ATATÜRK ÜNİVERSİTESİ YAYINLARI
ATATURK UNIVERSITY PUBLICATIONS

Derleme / *Review*

DOI: 10.5281/zenodo.12600950

Necessity of Raising Individuals Awareness to Protect Personal Data

Kişisel Verileri Korumak İçin Kişilerin Bilinçlenmesinin Gerekliliği

Murat Osman KANDIR

Eskişehir Osmangazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Eskişehir, Türkiye

ABSTRACT

Every value related to human is precious. Personal data is one of human values and at the same time a right granted to individuals. The advancement of technology has given personal data a separate value. Understanding this value is the first step towards protecting personal data. The digital transformation in human life has had significant effects on daily life. Digital transformation has led to the formation of a digital state, which in turn has led traditional services to transform into digital services. The transition of essential services such as healthcare and banking to the digital world has led to the growth of digital footprints left by individuals in the virtual world. With the widespread access of the internet to every home and the economic accessibility of mobile devices, it has paved the way for everyone to carry a computer in their pocket. There has been a transformation towards a society that prefers virtual socialization over traditional socialization, leading to a frenzy of sharing using social media applications, with almost everyone having a profile. Through social media applications, personal data has been scattered, and the winner has been yet another new technology, artificial intelligence. Artificial intelligence technologies, which will fundamentally change the future, have been nourished by personal data and have produced products beyond predictions. While efforts are made to ensure the privacy of individuals, the privacy of future generations, namely children, has been left vulnerable to threats without even their knowledge. Efforts have begun to develop software development methods that will ensure data privacy in the design stage of applications that will process personal data. It has been understood that protecting personal data will not be possible solely through legal regulations, and the importance of raising awareness among individuals has emerged. This article raises awareness among individuals about the rights they have, while warnings about the threats behind the conveniences brought by the digital world. In particular, information was given about the possibility of meeting the data used by artificial intelligence technology to meet educational needs from individuals' personal data.

Keywords: Personal data, digital privacy, artificial intelligence, social network

ÖZ

İnsana ait her şey değerlidir. Kişisel veri de insanın değerlerinden birisi ve aynı zamanda kişilere addedilen bir haktır. Teknolojinin gelişimi kişinin verilerine ayrı bir değer yüklemiştir. İnsanın bu değeri anlaması kişisel verilerine sahip çıkması yolundaki ilk adımdır. İnsan hayatında yaşanan dijital dönüşüm günlük yaşamda büyük etkiler yaratmıştır. Dijital dönüşüm dijital devletin oluşmasını, o da geleneksel hizmetlerin dijital hizmetlere dönüşmesine sebep olmuştur. Sağlık ve bankacılık gibi temel hizmetlerin dijital dünyaya taşınması insanların sanal dünyada bıraktığı dijital ayak izlerinin büyümesini sağlamıştır. İnternetin her eve girmesi, mobil cihazların ekonomik olarak erişilebilir olması ile birleşince herkesin cebinde bir bilgisayar taşımasının yolunu açmıştır. Geleneksel sosyalleşmeden ziyade sanal sosyalleşmeyi tercih eden bir topluma dönüşüm yaşanmış ve bu durum neredeyse her kişinin bir profil sahibi olduğu sosyal ağ uygulamaları kullanılarak paylaşım çılgınlığına neden olmuştur. Sosyal ağ uygulamaları sayesinde kişisel veriler ortalığa saçılmış ve kazanan yine çok yeni bir teknoloji olan yapay zekâ teknolojisi olmuştur. Geleceği kökten değiştirecek olan yapay zekâ teknolojileri kişisel verilerden beslenmiş ve tahminlerin ötesinde ürünler ortaya çıkarmıştır. Kişilerin mahremiyeti sağlanmaya çalışılırken geleceğin büyükleri olan çocukların mahremiyeti onların haberleri bile olmadan tehditlere karşı savunmasız bırakılmıştır. Kişisel verileri işleyecek uygulamaların tasarlanmaları aşamasında veri mahremiyeti sağlayacak yazılım geliştirme yöntemleri kullanılmasına yönelik çalışmalar başlamıştır. Kişisel verileri korumanın sadece yasal düzenlemeler ile mümkün olmayacağı anlaşılmış ve kişilerin bilinçlendirilmesi gerekliliğinin önemi ortaya çıkmıştır.

Geliş Tarihi/Received 17.04.2024
Kabul Tarihi/Accepted 04.06.2024
Yayın Tarihi/Publication Date 30.06.2024

Sorumlu Yazar/Corresponding author:
E-mail:

Cite this article: Kandır, M. O. (2024). Kişisel verileri korumak için kişilerin bilinçlenmesinin gerekliliği. *Education and Technology in Information Science, 2*(1), 16-24.

Bu makalede bireylere sahip oldukları haklar ile ilgili bir farkındalık yaratırken dijital dünyanın getirdiği kolaylıkların arkasındaki tehditler konusunda uyarılara yer verilmiştir. Özellikle yapay zekâ teknolojisinin eğitim ihtiyacını karşılamak için kullandığı verilerin bireylerin kişisel verilerinden karşılama ihtimali konusunda da bilgilendirme yapılmıştır. Sağlayacak yazılım geliştirme yöntemleri kullanılmasına yönelik çalışmalar başlamıştır. Kişisel verileri korumanın sadece yasal düzenlemeler ile mümkün olmayacağı anlaşılmış ve kişilerin bilinçlendirilmesi gerekliliğinin önemi ortaya çıkmıştır. Bu makalede bireylere sahip oldukları haklar ile ilgili bir farkındalık yaratırken dijital dünyanın getirdiği kolaylıkların arkasındaki tehditler konusunda uyarılara yer verilmiştir. Özellikle yapay zekâ teknolojisinin eğitim ihtiyacını karşılamak için kullandığı verilerin bireylerin kişisel verilerinden karşılama ihtimali konusunda da bilgilendirme yapılmıştır.
Anahtar Kelimeler: Kişisel veri, dijital mahremiyet, yapay zekâ, sosyal ağlar

Giriş

Anayasanın 20. maddesine 2010 yılında 5982 sayılı Kanunla yapılan Anayasa değişikliği ile bir fıkra eklenerek kişisel veriler, "özel hayatın gizliliği ve korunması hakkı" kapsamında Anayasal güvence altına alınmıştır. İnsanın mahremiyetinin korunması, gücünü Anayasadan alan Özel hayatın gizliliği üzerine inşa edilmiş bir haktır (Şimşek, 2008, s. 4) İnsan ile ilgili bilgilerin özel bir korumaya ihtiyaç duyması dijital dönüşümün bir sonucu olarak karşımıza çıkmaktadır. Dijital yaşam ile birlikte önem kazanan kişiye ait bilgiler özel hayatın gizliliği kavramından ayrılmış ve farklı bir koruma alanına sahip olmuştur. Her ne kadar çatı kavram özel hayatın gizliliği olsa da kişisel verilerin her geçen gün artan değeri bu farklı bir alanın oluşmasını zorunlu hale getirmiştir. Türk hukukunda 2016 yılında kabul edilen Kişisel Verileri Koruma Kanunu ile söz konusu koruma alanının özel bir kanun koruması altına alınması sağlanmıştır. Kişisel veriler bağımsız bir hak olma niteliğine kavuşmuş ve her geçen gün yeni düzenlemelerle daha korumalı bir hak olma yolunda ilerlemektedir. Teknolojinin gelişi ile paralel sürekli olarak yeni düzenlemelere muhtaç olan bu alanı daha iyi anlamak için önce kişisel veriyi anlamak gerekmektedir.

Kişisel Veriyi Anlamak

Günümüzde etkin olan tüm evrensel kurallar belirli bir tarihsel süreç sonrasında şimdiki halini almıştır. Her hukuk kuralı bir ihtiyaca yönelik ortaya çıkmıştır. Tarihin başlangıcı kadar eski olan hukuk kuralları ilk zamanlarda bireyin canını ve mülkiyetindeki değerleri korumak ekseninde gelişmiştir. M.Ö. 753 yılında Roma'nın kuruluşuyla başlayan eski Roma döneminde özgürlüğün karşılığı insanın malını ve canını özgürce koruması olarak görülüyordu (Johnston, 1999). İnsanın canından ve malından başka değerlere de sahip olduğu keşfedildiğinde hukuk koruması da genişlemeye başladı. Manevi değerlerin de korunmaya muhtaç olduğunun anlaşılmasıyla mahremiyet kavramının sadece fiziksel mahremiyet ile sınırlı olmadığı kişinin kendisi ile ilgili her konunun kişinin kendi kontrolünde olması gerektiği sonucu ortaya çıktı. Mahremiyetin korunması özgürlüğün temeli olarak görülmeye başladı (Warren ve Brandeis, 1890, s. 194)

Dünyada kişisel verilerin önemli olduğu ve korunması gerektiği ilk olarak 1948 yılında imzalanan İnsan Hakları Evrensel Beyannamesi ile başlamıştır. 1950 yılında imzalanan Avrupa İnsan Hakları Sözleşmesi ile devam etmiştir. Kişisel verilerin korunması kapsamındaki ilk düzenleme ise Almanya'nın Hessen eyaleti tarafından 30.09.1970 tarihinde düzenlenen veri koruma kanunudur. 1973 yılında ise İsveç tarafından ülke genelinde yapılan ilk yasal düzenleme İsveç Veri Kanunu'dur. Fransa ve Federal Almanya Veri Kanunları ise 1973 yılında yapılmıştır. Sonraki yıllarda birçok ülke kendi ulusal düzenlemelerini yapmış ve yapmaya devam etmektedir (Gültekin, 2012, s. 22). Gelişen teknoloji ve özellikle internetin yaygınlaşması dijital bir dönüşümün başlamasına neden olmuştur. İnsanların en sık kullandıkları temel hizmetlerin süratle dijital dönüşüme uğraması insanlar ile ilgili veri üretiminin çoğalmasına sebep olmuş ve büyük veri gibi yeni kavramlar ortaya çıkmıştır. Hayatın her alanında yaşanan dönüşüm 21. Yüzyılın en değerli varlığının veri olduğunu ortaya çıkarmıştır. Sheffield matematikçisi Clive Humby 2006'da "Veri yeni petroldür" diyerek tüm dikkatin verinin üzerinde toplanmasına sebep olmuştur. Yazılım ve donanım alanında yaşanan her gelişme verinin değerine değer katmış ve katmaya devam etmektedir. Özellikle yapay zekâ teknolojisinin günümüzde artan başarısı ve popüler olması işlemci teknolojisinde yaşanan gelişmelere dayanmaktadır. Yapay sinir ağlarının eğitilmesinde ihtiyaç duyulan yüksek işlemci gücünün donanımda yaşanan gelişmeler sonucunda sağlanması bu yeni teknolojinin günümüzdeki değerini bulmasına sebep olmuştur.

Uluslararası alanda kişisel veriler ile ilgili yapılan ilk düzenlemeler elektronik veri bankalarında tutulan kişisel verilerin korunması için gerekli standartların belirlendiği 1973 ve 1974 yıllarında Avrupa Konseyi tarafından kabul edilen kararlardır. Bu kararlar sonradan yapılacak yasal düzenlemelerin temelini oluşturmaktadır. Her ne kadar uluslararası ve ulusal yasal düzenlemelerde kişisel verilerin neler olduğu belirtilmiş olsa da gelişen teknolojiler ve veri analizi tekniklerinde keşfedilen yeni yöntemler ile kişisel

verilerin çok daha geniş bir tanımının olduğu ortaya çıkmaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanununda kişilerin yapmış oldukları alışveriş bilgileri kişisel veri olarak belirtilmemiş olsa da bu tür verilerin analizi sonrası kişiler hakkında çeşitli verilerin meydana çıkarılacağı göz önüne alındığında kişisel veriler konusunda her geçen gün yeni ihtiyaçların ortaya çıkacağı sonucuna ulaşılmaktadır (Küzeci, 2019). Bu konuyla ilgili en güzel örnek ise Avrupa Birliği Adalet Divanı tarafından verilen SCHUFA, C-634-21 kararıdır. Almanya'da hizmet veren özel bir kredi skorlama kuruluşu olan SCHUFA, üçüncü şahıslara - özellikle de tüketicilere - ait bilgileri çeşitli veri tabanlarından toplayıp, bu bilgiler üzerinde çeşitli yapay zekâ algoritmaları kullanmaktadır. Elde ettiği sonuçları ise benzer davranışlar sergileyen diğer insanların talep etmiş oldukları kredileri geri ödeme ihtimallerini hesaplamakta kullanmaktadır. Söz konusu şirket veri üzerinde algoritmik yöntemler kullanarak tahminlerde bulunmaktadır. Bu kararda önemli olan husus ise yasal mevzuatta bahsedilmeyen ve mevcut verilerin analizi sonucunda ulaşılan verinin korunmasıdır.

Bilgisayar ve yazılım teknolojilerinin gelişmesi ile birlikte bilgisayar kullanımı yaygınlaşmıştır. Bilgisayarın neredeyse her eve girecek kadar yaygınlaştığı dönemde tüm kamu kurumları ve özel şirketler sahip oldukları bilgileri dijitalleştirerek bilgisayar ortamında tutmaya ve işlemeye başlamıştır. Bilginin dijital ortamda saklanmaya başlanması bilginin güvenliğinin sağlanması ihtiyacını da beraberinde getirmiştir. Veri analiz yöntemlerinin gelişmesi, ilk anda önemsiz gibi görünen verilerin dahi korunması gerektiğini göstermiştir. Kişisel veri kategorisinde olmayan verilerin çeşitli yöntemler ile analizi sonrasında profil çıkarma gibi sonuçlara ulaşılarak ilk andaki veriden anlamlı sonuçlar çıkartılabilmektedir. İşte bu nedenlerle her türlü bilginin korunması önem arz etmektedir. Zaten veri güvenliği genel ve öncelikli bir ihtiyaç olduğundan bilgi güvenliği konusu sürekli acil ve önemli bir ihtiyaç olarak görülmüştür. Verinin güvenli olarak işlenmesi ve muhafaza edilmesi dijitalleştiği ilk andan beri önemli olarak görülmüştür. İnsanın özel hayatına gösterilmesi gereken saygı ile ilgili anayasal düzeyde yapılan düzenlemeler teknolojinin gelişmesi sonrasında dijital ortamda oluşturulan kişi ile ilgili veriler kapsamında düşünüldüğünde bu alanda özel düzenlemeler yapılması ihtiyacı ortaya çıkmıştır. 2010 yılında Anayasamızda özel hayatın gizliliği ile ilgili maddeye yeni bir fıkra eklenerek kişisel verilerin korunması konusu en üst yasal düzenlemede yerini almıştır (Korkmaz, 2017, s. 86). Kişisel verilerin korunması kapsamında yapılan çalışmalar ve düzenlemeler incelendiğinde Kişisel verilerin kanunlar ile koruma altına alınma çabası görülmektedir. Ülkemizde kişisel verilerin korunmasını sağlamak ve kişilerde verilerin korunmasına yönelik farkındalık oluşturmak için Kişisel Verileri Koruma Kurumu kurulmuştur. Kurumun internet sitesinde Misyon olarak "Anayasada öngörülen özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması kapsamında, ülkemizde kişisel verilerin korunmasını sağlamak ve buna yönelik farkındalık oluşturarak bilinç düzeyini geliştirmek, aynı zamanda veri temelli ekonomide özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırıcı bir ortam oluşturmak." belirlenmiştir. Kamuoyunda kişisel verilere karşı farkındalık düzeyini artırmak ve veri ihlalleri hakkında bilgi vermek için meydana gelen veri ihlalleri Kurumun internet sitesinde duyuru olarak yayımlanmaktadır. Böylesi düzenlemelerin tek amacı kişisel verilerin korunmasıdır. Kurulun kamuoyunda bilinirliğinin artmasını sağlayan Yemek Sepeti veri ihlali kararı 23.12.2021 tarihinde Kurul'un internet sitesinde yayımlanmıştır. Kurul tarafından yayımlanan duyuruda meydana gelen ihlalden 21.504.083 Yemeksepeti kullanıcısının etkilendiği bilgisi verilmiştir. Bu veri ihlali Kurul tarafından yayımlanan en çok kullanıcı bilgisinin ihlale uğradığı veri ihlali olayları arasında yer almaktadır.

Dijitalleşen Yaşam

Teknoloji her alanda insan hayatını kolaylaştırmaktadır. Tüm hizmet üreten sektörler hem yaygınlaşma hem de kolaylaştırma maksadıyla teknolojiyi yaygın bir şekilde kullanmayı amaçlamaktadır. Kamunun verdiği hizmetlerde de bu düşüncenin olduğu görülmektedir. Sağlıktan adalete, bankacılıktan ticarete tüm alanlar süratle dijitalleşmekte ve internet ortamına taşınmaktadır. Stanford Üniversitesi bilim adamları tarafından yayımlanan AI indeks raporunun bu seneki sayısı oldukça kapsamlı bilgiler içeriyor (Stanford University, 2024). Bu raporda en çok göze çarpan çıkarımlardan birisi; yapay zekânın bazı alanlarda insandan iyi olduğunun kabul edilmesidir. Üretken yapay zekâya yapılan yatırımların artması ve insanların yapay zekânın olası etkilerinin farkında olmalarından kaynaklanan bilinçli olmaları ile bu durumun gergin olmalarına neden olması ise raporun dikkat çektiği hususlar arasındadır.

İnternetin insan yaşamında bulunduğu seviyeye gelmesi beklenenden hızlı olmuştur. Her eve internetin girmesi süreci her eve bilgisayarın girmesi sürecinden çok daha kısa bir sürede tamamlanmıştır. Mobil cihazların gelişmesi ve ekonomik olarak ucuzlaması dijital dönüşümü daha da hızlandırmıştır. Teknik özelliklere bakıldığında mobil cihazların her birisinin neredeyse orta seviye bir bilgisayarın teknik özelliklerine sahip olduğu görülmektedir. Birçok akıllı cep telefonunun üst düzey bilgisayarlar seviyesinde teknik özelliklere sahip olduğu ise bir gerçektir. Her insan cebinde bir bilgisayar taşıyor desek yanlış bir cümle kurmamış oluruz.

Her kişinin bir ucu internete açılan bir mobil cihaza sahip olması dijital dünyanın en büyük sorunu olan dijital güvenlik konusunun önemini artırmaktadır. Özellikle yakın geçmişte yaşanan pandemi nedeniyle insan yaşam sürecinde yeni yöntemler ve ortamlar ortaya çıkmıştır. Ticaret neredeyse tamamen dijitalleşerek internet ortamına taşınmıştır. Uzaktan çalışma bir yöntem olmaktan çıkmış adeta bir zorunluluk halini almıştır. Eğitimin internete taşınması başlangıçta bir çare olarak görülse de pandemi sonrasında bir tercih olmaya başlamıştır. Ekonomi yön değiştirmiş ve neredeyse dijitalleşmeyen bir alan kalamamıştır. Geçmişte kahve fincanlarından bakılan kahve falları bile kahve fincanı fotoğraflarının dijital fal bakma platformlarına gönderilmesi ile dijital kahve fallarına dönüşmüştür.

Bir insan karlı bir arazide nasıl yürüdükçe iz bırakıyorsa internette yaptığı her işlem ile de bir iz bırakmakta, bir veri üretmektedir. Amerikalı bilgisayar korsanı Kevin Mitnick 15 Mayıs 1995'te dijital ortamda bırakmış olduğu izlerin FBI tarafından takip edilmesi sonucunda yakalanmıştı. Bu olay sonrası Amerika Birleşik Devletleri'nin Philadelphia eyaletindeki The Philadelphia Inquirer gazetesi ilk kez "digital footprint" kavramını dijital dünyada bırakılan izlerin karşılığı olarak kullanmıştır. Dijital Ayak İzi kavramı bu şekilde ortaya çıkmış ve neredeyse her ortamda kullanılmaya başlanmıştır. İnternet kullanıcılarının web tarayıcılarını kullanarak erişim yaptıkları her sitede bir iz bırakmaları ve bu izlerin de saklanmasıyla bir veri havuzu oluşmaktadır. Web ortamında bırakılan izler kadar bıraktırılan izler de bulunmaktadır. Bu iz bırakmaya zorlanma konusunun kavramsal ifadesi çerez (cookies) olarak adlandırılmaktadır. Çerez kavramı, internet kullanıcısı bir web sitesini ziyaret ettiği zaman web sitesinin kullanıcıdan bazı bilgiler istemesi yöntemi olarak tanımlanabilmektedir. İlk kez 1994 yılında Netscape firması çalışanı Lou Montulli tarafından kullanılan ve yalnızca kullanıcılar ile ziyaret ettikleri web sitesi arasında bilgi alışverişi yapmak için tasarlanan küçük program parçaları çerez olarak adlandırılmıştır. Internet kullanıcısının web tarayıcı bilgisi, IP numarası, dil tercihi, web sitesini ziyaret sıklığı gibi bilgiler çerezlerin tuttuğu bilgilere örnek olarak gösterilebilmektedir. Web siteleri bu bilgileri birçok amaç için tutarken hedeflerinin başında kullanıcıların alışkanlıklarını analiz ederek daha performanslı ve tercih edilir web siteleri oluşturmaktır. Ancak günümüzdeki kullanım öncelikleri reklam ve pazarlama alanına yönelmiştir.

Dijital Mahremiyet

Dijital ayak izlerinin verilere dönüşmesiyle büyük veri kavramı ortaya çıkmıştır. Teknolojinin gelişimi bilgisayarlardaki işlemci gücünün ciddi bir artışına neden olmuştur. Artan işlemci gücü ise birim zamandaki işlem miktarının artmasına bu artış da istatistik biliminin gelişmesine neden olmuştur. Geçmişteki bilgilerin çeşitli veri analiz yöntemleri ile işlenmesi hem kullanıcı alışkanlıklarının tespit edilmesine hem de gelecekteki beklenen davranış şekillerinin doğru tahmin edilmesinde yüksek başarı yüzdelerine ulaşılmasına imkân vermiştir. Veri analizi bir yöntem olmayı aşarak bir mühendisliğe (veri mühendisliği) dönüşmüş ve yeni bir meslek olarak ortaya çıkmıştır. Verilerden ulaşılan bilgilerin çeşitliliği ve kullanılabilirliğinin keşfedilmesi ile birlikte dijital ayak izinin önemi artmış ve bu veriler ekonomik olarak da değer kazanmaya başlamıştır. İnternet ortamında kullanıcıların tercihleri yeni dijital izlerin oluşmasına neden olmaktadır. Mobil cihazların kullanımının artmasıyla mobil uygulamaların daha çok kullanılması ve bu uygulamaların da cihazlardaki erişim izinleri ile birçok veriye kolayca erişmesi mümkün olmuştur. Uygulamaların üreticisi olan şirketler elde ettikleri verileri öncelikle hedeflenmiş reklamlarda kullanmak üzere pazarlamaya başlamışlardır. Böylece veri ticareti başlamıştır. Bu ticaret mobil uygulama ve internet kullanıcılarının dijital ayak izlerinden elde edilen kişisel tercihlerinin ekonomik kazanç amaçlı kullanımına hizmet etmeye başlamıştır.

Kişisel veri kavramı tanımındaki verilere gösterilen dikkatin tüm verilere gösterilmesi gerekmektedir. Çünkü herhangi bir veri bir gerçek kişiyi belirlemede bir rol oynuyorsa o veri de kanun kapsamında koruma altında olmaktadır. Yasal olarak korunmayan verilerin gelişmiş veri analiz yöntemleri ile anlamlandırılarak veri sahibi kişilerin kimlik bilgilerine erişim sağladığı görülmektedir. 6698 Sayılı Kişisel Verileri koruma Kanunu'nun Tanımlar kısmındaki "Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi," tanımında da görüleceği üzere tanımdaki belirlenebilir sözcüğü, bir anlamda verinin işlenmesi sonucunda gerçek kişiye erişebilirliği belirtmektedir.

Günlük yaşamda kolayca belirleyebileceğimiz mahremiyet sınırları dijital ortamda fiziksel ortamın tam tersine bir özellik göstermektedir. Gerçek dünyada çekirdek aile üyeleri, anne ve baba, kardeşler, karı-koca gibi çok yakınların girebileceği alan mahrem alan olarak tanımlanır. Başka insanlar bu alana girerse rahatsız olur, çeşitli tepkiler veririz. Edward Twitchell Hall'ın "proksemik", kişisel alan teorisine göre mahrem alan genelde 45 santim ve aşağısı olarak kabul edilir. Kişisel alan ise aile üyeleri ve arkadaşlar için belirlenen alandır. Kişilere fiziksel olarak 120 santim ve aşağısındaki mesafelere girildiğinde kişisel alanına girmişsiniz diyebiliriz. Bilimsel olarak bu mesafelerin net olarak belirlenebilmesi kişiler tarafından bakıldığında kişinin belirleyebileceği ve kişiye özgülenmiş bir hak olarak görülmektedir. Sınırlarını kişinin çizdiği bir hak dijitalleşen

dünyada kolayca kontrol edilememektedir. Sadece yakın arkadaşlarının erişimine izin verilen bir sosyal ağ paylaşımı kolayca tüm sosyal ağ kullanıcıları tarafından erişilebilir bir duruma dönüşebilmektedir. Dijital dünyada kolayca kopyalanabilme, hızla yayılma gibi özellikler nedeniyle kişisel mahremiyet çok daha fazla zarar görebilmektedir. Kişinin yakın çevresi ile paylaştığı özel hayatındaki özel anların fotoğraf ve videoları kötü niyetle veya bilinçsiz bir şekilde mesleki yaşamındaki iş arkadaşlarının eline geçebilmektedir. Kişinin özel paylaşımlarına erişim hakkı olan bir yakın arkadaşın yapmış olduğu bu istenmeyen paylaşımlar kişinin zor durumlar yaşamasına, kariyerinin zarar görmesine neden olabilmektedir. Kişinin yapmış olduğu ve tercihlerini ortaya çıkaracak sosyal ağ paylaşımları ile kötü niyetli kişilerin manipülasyonuna açık duruma gelmesi de bir başka ihtimaldir. Özellikle kamuoyu önünde çokça bulunan ünlülerin özel hayatlarına ait fotoğraflarının kullanılarak sahte sosyal ağ hesapları açılmasıyla ilgili gerçekleşen birçok olaya ait haberler zaman zaman basında yer almaktadır. Her ne kadar kişisel verilerin korunması kapsamında sürekli gelişen yasal düzenlemeler yapılsa da sosyal ağların büyülü dünyası karşısında dijital mahremiyetin korunması çok da kolay olmamaktadır.

Sosyal Ağlarda Beğenilme

Endüstri 4.0 ile hayatımıza giren yeni teknolojiler birçok alanda insan yaşamını kolaylaştırıcı makinelerin gelişimini sağlamaktadır. Yıllar önce elde yıkanan çamaşırlar ilk önce makinalara girmiş şimdi ise deterjan ve yıkama tercihini makinelerin belirlediği bir teknolojiye kavuşmuştur. Yüksek teknoloji sunan bu yeni çağ, her alanda insanlığın faydasını ön planda tutmaktadır. Teknolojinin gelişme nedenleri arasında sayılan kolaylaştırma ve konfor artırma sosyal ağların yaygınlaşma nedenleri olarak da gösterilebilmektedir. Bir sosyal ağ uygulamasına giriş yapmak için sadece bir e-posta adresine sahip olmak yeterli olmaktadır. Bu kadar kolay erişim kullanımı da kolaylaştırmaktadır. Sosyal ağlarda profil oluşturmanın kolaylaştırılması ve sade tutulması bu uygulamaların kısa sürede yaygınlaşmasını sağlamıştır (Boyd ve Ellison 2008, s. 223) Sosyal ağ uygulamalarının mobil cihazlar ile kullanılabilmesi eli telefon tutan! herkesin bu uygulamalarda yerini almasını sağlamıştır. Ulusal ve uluslararası istatistiklere bakıldığında neredeyse her mobil cihaz kullanıcısının aynı zamanda sosyal ağ kullanıcısı da olduğu görülmektedir. Bir uluslararası istatistik hazırlama ajansı olan We are Social tarafından hazırlanan Dijital Türkiye 2023 Raporunda 85,59 milyonluk Türkiye nüfusunun 81,68 milyon akıllı telefon kullanıcısı olduğu belirtilmiştir. Aynı raporda 71,38 milyon internet kullanıcısının 62,55 milyonunun aktif sosyal ağ kullanıcısı olarak yer aldığı görülmektedir (Clicks'us Digital, 2023). Sosyal ağların temel amacı olan sosyalleşme, diğer anlamıyla her profilin ağını genişletmesi kullanıcıların birçok kullanıcıyla bağ kurmasını sağlamaktadır. Bir diğer amaç ise paylaşmaktır. İçerik üretmek ve paylaşmak her kullanıcının sosyal ağlardaki bir diğer hedefi olmaktadır. Paylaşım yapmak ve diğer kullanıcılar tarafından yapılan paylaşımları izlemek sosyal ağların merkezinde yerini almıştır (Van Dijck, 2013, s. 206) Yapılan paylaşımları izleyen her kullanıcı bu paylaşımlar üzerinden paylaşım yapan kullanıcılar ile etkileşime girmektedir. Sosyal ağların besini ise beğenidir. Yani global ismi ile "like". Her bir paylaşım altında yer alan beğeni seçeneği tıklanarak içeriğin güzel bir içerik olduğu belirtilmekte ve paylaşım sahibiyle olumlu bir etkileşim yaşanmaktadır (Türk ve Demirci, 2016, s. 518).

İşte böylesi bir öneme sahip olan beğeni kavramı kullanıcıları paylaşım yapmaya zorlamakta ve kullanıcıların paylaşılan içeriğe gösterdikleri tepkilere bir önem yüklemektedir. Sosyal ağ kullanıcılarının duyduğu bu büyük "beğeni" açlığı yaptıkları paylaşımlarda aşırılığa kaçmalarına ve bir paylaşım çılgınlığı yaşamalarına sebep olmaktadır. Zaman zaman bu çılgınlık akıl almaz derecede tehlikeli içerikler yaratmaya kadar varmaktadır. Özellikle son zamanlarda sosyal ağ kullanıcısı olan ebeveynlerin çocukları hakkında oluşturdukları içerikleri sıkça paylaştıkları görülmektedir (Sütlüoğlu, 2015, s. 125) Yapılan bu paylaşımların kişisel verilere karşı oluşturduğu riskleri şu şekilde sıralayabiliriz:

- Kişisel verilerin kötü niyetli kişilerce dolandırıcılık suçunda kullanılması
- Paylaşımlardan elde edilen verilerin taciz, cinsel istismar gibi suçlara temel oluşturması
- Üretken yapay zekâ kullanımıyla kötü niyetli fotoğraf ve video üretilmesi
- Elde edilen verilerin tehdit ve şantaj gibi suçlarda kullanılması
- Paylaşım alışkanlığının bağımlılığa dönüşmesine neden olması
- Sosyal ağlarda paylaşılan içeriklerin çocukların geleceğini olumsuz etkilemesi
- Kötü niyetli kişilerin kişisel verileri kullanarak gerçek dünyada veri sahiplerine zarar vermeleri
- Sosyal ağ paylaşımlarının takip edilerek hırsızlık, gasp gibi suçlara zemin hazırlanması

Basında yer alan dolandırıcılık olaylarında suçluların

istihbarı bilgileri mağdurların sosyal ağ paylaşımlarından elde ettikleri bilgisine ulaşılmaktadır. Herhangi bir süzgeçle elenmeden sosyal ağlarda yapılan paylaşımlardaki veriler büyük risklere neden olmaktadır. Ebeveynlerin çocuklarının geleceğini olumsuz etkilememek adına mutlaka yukarıda açıklanan riskleri göz önünde bulunarak paylaşım yapmaları gerekmektedir.

Sosyal Ağlarda Çocukların Mahremiyeti

Sosyal ağlarda yaşanan paylaşım çılgınlıklarından belki de en tehlikelisi ebeveynlerin çocuklarının yer aldığı içerikleri çokça paylaşmalarıdır. Henüz kendi kişisel verileri hakkında karar verme yetisine sahip olmayan çocukların fotoğraf ve videolarının ebeveynleri tarafından herkesin erişebileceği sanal ortamlarda paylaşılması gelecekte onarılması güç sonuçlar doğurabilecektir (Üstündağ, 2020).

Teknolojide yaşanan hızlı gelişim yazılım teknolojilerinin de gelişmesine ve yapay zekâ algoritmalarının birçok alanda kullanılmasının yaygınlaşmasını sağlamıştır. Özellikle yapay zekâ teknolojisi bambaşka bir çağın yaşanmasına neden olmaktadır. Veri setleri ile eğitilen yapay sinir ağı algoritmaları sınıflandırmadan kümelemeye, veri madenciliğinden görüntü işlemeye birçok alanda başarıyla kullanılmaktadır. Sosyal ağlarda paylaşılan çocuk fotoğrafları ile eğitilen yapay zekâ algoritmaları gerçekte var olmayan yeni çocuk fotoğrafları üretebilmektedir. Üretken yapay zekâ olarak adlandırılan bu teknoloji mevcut fotoğrafları kullanarak benzersiz yeni fotoğraflar üretebilmektedir (Kandır, 2023, s. 205).

Özellikle çocukların korunması kapsamında büyük hassasiyet gösteren yasa koyucu çocuğu karşı karşıya kalabileceği her türlü istismara karşı korumaya çalışmaktadır. Türk Ceza Kanununda Altıncı Bölüm “Cinsel Dokunulmazlığa Karşı Suçlar” başlığı altında bu suçlar tanımlanmış ve bu suçların karşılığı cezalar yer almaktadır. Yasa koyucu bu başlık altında genel suç tanımlarıyla yetinmemiş ve 103. Maddede “Çocukların cinsel istismarı” suçunu tanımlamıştır. Sadece tanımlamakla kalmamış hem cezaları artırmış hem de suç olabilecek davranışları genişletmiştir. Yasa koyucu çocukların korunmasına böylece çok daha fazla önem vermiştir. Ancak yaşanan büyük dijital dönüşüm sonucunda birer profesyonel fotoğraf makinesine dönüşen mobil cihazlar kullanılarak sürekli oluşturulan dijital içerikler çocuğun kişisel verilerinin istismara açık hale gelmesine neden olmaktadır.

Ebeveynlerin dikkatsizce yaptıkları sosyal ağ paylaşımları çocukların kişisel verilerinin kötü amaçlı kullanıma açık fotoğraf veri setlerinin arasında yerlerini almasını sağlamaktadır (Timurturkan, 2019, s. 318). Çocuk istismarlarını engelleme amaçlı güvenlik güçlerince yapılan bir araştırmanın sonuçları dehşet vericidir. Yapılan bu araştırmada; özellikle çocuk müstehcenliği içeren internet sitelerinde yer alan görsellerin %50’sinin sosyal medya platformlarından elde edildiği tespit edilmiştir. Üretken yapay zekâ tarafından mevcut fotoğraflardan eğitilerek yeni fotoğraflar üretilmesinin keşfi sonrasında çocuk müstehcenliği ile ilgili yeni fotoğraflar üretildiği bilgisine ulaşılmıştır. Dikkatsiz yapılan çocuk fotoğrafları gelecekte çocukların karşısına utanç verici içerikler olarak çıkabilecektir (Şirin, 2017, s. 52).

Yapay Zekâ Etkisi

Geçtiğimiz yüzyılın buluşu olan internetten sonra yapay zekâ teknolojisi de bu yüzyılın buluşu olma yolunda hızla ilerlemektedir. Temelinde verinin analizi ve çeşitli matematiksel işlemler ile işlenerek anlamlı bilgilere ve tespitlere ulaşma olan yapay zekâ teknolojileri gücünü veriden almaktadır. Büyük veri kavramının üzerinde geliştirilen yapay zekâ teknolojileri günümüzde neredeyse her alanda kullanılmaktadır. Özellikle sağlık alanında kullanılan görüntüleme sistemlerinin hemen hemen hepsinde yapay zekâ algoritmaları çalışmaktadır. Radyologların önüne yapay zekâ tarafından anlamlandırılarak sunulan raporlar teşhislerin konulmasında ve tedavilerin planlanmasında büyük kolaylık sağlamaktadır. Dijital akciğer grafilerinin yapay zekâ destekli bilgisayarlarla değerlendirmesi ile kolayca fark edilemeyecek ve tespiti tecrübeyle sağlanacak olan akciğerde oluşan kitlelerin tespit ve teşhisi yapılmaktadır. Her ne kadar günlük yaşamdaki ihtiyaçlara çare olmak için geliştirilmiş olsa da her şekilde insana temas etmektedir. Belki de en zor tahmin edilebilir olan insan davranışları alanında her geçen gün kullanımı artmakta ve yaygınlaşmaktadır. Kişisel verileri koruma kanunu kapsamında hassas veri olarak nitelendirilen sağlık verileri sağlık sisteminde kullanılan cihazlarda uzun zamandır kullanılmaktadır. Sağlık sisteminin yanında güvenlik sistemlerinde de insanların surat fotoğraflarının kullanıldığı görülmektedir (Durham-Hutchins, 2024). İnsana ait verilerin işlenmesi ve sonrasında muhtemel insan davranışlarının tahmin edilmesi kapsamında yapay zekâ sistemlerinin eğitilmesinde kişisel veriler kullanılmaktadır. İnsanların fotoğrafları kullanılarak eğitilen yapay zekâ algoritmaları yeni insan yüzleri oluşturmaktadır. Hatta yapay olarak oluşturulan bu yüzler çeşitli yapay zekâ teknolojileri sayesinde canlı video görüşmelerinde yüz değiştirme yöntemleri ile birlikte kullanılarak bambaşka sonuçlara sebep olmaktadır (Bolayır, 2024, s. 118). Pandemi sonrası birçok iş görüşmesi Zoom gibi çeşitli telekonferans yazılımları kullanılarak çevrimiçi yapılmaktadır. Fiziksel olarak yüz yüze yapılmayan iş toplantılarında yetkisiz

kişilerin Deepfake teknolojileri kullanarak farklı kişilermiş gibi hareket ettikleri ve bu çevrimiçi toplantılara katıldıkları görülmüştür (Çetindemir, 2024).

İnternette yapılan basit bir arama ile insan yüzü değiştirme ve insan sesi değiştirme yapabilen yazılımlara ulaşılabilmektedir. Bu tür yazılımların çok daha gelişmiş türleri ise belirli ücretler karşılığı edinilebilmektedir (Elitaş, 2022, s. 115). Böylesi gerçekçi sonuçların ortaya çıkması internet ortamında bolca bulunan insan fotoğraf ve ses dosyaları sayesinde olmuştur. Özellikle sosyal ağ kullanıcılarının yapmış oldukları paylaşımlar yapay zekâ algoritmalarının eğitimlerinde kullandıkları veri setlerine dönüşmüşlerdir. Ne kadar fazla veri olursa o kadar gerçekçi sonuçlara ulaşmak mümkün olmaktadır. Derin öğrenme (Deep Learning) sözcüğü ile sahte (Fake) sözcüğünün birleştirilmesiyle oluşturulan yeni bir kavram olan Deepfake sözcüğü her geçen gün kendisinden daha fazla söz edilir hale gelmiştir (Westerlund, 2019, s. 40).

Sosyal ağlardan toplanan milyonlarca insan yüzü ile eğitilen yapay sinir ağları insan yüzünün özelliklerini öğrendikten sonra gerçekte olmayan insan yüzlerini de oluşturma yeteneğine kavuşmaktadır. https://thispersondoesnotexist.com adresli internet sitesinde StyleGAN isimli yapay sinir ağı gerçekte mevcut olmayan insanların yüzlerini üretmekte ve internet sitesinde kullanıcılara sunmaktadır. Deepfake teknolojisi 2017 yılından itibaren bazı Amerika Birleşik Devletleri eyaletlerinde tehdit olarak kabul edilmiş ve yasalarda yerini almıştır. Günümüzde deepfake bir siber tehdit olarak kabul edilmektedir (Temir, 2020, s. 1014). Deepfake teknolojisi mevcut veri setleri ile eğitilince yeni bir ürün ortaya koyabilen üretken yapay zekânın ortaya çıkardığı bir kavramdır. Bilindiği üzere yapay sinir ağları veri setleri kullanılarak eğitilmektedir. Özellikle bilimsel alanlarda çalışmalar yapılması için çok çeşitli veri setleri mevcuttur. Ancak bu veri setleri bitkiler, hayvanlar gibi insan dışındaki varlıkların verilerinden oluşmaktadır. Son zamanlarda artan veri seti ihtiyacı nedeniyle internet ortamında açık kaynaktan veri seti oluşturmak için veri toplama işlemleri yapılmaktadır. Bu tür verilerin toplanması için kullanıcıların sosyal ağlarda herkesin erişimine açık olarak yaptıkları paylaşımlar kullanılmaktadır. Deepfake teknolojisi de bu şekilde oluşturulan insanların fotoğraflarından oluşan veri setleri ile eğitilmektedir. Kişisel verilerin kontrolsüzce sosyal ağlarda paylaşılması bu veri setlerinin gelişmesine ve üretken yapay zekâ teknolojisinin de kusursuzluğa doğru kendini geliştirmesine imkân vermektedir.

Tasarımda Gizlilik (Privacy by Design)

Her ne kadar sistemlerin güvenliğinin sağlanması için Firewall ve Saldırı Tespit Sistemleri benzeri Ağ güvenlik sistemleri kullanılsa da Kişisel Verileri muhafaza eden ve işleyen yazılımların güvenli olması da son derece önemlidir. Bu maksatla güvenli yazılım geliştirme yöntemleri ger geçen gün daha önemli hale gelmektedir. Yazılım geliştirilme safhasında henüz kodlama işlemleri başlamadan sağlanacak güvenli bir tasarım son derece önemlidir. Kişisel bilgilerin toplanmasını işlenmesini ve muhafaza edilmesini içeren her türlü yazılımın henüz başlangıç safhasından itibaren mahremiyeti dikkate alarak geliştirilmesi ihtiyacı bir veri gizliliği yaklaşımı olarak tanımlanmaktadır.

Dünya çapında standartları geliştirmek ve uluslararası eşgüdümü sağlamak için kurulan International Organization for Standardization (ISO) son kullanıcı olan tüketicilerin verilerinin gizliliğinin sağlanması kapsamında gerekli kuralların oluşturulması maksadıyla 2023 yılının ocak ayında ISO 31700-1:2023 (ISO, 2023a) ve ISO/TR 31700-2:2023 (ISO, 2023b) numaralı standartlarını yayınlamıştır. Söz konusu standartlar her türlü projede henüz başlangıç aşamasında ihtiyaç duyulan gizlilik önlemlerinin alınmasını, yapılan işlemlerin belgelenmesini, gerekli kontrollerin yapılmasını ve son dönemde önemi artan kişisel verilerin mahremiyetini sağlayarak veri ihlallerinin önüne geçme çalışmalarının tasarım aşamasında gerçekleştirilmesine imkân vermektedir. Yazılımlarda henüz tasarım aşamasında mevcut kişisel verileri koruma mevzuatına uygun çalışmalar yapılması gelecekte meydana gelebilecek yazılımlardan kaynaklanan veri ihlallerinin önüne geçebilecektir.

Yazılımların gerçekleştirilmesinde görev alan yazılımcıların veri mahremiyeti hakkında bilgilendirilmesi bir zorunluluktur. Disiplinler arası çalışmaların sağlanması için Yüksek Öğretim Kurumu (YÖK) yeni dersler ve yüksek öğrenim programları açılması çalışmaları yapmaktadır. YÖK tarafından Mart 2024 tarihinde yapay zekâ, dijitalleşme ve büyük veri alanlarında üniversitelerde 2'si ilk kez olmak üzere 5 lisans ve tamamı yeni 12 ön lisans programı açılacağını açıklanmıştır. Veri güvenliği düşüncesinin kişisel veriler ile birlikte veri mahremiyetini de içerisine alacak şekilde genişletilmesi ve bu konuda yazılımcıların eğitilmesi artık günümüzde ileri seviye bir eğitim ihtiyacı olarak ortaya çıkmaktadır. Disiplinler arası çalışmanın kaçınılmaz olduğu bir çağı yaşıyoruz. Bunun yanında uzaktan çalışmanın da özellikle yazılım üreten mesleklerce sıça kullanılmaya başlanmasıyla birlikte proje yöneticisi olarak bilinen görevlerin yavaş yavaş ortadan kalktığını görmekteyiz. Ucuz yazılım mühendisi işgücünün uzaktan çalışma ile temin edildiği düşünüldüğünde yazılım üreten mühendislerin sadece çalışır yazılım üretmekten sorumlu olmayacağı mesleğin etik ilkelerinden de sorumlu olacağı bir gerçektir. Hemen hemen her sistemde yerini alan yapay zekâ teknolojisi ile veri seti hazırlanmasından kullanılacak yapay

sinir ağına kadar etik çerçeve içerisinde yazılım geliştirmek artık bir zorunluluk halini almıştır. Başta yapay zekâ teknolojileri olmak üzere kişisel veriler gibi bir çok alanda ulusal ve uluslararası yasal düzenlemelerin diğer disiplinlerce de bilinmesi gerekmektedir. Konumuz kapsamındaki özel alanda ise mühendislerin Kişisel Verilerin Korunması Kanunu kapsamında yeterli bilgiye sahip olmaları sağlanmalıdır. Ancak bu farkındalık sağlandıktan sonra yazılımlarda kaynaklanan veri ihlallerinin önüne geçilebilecektir. Özellikle kodlama aşamasında güvenli yazılım geliştirme yöntemleri kullanılmalı ve sürekli kontroller yapılmalıdır. Tüm bu güvenli yazılım geliştirme tedbirlerinin yanında evrensel etik ilkelere uygun yazılımlar geliştirilmesi öncelikli olmalıdır.

Bilişim sistemlerinde milli güvenliği tehdit edebilecek tehditlerin bertaraf edilmesi ve milli siber güvenlik stratejisinin bir parçası olması maksadıyla T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığının koordine ederek hazırlanmasını sağladığı "Bilgi ve İletişim Güvenliği Rehberi" 2020 yılında tamamlanmıştır (Dijital Dönüşüm Ofisi, 2020). Halihazırda Kamu kurumları ve kritik altyapı hizmeti veren işletmelerce uyulması gereken Bilgi ve İletişim Güvenliği tedbirlerine yönelik denetimler yapılmakta ve T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin Portalına denetim sonuçları yüklenmektedir.

Bilgi ve İletişim Güvenliği Rehberinin Varlık Gruplarına Yönelik Güvenlik Tedbirleri bölümünün Uygulama ve Veri Güvenliği başlığı altında Kişisel verilerin uygulamalarda korunması kapsamında denetim soruları bulunmaktadır (Dijital Dönüşüm Ofisi, 2020, s. 98). Özellikle güvenli yazılım geliştirmeye yönelik tedbirler ve bu tedbirlerin denetimine yönelik ifadeler kişisel verilerin yazılım geliştirilmesi sürecinde göz önüne alınmasının önemini ortaya koymaktadır. Bilgi ve İletişim Güvenliği Rehberinin Uygulama ve Veri Güvenliği bölümündeki Güvenli Yazılım Geliştirme kısmındaki tedbir tanımlarında "Yazılım geliştirme sürecinde güvenlik gereksinimleri tanımlanmalı ve bu gereksinimler göz önünde bulundurularak tasarım yapılmalıdır." ibaresi yer almaktadır. Rehberin birçok bölümünde kontrol edilen hususlar arasında veri güvenliği tedbirleri yer almaktadır. Milli Siber Güvenliğin sağlanması maksadıyla söz konusu rehbere uyumun tüm kurum ve kuruluşlara yaygınlaştırılacağı düşünüldüğünde tasarım aşamasında gizlilik kavramının her geçe gün önem kazanacağı görülmektedir.

Sonuç

En kapsayıcı yasal düzenleme olan Anayasa ile korunan insan hakları ve genel kamu düzeni, özel alanlarda oluşturulan birçok kanun ile tamamen bir hukuk şemsiye ile korunmaktadır. Ancak gelişen teknoloji bu korumanın sadece kanunlar ile olamayacağı görülmektedir. Özellikle kişisel veriler alanında en büyük otoritenin, verinin sahibi olan kişinin kendisi olduğu ortaya çıkmaktadır. Kişinin verisini öncelikle kişi kendisi korumalıdır. Sosyal ağlar gibi kişileri veri paylaşmaya teşvik eden uygulamalar sayesinde mükemmele yakın sonuçlar üreten yapay zekâ uygulamaları ortaya çıkmıştır. Gelinen süreçte görülmüştür ki; kanunların kişilerin verisini koruması ancak kişilerin de aynı doğrultu da hareket etmesiyle mümkün olabilecektir. Kişinin kendi verisinin değerine önce kendisinin farkına varması ve koruma çabasında olması bu alanda ulaşılması gereken ana hedef olmalıdır. Bu hedefe ulaşmak ta ancak farkındalık yaratmak ve bilinçlendirmekle mümkün olabilecektir. Dijital okur yazarlık olarak adlandırılan ve dijital cihazlar ile internet ortamının güvenli ve bilinçli kullanımı anlamına gelen bu kavramın tüm kişilerce benimsenmesi ve öğrenilmesi gerekmektedir. Kişisel verileri korumak için kanunların yanında mutlaka bilinçli veri sahipleri olmalıdır.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazar, çıkar çatışması olmadığını beyan etmiştir.
Finansal Destek: Yazar, bu çalışma için finansal destek almadığını beyan etmiştir.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflicts of interest to declare.
Financial Disclosure: The author declared that this study has received no financial support.

Kaynakça

Bolayır, M. A. (2024). Yapay zekâ, insan hakları ve insan haklarının korunması açısından yapay zekânın denetimi. *TIDE AcademIA Research*, *5*(2), 117-145.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 208-229.

Clicks'us Digital. (2023). *Dijital Türkiye 2023 raporu*. https://www.clicksus.com/we-are-social-2023-global-ve-turkiye-raporu

Çetindemir, Ç. (2024, 06 Şubat). *'Deepfake' tuzağıyla 25 milyon dolarlık vurgun*. https://www.aa.com.tr/tr/teyithatti/blog/deepfake-tuzagiyla-25-milyon-dolarlik-vurgun/1817367

Dijital Dönüşüm Ofisi. (2020). *Bilgi ve iletişim güvenliği rehberi*. T. C. Cumhurbaşkanlığı.

Durham-Hutchins, L. (2024, 7 Mart). *Facial recognition and data Protection: What you need to know*. https://www.dataprivacyadvisory.com/facial-recognition-and-data-protection-what-you-need-to-know/

Elitaş, T. (2022). Djital manipülasyon 'deepfake' teknolojisi ve olmayanın inandırıcılığı. *Hatay Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *19*(49), 113–128.

Gültekin, N. M. (2012). *Kişisel verilerin ceza hukuku yönünden korunması* (Yayımlanmamış yüksek lisans tezi). Galatasaray Üniversitesi.

International Organization for Standardization. (2023a). ISO 31700-1:2023(en) Consumer protection-Privacy by design for consumer goods and services-Part 1: High-level requirements.

International Organization for Standardization. (2023b). ISO 31700-2:2023(en) Privacy by design for consumer goods and services Part 2: Use cases.

Johnston, D. (1999). *Roman law in context.* Cambridge University Press.

Kandır, M. O. (2023). Deepfake teknolojisi ile çocuk müstehcenliği ve çocuk mahremiyetine dijital tehdit. In B. Kent, M. K. Baş, & M. Samar (Eds.), *İnternet Hukukunda Çocuğun Korunması ve Mahremiyeti* (pp. 195-213). Adalet Yayınevi.

Korkmaz, İ. (2017). *Kişisel verilerin ceza hukuku kapsamında korunması*. Seçkin Yayıncılık

Küzeci, E. (2019). *Kişisel verilerin korunması*. Turhan Kitapevi.

Stanford University. (2024). *AI index report 2024*. https://aiindex.stanford.edu/report/

Sütlüoğlu, T. (2015). Sosyal paylaşım ağlarında gençlerin sosyalleşme ve kimlik inşası süreçleri: Facebook örneği. *Folklor/Edebiyat*, *21*(83), 125-147.

Şimşek, O. (2008). *Anayasa hukukunda kişisel verilerin korunması*. Beta.

Şirin, M. C. (2017). Fransa ve Türkiye'de korunması gereken çocuk ve çocuk koruma idaresinin tarihsel gelişimi. *Çocuk ve Medeniyet Dergisi*, *2*(3), 43-69.

Temir, E. (2020). Deepfake: Dezenformasyon çağında yeni dönem ve güvenilir haberciliğin sonu. *Selçuk İletişim*, *13*(2), 1009-1024.

Timurturkan, M. (2019). Ebeveynlik ve dijital dünya: Anneliğe ilişkin yaratılan yeni temsiller ve dayanışma örüntüleri. *Mediterranean Journal of Humanities*, *9*(1), 315-333.

Türk, G. D., & Demirci, E. (2016). Sanal dünyada dönüşen mahremiyet algısı: Instagram örneği. In 1st International Academic Research Congress (pp. 518-525). Pegem Akademi.

Üstündağ, A. (2020). *Çocuk ve ekran: Dijital medya ve çocuk gelişimi*. Eğiten Kitap.

Van Dijck, J. (2013). You have one identity: Performing the self on Facebook and LinkedIn. *Media, Culture & Society*, *35*(2),199-215.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220.

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, *9*(11), 39-52.