Türkiye İletişim Araştırmaları Dergisi • Yıl/Year: 2020 • Sayı/Issue: 35 ss/pp. 139-163 • ISSN: 2630-6220
DOI: 10.17829/turcom.726309

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

İkna Yoluyla Dolandırıcılık: Dolandırıcılık Faaliyetlerinde İkna ve Etkili İletişim Yöntemlerinin Tespiti Üzerine Bir Araştırma

Fraud by Persuasion: A Research on Determination of Persuasion and Effective Communication Methods in Fraud Activities

Atalay BAHAR*

Öz

İkna, bireylerin sosyal çevreleri ve toplumsal dinamikleri dikkate alınarak, fikirlerin içselleştirilmesi ve tavırların özümsenmesine yönelik çabaların bütünüdür. İletişimin kişilerarası boyutu, araştırmanın temelini oluşturmakla beraber, bu araştırmada paradoksal bir perspektifle ikna stratejilerinin olumsuz süreçlerde de kullanılabileceğine dikkat çekilmektedir. Çalışmada; iknanın, toplumsal reflekslere ve bireysel kayıplara neden olan, *ikna yoluyla dolandırıcılık* suçunun gerçekleştirilmesindeki başat rolü ele alınmaktadır. İkna yoluyla dolandırıcılık, sahte çağrı merkezleri vasıtasıyla iletişime geçilen mağdurların kurgulanmış senaryolarla ikna edilerek, haksız kazanç sağlanmasıyla meydana gelmektedir. Nicel araştırma yöntemi ile gerçekleştirilen bu çalışmada içerik analizi tekniği kullanılmıştır. İkna yoluyla dolandırıcılıkta kullanılan yöntemler vaat, korkutma ve yardım kampanyaları şeklinde tasnif edilmiş ve bu üç yönteme ilişkin değişkenler belirlenmektedir. İstanbul'da 01.01.2019 ve 01.12.2019 tarihleri arasında gerçekleştirilen ikna yoluyla dolandırıcılık suçları tekniğine ilişkin demografik değişkenler kapsamında, elde edilen veriler ışığında bir durum tespiti ortaya konulmaktadır. Bu suçta öne çıkan sahte çağrı merkezlerinin sistematiği ile mağdurların cinsiyet, yaş ve öğrenim durumları incelenmektedir. Bu çalışmanın amacı, bu türden eylemler hakkında farkındalık oluşturmaktır. İkna yoluyla dolandırıcılık yöntemlerinin teknik özellikleri ile örgüt üyelerinin ileri düzeydeki iletişim yetkinlikleri, aynı düzlemde ele alınmaktadır. Örgüt üyelerinin ikna yoluyla dolandırıcılık suçunun işlenmesini kolaylaştıran iletişimsel becerileri ile mağduriyet oluşturan iletişim dinamikleri ve teknikleri arasında bir ilişkisellik görülmektedir. Öğrenim seviyesi yükseldikçe mağduriyet azalmakla birlikte, her öğrenim seviyesinden ikna yoluyla dolandırıcılık suçuna maruz kalındığı ve 35 yaş üzeri bireylerde, ikna yoluyla dolandırıcılık mağduriyetinin %70'i aştığı elde edilen önemli sonuçlardandır.

* Dr., İstanbul Emniyet Müdürlüğü, İstanbul, Türkiye, atk199@hotmail.com

Başvuru Tarihi/Received Date: 13.01.2020
Kabul Tarihi/Accepted Date: 23.03.2020

Anahtar Kelimeler: İkna Yoluyla Dolandırıcılık, İkna İletişimi, Etkili İletişim Yöntemleri, Sahte Çağrı Merkezi, VoIP Teknoloji

Abstract

Persuasion is the totality of efforts to internalize ideas and assimilate attitudes, taking into account the social environment and social dynamics of individuals. Although the interpersonal dimension of communication is the basis of this research, it is pointed out that persuasion strategies can also be used in negative processes with a paradoxical perspective. In the study, the dominant role of persuasion in the realization of "fraud by persuasion" crime, which causes social reflexes and individual losses, is discussed. Fraud through persuasion occurs when victims contacted through fake call centers are persuaded by fictionalized scenarios, resulting in unfair profits. In this study, which is carried out with quantitative research method, content analysis technique is used. The methods used in fraud through persuasion are classified into promises, scares and aid campaigns and variables for these three methods are determined. In the light of the data obtained, a due diligence is put forward within the scope of the demographic variables related to the technique of fraud crimes carried out between 01.01.2019 and 01.12.2019 in Istanbul. The systematic of the fake call centers that stand out in this crime and the gender, age and educational status of the victims are examined. The purpose of this study is to raise awareness about such actions. The technical characteristics of fraud methods through persuasion and the advanced communication competencies of the members of the organization are considered on the same plane. There is a relationship between the organizational members communicative skills that facilitate the processing of fraud by persuasion and the communication dynamics and techniques that create victimization. Although the victimization decreases as the level of education increases, it is one of the important results obtained that the fraud victimization exceeds 70% by persuasion in individuals over 35 years of age by persuasion.

Keywords: Fraud by Persuasion, Persuasion Communication, Effective Communication Methods, Fake Call Center, VoIP Technology

Giriş

İkna, belirlenen bir hedef doğrultusunda fikirlerin, tutumların ve davranışların benimsetilmesi, kısmen ya da tamamen değiştirilmesi amacıyla uygulanan sistemli bir iletişim sürecini içermektedir. Etkileme ve inandırıcılık ikna kavramının ilk basamağını, onaylama ve eyleme dönüştürme ise son basamağını temsil etmektedir. İki basamak arasında kalan boyut da, iknacının kabiliyetleri ve yönetim yeteneği bağlamında gerçekleştirdiği yönlendirme stratejilerinden oluşmaktadır (İplikçi, 2015, s. 68). Alıcı değişkenliğine göre iletişimsel parametreler doğrultusunda, özel çıktılar ve etkiler üretme faaliyetlerine başvurulmaktadır. Bu bağlamda çözümlenmiş mesajlarla inandırma ve manipülasyon odaklı, spesifik çıktıları hedefleyen bu metodoloji, *ikna iletişimi* olarak yorumlanmıştır.

İkna; bir iletişim etkinliğidir. İletişim herkesin bildiği ancak çok az kişinin doyurucu biçimde tanımlayabildiği bir insan etkinliğidir (Akpınar ve Akpınar, 2017, s. 103). İkna edici iletişim, iletişim becerilerinin etkili ve yerinde kullanımını ifade etmekte ve iletişimin kişilerarası boyutuna daha fazla vurgu yapmaktadır. İkna, bireylerin sosyal çevreleri ve toplumsal dinamikleri dikkate alınarak, fikirlerin içselleştirilmesi ve tavırların özümsenmesine yönelik çabaların bütünüdür

(Uztuğ, 2012, s. 14). Bu çabalar çoğunlukla gözetilen amaca ve beklentilere uygun, olumlu sonuçları hedefleyen bir iletişim sosyolojisini işaret etmektedir. Ancak çalışmada paradoksal bir perspektifle ikna stratejilerinin olumsuz süreçlerde kullanılabileceğine dikkat çekilerek, iknanın toplumsal reflekslere ve bireysel kayıplara neden olan *ikna yoluyla dolandırıcılık* suçunun gerçekleştirilmesindeki başat rolü ele alınmaktadır.

İletişim sürecinin başarılı bir şekilde sonuçlanması, kaynağın hedefe uygun bir mesaj üretmesi ve bunu elverişli bir kanal ile ulaştırmasına bağlıdır. Kaynak, hedefin duygu, düşünce ve/veya davranışlarını şekillendirmek zorundadır. Bu zorunluluk, iletişimin başarılı bir şekilde gerçekleştirilmesi zorunluluğu ile birleştiğinde, kaynağın işlevi öne çıkmaktadır. Bununla beraber kaynağın taşıması gereken özelliklerin niceliksel olarak sayısı artarken, bu özelliklerin niteliksel olarak da içeriği önem kazanmaktadır. (Akpınar ve Akpınar, 2017, s. 107). Kaynak, söz konusu özellikleri taşıdığı ölçüde ikna edici olmaktadır.

İkna yoluyla dolandırıcılık örgüt tarafından mobil telefonlarından çağrı alan bireylerin, etkili iletişim becerileriyle psikolojik zafiyetlerinin belirlenmesi, kişisel bilgilerine ulaşılması, öngörülen tepkilerin alınarak çıkar amaçlı kullanılması süreçlerinden oluşmaktadır. Bu çalışma kapsamında literatürde kullanımına rastlanılmayan bir kavram olan *ikna yoluyla dolandırıcılık* kavramsallaştırmasına, özgün bir şekilde ulaşılmıştır. Hukuksal mevzuatta nitelikli dolandırıcılık suçu kapsamında değerlendirilen bu eylemler, sahte çağrı merkezleri tarafından örgütlü olarak gerçekleştirilmektedir.

Araştırmanın örneklemini 01.01.2019 ve 01.12.2019 tarihleri arasında sahte çağrı merkezleri tarafından İstanbul'da gerçekleştirilen ikna yoluyla dolandırıcılık suçları oluşturmaktadır. Bu doğrultuda olay sayıları ile mağdurların cinsiyet, öğrenim ve yaş durumları, değişkenler olarak ele alınmakta, betimsel yönteme dayanarak içerik analizi tekniği ile elde edilen veriler değerlendirilmektedir. Bu çalışmada; sahte çağrı merkezleri tarafından İstanbul'da gerçekleştirilen ikna yoluyla dolandırıcılık suçlarına ve bu suçların mağduriyet oluşturmasına yönelik bir durum tespiti ortaya konmaktadır. Çalışma kapsamında; İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü'nden alınan bilgiler çerçevesinde, yazar tarafından ikna yoluyla dolandırıcılığa ilişkin veriler; vaat yöntemi, korkutma yöntemi ve yardım kampanyaları yöntemleri olarak kategorize edilmektedir. Bu örgütlü, karmaşık ve çok taraflı eylemlerin birey ve toplumda oluşturduğu rahatsızlık ve endişe ise, süreç analizi kapsamında ele alınmaktadır.

İknanın Epistemolojik Okunması Bağlamında İkna Yoluyla Dolandırıcılık

Tasarlanan geri dönüşümlerin elde edilmesi amacıyla, tutumların benimsetilmesi veya davranışların değiştirilmesi için gerçekleştirilen sistemli faaliyetler, ikna başlığı altında toplanmaktadır. İkna kavramı çoğunlukla iletişimsel parametrelerle açıklanan, olumlu davranış ve motivasyonu hedefleyen stratejileri kapsamaktadır. İkna, kelime anlamı olarak Türk Dil Kurumu sözlüğünde "bir konuda birinin inanmasını sağlama, inandırma, kandırma" şeklinde tanımlanmaktadır ("İkna", t.y.). Herhangi bir konuda hedeflenen amacın gerçekleşmesine yönelik bilgilendirme, isteklendirme, beklenen tutum ve davranış modellerini benimsetme ya

da değiştirmeye yönelik gerçekleştirilen fonksiyonlar, ikna kavramıyla açıklanmaktadır. (Esgin, 2018, s. 28). Paradoksal bir bakış açısıyla değerlendirilen ikna yoluyla dolandırıcılık kavramı ise, manipülasyonlarla bireylerin sağlıklı karar vermesini engelleyen, özellikle olumsuz tutumların geliştirilmesini amaçlayan, menfaat odaklı aldatmaya yönelik süreci içermektedir.

İkna ile ilgili yapılan çalışmaların kökleri, Antik Yunan dönemi filozoflarından Aristoteles'in (M.Ö.385-M.Ö.322) düşüncelerine dek uzanmaktadır. Gözlemlere dayanarak oluşturulan *Retorik* adlı çalışmada ikna, "belli bir durumda elde var olan inandırma yollarını gözlemleme yetisi" olarak ifade edilmektedir (Aristoteles, 2004, s. 21). Retorik'de belirtilen; ethos – kaynağın inanılırlığı ve karizması, patos – duygusal çekicilik ve erdem, logos-mantıksal çekicilik kavramları, literatürde ikna bileşenleri olarak yer almaktadır (Yüksel, 1994, s. 22). Aristoteles'ten esinlenen Fârâbî (870-950) Kitâbu'1-Hatâbe adlı eserinde, ikna yöntemlerini teknik ve teknik olmayan olarak iki bölüme ayırarak, ikna yöntemlerini on üç maddede sıralamaktadır. İbn Sînâ'nın eseri Kitâbu'ş-Şifâ'nın, mantık kısmının sekizinci bölümünü oluşturan el-Hatâbe, özgün kavramlar ve daha ayrıntılı bir tasnif içermektedir. İbn Sînâ (980-1037) belli bir konuda iknayı gerçekleştirmek için kullanılan sözleri; temel ifadeler, hünerler ve yardımcı unsurlar olmak üzere üç başlıkta ele almaktadır (Coşkun, 2014, s. 46-67).

17. ve 18. yüzyıllarda düşünürler kişilerarası ve toplumsal ilişkilere yoğunlaşarak, ikna sonucu ortaya çıkan tutum ve davranışların hangi güdülere dayandığını bulmaya çalışmışlardır. Thomas Hobbes kuvvet ve egoizm kavramlarını, Adam Smith kişisel çıkar kavramını, Jeremy Bentham ve James Mill hedonizm ve zevk düşkünlüğünü bireylerin ikna süreçlerinde davranışlarına yön veren temel güdüler olarak ele almışlardır (Kağıtçıbaşı ve Cemalcılar, 2014, s. 26). İkna odaklı iletişimsel çalışmaların temeli büyük oranda sosyal psikolojiye dayanmaktadır.

Carl Hovland ve arkadaşları, Yale İletişim Araştırmaları projesi kapsamında tutum değişimi ve ikna üzerine 1949 yılında ilk deneysel çalışmayı yapmışlardır (Demirtaş, 2004, s. 75). 1950'li yıllardan itibaren, iknanın gerçekleşmesinde etkili olduğu düşünülen; bilişsel, duygusal ve davranışsal süreçlerin açıklanmasına yönelik kuramlar geliştirilmiştir. Öğrenme kuramı (Hovland vd., 1950), tutarlılık kuramları çerçevesinde denge kuramı (Heider, 1958), bilişsel dengeleme kuramı (Rosenberg ve Abelson, 1960), bilişsel çelişki kuramı (Festinger, 1957), süreç yaklaşımları çerçevesinde bilişsel tepki modeli (Greenwald, 1968), ayrıntılandırma olasılığı modeli, (Petty ve Cacioopo, 1983) bu kuramların başlıcalarıdır ve Eagly ve Chaiken (1993) tarafından detaylı şekilde açıklanmıştır (Dursun ve Tümer, 2012, s. 78).

Tarcan Kumkale ve Dolores Albarracin'ün (2004) yaptığı meta-analiz çalışması; mesaj çarpıcı bir tesire sahip ise kaynak olumsuz dahi olsa, dinleyen bireylerin zaman içinde mesaja inandıklarını ve ikna olduklarını göstermektedir. Dijital mecraların etkinliği, zaman ve mekândan bağımsız içerik üreten, anlık paylaşıma olanak sağlayan akıllı telefonların ve taşınabilir cihazların yaygınlığı, bireylerin istenen tepkiler vermesinde önemli rol oynamaktadır (Oinas ve Harjumaa, 2008, s. 200). Bir başka ifade ile interaktif bilgi teknolojisi, kullanıcılarda tutum ve davranış değişikliğine neden olan ikna teknolojisine dönüşmektedir.

Alanyazında, ikna ve dolandırıcılık başlıkları altında ele alınmış çalışmalar bulunmakla birlikte; *ikna yoluyla dolandırıcılık* adı altında kavramsallaştırılan bir çalışmaya henüz rastlanılmamıştır. Bu çalışmanın özgün değeri bu noktada ortaya çıkmaktadır ve çalışmanın amacı; bu sınırlı sayıdaki alanyazına katkı sağlamaktadır.

İkna, iletişim, ikna ve dolandırıcılık, ikna ve dolandırıcılık türleri temasında alanyazında çeşitli ve sınırlı sayıda çalışma mevcuttur. Cengiz Bahar'ın (2018) *Etkili İletişim ve İkna* adlı eseri ile Ümit Arklan ve Zafer Kartal'ın (2018) *İkna Edici İletişim Tekniği Olarak Tek Yanlı ve İki Yanlı Sunumun Kriz Yönetimi Sürecine Etkisi* adlı çalışmalarında, ikna ve iletişim ilişkisi ele alınmaktadır. Gönül Akpınar ve Kadir Akpınar (2017) ise *İkna Edici İletişimde Kaynak* adlı çalışmalarında kaynağın iletişim gücüne vurgu yapmaktadır. Thomas J. Holt ve Danielle C. Graves'in (2007) *Qualitative Analysis of Advance Fee Fraud E-mail Schemes* başlıklı çalışmalarında, toplumsal alanda kişilerin deneyimlediği dolandırıcılık biçimlerinden olan e-postalar üzerinden dolandırıcılık ele alınmaktadır. Bunun yanı sıra, Gareth Norris, Alexandra Brookes ve David Dowell'ın (2019) internet üzerinden yapılan dolandırıcılığa sistematik bir bakış yönelten *The Psychology of Internet Fraud Victimisation: A Systematic Review* başlıklı çalışmaları, konuya ilişkin bütünlüklü bir bakış açısı sunmaktadır.

İkna yoluyla dolandırıcılık suçu, sahte çağrı merkezleri tarafından mağdurların mobil telefonları aranarak gerçekleştirilmektedir. Hukuksal mevzuatımızda örgütlü nitelikli dolandırıcılık suçu bağlamında değerlendirilen bu eylemler, iletişime geçilen mağdurların kurgulanmış senaryolarla ikna edilerek, haksız kazanç sağlanmasıyla meydana gelmektedir. Karmaşık bir suç olarak ikna yoluyla dolandırıcılık; sahte çağrı merkezleri örgüt üyelerince mobil telefonlarından çağrı alan bireylerin, etkili iletişim becerileriyle psikolojik zafiyetlerinin belirlenmesi, kişisel bilgilerine ulaşılması, öngörülen tepkilerin alınarak çıkar amaçlı kullanılması süreçlerinden oluşmaktadır.

Hiyerarşik yapılanma, uygun araç-gereç-yer tedarik etme ve önceden toplanan verilerle kişileri aldatmaya yönelik eylemleri nedeniyle, sahte çağrı merkezleri "suç işlemek amacıyla örgüt kurmak ve nitelikli dolandırıcılık suçlarını işlemektedir" (TCK, 2004, md.158/1-L ve md.220-221). Bu yasa dışı örgütlenmenin temel beslenme kaynağını, ikna faaliyetlerinde kullanılan kişisel bilgiler oluşturmaktadır. Bu nedenle elde edilen bilginin doğruluğu, suçun işlenebilmesi için önemli bir unsurudur. Kurum, şirket, banka vb. organizasyon çalışanlarıyla doğrudan ya da dolaylı irtibat sağlayarak, çalışanlar suçlara ortak edilmeye çalışmaktadır. Bunun yanında sanal ortamlarda kanunsuz faaliyetleri gerçekleştirmek için kurulan bilgi kaynaklarından da yararlanılmaktadır.

Kişilerin ikna edilmesinde, bilgi kaynağının çeşitliliği kadar güncelliği de önemlidir. Maalesef internet odaklı ortamlar, suç örgütlerinin çıkar amaçlı faaliyetlerinde kullanmak üzere, kişilerin güncel bilgilerine ulaşmakta yarış halinde oldukları bir alana doğru evrilmiştir. Kullanıcılar tarafından daha önceleri büyük uğraşlarla elde edilen verilerin, artık sanal mecralarda paylaşılmasında bir sorun görülmemektedir (Peltekoğlu, 2012, s. 7). Suçlarda kullanılmak üzere sanal platformlardan ve örtülü dijital ortamlardan, kullanıma hazır güncel bilgiler elde

edilebilmektedir. Gündemi çok iyi takip eden dolandırıcılık şebekeleri, günün şartlarına göre popüler bilgileri kullanarak, bireyleri dolandırıcılık eylemlerinin hedefi konumuna getirmektedir (Button ve Cross. 2017 s. 26). Ulaşılan verilerde yer alan kişi bilgi portföyleri, ikna yoluyla dolandırıcılık yöntemini de belirlemektedir.

İkna yoluyla dolandırıcılık süreci; suçun hazırlık hareketleri, suçun icrası ve suçun sonuçlanması aşamalarından oluşmaktadır (*Tablo 1*). Hazırlık aşamasına, insan sirkülasyonunun yoğun olduğu saklanmaya müsait lokasyonlarda, sahte ya da çalıntı kimliklerle örgüt merkezlerinin kiralanmasıyla başlanmaktadır. Yasal iş yeri görüntüsüyle kamufle olan örgüt ofisleri, ikna yoluyla dolandırıcılığa uygun biçimde tasarlanmaktadır. Teknik altyapı anonimlilik ve gizlilik esaslarıyla oluşturulmakta, genellikle başkalarına ait kimliklerle hatlar açılmaktadır. İnternet üzerinden ses görüşmesine olanak sağlayan *Voice Over Internet Protocol (VoIP)* teknolojisi kullanılmaktadır. Hazırlık döneminde göze çarpan önemli bir husus da örgüt üyesi seçimi ve eğitimidir. Örgüt üyeleri yasa dışı çevrenin sabıkalılarından sağlanmaktadır. Değişik sektörlerde çağrı merkezi elemanı olarak çalışmış, deneyimli kişiler de kandırılarak örgüte katılmaktadır. Ayrıca dolandırıcılık eylemleri sonucunda, elde edilen maddi değerin aktarılacağı hesap sahipleri belirlenmektedir. Bu veriler; İstanbul Emniyet Müdürlüğü, Siber Suçlarla Mücadele Şube Müdürlüğü ham verilerinin derlenmesiyle araştırmada yer almaktadır.

İstenen davranışların gösterilmesi ve bireylerin zaaflarının istismar edilmesi için, hazırlık aşamasında elverişli verilerin temini ikna yoluyla dolandırıcılığın ön koşulunu oluşturmaktadır (Atkins ve Huang, 2013, s. 23). Bu bağlamda örgütlerce yasal olmayan içeriklerin bulunduğu deep webten, çeşitli birimlere insider koduyla yerleştirdikleri sektörel köstebeklerden gerekli veriler sağlanmaktadır. Bununla birlikte veri hırsızlığı amaçlı oluşturulan phishing sitelerde yapılan online işlemler ile tüm çoklu sanal ortamlarda bırakılan izler, phisingciler ve iz sürücüler tarafından toplanarak, örgütlere pazarlanmakta ve ikna dolandırıcılığına kaynaklık teşkil etmektedir.

Fiziksel altyapı ve kişisel verilerin oluşturulması, örgüt üyelerinin temini ve eğitimlerini tamamlanmasıyla, yasa dışı çağrı merkezi örgüt üyeleri, potansiyel mağdurlarla iletişim sağlayarak tüm fonksiyonlarıyla suçun icrasına başlamaktadır. Örgüt tarafından VoIP sistemiyle sağlanan iletişimde, gerçek sektörlerden arandığını düşünen bireyler dolandırıcılığa açık hale gelmektedir (Hoffstadt, Rathgeb, Liebig, Meister, Rebahi ve Thanh, 2014, s. 807). Bu dönemde yoğun olarak ikna iletişimi yaşanmaktadır. Dolandırma maksadıyla irtibat sağlayan sahte çağrı merkezleri, bireylerin kredi kartı bilgilerine ulaşmak için, ikna edici ve itimat sağlayıcı bilgileri sıralamaktadır. Bu bilgiler *Tablo 1*'de belirtilen, kişilere doğru kaynak tarafından arandığını hissettiren; banka hesap bilgisi, ad-soyad, TC kimlik numarası, doğum tarihi, dijital mecrada yapılan en son işlem vb. gibi özelliklerden birini ya da tamamını barındırabilmektedir. Örgüt üyeleri kişilere ait özel bilgilerle, çeşitli kamu ve özel kurumların meslek temsilcileri gibi, vatandaşlarla mobil telefonlarından irtibata geçmektedir.

Son aşamada, örgüt üyeleri sahip oldukları özel bilgiler ve gündemin hassasiyetleri doğrultusunda, gerçek dışı vaatler ve kurgu olaylarla bireyleri ikna etmektedir. Bireylerden

işlemin sonlandırılması için, mobil telefonlarına gelen şifreyi tuşlamaları istenmektedir. Şifrenin tuşlanmasıyla, fark etmeden ödeme ya da transfer talimatı verilmektedir. İkna yoluyla dolandırıcılık suçu sonuçlanmakta ancak bireylerin mağduriyetleri henüz başlamaktadır. Dolandırıcılık neticesi haksız kazancın temin edilmesinde, birkaç husus belirleyici olmaktadır. E-ticaret sitelerinden mağdurlara ait kart bilgileri kullanılarak, kolaylıkla nakde çevrilebilecek malzemeler satın alınmaktadır. Hazırlık aşamasında tespit edilen hesaplar kullanılarak, mağdurların mevduatlarında bulunan tutarlar, üçüncü şahısların hesaplarına internet üzerinden EFT/havale yapılmaktadır. *Tablo 1*'de gösterildiği gibi ilgili banka şubelerinden EFT/havale yapıldıktan kısa bir süre sonra çekilerek ya da başka hesaplara transferler sağlanarak, ikna yoluyla dolandırıcılık suçu tamamen sonuçlanmaktadır.

Tablo 1. İkna Yoluyla Dolandırıcılık Süreci

SUÇUN HAZIRLIK HAREKETLERİ	SUÇUN İCRASI	SUÇUN SONUÇLANMASI
Gizlenmeye Uygun Lokasyonlarda Sahte Çağrı Merkezinin Belirlenmesi	Mobil Telefonlardan İletişimin Başlatılması	Hesap ve Kredi Kartı Bilgilerinin Elde Edilmesi
Fiziki Şartların Oluşturulması	**Vaatler Yöntemi** Kurgu Teklifler ve Senaryoların Kullanılması **Korkutma Yöntemi** Kamu ve Özel Sektör Görevlileri Unvan ve Sıfatlarının Kullanılması **Yardım Kampanyaları Yöntemi** Sözde Yardım Kampanyalarının Düzenlenmesi	Mobil Telefonlara Şifre Gönderilmesi ve Tuşlanma Talebinin İletilmesi • Şifrenin Tuşlanması ile Ödeme Talimatı • Hesaba Transfer/EFT/Havale Talimatı • E-ticaret Sitelerinden Alışveriş Talimatı
Teknik Altyapının Oluşturulması • VoIP Teknoloji Kullanımı	İkna İletişiminin Sürdürülmesi	İkna Dolandırıcılığının Gerçekleşmesi
Örgüt Üyesi Seçimi ve Eğitimi Son Hesap Sahiplerinin Tespiti Kişilere Ait Özel Verilerin Elde Edilmesi • Dark Web – Insider Faktörü • Phishing Siteler – Veri Çöplüğü Analizi		İkna Dolandırıcılığını Sonlandırılması • Banka Şubelerinden Mevduatın Çekilmesi • Başka Hesaba Transfer/EFT/Havale Edilmesi

Kaynak: Bu tablo, İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü'nden alınan verilerden hareketle yazar tarafından oluşturulmuştur.

İkna Yoluyla Dolandırıcılığın Etkili İletişim ile İlişkisi ve Tipolojisi

Etkili iletişim, duygu ve düşüncelerin elverişli ortamlarda paylaşılarak, tarafların inandırılma ve ikna edilme süreçlerini içermektedir. Etkili iletişim ile benzer ve kapsamlı metodoloji izlediğinden, ikna yoluyla dolandırıcılık suçunun işlenmesinde ikna iletişimi kavramının kullanılması uygun görülmektedir. İkna iletişiminin bileşenleri olan; etkileme, ilgi çekme,

benimsetme gibi duygusal ve bilişsel teknikleri kullanan örgüt üyeleri, ikna yoluyla dolandırıcılığın geçekleşmesinde önemli paya sahiptir.

Doğal hayatın akışı içerisinde alınan iletilere karşı tutumların geliştirilmesi, rasyonel ya da anlık tepkilerin verilmesi, genel iletişim döngüsünü oluşturmaktadır. Bu süreçte bireyler, bulundukları yer ve koşulların gerektirdiği iletişim yöntemlerini kullanmaktadır (Yıldırım, 2018, s. 13). Etkili iletişim ile sürdürülen aktif bilgi alışverişi, bireylerin yaşamı paylaşma ve algılama ölçütlerini belirlemektedir. İkna ise, iletişim teknikleri kullanılarak hedefin tavırlarında istenilen değişikliğin oluşturulmasıdır. Ece Karadoğan Doruk'un (2015) belirttiği üzere ikna, spesifik bir konuda muhataplarının inanmasını sağlamak için gerçekleştirilen etkin yöntemleri kapsamaktadır (s. 5). İknanın, etkili iletişim içerisinde kendine önemli bir yer edindiği görülmektedir (Kurudayıoğlu ve Yılmaz, 2014, s. 85). Bu bakımdan etkili iletişim ve ikna parametreleri hem subjektif çıkarımlarla insan ilişkilerinin merkezinde konumlanmakta hem de sunduğu katkılarla onu tamamlayan bir olguyu çağrıştırmaktadır.

İkna, gücün etkili stratejiler ve iletişimsel çabalar ile toplumsal yaşamda kullanılmasıdır (Naksawat, Akkakoson ve Loi, 2016, s. 4). İç içe geçmiş yapıları, süreçlerde kaynak, mesaj, araç ve alıcı/hedef gibi temel öğeleri kullanmaları nedeniyle etkili iletişim ve ikna kavramları, ikna iletişimi ortak paydası altında kodlanmaktadır. Tavır değişikliğini hedeflemeyen sıradan anlaşmaya yönelik iletişim çabaları bir kenara bırakıldığında, etkili iletişim yöntemlerinin başarısıyla, ikna sistematiği arasında yakın bir ilişki olduğu görülmektedir.

İkna iletişiminde kaynak, hedef bireylerle telefon irtibatı sağlayan sahte çağrı merkezleri örgüt üyelerinden oluşmaktadır. Alıcılar, örgüt elemanlarından ikna dolandırıcılığı amacıyla çağrı alan mağdur olabilecek bireylerdir. Mesajlar, örgüt elemanlarınca bireyde istenen etkiyi uyandırmak için mobil telefonlar aracılığıyla iletilmektedir. İkna iletişiminin yoğun olarak yaşandığı bu iletişimsel döngüde, bireylerin mağduriyeti ile sonuçlanan ikna yoluyla dolandırıcılığın iki temel tarafı bulunmaktadır. Bunlar alıcı konumundaki kişiler ve dolandırıcılık eylemini gerçekleştirmeye çalışan kaynak pozisyonundaki örgüt üyeleri olarak görülmektedir.

Bireyler doğal hayatın akışı içerisinde telefonları çaldığında, gereken dikkati gösteremeyebilir ve hata yapabilmektedir. Diğer taraftan örgüt üyeleri, mağdur edecekleri bireyler hakkında topladıkları bilgiler doğrultusunda planlı çağrılar yapmaktadır. İkna yetenekleriyle bireylerin güvenini kazandıktan sonra, dolandırıcılık eylemini daha kolay gerçekleştirmektedir. İkna iletişimi, mağdurlara düşünme fırsatı vermeden, örgüt üyesinin otoritesi ve yönlendiriciliği ile sürdürülmektedir. Bireylerden rasyonel olmayan, duygusal cevaplar vermesi beklenmektedir. Richard Petty, Thomas Ostrom ve Timothy Brock'un (2014) da işaret ettikleri gibi güçlü bir senaryo ve kurum profiliyle bireyleri şüphelendirmeyen özel jargon ve terminoloji ön plana çıkarılmaktadır (s. 6).

Bireylerin; korku, dikkatsizlik, hırs ve duygularının kötüye kullanımında, örgüt üyelerinin iletişimsel yetenekleri belirleyici olmaktadır. Örgüt elemanlarının ilgi çeken korkutucu ya da heyecan verici tekliflerine karşı duramayan bireyler, ikna iletişimi sonucunda dolandırıcılara yenik düşmektedir. İkna iletişimini etkili bir biçimde uygulayan ikna dolandırıcıları farklı

tipolojilerde karşımıza çıkabilmektedir. Bu tipolojiler, deep web kullanımını, veri çöplüğü analizini, insider faktörünü ve phishing yöntemini içermektedir.

Deep Web Kullanımı

Deep web, internette çeşitli teknik nedenlerle, açık hizmet veren geleneksel arama motorları tarafından ulaşılamayan, kapalı ve özel bir ağ sistemidir. Bu ağa ancak *The Onion Routing* sözcüklerinin baş harflerinden oluşan, *Tor tarayıcısı* ile anonim olarak ulaşılmaktadır (Spalevic ve Ilic, 2017 s. 75). Tor tarayıcısıyla ağ katmanlarından oluşan çoklu sanal ortamda, tüm internet kullanıcılarının ulaşamadığı web sitelerine ve verilere erişilmektedir.

Derin ağda yasal olamayan birçok içeriğe, internetin karanlık yüzünü betimleyen dark web katmanından *onion* ve *clos* uzantılı domainlerle ulaşılmaktadır (Rudesill, Caverlee ve Sui, 2015 s. 6). Bu çoklu sanal ortamlar; kurum ve şirketlerin veri tabanlarına, kişisel verilere, kredi kartı bilgilerine, sahte evrak ve belgelere yasa dışı ulaşımı mümkün kılmakta ve ikna yoluyla dolandırıcılığın alt yapısını oluşturmaktadır.

Veri Çöplüğü Analizi

Bilişim sistemlerindeki veri transferinin gerçekleştirildiği alanlar çeşitlenmiş, bu doğrultuda iletişim, davranışlarda farklılık oluşturan bir süreç olarak anılmaya başlamıştır (Karadeniz, 2010, s. 35). Sanal platformlar olanaklar ve riskler çelişkisini eş zamanlı sunmaktadır. Bireylerin kamu ve finans sektörlerinin yanı sıra alışveriş siteleri, sosyal medya platformları, forumlar ve bloglarda bıraktıkları kişisel izler, yasa dışı örgütlerce sıklıkla pazarlanır hale gelmektedir. Mustafa Ünver, Cafer Canbay ve Ayşe G. Mirzaoğlu'nun (2009) da belirttiği gibi sanal ortamın ve sosyal ağların veri çöplerini toplayan yasa dışı örgütler, dolandırıcılık girişimlerinde bu materyalleri kullanmaktadır (s. 19).

Insider Faktörü

Insider kavramı, dijital ortamda faaliyet gösteren bankacılık, finans, üretim, hizmet, bilişim gibi kurum ve organizasyonlardan çıkar amaçlı bilgi sızdıran, verilere ulaşma yetkisine sahip kişiler için kullanılmaktadır. Bu kişiler organizasyon yapısını bilen, teknik olarak yetenekli, kritik bilgilere erişebilen kurumsal casuslardır (Spitzner, 2003, s. 76). Köstebekler yasa dışı faaliyet gösteren örgütlerce, gizli ve güncel bilgileri temin etmek için kurumlara özelikle yerleştirilen kişilerdir. Köstebek temininde bir diğer yöntem de mevcut kurum çalışanlarıyla menfaat karşılığı bağlantı kurularak, kurum paydaş ve müşterilerinin önemli verilerine ulaşılmasıdır. Kurumsal ve ticari ilişkileri bulunan kişilerin detaylı bilgilerine bu yolla sahip olan örgüt üyeleri, ikna süreçlerinde ve dolandırıcılık eylemlerinde inandırıcılığını arttırmaktadır.

Phishing Yöntemi

Phishing, kullanıcı hesaplarına e-posta gönderilerek gerçekleştirilen çevrimiçi saldırı metotlarından biridir (Brody, Mulig ve Kimball, 2007, s. 45). Genellikle kullanıcı kimlik bilgileri, şifreler, kredi kartı bilgileri, ağ kimlik bilgileri gibi hassas ve gizli bilgilere ulaşmak amacıyla internet ortamında yapılan saldırılardır (Kirda ve Kruegel, 2006, s. 560). Bu saldırılarda kandırılan kullanıcı, oltaya takılan bir balığa benzetildiğinden dilimizde oltalama sözcüğü ile karşılık bulmaktadır.

Dolandırıcılık faaliyetlerinde kullanılabilecek bilgilere erişmek için bilinen ve güvenilen banka, firma veya kurumların aslından ayırt edilemeyen imajlarıyla kullanıcılara e-posta gönderilmektedir. Alıcılar iletilerin gerçek ve itimat edilir bir kaynaktan geldiğine inandırılmaktadır (Fette, Sadeh ve Tomasic, 2007, s. 249). Kullanıcılar tarafından sahte oldukları fark edilemeyen sitelerin, ek ve uzantılarına girilen tüm özel bilgiler saldırganların eline geçmektedir.

Amaç ve Yöntem

Araştırmanın Amacı

Bu çalışmanın amacı; sahte çağrı merkezleri tarafından İstanbul'da gerçekleştirilen ikna yoluyla dolandırıcılık suçlarına ve bu suçların mağduriyet oluşturmasına yönelik bir durum tespiti ortaya koymaktır. Mağdurların özellikleri dikkate alınarak ikna yoluyla dolandırıcılık yöntemlerinin, olay sayılarına göre dağılımları altı ana başlıkta toplanarak araştırma soruları oluşturulmuştur. Bu doğrultuda araştırmanın amacı çerçevesinde belirlenen altı amaç sorusu şunlardır:

1. Sahte çağrı merkezleri tarafından gerçekleştirilen ikna yoluyla dolandırıcılık, mağdurlarının cinsiyetlerine göre nasıl şekillenmektedir?
2. Sahte çağrı merkezleri tarafından gerçekleştirilen ikna yoluyla dolandırıcılık, mağdurlarının öğrenim durumlarında etkili midir?
3. Sahte çağrı merkezleri tarafından gerçekleştirilen ikna yoluyla dolandırıcılık suçlarında, mağduriyet ve yaş ilişkisinde belirleyici unsurlar nelerdir?
4. İkna yoluyla dolandırıcılık suçunda kullanılan yöntemler nelerdir?
5. İkna yoluyla dolandırıcılık yöntemlerinde, mağduriyet oranlarının tespitine yönelik veriler nelerdir?
6. Sahte çağrı merkezlerinin örgütsel sistematiği nasıldır?

Çalışmanın iki temel hipotezi bulunmaktadır ve bu hipotezler araştırma soruları kapsamında sınanmıştır:

– Sahte çağrı merkezlerinin belirli bir sistematiği, örgüt şeması bulunmaktadır.

– İkna yoluyla dolandırıcılık suçu demografik özelliklere göre değişiklik göstermektedir.

Sınanan hipotezlere dair veriler, çalışmanın bulgular kısmında yer almaktadır.

Araştırmanın Yöntemi

Çalışma kapsamında, söz konusu alt amaç sorularından hareketle; İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü kayıtlarında yer alan verilerin toplanması hedeflenmiştir. Araştırmada; betimsel yönteme dayanarak içerik analizi tekniği ile elde edilen veriler değerlendirilmiştir.

Gürol Cantürk ve Nergis Cantürk'e (2004) göre; suç eyleminden sorumlu bireylerin kişilik özelliklerini gösteren yöntem olan *suçlu profili* kapsamında yapılan tanımlama çalışmalarında suçlu kişiye dair birtakım veriler elde edilmektedir. Yine Cantürk ve Cantürk'ün (2004*) Suçlu Profili* başlıklı çalışmalarında, *Suçlu Kişilik Profili ile Elde Edilebilen Özellikler* kısmında, Geberth'in tasnifine göre; 22 özellikten 3'ü yaş, cinsiyet ve öğrenim durumudur. Bu nedenle, bu 3 özellik, çalışmanın analizi kısmında faydalı olacak verilerdendir.

01.01.2019 ve 01.12.2019 tarihleri arasında sahte çağrı merkezleri tarafından İstanbul'da gerçekleştirilen, ikna yoluyla dolandırıcılık suçlarına ilişkin verilerin özellikleri *Tablo 2*'de gösterilmektedir. Bu özellikler şu şekildedir: Araştırmadaki veriler, araştırmaya konu olan suç kapsamına dair sayısal veriler ve araştırmanın demografik verileri olmak üzere iki temel eksende konumlandırılmıştır. Araştırmaya konu olan suç kapsamına dair sayısal veriler kısmında, suça maruz kalanların İstanbul içi ve dışında ikamet etmelerine göre belirlenen nicelik değeri, mağdur sayılarının tespiti açısından önem arz etmektedir. Araştırmanın demografik verileri ise; yaş, cinsiyet ve öğrenim durumu öğelerinin söz konusu suçun vuku bulmasında etken olup olmadığı, öğrenim durumunun mağduriyette bir engel teşkil edip etmediği, cinsiyetin suça maruz kalmada belirleyici bir öğe olup olmadığı sorularından hareketle elde edilmiş verilerdir *(Tablo 2)*.

Tablo 2. İkna Yoluyla Dolandırıcılık Suç Araştırmasının Kategorik Özellikleri

Araştırmaya Konu Olan Suç Kapsamına Dair Sayısal Veriler	
İstanbul'da İşlenen İkna Yoluyla Dolandırıcılık Suçlarında İstanbul İkamet Eden Mağdurlar	240
İstanbul'da İşlenen İkna Yoluyla Dolandırıcılık Suçlarında İstanbul Dışında İkamet Eden Mağdurlar	174
Suça Maruz Kalan Toplam Mağdurların Sayısı	**414**
Araştırmaya Konu Olan Suç Kapsamına Dair Oransal Demografik Veriler	
Yaş	25 Yaş Altı %7, 26-35 Arası %21 36-45 Arası %27, 45-56 Arası%24, 56 Yaş Üzeri %21
Cinsiyet	Erkek %70, Kadın %30
Öğrenim Durumu	İlköğretim %20, Ortaöğretim %7 Lise %38, Önlisans %3, Lisans %30 Yüksek Lisans %1, Doktora %1

Kaynak: Bu tablo, İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü'nden alınan verilerden hareketle yazar tarafından oluşturulmuştur.

Araştırmanın Modeli

Çalışmada; betimsel yönteme dayanarak içerik analizi tekniği ile elde edilen veriler değerlendirilmiştir. Bu bağlamda 01.01.2019 ve 01.12.2019 tarihleri arasında meydana gelen ikna yoluyla dolandırıcılık olaylarının, mağdurlar açısından sayısal tanımlanması ve oransal dağılımından yararlanılmıştır. Bütünleşik bir bakış açısıyla araştırmaya kaynaklık eden tüm veriler birlikte ele alınmıştır.

Verilerin Toplanması ve İşlenmesi

Çalışmada araştırmaya dâhil edilen örneklem, 01.01.2019 ve 01.12.2019 tarihleri arasında sahte çağrı merkezleri tarafından İstanbul'da gerçekleştirilen, ikna yoluyla dolandırıcılık suçlarından oluşmaktadır. Belirtilen tarih aralığı, bu suçlara dair en güncel verileri içerdiğinden araştırmaya dahil edilmiştir. Mağdurların cinsiyet, öğrenim ve yaş durumları, temel kategorizasyon verisi olarak değerlendirilmiştir. Çalışma kapsamında üç farklı gerçekleştirme yöntemiyle ele alınan ikna yoluyla dolandırıcılık, oransal olarak çözümlenmiştir. İkna yoluyla dolandırıcılık suçlarında kullanılan yöntemlerin, alt kategorizasyon verileri, olay ve mağdurlara göre dağılımlardan oluşmaktadır. Son aşamada ise dolandırıcılık faaliyetlerinde kullanılan her yöntem, olay ve mağdur sayısı bağlamında detaylı olarak analiz ederek yorumlanmıştır.

Bulgular

Araştırmada bireyleri mağdur statüsüne taşıyan çok yönlü ikna yoluyla dolandırıcılık eylemleri, süreç analizi kapsamında ele alınmaktadır. Pragmatik anlayışla öncesi-sırası-sonrası parametreleriyle işlenen nitelikli ve örgütlü ikna yoluyla dolandırıcılık suçu, detaylı olarak değerlendirilmiş, sahte çağrı merkezleri kurularak işlenen bu türden eylemlerde, kişilerin güvenini kazanma metotları etraflıca incelenmiştir. Hukuksal, istatistiksel ve iletişimsel boyutlarıyla irdelenmiştir.

Araştırmada hile ve kandırmaya yönelik mobil telefonlar üzerinden bireylerle sağlanan irtibat, ikna iletişimi ve gerçekleştirilen eylemler; ikna yoluyla dolandırıcılık suçlarında demografik dağılım, ikna yoluyla dolandırıcılık yöntemleri, ikna yoluyla dolandırıcılık yöntemlerinde mağduriyet oranları ve sahte çağrı merkezleri örgüt sistematiği başlıkları altında sentezlenmiştir.

İkna Yoluyla Dolandırıcılık Suçlarında Demografik Dağılım

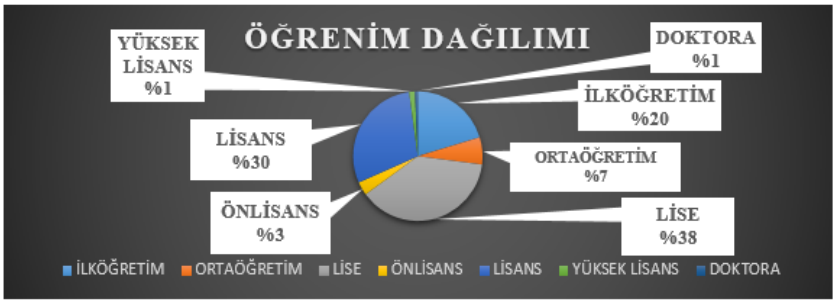
Araştırmanın amacı çerçevesinde oluşturulan 1. 2. ve 3. soruları kapsayan sahte çağrı merkezleri tarafından gerçekleştirilen ikna yoluyla dolandırıcılık suçlarında, cinsiyet, öğrenim ve yaş kriterlerinin mağduriyet oluşumundaki etkisi, demografik dağılım başlığı altında ele alınması uygun görülmüştür. Çalışmanın hipotezlerinden biri olan *ikna yoluyla dolandırıcılık suçu demografik özelliklere göre değişiklik göstermektedir* hipotezini doğrular nitelikte veriler elde edilmiştir.

İkna yoluyla dolandırıcılığa uğramış bireylerin cinsiyetlerine göre bir değerlendirme yapıldığında, erkek mağdur sayısının kadın mağdur sayısından daha fazla olduğu görülmektedir. Değişik yöntemleri bulunan toplam 414 ikna yoluyla dolandırıcılık eyleminde, erkek mağdurların rakamsal ifadesi 287 olarak belirtilirken, kadın mağdurlarda bu rakam 127 olarak görülmektedir. Bir başka ifade ile ikna yoluyla dolandırıcılığa maruz kalma oranları erkelerde yaklaşık %70, kadınlarda yaklaşık %30 olarak izlenmektedir (*Şekil 1*). Bu oransal durum iş yaşantısında erkeklerin, bilişim sistemlerini ve internet merkezli sanal ortamları daha fazla kullandıklarını ve bıraktıkları izlerle, örgütlerin hedefi haline geldiklerini göstermektedir.

Şekil 1. İkna Yoluyla Dolandırıcılık Suçunun Mağdur Cinsiyetine Göre Dağılımı

Kaynak: Bu şekil, İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü'nden alınan verilerden hareketle yazar tarafından oluşturulmuştur.

İkinci önemli veri de ikna yoluyla dolandırıcılık suçuyla, mağdurların öğrenim durumlarının irdelenmesi ile elde edilmektedir. Kayıtlarda; ikna yoluyla dolandırıcılık suçuyla karşılaşan ilköğretim-lise mezunu mağdurların oranı yaklaşık %65, ön lisans-doktora mezunu mağdurların oranı ise yaklaşık %35 olarak tespit edilmektedir (*Şekil 2*). Mağdurların öğrenim durumları dikkate alındığında, öğrenim süresi artıkça, ikna yoluyla dolandırıcılık suçunun azalma eğilimi gösterdiği görülmektedir.

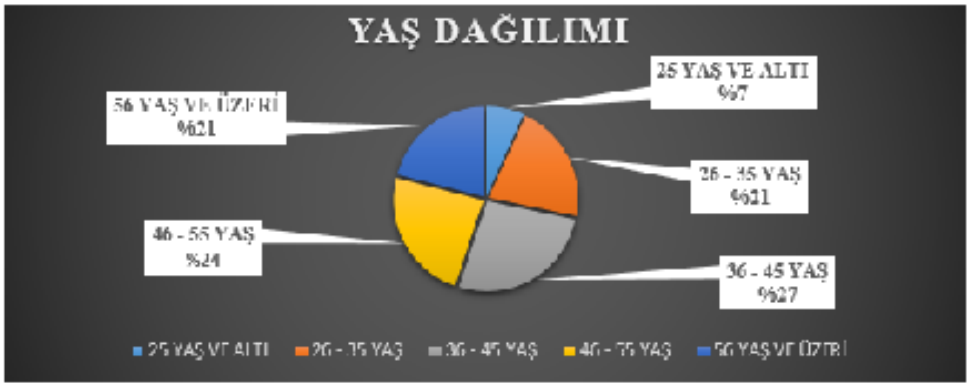


Şekil 2. İkna Yoluyla Dolandırıcılık Suçunun Mağdur Öğrenim Durumuna Göre Dağılımı

Kaynak: Bu şekil, İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü'nden alınan verilerden hareketle yazar tarafından oluşturulmuştur.

Demografik dağılımda diğer dikkate değer husus da ikna yoluyla dolandırıcılık suçlarında, yaşın belirleyici unsur olup olmadığıdır. Yaş ve mağduriyet arasındaki bağıntıda, örgüt profesyonelliğinin yanı sıra mağdurların arayanlara yaklaşım biçimleri de etkili olmaktadır. 35 yaş üstü mağdurlar, yaklaşık %72'lik bir oranla tüm ikna yoluyla dolandırıcılık suçlarında fark edilebilir bir paya sahiptir. Arayanlara şüpheci yaklaşmayan, teknoloji sistemlerinin dönüşümü ve buna bağlı değişen işleyiş biçimlerine adapte olmaya çalışan bu yaş grubu mağdurlarının, sahte çağrı merkezi üyelerince iyi niyetleri istismar edilmektedir (*Şekil 3*).

35 yaş altı mağdurlar, bilişim sistemlerinin kavramsal ve uygulamalı bilgilerini kullanmakta ve özellikle akıllı telefonların iletişimsel özelliklerini oldukça iyi bilmektedir. Potansiyel tehlikelerin farkındalığıyla arayanlara temkinli davrandıklarından, mağduriyet oranları, yaklaşık %28 bandında seyrettiği *Şekil 3*'de görülmektedir. Bu grupta öğrenim ölçütlerinin aksine, mağdur yaşının ve olay sayısının birlikte arttığı doğrusal bir ilişki izlenmektedir.



Şekil 3. İkna Yoluyla Dolandırıcılık Suçunun Mağdur Yaşına Göre Dağılım

Kaynak: Bu şekil, İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü'nden alınan verilerden hareketle yazar tarafından oluşturulmuştur.

İkna Yoluyla Dolandırıcılık Yöntemleri

Araştırmanın 4. sorusu ikna yoluyla dolandırıcılığın güncel metodolojisini belirleme ve yöntemlere ilişkin saptamaları, sistemli bir şekilde ifade etme imkânı sağlamaktadır. Çalışmanın temel veri olarak kabul ettiği, araştırma tarihleri arasındaki ikna yoluyla dolandırıcılık suçları, işleniş biçimleri ve belirgin özellikleri bakımında tasnif edilmiştir. Verilerinin analizi neticesinde ikna yoluyla dolandırıcılık suçlarında, örgütlerin kullandığı üç değişik yöntem, olay sayıları ile birlikte okunduğunda dramatik özelliklerinin öne çıktığı görülmektedir. Çalışmanın dinamikleri doğrultusunda ikna yöntemlerini; *Vaat Yöntemi, Korkutma Yöntemi* ve *Yardım Kampanyaları Yöntemi* biçiminde özgün başlıklar altında toplamak mümkündür. Her üç yöntem, gerçekleştirme biçimleri, olay ve mağdur sayıları ölçeğinde incelenmiş ve örgütlerin etkili iletişimleriyle ilgili çıkarımlar elde edilmiştir. Bu bağlamda *Vaat Yöntemi* ile dolandırıcılık; vize talebi onayı, aidat,

vergi, faiz, sigorta işlemlerinde iade ya da dosya masrafı silme, kefilsiz, faizsiz, belgesiz kredi talebi onayı vb. gibi, bireyleri aldatmaya yönelik taahhütleri kapsamaktadır. *Tablo 3*'de belirtildiği gibi, bütün içerisinde yaklaşık %80'lere ulaşan yüksek orandaki olay sayısı oldukça düşündürücüdür.

Bu tür suçlarda görülen örgütsel başarı, şüphesiz üyelerinin iletişimsel beceri ve yetkinliklerle ikna sürecini yönetmelerinden kaynaklanmaktadır. Ancak mağdurların istenen davranışları göstermelerine eleştirel bir bakış açısı getirilmelidir. Mağdurları hata yapmaya zorlayan; etkin dinleme yapmamaları, avantaj sağlama ve sahiplenme dürtülerine hâkim olamamaları, bilinmeyen bir kaynaktan karşılıksız bir şey verilmeyeceği gerçeğini unutmalarıdır.

Korkutma Yöntemi ile dolandırıcılık; kamu görevlisi, polis, vb. gibi adlar altında hesaplarda şüpheli hareket olduğu beyan edilerek ya da hukuk büroları çalışanı sıfatıyla icra takibi yapılacağını bildirerek, menfaat temin etme girişimleridir. Olay sayıları açısından bu yöntem, ikna yoluyla dolandırıcılık suçlarında yaklaşık %19 olarak tespit edilmiştir (*Tablo 3*). En temel özelliği, panik ve korku hissi uyandırarak kişilerin sağlıklı düşünmesini engellemek ve onları sömürmeye çalışmaktır. Bu dolandırıcılık yöntemine kamu spotlarında, geleneksel ve dijital medyada sıklıkla dikkat çekildiğinden, olay sayılarında oransal olarak azalma eğilimi görülmektedir.

Araştırma kapsamındaki üçüncü ikna yoluyla dolandırıcılık yöntemi ise; iyi niyetli, yardımsever bireylerin duygularını suistimal etmek amacıyla, sözde yardım kampanyalarıyla gerçekleştirilen aramalardan oluşmaktadır. *Yardım Kampanyaları Yöntemi* ile örgüt üyeleri engelli veya hasta çocukları bahane ederek senaryolaştırdıkları yardım kampanyalarıyla mağdurları aldatmaya çalışmaktadır. Bu içerikteki dolandırıcılığın, olay sayıları bakımından tüm yöntemler arasında yalnızca %1'lik bir oranı temsil ettiği *Tablo 3*'de görülmektedir. Sonuçlara bakıldığında sağlık ve yardım konularının kötüye kullanımına karşı toplumda bir bilinçlenme olduğu görülmektedir. Diğer taraftan üzerinde durulan iki yöntemle karşılaştırıldığında, toplumun bu içerikteki aramalara ehemmiyet göstermediği ve üçüncü şahısları ilgilendiren konulara oldukça mesafeli baktığı gözlenmektedir.

İkna Yoluyla Dolandırıcılık Yöntemlerinde Mağduriyet Oranları

Araştırmanın 5. sorusu, ikna yoluyla dolandırıcılık yöntemlerinin içerikleri, sınıflandırılması ve mağduriyet oluşumları hakkında oransal çıkarımları amaçlamaktadır. İkna yoluyla dolandırıcılığı yöntemleri, mağdur sayıları açısından da üç temel özellikte gruplanmaktadır. *Vaat Yöntemiyle*, vize talebi onayı, aidat, vergi, faiz, sigorta işlemlerinin iadesi kapsamında 161; dosya masrafı silme, kefilsiz, faizsiz, belgesiz kredi talebi onayı kapsamında 46 kişi ikna yoluyla dolandırıcılık suçlarından mağdur olmuştur. Toplamda 207 mağdura ulaşan *Vaat Yöntemi*, genel ortalamada yaklaşık %50'lik bir hacime sahiptir (*Tablo 3*). Veriler birlikte sentezlendiğinde olay sayılarının yüksekliği, mağdur sayılarını da arttırdığı değerlendirilmektedir.

Korkutma Yöntemiyle ise; kamu görevlisi, polis, vb. gibi adlar altında hesaplarda şüpheli hareket olduğu beyan edilerek 36 kişi**;** hukuk büroları çalışanı sıfatıyla icra takibi yapılacağı kurgulanarak yapılan aramalarda ise 119 kişi mağdur edilmiştir. Toplam 155 mağdur ve yaklaşık %38 oranla, ikna yoluyla dolandırıcılık suçlarında, ikinci yüksek veri elde edilmiştir. Tüm kitlesel

medya araçlarıyla ve sanal ortamlarda yapılan uyarılara rağmen, resmi kurum görevlisi veya polis unvanları kullanarak, yaklaşık %9'luk bir oranla ikna dolandırıcılığı yapılabilmektedir. Bireyler anlık refleksleri ve gündelik hayatın stresi nedeniyle mağdur olurken, sahte çağrı merkezi örgüt üyelerinin iletişim yönetimindeki kabiliyetleri öne çıkmaktadır. İcra takibi öne sürülerek korku ve panik oluşturmak suretiyle işlenen dolandırıcılık suçu, son dönemlerde ortaya çıktığından, yaklaşık %29'luk bir oranla, mağdur sayısında önemli bir artış söz konusudur (*Tablo 3*). Bundan dolayı örgüt üyelerinin strateji ve taktikleri deşifre oldukça değişen gündemi takip ederek yeni tekniklerle dolandırıcılık eylemlerini sürdürdüğü anlaşılmaktadır.

Çalışmanın dayanak noktasını oluşturan polis kayıtlarında, *Yardım Kampanyaları Yöntemi* ile gerçekleştirilen dolandırıcılık eylemlerinde, olay sayısı 1 ve bu olayın mağdur sayısı 52 olarak görülmektedir. Çeşitli çevrelerden elde ettikleri verilere istinaden, özellikli bir dolandırıcılık eylemi üzerine odaklanarak kurulan sahte çağrı merkezi örgütleri yakalandıklarında, gerçekleştirdikleri ikna yoluyla dolandırıcılık suçu, olay sayısı olarak numaralandırılmaktadır. Olaylara özgü dinamikler ve mağdur sayısı göreceli olarak değişmektedir. Çalışmada belirtilen zaman aralığında, engelli veya hasta çocuklar için yardım kampanyası adı altında yapılan dolandırıcılıkta mağdur sayısı yaklaşık %12 olarak tespit edilmiştir (*Tablo 3*). Bu yüzdesel ifade, yalnızca bir olayda dahi yüksek mağdur sayısına ulaşabilen ikna yoluyla dolandırıcılık eylemlerinin, toplumda oluşturduğu rahatsızlık ve endişe boyutunu ortaya koymaktadır. Altı çizilmesi gereken önemli husus, bu türden nitelikli dolandırıcılık suçunu işleyen örgütlerin, bireylerin hayatında ekonomik, psikolojik ve sosyolojik deformasyonlara sebebiyet vermesidir.

Tablo 3. İkna Yoluyla Dolandırıcılık Yöntemlerinin Olaya ve Mağdura Göre Dağılımı[1*]

	YÖNTEM	OLAY SAYISI	YÜZDELİK ORAN	MAĞDUR SAYISI	YÜZDELİK ORAN
VAAT YÖNTEMİ	**VAAT YÖNTEMİ-1** Vize talebi onayı, aidat, vergi, faiz, sigorta işlemlerinin iadesi vaadiyle dolandırıcılık	125	%48	161	%38
	VAAT YÖNTEMİ-2 Dosya masrafı silme, kefilsiz, faizsiz, belgesiz kredi talebi onayı vaadiyle dolandırıcılık	80	%32	46	%12
	TOPLAM VAAT YÖNTEMİ	205	%80	207	%50

1 *Tablo 3. İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü'nden alınan verilerden hareketle yazar tarafından oluşturulmuştur.

KORKUTMA YÖNTEMİ	**KORKUTMA YÖNTEMİ-1** Hesaplarda şüpheli hareket olduğu beyan edilerek kamu görevlisi, polis, vb. gibi sıfatlarla dolandırıcılık	**46**	**%17**	**36**	**%9**
	KORKUTMA YÖNTEMİ-2 İcra takibi yapılacağını bildirerek hukuk büroları çalışanı vb.gibi sıfatlarla dolandırıcılık	**5**	**%2**	**119**	**%29**
	TOPLAM KORKUTMA YÖNTEMİ	**51**	**%19**	**155**	**%38**
YAR. KAM. YÖNTEMİ	**YARDIM KAMPANYALARI YÖNTEMİ** Engelli veya hasta çocuklar için yardım kampanyası adı altında dolandırıcılık	**1**	**%1**	**52**	**%12**

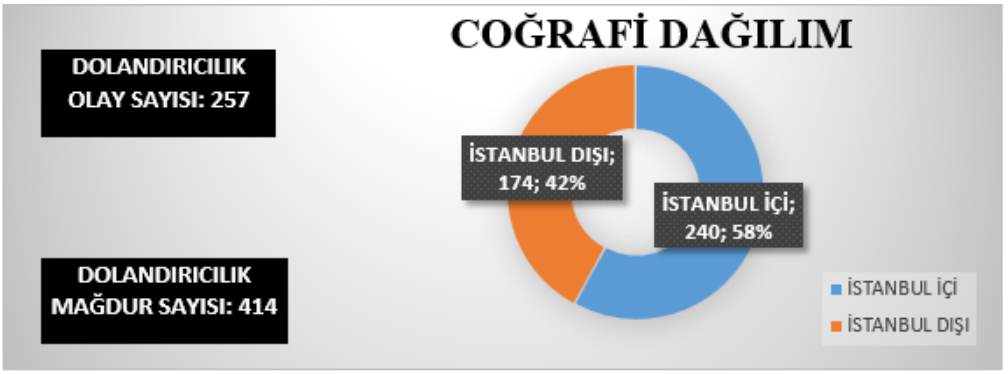
Kaynak: Bu tablo, İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü'nden alınan verilerden hareketle yazar tarafından oluşturulmuştur.

Sahte Çağrı Merkezleri Örgüt Sistematiği

Dolandırıcılık suçunu işlemeye elverişli verilere ve teknolojik donanıma sahip sahte çağrı merkezlerinin kurulmasıyla belirginleşmeye başlayan örgüt şeması; örgüt elamanlarının temini ve bireylerle mobil telefonlarından iletişime geçerek suçu sonuçlandırmaya yönelik eylemleri neticesinde bir bütün olarak şekillenmektedir. Bu metodoloji araştırmanın hipotez olarak belirlediği *Sahte çağrı merkezlerinin belirli bir sistematiği, örgüt şeması bulunmaktadır* hipotezini destekler mahiyettedir. Örgütsel akış şeması dâhilinde *Tablo 1*'de gösterildiği gibi ikna dolandırıcılığı süreci, mağdurların mevduatlarını başka hesaplara aktarılması ya da e-ticaret sitelerinden alışveriş gerçekleştirmek suretiyle sonlanmaktadır.

Sahte çağrı merkezlerinin örgüt üyelerinin mağdurlarla etkili iletişimleri, diyalog kurma metotları ve kandırma kabiliyetleri, ikna yoluyla dolandırıcılık suçunun önemli unsurlarından biridir. Örgüt üyelerinin toplumda bilinen kamu ve özel teşebbüs temsilcisi sıfatıyla, kurumlara özgü diksiyon ve jargonla, kişileri mobil telefonlarından ikna ederek dolandırıcılık faaliyetlerini gerçekleştirdikleri görülmektedir.

Sahte çağrı merkezleri tarafından 01.01.2019 – 01.12.2019 tarihleri arasında, İstanbul'da değişik yöntemlerle gerçekleştirilen ikna yoluyla dolandırıcılık suçlarında toplam olay sayısı 257'dir. Bu olaylarda toplam 414 mağdur bulunmaktadır. Veriler ve olaylarda kullanılan yöntemlere göre mağdur sayısı değişkenlik göstermektedir. *Şekil 4*'de İstanbul merkezli yapılan polis operasyonlarının coğrafik dağılımlarında mağdurların 240'ı İstanbul'un 35 farklı ilçesinde yaşarken, 174 mağdurun da İstanbul'un dışında ikamet ettiği görülmektedir. Esasen bu tasnifin nedeni, örgüt sistematiğidir. Bu bakımdan ağ teknolojileri ve sosyal ortam bilgilerini referans alan ikna yoluyla dolandırıcılık suçunun fiziki sınırları bulunmamaktadır.



Şekil 4. İkna Yoluyla Dolandırıcılık Suçunun Mağdurlara Göre Coğrafik Dağılımı

Kaynak: Bu şekil, İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü'nden alınan verilerden hareketle yazar tarafından oluşturulmuştur.

Tartışma ve Sonuç

İkna; özellikli bilgi, beceri ve stratejiler kullanılarak, önceden planlanan geri dönüşlerin alınması amacıyla yürütülen sistemli çalışmalar bütünüdür. Etkili iletişim yöntemlerinin uygulandığı toplumsal dinamiklere ve psikolojik hassasiyetlere yönelik birçok alanda, ikna olgusunun öne çıktığı görülmektedir. Diğer taraftan iknanın yasal olmayan aldatmaya yönelik faaliyetlerde kullanılması, araştırmanın odaklandığı dolandırıcılık suçunu oluşturmaktadır.

Dijital teknolojilerin toplumsal hayatın her alanında yer almasıyla dolandırıcılık, bir bilişim suçu haline gelmiştir. Bu alanda, çeşitli başlıklarda çalışmalar mevcuttur: VoIP güvenlik açıkları (Keromytis, 2010), phishing saldırıları (Kumar ve Kumar, 2015), siber suçlar (Yetim, 2014), deep web kullanımı (Spalevic ve Ilic, 2017), veri aldatmaları (Ford, 2019) gibi güncel konulu çalışmalar, bilişim sistemleri aracılığıyla dolandırıcılık suçu kapsamında ele alınmaktadır. Dolandırıcılık suçu hakkında alanyazındaki mevcut araştırmalar, gündelik hayatta bırakılan kişisel izlerden ve çeşitli siber tuzaklardan elde edilen verilerin, kötüye kullanılmasına yoğunlaşmaktadır.

İkna ve suç unsurlarının birlikte ele alındığı bu özgün çalışma, elde edilen verilerin örgüt sistematiği içerisinde ve etkili iletişim teknikleri ile dolandırıcılık faaliyetlerinde kullanıldığını ortaya koymaktadır. İkna yoluyla dolandırıcılık olarak kavramsallaştırılan çalışma alanyazınına bir katkı sunarak, mobil telefonlar aracılıyla işlenen dolandırıcılık suçlarına dikkat çekmektedir. Araştırmada; örgütlerin ikna yoluyla dolandırıcılık girişimlerinde kullanmak maksadıyla geliştirdikleri özel bilgilere ulaşma yöntemlerine detaylı yer verilmektedir. Çünkü örgütler çoklu sanal ortamlarda ulaştıkları verilerle, ikna yoluyla dolandırıcılık suçunun işlemektedir.

Doktrinde dolandırıcılık suçunun oluşabilmesi için, mağdurun hileli davranışlarla aldatılmış olması gerekmektedir (Eker ve Zeyrek, 2019, s. 529). Bu açıdan ikna dolandırıcılığı suçunun hazırlık hareketlerinden sonuçlanma aşamasına kadar her aşaması önem arz etmektedir. Ayrıca

bireylerin güvenini kazanmak için örgüt elemanlarının; etkileme, ilgi çekme, benimsetme gibi duygusal ve bilişsel teknikleri kullanmakta olduğu görülmektedir. Bireyler belirtilen stratejileri içeren dolandırıcılık teşebbüsü ile karşılaştıklarında, rasyonel davranarak örgütlerinin tuzaklarından kurtulabileceklerdir.

Çalışmanın temel verileri, 01.01.2019 – 01.12.2019 tarihleri arasında İstanbul merkezli ikna yoluyla dolandırıcılık suçlarının analizlerinden elde edilmiştir. Olay sayılarıyla; mağdurların cinsiyet, öğrenim ve yaş durumları ile bu değişkenlerin birbirleriyle ilişkileri, istatistiksel analize tabi tutulmuştur. Erkek mağdurların, kadınlardan oransal olarak fazla olduğu anlaşılmaktadır. Öğrenim seviyesi yükseldikçe mağduriyet azalmakla birlikte, kamuoyuna yansıdığı gibi her öğrenim seviyesinden ikna yoluyla dolandırıcılığa maruz kalınmaktadır. Yükseköğrenim seviyesindeki bireyler dahi özensizlik, hırs ya da panikle örgütlerce istismar edilebilmektedir. Çalışmada ikna kavramının, dolandırıcılık suçu ile ilişkilendirilme nedenlerinden biri de bu saptamadır. Örgüt elemanlarının yükseköğrenim seviyesinden bireyleri aldatabilmeleri, onların ikna iletişimindeki yeteneklerini göstermektedir. Senaryolarla desteklenen bu hafife alınamayacak iletişim yönetimi hakkında bilgilendirme çalışmalarının yetersiz kaldığı görülmektedir.

Benzer biçimde siber tehlike farkındalıkları ve hâkimiyetleri, 35 yaş altı bireylerde daha yüksektir. Her yaş grubu bu örgütlü suçtan mağdur olabilmektedir. Ancak 35 yaş üzeri bireylerde ikna dolandırıcılığı mağduriyeti %70'i aşmaktadır. Araştırma periyodundaki verilere göre ikna yoluyla dolandırıcılık*; Vaat Yöntemi, Korkutma Yöntemi* ve *Yardım Kampanyaları Yöntemi* şeklinde adlandırılmıştır. Olay ve mağdur sayısı açısından bireyler en yüksek oranda *Vaat Yöntemiyle*, en düşük oranda ise *Yardım Kampanyaları Yöntemiyle* dolandırıcılığa maruz kalmıştır.

Farkındalık oluşturan medya bilgilendirmelerinin etkisiyle, *Korkutma Yöntemi* aynı ölçeklendirmede ikinci sırada gelmektedir. Polis kayıtlarında *Vaat Yöntemi* ile dolandırıcılık mağduriyeti, %50 olarak tespit edilmiştir. *Vaat Yönteminin* oransal yüksekliği, sahte çağrı merkezi örgüt üyelerinin iletişimsel kabiliyetleriyle birlikte, bireylerin verilen sözlere itibar etmelerinden kaynaklanmaktadır. Buna karşın yardım kampanyaları yönteminin oransal düşüklüğü, kamuoyundaki bilinçlenmenin yanı sıra, bireylerin yardım içerikli aramaları görece dikkate almadıklarına işaret etmektedir.

Kişilere ait özel verilerin elde edilmesi, örgüt üyelerinin tespiti, araç-gereç ve teknolojilerin sağlanmasıyla, ikna yoluyla dolandırıcılık faaliyetlerine başlayan sahte çağrı merkezileri, mağdurların mevduatlarını başka hesaplara aktararak eylemlerini sonuçlandırmaktadır. Örgütler, gündemde yer alan olay ve gelişmeler karşısında pozisyon alarak dolandırıcılık kurgularını güncellemektedir. Ancak ikna iletişimi kapsamında örgüt üyelerinin ilgi çeken, korku uyandıran ya da heyecan verici konuşmalarıyla, bireylere hata yaptırma teknikleri değişmemektedir. Bu bakımdan bu makale, başka çalışmalara örnek olabilir ve benzer konularda öncülük yapabilir.

Bu örgütlü, karmaşık ve çok taraflı eylemler hakkında bilinirliliğin sağlanması, çalışmanın temel amacıdır. Bireylerin etkin dinleme yapmamaları, sunulan ödül ve fırsatı kaçırmak istememeleri, menfaat sağlama dürtülerini engelleyememeleri, ikna yoluyla dolandırıcılığın gerçekleşmesine imkan sağlamaktadır. Duyguları suistimal eden bu türden örgütlere

temkinli yaklaşılması, yalnızca mobil telefon tanışıklığı sağlanan kişilere, kurum ve unvanları sorgulanmadan kolaylıkla itibar edilmemesi gerekmektedir. Çünkü suç işlemeye elverişli her türlü bilgiyi referans alan bu eylemlerde, fiziki sınırların bulunmadığı görülmektedir.

İkna yoluyla dolandırıcılık suçundan korunma metotlarına ilişkin, geleneksel ve internet odaklı medyada kamu spotları yayınlanmakta, ilgili bakanlıklar ve kurumlar tarafından mobil telefonlara mesajlar gönderilmektedir. Bu türden suçlara karşı toplumsal bilincin oluşturulması amacıyla yapılan çalışmalara rağmen bu suç, gündemin yoğunlaştığı konularda farklı versiyonları ile işlenmeye devam etmektedir. Bireyler her dijital verinin bir iz bıraktığını düşünerek suçtan korunma yöntemleri geliştirmelidir. Bu bakımdan mobil telefonlarına tanımadıkları bir kaynaktan gelen çağrılara itibar etmemeleri en önemli ön tedbir olacaktır.

Mobil telefon aramalarında kişisel bilgilerin, hesap ve kredi kartı bilgilerinin verilmemesi temel korunma yöntemidir. Vatandaşını korkutarak talepte bulunan bir resmi kurum ya da çalışanın olmadığını unutmamak gerekir. İletişimsel kabiliyetlerle paniğe sevk edici bu çağrılarda, soğukkanlılık korunarak iletişime son verilmeli, dolandırıcıların; kurgunun bir parçası olarak verdiği numaradan değil, bilinen resmi kurum numaralarından, zaman geçirmeksizin gerekli ihbarlar yapılmalıdır.

Ayrıca bilinmeyen sektör ya da kişilerden gelen vaatlerin gerçekleşmesi mümkün değildir. İkna yolunu kullanan dolandırıcıların iletişimsel becerilerle, anlık akıl tutulmalarını hedefledikleri düşünülerek, en doğru davranış biçimi bu çağrılara ehemmiyet vermemektir. Bu kapsamda doğal hayatın akışı içerisinde bireylerin sevinç, üzüntü ve duygusal durumlarının istismarına yönelik dikkat edilmesi gereken çağrılardan biri de yardım kampanyalarının bahane edilmesidir. Teyide muhtaç bir konuda yapılan yardımın yerine ulaşmayacağı değerlendirilerek bu çağrılara önem verilmemesi, ikna yoluyla yapılacak dolandırıcılığın gerçekleşmesini önlemektedir.

İkna yoluyla dolandırıcılığa maruz kalmamak için, internet odaklı ortamlarda bireysel korunma yöntemleri geliştirilmelidir. Korunma, dijital mecralardan ve sosyal medya platformlarından uzak kalma değildir. Hiç şüphesiz yarın, bugünden daha fazla bilişim teknolojileri kullanılacaktır. Makalede örgütlerin bu ortamlardan beslendiği gerçeğinden hareketle, dijital mecraların dikkatli kullanılması, ikna yoluyla dolandırıcılık suçlarına karşı tutum geliştirilmesi tavsiye edilmektedir. Korunma tedbirlerine rağmen iletişim sağlanması halinde zarar görmemek için, bilinmeyen numara ve tanınmayan kaynaktan gelen çağrılara temkinli yaklaşılmalı, şüphe halinde iletişime derhal son verilmelidir.

İletişim alanında yapılan çalışmalar, kuramsal bilgi birikiminin yanı sıra, özellikle gündelik hayat pratiklerine yönelik güncel araştırmalarla elde edilecek verilerle desteklenmeye ve güçlendirilmeye ihtiyaç duymaktadır. İkna yoluyla dolandırıcılık suçu, gerçekleştirme metotları açısından hukuksal, toplumdaki izdüşümleri nedeniyle sosyolojik ve etkileşim süreçleri bakımından iletişim bilimlerinin ortak sorunsalı olarak karşımıza çıkmaktadır. Bu bakımdan iletişim dinamikleri ile suç olgusu arasındaki yakın ilişkiye dikkat çeken bu özgün çalışmanın, ikna ve suç olgusuna ilişkin interdisipliner araştırmalara ve uygulamalara bir katkı sağlayacağı değerlendirilmektedir.

Son Notlar

1 – Çalışmada kullanılan bilgiler, etik ilkeler çerçevesinde, özel izinle İstanbul Emniyet Müdürlüğü'nden edinilmiştir.

2 – İkna dolandırıcılığına ilişkin tablo ve şekiller, Siber Suçlarla Mücadele Şube Müdürlüğü'nden alınan istatistiksel verilerden yararlanarak oluşturulmuştur.

Kaynaklar

Akpınar, G. ve Akpınar, K. (2017). İkna edici iletişimde kaynak. *Sosyal ve Beşeri Bilimler Araştırmaları, 2017. 12*(01),103-108

Aristoteles. (2004). *Retorik.* Mehmet H. Doğan. (Çev.) İstanbul: Yapı Kredi Yayınları.

Arklan, Ü ve Kartal. N. (2018). İkna edici iletişim tekniği olarak tek yanlı ve iki yanlı sunumun kriz yönetimi sürecine etkisi. *Süleyman Demirel Üniversitesi Vizyoner Dergisi, 9*(20), 39-52.

Atkins, B. ve Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences*, *1*(03), 23-32.

Bahar, C. (2018). *Etkili iletişim ve ikna.* Ankara*:* Tutku Yayınevi

Brody, R. G., Mulig, E. ve Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting & Financial Studies Journal, 11*(3),43-56.

Button, M. ve Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.

Cantürk, G. ve Cantürk, N. (2004). Suçlu profili. *Adli Tıp Dergisi, Journal of Forensic Medicine*, *18*(2), 27-37.

Coşkun, A. (2014). *İbn Sînâ Felsefesinde Retorik*. İstanbul: Litera Yayıncılık.

Demirtaş, H. A. (2004). Temel ikna teknikleri: Tutum oluşturma ve tutum değiştirme süreçlerindeki etkilerinin altında yatan nedenler üzerine bir derleme. *Gazi Üniversitesi İletişim Fakültesi Dergisi*, *19*(3),73-91.

Dursun, İ. ve Tümer Kabadayı, E. (2012). Tüketicilerin ikna çabalarına karşı gösterdikleri direnç: Tutum gücü, tutum yönü ve mesaj gücünün etkileri üzerine deneysel bir araştırma. *Uluslararası Yönetim İktisat ve İşletme Dergisi*, *8*(16), 75-97.

Doruk, E. K.(2015). *İknanın sosyal psikolojisi.* İstanbul: Derin Yayınları.

Eker B. ve Zeyrek.(2019). TCK'da dolandırıcılık suçu. D.E.Ü. Hukuk Fakültesi Dergisi, Özel Sayı, *C.21,* 517-583

Esgin, Y.(2018). *İkna teknolojileri.* İstanbul: Çizgi Kitabevi.

Fette, I., Sadeh, N. ve Tomasic, A. (2007). Learning to detect phishing emails. In *Proceedings of the 16th International Conference on World Wide Web* (649-656). ACM.

Ford, R. A. (2019). Data scams. University of Chicago and Northwestern University Hous. L. Rev., *11*(57), 111-183

Hoffstadt, D., Rathgeb, E., Liebig, M., Meister, R., Rebahi, Y. ve Thanh, T. Q. (2014). A comprehensive framework for detecting and preventing VoIP fraud and misuse. In *2014 International Conference on Computing, Networking and Communications (ICNC)* (807-813). IEEE.

Holt, T. J. ve Graves, D. C. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology*, *1*(1), 137-154.

"İkna" (t.y.). *Türk Dil Kurumu,* 19.03.2020 tarihinde https://sozluk.gov.tr/?kelime= adresinden edinilmiştir.

İplikçi, H. G. (2015). Reklamlarda tüketiciyi ikna etmek için kullanılan stratejiler ve reklam örnekleri. *Sosyal ve Beşeri Bilimler Dergisi*, *7*(1), 65-77.

Kağıtçıbaşı, Ç ve Cemalcılar, Z. (2014). *Dünden bugüne insan ve insanlar sosyal psikolojiye giriş.* İstanbul: Evrim Yayınevi.

Karadeniz, M. (2010). *Halkla ilişkiler faaliyetlerinin rolü ve önemi.* İstanbul: Beta Yayıncılık.

Keromytis, A. D. (2010). A look at VoIP vulnerabilities. New York: Columbia University Press

Kirda, E. ve Kruegel, C. (2006). Protecting users against phishing attacks. *The Computer Journal*, *49*(5), 554-561.

Kumar, V. ve Kumar, R. (2015, April). Detection of phishing attack using visual cryptography in ad hoc network. In 2015 International Conference on Communications and Signal Processing (ICCSP) (pp. 1021-1025). IEEE.

Kumkale, G. T. ve Albarracin, D. (2004). The sleeper effect in persuasion: A meta-analysis. *Psychological Bulletin, 130*(1), 143-172.

Kurudayıoğlu, M. ve Yılmaz, E. (2014). How are we persuaded? Persuasive text and structure/Nasıl ikna ediliyoruz? İkna edici metin ve yapısı. *Eğitimde Kuram ve Uygulama*, *10*(1), 75-102.

Naksawat, C., Akkakoson, S. ve Loi, C. K. (2016). Persuasion strategies: Use of negative forces in scam e-mails. *GEMA Online® Journal of Language Studies*, *16*(1), 1-17

Norris, G., Brookes, A. ve Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*(3), 231-245.

Oinas, K. ve Harjumaa, M. (2008). Towards deeper understanding of persuasion in software and information systems. In *First International Conference on Advances in Computer-Human Interaction* (s. 200-205). IEEE.

Peltekoğlu, F.B. (2012). Sosyal medya sosyal değişim. T. Kara ve E. Özgen. (Ed.) *Sosyal medya /akdemi*. (s. 3-8). İstanbul: Beta Yayıncılık.

Petty, R., Ostrom, T. M. ve Brock, T. C. (2014). *Cognitive responses in persuasion*. NewYork: Psychology Press.

Rudesill, D. S., Caverlee, J. ve Sui, D. (2015). The deep web and the darknet: A look inside the internet's massive black box. *Woodrow Wilson International Center for Scholars, STIP*, *3*.

Spalevic, Z. ve Ilic, M. (2017). The use of dark web for the purpose of illegal activity spreading. *Ekonomika, Journal for Economic Theory and Practice and Social Issues*, *63(*1350-2019-2771), 73-82.

Spitzner, L. (2003). Honeypots: Catching the insider threat. In *19th Annual Computer Security Applications Conference* .(170-179). IEEE.

"Türk Ceza Kanunu". (2004, 12 Ekim). *Resmi Gazete* (Sayı:25611). 09.06.2019 tarihinde https://www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm adresinden edinilmiştir.

Uztuğ, F. (2012). İkna edici iletişim kampanyalarında pazarlama ve iletişim hedefleri. *İstanbul Üniversitesi İletişim Fakültesi Dergisi*, *8*(3), 1-17.

Ünver, M., Canbay, C. ve Mirzaoğlu, A. G. (2018). *Siber güvenliğin sağlanması: Türkiye'deki mevcut durum ve alınması gereken tedbirler.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Yetim, S. (2014). Siber suçlar, yargılama yetkisi ve yeni bir model önerisi. Yazım ve yayım kuralları, Türkiye Adalet Akademisi Dergisi *17*(2), 177-231

Yıldırım, G. (2018). *İkna odaklı halkla ilişkiler Yazarlığı.* İstanbul: Beta Yayıncılık.

Yüksel, A.H. (1994). *İknanın psikolojik, toplumsal ve mantıksal boyutları*. M. Oyman (Ed.) İkna Edici İletişim. (1-41) Eskişehir: Anadolu Üniversitesi Açık Öğretim Fakültesi Yayınları.

Fraud by Persuasion: A Research on Determination of Persuasion and Effective Communication Methods in Fraud Activities

Atalay BAHAR*

Persuasion involves activities for adopting expected behavior models. (Esgin, 2018, p. 28). Ece Karadoğan Doruk (2015) sees persuasion as an act of persuasion and Handan Güler İplikçi (2015) as a guiding strategy. In the study entitled "Rhetoric" based on observations, persuasion is expressed as "the ability to observe the believable ways available in a particular situation" (Aristoteles, 2004, p. 2). İbn Sînâ deals with persuasion under three headings as basic expressions, skills and auxiliary elements (Coşkun, 2014, pp. 46-67). The first experimental study on persuasion was made by Carl Hovland et al. in 1949, and theories were developed to explain behavioral processes in the following years (Demirtaş, 2004; Dursun & Tümer, 2012). Attention was drawn to the close relationship of communication and persuasion. (Karadeniz, 2010, p. 35).

The close relationship between communication and persuasion has been revealed. (Karadeniz, 2010; Kurudayıoğlu & Yılmaz, 2014). Naksawat, Akkakoson and Loi (2016), also point out that communication power directly affects persuasion processes and Ferruh Uztuğ (2012), considers it as activities aimed at internalizing ideas. Çiğdem Kağıtçıbaşı and Zeynep Cemalcılar (2014), treat persuasion as the basic motives that guide behavior, while Tarcan Kumkale and Dolores Albarracin (2004), show that individuals are convinced over time, even though they contain a negative message.

In this study, the function of persuasion phenomenon in fraud activities is discussed. These illegal actions are defined of "persuasion fraud", while effective communication methods are met with the concept of "persuasion communication". It mainly focuses on the systematic of persuasion fraud, the use of communicative paradigms in deception processes and their social effects.

* PhD, Deputy Police Chief, Istanbul Police Department, İstanbul, Turkey, atk199@hotmail.com

Received Date: 13.01.2020
Accepted Date: 23.03.2020

The prevalence of smartphones and portable devices that allow instant sharing plays an important role in individuals' desired responses (Oinas and Harjumaa, 2008, p. 200). Various online attack methods are used. (Brody, Mulig and Kimball, 2007, p. 45).This study, which uses categorical content analysis technique is a descriptive field research. Persuasion fraud consists of the process of identifying the psychological weaknesses of the individuals who receive calls from mobile phones by the members of the Fake Call Centers organization with effective communication skills, accessing their personal information, taking the predicted responses and using them for self-interest purposes. The process of persuasion fraud consists of preparation movements of the crime, execution of the crime and conclusion of the crime. During the preparation phase, Voice Over Internet Protocol (VoIP) technology is used to enable voice calls on the basis of anonymity and confidentiality.

As Richard Petty, Thomas Ostrom and Timothy Brock (2014) point out, special jargon and terminology are brought to the fore with a strong scenario and corporate profile, which does not suspect individuals (p. 6). In the communication provided by the organization with the VoIP system, individuals who think that they are called from real sectors become vulnerable to fraud. (Hoffstadt, Rathgeb, Liebig, Meister, Rebahi & Thanh, 2014, s.807).

The provision of appropriate data is a prerequisite for persuasion fraud in preparation for the demonstration of desired behavior and exploitation of individuals weaknesses (Atkins & Huang, 2013, s.23). Necessary data is provided from the sectoral mole, which is placed in various units by insider code, from the dark net where illegal content exists by organizations. (Spitzner, 2003; Rudesill, Caverlee ve Sui, 2015). There are studies on various topics in this area: VoIP vulnerabilities (Keromytis, 2010), phishing attacks (Kumar, 2015), cybercrime (Yetim, 2014), deep web usage (Spalevic and Ilic, 2017), data deceptions (Ford, 2019 Current topics such as) are dealt with within the scope of fraud by means of information systems. Traces left on phishing sites in multiple virtual environments by online transactions are collected by phisingists and trackers and are a source of persuasion fraud (Kirda ve Kruegel, 2006, s. 560). With the communication provided by VoIP system by the organization, the execution of the crime begins.

In the final stage, individuals are asked to key in the password that comes to their mobile phone to end the transaction. Individuals are believed that calls come from reliable sources (Fette, Sadeh and Tomasic, 2007; Yıldırım 2018).By dialing the password, you are instructed to pay or transfer without notice. Fraud networks, which follow the agenda very well, use popular information according to the conditions of the day, making individuals the target of fraudulent actions (Button and Cross. 2017 p. 26). By using the accounts determined during the preparatory phase, the amounts found in the deposits of the victims are made to the accounts of third parties via eft / money order, and the persuasion fraud is completely completed.

The main data of the study are obtained from the analyzes of the conviction fraud crimes based on Istanbul between 01.01.2019 – 01.12.2019. According to the classification of Geberth in Cantürk and Cantürk (2004) titled Criminal Profile, in the Features Achievable with Criminal Personality Profile section; 3 out of 22 characteristics are age, gender and education. The number

of incidents and the gender, education and age of the victims were evaluated using statistical data. In terms of the number of victims and incidents, it is seen that individuals are exposed to fraud at the highest rate by Promise Method and at the lowest rate by Aid Campaign Method. With the effect of awareness-raising information, the Intimidation Method comes second in the same scaling.

There are various and limited number of studies in the literature on the theme of persuasion, communication, persuasion and fraud, persuasion and fraud types. In Cengiz Bahar's (2108) Effective Communication and Persuasion and Arklan and Kartal's (2018) Persuasive Communication Technique, the effect of unilateral and bilateral presentation on Crisis Management Process is dealt with. On the other hand, Gönül Akpınar and Kadir Akpınar (2017) emphasize the communication power of the resource in his work titled Persuasive Communication. In the studies titled Qualitative Analysis of Advance Fee Fraud E-mail Schemes by Thomas J. Holt and Danielle C. Graves (2007), fraud is addressed through e-mails that are among the forms of fraud experienced by people in the social field. In addition, the work of The Psychology of Internet Fraud Victimisation: A Systematic Review, which provides a systematic view of Gareth Norris, Alexandra Brookes and David Dowell (2019), provides an integrated view of the subject.

Although there are studies in the literature covered under the titles of persuasion and fraud; A study conceptualized under the name of fraud by persuasion has not yet been encountered. The original value of this study emerges at this point and the purpose of the study; contributes to this limited number of literature.

Despite the efforts to create social awareness against these kinds of crimes, this crime continues to be processed with different versions of the agenda. It is within the overall design of the study that such organizations that abuse emotions should be approached cautiously, and that only those with whom mobile phone acquaintance is provided should not be easily recognized without questioning their institutions and titles. It should not be forgotten that there is no official institution or employee making a request frightening its citizens. In order not to be harmed in case of communication despite the protection measures, calls from unknown numbers and unrecognized sources should be approached cautiously, and in case of doubt, communication should be stopped immediately.

Keywords: Fraud by Persuasion, Persuasion Communication, Effective Communication Methods, Fake Call Center, VoIP Technology