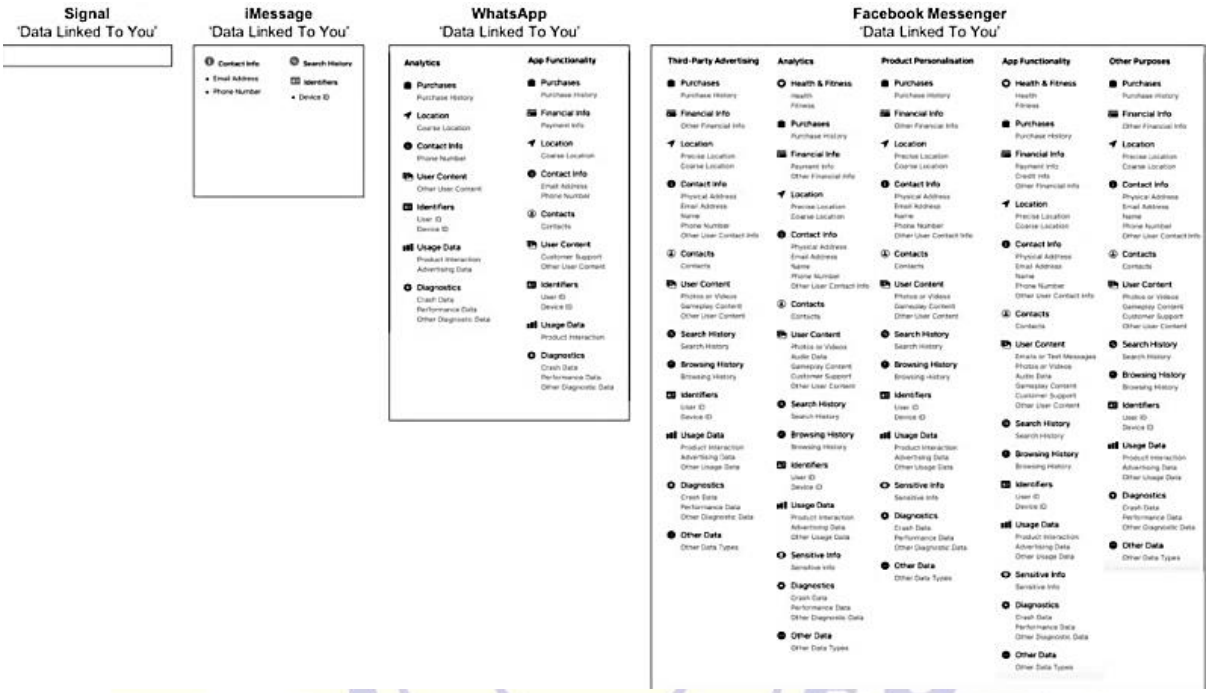
- ad
- soyad
- adres
- cinsiyet
- doğum tarihi
- kimlik numarası
- ilgi alanı
- arkadaş listesi
- doğum günü
- biyografi
- faaliyetler
- haber makalesi etkinliği
- kitap etkinliği
- check-in'ler
- Şu anki şehir
- Eğitim tarihi
- Etkinlikler
- fitness etkinliği
- oyun etkinliği
- gruplar
- Memleket
- ilgi alanları
- seviyor
- müzik etkinliği
- notlar
- çevrimiçi varlık
- Açık Grafik etkinliği
- fotoğraflar
- sorular
- ilişkiler
- ilişki ayrıntıları
- din / siyasi görüşler
- durum
- abonelikler
- videolar
- video izleme etkinliği
- Web Sitesi URL'si
- iş geçmişi

Diğer taraftan akıllı cihazlara yüklenen anlık ileti uygulamaları, kişisel verilerin korunması için risk oluşturmaktadırlar. Bunun nedeni, uygulamaların kullanıcı mesajlarını uçtan-uca şifrelemelerine rağmen üst veriler, konum verileri ve rehber bilgileri gibi büyük miktardaki diğer kişisel verileri toplayıp kullanmalarıdır.

[10] https://www.forbes.com/sites/zakdoffman/2021/01/03/whatsapp-beaten-by-apples-new-imessage-update-for-iphone-users/?sh=7564c56a3623

[11] The Humanitarian Metadata Problem: "Doing No Harm" In The Digital Era, October 2018

Aşağıdaki karşılaştırma tablosu Facebook ve WhatsApp'ın doğrudan ya da dolaylı olarak topladıkları kişisel verilerin çeşitliliğini göstermektedir. WhatsApp'ın mevcut sözleşmesine göre topladığı bu kişisel verilerden elde ettiği katma değerin boyutları ortadadır. Bu boyutu yarattıkları veri ya da bilgi ekonomisi ile elde ettikleri kazançlarda görmek mümkündür[12].



Tablo 1 - Anlık ileti uygulamalarının topladığı kişisel veriler

5 ANLIK İLETİ UYGULAMALARI

Anlık ileti uygulamaları teknik yetenekleri ile kullanıcılara sağladıkları özellik ve kolaylıklara göre önceliklendirilerek tercih edilmektedir.

5.1 İLETİ PROTOKOLLERİ

5.1.1 Anlık İleti Protokolleri

Bu rapor kapsamında anlık ileti uygulamalarında yaygın olarak kullanılan üç temel protokol yer almaktadır:

1. **iMessage;** Apple tarafından geliştirilip ve kendi ileti uygulamasında kullanılmaktadır.

2. **Signal Protokolü;** *Open Whisper Systems* tarafından geliştirilip Signal uygulamasında kullanılmaya başlayan ve WhatsApp, Facebook Messenger, Google Allo, Skype gibi çeşitli uygulamalarda da kullanılmaktadır.

3. **MTProto;** Telegram tarafından geliştirilmiş olup kendi uygulamasında kullanılmaktadır.

[12] https://9to5mac.com/2021/01/04/app-privacy-labels-messaging-apps/

5.1.2 Kişisel Bilgi Kasası : Solid Protokolü

İnterneti bulan kişi kabul edilen Tim Berners-Lee'nin internetteki kişisel verilerin gizliliğine (mahremiyetine) ve güvenliğine ilişkin olarak yaptığı değerlendirme şöyledir: [13]

> **"İnternetin mucidi TİM BERNERS-LEE: Mahremiyet Önemli**
> *Sör Tim Berners-Lee, 1989'da CERN'deki ofisinde bizim bildiğimiz interneti icat eden isim. İnternet başta yalnızca bilimsel dokümanların link'lerle bağlanmasını sağlıyordu. CERN'ün halka açmasıyla World Wide Web (dünya çapında ağ) haline geldi. '**www**'yu yaratan Tim Berners-Lee, internetin 25'inci yılında (2014) Wired dergisine yazdığı makalede bugünlerin geleceğini öngörmüş ve internetin tehdit altında olduğunu anlatmıştı. Mahremiyet ve ifade özgürlüğü kısıtlanabilirdi... Berners-Lee, internet merkezi yapıda olmadığı halde bazı popüler ve başarılı servislerin tekelleşmeye başladığını anlatıyordu: Arama, sosyal ağlar ve e-posta. Ona göre sansür, ifade özgürlüğünü kısıtlarken bugün tadımızı kaçıran reklamlar ve kişisel bilgilerin toplanması daha sinsi bir tehdit oluşturuyordu. Dolayısıyla ifade özgürlüğünün korunamadığı bir ortamda mahremiyetin korunması daha da önemliydi.*
>
> *"Web'in geleceği sıradan insanların bu sıradışı kaynağın sorumluluğunu almalarına ve onu manipüle etmek isteyenleri zorlamalarına bağlı" diyen Tim Berners-Lee, insanlığın kontrolü geri alabileceğine inanıyor ve yeni bir yöntem geliştiriyor. Şimdiki modelde Facebook, Google gibi şirketlere ve uygulamalara kişisel bilgilerimize erişim, saklama ve kullanma izni veriyoruz. Berners-Lee'nin geliştirdiği '**Solid**' adlı protokolse **bir kişisel bilgi kasası**. Bilgilere ihtiyaç duyan üçüncü partiler güvenli bir bağlantıyla kasaya erişecek ancak bilgileri saklayamayacaklar.* [14]
>
> *Herkes kendi bilgisini kendisi koruyacak. Böylece kontrol büyük şirketlerde değil, bireylerin kendisinde olacak."*

5.2 UYGULAMA SEÇİM ÖLÇÜTLERİ

Anlık ileti uygulamalarının teknik özellikleri, kullanım özelliklerine göre sıradan kullanıcılar tarafından daha az dikkat edilen ölçütler gibi görünmektedir. Ancak, anlık ileti sistemlerinin teknik özellikleri kullanım özelliklerine göre çok daha önemli ve kritiktir.

5.2.1 Yazılım Geliştirme Yöntemleri

Teknik özelliklerin başında uygulamaların **yazılım geliştirme yöntemleri** gelmektedir. Çoğu uygulama yazılımı kapalı, yani kaynak kodu sadece geliştirici ve/veya hizmet sağlayan tarafından görülebilen yazılımlardır. Dolayısıyla bu yazılımların nasıl çalıştıkları, arka kapı veya belirtilenden farklı işler yapıp yapmadığı kontrol edilemezler. Bu nedenle diğer birçok alanda olduğu gibi anlık ileti hizmetlerinde de **açık kaynaklı, özgür yazılımların** kullanılıyor olması en önemli ölçütlerden birisidir. Ancak, kişisel/ulusal verilerin belirtilen önem ve hassasiyeti göz önünde bulundurularak anlık ileti sistemlerinde kullanılacak açık kaynaklı, özgür yazılımların seçim, güvenli geliştirme, test ve konfigürasyon özelliklerine dikkat edilmelidir.

---

[13] https://www.hurriyet.com.tr/yazarlar/umut-firat-eroglu/derin-konu-siber-guvenlik-41722712
[14] https://turk-internet.com/www-mucidi-tim-berners-lee-interneti-degistirmeye-hazirlaniyor/

5.2.2 Şifreleme

İkinci bir teknik özellik ise iletilerin (metin, ses, görüntülü bütün mesajların) ve sesli veya görüntülü iletişimin **uçtan-uca şifrelenmesidir**. Bu özellik, iletilerin sağlam ve güvenilir bir şifreleme yöntemiyle gönderenin cihazında şifrelenmesi ve sadece alıcıların cihazlarında çözülerek okunabilmesi en temel güvenlik önlemi olarak kabul edilmektedir.

Ancak mesaj içeriklerinin uçtan-uca şifrelenmesi çok önemli bir güvenlik önlemi olmasına rağmen, iletilere ait üst verilerin -özetle iletilerin içerikleri dışındaki alıcı ve gönderici bilgileri- iletinin taşınmasında bir gereklilik veya zorunluluk olarak kalması, gönderen ve alıcı hakkındaki üst verilere erişim ile kişilerin anlık ileti uygulamalarını nasıl kullandıkları, kimlerle mesajlaştıkları ve mesajları ne zaman gönderdikleri hakkında birçok veri oluşturmaktadır.

Signal, beta sürümünde "gizli gönderen (SealedSender)" özelliğini test etmektedir. Bu yöntemle, sunucunun gönderenleri doğrulama yeteneğini ortadan kaldırdığından, kullanıcıların gelen iletileri kimin gönderdiğini doğrulamaya devam etmesine ve kötüye kullanım amaçlı içerik alma olasılıklarını azaltmasına izin veren geçici çözümler eklenmektedir. En önemlisi, Signal yalnızca "gizli gönderen" mesajlarının, özellikle de birbirlerinin kişi listelerinde kalarak hâlihazırda güven oluşturmuş hesaplar arasında geçişine izin vermektedir.[15]

5.2.3 İletilerin Sunucuda Saklanma Durumu

Diğer bir özellik ise, her türlü ileti ve iletişimin hizmet sağlayıcının sunucularında saklanıp saklanmadığıdır. Çünkü, iletilerin kopyalarının herhangi bir nedenle **hizmet sağlayanın sunucularında saklanması**; söz konusu iletilerin, iletişimin ve eklerinin güvenliğini tehlikeye atan bir durumdur.

5.2.4 Süreli İleti Özelliği

İletilerin güvenliğine yönelik bir diğer özellik de **süreli ileti özelliği**dir. Bu özellik iletilerin belirlenen süre sonunda tüm ortamlardan kendiliğinden silinmesidir.

5.2.5 Üçüncü Kişi ve Kurumlarla Veri Paylaşımı

Genellikle bulut ortamında sunulan anlık ileti hizmetlerinde belki de en kritik özellik bu uygulamaların gerek kayıt aşamasında gerekse de uygulamaların kullanımı sırasında **toplanan kişisel veriler** ile **bu verilerin paylaşıldığı kişi, şirket ve kurumlar**dır. Anlık ileti uygulamaları genel olarak ad, soyad ve telefon numaralarının yanısıra kullanıcı cihaz bilgileri, konum verileri, adres defteri, arama ve mesaj kayıtları ile birlikte fotoğraf albümleri ve dosyalara yönelik bazı bilgileri de toplamaktadır.

5.2.6 Diğer Uygulamalarca Toplanan Veriler

Son dönemde tartışılan bir diğer kritik konu da bu uygulamaların kullanıcı cihazlarındaki **diğer uygulamalara ait ve o uygulamalar tarafından toplanan verileri de gözetleyip toplamaları**dır**.** Böylelikle kullanıcılar hakkında çok ayrıntılı profilleme fırsatına da sahip olunmaktadır. Bu **kullanıcı profilleri** satış, pazarlama, finansman gibi daha sıradan alanlardan politik yönlendirmelere kadar değişik alanlarda çok etkili olarak kullanılmaya başlamıştır.

[15] https://www.wired.com/story/signal-sealed-sender-encrypted-messaging/ (Ocak 2021)

5.2.7 Sunucuların Bulunduğu Ülkeler

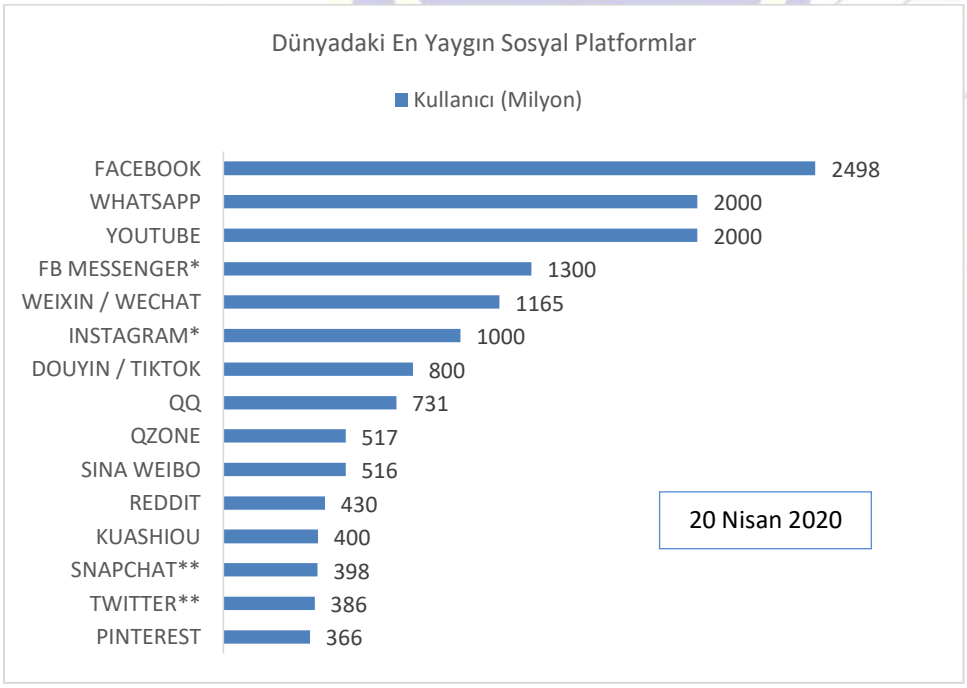
Son olarak anlık ileti hizmetinin sağlandığı **sunucularının bulunduğu ülkeler** de güvenlik açısından göz önünde tutulması gereken bir noktadır.

5.3 ANLIK İLETİ UYGULAMA ÖRNEKLERİ

Günümüzde oldukça yaygın olarak kullanılan anlık ileti uygulamalarını, birçok açıdan inceleyip değerlendirmek gerekmektedir. Çünkü, özellikle mobil cihazlardaki uygulamaların kullanım kolaylıkları, kullanıcı özellikleri ve yaygınlıklarının yanısıra gizlilik politikaları ile teknik özellikleri bazı benzerliklerin yanında büyük farklılıklar da gösterebilmektedir.

Kullanıcı özellikleri ve kullanım kolaylıklarının başında uygulamanın yüklenmesi ve sisteme kaydolmak gelmektedir. Anlık ileti uygulamaları kayıt için ad, soyad, telefon numaraları, e-posta adresleri gibi bir takım kişisel veriler istemektedir. Kullanımda ise, basit metin iletilerinin yanısıra ses, resim ve video ile birlikte çeşitli dosyaları ekleyerek de gönderme yetenekleri bu uygulamaların seçilmesinde önemli ölçütler niteliğindedir. Ayrıca masaüstü bilgisayar uygulamalarının varlığı ve bunların sunduğu özellikler yine kullanıcıların tercihlerinde önemli bir rol oynamaktadır. Etiketler (sticker), görüntülü sohbet (video chat), arkaplan, emoji ve ileti renklerinin ve resimlerinin kullanıcı tarafından değiştirilebilmesi gibi diğer özellikler de uygulamaya değer katmaktadır.

Bir diğer husus da bu uygulamaların erişilebilirlikleridir. Bu başta görme engelliler olmak üzere engelli bireylerin iletişimi açısından oldukça önemlidir.



Tablo 2 - Dünyadaki en yaygın sosyal platformlar ve kullanıcı sayıları (milyon kişi)[16]

16 https://wearesocial.com/blog/2020/04/digital-around-the-world-in-april-2020

5.3.1 Küresel Uygulamalar

5.3.1.1 WhatsApp

WhatsApp şirketi 2009 yılında kurulmuş olup mobil ortamda anlık mesajlaşma hizmetini 2010 yılında ücretsiz bir uygulama olarak, önce ABD'deki kullanıcıların hizmetine sunmaya başlamıştır. Benzer biçimde akıllı telefon kullanıcılarına yönelik diğer mobil mesajlaşma uygulamaları da geliştirilmiştir. WhatsApp dünya çapında 2,0 milyar kullanıcısı ile en büyük mobil mesajlaşma hizmetidir.

WhatsApp tarafından "kullanıcının telefon numarası, adres defterinde bulunan telefon numaralarını, grup ve liste bilgileri, kullanım ve kayıt bilgileri, uygulama mağazalarından veya ödeme işleme alan diğer üçüncü taraflardan ödeme makbuzları gibi bilgi ve onaylar, telefon donanım modeli, işletim sistemi bilgileri, tarayıcı bilgileri, IP adresi, telefon numarası dahil olmak üzere mobil ağ bilgileri ve cihaz tanımlayıcıları gibi bilgileri, konum özelliklerinin kullanılması durumunda (*ör. konumunuzu kişilerinizle paylaşmanız ya da yakındaki veya başkalarının sizinle paylaştığı konumları görüntülemeniz gibi durumlarda*), çerez (gözlemci) ve durum (çevrimiçi olma gibi) bilgileri, 3. Taraf bilgileri (*örneğin, tanıdığınız diğer kullanıcılar WhatsApp'ı kullandığında, mobil adres defterlerinde bulunan telefon numaranızı WhatsApp'a sağlayabilir (aynı şekilde siz de bu kişilerin bilgilerini sağlayabilirsiniz), size veya sizin de içinde bulunduğunuz gruplara mesaj gönderebilir ya da sizi arayabilirler*) gibi kişisel verilerin yanısıra 3. Taraf Sağlayıcılar ve 3. Taraf Hizmetlerden edindikleri kullanıcıya ait kişisel verileri toplayıp işlemektedir. [17]

WhatsApp uçtan uca şifreleme özelliği ile kendisini güvenli olarak tanımlayarak teslim edilemeyen iletilerin sunucularında en fazla 30 gün saklandığını belirtmiş, bunun dışında hiçbir verinin sunucularında saklanmadığını belirtmekle birlikte, Gizlilik Politikası'nda "Performansı artırmak ve medya mesajlarını daha verimli bir şekilde iletmek için, örneğin birçok kişi popüler bir fotoğrafı veya videoyu paylaşırken, bu içeriği sunucularımızda daha uzun bir süre saklayabiliriz." ifadeleri yer almaktadır.[18]

5.3.1.2 Signal

2013 yılında kurulan Signal, gizlilik savunucuları ve diğer aktivistler tarafından da uzun zamandır kullanılan açık kaynak kodlu bir yazılımı kullanmaktadır. Siber güvenlik konusunda adı çok yaygın olarak geçen Edward Snowden, 2015 yılında Signal uygulamasının en güvenli uygulama olduğunu söyledi.
Facebook'un WhatsApp'ı satın almasından sonraki politikalarından rahatsız olan WhatsApp'ın kurucusu ve CEO'su olan Brian Acton 2016 yılında şirketten ayrılarak Signal Vakfı'na 50 milyon $ bağışlamıştır.

Signal'in Tesla CEO'su Elon Musk ve Twitter CEO'su Jack Dorsey gibi birçok tanınmış kişi tarafından önerilmesi, Signal uygulamasını 2021'in başında Apple ve Google'ın uygulama mağazalarında üst sıralara çıkarttı.

Avrupa Birliği (AB) Komisyonu çalışanlarına kurum dışı mesajlaşmalarında Signal mesajlaşma uygulamasının "*genel anlık mesajlaşma için önerilen uygulama olarak seçildiğini*" bildirmiştir.[19]

Signal'in kullanıcı sayısının Ocak 2021 itibarı ile 50 milyonu geçtiği belirtilmektedir.

[17] https://www.whatsapp.com/legal/client
[18] https://www.whatsapp.com/legal/privacy-policy/?lang=en
[19] https://www.politico.eu/article/eu-commission-to-staff-switch-to-signal-messaging-app/

Ağustos 2018 itibariyle, Signal Protokolü WhatsApp, Facebook Messenger, Skype ve Google Allo'da kullanılmaya başlanmıştır. Google Allo, Skype ve Facebook Messenger'da, görüşmeler varsayılan olarak Signal Protokolü ile şifrelenmez; yalnızca isteğe bağlı bir modda uçtan uca şifreleme sunmaktadır.[20]

Geçmişte FBI, Signal uygulamasını kullanan bir kullanıcı hakkında bilgi almak için mahkeme yoluyla talepte bulundu. Signal'in sunabildiği tek veri, kullanıcının hesap oluşturma tarihi ve en son oturum açtığı zamandı.[21]

Signal, barındırma için Amazon Web Hizmetlerini kullanmaktadır. Ayrıca, Signal 2018 yılından beri IP adreslerini ve diğer üst verileri şifrelemek için çalışmaya başlamış[22] ve gizli gönderen özelliğini uygulamaya almıştır.

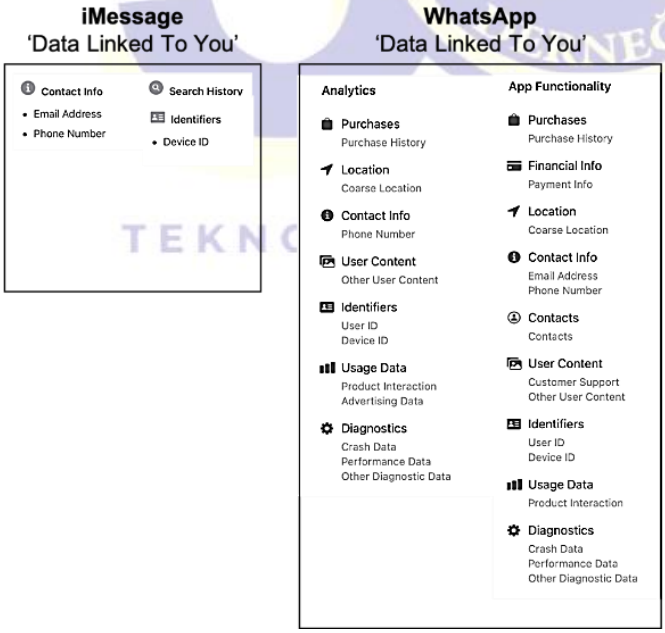
5.3.1.3 Telegram

400 milyon kullanıcısı olan Telegram, diğer güvenli mesajlaşma uygulaması seçeneklerinin aksine, varsayılan olarak uçtan uca şifrelemeye sahip değildir. Telegram'da uçtan uca şifrelemeyi etkinleştirmek için sohbet ayarlarında "gizli" modun seçilmesi ve bu seçimin mesajlaşılacak her bir kişi tarafından ayrı ayrı yapılması gerekmektedir. Ancak bu durumda bile, Telegram'ın tüm mesajlaşma özellikleri uçtan uca şifrelenmez.

Telegram'ın en popüler özelliklerinden biri olan "grup sohbetleri" uçtan uca şifreleme özelliğini desteklememektedir. Ayrıca, masaüstü uygulamasında da macOS dışında hiçbir platformda yani Windows ve Linux'ta uçtan uca şifreleme özelliği desteklenmemektedir.[23]

5.3.1.4 iMessage

1,3 milyar kullanıcısı olan iMessage uygulamasının kullanımı Apple cihazlarıyla sınırlıdır.



Tablo 3 - iMessage ile WhatsApp topladığı kişisel veriler

[20] https://en.wikipedia.org/wiki/Signal_(software)
[21] https://arstechnica.com/tech-policy/2016/10/fbi-demands-signal-user-data-but-theres-not-much-to-hand-over/
[22] https://www.wired.com/story/signal-sealed-sender-encrypted-messaging/
[23] https://shiftdelete.net/whatsapp-telegram-signal-karsilastirma-hangisi-daha-guvenli

5.3.1.5 Küresel Uygulamalar Karşılaştırma Tablosu

Özellik \ Platform	bip	Whatsapp	Telegram	Signal
Sahiplik	Turkcell (BiP A.Ş)	Facebook	Telegram	Signal Vakfı
Yazılım Yapılan Ülke	Türkiye %100 Yerli	ABD	Rusya	ABD
Verilerin Saklandığı Ülke	Türkiye (İstanbul & Ankara)	ABD	Rusya	ABD
Şifreleme	Şifreli *Uçtan Uca Şifreleme Yakında*	Uçtan Uca Şifreli Yedekler şifreli değil	Şifreli *Gizli Mesajlar Uçtan Uca Şifreli*	Uçtan Uca Şifreli
Açık Rıza Olmadan Verilerin İşlenmesi & Paylaşılması	Paylaşılmıyor	Paylaşıyor	Paylaşılmıyor	Paylaşılmıyor
Anlık Mesaj, Sesli & Görüntülü Görüşme, Medya, Doküman, Ses Kaydı Gönderimi	Var	Var	Var	Var
Acil Yardım Butonu (Deprem Afet)	Var	Yok	Yok	Yok
Grup Mesajlaşma Katılımcı Sayısı	1000	250	200K	150
Grup Sesli & Görüntülü Arama	HD Kalite	Standart Görüntü Kalitesi	Grup görüntülü arama yok	Standart Görüntü Kalitesi
Grup Görüntülü Görüşme Katılımcı Sayısı	10	8	Yok	5
Anlık Çoklu Dilde Tercüme	106 dil desteği	Yok	Yok	Yok

Tablo 4 - Bazı anlık ileti uygulamalarının güvenlik karşılaştırması[24]

5.3.2 Yerli Uygulamalar

5.3.2.1 BİP

Turkcell tarafından yerli çözüm olarak geliştirildiği[25] ve operatör bağımsız olarak 192 ülkede, 70 milyonu aşkın indirme, 30 milyonu aşkın kullanıcı tarafından kullanıldığı belirtilen BiP'in gizlilik politikasına baktığımızda kimlik ve iletişim bilgileri, kullanım verileri, konum verileri, ödeme verileri, cihaz verileri, iletişim verileri, yedekleme verileri ve rehberin toplandığı görülmektedir. Turkcell bu bilgilerin hizmet sağlayacılar, ortaklar ve danışmanlar ile paylaşabileceğini belirtmektedir. Ayrıca, elde edilen kişisel verilerin Avrupa Birliği dışındaki ülkeler dahil olmak üzere kullanıcının bulunduğu yargı alanı dışındaki ülkelere aktarabileceği ve bu ülkelerde saklanabileceği ifade edilmiştir."[26]

BİP tarafından kendi gizlilik politikasındaki işlenebilecek kişisel verilere ait kategoriler aşağıdaki gibidir:[27]

- ***Kimlik ve İletişim Bilgileri:*** *Telefon numarası, kullanıcı adı (rumuz), avatar, GSM operatörü ve hesabı güvenli tutmak için kullanılan şifreler;*
- ***Kullanım Bilgileri:*** *Cihazınızdan teknik ekipmanlar yoluyla toplanan teknik veriler, (içeriği hakkında hiçbir bilgi toplamaksızın) gönderilmiş iletilerin türü (yazılı mesaj, video vb.), aktif kullanılan zamanlar, kullanılan hizmetlerin türü, Uygulama arayüzüne ilişkin kullanım alışkanlıkları, Uygulamaya en son giriş yapılan tarih, Uygulamanın kullanımı sırasında meydana gelen hatalar ve hataya ilişkin bilgiler. İletişim türü (BiP Çağrıları, anlık mesajlar vb.), iletişimin süresi, tarihi ve tarafları, iletişim kurulan kişiler ile ilgili veriler. BiP, Uygulama üzerinden kurulan iletişiminizin içeriğiyle ilgili herhangi bir veri toplamaz.*

[24] https://www.ajanskamu.net/dijital-sosyal-medya/bip-whatsapp-telegram-ve-signal-in-guvenlik-ve-aciklari-bakimindan-h122557.html
[25] https://selcukcelik.org/turkcell-bip-teknik-ve-teknolojik-incelemesi/
[26] https://shiftdelete.net/whatsapp-telegram-signal-karsilastirma-hangisi-daha-guvenli
[27] https://bip.com/tr/gizlilik-politikasi/#KisiselVerilerinizHangiAmaclarlaIsleniyor?

- ***Kişiselleştirme Bilgileri ve Anketler:*** *Rumuz, Profil Fotoğrafı, Durum Bilgisi, Engellenen Numaralar. Uygulama aracılığıyla yapılan anketlerin sonuçlarına ilişkin veriler.*
- ***Konum Bilgileri:*** *Kullanıcıların konum ile ilgili fonksiyonları kullanmaları halinde cihazlarının ayarlarına bağlı olarak (yaklaşık) konumlarına ilişkin veriler.*
- ***Cihaz Bilgileri:*** *Cihaz modeli, cihazın işletim sistemi, tercih edilen telefon dili, kullanıcıların hangi operatörü kullandığına ilişkin bilgiler, ülke bilgilerine ilişkin veriler.*
- ***Yedekleme Bilgileri****: Kullanıcıların talep etmesi durumunda, iletişim verileri BiP tarafından yedeklenebilir.*
- ***Adres Defteri Bilgileri:*** *Telefon numaraları, ve kullanıcının cihazında depolanan Kişi Listesi.*

BiP sunucuları Türkiye'de bulunmakta olup, kullanıma ilişkin tüm veriler Türkiye'de saklanmaktadır.

Yurtdışında bulunan operatörlerin işbirliği kapsamında, kendi ülkelerinde BiP kullanımları doğrultusunda bu ülke kullanıcıları ile ilişkili veriler ilgili operatöre aktarılabilir ve o operatör sunucularında saklanabilir.

BİP Uygulamasının Google Play platformundaki tanımında belirttiği hangi kişisel verilere eriştiği bilgileri:

Bu uygulamanın şunlara erişimi vardır:[28]

Cihaz kimliği ve çağrı bilgileri
- read phone status and identity

Yer
- approximate location (network-based)
- precise location (GPS and network-based)

Kamera
- take pictures and videos

Depolama
- modify or delete the contents of your USB storage
- read the contents of your USB storage

Kablosuz bağlantı bilgileri
- view Wi-Fi connections

SMS
- receive text messages (SMS)
- send SMS messages
- read your text messages (SMS or MMS)
- receive text messages (MMS)
- edit your text messages (SMS or MMS)

Kişiler
- read your contacts
- find accounts on the device
- modify your contacts

Telefon
- directly call phone numbers
- read phone status and identity
- write call log
- read call log

Fotoğraflar/Medya İçerikleri/Dosyalar
- modify or delete the contents of your USB storage
- read the contents of your USB storage

Kimlik
- find accounts on the device
- add or remove accounts

Cihaz ve uygulama geçmişi
- read your Web bookmarks and history
- retrieve running apps

Mikrofon
- record audio

Diğer
- read sync statistics
- receive data from Internet
- run at startup
- draw over other apps
- read sync settings
- access Bluetooth settings
- prevent device from sleeping
- control vibration
- allow Wi-Fi Multicast reception
- install shortcuts
- send sticky broadcast
- view network connections
- pair with Bluetooth devices
- read Google service configuration
- control Near Field Communication
- create accounts and set passwords
- toggle sync on and off
- change your audio settings
- full network access

[28] https://play.google.com/store/apps/details?id=com.turkcell.bip&hl=tr&gl=US

BİP uygulaması yayımladığı gizlilik sözleşmesinde kişilerin adres defterlerini kopyaladığını belirtmektedir. Ancak Turkcell tarafından:

"BiP'te veri güvenliği, mesajların iletildiği cihazlar ve sunucular arasındaki bütün iletişimin uluslararası standartlara uygun biçimde TLS şifreleme yöntemiyle güvenli bir şekilde taşınması ile sağlanmaktadır. Bu sayede, herhangi bir üçüncü kişinin mesajlara erişmesi mümkün olmadığı gibi, mesajlar karşı tarafa iletilene kadar yüksek güvenlikli sunucularda şifrelenmekte; mesajın iletilmesiyle birlikte sunuculardan tamamen ve geri döndürülemeyecek şekilde silinmektedir.

Kullanıcıların, "mesaj yedekleme" seçeneğini kendi tercihleriyle aktif hale getirmeleri durumunda ise, ilgili veriler veri merkezlerinde kullanıcılar adına şifrelenerek saklanmaktadır. Ayrıca, Türkiye'deki BiP kullanıcıları arasındaki veri iletişimi yalnızca Türkiye'de bulunan sunucular üzerinden gerçekleştirilmekte ve BiP uygulama kodları da tamamen Türkiye'de tutulmakta; hiçbir bir veri yurtdışına çıkarılmamaktadır.

BiP'in servislerini sunabilmesi için, örneğin mesaj atmak, arama veya görüntülü görüşme yapmak, rehberde kayıtlı bir kişiye konum, albümden bir fotoğraf ya da bir belge göndermek istendiğinde, BiP, telefonun mikrofon, kamera, fotograf galerisi, rehber gibi ilgili kaynaklarına erişebilmek için kullanıcı iznini ister. Bu izin verilmedikçe de ilgili kaynak ve verilere erişim söz konusu olmaz.

Kullanıcılar arasındaki iletişimin ve kullanıcı verilerinin gizliliğinin korunması, BiP servisinin temelini oluşturmakta ve platformda yapılan tüm geliştirmeler bu temel üzerine inşa edilmektedir. BiP, kullanıcı verilerini reklam, promosyon veya teklif gibi ticari faaliyetler için üçüncü kişilerle paylaşmamaktadır. Kullanıcılar verilerinin üçüncü kişilere paylaşıma izin vermeden de BiP servislerinden faydalanmaya devam edebilirler. BiP Kullanıcı Şartlarının onaylanması veya Gizlilik Bildiriminde yer alan verilerin işlenmesine/paylaşılmasına yönelik aydınlatma amaçlı belirtilen açıklamalar kullanıcılar bakımından bu kapsamda bir izin verildiği anlamına gelmemektedir.

Yurtdışında bulunan operatörlerin işbirliği kapsamında, kendi ülkelerinde BiP kullanımları doğrultusunda bu ülke kullanıcıları ile ilişkili veriler ilgili operatöre aktarılabilir ve o operatör sunucularında saklanabilir."

olduğu belirtilmektedir.

Bu konuda kamuoyuna yansıyan aşağıdaki iddialar da bulunmaktadır:

- Turkcell'in başvurusunda bulunduğu patentler arasında en ilginç olanlardan bir tanesi mühendislerden Necmi KILIÇ'ın geliştirdiği ve 2020/17609 başvuru numarasıyla kayıtlara geçen 4 Kasım 2020 tarihli **Bir Müzik Öneri Sistemi** başlıklı patent başvurusu. Başvurunun kısa tanıtımında ise "*Bu buluş, kullanıcıların mobil cihazları üzerinde kullandıkları mesajlaşma uygulamasındaki (3) yazışmalardan doğal dil işleme (NLP-Natural language processing) ile duygu durumunun belirlenmesine ve belirlenen duygu durumuna göre kullanıcıya müzik önerisinde bulunulmasına imkân sağlayan bir sistem (1) ile ilgilidir*" deniliyor.[29]

[29] https://btdunyasi.net/turkcell-yazismalarimizin-icerigine-gore-muzik-onerecek-psikolojik-durumumuzu-analiz-edecek/

- **CURIO'yu duydunuz mu?** Duymadınız değil mi? Turkcell in mobil analitik yazılımı. Bu Turkcell BİP'in içi bununla bezenmiş. Sizin her türlü hareketinizi yazıyor bir yerlere kaydediyor! Ayrıca cihazınız ile ilgili her türlü bilgiyi de kaydediyor. Yok derlerse inanmayın. Turkcell neden bu BİP i ortaya çıkardı ki. Bilgiye sahip olan kazanır.[30]

5.3.2.2 DEDİ

Bilgi Teknolojileri ve İnternet Derneği (BTİDER) tarafından geliştirilen ve 2018'de yayınlanan yerli mesajlaşma uygulamasıdır.[31]

Dedi, güvenli mesajlaşma konusunda endüstri standartlarını belirleyen Signal uygulaması üzerine geliştirilmiştir. Kaynakları açıktır, herkes tarafından incelenebilir.[32]

Dedi'de arama ve mesajlaşmalar uçtan uca şifreleme yöntemi ile korunmaktadır. [33]

Dedi uygulamasının veri işleme politikasına göre:

HANGİ VERİLERİNİZİ İŞLİYORUZ?[34]

Hesap Bilgileriniz

Cep Telefonu Numaranız

Dedi uygulamasını kullanabilmeniz için öncelikle cep telefonunuz ile kayıt olmanız gerekmektedir. Telefon numaranız Türkiye'de bulunan sunucularımızda şifreli olarak saklanmaktadır.

Kullanıcı Adı ve Profil Resminiz

Hesabınıza opsiyonel olarak profil resmi ve kullanıcı adı ekleyebilirsiniz. Bilgilerinizi her zaman Dedi'nin "Ayarlar" kısmından güncelleyebilirsiniz. Bu bilgiler Türkiye'de bulunan sunucularımızda şifreli olarak saklanmaktadır.

Kimlik ve İletişim Bilgileriniz

Destek almak, şikayet ya da öneride bulunmak amaçlarıyla bizimle iletişime geçmeniz halinde paylaştığınız bilgiler yalnızca bu amaçlarla sınırlı olarak kullanılacak ve sonrasında tüm bilgiler silinecektir.

Kullanım Bilgileriniz

Mesajlarınız

Mesajlarınız uçtan uca şifrelendiğinden Dedi veya üçüncü taraflar mesajlarınızın içeriğine ulaşamazlar. Mesajlarınız Dedi'nin sunucularında değil, Dedi'yi kullandığınız cihazınızda saklanır. Ancak iletilmemiş mesajlarınız (Örneğin mesajın alıcısının telefonunun kapalı olması sebebiyle) sunucularımızda mesaj iletilene kadar geçici bir süreyle şifreli olarak saklanır. Bunun yanında

[30] https://selcukcelik.org/turkcell-bip-teknik-ve-teknolojik-incelemesi/
[31] https://www.webtekno.com/btider-mesajlasma-uygulamasi-dedi-ios-android-indir-h104577.html
[32] https://dedi.com.tr/
[33] https://dedi.com.tr/
[34] https://www.dedi.com.tr/privacy-tr.html

medya mesajları, iletimlerini daha verimli hale getirmek amacıyla sunucularımızda geçici bir süreyle şifreli olarak saklanır.

Dedi'nin mesajlarınıza erişimi bulunmamaktadır. Uygulamanın etkin bir şekilde çalışmasını sağlamak amacıyla mesajlaşmaya ilişkin kılavuz verileri (mesajlaşmanın tarihi ve tarafları gibi) Türkiye'de bulunan sunucularımızda şifreli olarak saklanmaktadır.

Sohbet Grupları

İçerisinde bulunduğunuz sohbet grupları Türkiye'de bulunan sunucularımızda şifreli olarak saklanmaktadır.

Kişi Listesi Bilgileriniz

Dedi'yi etkin olarak kullanabilmek için Dedi'nin rehberinizdeki hangi kişilerin Dedi kullanıcısı olduğunu göstermesini tercih edebilirsiniz. Bu durumda sizin ve rehberinizdeki kişilerin mahremiyeti tamamen korunarak kişi listeniz Türkiye'de bulunan sunucularımızda şifreli olarak saklanır.

Teknik Bilgiler

Arama ve mesajlaşmaların etkin çalışmasını, bildirim alımını ve hesabın güvenliğini sağlamak için anahtarlar gibi ilaveten teknik bilgiler sunucularımızda şifreli olarak saklanır. Dedi bu teknik bilgileri uygulamanın çalışması için gerekli olan minimum düzeyde tutar.

VERİLERİNİZİ KİMLERE AKTARIYORUZ?

Dedi uygulamasının etkin bir şekilde çalışmasını sağlamak amacıyla üçüncü taraflarla birlikte çalışabilmekteyiz. Örneğin, uygulamaya kayıt esnasında cep telefon numaranızın doğrulanması amacıyla cep telefonu numaranız ilgili operatöre aktarılmakta ve böylece doğrulama kodunun tarafınıza iletilmesi sağlanmaktadır. Verileriniz yalnızca Dedi'nin fonksiyonları için zorunlu olduğu durumlarda aktarılmakta, hizmet veya ürün tanımı gibi herhangi bir ticari amaçla kesinlikle aktarılmamaktadır.

Dedi, hukuki bir yükümlülük dahilinde yukarıda bahsedilen verileri yetkili makamlar ile paylaşabilir. Ayrıca Dedi, kendi ve üçüncü kişilerin haklarını, güvenliğini veya mülkiyetini korumak için yukarıda bahsedilen verileri yetkili makamlar ile paylaşabilir.

Verileriniz Dedi'nin Türkiye'de yer alan sunucularında bulunmakta ve yurt dışına aktarılmamaktadır.

VERİLERİNİZİ NASIL SAKLIYORUZ?

Kişisel verilerinizi yalnızca yukarıda amaçlar için gerekli olan sürelerle şifreli olarak Türkiye'deki sunucularda saklıyoruz.

Dedi, kişisel verilerinizi yürürlükteki mevzuatın belirlediği süreler boyunca saklamaktadır.

DEDİ Uygulamasının Google Play platformundaki tanımında belirttiği hangi kişisel verilere eriştiği bilgileri:

Bu uygulamanın şunlara erişimi vardır:

Depolama
modify or delete the contents of your USB storage
read the contents of your USB storage
Telefon
read phone status and identity
Kablosuz bağlantı bilgileri
view Wi-Fi connections
Yer
approximate location (network-based)
precise location (GPS and network-based)
Kimlik
find accounts on the device
modify your own contact card
read your own contact card
Fotoğraflar/Medya İçerikleri/Dosyalar
modify or delete the contents of your USB storage
read the contents of your USB storage
Cihaz kimliği ve çağrı bilgileri
read phone status and identity
Takvim
add or modify calendar events and send email to guests without owners' knowledge
read calendar events plus confidential information
Kişiler
read your contacts
find accounts on the device
modify your contacts
Kamera
take pictures and videos
Mikrofon
record audio
Diğer
send WAP-PUSH-received broadcast
receive data from Internet
run at startup
draw over other apps
read sync settings
disable your screen lock
prevent device from sleeping
control vibration
connect and disconnect from Wi-Fi
install shortcuts
send sticky broadcast
view network connections
pair with Bluetooth devices
change network connectivity
create accounts and set passwords
use accounts on the device
toggle sync on and off
change your audio settings
set wallpaper
full network access

Dedi uygulamasının sahibi olan BTİDER'in resmi sitesinde ve uygulamanın kendi sitesinde kullanım koşulları ve gizlilik sözleşmesine ilişkin bir bilgi bulunmamaktadır. Uygulamayı kurmadan gizlilik sözleşmesine ulaşma olanağı gözükmemektedir. Bu nedenle KVKK uyumu konusunda ciddi şüpheler uyandırmaktadır. Ayrıca Dedi, açık kaynak kodlu Signal protokolünü kullandığını belirtmesine rağmen kaynak kodlarına erişim söz konusu olmadığı için özgür yazılım olarak değerlendirilememektedir.

6 WHATSAPP SÖZLEŞME DEĞİŞİKLİĞİ

WhatsApp'tan yapılan resmi paylaşımda son gönderilen sözleşme ile gelen değişikliğin WhatsApp'taki **işletme hesapları** ile yapılan mesajlaşmalarla sınırlı olduğu belirtilmektedir. Ayrıca, burada da basit bir mantıkla, **işletme hesapları** ile yapılan sohbetlerden elde edilebilecek kişisel verilerin ticari amaçlarla kullanılabileceğinin anlaşılacağı vurgulanmıştır.

Kullanıcılara gönderilen yeni sözleşmede;
"[…] Mesajlarınız.

- *Hizmetlerimizi size sunmak üzere izlediğimiz olağan iş akışında mesajlarınızı saklamayız.*
- *Mesajlarınız (sohbetleriniz, fotoğraflarınız, videolarınız, sesli mesajlarınız, dosyalarınız ve konum paylaşım bilgileriniz dahil) teslim edildikten sonra sunucularımızdan silinir.*

- *Mesajlarınız kendi cihazınızda saklanır.*
- *Gönderdiğiniz bir mesaj çevrimdışı olmanız gibi bir sebepten ötürü hemen teslim edilemezse mesajı en fazla 30 gün boyunca sunucularımızda tutabiliriz ve bu süre içinde mesajı teslim etmeye çalışırız. 30 günden sonra hâlâ teslim edilmemişse bu mesajı sileriz.*
- *Pek çok kişinin popüler bir fotoğrafı veya videoyu paylaşması gibi durumlarda performansı iyileştirmek ve medya mesajlarını daha verimli bir şekilde iletmek amacıyla bu içerikleri sunucularımızda daha uzun bir süre boyunca tutabiliriz.*
- *Ayrıca, mesajlaştığınız kişiler ve siz uygulamamızın 2 Nisan 2016'dan sonra kullanıma sunulmuş sürümlerinden birini kullanıyorsanız Hizmetlerimizde uçtan uca şifreleme işlevini sunarız. Bu işlev, varsayılan olarak açık durumdadır. Uçtan uca şifreleme, hem bizim hem de üçüncü tarafların okumasını önlemek amacıyla mesajlarınızın şifrelendiği anlamına gelir."*

ifadeleri yer almaktadır.

Bu değişiklik ile WhatsApp uygulamasını kullanmaya devam etmek isteyen kullanıcılar bu koşulları kabul etmek zorunda bırakılmışlardır. Değişikliği onaylamayan kullanıcıların 8 Şubat 2021'den sonra uygulamayı kullanamayacakları belirtilmiş ancak, daha sonra bu süre 15 Mayıs 2021 tarihine ertelenmiştir. Bu erteleme ile sözleşme değişikliğinde geri adım atılmamıştır.

WhatsApp'ın yöneticisi olan Will Cathcart, tepkiler üzerine paylaştığı mesajda özetle; kişisel kullanıcıların kendi aralarındaki mesajlaşmaların bundan önce olduğu gibi yine uçtan uca şifreleme yöntemi ile korunacağını ve bu yöntemin, verilerin 3. şahıslara geçmesini olanaksız kıldığını belirti. Bu yöntemi her zaman önemsediklerini ve kişisel kullanıcıların karşılıklı gizliliğini her zaman koruyacaklarını belirten Will Cathcart, değişikliğin WhatsApp'taki işletme hesapları ile yapılan mesajlaşmalarda olduğunu belirtti. Burada da basit bir mantıkla, işletme hesapları ile yapılan sohbetlerden elde edilebilecek verilerin ticari amaçlarla kullanılabileceğini; bunun ise birçok sosyal medya uygulamasının yanı sıra Google ve Facebook'un diğer uygulamalarının da zaten o platformlardaki beğeni, takip, izleme gibi aktivitelerden yaptığını belirtti.

WhatsApp şirketi yaptığı açıklamada, yeni güncellemenin mesajlaşma sistemini değiştirmeyeceğini; kullanıcıların WhatsApp üzerinden bir işletmeye mesaj göndermesi için yeni seçenekler içerdiğini, verilerin nasıl toplandığı ve kullanıldığı konusunda daha fazla şeffaflık sağlandığını belirtti. Ayrıca, güncellemenin WhatsApp'ın Facebook ile veri paylaşma yeteneğini değiştirmediği iddia edildi.

7 ÇİFTE STANDART

WhatsApp tarafından ülkelere göre farklı uygulama yapıldığı görülmüştür. Bu sürecin başında WhatsApp ve Facebook sözleşme değişikliği konusunda ön bilgi vermek üzere İrlanda Veri Koruma Komisyonu'na başvurarak AB ülkeleri açısından bir değişikliğin olmayacağını taahhüt etmiştir. Dolayısıyla AB'deki muhatap düzenleyici kurum olarak İrlanda Veri Koruma Komisyonu yeni WhatsApp Hüküm ve Koşullarına herhangi bir itirazda bulunmamıştır.

WhatsApp'ın kendisi de bu güncelleme kapsamında dünyanın herhangi bir yerindeki veri paylaşım uygulamalarında hiçbir değişiklik olmadığını iddia etmiştir.

Bu değişiklikle ilgili yalnızca İtalyan kamuoyunda tereddütler oluşması üzerine İtalyan veri koruma otoritesi olan "Garante"nin WhatsApp'ın Gizlilik Politikası güncellemesiyle ilgili açıklama yapmıştır. Buna göre, "*Politika güncellemesinin arkadaşlarınız veya ailenizle olan mesajlarınızın gizliliğini hiçbir şekilde etkilemediğini veya İtalyan kullanıcıların Facebook ile yeni veri paylaşım uygulamalarını kabul etmelerini gerektirmediğini açıklığa kavuşturmak istiyoruz"* demiştir.

GDPR'nin tek noktadan yönetim mekanizması, sınır ötesi şikayetlerin, bir şirketin ana bölgesel tabanına sahip olduğu (WhatsApp örneğinde İrlanda) bir lider veri sorumlusu aracılığıyla yönlendirilmesi anlamına gelmektedir. WhatsApp'ın sözleşme değişikliği konusunda İrlanda Veri Koruma Komisyonu, mevcut haliyle WhatsApp'ın güncellenmiş Şartlar ve Koşulları'nda bir sorun olmadığını belirtmiştir.

Bununla birlikte, İtalyan Veri Koruma Otoritesi (Garante) GDPR uyarınca, diğer Veri Koruma Otoriteleri (DPA), kullanıcıların verilerine yönelik acil bir risk olduğuna inandıklarında kendi mevzuatlarına göre hareket etme yetkisine sahip olduklarını beyan etmiştir. [35]

AB ülkelerine ilişkin uygulaması konusunda önden bilgi veren WhatsApp ve Facebook'un aynı tutumu Türkiye için göstermeyerek çifte standart uyguladığı değerlendirilmektedir.

WhatsApp bu sözleşme değişikliği kapsamına AB ülkelerini almazken içinde Türkiye'nin de bulunduğu diğer ülkelerde ise zorunlu kılmıştır. Avrupa ve diğer ülkeler arasındaki bu farklı uygulamanın temelinde GDPR düzenlemelerinin (General Data Protection Regulation) caydırıcı gücü yatmaktadır. Bu ve benzeri nedenlerle 2016 yılından beri yürürlükte olan 6698 sayılı KVKK'nın (Kişisel Verilerin Korunması Kanunu) On Birinci Kalkınma Planı'nda da öngörüldüğü üzere, AB ülkelerinde kişisel verilere sağlanan koruma düzeyine ulaşacak şekilde hızla iyileştirilmesi gerekmektedir.

8 ANLIK İLETİ HİZMETLERİNDE YERLİLİK VE SÜRDÜRÜLEBİLİRLİK

WhatsApp tarafından Facebook ile veri paylaşım politikasındaki değişikliği ve bu değişikliğin dayatılma tarzı, WhatsApp hizmetinin dünya çapındaki tüm kullanıcıları gibi Türkiye'deki kullanıcıları da fazlaca rahatsız etti.

WhatsApp'ın yeni politikasının yürürlük tarihi 8 Şubat 2021'den 15 Mayıs 2021 tarihine ertelenmiştir. Buna rağmen WhatsApp uygulamasının alternatiflerini arayan kişi sayısında çok ciddi bir artış görülmektedir.

Diğer ülkelerde olduğu gibi ülkemizde de bu arayışların bir bölümü yerel seçeneklere yönelmektedir. Yerli çözümlerin önemi TBD tarafından yayımlanan "Yerli ve Milli Yazılım Endüstrisi Raporu"nda incelenmiştir.[36]

[35] https://techcrunch.com/2021/01/14/confusion-over-whatsapps-new-tcs-triggers-privacy-warning-from-italy/

[36] https://www.tbd.org.tr/tbd_yerli_milli_yazilim_endustrisi_raporu_surum1/

8.1 YAZILIM GELİŞTİRME

Anlık ileti hizmeti uygulamalarında yerlilik ve milliliğin mümkün olup olmadığı tartışılması gereken bir konudur.

Yazılım geliştirme süreci uygulamaların, çerçevelerin veya diğer yazılım bileşenlerinin oluşturulması ve sürdürülmesinde yer alan analiz, tasarım, geliştirme, test, belgeleme ve bakım ve destek aşamalarının tamamını içermektedir.

Yazılımın teknolojik gelişmeler, değişen gereksinimler ve kullanıcı memnuniyeti göz önüne alındığında uzun süre varlığını sürdürebilmesi için bakım ve destek önemlidir. Tahmin edilenin aksine bakım ve destek süreçleri yazılım maliyetlerinin beklenenden daha büyük bir kısmını oluşturmaktadır. Belirli bir yazılıma uzun süre bakım ve destek hizmeti sağlanması, söz konusu yazılımın teknolojideki gelişmelere ayak uydurabildiği ve zaman içinde değişen gereksinimleri uzun süre karşılayabildiğini göstermektedir. Anlık ileti uygulamaları küresel yaygınlığı, çok çeşitli veri kullanma, şifreleme, anlık işlem sayısı, aktardığı veri çeşidi gibi özellikleri ile ayrı bir kategoride değerlendirilmelidir. Bu nedenle büyük ölçekte talepleri karşılayarak kesintisiz hizmet sunabilecek insan gücüne, donanım ve iletişim altyapılarına gereksinim duymaktadır.

Diğer taraftan, kişisel verilerin gizliliği konusundaki anlık ileti uygulamalarının doğru değerlendirilebilmesi için önerilmesi gereken yerli olmaları kadar açık kaynak kodlu ve özgür yazılım olmalarıdır. Örneğin, anlık ileti hizmetleri konusunda kamuoyunda öne çıkan BİP ve Dedi uygulamaları güvenilirlik, güvenlik ve şeffaflık konusunda en önemli ölçüt olan açık kaynak kodlu ve *özgür yazılım* olma ölçütünü karşılamamaktadırlar; [37] kaynak kodları açık değildir. Dedi uygulaması Signal'in açık kaynak kodlu yazılımını kullandığını belirtmektedir.

8.2 ALTYAPI GEREKSİNMELERİ

Bu uygulamaların üzerinde çalışacağı **donanım parkı** ve **iletişim alt yapısı** ile **enerji gereksinimi** bu hizmetlerin kabul edilebilir ölçeklerde sunulabilmesi için öne çıkan altyapıların başında gelir. Bu hizmetlerin niteliği gereği 7/24 sürekli ve kesintisiz hizmet vermek üzere **işletim ve bakım desteği** kadar gereksinim duyulan **nitelikli insan gücü** de önemlidir. Bu tür uygulamaların hizmet verdiği platform olarak büyük ölçekli veri merkezlerinin kullanıldığı görülmektedir.

Verilerin yerelde saklanması durumunda belli standartlarda transfer edilmesi ve nasıl saklandığının denetlenebilirliği önem kazanmaktadır.

8.3 İŞLETME VE SÜRDÜRÜLEBİLİRLİK

Başarılı ve yaygın olarak kullanılan anlık ileti hizmetleri bütün dünyada ücretsiz olarak sağlanmaktadır. Ancak, yatırım ve işletme maliyetlerinin karşılanması amacıyla hazırlanan iş planlarında "veri"nin olmazsa olmaz yeri bulunmaktadır.

[37] https://selcukcelik.org/turkcell-bip-teknik-ve-teknolojik-incelemesi/

Ayrıca, Türkiye'de veri merkezi işletim maliyetleri yurt dışındaki benzerlerine göre çok yüksektir. Özellikle elektrik dünyaya kıyasla çok pahalıdır. Ek olarak, internet için gerekli olan fiber optik altyapısı yetersiz olup genel olarak iletişim maliyetleri çok yüksektir. Aynı zamanda yerli veri merkezi şirketleri yetişmiş eleman bulamamaktan, bulduklarını da uzun süre çalıştıramamaktan şikayetçidir.

Bu ücretsiz olarak sağlanan hizmeti sürdürebilmek için yeterli finansmana ve sağlıklı bir iş planına gereksinim olduğu çeşitli örneklerde de görülmektedir.

8.3.1 Signal Örneği

21 Şubat 2018'de Moxie Marlinspike ve WhatsApp'ın kurucu ortağı Brian Acton kâr amacı gütmeyen bir kuruluş olan Signal Foundation'ın kurulduğunu duyurdu. Vakıf, Eylül 2017'de WhatsApp'ın ana şirketi Facebook'tan ayrılan Acton'dan 50 milyon dolarlık bir fonla çalışmaya başladı. Basın Özgürlüğü Vakfı daha önce Signal projesinin mali sponsoru olarak görev yapmış ve vakfın kâr amacı gütmeyen statüsü beklemedeyken proje adına bağış kabul etmeye devam etmişti.

İlk 50 milyon dolarlık finansman, Brian Acton'dan yeni kâr amacı gütmeyen Signal Technology Foundation'a bağış olarak değil, kredi olarak sağlanmıştı. 2018 yılı sonunda, teminatsız ve %0 faizli olan bu kredi 28 Şubat 2068'de geri ödenecek biçimde 105.000.400 dolara yükseltildi[38].

8.3.2 Önemli Bir Ders: Hindistan Örneği

2012 yılında kurulan mesajlaşma uygulamasını geliştiren Hike Messanger şirketi, 2016 yılında yeni yatırımcılar Çinli internet devi Tencent ve imalat firması Foxconn liderliğinde 175 milyon dolarlık fon sağlamıştır. WeChat ile mesajlaşmaya öncülük eden şirket Tencent başta olmak üzere Tiger Global, Bharti ve SoftBank ve ABD merkezli bazı stratejik yatırımcıları da Hike Messanger firmasına 250 milyon dolardan fazla fon sağlanmasına katkıda bulunmuşlardır.[39]

Aynı yıl şirkete 1,4 milyar dolar değer biçilmiştir.

Ne var ki, tüm bu finansman desteğine rağmen Hike Messenger şirketi Hindistan'da WhatsApp'a alternatif olarak geliştirilen mesajlaşma uygulaması StickerChat'i 2021 yılı başında kapattığını duyurdu.[40]

9 KAMU KURUMLARININ YAKLAŞIMLARI

2021 yılı başında WhatsApp tarafından kullanıcılarına gönderilen sözleşme değişikliği dayatması üzerine Türkiye'de ve Hindistan'da ciddi kamuoyu tepkisi oluştu. Bu tepkiler üzerine önce Rekabet Kurulu Facebook ve WhatsApp hakkında resen soruşturma başlattı ve WhatsApp verilerinin paylaşılması zorunluluğunu durdurdu.

[38] https://en.wikipedia.org/wiki/Signal_Foundation
[39] https://techcrunch.com/2016/08/16/indias-whatsapp-rival-hike-raises-175m-led-by-tencent-at-a-1-4b-valuation/
[40] https://techcrunch.com/2021/01/18/tencent-backed-hike-once-indias-answer-to-whatsapp-has-given-up-on-messaging/

Ardından, Kişisel Verileri Koruma Kurulu 12.01.2021 tarihli ve 2021/28 sayılı Kararı ile WhatsApp Inc. hakkında resen inceleme başlatılmasına karar vermiştir. Sürece ilişkin olarak 08.02.2021 tarihinde Kurul tarafından yeni bir değerlendirme yapılacağı kamuoyuna duyurulmuştur.

9.1 REKABET KURUMU KAMUOYU AÇIKLAMASI

Rekabet Kurulu Facebook ve WhatsApp hakkında resen soruşturma başlattı ve WhatsApp verilerinin paylaşılması zorunluluğunu durdurdu (11.1.2021)[41]

> *"Rekabet Kurulu'nun 11.01.2021 tarihli ve 21-02/25-M sayılı kararıyla, WhatsApp kullanıcılarına getirilen veri paylaşma zorunluluğu hakkında Facebook Inc., Facebook Ireland Ltd., WhatsApp Inc. ve WhatsApp LLC (hepsi birlikte "Facebook" olarak anılacaktır) hakkında 4054 sayılı Rekabetin Korunması Hakkında Kanun'un 6. maddesinin ihlal edip edilmediğinin tespiti amacıyla resen soruşturma açılmıştır.*
>
> *Bilindiği üzere; son günlerde, WhatsApp kullanıcılarına, WhatsApp kullanım koşullarının ve gizlilik ilkesinin güncelleneceğine ilişkin bilgilendirme yapılmış, söz konusu bilgilendirmede "kullanıcıların WhatsApp'ı kullanmaya devam edebilmeleri için WhatsApp verilerinin Facebook şirketleri ile paylaşılmasına onay vermeleri gerektiği, aksi halde 8 Şubat 2021'den itibaren WhatsApp'ı kullanamayacakları" belirtilmiştir. Bu haliyle güncelleme, daha fazla verinin Facebook tarafından toplanmasını, işlenmesini ve kullanılmasını içermektedir.*
>
> *Alınan kararda ayrıca söz konusu uygulamaların soruşturma sonucunda alınacak nihai karara kadar ciddi ve telafi olunamayacak zararlar doğurma ihtimalini haiz olduğundan 4054 sayılı Kanun'un 9. maddesi çerçevesinde geçici tedbir alınması ve bu kapsamda Facebook'un Türkiye'de, WhatsApp kullanıcılarının verilerinin 8 Şubat 2021 tarihinden itibaren başka hizmetler için kullanılmasına yönelik getirdiği koşulları durdurması ve bu koşulları kabul eden veya bilgilendirmeyi alarak kabul etmeyen tüm kullanıcılara Facebook'un veri paylaşımını içeren yeni koşulları durdurduğunu anılan tarihe kadar bildirmesi gerektiğine karar verilmiştir.*
>
> *Kamuoyuna saygıyla duyurulur."*

9.2 KİŞİSEL VERİLERİ KORUMA KURUMU KAMUOYU DUYURUSU

"WHATSAPP UYGULAMASI HAKKINDA KAMUOYU DUYURUSU [42]

> *Bilindiği üzere; 7 Nisan 2016 tarihli Resmî Gazete'de yayınlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 2 nci maddesinde "Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi*

[41] https://www.rekabet.gov.tr/tr/Guncel/rekabet-kurulu-facebook-ve-whatsapp-hakk-14728ae4f653eb11812700505694b4c6
[42] https://kvkk.gov.tr/Icerik/6856/WHATSAPP-UYGULAMASI-HAKKINDA-KAMUOYU-DUYURUSU

bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır" hükmü yer almaktadır.

Kişisel verilerin işlenebilmesi için ise, Kanunun 5 inci ve 6 ncı maddelerinde yer alan işleme şartlarından herhangi birinin mevcut olması gerekmektedir. Kanunun 5 inci maddesinin (2) numaralı fıkrasına göre; "kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması," işleme şartlarından herhangi birinin varlığı halinde kişisel veriler işlenebilecektir. Bu şartların bulunmadığı durumlarda ise kişisel veriler ancak ilgili kişinin açık rızası alınmak suretiyle işlenebilecektir.

Kanunun 3 üncü maddesinde açık rıza; "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" olarak tanımlanmış olup, buna göre açık rızanın üç unsuru bulunmaktadır:

- *Belirli bir konuya ilişkin olması,*
- *Rızanın bilgilendirmeye dayanması,*
- *Özgür iradeyle açıklanması.*

Söz konusu unsurlar açısından değerlendirildiğinde açık rıza, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile hukuka uygun şekilde onay vermesi anlamını taşımaktadır. Açık rızanın bir diğer önemi de veri sorumlusuna, gerçekleştireceği kişisel veri işleme faaliyeti konusunda yol göstermesidir. Kişi açık rıza açıklaması ile aslında veri sorumlusuna kendi hukuksal değerine ilişkin verdiği kararı bildirmiş olmaktadır. Açık rıza, ilgili kişinin işlenmesine izin verdiği verinin sınırlarını, kapsamını, gerçekleştirilme biçimini ve süresini de belirlemesini sağlayabilmektedir. Bu anlamda açık rıza, rıza veren kişinin olumlu irade beyanını içermelidir.

Kişisel verilerin işlenmesine açık rıza vermek, kişiye sıkı sıkıya bağlı bir hak olduğundan verilen açık rıza geri alınabilir. Bu bağlamda kişisel verilerin geleceğini belirleme hakkı ilgili kişiye ait olup, kişi dilediği zaman veri sorumlusuna vermiş olduğu açık rızasını geri alabilir. Ancak, geri alma işlemi ileriye yönelik sonuç doğuracağından, açık rızaya dayalı olarak gerçekleştirilen tüm faaliyetler geri alma beyanının veri sorumlusuna ulaştığı andan itibaren veri sorumlusu tarafından durdurulmalıdır. Bir diğer deyişle, geri alma beyanı veri sorumlusuna ulaştığı andan itibaren hüküm doğurur.

*Kişisel verilerin işlenmesinde hukuki sebep olarak "açık rıza"nın belirlenmesinin söz konusu olduğu ve verilen hizmetin açık rıza şartına bağlandığı hususlara ilişkin olarak 2 Ağustos 2018 tarihinde Kurum internet sayfasında, Kişisel Verileri Koruma Kurulunun (**Kurul**) 16.02.2018 tarihli*

ve 2018/19 sayılı Kararının özeti[43] yayınlanmıştır. Söz konusu Kurul kararında da belirtildiği üzere, öncelikle kişisel verilerin işlenmesi sırasında ilgili kişilerden alınan açık rıza, veri sorumluları tarafından bir hizmetin ifası için ön şart olarak ileri sürülemeyecektir.

Kanunun 4 üncü maddesi uyarınca kişisel verilerin, hukuka ve dürüstlük kurallarına uygun, belirli, açık ve meşru amaçlarla ve işlenme amacı ile bağlı, sınırlı ve ölçülü olma ilkelerine uygun olarak işlenmesi, hangi kişisel verilerin işleneceği veya hangi amaçlarla kimlere aktarılacağı hususlarında gerekli bilgilendirmenin yapılmış olması ve her bir işleme/aktarma faaliyetine yönelik seçenek sunulmak suretiyle ayrı ayrı açık rıza alınması gerekmektedir.

Diğer taraftan, Kanunun "Kişisel verilerin yurt dışına aktarılması" başlıklı 9 uncu maddesinde; kişisel verilerin, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamayacağı; ancak anılan hükmün ikinci fıkrası uyarınca Kanunun 5 inci maddesinin ikinci fıkrası ile özel nitelikli kişisel veriler bakımından 6 ncı maddesinin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması, yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul izninin bulunması kaydıyla kişisel verilerin ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabileceği düzenlenmiştir.

WhatsApp Inc. tarafından, WhatsApp uygulamasını kullanmak isteyen kullanıcıların kişisel verilerinin işlenmesine ve yurtdışında bulunan üçüncü taraflara aktarılmasına rıza verilmesini içerecek şekilde kullanım şartlarının güncellendiği, bu kapsamda rıza vermeyen kullanıcıların uygulamayı kullanamayacağına ve hesaplarının silineceğine dair kullanıcılara bilgilendirme iletildiği tespit edilmiştir.

Söz konusu bilgilendirme metninde yönlendirme yapılan Gizlilik Politikasında ise, hangi verilerin hangi amaçlarla işleneceği ifade edilmekle birlikte, işlenen kişisel verilerin WhatsApp Inc. tarafından yurtdışında yerleşik bulunan hizmet aldığı ve hizmet verdiği Facebook grup şirketleri, tedarikçileri, iş ortakları, hizmet sağlayıcıları ve diğer üçüncü taraf veri sorumluları gibi net olarak belirli olmayan taraflara teknik destek, teslimat ve diğer hizmetleri sağlamak, araştırma yapmak, pazarlama ve anket vb. gibi yine belirli olmayan amaçlarla aktarılacağının ifade edilmekte olduğu görülmektedir.

Kişisel verilerin, yurtdışında yerleşik bir veri sorumlusu olan WhatsApp Inc. tarafından işlenmesine ve yurtdışında yerleşik başka veri sorumlularına aktarılmasına ilişkin açık rıza alınması hususunda yapılan ön değerlendirme sonucunda;

- *Kullanıcılardan kişisel verilerinin işlenmesine ve yurtdışında yerleşik üçüncü taraflara aktarılmasına yönelik rıza alınması işleminin ayrıştırılmadığı ancak kullanıcıların kişisel verilerinin işlenmesine rıza verirken yurtdışında başka bir veri sorumlusuna aktarılmasına rıza vermeyebileceği dikkate alındığında söz konusu uygulamanın kullanım yaygınlığı da göz önünde bulundurularak bu durumun Kanunda belirlenen açık rızanın unsurlarından "özgür iradeyle açıklanması" açısından bir ihlal oluşturup oluşturmadığı,*

[43] https://kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi

- *Yurtdışında bulunan başka bir şirkete aktarım yapılmak şartıyla uygulamanın kullanılmasına izin verilmesinin Kanunun 4 üncü 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 vermediği,*
- *Sunulan hizmetin açık rıza şartına bağlanmış olmasının verilen açık rızayı sakatlayabileceği bu durumun da kişisel verilerin hukuka aykırı işlenmesi sonucunu doğurabileceği dikkate alındığında Whatsapp Inc. tarafından yapılan güncelleme ile hizmetin rıza şartına bağlanması durumunun ortaya çıkıp çıkmadığı,*
- *WhatsApp Inc. tarafından yurtdışında yerleşik veri sorumlularına yapılacak aktarım hususunda Kanunun 9 uncu maddesi hükümlerine aykırılık olup olmadığı*

hususları açısından, Kişisel Verileri Koruma Kurulunun 12.01.2021 tarihli ve 2021/28 sayılı Kararı ile WhatsApp Inc. hakkında resen inceleme başlatılmasına karar verilmiştir.

Sürece ilişkin olarak 08.02.2021 tarihinde Kurul tarafından yeni bir değerlendirme yapılacaktır.

Kamuoyuna saygıyla duyurulur."

10 AB KURUMLARININ YAKLAŞIMLARI

Facebook, WhatsApp'ı 2014 yılında satın aldı. O sırada WhatsApp'ın gizlilik politikası, uygulamanın herhangi bir kullanıcının kişisel verilerini Facebook ile paylaşmasını engelliyordu. Facebook, Avrupa Komisyonu'na Facebook profillerini WhatsApp kullanıcılarıyla güvenilir ve otomatik olarak eşleştiremeyeceğini bildirdi.

Ağustos 2016'da WhatsApp, gizlilik politikasını, WhatsApp'ın kullanıcıların kişisel verilerini üç amaç için "Facebook şirketler ailesi" ile paylaşacağını belirtecek şekilde güncelledi: iş analizi, sistem güvenliği ve hedefli reklamcılık. Mevcut kullanıcılar, hedeflenen reklamcılığa izin vermeyebilir. Diğer herhangi bir itiraz için tek seçenek WhatsApp'ı kullanmayı bırakmaktı. Burada, kullanıcılara sağlanan bilgi ve seçeneklerin eksikliği konusunda endişeler dile getirildi. AB veri koruma gereksinimleri açısından, WhatsApp'ın kullanıcıların kişisel verilerini Facebook ile adil bir bildirim veya meşru bir yasal dayanak olmaksızın paylaştığı iddia edildi.

AB veri koruma mevzuatı 2018 Genel Veri Koruma Yönetmeliği (GDPR) ile uyumlu hale getirilmeden önce, çeşitli AB üye devletleri, WhatsApp'ın kişisel kullanıcıların verilerini Facebook ve "Facebook şirketler ailesi" ile paylaşmasının mevcut AB gizlilik standartlarını ihlal ettiğine karar vermişti. Nisan 2017'de Almanya Yüksek İdare Mahkemesi, Facebook'un WhatsApp kullanıcılarının verilerini kendi amaçları için kullanmasını yasaklayan bir idari emri onayladı. Fransa'da, **Fransız Veri Koruma Otoritesi (CNIL)** tarafından WhatsApp'a karşı resmi işlem yapıldı. CNIL, şirketin Facebook ile kullanıcı verilerini paylaşmak için yasal bir dayanağı olmadığını ve Fransız yetkililerle işbirliği yapma yükümlülüğünü ihlal ettiğini iddia etti. 15 Mart 2018'de, **İspanyol Veri Koruma Ajansı (AEDP)**, Facebook ve WhatsApp'a 300.000 kişinin kişisel verilerini izinsiz olarak işlediği için idari para cezası verdi.

Bu arada, **Birleşik Krallık'ta Bilgi Komiserliği Ofisi (ICO)** tarafından daha geniş bir soruşturma yürütüldü. Mayıs 2018'de sunulan sonuçlar, WhatsApp'ın kişisel verilerin Facebook ile işlenmesi ve paylaşılması için yasal bir dayanak belirlemediğini ortaya koydu. Şirket ayrıca, yeterli adil işlem bilgisi sağlayamamıştır. Bu nedenle, mevcut herhangi bir kullanıcının verilerinin paylaşılması, verilerin elde edilme amacına uygun olmadığı için *Birleşik Krallık Veri Koruma Yasası'nı (1998)* ihlal etmiştir.

Bu soruşturmalar sonucunda WhatsApp, 25 Mayıs 2018'de GDPR'nin uygulanmasından önce AB kullanıcılarının kişisel verilerini Facebook ile paylaşmamayı açıkça taahhüt etti. Bu tarihten sonra, herhangi bir veri paylaşımının GDPR'ye uygun olarak yapılacağı bildirildi.

WhatsApp, soruşturma sırasında hiçbir AB kullanıcısının kişisel verilerinin Facebook ile paylaşılmadığını doğrulasa da, aynı durumun AB dışındaki kullanıcılar için geçerli olup olmadığı belirsiz kalmıştır.[44]

Ayrıca, 23 Haziran 2020 tarihinde **Alman Federal Adalet Divanı**, Facebook'un hakim durumu kötüye kullandığı iddiasını geçici olarak onayladı[45].

Temel nokta, daha ziyade, özel Facebook kullanıcılarını;

- *ağı, kullanıcı deneyimini Facebook'un potansiyel olarak sınırsız erişimiyle, aynı zamanda kullanıcıların İnternet'in "Facebook dışı" kullanımıyla ilgili özelliklere bağlayarak daha kişiselleştirilmiş bir şekilde kullanmak isteyip istemediklerine ilişkin olarak; veya*
- *facebook.com'da kendilerinin paylaştıkları verilere dayanan bir kişiselleştirme seviyesini kabul etmek isteyip istemedikleri konusunda*

herhangi bir seçimden mahrum bırakıyorsa, hizmet şartlarının durumu kötüye kullanmasıdır.

AB, İnternet Yönetişim Forumları (Internet Governance Forum)[46] ve Dünya Bilgi Toplumu Zirvesi (World Summit on the Information Society – WSIS) üzerinden yıllardır bu konuda kontrol ve vergi gücü elde etmeye çalışıyor, ama ABD tarafından engelleniyor. Şimdilerde bu firmaların Avrupa operasyonlarını satmaları ya da Avrupalı rakiplerinin boyutlarına indirmeleri istendi. Son olarak 15 Aralık 2020'de ortaya konan 2 yeni kanun taslağı, önümüzdeki yıllarda Avrupa'nın bu firmaları daha fazla kontrol altına alma isteğinin bir tezahürü[47] durumunda.

11 KİŞİ, KURUM VE STK'LARIN GÖREV VE SORUMLULUKLARI

11.1 KİŞİLERİN GÖREV VE SORUMLULUĞU

WhatsApp tarafından dayatılan sözleşme değişikliği sonrasında kişilerin aceleyle ve hiçbir araştırma yapmaksızın başka uygulamalara yöneldiği görülmektedir. Anlık ileti uygulamaları,

[44] The Humanitarian Metadata Problem: "Doing No Harm" in The Digital Era, October 2018
[45] https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2020/23_06_2020_BGH_Facebook.pdf?__blob=publicationFile&v=2
[46] https://en.wikipedia.org/wiki/Internet_Governance_Forum
[47] https://turk-internet.com/abde-beklenen-internet-kanunlari-ortaya-cikti-teknoloji-devleri-icin-buyuk-cezalarla-desteklenen-yeni-kurallar-geliyor/

ücretsiz olarak sunulan diğer uygulamalar gibi, sundukları hizmet karşılığında kişilerin birtakım verilerine erişmekte ve çoğu durumda bu verileri işleyip yurt dışına aktarmaktadırlar.

Bireylerin her şeyden önce bilinçli kullanıcı ve bilinçli tüketici olması gerekir. Bu bilincin en önemli noktalarından biri kişisel verilerinin öneminin, kırılganlığının ve verinin saçılmasının geri dönülemez sonuçları olabileceğinin farkında olmalarıdır. Bu raporda anlık ileti uygulamaların toplayıp işlediği kişisel verilere yönelik riskler ile birlikte teknik seçme ölçütleri ayrıntılı olarak anlatılmıştır.

Kullanıcıların bu riskler ve karşılık gelen teknik ve hukuki seçme ölçütlerini dikkatlice inceleyerek tercihte bulunmaları, uzun vadede kişisel verilerinin saçılma riskine yönelik en sağlam adım olacaktır. Bu kapsamda, söz konusu uygulamaların hizmet ve gizlilik sözleşmeleri tam olarak okunmalı, ihtiyaç duyulan doğru teknik ve hukuki bilgi güvenilir kaynaklardan elde edilmelidir.

Dolayısıyla kullanıcıların, sadece anlık ileti uygulamalarında değil, yükledikleri tüm uygulamalarda kişisel verilerinin nasıl işlenip paylaşılacağını iyice anladıktan sonra en güvenli gördükleri yerli ya da yabancı bir uygulamada karar kılmaları önerilmektedir.

11.2 DÜZENLEYİCİ KURUMLARIN GÖREV VE SORUMLULUKLARI

WhatsApp tarafından dayatılan sözleşme değişik sürecinde yaşanan en büyük hayal kırıklığı uygulamadaki çifte standart olmuştur. Ancak, gelişmeler göstermektedir ki, özellikle Avrupa Birliği'ndeki düzenleyici kurumlar düzenleme ve denetleme faaliyetlerini çok önceden başlatmışlar, bir dizi önlemi de önceden almışlardır.

Nitekim WhatsApp sözleşme değişikliği konusunda AB düzenleyici kurumlarını önceden bilgilendirip ön onay almıştır. Ülkemizde ise düzenleyici kurumların durumdan kullanıcılarla aynı zamanda bilgi sahibi oldukları ve kamuoyunda oluşan tepkiler sonucunda konuyu acilen gündemlerine aldıkları görülmüştür. Rekabet Kurumu ve Kişisel Verileri Koruma Kurumu kamuoyuna ayrı ayrı açıklama yapmıştır.

Başta WhatsApp ve Facebook olmak üzere sosyal medya ve anlık ileti uygulamalarının kişisel verileri baştan beri "zorunlu rıza" ile toplayıp işlemekte ve paylaşmaktadırlar. Bu nedenle, düzenleyici kurumların tepki olarak değil, zamanında gerekli önlemleri almaları tıpkı AB'de olduğu gibi daha etkin olurdu.

Bundan sonra benzeri süreçlerin daha sağlıklı ve etkin işletilebilmesi için:

- Proaktif inceleme ve düzenlemeler yapılmalı
- Teknik değerlendirmeler kapsamlı olarak ele alınmalı
- Avantajlar ve riskler ayrıntılı olarak incelenmeli
- Kurumlararası işbirliği ve sinerji ortamları oluşturulmalı

ve bunlar STK, akademi, sanayi, kamu kurumları gibi paydaşlarla katılımcı ve saydam bir işbirliği içinde yapılmalıdır. Buna göre:

- KVKK'nın güncellenmesi kapsamında yapılacak çalışmalarda ve düzenlemelerde paydaşlarla işbirliği yapılmalıdır.
- Bu ve benzeri durumlara karşı hazırlıklı olmak üzere paydaşlarla birlikte orta ve uzun vadeli strateji ve planların oluşturulmasında geniş katılımlı çalıştay, konferans ve şûra benzeri organizasyonlar yapılmalıdır.

11.3 SİVİL TOPLUM KURULUŞLARININ GÖREV VE SORUMLULUKLARI

Düzenleyici kurumlarla birlikte paydaş olarak yapacakları çalışmalara ek olarak STK'lar:

- Her kesimiyle toplumun sosyal medya ve teknoloji kullanımı, bilişim okur-yazarlığı ve kişisel verilerini koruma duyarlılığı konusunda eğitilmesi ve bilinçlendirilmesinde etkin rol almalıdır.
- Uluslararası benzer kuruluşlar ile işbirliği yaparak dünyadaki hukuki ve idari uygulama ve deneyimlerin ülkemize kazandırılmasına yardımcı olmalıdır.

12 SONUÇ VE DEĞERLENDİRMELER

Kişisel verilerin korunması ile başlayan mahremiyetin (gizlilik) yalnızca bir anlık ileti hizmeti veya sosyal medya ortamı sorunu olarak değerlendirilmeyip ulusal çıkarları ve güvenliği gözetecek biçimde teknik, ekonomik, politik ve kültürel açıdan ele alınması gerekmektedir.

Kişilerin gerek Anayasa gerekse de 6698 sy. KVKK'nın kendilerine sağladığı hakların bilincinde olması ve başta akıllı cep telefonları üzerinden kullandıkları her türlü uygulamanın ve sosyal medya kullanımları sırasında toplanan kişisel verileri ve özel nitelikli kişisel verileri hakkında sağlanan bilgileri dikkatlice incelemeleri, bu bilgileri sağlamayan veya uygulama üzerinden aldıkları hizmet ile örtüşmeyen bir veri işleme durumuyla karşılaştıklarında ilgili uygulamayı kullanmamaları ve 6698 sy. KVKK'daki haklarını kullanmaları gerekir.

Bu farkındalığa sahip olmak ve çevremizi her zaman bilgilendirmek her bilinçli bilişimcinin temel görevi olmalıdır.

Diğer yandan, kanun koyucu, hiçbir yazılım veya donanımda kasten arka kapı bırakılmasına izin vermemeli ve en ileri derecedeki şifreleme tekniklerinin elektronik haberleşme teknolojileri başta olmak üzere bu gibi teknolojilerde kullanılmasını zorunlu kılan düzenleme ve uygulamaları hayata geçirmelidir. Bu teknolojilerde kasten bırakılacak güvenlik açıkları ve açık/arka kapılar yalnızca iyi niyetli taraflarca ve hukuk çerçevesinde kullanılmakla kalmayıp kötü niyetli kişi ve kurumlarca da suiistimal edilebilir.

Toplumun sosyal medya, bilişim araçları ve teknoloji kullanımı, bilişim okur-yazarlığı ve özellikle kişisel verilerini koruma duyarlığı konusunda eğitilmesi ve bilinçlendirilmesi topyekün bir seferberlik olarak ele alınmalıdır. Böylelikle Y ve Z kuşağı başta olmak üzere her kesimin kendi

kişisel verisine sahip çıkması sağlanarak bu verilerin saçılmasının orta ve uzun vadede yaratacağı risk ve tehlikelerin önüne geçilecektir.

Uluslararası gelişmelerin sürekli ve yakından izlenmesini sağlayacak kalıcı kurumsal mekanizmaların oluşturulması hem ülkemizin hem de düzenleyici kurulların etkisini ve itibarını arttıracaktır.

Kişisel Verileri Koruma Kurumu bünyesinde küresel boyuttaki gelişmeleri yakından izleyip değerlendirecek ve ileri düzey teknik destek sağlayacak, STK ve üniversitelerin katılımı ile bir "görev gücü" (Advanced Technology Task Force) oluşturulmalıdır.

KVKK'nın mevcut durumu ile çifte standart olarak algılanacak uygulamalarla sık sık karşı karşıya kalınabilecektir. T.C. Cumhurbaşkanlığı 11. Kalkınma Planı'nda da yer aldığı üzere KVKK'nın GDPR koşullarına uygun biçimde ivedilikle güncellenmesi gerekmektedir. Ancak belirtmek gerekir ki, veri ekonomisinden gücünü alan bu gibi uygulamaların ve şirketlerin gerçekleştirdiği hak ihlalleri ile mücadelede yalnızca kişisel verilere ilişkin düzenlemeler yeterli olmamaktadır. Bu bağlamda, insan hakları hukuku, sözleşme hukuku, rekabet hukuku ve tüketici hukuku gibi diğer hukuk dallarının etkisi de göz önünde bulundurulmalı ve yapılacak düzenleme değişiklikleri ile uygulamalarda hukukun üstünlüğünü hâkim kılan bütüncül bir yaklaşım geliştirilmelidir.

Her devlet kendi egemenlik haklarını ve vatandaşlarını korumalıdır. Ancak büyük teknoloji şirketlerinin faaliyetlerini düzenlemede ulusal düzenleme ve yaptırımların yeterli etkiyi ve değişimi getirmediği gözlenmektedir. Bu nedenle, büyük teknoloji şirketlerine yönelik düzenlemelerde hukukun üstünlüğü ve insan hakları başta olmak üzere ortak değerleri paylaştığımız Avrupa Konseyi ve Avrupa Birliği gibi gelişmiş uluslararası ve bölgesel kurumlarla iş birliğine özel önem verilmelidir.

Verilerin yerelde saklanması, belli standartlarda transfer edilmesi ve nasıl saklandığının denetlenebilirliği önemlidir. Anlık ileti hizmetlerinin yurtdışı mesajlaşmaları da içermesi nedeniyle kişisel verilerin yalnızca Türkiye'deki sunucularda, veri merkezlerinde tutulması zorunluğu bu hizmetlerin sağlanmasında teknik, altyapı, hukuki ve idari açıdan zorluklara neden olmaktadır. KVKK tarafından açıklanacak "Güvenli Ülkeler" listesi bu zorlukların kısmen aşılmasına yardımcı olacaktır.

Son olarak WhatsApp, önerdiği sözleşme değişikliği ile oluşan çifte standart algısının aksine her ülkede yürürlükte olan düzenlemeye göre davranmaktadır. Bu nedenle, Kişisel Verileri Koruma Kanunu'nda, özellikle denetim ve yaptırımlardaki GDPR ile olan farklılıklar giderilerek ivedilikle uygulamaya alınmalıdır.

TÜRKİYE BİLİŞİM DERNEĞİ
1971
.yıl
TEKNOLOJİ ÜRETEN TÜRKİYE

TÜRKİYE BİLİŞİM DERNEĞİ
1971
.yıl
TEKNOLOJİ ÜRETEN TÜRKİYE

www.tbd.org.tr