ESKİŞEHİR BAROSU DERGİSİ

Sosyal Medyanın Bilişim Suçlarına Etkisi

Av. Murat Osman KANDIR*

Öz

İnternet siteleri ve mobil uygulamalardan oluşan sosyal medyanın en popüler tarafı olan sosyal ağlar kullanıcılara online profil oluşturarak kendi yaşamları ile ilgili resim, video, konum, düşünce gibi kişisel bilgileri paylaşma imkânı vermektedir. Bazen bu sosyal ağlarda yapılan paylaşımlar siber suçların kaynağı olmaktadır. Sosyal medya ortamında işlenen suçlar teknolojinin yaygınlaşmasına paralel olarak artış göstermiştir. Siber suçlar üzerindeki etkisini anlayabilmek için sosyal medya kavramını anlamak gerekmektedir.

Anahtar Kelimeler

Sosyal medya, Siber suç, Sosyal ağ, Facebook, Instagram.

* Eskişehir Barosu,, mkandir@yahoo.com, ORCID: 0000-0001-6918-6622.

ESKİŞEHİR BAR ASSOCIATION JOURNAL

The Effect of Social Media on Cyber Crimes

Abstract

Social networks, which are the most popular part of social media consisting of websites and mobile applications, allow users to create an online profile and share personal information such as pictures, videos, locations, thoughts about their own lives. Sometimes, the posts made on these social networks are the source of cybercrime. The crimes committed in the social media environment have increased in parallel with the widespread use of technology. In order to understand its impact on cybercrime, it is necessary to understand the concept of social media.

Keywords

Social Media, Cyber crime, Social network, Facebook, Instagram.

GİRİŞ

Dijital dönüşümün yaşanmasıyla birlikte çevremizdeki her şey dijital ortama taşındı. Sohbetler ve arkadaşlıklar da buna dahildir. Sosyal ağ uygulamalarının hayatımıza girmesiyle birlikte bireyler arasında ve bireylerin oluşturduğu grupların içerisinde çok farklı bir iletişim şekli oluştu. Geleneksel arkadaşlıklar geri planda kalırken yeni tip sanal arkadaşlıklar ön plana çıkmaya başladılar. Bu yeni tip iletişimin en büyük özelliği yüz yüze iletişimden uzaklaşmak ve dijital iletişime geçiş yapılmasıdır. Bu yeni iletişim modeli kendine has suç ve suçluları da beraberinde getirdi. Suç ve suçlu profilleri de bu dijital çağa uygun bir hal almaya başladılar. Kanun koyucu dijital ortama uygun hukuksal düzenlemeleri yapsa da tüm suç tiplerinin belirlenmesi elbette mümkün olmadı. Türk Ceza Kanunu'nda Bilişim Suçları başlığı altında dijital ortamda işlenen bazı suç tipleri tanımlansa da bilişim suçlarının buradaki suç tipleri ile sınırlı olmadığı kısa zamanda görülmüştür. Bilişim Suçları başlığı altında tanımlanan suç tipleri ile ilgili somut olaylar ile karşılaşma sıklığının bilişim sistemleri aracılığıyla işlenen geleneksel suç tipleri kadar olmadığı görülmüştür. Özellikle Sosyal Medya platformları kullanılarak hakaret, tehdit, cinsel taciz, çocuk pornografisi vb. yeni suç kavramlarının gün geçtikçe daha sık karşılaşılır olduğu belirlenmiştir[1]. Suç tipleri incelendiğinde sosyal ağlar kullanılarak işlenen suç tiplerinin hem bilişim suçları başlığı altındaki suçların hem de bilişim sistemleri kullanılarak işlenen suçların oluşturduğu grupların içinde oldukları görülmektedir. Birde bu sosyal ağ ortamlarının kullanılmasıyla işlenen suçları da düşündüğümüzde üç farklı suç grubuyla karşılaşıyoruz. Dijital çağda her yeni teknolojik keşif kendi suçlarını da beraber getiriyor. Bilişim sistemleri ve sosyal ağların içinde olduğu somut adli olayları düşündüğümüzde, geleneksel suçların işleniş yöntemleri, delillerin tespit edilmesi, delillerin değerlendirilmesi gibi özellikleri ile geleneksel suç tiplerinden çok farklı oldukları görülmektedir. Her ne kadar dijital deliller hayatın her alanında ve hukuk sisteminin her noktasında da sıklıkla görülmeye başlansa da dijital çağın suçları ve suçlularının kendine özgü bir dünyası olduğu tartışılmaz bir gerçektir. Bir de her yaştan kullanıcısıyla birlikte hayatımızın tam ortasında yer alan sosyal ağ uygulamaları düşünüldüğünde iletişim teknolojileri bakımından bambaşka bir çağın başladığını söyleyebiliriz. Sosyal ağların her yönüyle hayatımızı etkilemesini izlerken buradaki iletişim ve etkileşimlerin suç ve suçlular üzerindeki etkisini de göz ardı edemeyiz. Önce bu ilginç ve yeni iletişim ortamını tanımak gerekiyor.

[1] Nursel Yalçın ve Filiz Gürbüz, 'Sosyal Ağlarda İşlenen Suçlar, Facebook Sosyal Ağı Örneği', Akademik Bilişim Konferansı, Eskişehir 2015.

I. SOSYAL MEDYA VE SOSYAL AĞLAR

Lietsala/Sirkkunen sosyal medya kavramını bir şemsiye kavram (üst kavram) olarak kabul etmektedir, bunun altında online içerik ve sisteme içerikle dahil olan kişilerle bağlantılı olan çeşitli ve farklı kültürel uygulamaların bulunduğunu belirtmektedir[2]. Sosyal medya şemsiyenin altına girdiğimizde karşımıza önce sosyal ağ uygulamaları çıkmaktadır. En son hayatımıza giren ama en öne çıkan uygulamaların da bu sosyal ağ uygulamaları olduğunu söyleyebiliriz. Daha sonra ise geçmişte çok popüler olan ama sosyal ağ uygulamalarının hayatımıza girmesiyle birlikte o eski popülerliğini kaybeden bloglar karşımıza çıkmaktadırlar. Kendilerine artık pek ihtiyaç duyulmayan sohbet siteleri de artık çok fazla kullanıcıya hitap etmemektedirler. Forumlar ise teknik bilgi paylaşım siteleri olarak bu şemsiye altında yerini almaktadır. Aslında WhatsApp uygulamasında kurulan gruplar artık bu teknik bilgi paylaşılan sabit forumların yerlerini çoktan aldılar. Forum sitelerinin WhatsApp uygulamasına karşı tek artı özelliği kimlik ve telefon numarası paylaşılmadan üyelik imkânı vermesi gösterilebilir. İnternet sözlükleri de yine karşılıklı bilgi paylaşımlarına imkân veren internet kaynakları olarak sosyal medya kavramının içerisinde kabul edilmektedir.

Yaygın kullanılan sosyal ağ uygulamalarına odaklanırsak ilk farkına vardığımız özellik her ortama uygun uygulamalar olduğudur. Her türlü işletim sistemi için hazır uygulamaları olan, her türlü bilişim cihazında çalışma özelliğine sahip olan uygulamalar olduğunu görebiliyoruz. Bu sunulan uygulama çeşitliliği platform bağımsız denilebilecek bir özelliktir. Bizden kaçamazsınız! der gibiler sanki. Hemen ilk aklımıza gelen sosyal ağ uygulamalarından Instagram ve Facebook bu konuda en güzel örneklerdir. Tüm amaç profil oluşturmak ve olabildiğince çok profili arkadaş ağına dahil etmektir. Kullanıcılar sürekli bir içerik oluşturma ve veri paylaşma eğilimi içerisindedirler. Bu durumdan da anlaşıldığı üzere sosyal ağlarda sürekli bir veri üretimi ve veri paylaşımı olmaktadır.

Dijital pazarlama ajansı We Are Social'ın "Digital in 2022" raporunda Türkiye istatistiklerine bakıldığında Ocak 2022 itibariyle Türkiye'de kişilerin günlük ortalama 8 saat internet kullandığı görülmektedir. Ülkemizde 69,95 milyon internet kullanıcısı mevcuttur. Okul öncesi çocukları hesaba katmazsak neredeyse ülkenin tamamına yakını internet kullanmaktadır diyebilecek durumdayız. Bugünkü nüfusun %82'si internet kullanıcısı olarak görülmektedir. Aynı rapora göre bilgisayar başında geçirilen süre 3 saat 31 dakika iken bu sürenin 2 saat 59 dakikası sosyal medyada geçirilmektedir. Türkiye'de insanların günlük 4 saat 24 dakikasını

[2] Katri Lietsala ve Esa Sirkkunen, Social Media. Introduction To The Tools And Processes Of Participatory Economy (Tampere Üniversitesi Yayınları 2008) 17-18.

mobil cihazlarda geçirdiği yine rapordan anlaşılmaktadır. Raporda verilen zamanlar göz önüne alındığında sosyal ağların insanları etkileme gücü görülecektir[3].

Türkiye'de Facebook uygulaması kullanıcı sayısı Ağustos 2021 itibarıyla yaklaşık 62 milyon ve Instagram uygulaması kullanıcı sayısı ise yaklaşık 50 milyon civarındadır[4]. Söz konusu platformlar arkadaş sayısı veya takipçi sayısı gibi farklı isimlendirmelere sahip olsa da aynı amaca hizmet eden bir yayılma politikası izlemektedirler. Çeşitli yöntemler kullanarak daha geniş kitlelere yayılma çabası göstermekteler. Bahse konu platformlar, bazen kullanıcılarını motive etmek için kullandıkları reklam kazancı gibi ekonomik, bazen de daha çok takipçisine sahip olan profil sahipliği gibi sosyolojik hedeflerle yayılımcı bir politika izlemekteler.

Sosyal ağ uygulamalarında profil oluşturmak başlangıçtır. Sosyal ağ mantığında en önemli konu olabildiğince verinin toplanması ve veri analitiği çalışmaları ile anlamlı sonuçlar üretilmesidir. Veri madenciliği en çok kullanılan yöntemlerden birisidir. Sosyal ağ platformları tarafından yapılan iş, kullanıcılardan toplanan veriler işlenerek elde edilen bilgilerin kullanılması ve kullanıcılara yeni profillerin sunulması işlemidir. Daha doğrusu çok paylaşım yapan ve çok içerik üreten kullanıcı profili sosyal ağlar tarafından daha fazla tercih edilen kullanıcı olmaktadır. Anaokulu bilgisini profilinde paylaşan bir kullanıcı aynı anaokulunda aynı zamanda bulunmuş olan diğer profillerin ağına dahil olmakta ve ağını geliştirmektedir. Bu bir alışkanlık haline dönüşmekte ve her türlü kişisel bilginin arkadaş ağını genişletmek maksadıyla sosyal ağlarda paylaşılmasına neden olmaktadır. Aynı ortak geçmişe, aynı ilgi alanlarına sahip kişiler birbirlerini bu siber dünyada kolayca bulmakta ve birbirleriyle bağlantı kurabilme imkanına sahip olmaktadırlar.

İnternetin hızla yaygınlaşması ve bilişim cihazlarının zorunlu birer ihtiyaca dönüşmesi sosyal ağların yaygınlaşmasının en önemli nedeni olmuştur. Sosyal ağ uygulamalarının ilklerinden olan Facebook 4 Şubat 2004 tarihinde hayatımıza girmiştir[5]. Bu tarihten itibaren internette boy gösteren sosyal ağ uygulaması sadece internet tarayıcıları ile görüntülenebiliyordu. Kullanıcılar Facebook uygulamasına bilgisayarlarından ulaşabiliyor ve bir e-posta adresi ile profil oluşturabiliyorlardı. Teknolojinin gelişimi ve mobil cihazların siber dünyada yerlerini almalarıyla mobil cihazlara uygun mobil uygulamalar geliştirilmeye

[3] Simon Kemp, 'Another Year Of Bumper Growth' (Digital 2022) <https://wearesocial.com/uk/blog /2022/01/digital-2022-another-year-of-bumper-growth-2> Erişim Tarihi 21 Aralık 2022.
[4] https://www.statista.com, Erişim Tarihi: 21 Ekim 2021
[5] Emily Scanlan, Parker Davis, Bethany Curtis ve Bailey Newman, 'Censorship on Facebook', BYU School of Communications COMMS 382: Global Issues in Communications, (12 Nisan 2022).

başlandı. Mobil uygulamalarda ilk olanlar sosyal ağ uygulamalarıydı. Kullanıcı dostu arayüz tasarımları ve oldukça kolay olan profil oluşturma yöntemleri ile kısa zamanda mobil cihazların vazgeçilmezleri oldu. Halihazırda birçok mobil işletim sistemleri mobil cihazlar üzerinde sosyal ağ uygulamalarını içerecek şekilde kullanıcılara sunulmaktadır[6].

Sosyal ağ uygulamalarında kolay profil oluşturma ve bir an önce paylaşım yapma isteği kullanıcıları hızlı ve dikkatsiz davranmaya itmektedir. Zorunlu bilgileri bir an önce doldurup hemen siber dünyada yerini almaya çalışan kullanıcılar sosyal ağ platformlarının kullanıcılara sunduğu üyelik sözleşmelerini bile okumadan onaylamakta ve bir an önce uygulamayı kullanmaya çalışmaktadırlar. Kullanıcı ve üyelik sözleşmeleri son derece önemli sözleşmelerdir. Kullanıcıları sorumluluk altına sokan ve uygulama sahibi olan şirketlerin ise kullanıcılara karşı sorumluluklarını sınırlayan maddelerle doludurlar. Kullanıcılar birçok sorumluluğu uygulamayı kullanarak peşinen kabul etmiş sayılmaktadırlar. Bu durumu ancak bir güvenlik problemi ile karşılaşıp kabul ettikleri sözleşmeleri okumak zorunda kaldıklarında fark edeceklerdir[7].

II. SOSYAL AĞLAR VE KİŞİSEL VERİLER

Ülkemizde en çok kullanılan sosyal ağ uygulamalarının başında gelen Instagram ve Facebook uygulamalarının kullanıcı ve üyelik sözleşmeleri incelendiğinde yukarıda açıklandığı gibi kullanıcıya ağır sorumluluklar yükledikleri açıkça görülmektedir. Neredeyse bir kitap kapsamı kadar bilgiye sahip olan Hakkında, Koşullar, Gizlilik, Yardım vb. başlıklara sahip bilgilendirici bölümlerde hemen hemen her konuda açıklamalar bulunmaktadır. Birçok dilde hazırlanan bu bölümlerde kullanıcılara paylaştıkları verilerin nasıl kullanılacağı açıkça anlatılmaktadır. Kullanıcıların paylaştıkları kişisel verilerin hangi şirketlere verilebileceği, hangi uygulamalarda kullanılabileceği vb. bilgiler açıklanmaktadır. Aynı ilaç prospektüslerini sadece yan etkiler oluştuğunda okuma ihtiyacı duyulduğu gibi bu tür bilgilerin verildiği sayfalara da ancak bir sorunla karşılaşıldığı zaman başvurulması sıklıkla karşılaşılan bir durumdur.

Endüstri 4.0 ile birlikte en değerli varlık olan "veri" korunmaya muhtaçtır. Verinin korunması için her yerde paylaşılmaması ve dikkatli kullanılması şarttır. Dağınık olarak sosyal ağlarda paylaşılan içerikler uygun şekilde toparlanıp analiz edildiğinde değerli bilgilere

[6] Sajithra K ve Rajindra Patil, 'Social Media – History and Components', 2013 7 (1), IOSR Journal of Business and Management 69, 69-74.
[7] Murat Kandır, 'Instagram Kullanım Koşulları' <https://www.mkandir.av.tr/2022/03/19/instagram-kullanim-kosullari-1/> Erişim Tarihi 3 Ocak 2023.

dönüşmektedirler. Maalesef bu çok değerli bilgiler kişilerin kendi rızalarıyla paylaştıkları verilerden oluşmaktadırlar. Her geçen gün Kişisel Verilerin değeri artmakta ve korunmaları için yeni yasal düzenlemeler yapılmaktadır. Dijital dönüşümün hızlı bir şekilde gerçekleşmesi kişisel verilerin değerini artırmıştır. Birçok hizmetin siber ortama taşınarak dijitalleşmesi ve bu hizmetlere erişim sağlanırken kişisel verilerden faydalanılması güvenli erişim için veri güvenliğinin önemini ortaya çıkarmıştır. Siber suçlular yapmayı planladıkları siber saldırıların ilk adımı olarak keşif yapmaktadırlar. Bu keşfin amacı ise kendilerine hedef seçtikleri kullanıcılara ait verileri sosyal medyadan temin etmek ve bu verileri kullanarak saldırılarını gerçekleştirmektir.

İnternetin Derin Web (Derin Ağ) veya Dark Web (Karanlık Ağ) olarak bilinen bir bölümü vardır. Bu bölümde uyuşturucudan silaha, yasal olmayan içeriklerden kişisel verilere kadar birçok şeyin ticareti yapılmaktadır. Kişisel verileri bir şekilde ele geçiren siber suçlular DeepWeb ya da Dark Web olarak adlandırılan bölümdeki yasal olmayan internet sitelerinde verileri pazarlamaktadırlar[8]. Dünyadaki istihbarat örgütlerinin ihtiyaç duydukları bilgilerin %80 gibi bir miktarını açık kaynak dediğimiz ortamlardan elde ettikleri gerçeği istatistik olarak bilinmektedir[9].

III. AÇIK İSTİHBARAT KAYNAĞI OLARAK SOSYAL AĞLAR

Sosyal Ağların ana hedefi kullanıcıların içerisinde oldukları sosyal ilişkiler yardımıyla diğer profilleri ağlarına dahil etmeleri veya onların ağlarına dahil olmalarıdır. Bu şekilde ağlar genişlemekte ve takipçi sayıları, arkadaş sayıları gibi sosyallik ölçüm parametreleri artmaktadır. Sosyal ağlarda başarı bu sayıların büyüklüğüyle ölçülmektedir. Bu sayılar sosyalleşmenin bir göstergesi olduğu kadar sayılar büyüdükçe kontrolde zorlaşmaktadır. Binlerce arkadaşı olan bir profil sahibi arkadaşlarının profillerini takip edememekte ve hiç tanımadığı kullanıcıların bir şekilde ağına sızmalarına engel olamamaktadır. Sosyal ağ kullanıcıları ilgi alanlarına uygun içeriklerin olduğu sayfaları takip etmekte ve bu tür paylaşımların yapıldığı gruplara üye olmaktadırlar. Kullanıcıların sosyal ağ kullanım eğilimleri bilen siber korsanlar tuzak sayfalar hazırlamakta ve gruplar oluşturmaktadır. Bu gruplara katılan kullanıcıların bilgilerini sosyal mühendislik tekniklerini kullanarak ele geçirmeye çalışmaktadırlar. İlgi alanlarına yönelik güncel içerikleri takip eden kullanıcıları sahte

[8] Miloš Ilić ve Žaklina Spalević, (2017) 'The Use of Dark Web for the Purpose of Illegal Activity Spreading', (2017) 63 (1) Ekonomika, 73-82.
[9] Sudhanshu Chauhan ve Nutan Kumar Panda, 'Hacking Web Intelligence', (2015) (8) Network Security.

içeriklerle aldatarak kullanıcıları istismar etmekte ve kişisel verilerini ele geçirmeye çalışmaktadırlar[10].

Siber saldırı çeşitli adımlardan oluşan planlı ve sistematik bir eylemdir. Bu eylemin ilk adımı belirlenen hedefe yönelik saldırı yöntemini seçmek için hedefle ilgili bilgi toplama adımıdır. Bu aşamada hedefle ilgili her türlü bilgiye ihtiyaç duyulmaktadır. Ne kadar çok veri toplanırsa seçilecek saldırı yönteminin başarısı o derece artacaktır. Özellikle kişiler hakkında bilgi toplamak için Facebook ve Instagram gibi çokça kişisel medya içeren sosyal ağların kullanıldığı bilinmektedir. Söz konusu sosyal ağları sıkça kullanan profil sahipleri günlük rutinlerini bu ortamda çeşitli metin ve görsel içeriklerle tüm profillerin erişimine açık olarak paylaşmaktadırlar. Geleneksel suçların internet ve bilişim cihazları kullanarak işlendiği hallerde sosyal ağlardaki kişisel paylaşımlardan elde edilen bilgilerin önemi büyüktür[11].

Bir hırsızlık suçunun sosyal ağlardan elde edilen bilgilere dayandırılması belki de bu alanda verilebilecek en güzel örnek olacaktır. Tatilde olduğunu gösteren içerikleri sosyal ağ hesabından paylaşan bir aile tatil sonrası evine döndüğünde evinin hırsızlar tarafından soyulduğunu görmüştür. Hedef olarak bu ailenin seçilmesi sosyal ağlarda tüm ailenin paylaştığı tatil içerikleri sonrasında evin boş olduğunun hırsızlar tarafından öğrenilmesinden kaynaklanmıştı. Sosyal ağlar olmasa ve bu paylaşımlar yapılmasaydı evin boş olduğunu tespit etmek için hırsızlar günlerce izlemek zorunda kalacaklardı. Hiçbir zaman ailenin dönüş zamanını kestiremeyecekler ve bu kadar rahat hareket edemeyeceklerdi. Bu hırsızlık olayı sosyal ağların tüm suçlular tarafından bilgi ve istihbarat kaynağı olarak kullanıldığının en güzel örneğidir[12].

Teknolojinin her geçen gün gelişmesi çok farklı suç tipleri ile karşılaşılmasına neden olmaktadır. Yapay zekâ teknolojilerindeki gelişmeler de suçlular tarafından kullanılınca o güne kadar hiç karşılaşılmayan suçların gerçekleşmesine ve siber ortamın kendi suçlularını yaratmasına imkân vermektedir. Yapay zekâ teknolojisinin temelinde yapay sinir ağları bulunmaktadır. Yapay sinir ağları verilerle eğitilerek istenilen sonuçları elde etmektedir. Ses ve görüntü dosyaları ile eğitilen yapay sinir ağları benzer ses ve görüntü dosyalarını tekrardan istenilen şekilde üretme yeteneğine sahip olmaktadırlar. Özellikle Çekişmeli Üretici Ağ

[10] C.Dianne Martin, 'Taking The High Road White Hat, Black Hat: The Ethics Of Cybersecurity', (2017) 8 (1) ACM Inroads Magazine, 33, 33–35.
[11] Regner Sabillon, Jeimy J. Cano, Víctor Cavaller Reyes ve Jordi Serra Ruiz, 'Cybercrime And Cybercriminals: A Comprehensive Study' (2016) 4 (6) International Journal of Computer Networks and Communications Security 165, 165–176.
[12] Kolokotronis Nicholas ve Shialis Stavros, Cyber-Security Threats, Actors, and Dynamic Mitigation (1. B. CRC Press 2021) 372.

(Generative adversarial networks) olarak adlandırılan yapay sinir ağları ile resim ve video dosyaları gerçeğinden ayırt edilemeyecek şekilde yeniden üretilebilmektedir[13].

Bu yeni teknoloji ile şu an hayatta olmayan insanların bir şarkıyı seslendirmesi, bir reklam filminde oynaması mümkün olmaktadır. İnsanlar hiç gitmedikleri ülkelerde çekilmiş fotoğraflarını kolayca oluşturmakta ve sanki bir film yıldızı gibi ünlü filmlerde boy göstermektedirler. Hemen hemen her kullanıcının cep telefonunda bir yapay zekâ destekli fotoğraf işleme uygulaması bulunmaktadır. Kullanıcılar fotoğraflarını ya da kamera yardımıyla o anda çektikleri fotoğraflarını bu uygulamalar ile işleyerek kendilerinin çeşitli filtreler yardımıyla işlenmiş görüntülerine kavuşabilmektedirler. Ancak bu uygulamalar işlemek için bizde aldıkları her fotoğrafımızı veri tabanlarına eklemekte ve gerçek verilerden oluşan bir fotoğraf havuzu oluşturmaktadırlar. Mobil cihazlarımızda kullandığımız bu uygulamaların bizim fotoğraflarımızla kimlerle ve niçin paylaştığını tespit etmemize ne imkân vardır ne de engelleyebiliriz. Zaten uygulamaları bizden istediği erişim izinleriyle mobil cihazlarımıza kurduğumuz andan itibaren peşinen her türlü şartını kabul etmiş oluyoruz.

Mobil uygulamaların paylaşıldığı Playstore ve Applestore gibi platformlarda sunulan ücretsiz uygulamalar aslında kullanıcıların en değerli varlıklarını yani kişisel verilerini ücret olarak almaktadırlar. Ancak kullanıcılar ekonomik bir değer karşılığı bu uygulamalara sahip olmadıkları için ücret vermediklerini düşünmektedirler. Bu konuda söylenecek en güzel söz "Eğer bir şey için ücret ödemiyorsanız ücret -siz- oluyorsunuz demektir".

Kişilerin hiç söylemedikleri kelimeleri söylemiş ve hiç olmadıkları yerde bulunmuş gibi video ve resimlere sahip olduklarını görebilmekteyiz. Özellikle toplumca tanınmış kişilerin söylemedikleri sözleri onların seslerinden ve gerçeğinden ayırt edilemeyecek kadar sahici olarak duyabilmekteyiz. Günümüzde yapay zekâ ve bilgisayar yazılımlarının gerçek ses verisi ile çalışması sonucunda gerçekten ayırt edilemeyecek kadar başarılı, taklit ses verisi üretilmektedir. Aynı başarı görsel olarak da video ve resim üretilmesinde kullanılmış ve başarılı olunmuştur[14]. Bu tür taklit ses, resim ve video üretimi için bu medyaların gerçek örneklerine ihtiyaç duyulmaktadır. İşte bu taklit üretim sürecinin olmazsa olmaz parçası olan gerçek örnekler de çok rahat bir şekilde sosyal ağlar üzerindeki paylaşımlardan temin edilebilmektedir.

[13] Mukhiddin Toshpulatov, Wookey Lee ve Suan Lee, 'Generative Adversarial Networks And Their Application To 3D Face Generation: A Survey', 2021, 108 Image and Vision Computing, <https://www.sciencedirect.com/science/article/abs/pii/S026288562100024X> Erişim Tarihi: 19 Ocak 2023.
[14] Tianxiang Chen, Avrosh Kumar, Parav Nagarsheth, Ganesh Sivaraman ve Elie Khoury, 'Generalization Of Audio Deepfake Detection' Odyssey 2020 The Speaker and Language Recognition Workshop 1-5 November 2020, Tokyo, Japan, <https://www.isca-speech.org/archive_v0/Odyssey_2020/abstracts/29.html> Erişim Tarihi: 19 Ocak 2023.

Böylesi önemli olan kişisel verilerimizden ses, resim ve videolarımızı sosyal ağlar da paylaşmadan önce bir daha dikkatlice düşünmek büyük önem arz etmektedir.

Sosyal Ağ profilimizden paylaştığımız bilgiler hesabımıza giriş yaptığımız şifrelerimizi ele verebilmektedir. Eğer tüm bilgilerimizi ağımızda bulunan profillere değil de herkesin paylaşımına açarsak ve herkes bu bilgilere erişebilir ise bilgilerimiz profilimizin ya da e-posta adresimiz gibi diğer hesaplarımızın şifrelerinin tahmin edilmesinde kullanılabilmektedir. Doğum tarihi, eğitim bilgileri, aile fertleri, ev adresi, işyeri bilgileri vb. kişisel bilgilerin herkese açık ağda paylaşılması halinde böylesi bir sakınca bulunmaktadır. Herkese açık olarak paylaşılan bu bilgiler dünyada çokça kullanılan şifre oluşturma eğilimleri ile birleştirildiğinde ortaya muhtemel şifreler çıkmaktadır. Siber suçlular sadece belirli aralıklarla oluşturduğu muhtemel şifreleri hedef kullanıcıların çeşitli hesaplarının şifre bölümlerinde kullanarak hesapları ele geçirmeye çalışacaklardır[15].

IV. SOSYAL MEDYANIN VERDİĞİ ANONİMLİK DUYGUSU

Suç sosyolojisinde internet ortamında suçluları suç işlemeye yönelten önemli motivasyonlardan birisi de yakalanma riskinin düşük olduğunun düşünülmesidir. Özellikle "doğru olmayan kimlik bilgileri" ile oluşturulan profiller kullanılarak işlenen suçların da bu motivasyonla işlendiği düşünülmektedir. Gerçek sahibi bilinmeyen bu tür profiller üzerinden işlenen suçlar sonrasında kolluk kuvvetleri ve soruşturmadan sorumlu adalet birimlerinin iş yükü artmaktadır. Bu tür profiller suç sonrası kapatılarak delil toplanmasının engellenmeye çalışılması da ayrı bir yük getirmektedir. Bir de bu tür suçların büyük bir çoğunluğunun şikâyete bağlı olması ve şikâyet süresinin ise 6 ay olmasıyla birlikte bir süre kısıtlaması da durumu daha da karmaşıklaştırmaktadır.

Sosyal Medya kullanıcıları tarafından internet ve haberleşme teknolojisinin tam olarak bilinmemesi nedeniyle bu ortam bir anonimlik hissi vermektedir. Siber suçlular yakalanma risklerinin düşük olduğu kanısıyla suç işlerken rahat olmaktadırlar. Ancak siber dünya olarak adlandırılan bu ortamda hiçbir iz gerçekten silinmemektedir. İnternette gerçekleşen iletişim yöntemlerinin teknik tarafları incelendiğinde hiçbir veri hareketinin izinin tamamen silinmediği görülecektir. Dünyaca ünlü siber suçluların güvenlik güçleri tarafından yapılan dijital iz takipleri sonucunda yakalanmaları bu konuya en güzel örnek olacaktır. Bu ortamda yapılan her eylem mutlaka kaydedilmektedir. Nasıl dijital delillerde silinen veriler

[15] Gautam Kumar, Dinesh Kumar Saini ve Nguyen Ha Huy Cuong, Cyber Defense Mechanisms: Security, Privacy, and Challenges (Artificial Intelligence (AI): Elementary to Advanced Practices (1. B. CRC Press 2020) 230.

çeşitli teknik çalışmalar sonucunda geri getirilerek erişim sağlanabiliyorsa internette de paylaşılan her türlü veriye erişim sağlanabilmektedir[16].

Instagram ve Facebook kullanıcıları profillerini ve bu profilde paylaştıkları içerikleri silmeye karar verip sildiklerinde bu veriler 30 gün süre ile geri döndürülebilir şekilde sosyal ağ platformu sahibi şirketlerin sunucularında tutulmaktadır. Kullanıcı bu süre içerisinde fikrini değiştirirse tekrar profilini canlandırabilmektedir. Güvenlik önlemleri nedeniyle sosyal ağ platform sahibi şirketler tüm verilerini fiziksel olarak başka yerlerdeki veri tabanlarında da depoladıkları için profil sahibi tarafından silinen hesapların yedeklendiği veri tabanından silinmesi ise yaklaşık 90 günlük bir süre almaktadır. Bunlara ek olarak eğer sosyal medya platformlarının sahibi olan şirketler, bu silinen profildeki bilgilerin gelecekte sorun çıkarabilecek yapıda olduğu kanısına varırlarsa bu verileri hiç silmeyebilmektedirler. Görüldüğü üzere sosyal ağlar başta olmak üzere bir kez internet ortamında paylaşılan verilerin tamamen bu ortamdan silinmesi çok uzun zaman almaktadır. Eğer bir de internet sitelerinin birer örneklerini sürekli kopyalayıp depolayan arşiv maksatlı internet siteleri hesaba katıldığında paylaşılan verilerin sürekli dolaşımda kaldığı söylenebilir.

V. SOSYAL AĞLARIN KİŞİSEL VERİLERİN KORUNMASI KAPSAMINDA İNCELENMESİ

Özellikle Avrupa'nın Kişisel Veriler kapsamında yaptığı düzenleme olan General Data Protection Regulation (GDPR) sonrasında kişisel verilerin korunması büyük önem taşımaya başlamıştır. En çok kişisel verinin işlendiği ortamlar da Sosyal Ağlar olduğundan tüm dikkatler bu alana yönelmiştir. İnternete taşınan her türlü hizmet kişisel verileri kullanmaktadır. Hem resmî kurumlar hem de ticari çaba içerisinde olan şirketler kullanıcılardan en az adı soyadı ve telefon numarası bilgisi talep etmektedir. Bir de geri dönüşüm sağlamak ve kullanıcı adı olarak kullanmak için talep edilen e-posta adresi düşünüldüğünde kontrolsüzce ortada dolaşan kişisel verilerin olduğu aşikardır.

Sosyal ağlar ve bulut alanlarında kullanıcılara tahsis edilen alanların ücretsiz olduğu düşünüldüğünde kişisel verilerin önemi bir kez daha ortaya çıkmaktadır. Kişisel verilerin toplanarak büyük verinin oluşturulması ve bu verinin birçok alanda kullanılması yapay zekâ çağında büyük önem taşımaktadır. Sosyal ağ platformlarına sahip olan şirketler kullanıcılardan

[16] Turgay Henkoğlu, Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi (2. B. Pusula Yayınevi 2014) 290.

bir hizmet bedeli talep etmemektedirler. Kullanıcılar ise bu ücretsiz olan hizmetlerde aslında ücret olarak kişisel verilerini verdiklerinin çoğu zaman farkında değildirler[17].

Siber dünyada meydana gelen siber saldırıların çoğunda hedef kişisel veriler olmaktadır. Böylesi değerli verinin kendi isteğiyle kişiler tarafından sosyal ağ şirketlerine teslim edilmesi sürecinde şirketler tarafından kişiler ile yapılan sözleşmelerin önemli bir yeri vardır. Sosyal Ağ uygulamalarının kurulması sürecinde bazı sözleşmelerin kullanıcıya onaylatılması gerekmektedir. Kullanıcılar tarafından kişisel verilerine yönelik işlenmesi, transfer edilmesi, kullanılması ve paylaşılması hususlarında izin ve onay verilirken bilinçli olunması gerekmektedir. Onay verilirken onay kapsamı ve izinlerin gerekliliği sorgulanmalıdır[18]. Aksi halde verilen izinler sonrasında sosyal ağlarda paylaşılan kişisel veriler siber saldırganlar tarafından ele geçirilmekte ve sonrasında planlanan siber saldırılar için keşif bilgisi olarak kullanılmaktadır. Yapılan araştırmalar siber saldırılar öncesi siber korsanlar tarafından yapılan keşif çalışmalarında önceliğin sosyal ağlarda olduğunu göstermiştir[19].

VI. SOSYAL MEDYA YOLUYLA İŞLENEN SİBER SUÇLAR

Sosyal medyada karşılaşılan ve içerisinde bilişimin, bilişim cihazlarının etkili olduğu suçlara bakıldığında bir ayrım yapmak gerektiği anlaşılmaktadır. Yargıtay kararlarının incelenmesinde de bu tür bir ayrım yapıldığı görülmektedir. Bilişim suçları; doğrudan bilişim suçları (gerçek bilişim suçları); TCK. m. 243, 244, 245, 245/A ve 246. maddelerinde yer alan suçlar ve dolayısıyla bilişim suçları (bilişim bağlantılı suçlar); TCK. m. 112, 113, 125, 132, 133, 134, 135,136, 138, 142/2-e, 158/1-f, 213, 218, 226 ve 228. maddelerinde yer alan suçlar olarak ikiye ayrılmaktadır[20].

Doğrudan bilişim suçları mantık olarak bir bilişim sistemini hedef olarak alınan suçlar olarak düzenlenmiştir. Bilişim sistemleri ve bilişim sistemlerinin sahip olduğu veriler bu kapsamda suçun zarar verdiği süje olarak belirlenmiştir[21]. Bilişim sistemlerine yetkisiz erişim sağlanması, erişim sağlanan bilişim sisteminde bulunan verilerin bir şekilde zarar uğraması ya da bu verilerin manipüle edilmesi gibi çeşitli eylemler suç kapsamına alınmıştır. Ancak bilişim

[17] Olga Stepanova, ve Patricia Jechel 'The Privacy, Data Protection and Cybersecurity Law Review: Germany'. (2020) < https://t.ly/cEAF > Erişim Tarihi: 23 Aralık 2022.
[18] Ayşe Nur Akıncı, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, Kalkınma Bakanlığı (2017) <http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf> Erişim Tarihi: 24 Aralık 2022.
[19] Martin (n 10) 33–35.
[20] Yargıtay Ceza Daireleri Uygulamasında Sıklıkla Rastlanan Bozma Sebepleri (2. B. Türkiye Adalet Akademisi Yayınları 2018) 829.
[21] Yavuz Erdoğan, Türk Ceza Kanunu'nda Bilişim Sistemini Engelleme Bozma Verileri Yok Etme Değiştirme Suçu (Yayımlanmamış Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü 2011) 31.

gibi her gün yeni bir gelişmenin yaşandığı alanda kesin suç tanımları yaparak tüm alanı kontrol altında tutmak kolay değildir. Bu nedenle bazı eylemlerin hangi kanun maddesi kapsamına gireceğini belirlemek oldukça zor bir çalışma sonucunda ortaya çıkmaktadır. Özellikle konunun tamamen teknik olması bu durumu daha da zorlaştırmaktadır. Bilirkişilerin raporları bu alandaki mahkeme kararlarında oldukça belirleyici bir etkiye sahip olmaktadır. Hatta zaman zaman Bilişim suçları ile ilgili hazırlanan bilirkişi raporlarını anlaşılabilir kılmak için ayrı bir bilirkişiye bile ihtiyaç duyulabilmektedir.

Sosyal ağlarda doğrudan bilişim suçları kapsamında karşımıza çıkan siber saldırı yöntemleri genelde kişisel bilgileri hedef alan Kimlik Avı saldırılarıdır. Kullanıcıların sosyal ağ, e-posta, internet bankacılığı vb. dijital erişim bilgilerini ele geçirmek için sosyal ağların kullanım eğilimlerini ve alışkanlıklarını kullanan bu saldırılar kullanıcıları aldatmaya yönelik saldırılardır. Kişilerin iradelerini sakatlayarak onlardan gerçekte asla vermeyecekleri bilgileri ele geçirmeye yönelik yapılan eylemlerdir[22]. Bir de bu saldırıların daha teknik olan tarafı vardır. Bilişim sitemlerine yetkisiz erişim yapılması kapsamında zararlı yazılımların (virüs, truva atı, vb.) kullanılarak hedef bilgisayarda erişim hakkı kazanılması kapsamında sosyal ağlar kullanıcılara bu yazılımların gönderilmesi amacıyla kullanılmaktadır[23]. Bu nedenle güvenlik uzmanları sürekli olarak kullanıcıları sosyal ağlardan kendilerine gönderilen mesajlardaki bilinmeyen bağlantılara tıklamamaları gerektiği, bilinmeyen Ek dosyaları indirmemeleri gerektiği konularında uyarmaktadırlar.

Dolaylı bilişim suçlarında ise bilişim cihazları bir araç olarak kullanılmaktadır[24]. Buradaki geleneksel ve klasik olan suçlar internetin ve bilişim cihazlarının sağladığı bazı avantajların kullanılması yardımıyla işlenmektedir. İnternetin sağladığı anonimlik b kapsamda büyük rol oynamaktadır. Kullanıcıların kendilerini görünmez olarak hissetmeleri bu bölümdeki suçların gerçek dünyada yüz yüze olarak işlenmesiyle karşılaştırıldığında çok daha kolay işlenir olduğunu göstermektedir. Sosyal ağlar dolaylı bilişim suçlarında ise bir suç işleme platformu şekline dönüşmektedir. Gerçek hayatta bir araya gelmeleri çok zor olan binlerce insan bir sosyal ağ uygulamasının sunduğu hizmetle bir grup oluşturarak anında iletişim ve etkileşim imkanına kavuşmaktadır. Bir müddet sonra bu ortam bir suç mahaline dönüşebilecektir.

[22] Mert Küçükvardar, 'Suç Olgusunun Değişen Yüzü: Siber Suçlar' (2018) (1) Uluslararası Bilişim, Teknoloji ve Felsefe Dergisi 1, 1-17.
[23] Özge Apiş, 'Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri' (2018) (37) Yasama Dergisi 49, 49-86.
[24] Ahmet Gül, Doğrudan Dolaylı Bilişim Suçları (3.B, Seçkin Yayıncılık 2021, Ankara) 56-57.

Sosyal ağların suç işleme maksatlı kullanımından önce bilgi toplama amaçlı kullanıldığından bahsetmiştik. Son yıllarda sosyal ağların yeni medya kapsamında kitleleri etkileme gücünün büyük bir hızla arttığına şahit olduk. Bu kapsamda dezenformasyon ve manipülasyon yapılarak sosyal ağ kullanıcılarının etkilenmesinin mümkün olduğu görülmüştür. Böylesi güçlü bir teknolojinin merkezinin yurt dışında olması bu gücün etkilerinden zarar görmemek için alınabilecek önlemler açısından da büyük bir güçlük çıkarmaktadır. Bu kapsamda 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun kapsamında değişiklikler yapılarak çeşitli önlemler alınmaya çalışılmıştır.

Uygulamada karşılaşılan suçlara bakıldığında sosyal ağlar ve internette yayımlanan diğer blog, internet sitesi, forum vb. platformlar kullanılarak işlenen suçların büyük bir çoğunluğunun bilişim sistemlerinin araç olarak kullanıldığı suçlar olduğu görülmektedir. Klasik olarak işlenen suçlar olan hakaret ve tehdit bilişim sistemleri kullanılarak gerçekleştirilebilmektedir. Sözlü, yazılı ve yüz yüze olarak işlenen hakaret ve tehdit suçları bilişim sistemleri üzerinden işlendiğinde de aynı şekilde ve aynı hükümlere göre cezalandırılacaktır. Ancak burada bir fark ortaya çıkmaktadır. Suçu işleyen kişi yüz yüze bir ortam olmayan internet ortamında istediği bir kimliğe bürünebilmektedir. Sosyal ağların en büyük zaaflarından birisi olan anonimliğe izin vermesi ile bu tür suçlarda kolayca suç işleyenin kimliğine erişmek mümkün olmamaktadır. Suçun failinin sosyal ağlar üzerinden gerçek olmayan kimlik bilgileri ile yaratmış olduğu sosyal ağ profilini kullanarak, "kendini tanınmayacak bir hale sokarak" işlemesi durumunda failin cezasının TCK m. 106/2(b)'deki "Kişinin kendisini tanınmayacak bir hâle koyması suretiyle..." düzenlemesi nedeniyle ağırlaştırılması söz konusu olacaktır.

Suç işlendikten sonraki soruşturma süreci ise geleneksel suçlara oranla daha karmaşık bir hal almaktadır[25]. Suçun işlendiği ortam siber ortamdır. Kimliklerin net olmadığı profillerin gerçeği yansıtıp yansıtmadığının belli olmadığı adeta karanlık bir samanlık gibidir. Böylesi bir ortamda dijital deliller ve dijital delillerin hemen elde edilmesi hususu çok önemli bir hale gelmektedir[26]. Büyük bir hız ve hassasiyetle delillerin toplanması ve soruşturmaya başlanması

[25] Cumhur Şahin, 'Ceza Muhakemesinde Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma' (2019) 1 (2) Yaşar Hukuk Dergisi 271, 271-286.
[26] Merve Erdem ve Gürkan Özocak, 'Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği' <http://ozocak.com/Dosyalar/d863d5.pdf> Erişim Tarihi: 15 Kasım 2021.

bir zorunluluktur. Aksi halde dijital delillere ulaşmak mümkün olmayacak ve suçla ilgili en önemli ispat aracı olan dijital delillerden mahrum kalınacaktır[27].

Sosyal ağlarda hakaret, tehdit gibi suçlar uygulamada en çok karşılaşılan suç tipleridir. Bu suçların yanına cinsel taciz suçu da eklenebilir. Özellikle sosyal ağlara üyelik esnasında ciddi bir yaş sınırlaması olmadığından hemen her yaştan bilişim sistemi kullanıcısı rahatça sosyal ağ profilleri oluşturup kullanıcı olabilmektedirler. Sosyal Ağ Uygulamalarının sahibi olan şirketler beyana dayalı bir üyelik sistemine sahiptirler. Her ne kadar bazı uygulamaları 18 yaş üzeri kullanıcıların hizmetine sunuyor olsalar da bu yaş kontrolü kullanıcıların beyanı ile yapılmaktadır. Cinsel taciz ve özellikle çocukların hedef alındığı müstehcenlik ya da daha çok çocuk pornografisi olarak da bilinen bu suçların öncelikli hedefi çocuk yaştaki sosyal ağ kullanıcıları olmaktadır. Sosyal ağların herkesin birlikte aynı ortamda bulunacağı bir şehir meydanı gibi düşünüldüğünde hedef olarak belirlenen kişilere ulaşmak çok kolay olmaktadır. Böylesi sisli bir ortam her türlü suçun işlenmesine kolaylık sağlayan bir ortam haline gelmiştir. Sosyal ağların yapısı itibarıyla ve cinsel taciz suçunda kanun koyucunun failin fiziksel temasını aramaması, failin mağduru "cinsel amaçlı olarak taciz etmek" davranışını suçun oluşması için yeterli görmesi sosyal ağlarda özellikle mesajlaşma kapsamındaki etkileşimlerde fazlaca karşılaşılan bir suç olarak karşımıza çıkartmaktadır. Failin mağdura karşı cinsel içerikli sözler söylemesi veya bu amaçla görseller paylaşması cinsel taciz suçunu oluşturacaktır.

Özellikle yeni teknolojiler olarak adlandırabileceğimiz Blockchain, NFT ve Metaverse gibi kavramlar sosyal ağların bu teknolojilerin tamamlayıcısı olarak kullanılmasına neden olmuştur. Non-fungible token kelimelerinin kısaltması olan NFT Türk Dil Kurumu tarafından Nitelikli Fikri Tapu olarak Türk diline kazandırılmıştır. Resim, müzik, video, tweet, sosyal ağ durumları, makaleler, pul koleksiyonlarındaki pulların dijital görünümleri ve dijitalleştirilebilen her türlü medya NFT olarak dijital ortama aktarılabilmektedirler. NFT ticareti internet üzerinde kurulan pazaryeri adı verilen internet sitelerinde yapılmaktadır. Kripto varlıklara ve Blockchain teknolojisine ilgi duyan meraklıların aktif olduğu birçok sosyal ağ grupları ve sayfaları bulunmaktadır. Sosyal ağlarda irili ufaklı birçok bu tür grup görmek mümkündür. Bunu fırsat bilen siber korsanlar kullanıcıları tuzağa düşürmek için ünlü grupların sahte profillerini ve sayfalarını açarak var olmayan NFT'leri kullanıcılara satmaya çalışmaktadırlar. NFT'lere merak duyan kişilerin bu merakını kullanan siber korsanlar hem

[27] Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku (9. B. Seçkin Yayıncılık, 2022) 741

kişisel verilerin hem de haksız kazanç elde etmenin peşindeler. Siber hırsızlar NFT hırsızlığı için Sosyal ağları yoğun bir şekilde kullanmaktadırlar.

SONUÇ

Doludizgin yaşadığımız internet sürecinin en önemli aktörleri tartışmasız sosyal ağ uygulamalarıdır. İnternet kullanım yaşının anaokulu yaşı ile eşit seviyede olduğu bir çağ yaşanmaktadır. Mobil cihazlar bebeklerine mama yedirirken annelerin en büyük yardımcısı olmuş durumda! Amerikan ordusu bağımlılık listesine cep telefonu ve internet bağımlılığını ekledi. Yakın bir gelecekte sosyal ağ bağımlılığının da Amerikan ordusunda bağımlılık olarak tanımlanacağı konuşuluyor. İnterneti eğitim amaçlı kullananların sayısının internette sadece sosyal ağları kullananların sayısına oranla çok daha az bir miktarda olduğu araştırma sonuçlarına yansımaktadır. Sosyal ağlar sayesinde nickname denilen isimlendirme şekli hayatımıza girmiş durumda. Sosyal ağlarda ünlüler ve ticari işleri için kullananlar hariç kendi kimliğini kullananların sayısı her geçen gün düşüyor. E-posta ve sosyal ağ profillerinin oluşturulma koşullarının kontrol altında olmamasından kaynaklanan bir karmaşa ortama hakim olmuş durumda.

Sosyal ağlara üye olmak için sadece bir e-postanızın olması yeterli olmakta. O e-posta sahibi olmak için ise hiçbir bilginizin kontrol edilmemesi zaten ortamdaki kimlik doğrulama sürecinin ne durumda olduğunu gözler önüne seriyor. Maalesef bu belirsizlik karanlık bir ortamın oluşmasına meydan veriyor. Böylesi bir bilinmezlik kendi suç ve suçlularını yaratmakta hiç geç kalmıyor. Sosyal ağlarda işlenen siber suç olarak tanımladığımız suçların kolayca işlenmesi kullanıcıların profil oluştururken kimliklerini maskeleyerek ağlarda boy göstermelerine doğrudan bağlı olarak gözükmektedir. Bahsettiğimiz anonimlik hissi kullanıcıların gerçek dünyaya oranla daha rahat hareket etmelerine olanak veriyor. Son yüzyılda bilgisayar oyunlarına gösterilen ilgi sanal dünyada farklı kimliklere bürünme konusunun daha fazla ilgi çekmesine neden oldu. Özellikle internet üzerinden gerçek kişilerin çevrimiçi olarak birbirlerine karşı oynadıkları ve yoğun şiddet içeren oyunlar insanların zihninde sanal dünya ile gerçek dünyanın zaman zaman birbirine karışmasına neden olmaya başladı.

Okula giderken çocuklarını tanımadıkları yabancı kişilere karşı sıkı sıkıya tembihleyen anneler çevrimiçi oyunlarda tanımadıkları yabancı kişilere teslim ederken aynı hassasiyeti göstermiyorlar. Muhtemelen bu rahatlık fiziksel temasın olmayacağı düşünülmesinden kaynaklanıyor. Ancak birçok suçun işlenmesi için aynı fiziksel ortamda bulunulma zorunluluğun olmaması göz ardı ediliyor. Toplu taşıma aracında çocuğuna biraz dikkatlice bakan kişilerden rahatsız olan ebeveynler, çocuklarının resimlerini sosyal ağlar

üzerinden milyonlarca insanın görebileceği bir erişim yetkisiyle paylaşabiliyor. Ancak ciddi bir adli olay yaşandığında sanal ortamın da en az gerçek dünya kadar zararlı ve tehlikeli olduğu anlaşılıyor. Buradaki problem sahalarının en başında ebeveynlerin dijital okur yazarlık konusundaki eksiklikleri geliyor. Bu eğitim eksikliğinin sonucunda ise mağdur çocuklar ve dolayısıyla mağdur ebeveynler olmaktadır.

Pandemi döneminin eğitim ve ticaret alanlarında internet kullanımını neredeyse zorunlu hale getirmesiyle artan internet kullanımı kullanıcı sayısının artmasına ve kullanıcı yaşının düşmesine neden olmuştur. Artan teknoloji kullanıcısı sayısına karşın kullanıcıların siber güvenlik bilgisinin yeterli olmaması da siber suçların artışında etkili olmuştur.[28] İnsanların gerçek kimliklerini, yaşlarını, cinsiyetlerini vb. özelliklerini saklayarak bu ortama girmeleri hayal ettikleri kimliklere bürünmeleri ve daha da önemlisi dijital ortamda kimlik tespitinin çok daha zor olması bu ortamda suç işlemeyi çekici hale getirmiştir. Sosyal ağlar yardımıyla yapılacak dezenformasyonun kısa zamanda göstereceği yıkıcı etki de göz önüne alındığında bu sosyalleşme ortamlarının ne kadar tehlikeli olabileceği tahmin edilebilecektir. Ülkemizde yapılan yasal düzenlemelere rağmen hala sosyal ağ platformlarının sahibi şirketler gerekli önemi göstermemekte ve yetkili kişilerini ülkemizde görevlendirmemektedirler. Halihazırdaki internet teknolojileri merkeziyetsiz uygulamalara sahip değildir. Gelecekte bir de merkeziyetsiz internet teknolojilerinin hayatımıza gireceği düşünüldüğünde gerektiğinde sorumlu tutulacak sosyal ağ platformu sahibi bir şirket bulamayacağız. Halen tam otonom araç teknolojilerinde bir kaza sonrasında sorumluluğun kimde olacağı konusu açıklığa kavuşamamışken, yapay zekanın sorumluluk sahibi olup olamayacağı tartışmaları devam ederken merkeziyetsiz internet teknolojilerinde kime hesap sorulacağı konusuyla ilgili ortada hiçbir ipucu bulunmamaktadır.

[28] James H. ve Usha D., The Pocket Guide to Cyber Security, (Amazon Digital Services LLC - KDP Print US, 2020) 84.

KAYNAKÇA

Akıncı AN, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, Kalkınma Bakanlığı (2017) <http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf> Erişim Tarihi: 24 Aralık 2022.

Apiş Ö, 'Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri' (2018) (37) Yasama Dergisi, 49-86.

Chauhan S. ve Panda NK, 'Hacking Web Intelligence', (2015) (8) Network Security.

Chen T, Kumar A, Nagarsheth P, Sivaraman G. ve Khoury E, 'Generalization Of Audio Deepfake Detection' Odyssey 2020 The Speaker and Language Recognition Workshop 1-5 November 2020, Tokyo, Japan, <https://www.isca-speech.org/archive_v0/Odyssey_2020/abstracts/29.html> Erişim Tarihi: 19 Ocak 2023

Dülger MV, Bilişim Suçları ve İnternet İletişim Hukuku (9. B. Seçkin Yayıncılık, 2022)

Erdem M. ve Özocak G, 'Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği' <http://ozocak.com/Dosyalar/d863d5.pdf> Erişim Tarihi: 15 Kasım 2021.

Gül A, Doğrudan Dolaylı Bilişim Suçları (3.B, Seçkin Yayıncılık 2021, Ankara)

Henkoğlu T, Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi (2. B. Pusula Yayınevi 2014)

Ilić M. ve Spalević Z, (2017) 'The Use of Dark Web for the Purpose of Illegal Activity Spreading', (2017) 63 (1) Ekonomika, 73-82.

James H. ve Usha D., The Pocket Guide to Cyber Security, (Amazon Digital Services LLC - KDP Print US, 2020)

Kandır M, 'Instagram Kullanım Koşulları' <https://www.mkandir.av.tr/2022/03/19/instagram-kullanim-kosullari-1/> Erişim Tarihi 3 Ocak 2023.

Kemp S, 'Another Year Of Bumper Growth' (Digital 2022) <https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2> Erişim Tarihi 21 Aralık 2022.

Kumar G, Dinesh Kumar Saini ve Nguyen Ha Huy Cuong, Cyber Defense Mechanisms: Security, Privacy, and Challenges (Artificial Intelligence (AI): Elementary to Advanced Practices (1. B. CRC Press 2020)

Küçükvardar M, 'Suç Olgusunun Değişen Yüzü: Siber Suçlar' (2018) (1) Uluslararası Bilişim, Teknoloji ve Felsefe Dergisi, 1-17.

Lietsala K. ve Sirkkunen E, Social Media. Introduction To The Tools And Processes Of Participatory Economy (Tampere Üniversitesi Yayınları 2008)

Martin DC, 'Taking The High Road White Hat, Black Hat: The Ethics Of Cybersecurity', (2017) 8 (1) ACM Inroads Magazine, 33–35.

Nicholas K ve Stavros S, Cyber-Security Threats, Actors, and Dynamic Mitigation (1. B. CRC Press 2021)

Sabillon R, Cano JJ, Cavaller Reyes V. ve Serra Ruiz J, 'Cybercrime And Cybercriminals: A Comprehensive Study' (2016) 4 (6) International Journal of Computer Networks and Communications Security, 165–176.

Sajithra K ve Patil R, 'Social Media – History and Components', 2013 7 (1), IOSR Journal of Business and Management, 69-74.

Scanlan E, Davis P, Curtis C. ve Newman B, 'Censorship on Facebook', BYU School of Communications COMMS 382: Global Issues in Communications, (12 Nisan 2022).

Stepanova O, ve Jechel P, 'The Privacy, Data Protection and Cybersecurity Law Review: Germany'. (2020) < https://t.ly/cEAF >Erişim Tarihi: 23 Aralık 2022.

Şahin C, 'Ceza Muhakemesinde Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma' (2019) 1 (2) Yaşar Hukuk Dergisi, 271-286.

Toshpulatov M, Lee W. ve Lee S, 'Generative Adversarial Networks And Their Application To 3D Face Generation: A Survey', 2021, 108 Image and Vision Computing, <https://www.sciencedirect.com/science/article/abs/pii/S026288562100024X> Erişim Tarihi: 19 Ocak 2023.

Yalçın N. ve Gürbüz F, 'Sosyal Ağlarda İşlenen Suçlar, Facebook Sosyal Ağı Örneği', Akademik Bilişim Konferansı, Eskişehir 2015.

Yargıtay Ceza Daireleri Uygulamasında Sıklıkla Rastlanan Bozma Sebepleri (2. B. Türkiye Adalet Akademisi Yayınları 2018)

Yavuz Erdoğan, Türk Ceza Kanunu'nda Bilişim Sistemini Engelleme Bozma Verileri Yok Etme Değiştirme Suçu (Yayımlanmamış Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü 2011)

<https://www.statista.com>, Erişim Tarihi: 21 Ekim 2021