ZfWT Vol 12, No. 3 (2020) **323-339**

BİLİŞİM TEKNOLOJİLERİNİN SUÇ EYLEMİ ÜZERİNDEKİ ETKİSİ: İNTERNET HABERLERİNDE DİJİTAL SUÇ ÖRNEĞİ

EFFECT OF INFORMATION TECHNOLOGIES ON CRIMINAL ACT: THE CASE OF DIGITAL CRIME ON INTERNET NEWS

Suat KOLUKIRIK[*]
Elif GÜN[**]

Özet

Zaman ve mekanın sınırlarını ortadan kaldıran bilişim teknolojileri sunduğu imkanlar ve sağladığı olanaklarla toplumsal ve bireysel yaşamın her alanında etkili olmaktadır. Dijital dönüşümün yol açtığı yeni pratikler, bireysel ve toplumsal yeni görünümler ortaya çıkarmakta ve farklılaşmaktadır. Öyle ki gündelik pek çok eylemimiz gibi suç türleri de giderek dijitalleşmekte, kapsamı ve niteliği değişerek daha kolay gerçekleştirilebilir hale dönüşmektedir. Dijitalleşmeyle birlikte ön plana çıkan suçlar ise doğrudan bilişim sistemini, verilerini ve bütünlüğünü hedef alan eylemlerle önemli bir güvenlik sorunu olarak kendisini hissettirmektedir. Bu perspektiften hareketle çalışmada, bilişim teknolojileriyle birlikte kapsamı ve niteliği değişen suç türleri irdelenerek artan teknolojik imkanların suç eylemleri üzerindeki etkisi belirlenmeye çalışılmıştır. İnternet haberleri bağlamında dolandırıcılık yöntemleri örneklem alanı olarak belirlenmiş, 2008 ve 2019 yıllarında dolandırıcılıkla ilgili en fazla içeriğe sahip olduğu belirlenen ve içinde dolandırıcılık kelimesi geçen hurriyet.com.tr'de yer alan toplam 464 haber değerlendirmeye alınmıştır. Çalışmada içerik analizi tekniği kullanılmış, gerçekleşme biçimlerine bağlı olarak, dolandırıcılık eylemini işleme biçimleri ve araçları kategorize edilerek sınıflandırılmıştır. Araştırmanın sonuçları bağlamında teknolojik ilerlemelerin beraberinde geleneksel suç eylemlerini dönüştürdüğü ve dijitalleşmeyi araçsallaştırdığı bulgulanmıştır.

Anahtar Kelimeler: Bilişim Teknolojileri, Dijitalleşme, Dijital/Siber Suç, Güvenlik, Dolandırıcılık

Abstract

Information technologies, which eliminate the boundaries of time and space, are effective in all areas of social and individual life with the opportunities and

[*] Prof. Dr., Akdaniz Üniversitesi Edebiyat Fakültesi Sosyoloji Bölümü Antalya /TÜRKİYE suatkolukirik@gmail.com Orcid: 0000-0003-0399-666X

[**] Arş. Gör., Akdaniz Üniversitesi Edebiyat Fakültesi Sosyoloji Bölümü Bölümü Antalya / TÜRKİYE *elifgun@akdeniz.edu.tr Orcid: 0000-0002-5916-7871*

possibilities they provide. Recent practices created by digital transformation reveal new personal and social profiles and differentiate. So much so that, like many of our daily actions, crime types are gradually becoming digital, changing their scope and nature, and becoming more easily realizable. Crimes that come to the fore with digitalization make themselves felt as an important security problem with actions that directly target the information systems, their data, and integrity. From this perspective, in this study, it is aimed to determine the effect of increasing technological opportunities on criminal acts by examining the types of crimes whose scope and nature changed with information technologies. In the context of internet news, fraudulence methods were determined as the sample, and a total of 464 news articles on hurriyet.com.tr, which included the word fraud and were determined to have the most content related to fraudulence between 2008 and 2019, were taken into consideration. Content analysis technique was used in the study, and the ways and means of processing fraudulent activity were categorized and classified depending on the realization methods. In the context of the results of the research, it has been found that technological advances have transformed traditional criminal acts and instrumentalized digitalization.

Keywords: Information Technologies, Digitalization, Digital/Cyber Crime, Security, Fraud

Giriş

Sapma ve suç bireyin doğayı ve kendini anlamlandırma ve yorumlama çabasının bir sonucu olarak toplumlar ve gruplar tarafından düzeni ve kontrolü sağlamak amacıyla gerçekleştirilmesi yasaklanmış davranışları ifade etmektedir. Sapkınlık bir toplumun çoğunluğu tarafından kabul edilen kurallara uygun davranmama olarak tanımlanırken bir alt sınıfı olan suç ise hukuki düzeyde yasaklanan ve sonucunda yasalar tarafından belirli yaptırımların uygulandığı eylemlere karşılık gelmektedir (Giddens, 2012, s. 842, 858). Dönemin koşulları, özgürlük anlayışı, bireyin değeri ve doğa ile olan ilişkisi, suç eylemine ve failine yaklaşım biçimini belirlemekte ve cezai yaptırımlar ve hukuki görünümler bu doğrultuda düzenlenmektedir. İlkel toplumlarda bilinmeyen doğa karşısında onlara tek rehber olan grup kurallarından sapan bireyler, tanrının öfkesinden kurtulabilmek için cezalandırılmaktayken bir sonraki aşamada, suçun özgür iradeyle gerçekleştirdiği düşüncesi hakim olmuş ve toplum, bireyin bu gönüllü eylemi karşısında ondan intikam almak amacıyla yaptırımlar uygulamıştır (Barnes ve Teeters, 2011, s. 163-164). Bedene acı çektirme ve bu acının sahnelenerek bir seyir unsuru olarak sunulduğu ceza anlayışı 18. yüzyıldan itibaren yerini yaygın yaptırım biçimi olan hapishanelere bırakmıştır (Foucault, 1992). Zira sosyo-ekonomik yapısıyla birlikte suçların kapsamı ve suç işleme eğilimleri değişmiş ve bunun bir sonucu olarak cezai yaptırımların yeniden düzenlenmesine ilişkin tartışmalar yoğunlaşmıştır. Bilgi ve iletişim teknolojilerinde yaşanan gelişmelerle birlikte suç unsuru

teşkil eden durumlar, eylemler, araçlar, suç faili ve mağduru farklı bir görünüm kazanmıştır. Nitekim bilginin güvenliği ve gizliliği, dönemin etik meselelerinin merkezinde konumlanır hale dönüşmüş (Sembok, 2004, s. 241) ve *Risk Toplumu* olarak ifade edilen olaylar yaşanır hale gelmiştir (Beck, 2019).

Bilişim teknolojileri, yeni suç türlerinin ortaya çıkmasının yanı sıra var olan suçların daha kolay bir şekilde işlenmesinin önünü açmıştır (Koçak ve Dandin, 2017, s. 138). Ortaya çıkan yeni suç türleri, sınırları aşan özellikleriyle de ön plana çıkmaktadır. Ulusal ve ulus ötesi suçların neredeyse hiçbir sınırı olmayan yeni biçimleri görülmektedir (Sembok, 2004, s. 242). Küresel düzeyde devletlerin ve kurumların bilişim teknolojilerine bağımlılığının artması, siber tehlikelere karşı daha kırılgan hale gelinmesini sağlamaktadır (Ghernaouti, 2013, s. 4). Dijital ve küresel dünyada bilişim sistemleri aracılığıyla zamansal ve mekânsal sınırlar ortadan kalkmış, kurumlar, şirketler ve bireyler hiç olmadığı kadar birbirine bağlı ve dışsal etkilere açık hale gelmiştir. Sunduğu yeni yaşam biçimleriyle birlikte teknoloji, toplumsal ve bireysel yaşamın her alanına hızla nüfuz etmiştir. Teknolojik gelişmelerin yaygınlaşmasıyla birlikte güvenlik, dijital çağın önde gelen problemlerinden birisi olmuştur. Diğer bir ifadeyle suçun kapsamı ulus ötesine taşınmış ve suç eylemi daha kolay gerçekleştirilebilir hale gelmiştir.

Bu çalışma kapsamında, günümüz dijital dünyasının güvenlik meselelerinin merkezinde yer alan suçun yeni görünümleri ve yükselen yeni eğilimi olarak karşımıza çıkan siber suçlar ele alınmakta ve değerlendirilmeye çalışılmaktadır. Çalışma kapsamında bilişim sistemlerinden ve imkanlarından yararlanılarak gerçekleştirilen klasik suç türlerine odaklanılmıştır. Türkiye'de son yıllarda dolandırıcılık suçunun teknolojik araçlar kullanılarak gerçekleştirildiği olaylar sıklıkla gündeme gelmektedir. Dolandırıcılık suçu 5237 sayılı TCK'nın 157. maddesi gereğince "[h]ileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan" eylemleri ifade etmektedir. 158/1. ve 2. bentleri gereğince ise dolandırıcılık suçunun nitelikli halleri tanımlanmıştır. Araştırma konusu kapsamında değerlendirilebilecek olan 158/1/f bendi gereğince ise "[b]ilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle" işlenen dolandırıcılık suçları tanımlanmıştır. Bu bağlam içerisinde çalışmada internet haberlerine konu olan olaylar sosyolojik bir perspektifle ve gerçekleştirilme yöntemleri özelinde irdelenerek değerlendirilmiştir.

1.Kuramsal Çerçeve

İçinde yaşadığımız dijital dünya tehlikeli bir alana dönüşmüş ve risk, saldırı, savunma ve koruma gibi yeni kavramlar ile özdeşleşir hale gelmiştir. Siber suçlar gizlilik ve anonimlik, motivasyon, fırsatlar, koruma ve sınır ötesilik gibi ortak temalarla şekillenir olmuştur (Grabosky ve Smith, 2001, s. 34-39). Teknolojik gelişmeler zamansal ve mekânsal sınırları ortadan kaldırma, gizlenebilme ve uzaktan erişebilme gibi imkanları ile yeni suç türleri ve eylemleri için fırsatlar sunmaktadır. Dönemin getirdiği imkanlar ve kolaylaştırıcı etkileriyle ön plana çıkan siber suçları anlama ve açıklamada, suç eylemini buna olanak sağlayan koşullar temelinde ele alan suç fırsatları yaklaşımları kapsamlı bir perspektif sağlamaktadır. Bu yaklaşıma göre fırsat, suçun ortaya çıkmasında temel rol oynamakta ve bazı ürünler, teknolojik ve sosyal değişimler, suç işlenmesi ve yeni suç türleri için cazip fırsatlar yaratabilmektedir (Felson ve Clarke, 1998). Bireylerin veya grupların suç işleme sebepleri ve kaynakları çeşitlenebilmekle birlikte, suç eylemi en iyi şekilde mevcut fırsatlar ve koşullar kapsamında anlaşılabilir olmaktadır (Clarke, 1983, s. 227). Diğer bir ifade ile fırsatın doğası, suçun nerede, nasıl ve kime karşı işleneceğini belirleyen ve etkileyen bir faktör olarak karşımıza çıkmaktadır (Lilly vd., 2019, s. 613).

Felson ve Clarke (1998) suç fırsatları yaklaşımını, suçu farklı açılardan ele alan ancak fırsatlar temelinde açıklama getiren 3 temel teoriyi içerdiğini ifade etmektedir. Bu kapsamda Suç Deseni Teorisi (crime pattern theory), Rasyonel Tercih Teorisi (rational choice perspective) ve Rutin Aktiviteler Teorisi (routine activity approach) sıklıkla kullanılan yaklaşımlardır. Suç Deseni Teorisine göre bireylerin ev, iş, okul, alışveriş ve eğlence mekanları gibi belirli güzergahlarda rutinleşmiş eylemleri sonucunda oluşan yoğunlaşmalar, zaman ve mekân bileşenleri içerisinde suç faili için çeşitli fırsatlar yaratmaktadır. Rasyonel Tercih Teorisi ise kişilerin suç eyleminin faydaları ve risklerini göz önünde bulundurarak suç eylemine yönelmelerine odaklanmaktadır (Felson ve Clarke, 1998, s. 6-7). Kişilerin gündelik yaşamlarında izledikleri rutinlere odaklanan Rutin Aktiviteler Teorisine göre ise motive olmuş suçlu, uygun hedef ve hedefin koruyucudan yoksunluğu, suç oranlarının anlaşılır olmasını sağlayan üç temel unsurdur ve bunların herhangi birinin eksikliği suç eyleminin gerçekleşmesine engel olabilmektedir (Cohen ve Felson, 1979). Aynı zamanda hedefin suça maruz kalma riskini belirleyen çeşitli unsurlar da söz konusudur. Bunlar, belirli bir değere sahip olan hedef ve bu hedefin taşınabilir, görünür, erişilebilir ve korumasız olmasıdır (Felson ve Clarke, 1998, s. 5). Bu risk unsurları dijital dünyaya taşındığında belirli değere sahip olan dijital varlıklar, dijital izler sayesinde kazandığı görünürlükle, uzaktan ulaşılabilir ve erişilebilir olabilmektedir. Aynı zamanda gerekli koruma alternatiflerinin olmaması,

güvenlik duvarlarının aşılması veya aldatılma gibi çeşitli yöntemlerle dijital kişisel verilere uzaktan ulaşım ve erişim sağlanabilir hale gelebilmektedir.

Suç fırsatları yaklaşımı suçun sebeplerine ve suçluyu rehabilite etme durumlarına odaklanmaktan ziyade, suçun oluşmasını sağlayan fırsat yaratıcı durumların ve koşulların kaldırılması ile suç eyleminin azaltılabileceği fikrine dayanmaktadır (Lilly vd., 2019, s. 613). Bilişim teknolojilerinin sağladığı kolaylık ve olanaklarla ortaya çıkan siber suçların azaltılabilmesi noktasında suç fırsatları yaklaşımının çözüm önerileri önemli bir perspektif sağlamaktadır. Günümüzde, siber risklere karşı korunma ve bilgi güvenliği sağlama amacıyla bireysel, kurumsal ve ulusal ölçekte ciddi yatırımlar yapılmakta ve önlemler alınmaktadır. Doğrudan, dolaylı ve savunma amaçlı olmak üzere pek çok toplumsal maliyeti olan siber suçlar, etki alanıyla birlikte mağdur ve suçluyu aşan dijital çağın önemli meselelerinden birisi olarak karşımıza çıkmaktadır (Anderson vd., 2013).

2.Dijital/Siber Suç ve Türleri

Günümüzde özellikle elektronik ağlar aracılığıyla gerçekleştirilen dolandırıcılık suçları yaygınlık kazanmakta ve büyümekte olan suç türleri olarak karşımıza çıkmaktadır (European Commission, 2007, s. 3). Dolandırıcılık en genel ifadeyle yalan ve yanlış beyanlarla başkasının zararına olacak şekilde onu kandırmak olarak tanımlanmaktadır (Black's Law Dictionary, 2004, s. 685). Günümüzde dolandırıcılığın nedenleri, motivasyonları ve amaçları aynı kalmaya devam etmekle birlikte eylemin gerçekleştirildiği ortamlar değişmiş ve dijital alanda var olmaya başlamıştır (Kovacich, 2008, s. 23-24). Başlı başına önlenebilmesi zor olan dolandırıcılık suçunun üstesinden gelebilmek, teknoloji ve küreselleşmeyle giderek daha da zorlaşmıştır (Anderson vd., 2013, s. 267).

Üzerinde uzlaşılmış bir tanım olmamakla birlikte siber suç, bilgi ve iletişim teknolojileri kullanılarak gerçekleştirilen çeşitli illegal aktiviteleri kapsamaktadır (Ghernaouti, 2013, s. 30-31). Bilgi ve iletişim teknolojileriyle her geçen gün iç içe geçmeye başlayan ve yeni türleri ortaya çıkan siber suçları sınıflandırmak ve kapsamına dahil olan suçları tasnif edebilmek, üzerinde uzlaşı sağlanamayan bir diğer durumdur. Dijital ya da siber suç türlerine ilişkin sınıflandırmalar aynı zamanda suçu anlama, önlem alabilme, hukuki temellerini ve cezai yaptırımlarını belirleyebilme noktasında işlevsel bir öneme sahiptir. Bu kapsamda literatürde çeşitli sınıflandırma girişimlerinin olduğu görülmektedir:

Council of Europe (2005) dijital/siber suçları 4 başlık altında sınıflandırmaktadır:

- Bilgisayar verilerinin ve sisteminin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı işlenen suçlar (Bilgisayar korsanlığı, casusluğu vb.)
- Bilgi teknolojileri kullanılarak işlenen klasik suçlar (Dolandırıcılık vb.)
- İçerik ile ilgili suçlar (Çocuk pornografisi, ırkçılık, sabotaj vb.)
- Verilerin telif haklarıyla ilgili suçlar (Bilgisayar programı, video, kitap vb.)

European Commission (2007, s. 2) ise dijital/siber suç türlerini 3 kategori içerisinde ele almaktadır:

- Ağ ve bilişim sistemlerinden yararlanılarak gerçekleştirilen geleneksel suçlar (Dolandırıcılık, sahtekarlık vb.)
- Yasa dışı içerik yayınlama (Irkçılık, çocuk istismarı vb.),
- Elektronik ağlara özgü suçlar (Bilgi sistemine yönelik saldırılar, bilgisayar korsanlığı vb.)

Furnell (2001) ise UK Denetleme Komisyonunun (UK Audit Commission) dijital/siber suç kapsamında ele aldığı suçları inceleyerek 2 ayrı kategori içerisinde değerlendirme yapmıştır:

- Bilgisayar destekli suçlar: Bilgisayar sistemi ortaya çıkmadan önce de var olan ancak bilgisayar teknolojilerinin imkânlarından yararlanarak gerçekleştirilmeye devam eden suçları ifade etmektedir. Dolandırıcılık, sabotaj ve hırsızlık gibi suçlar da bu kapsamda yer almaktadır.
- Bilgisayar odaklı suçlar: Bilgisayar teknolojisinin bir sonucu olarak ortaya çıkan suçlardır. Bilgisayar korsanlığı ve virüs gibi yazılım temelli suçlar bu sınıflandırmada yer almaktadır. Kötüye kullanım başlangıçta klasik suçların bilişim teknolojilerinden faydalanılması şeklinde görünür olurken ilerleyen zamanlarda yeni suç türleri de ortaya çıkmaya başlamıştır (Furnell, 2001, s. 35-37).

Türk Ceza Kanunu'na (TCK, 2004) baktığımızda ise bu kapsamdaki suçların iki farklı kategoride ele alındığı görülmektedir. Bunlardan ilki, bilişim sistemine ve verilerine, yasak programların kullanımı ve dağıtımına, banka ve kredi kartlarının veya bilgilerinin ele geçirilerek kötü amaçlı kullanımına odaklanan suçlar, *bilişim alanında suçlar* kapsamında yer almaktadır. İkincisi ise klasik suçların bilişim sistemlerinin araç olarak kullanılması suretiyle gerçekleştirildiği durumlar olarak karşımıza çıkmaktadır. Bu tür suçlar genel olarak *mal varlığına karşı işlenen suçlar* kapsamında yer alan dolandırıcılık, hırsızlık ve kumar suçlarının nitelikli halleri kapsamında değerlendirilmektedir. Yargıtay Başkanlığı tarafından yayımlanan Ceza Genel Kurulu 2009/11-193 E., 2009/268 K. nolu emsal

kararına göre bilişim sistemlerinin kullanımı suretiyle işlenen suçlar TCK'da da kabul edildiği üzere öğreti ve uygulamada "doğrudan bilişim suçu (gerçek bilişim suçları)" ve "dolayısıyla bilişim suçu (bilişim bağlantılı suçlar)" olarak iki ayrı başlık altında ele alınmaktadır. Bu karara göre bilişim suçu "klasik suçların bilişim sistemlerinden yararlanılarak işlenmesini" ifade etmekte olup o suçların nitelikli halleri içerisinde yer almaktadır (Yargıtay Başkanlığı, 2009).

3.Metodoloji

Araştırmanın amacı bilgi teknolojilerinin suç eylemleri üzerindeki etkisini ve rolünü belirlemek ve analiz etmektir. Bu kapsamda araştırma alanı olarak belirlenen dolandırıcılık eyleminin belli bir zaman aralığındaki görünürlüğü dikkate alınmış ve internet haberlerine yansıyan olaylarla çalışmanın kapsamı sınırlandırılmıştır. Araştırmanın kapsamı ve sorgu alanı içerisinde en çok ziyaret edilen ve konuyla ilgili en fazla sayıda haber sunan internet siteleri belirlenmeye çalışılmış ve iki araştırma şirketinin istatistiki verilerinden yararlanılmıştır. Bu bağlamda ülkemizde Similarweb'in haber ve medya alt kategorisinde en çok ziyaret edilen ve Alexa'nın üç aylık veriler halinde sunduğu en çok internet trafiğine sahip olan haber siteleri temel alınmıştır. Buna göre en çok ziyaret edilen ve konuyla ilgili en fazla sayıda haber içerdiği tespit edilen "hurriyet.com.tr" araştırmanın örneklem alanı olarak belirlenmiştir. 2008 ve 2019 yılları arasındaki zaman dilimi referans alınarak bu süreç içerisinde eğilimin yönü irdelenmiştir. Beraberinde dolandırıcılık eyleminde kullanılan araçların tarihsel süreçte gösterdiği değişim de ortaya çıkarılmak istenmiştir.

Haber metinlerinin değerlendirilmesinde içerik analizi tekniğinden yararlanılmıştır. Zira içerik analizi, araştırmanın amacı ve soruları kapsamında kategoriler oluşturma, verileri bu kategoriler çerçevesinde değerlendirme, bunların istatiksel dökümünü gerçekleştirme ve literatür ile ilişkilendirme süreçlerini içeren bir tekniktir (Berg ve Lune, 2015, s. 389-407). Bu temelden hareketle "hurriyet.com.tr" sitesinin arama çubuğu kullanılmış ve içinde "dolandırıcılık" kelimesi geçen 2008 ve 2019 yılındaki tüm haber metinlerinin içerikleri incelenmiştir. Açık bir şekilde dolandırıcılık suçunun hangi araçlar ile gerçekleştirildiği ve dolandırılacak hedef bireylere hangi araçlar kullanılarak ulaşıldığını aktaran haberler analiz birimine dahil edilmiştir. Bu şartları sağlayan 2008 yılında 223 ve 2019 yılında 241, toplamda ise 464 habere ulaşılmıştır.

Haberler analiz edilirken Yılmaz'ın (2015) 2010 ve 2014 yılları arasında jandarma sorumluluk sahasında meydana gelen yaklaşık 10 bin dolandırıcılık olayının gerçekleşme şekillerini inceleyerek tasnif ettiği dolandırıcılık tipolojileri/türleri/yöntemlerinden yararlanılmıştır. Çalışma

kapsamında üst ve alt kategorilerden oluşan bu dolandırıcılık yöntemlerinin sadece üst kategorilerinden (*kapıdan satış, ön ödeme, sosyal mühendislik/senaryo, sigorta, Sosyal Güvenlik Kurumu'nun dolandırılması (SGK), para toplama, büyü ve muska vb., evlendirme veya evlenme, kendine ait olmayan yeri/malı satma/kiralama, sözde fırsat yatırımı, satış işleminde dolandırıcılık, çek ve senet – değerli kâğıt (bilet vb.), kimlik ve kredi kartı dolandırıcılığı, kamudan haksız menfaat ve diğer yöntemler*) faydalanılmıştır. Dolandırıcılık olayları analiz edilirken ilk olarak her bir olay, mağdurların evlilik ve yatırım gibi aldatılma vaatlerini ortaya çıkaran dolandırıcılık yöntemine göre sınıflandırılmıştır. Yöntemine göre tasnif edilen her bir olay, ardından dolandırıcılık suçunu işleme araçları ve dolandırılacak kişilere ulaşma araçlarına göre tasnif edilmiştir. Bu analiz işlemi, araştırmanın amaçları doğrultusunda belirlenmiş ve analiz aşamasında ortaya çıkan yüz yüze, zorbalık ve şiddet, sahte evrak, telefon, internet sitesi, sosyal medya, bankamatik/pos cihazı ve diğer iletişim araçları (gazete, radyo ve televizyon) olarak belirlenen kategorilere göre gerçekleştirilmiştir. Böylece dolandırıcılık yöntemleri kapsamında kullanılan araçların yıllar bazındaki dağılımı ortaya çıkartılarak, bilgi teknolojilerinin suç eylemleri üzerindeki payı ve etkisi değerlendirilmiştir. Haberlerde dolandırıcılık yöntemini ve araçlarını betimleyen anahtar kelimelerden yararlanılarak MAXQDA programı aracılığıyla kelime bulutu oluşturulmuştur. Böylelikle dolandırıcılık olayları ve kullanılan araçların yanı sıra haberlerin tasnif edilme ve sınıflandırılma biçiminin bir görseli sunulmuştur.

4. Bulgular

Haber analiz sonucunda 2008 ve 2019 yılındaki dolandırıcılık olaylarında saptanan farklılıklar dijitalleşen dünyanın suç eylemine yansımaları olarak ortaya çıkmıştır. Şekil 1 ve 2'de 2008 ve 2019 yılındaki olayları betimleyen ifadelerden yararlanılarak oluşturulan kelime bulutu ile olayların işleniş biçimleri görselleştirilmiştir. 2008 yılında mağdurların güvenleri kazanılarak dolandırma eyleminin hakim olduğu, sahte doküman ve evrakların düzenlendiği, suçlu ve mağdurun doğrudan ve aracısız temasının yoğun olduğu, bankamatik ve pos cihazına yerleştirilen çeşitli aparatların kullanılarak gerçekleştirilen dolandırıcılık olayları 2008 yılındaki haberleri büyük oranda karakterize etmektedir. Aynı zamanda şiddet ve tehdide dayalı eylemlerin de yaşanabildiği görülmektedir. Arama, mesaj gönderme ve internet siteleri de kullanılan teknolojik araçlar olarak dolandırıcılık olaylarında gündeme gelmeye başlamıştır.

Şekil 1: 2008 Yılı Dolandırıcılık Olaylarına İlişkin Kelime Bulutu

Analiz edilen haberler sonucunda 2008 yılında gerçekleştirilen dolandırıcılık olaylarında telefon, bankamatik/pos cihazı, yüz yüze, zorbalık ve şiddet, internet siteleri (alışveriş, evlilik siteleri, banka web sayfaları vd.), sahte evrak ve diğer iletişim araçlarının (radyo, gazete ve televizyon) kullanıldığı görülmektedir.

Elde edilen verilere göre 2008 yılındaki dolandırıcılık eylemleri geniş bir yelpazede ortaya çıkmış; kapıdan satış, ön ödeme, senaryo oluşturma, kamu imkanlarına haksız ulaşma, para toplama, büyü, evlendirme, başkasına ait mülkü satma, değerli kağıtlar ve kredi kartı dolandırıcılığı gibi çeşitli yöntemlerle gerçekleştirilmiştir. Bu eylemler içerisinde 2008 yılında dijital araçları kullanma oranı daha düşük düzeydedir.

2019 yılında ise dijital araçlar yoğun bir şekilde kullanılmaya başlanmıştır. 2008 yılında güven kazanmak amacıyla gerçekleştirilen yüz yüze eylemler ve kullanılan sahte evraklar 2019 yılında yoğunluğu internetin sunduğu olanaklara, teknolojik araçlara ve gelişmelere bırakmıştır. Belirli ve kısıtlı sayıda kişiyi kapsayan olaylar aşılarak kitleleri hedef olarak belirleyen dolandırıcılık eylemleri görünürlük kazanmıştır.

Şekil 2: 2019 Yılı Dolandırıcılık Olaylarına İlişkin Kelime Bulutu

2019 yılında gerçekleşen dolandırıcılık olaylarının telefon, sosyal medya, internet siteleri (alışveriş, evlilik siteleri, banka web sayfaları vd.), yüz yüze, bankamatik/pos cihazı, sahte evrak, zorbalık/şiddet yoluyla ve diğer iletişim araçları (radyo, gazete ve televizyon) kullanılarak gerçekleştirildiği görülmektedir. Haber analizleri sonucunda saptanan dolandırıcılık araçları, mağdur ile dolandırıcının etkileşim kanallarını ve biçimini göstermektedir.

Farklı zaman dilimleri temel alınarak dolandırıcılık suçu özelinde yeni yönelimlere ve eğilimlere ışık tutulmaya çalışılmıştır. Buna göre telefon aracılığıyla gerçekleştirilen olaylar, dolandırıcının mesajlaşma veya konuşma yoluyla mağdurun doğrudan hedef olarak seçildiği durumları içermektedir. Bu araçla çeşitli kurgular oluşturularak toplumsal korkulardan yararlanılmakta ve özellikle kişilerin çocukları ve eşleri gibi birinci dereceden yakınlarının başlarının dertte olduğu yönünde bir algı oluşturulmaktadır. Yoğunluklu olarak kullanılan yönteme bakıldığında polis, asker gibi asayiş sağlayan meslek grupları olduklarına dair profesyonelce bir izlenim yaratılarak kişiler kandırılmakta ve telefonda verilen talimatlara uymaları sağlanmaktadır. Aynı zamanda gönderilen mesajların da dolandırıcılık olaylarında önemli bir paya sahip olduğu görülmektedir. Mağdurlara hediye, bedava tatil veya indirim kazandıklarını belirten çeşitli mesajlar iletilerek kişilerin yönlendirmeleri takip etmeleri sağlanmaktadır.

Sosyal medyada oluşturulan kurum ve alışveriş sitelerine ilişkin sahte reklamlar ve sayfalar aracılığıyla kişilerin bilgilerine erişim sağlanabilmektedir. Aynı zamanda bu mecralar yoluyla gerçekleşen tanışmalar sonucunda yaşanan dolandırıcılık olayları da ön plana çıkmaktadır. Alışveriş, evlilik, emlak siteleri, sanal mağazalar, e-posta göndererek gerçekleştirilen sahte yönlendirmeler gibi durumlar ise internet siteleri aracılığıyla gerçekleştirilen olaylar kapsamında ele alınmıştır. İnternet sitelerinin kullanımı ise doğrudan bir kişi hedeflenmeden otel, banka ve alışveriş gibi sitelerin kopyalanarak belirli bir ihtiyacını karşılamak için harekete geçen kitlelerin bilgilerini ele geçirmeye yönelik durumları kapsamaktadır. Aynı zamanda kişilere e-posta yoluyla ulaşılarak sahte internet sitelerine yönlendirilmeleri de bu kapsamda ele alınmıştır.

Yüz yüze gerçekleştirilen olaylar ise dolandırıcının doğrudan mağdurla temasa geçerek sözlü beyan ile onu kandırması şeklindedir. Kişileri belirli davranışları sergilemeleri yönünde aldatıcı şekilde yönlendirmeleri, güven sağlamaları ve onları inandırmalarını içeren yüz yüze gerçekleşen durumları kapsamaktadır. Ellerindeki dövizin veya maddenin değerli olduğuna inandırma, ihtiyaç sahibi grupların adları öne sürülerek yardım toplama veya aynı malı birden fazla kişiye satma gibi çeşitli yöntemleri içerebilmektedir. Yüz yüze eylemler, doğrudan dolandırıcının kimliğini teşhis etmeyi ve kişiye ulaşabilmeyi ve doğrudan kişiden şikayette bulunabilmeyi kolaylıkla sağlayabilmesi sebebiyle diğerlerinden ayrılmaktadır.

Bankamatiklere kart bilgilerinin kopyalanmasını sağlayan aletler yerleştirilmesi veya pos cihazları aracılığıyla kart bilgilerine erişim sağlandığı dolandırıcılık olayları da söz konusudur. Bunlar kısmen teması ve doğrudan etkileşimi gerektiren durumları kapsamaktadır. Bu manada gerçekleştirilen olaylarda bankamatiklere yerleştirilen kameralar aracılığıyla veya pos cihazı kullanılarak alışverişin gerçekleştirildiği mağaza, restoran gibi mekanlar incelenerek süreç takip altına alınabilmektedir.

Sahte evraklar dolandırıcılık yöntemlerinde kullanılan bir diğer araçtır. Sahte bilet, doküman ve belge imal etme ve sahte kimlik çıkarma yoluyla kişilerin ve kamu kurumlarının dolandırılması gibi çeşitli durumları kapsamaktadır. Diğer iletişim araçları ise radyo, televizyon ve gazeteyi içermektedir. Radyo ve televizyon kanalları üzerinden verilen reklamlarla kişilere sahte ürün satma veya gazete ilanlarıyla iş verme veya evlenme gibi vaatlerle iletişimin sağlandığı çeşitli haberleri kapsamaktadır. Zorbalık ve şiddet yoluyla gerçekleştirilen olaylar kişileri doğrudan tehdit ederek veya baskı uygulayarak zorla malını sattırma ve çeşitli evrakları imzalatma gibi durumları içermektedir.

Yıllar içerisinde yararlanılan araçların değişkenlik gösterdiği ve dolandırıcılık türüne göre kullanılan araçların da farklılaştığı saptanmıştır. *Ön ödeme, para toplama* ve *sözde fırsat yatırımı* yönteminin kullanıldığı dolandırıcılık suçları 2008 yılında yoğun bir şekilde yüz yüze (sırasıyla %80, %66,66, %100) gerçekleştirilmekle birlikte 2019 yılında da yüz yüze (%28,57, %42,85, %37,5) gerçekleştirilen olaylarla karşılaşılmıştır. Farklı olarak bu yöntemler kapsamında işlenen suçlarda 2019 yılında telefon (%7,14, %42,85, %25), sosyal medya (%17,85, -, %12,5) ve internet sitelerinin (%32,14, %14,28, %12,5) kullanımı oldukça artmıştır.

Sosyal mühendislik/senaryo yöntemi kapsamındaki suçlar 2008 yılında çoğunlukla yüz yüze (%67,34) işlenirken 2019 yılında bu suç türünde telefon (%66,26) en çok fayda sağlanan araç olmuştur. *Büyü ve muska vb.* yöntemlerle gerçekleştirilen dolandırıcılık suçları 2008 (%100) ve 2019 (%50) yılında genel olarak yüz yüze gerçekleştirilmiştir. Aynı zamanda 2019 yılında bu kapsamdaki olaylarda sosyal medya (%33,33) ve diğer iletişim araçlarının (%16,66) kullanılmaya başlanıldığı görülmektedir. *Evlenme veya evlendirme vaadi*yle gerçekleştirilen olayların çoğu 2008 (%66,66) ve 2019 (%37,5) yılında yüz yüze gerçekleşirken, 2019 yılında sosyal medya (%50) kanalıyla tanışma sonucunda gerçekleşen olaylar belirginlik kazanmıştır. *Sosyal Güvenlik Kurumu'nun dolandırılması* (2008 yılında %75; 2019 yılında %100) ve *kamudan haksız menfaat* (2008 yılında %100; 2019 yılında %100) kapsamına giren dolandırıcılık suçlarında her iki dönemde de sahte evraklardan yararlanılmıştır.

Çek ve senet- değerli kâğıt yöntemiyle gerçekleştirilen eylemlerde 2008 yılında sahte evraklar (%100) kullanılırken 2019 yılında da sahte evraklardan (%37,5) faydalanılmaya devam edilmiştir. 2019 yılında dolandırıcının mağdurla yüz yüze (%50) gerçekleşen olayların yanı sıra internet siteleri (%12,5) de bir araç olarak yer almaya başlamıştır. *Kendine ait olmayan yeri satma/kiralama* kapsamındaki suçlarda farklı dağılımlar söz konusu olmakla birlikte her iki dönemde de sahte evrak (2008 yılında %40; 2019 yılında %25) ve internet siteleri (2008 yılında %40; 2019 yılında %50) ön plandadır. *Satış işleminde dolandırıcılık* olaylarında 2008 yılında yoğunlukla sahte evraklar (%58,82) yer alırken 2019 yılında sahte evrakın (%4,54) yanı sıra internet siteleri (%38,63), yüz yüze (%22,72), sosyal medya (%15,9) ve telefon (%11,36) aracılığıyla gerçekleştirilen olaylar kendisini göstermektedir

Kimlik ve kredi kartı dolandırıcılığı suçlarında 2008 yılında sahte evraklar (%42,85) araç olarak kullanılmakla birlikte 2019 yılında sahte evrakın (%20) yanı sıra sosyal medya (%32), internet siteleri (%32) ve bankamatik/pos cihazı (%16) yaygınlık kazanmıştır. Yılmaz'ın *diğer*

yöntemler (*tırnakçılık/el çabukluğu, kasada oyalama/kafa karışıklığı yaratma, değersiz döviz, bankamatik, borsa dolandırıcılığı (pump and dump), malın yönlendirilmesi, nakliye için verilen malı satma/kullanma, çalıştığı kurumu/iş yerini dolandırma*) olarak tasnif ettiği dolandırıcılık türlerinde ise 2008 yılında yoğunlukla yüz yüze (%20) ve sahte evraklardan (%62,5) faydalanılmakta iken 2019 yılında yüz yüze (%81,81) gerçekleştirilen olaylar belirginlik kazanmakta ve sosyal medya (%9,09) ve internet sitelerinden (%9,09) yararlanıldığı görülmektedir.

Dolandırıcılık yöntemi kapsamında incelenen olayların yanı sıra bilgi ve iletişim teknolojilerinin suç eylemleri içindeki payını ortaya çıkarabilmek adına yalnızca kullanılan araçların kendi içindeki sıralaması ve dağılımı Tablo 1 ve 2'de gösterilmiştir.

Tablo 1: 2008 Yılı Dolandırıcılık Araçlarının Dağılımı

Dolandırıcılık Aracı	**Haber Sayısı (223)**	**Yüzde (%)**
Yüz yüze	100	% 49,09
Sahte evrak	62	% 32,43
İnternet siteleri	23	% 10,36
Telefon	16	% 7,2
Bankamatik/pos cihazı	11	% 4,95
Zorbalık ve şiddet	9	% 4,05
Diğer iletişim araçları	2	% ,90

Tablo 2: 2019 Yılı Dolandırıcılık Araçlarının Dağılımı

Dolandırıcılık Aracı	**Haber Sayısı (241)**	**Yüzde (%)**
Telefon	67	% 27,8
Yüz yüze	64	% 26,55
İnternet siteleri	46	% 19,08
Sosyal medya	32	% 13,27
Sahte evrak	19	% 7,88
Bankamatik/pos cihazı	5	% 2,07
Diğer iletişim araçları	5	% 2,07

Zorbalık ve şiddet	2	% ,82

Elde edilen bulgularda ön plana çıkan durumlardan birisi 2008 yılında sosyal medya bir araç olarak karşımıza çıkmazken 2019 yılında kullanılan araçlar içerisinde sosyal medyanın 4. sırada (%13,27) yer almasıdır. Bu durum, on yıllık bir süreç içerisinde kullanımının artmasıyla birlikte sosyal medyanın oldukça hızlı bir şekilde suç eyleminin merkezinde yer almaya başladığını göstermektedir. Aynı zamanda zorbalık ve şiddet yoluyla gerçekleştirilen dolandırıcılık haberleri 2008 yılına (%4,05) kıyaslandığında 2019 (% ,82) yılında azalmıştır.

İncelenen haberler sonucunda 2008 yılında gerçekleştirilen dolandırıcılık suçlarının yaklaşık yarısı yüz yüze (%49,09) işlenmekteyken 2019 yılında yüz yüze (%27,8) gerçekleştirilen eylemlerin oranının oldukça düştüğü görülmektedir. Dolandırıcılık eylemlerinde 2008 yılında önemli oranda yüz yüze (%49,09) ve sahte evrak (%32,43) kullanılırken 2019 yılında telefon (%27,8), internet siteleri (%19,08) ve sosyal medya (%13,27) gibi iletişim araçlarından faydalanılmaya başlanmıştır. Önceden doğrudan mağdur ve suçlunun temasıyla gerçekleşen suçlar artık araya giren teknolojiyle birlikte suçluyu görünmez ve yakalanması zor kılmıştır. Sağladığı fırsatlar ve olanaklardan yararlanılan teknoloji, suç eyleminde araçsallaştırılmış ve suç eyleminin daha kolay gerçekleştirilebilmesine olanak sağladığı için dijitalleşen bir görünüm kazanmaya başlamıştır. 2019 yılında bilişim araçlarının suç eylemindeki kullanım oranlarının artması, TÜİK (2020) verilerine göre 2004-2020 yılları arasında hanelerde ve girişimlerde bilişim teknolojileri kullanım oranlarının giderek yaygınlık kazanması durumuyla da paralellik göstermektedir.

5.Değerlendirme ve Sonuç

Araştırmanın sonuçları bağlamında dijitalleşmenin suç eylemlerinin dönüşümüne de fırsat verdiği ve yeni yöntemlerle kendisini araçsallaştırarak varlığını devam ettirdiği görülmektedir. Diğer bir ifadeyle suç, dijitalleşen çağa uyum sağlamış ve teknik bir bilgi birikimi ve beceri meselesi haline gelmiştir. 2008 ve 2019 yılları arasında incelen haberlerden hareketle kişilerin dolandırılma biçimlerinin, senaryoların ve sunulan vaatlerin neredeyse hiç değişmediği ancak kullanılan araçların değiştiği ve dijital çağın ögelerinden yararlanmaya yönelik bir eğilim olduğu görülmüştür. Bilişim teknolojilerini kullanıyor olmak başlı başına mağdur olma riskini taşımakta ve önlem almak dahi yeterli olmayabilmektedir. Zira teknolojik gelişmeler, dijital suçların daha kolay bir şekilde işlenebilir olmasını ve insanlara daha hızlı şekilde ulaşılabilmesini sağlamaktadır. Bu durumun suç

oranlarını etkilemesi ve teknolojik gelişmelerle birlikte yeni suç türlerinin ortaya çıkmasına olanak sağlayabilme durumu değerlendirilmelidir.

Doğrudan etkileşim zorunluluğunu ortadan kaldıran sosyal medya, internet siteleri ve telefon, kimliğin gizlenebilmesini ve çeşitli senaryolar yaratılarak kandırma eylemini daha kolay bir şekilde gerçekleştirme imkanı sağlamıştır. Alışveriş ve para transferi gibi pek çok işlemin online bir şekilde yönetilebilme seçeneği, kimlik ve iletişim bilgilerini teknolojik araçlarla paylaşma gerekliliğini beraberinde getirmiştir. Dijital platforma taşınan bilgiler, böylece o bilgilerin hileli yöntemlerle elde edilmesi için de fırsatlar sunmaktadır. Özellikle otel, banka ve alışveriş hizmeti sunan platformların kopyalanarak oluşturulan sahte sitelere kullanıcıların yönlendirilmesi sonucunda kimlik bilgilerine ulaşılması ve paraların zimmete geçirilmesi ya da alışveriş yapılması sıklıkla rastlanan dolandırıcılık olayları arasındadır.

İncelenen haberlerde dolandırıcıların eylemlerini gerçekleştirirken toplumsal kargaşa, ihtiyaç (terör, işsizlik vb.), korku ve risklerden beslendiği ve yöntemlerinde bunları kullandıkları görülmüştür. Vizyona girecek filmler, kripto para ve konser gibi gündemdeki olayları ve popüler konuları yakından takip ederek kitlelerin ilgisinin kötüye kullanıldığı çeşitli dolandırıcılık olayları da gündeme gelmektedir. Bunun yanı sıra incelenen haberlerde polislerin ve mağdurların, dolandırıcılara ulaşmak için bilişim teknolojilerinin sağladığı anonimlikten faydalandıkları bilinmektedir. Öte taraftan 2008 yılında yoğun bir şekilde yüz yüze ve sahte evraklar ile gerçekleştirilen dolandırıcılık olayları, 2019 yılında yerini telefon, internet siteleri ve sosyal medya gibi bilişim ve iletişim teknolojilerine bırakmıştır. Bu manada dolandırıcılık yöntemine özgü olarak kullanılan geleneksel araçlar farklılaşarak teknolojik imkanlarla aynı amaca ulaşma ön plana çıkmıştır. Başka bir ifade ile suçun işlendiği fiziksel ortam değişerek, suç mahali belirsizleşmiş ve teknik bir bilgi meselesi haline gelerek dijital bir görünüm kazanmıştır.

Sonsöz olarak, teknolojik imkanların yeni suçların kapsamı ve uygulanma biçimleri için çeşitli olanaklar taşıyan bir zemin oluşturduğu görülmektedir. Dahası teknolojinin beraberinde getirdiği fırsatlar ve olanaklar görünürlüğü artan dijital/siber suçların anlaşılmasında oldukça önemli bir yer işgal etmektedir. Teknolojik araçların sağladığı çeşitlilik irdelenmesi ve dijitalleşen suçların anlaşılabilir olmasında ve önlenebilmesi noktasında suç fırsatları yaklaşımı önemli bir bakış açısı sağlamaktadır. Gelişmeler sayesinde birebir etkileşimi gerektirmeden daha fazla sayıda bireyle daha hızlı ve kolay bir şekilde iletişime geçilebilmektedir. Çeşitli kurgular üretilerek aldatmanın yanı sıra sadece bilişim teknolojileri aracılığıyla mağdurların çok daha sonra farkına varabilecekleri şekilde

kolaylıkla kimlik bilgileri ele geçirilebilmektedir. Teknolojik ögelerin sunduğu koşullar, suç eyleminde bir fırsat olarak kullanılabilmekte ve varlığını korumaktadır.

Kaynakça

Alexa (2019). *Top Sites in Turkey.* 8 Mart 2019, https://www.alexa.com/topsites/countries/TR.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T. & Savage, S. (2013). Measuring the Cost of Cybercrime. R. Böhme, (Ed.). *The Economics of Information Security and Privacy* içinde (265-300). Berlin, Heidelberg: Springer.

Barnes, H. E. & Teeters, N. K. (2011). İlkel Cezalar ve Fiziksel Cezanın Başlıca Türleri. (D. Aydın, Çev.). *Ankara Barosu Dergisi*, (4), 163-176.

Beck, U. (2019). Risk Toplumu: Başka Bir Modernliğe Doğru. (K. Özdoğan ve B. Doğan, Çev.). İstanbul: İthaki Yayınları

Berg, B. L. & Lune, H. (2015). *Sosyal Bilimlerde Nitel araştırma Yöntemleri*. (H. Aydın, Çev. Ed.). Konya: Eğitim Yayınevi.

Black's Law Dictionary (2004). (Eighth Edition). B. A. Garner, (Ed. In Chief). St. Paul MN: Thomson/West.

Clarke, R. V. (1983). Situational Crime Prevention: Its Theoretical Basis and Practical Scope. *Crime and Justice*, *4*, 225-256.

Cohen, L.E. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44* (4), 588-608.

Council of Europe (2005) *Organised Crime Situation Report 2005: Focus on the Threat of Economic Crime*. Octopus Programme, Strasbourg. https://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Report2005E.pdf.

European Commission (2007). *Communication From the Commission to the European Parliament, the Council and the Committee of the Regions, Towards a General Policy on the Fight Against Cyber Crime.* COM (2007) 267 final. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

Felson, M. & Clarke, R. V. (1998) *Opportunity Makes the Thief: Practical Theory for Crime Prevention*. Home Office Policing and Reducing Crime Unit, Police Research Series Paper 98.

Foucault, M. (1992). *Hapishanelerin Doğuşu.* (M. A. Kılıçbay, Çev.), Ankara: İmge Kitabevi.

Furnell, S. M. (2001). Categorising Cybercrime and Cybercriminals: The Problem and potential Approaches. *Journal of Information Warfare*, *1*, (2), 35-44.

Ghernaouti, S. (2013). *Cyber Power: Crime, Conflict and Security in Cyberspace.* Switzerland: EPFL Press.

Giddens, A. (2012). *Sosyoloji*. (C. Güzel, Yay. Haz.). İstanbul: Kırmızı Yayınları.

Grabosky, P. & Smith, R. (2001). Telecommunication Fraud in the Digital Age: The Convergence of Technologies. D. S. Wall, (Ed.), *Crime and the Internet: Cybercrimes and Cyberfears* içinde (29-43). London: Routledge.

Koçak, H. ve Dandin, A. N. (2017). Toplumsal ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, *19* (1), 137-152.

Kovacich, G. L. (2008). *Fighting Fraud: How to Establish and Manage an Anti-Fraud Program.* USA: Butterworth-Heinemann.

Lilly, J. R., Cullen, F. T. & Ball, R. A. (2019). *Criminological Theory: Context and Consequences* (Seventh Edition). Thousand Oaks, California: SAGE

Sembok, T. M. T. (2004). *Ethics of Information Communication Technology (ICT)*. P. Bergstrom, (Ed.), *Ethics in Asia-Pacific* içinde (239-326). Regional Unit for Social and Human Sciences in Asia and the Pacific. Thailand, Bangkok: UNESCO Asia and Pacific Regional Bureau for Education.

Similarweb (2019). *Top Websites Ranking.* 8 Mart 2019, https://www.similarweb.com/top-websites/turkey.

TÜİK (2020). *Bilgi Toplumu İstatistikleri, 2004-2020*. 18 Ekim 2020, https://data.tuik.gov.tr/tr/main-category-sub-categories-sub-components2/.

Türk Ceza Kanunu (TCK) (2004). *T.C. Resmi Gazete 25611,* 12/10/2004.

Yargıtay Başkanlığı. Ceza Genel Kurulu 2009/11-193 E., 2009/268 K. Nolu Emsal Kararı. 6 Mayıs 2019, https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/.

Yılmaz, A. (2015). Türkiye'deki Dolandırıcılık Tipolojileri: Dolandırıcılık Olaylarının Kategorik Tasnifi ve Yapılış Şekilleri. *Hacettepe Üniversitesi Sosyolojik Araştırmalar E-dergisi*, 1-26.