

DİJİTAL İLETİŞİM TEKNOLOJİLERİNİN GETİRDİĞİ SUÇ TEHLİKESİNİN UNFRIENDED DARK WEB FİLMİ ÜZERİNDEN İNCELENEMESİ

**Muhammed Taha CUMAN*

ÖZET

Dijital iletişim teknolojileri, insanlara kendilerini ifade etmeleri, başkalarıyla bağlantı kurmaları ve çeşitli nedenlerle örgütlenmeleri için alan oluşturmaktadır. Teknolojinin hızlı ilerlemesi kolaylık sağlamakla beraber ciddi tehlikeleri de beraberinde getirmektedir. Bu çalışmanın amacı, dijital iletişim teknolojilerinin ilerlemesi ile ortaya çıkan takip edilmesi güç suç alanı yarattığına dikkat çekmek ve sinemada nasıl yansıtıldığını incelemektir. Nitel araştırma yöntemiyle yapılan bu çalışma, amaçlı örneklem yoluyla seçilen Unfriended Dark Web filmi ile sınırlandırılmıştır. Unfriended Dark Web filmi dijital iletişim teknolojilerinin karanlık tarafını ve internetin görünmeyen tarafını ortaya koyan bir filmidir. Bu kapsamda betimsel analiz ile yapılan çalışmada belirli dikkat çekilmesi gereken noktalar saptanmış ve filmin içeriği bu noktalar çerçevesinde incelenmiştir. Bu film Dark Web ile gelen tehlikeleri öngörmektedir. Dark Web genellikle suçlular ve bilgisayar korsanları için bir sığınak olarak tasvir edilmektedir. Ancak film, Dark Web'in derinlerine inildiğinde meydana gelebilecek rahatsız edici ve tehlikeli durumları göstererek onu bir adım öteye taşımaktadır. Film, internetin birçok alanını keşfederken dikkatli olunması gerektiğini ve dijital iletişim teknolojilerinin kullanımının yeterli denetim yapılmadığı ve önlem alınmadığı takdirde kişisel gizliliği ortadan kaldırabilmektedir.

Anahtar Kelimeler

Dijital iletişim teknolojileri, Unfriended: Dark Web, Suç, Dark Web, Kişisel veri gizliliği

ABSTRACT

Digital communication technologies are enabling people to express themselves, connect with others and create space for them to establish and organize for various reasons. The fast pace of technology progress brings convenience but also serious dangers. This The aim of the

study is to analyze the difficult-to-trace emergence of digital communication technologies with the advancement of to draw attention to the fact that it creates a space for crime and to examine how it is reflected in cinema. Qualitative This study, which was conducted with the research method, was conducted with Unfriended Dark It is limited to the movie Web. The movie Unfriended Dark Web is an example of how digital communication Technologies is a movie that reveals the dark side and the invisible side of the internet. In this context In the study conducted with descriptive analysis, certain points to be noted were identified and The content of the movie is analyzed within the framework of these points. This movie explores the dangers of the Dark Web foresees. The Dark Web is often used as a haven for criminals and hackers. Is depicted. However, the movie also depicts what can happen when you go deeper into the Dark Web. It takes it a step further by showing disturbing and dangerous situations. The movie shows that the internet that caution should be exercised when exploring many areas of digital communication technologies. The use of personal privacy unless adequate supervision is carried out and precautions are taken. Can handle it.

Keywords

Digital communication technologies, Crime, Dark Web, Personal data privacy, Unfriended: Dark Web

GİRİŞ

İnsanlık tarihi boyunca iletişim en önemli varlık tescili olmuştur. İletişim, insanların birbirleriyle bilgi, fikir ve duyguları paylaşmasını sağlayan temel bir araçtır. İnsanlar, binlerce yıldır iletişim yoluyla bilgi aktarmış, ilişkiler kurmuş ve toplumlar oluşturmuşlardır. İletişimin önemi ve etkisi, teknolojik ilerlemelerle birlikte daha da artmıştır. Günümüzün iletişim teknolojileri mekanı önemsiz kılacak seviyeye gelmiştir. İletişim ve teknoloji alanında kaydedilen hızlı gelişmeler, insan yaşamını kökten değiştirmiştir. Bu değişimin temel taşlarından biri ise internettir. İnternet, günümüzde milyarlarca insanın günlük hayatının bir parçası haline gelmiştir. 2000'li yıllarda, mobil cihazlar ve kablosuz internet teknolojilerinin gelişimiyle birlikte, internet erişimi daha kolay bir hale gelmiştir. Artık insanlar, cep telefonları, tabletler ve diğer taşınabilir cihazlar aracılığıyla her zaman ve her yerde internete bağlanabilmektedir. Bu da iletişimi, bilgiye erişimi ve çevrimiçi işlemleri daha da

yaygınlaştırmıştır. Arkadaş toplantıları, aile ziyaretleri, eğitim toplantıları gibi toplu aktiviteler fiziksel efor sarfetme gereksinimi duyulmadan internet aracılığı ile yapılabilir. Ancak bu durum sağladığı ciddi faydaların yanında büyük tehlikeleri de beraberinde getirmiştir.

İnternetin getirdiği birçok fayda olduğu gibi, aynı zamanda potansiyel tehlikeler de içermektedir. Siber uzay, sosyal etkileşimin yeni bir boyutunu yaratmış, zaman ve mekanı aşmıştır. Bu nedenle, fiziksel bağlam artık sosyal durumla bağlantılı değildir. İnternetin anonimliğini kullanan günümüz gençliğinin olumsuz siber davranışlarını, siber suçlar ya da bilgisayar korsanlığı ve giderek artan suçları araştırmak ve anlamak kritik hale gelmiştir. (Richet, 2018, s.51) Bilgi güvenliği, kişisel veri güvenliği, siber zorbalık ve internet bağımlılığı gibi riskler insan hayatını tehdit edebilecek seviyelerde görülebilmektedir. Bu durum dark web, siber suçlar, deep web ve insanların bunu kullanımı gibi kavramların anlamlarının ve aralarındaki farkların ayrıntılı bir şekilde incelenmesini gerektirmektedir. Teknoloji insanlara daha önce benzeri görülmemiş bir kimliklerini anonimlik kılıfı altında gizleyebilir ve utanç verici veya gayrimeşru faaliyetlerin cezasından kaçınabilirler. Oysa çok az insan bir oda dolusu yabancılarla çıplak fotoğraflarını paylaşabilir, seks hakkında konuşabilir veya yasadışı uyuşturucu kullanımını tartışabilirler. (Richet, 2018, s.51) Sinema filmlerinde de bu tehlikeler farklı yorumlarla ele alınmaktadır.

DİJİTAL İLETİŞİM TEKNOLOJİLERİ

Son yıllarda, dijital iletişim teknolojileri hızlı bir şekilde gelişmiş ve iletişim şekillerimizi kökten değiştirmiştir. Geleneksel iletişim araçlarına kıyasla dijital iletişim, daha hızlı, daha kolay ve daha etkili bir şekilde bilgi alışverişi yapmamızı sağlamaktadır. Sanayinin makineleşmeden başlayarak, elektrik endüstrisine otomasyondan ve İnternete doğru ilerleyen bir teknoloji devriminden söz edilmektedir. Bu bağlamda endüstri 4.0; bilişim, iletişim, internet, otomasyon, yapay zekâ ve robotik teknolojilerinin üretim süreçlerini yoğun biçimde etkileyen ve onların dönüştürmesi ile ortaya çıkan yeni bir durumu göstermektedir. (Görgün, A., 2020) Dijitalleşme veriyi sayısallaştırarak bilgisayarda okunabilir bir formata dönüştürmüştür. Bu sayede bilgisayara aktarılan veri hızlı ve kolay bir biçimde işlenerek diğer ağlara aktarılabilir. (Söğüt, Y. & Öngel, A., 2022) Ancak bu durum siber uzay içerisine girmiş verilerin başkaları tarafından da ulaşılabilir olmasını sağlayabilmektedir. Belli güvenlik önlemleri olsa da dijital ortamı yönetebilecek ve iyi düzeyde yazılım bilgisine sahip kişiler,

kişisel duvarları yıkarak özel hayatı ifşa edebilmektedirler. Bu durum kişiler arası özel görüşmelerin güvenliğini ciddi tehlikeye atabilmektedir.

DARK WEB

İnternetin derinliklerinde, genel erişime kapalı bir bölge olan Dark Web, gizlilik ve anonimlik arayan kullanıcılar için bir ortam sağlamaktadır. Dark Web, çoğunlukla yasa dışı faaliyetlerin gerçekleştirildiği, illegal mal ve hizmetlerin alınıp satıldığı bir alan olarak bilinmektedir. Günlük hayat içerisinde erişim olanağı olan internet ortamı, web tarayıcılarının eriştiği web sayfalarından ve arama motorları aracılığı ile listelenen web sayfalarından oluşmaktadır. Bu ortam internetin küçük bir kısmını oluşturmaktadır. Geri kalan büyük kısmı oluşturan parçalar da DeepWeb (derin ağ) ve DarkWeb (karanlık ağ) olarak adlandırılmaktadır. (Sönmez, G. & Çelik, E., 2020) Dark Web, dünyanın çeşitli yerlerinde konumlandırılmış bilgisayarlar ve farklı erişim yöntemleri ile bağlantı sağlanan ortamlardır. Ancak gündelik hayatta kullanılan web tarayıcıları ile erişmek mümkün değildir. Dark Web'e erişebilmek için özel ağ ayarları ve bu ağ üzerinden özel bir tarayıcı kurmak gerekmektedir.

Dark Web, siber suçluların güvenli bir şekilde iletişim kurduğu, bilgi ve diğer metaları paylaştıkları bir ortamdır. Dijital paranın çıkmasıyla ve ödeme aracı olarak kullanılmaya başlamasıyla Dark Web içerisinde para ile suç işlenmesinin önü de açılmıştır. Dijital para birimleri, kripto para birimleri ve sanal varlık hizmet sağlayıcılarının kullanımı, çok yüksek bir anonimlik seviyesi ve hareket kabiliyeti sağlayarak teröristlerin işini kolaylaştırmaktadır. (Yanarışik, O., 2022) Paranın kaynağına ilişkin hiçbir bilgi bulundurmadığından ve gerektiğinde sahibi tarafından nakit paraya dönüştürülebildiğinden ve alınıp satılabildiğinden dolayı kripto paralar, yasadışı faaliyetleri ve terörizmi destekleyebilmektedir.

SİBER SUÇ

Dijital iletişim teknolojilerinin gelişmesi ve yayılmasıyla dilimize yeni kavramlar da girmeye başlamıştır. Bunlardan en önemli olanı “siber” kelimesidir. “Siber” bilgisayar ve iletişim ağlarına yönelik, onları betimlemek için kullanılan bir sözcüktür. Çok sayıda metinde karşılaşılan siber alan kelimesi ise farklı şekillerde de olsa birbirleriyle etkileşim halinde olan sistemlerin ve insanların oluşturduğu alanı ifade etmek için kullanılır (Klimburg, A., akt. Küçükvardar, M. 2018). Siber uzay suçun ölçeğini ve kapsamını dönüştürür; kendi sınırları,

etkileşim biçimleri, rolleri, kuralları ve kendine özgü suç işleme biçimleri vardır. Bazı durumlarda, siber suç "geleneksel" suça yardımcı olmak için bilgisayar kullanımını kapsayabilir, ancak aynı zamanda teknoloji aracılığıyla aracılık edilen bir suç veya hizmet reddi gibi özel bir teknolojik suç da olabilir. (Görgün, A., 2020) Yar'a göre siber uzay ortamının yeni sosyo-etkileşimsel özellikleri (öncelikle mekansal-zamansal engellerin ortadan kalkması, çoktan çoğa bağlanabilirlik ve çevrimiçi kimliğin anonimliği ve esnekliği) yeni yasadışı faaliyet biçimlerini ve kalıplarını mümkün kılmaktadır. (akt. Richet, J-Y., 2018) Siber uzay suçun ölçeğini ve kapsamını dönüştürür; kendi sınırları, etkileşim biçimleri, rolleri vardır ve kuralları, kendine özgü suç işleme biçimleri vardır. (Capeller, 2001). Elektronikteki hızlı değişim ile gelişim ve elektronik süreçteki hız, elektronik ortamda işlenen suçlara ceza hukukunun ve bu suçların kendilerine uygun biçimde elektronik ortamda soruşturulması ve failin belirlenebilmesi yönünde, Ceza Muhakemesi Hukukunun uyum göstermesi zorunluluğunu doğurmuştur. (Keskin, S., 2001) Birçok ceza hukuku akademisyeni yasal çerçeveye odaklanmaktadır. Örneğin Wall ceza hukuku kategorilerini siber suç kategorileri oluşturmak için kullanmaktadır. Diğerleri ise siber suçları bir "bilgisayarlarla ilgili, içerikle ilgili veya gizliliğe, bütünlüğe ve kullanılabilirliğe karşı suç, bilgisayar veri ve sistemlerine karşı işlenen suçlar."

Siber ortamda işlenen suçların takibi ve denetiminin zorunlu olduğu görülmektedir. Ancak bu alanda denetim oldukça zordur. Öztürk siber güvenlik denetim modeli üzerine yaptığı çalışmada şu şekilde bir öneride bulunmuştur; *Siber güvenlik denetim faaliyetleri denetim ekibinin kontrolünde sürekli güncellenen denetim araçları ile gerçekleştirilmektedir. Siber saldırıları tespit edebilen teknolojik sistemler, güvenlik duvarları, anti virüs programları, Proxyler, tarayıcılar, IP adres takip sistemleri, bal küpleri, kriptolama algoritmaları, şifreleme sistemleri ile kod çözme ve şifre çözme sistemleri gibi sistem, program ve yazılımlar, denetim araçlarına örnek teşkil etmektedir. Denetim ekibinde, bilgi teknolojileri ve siber güvenlik konusunda uzman olan kişiler görev yapmalıdır. Denetimlerin bilgi teknolojileri departmanı ile icra edilmesi daha çok başarı sağlayacaktır.*

KİŞİSEL VERİ GİZLİLİĞİ

Kişisel veri, bireylerin kimliklerini belirli hale getirmeye elverişli her türlü bilgidir. Kişinin kimlik, iletişim, sağlık ve mali bilgileri ile özel hayatına, dini inancına ve siyasi görüşüne ilişkin bilgiler, kişisel veri olarak nitelendirilmektedir. (Çelik, Y., 2017) Kişisel verilerin korunması hakkının esas amacı, kişilerin özel hayatının gizliliğini güvence altına

olarak kamu veya özel sektör tarafından tutulan kayıtların korunması için gerekli önlemlerin alınması ve bu vasıta ile kişileri korumaktır. İnsan Hakları Evrensel Beyanname'si'nin 12. maddesi ile Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'nin 17. maddesi özel hayatın gizliliğinin korunması kapsamında "kişisel verilerin" korunmasına temel teşkil eden ilk uluslararası genel mahiyet taşıyan metinler olduğunu söylemek mümkündür (Kılınç, 2012) Elektronik haberleşme alanında meydana gelen gelişmeler kişi temel hak ve özgürlüklerinin koruma önlemlerinin geliştirilmesi ve özel hayata saygı ilkelerinin belirlenmesini gerekli kılmıştır. Kişisel verilerin korunması, çağımızda, insan hakları kavramı ve korunması bilincinin gittikçe gelişmesine paralel olarak önemini artırmaktadır. (Özdemir, H., 2009) Kişisel veri gizliliğine yönelik risklerin önemli bir boyutu ise, internette ve sosyal ağ sitelerinde bireylerin paylaştıkları kişisel bilgilere kimlerin erişebildiğidir. Bu bağlamda çevrimiçi gizlilik ve mahremiyet tehditleri ve riskleriyle ilgili tartışmalarda kişisel olarak nitelendirilebilecek bilgilerin tanımlanması ve bu bilgilere yönelik farkındalığın oluşturulması önemli olmaktadır (Aïmeur, Gambs, Ho, 2010)

UNFRIENDED DARK WEB FİLMİ ÖRNEĞİ

Bir internet kafede çalışmakta olan 20'li yaşlarındaki Matias, uzun süredir kafede duran ve kimsenin almadığı bir laptopu sahipsiz olduğunu düşünerek alır. Bilgisayarı kullanmaya başladığında ise içerisinde bazı gizli dosyalar bulur. Dark Web'e açılan bu dosyaları açtıktan sonra illegal bir örgütle karşı karşıya kalır.

Filmin çekiminde yeni iletişim teknolojileri kullanılmıştır. Kamera çekimlerinden faydalanılsa da seyirci yeni iletişim teknolojileriyle muhatap olacağı bilgisayar ve telefon ekran paylaşımlarıyla karşılaşmaktadır. Bir grup gencin sohbet amaçlı bulunduğu platform üzerinden tüm karakterlerin mekan tanıtımları tek bir ekran üzerinden yapılmaktadır. Filmin ana karakteri Matias'tır. Matias bilgisayarının eski olmasının verdiği eksiklik hissi ile çalıştığı internet kafede bulunan başıboş bir bilgisayarı çalar. Bu bilgisayar Dark Web üzerinde kurulmuş bir suç örgütü üyesinin bilgisayarıdır. Matias bilgisayarı kişisel cihazı olarak kullanmaya başlar. Kişisel bilgilerini bilgisayara girdikten sonra Matias'ın tüm bilgileri suç örgütünün eline geçer. Matias bilgisayarın içerisinde bulunan bazı dosyaları merak eder ve bunların içine girer. Bu dosyaların içerisinde bazı işlenmiş suçları görmesiyle suç örgütünün hedefi haline gelir.

Filmde Dark Web içerisinde kurulmuş olan ve insanlara çeşitli işkenceler yaparak bunu kaydedip yayınlarak gelir elde eden bir suç örgütü gösterilmektedir. Charon isimli örgütte

üyelerin sınıfları bulunmaktadır. Bulundukları kademeye göre numaralandırılmışlardır. Bu örgüt kendi içlerinde siber uzayda buldukları açıklarla suç işlemekte ve işledikleri suçları canlı olarak insanlara aktarmaktadırlar. Eğlence olarak suç işlemelerine rağmen herhangi bir denetim mekanizması ile karşılaşmadıkları görülmektedir. Dark Web içerisinde olmayan sıradan bir insanla karşılaştıklarında ise yakalanma ihtimallerine karşı her türlü kötülüğü yapabilmektedirler.

Suç örgütü sadece Matias'ın kullandığı bilgisayara erişim sağlayarak Matias ve görüşme sağladığı oturumda bulunan tüm arkadaşlarının IP adreslerinden bulundukları konumu, isimlerinden kişisel bilgilerini elde eder. Sadece Matias'ın bilgisayarı içerisinde bulunan bilgilerden yola çıkarak diğer arkadaşlarının kişisel bilgilerine, fotoğraflarına, anılarına ve bulundukları adrese onlarca bilgiye ulaşabilmektedirler. Ulaştıkları verileri kullanarak gençlerden birinin evine giderek intihar süsü vererek ölümüne sebep olurlar. Ölüm anında ise bulunulan çevredeki IP adreslerinden yayın yapan herhangi birinin telefonundaki görüntüyü gençlere izletirler. Bir diğer gencin ise daha önceden çekmiş olduğu videolardan ses kayıtlarını alıp montajlayarak polise terör eylemi hazırlığında olduğuna dair ihbarda bulunurlar. Eve polis geldiğinde ise bilgisayarına bağlanarak hoparlörden silah kabza sesi çıkartırlar. Çıkan sesle birlikte polis gence ateş eder ve ölümüne sebep olur. Elde ettikleri veriler ile tüm gençlerin arkalarında iz bırakılmadan ölümüne sebep olurlar. Matias tüm bu olanlardan kız arkadaşını kurtarmak için evinden çıkmışken suç örgütü eve işkence ettikleri bir kızı götürür. Son kalan arkadaşının adına film başından itibaren işlenen tüm suçları kendilerinin işlediğine dair mektup yazdırıp intihar süsü vererek öldürürler. Sonucunda da işlenen cinayetler ve suçlar üstüne kalmış olan Matias için bir oylama başlatıldığı gösterilir. Bu da suç örgütünün sadece suçları işleyen kişilerden olmadığını yüzlerce insanın bu suçları izlemek için para ödediği ve bundan keyif aldığı gösterilmektedir. Bu filmde Dark Web'in insan hayatını tehlikeye atan bir boyutu ve denetiminin zor veya eksik olmasından kaynaklı yaşanabilecek hatta belki yaşanan bir durumu ortaya koymuştur.

SONUÇ

İnternet günlük hayatımızı işlerimizi kolaylaştırmasının yanı sıra hayati riskleri de barındırmaktadır. Resmi ve gündelik işlerimizin büyük bir oranının dijital ortamda işlenmesi tüm bilgilerimizi internet ortamında paylaşmamızı gerektirmektedir. Ancak internet ortamında paylaşılan bu bilgiler bazı yazılımlar kullanılarak ele geçirilebilmektedir. Bu da ciddi güvenlik

sorunlarının ortaya çıkmasına sebep olmaktadır. Denetlenebildiği takdirde önüne geçilebileceği düşünülebilir. Ancak Dark Web denetim mekanizmasına tabi tutulabilecek veya takibi kolaylıkla sağlanabilecek bir ortam değildir. Sinemada bu konu üzerinde bilinçlendirme amaçlı filmler çekilmeye başlanmıştır. Makalede konu alınan *Unfriended Dark Web* filmi bu oluşumun ortaya çıkardığı insan hayatını takip edilemeyecek bir biçimde tehdit oluşturabileceği yönünde yorumlanmıştır.

KAYNAKÇA

Görgün A. , *Gençlik ve dijital çağ*, Hacettepe Üniversitesi, 2020

Söğüt, Y. & Öngel, A. (2022), *Yeni Medya-Dijitalleşme ve Tık Odaklılık: Habertürk ve Hürriyet Gazetesi Örneği*, ESAM Ekonomik ve Sosyal Araştırmalar Dergisi, c: 3 s: 2, Yıl: 2022, s. 212-230.

Sönmez G. & Çelik, E. (2020), *Anonimlik ile İlegalite Arasında: Deep Web, Dark Web ve Devlet Dışı Silahlı Aktörlerin Uluslararası Siber Faaliyetleri*, Güvenlik Çalışmaları Dergisi, 2022, c:22, s:1

Coşar M. , *Siber Dünyanın Karanlık Yüzü*, Journal of Management Theory and Practices Research, c:3, s:1, sf:58-71

Yanarışık O. (2022), *Terörizmin Finansmanında Siber Tehditler ve Kripto Paraların Rolü*, Üçüncü Sektör Sosyal Ekonomi Dergisi, s:57, sf: 3229-3241

Çelik, Y., (2017), *Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı*, TAAD, yıl:8, s.:32, sf: 391-410

Richet, J-Y., (2018), *How to Become a Cybercriminal? An Explanation of Cybercrime Diffusion*, The Dark Web:Breakthroughs in Research and Practice, sf: 51-63

Capeller, W. (2001). *Not such a neat net: Some comments on virtual criminality*, Social & Legal Studies, 10(2), 229-242.

Keskin, S., (2001), *Avrupa Konseyi Siber Suç Sözleşmelerinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi*, İstanbul Üniversitesi Hukuk Fakültesi Dergisi, sf. 155-180

Küçükvardar, M. (2018), *Suç Olgusunun Değişen Yüzü: Siber Suçlar*, I Sophos: Uluslararası Bilişim, Teknoloji ve Felsefe Dergisi, s:1, sf: 1-17

Öztürk, M.S. (2018), *Siber Saldırıları, Siber Güvenlik Denetimleri ve Bütüncül Bir Denetim Modeli Önerisi*, Muhasebe ve Vergi Uygulamaları Dergisi, sf: 208-232

Kılınç, Doğan (2012), *Anayasal Bir Hak Olarak Verilerin Korunması*, AÜHFD, s:61, sf:1089-1169.

Özdemir, H. (2009), *Haberleşmenin Gizliliği ve Kişisel Veriler*, Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi, s:13, sf: 285-303

Aïmeur, E., Gambs, S. ve Ho, A. (2010). *Towards a privacy-enhanced social networking site*. 2010 International Conference on Availability, Reliability and Security, sf: 172-179