



ISSN: 1306-3111/1308-7444
NWSA-Social Sciences
NWSA ID: 2013.8.3.3C0111

Status : Original Study
Received: January 2013
Accepted: July 2013

E-Journal of New World Sciences Academy

Ahsen Kaya

Ege University Department of Forensic Medicine, Izmir-Turkey

Umut Erdar Bilgin

Bergama State Hospital, umuterdarbilgin@hotmail.com, Izmir-Turkey

Abdullah Mollaoğlu

Izmir Public Security Directorate, okaygisiz26@hotmail.com,
Izmir-Turkey

Aytaç Koçak

Ekin Özgür Aktaş

Ege University Department of Forensic Medicine, Izmir-Turkey

<http://dx.doi.org/10.12739/NWSA.2013.8.3.3C0111>

**TÜRKİYE GENELİNDE BİLİŞİM YOLU İLE İŞLENEN
DOLANDIRICILIK SUÇU: 16 OLGU**

ÖZET

Teknoloji alanında yaşanan gelişmeler hayatımızı kolaylaştırmakla birlikte, bu teknolojik gelişmeler aynı zamanda farklı problemleri ve suç tiplerini de beraberinde getirmektedir. Dolandırıcılık suçu, kamu düzenine karşı işlenen suçlardan biridir. Bu çalışmada, bir suç örgütü tarafından Türkiye'nin farklı illerinde yaşayan 16 kişiye karşı gerçekleştirilmiş bilişim yoluyla işlenen dolandırıcılık suçu sunulmuş olup, bu olgular üzerinden bilişim yoluyla işlenen suçlarda alınabilecek önlemler vurgulanmaya çalışılmıştır. Bilişim yoluyla işlenen suçlar her geçen gün artmaktadır. Bu nedenle oluşabilecek zararların azaltılması için yasal önlemler alınmalı, kurumlar arası işbirliği sağlanmalı, toplumsal bilinçlendirme ihmal edilmemelidir.

Anahtar Kelimeler: Kamu Düzenine Karşı Suçlar, Dolandırıcılık Suçu, Bilişim Suçu, Cep Telefonu, Teknoloji

**FRAUDS BY INFORMATICS COMMITTED THROUGH AN ORGANIZATION IN DIFFERENT
COUNTRIES OF TURKEY: 16 CASES**

ABSTRACT

Although technological advances facilitate our lives, these technological advances bring with the different problems and crime types. Fraud crimes are one of the crimes against public order. Cases of 16 frauds by informatics, which are committed through an organization in different countries of Turkey, were given in this study. It was wanted to emphasize basically which precautions could be taken for the prevention of the crimes committed by informatics. Crimes committed by informatics are increasing with each passing day. In this regard, for decreasing the harms which are the cause of these crimes, legal precautions should be taken, as well as inter-agency cooperation should be provided, should not be neglected in the subject of public awareness.

Keywords: Crimes Against Public Order, Fraud, Informatics, Mobile Phone, Technology

1. GİRİŞ (INTRODUCTION)

Bilimin ilerlemesi ve buna bağlı olarak teknolojinin gelişmesiyle hayatımız kolaylaşmış olmakla birlikte, gelişen teknolojinin hızına ayak uydurmak hem kişisel olarak, hem de kurumlar düzeyinde zorlaşmıştır. Bu durum, uygulamada çeşitli zorluklara, bazen hak kayıplarına ve bazen de teknolojik imkanlar kullanılarak işlenen suçların mağduru olmaya sebep olmaktadır.

Teknolojideki gelişmeler her alanda etkisini göstermiş olup, haberleşme alanında da büyük ilerlemeler kaydedilmiştir. Türkiye’de 1960-70’li yıllarda sabit telefon bağlatmak o kadar zorken, sabit telefon bağlatmak için “telefona yazılmak” diye bir kavram söz konusu iken ve yine eve telefon bağlansın diye oldukça yüklü miktarda paralarla birkaç yıl sıra beklenirken, günümüzde artık sabit telefon kullanımı yerini internet bağlantılı cep telefonlarına, internet üzerinden hem sesli, hem de görüntülü görüşme olanaklarına bırakmıştır.

Teknolojinin haberleşme alanındaki kullanımı uzakları yakın etmiş, sevdiklerimizle istediğimiz her an iletişim halinde olmamızı, iş hayatında işlerin daha hızlı ve kolay bir şekilde çözülmesini sağlamıştır. Ancak, teknolojideki bu gelişmeler farklı suç türlerini ve daha önceki suç türlerinde teknolojinin getirdiklerinden yararlanmayı ön plana çıkarmış olup, kontrol edilmesi güç sorunları da beraberinde getirmiştir [1,2]. Neticede, “bilişim suçları” kavramı ve “bilişim yolu ile işlenen suçlar” kavramı ortaya çıkmıştır. Bilginin, programların, servislerin, ekipmanların veya haberleşme ağlarının yıkımı, hırsızlığı, yasadışı kullanımı, değiştirilmesi veya kopyalanması, “bilişim suçları” olarak tanımlanırken, bu sistemlerin sadece araç olarak kullanıldığı, geleneksel suçlar olarak tabir edilen tipleri de “bilişim sistemleri aracılığı ile işlenen suçlar” olarak isimlendirilmektedir [3]. Bu bağlamda, hırsızlık, dolandırıcılık, tehdit, hakaret, kişisel verileri yayma ve özel hayatın gizliliğini ihlal gibi asayiş suçları da bilişim sistemleri aracılığı ile işlenen suçlar arasında yer almaktadır.

2. ÇALIŞMANIN ÖNEMİ (RESEARCH SIGNIFICANCE)

Bu çalışmada; Türkiye genelinde bir örgüt aracılığıyla bilişim yoluyla işlenen 16 dolandırıcılık suçu örneği verilerek, bilişim yolu ile işlenen dolandırıcılık suçu özellikleri üzerinden, Türkiye’de bilişim suçlarının önlenmesi için temelde alınması gereken tedbirler vurgulanmak istenmiştir. Ayrıca işlenen bilişim suçu bilimsel ortamda sunulurken, farkındalığın artırılması amaçlanmıştır.

3. BULGULAR (FINDINGS)

2012 yılı içerisinde 16 kişiyi (savcı ve polis unvanlarını kullanarak ve banka aracı yapılarak) iletişim yoluyla dolandıran bir örgüt tespit edilmiştir.

Eylemlerle ilgili olarak faillerin dördünün kimliği tespit edilmiş ancak iki farklı telefon numarasını kullanan diğer kişi ya da kişilerin açık kimlikleri tespit edilememiştir. Açık kimliği tespit edilen faillerin olay tarihi itibarıyla 3’ünün 20’li yaşlarda, birinin 40 yaşında olduğu belirlenmiştir.

Olay tarihinde mağdurların en küçüğü 37, en büyüğü ise 62 yaşında olup, yaş ortalaması 53±9.9’dur. Faillerin mağdurlarını, çeşitli illerin İl Özel İdarelerinden, Orman Bölge Müdürlüklerinden ve TCDD çalışanlarından seçtiği, 1 mağdurun da Çocuk Büro Amirliği’nde çalışan komiser yardımcısı olduğu görülmüştür. Mağdurların 10’unun idareci, 6’sının memur konumundaki kişilerden oluştuğu belirlenmiştir.

Çalışmaya konu olan suçların 14'ü dolandırıcılığa teşebbüs, 2'si ise dolandırıcılık suçu niteliğindedir. Bilişim yoluyla işlenen dolandırıcılık ya da dolandırıcılığa teşebbüs eylemlerinin özellikleri Tablo 1'de verilmiştir.

Tablo 1. Bilişim Yoluyla İşlenen Dolandırıcılık/Dolandırıcılığa Teşebbüs Suçlarının Özellikleri
(Table 1. The features of fraud by informatics or attempt to fraud by informatics)

Suç Tarihleri	02-18 Ağustos 2012
Suçun Yeri (Mağdur Sayısı)	Denizli (2), Elazığ (2), Hakkari (1), İzmir (2), Kastamonu (3), Samsun (2), Şırnak (1), Tekirdağ (2), Zonguldak (1)
Suçun Niteliği	Örgüt Kurarak Bilişim Yoluyla Dolandırıcılık ve Dolandırıcılığa Teşebbüs
Toplam Fail Sayısı	Kimliği belirlenen 4 kişi
Bir Olaydaki Fail Sayısı	En az 2
Faillerin Kullandıkları Unvanlar	Komiser ve Cumhuriyet Savcısı
Bilişim Aracı	Cep Telefonu
Eylemin Şekli	Mağdurlara, "bir suç şebekesinin kredi kartına girerek para çektiği, kişilerin tespit edildiği ve yakalanmaları için yardımcı olmasının gerektiği, operasyonun gizli olduğu, bu nedenle kimseye bir şey söylenmemesi ve telefonun sürekli açık tutulması gerektiği, Adliyeye giderek nöbetçi Cumhuriyet Savcısıyla görüşmesi gerektiği" söylenmiştir. Bu arada 2. fail adliye girişindeki polis memurunu arayarak, kendisini savcı olarak tanıtmıştır. 1. failin telefonda görüştüğü mağdurun adını söyleyerek, bu kişinin yakını olduğunu ve adliyeye geleceğini, ancak kendisinin adliyede olamayacağı için .. nolu telefondan kendisine bilgi verilmesini istediği tespit edilmiştir. Mağdurun adliye gelmesi üzerine, polis memuru belirtilen numaradan kendisini savcı olarak tanıtan kişiyi arayarak, telefonu mağdura vermiştir. Mağdur kendisini savcı olarak tanıtan kişiyle konuşmuş ve 2. fail kendisinden en yakın ... bankasından TL kredi çekmesini ve talimat beklemesini istemiştir.

4. TARTIŞMA VE SONUÇ (DISCUSSION AND CONCLUSION)

Bilişim suçu türleri teknolojinin suç aracı olarak kullanılmasına paralel olarak artış göstermektedir [3-5]. Bu artış sadece suçun türü açısından söz konusu olmayıp, sayısal olarak da bilişim suçlarında ve bilişim yoluyla işlenen asayiş suçlarında söz konusudur [5].

Asayiş suçları arasında yer alan dolandırıcılık suçunun, insanlık tarihi kadar eski olduğu belirtilmektedir [6]. Dolandırıcılık suçu, ekonomik suç türleri başlığı altında incelenmekte olup, 5237 sayılı Türk Ceza Kanunu'nun (TCK) 157. maddesinde "Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamak" şeklinde tanımlanmıştır ve TCK'nın 158. maddesinde dolandırıcılık suçunun nitelikli halleri belirlenmiştir [7,8]. TCK'nın 158. maddesinin 1/f bendinde ise, bilişim yoluyla işlenen dolandırıcılık suçuna yer verilmiştir ve suçun telefon, bilgisayar gibi bilişim araçları ile işlenmesi ağırlaştırıcı sebep olarak değerlendirilmiştir [7].



Dolandırıcılık suçunu işleyenlerin genel özelliklerini belirten çalışmalar yapılmıştır [8]. Sunulan çalışmada da; faillerin bir takım özellikleri belirlenmiş olup, çalışmadaki faillerin yaşının ve cinsiyet özelliğinin yapılan çalışma ile benzer olduğu tespit edilmiştir. Bilişim yolu ile işlenen suçlarda fail ve mağdur profilleri ile suç profillerinin çıkarılmasının, eylemlerin çözümünü kolaylaştıracağı düşünülmüştür. Her kesimden kişiler mağdur olabilmekte olup, bu çalışmadaki mağdurların daha çok idareci konumundaki kişilerden oluştuğu belirlenmiştir. Mağdurların ayrıca belli kamu kurumlarından seçilmiş olduğu saptanmıştır. Bu durum, bilişim suçları ile mücadele için emniyet güçlerinin yanında; kamu ve özel kurum ve kuruluşların işbirliği içerisinde olması ve kurumlar düzeyinde de önlemlerin alınması gerekliliğini göstermektedir.

2010 yılında Adana'da yapılan bir yüksek lisans tezinde 2006-2009 yılları arasında meydana gelen bilişim suçları değerlendirilmiş ve internet üzerinden işlenen suçların ilk sırasında dolandırıcılık suçu tespit edilmiştir [9]. Bilişim yolu ile işlenen dolandırıcılık suçunda da en sık kullanılan yöntemlerden birisi bankaların aracı kılınması durumudur [9]. Bu çalışmada da, bankaların aracı kılındığı tespit edilmiştir. Bankaların bilişim yoluyla işlenen suçların önlenmesinde en önemli basamaklardan birini oluşturduğu göz ardı edilmemelidir. Konunun, bilişim uzmanları tarafından bankalar düzeyinde ele alınarak, yeni ve etkili güvenlik tedbirlerinin ortaya konulmasına ihtiyaç olduğu düşünülmektedir.

Suçun işlenmesi sırasında unvan kullanımının sık olduğu bilinmektedir. Bu çalışmada da komiser ve Cumhuriyet Savcısı unvanlarının kullanıldığı görülmüştür. Emniyet güçleri tarafından zaman zaman bu kapsamda bilgilendirme mesajları cep telefonlarına gönderilmektedir. Halkın bilgilendirilmesi amacıyla gönderilen bu mesajlarda "adınıza çok sayıda hat çıkarılmış ve terör örgütü tarafından kullanılıyor" ya da "banka hesaplarınıza giriliyor, biz bu şahısları tespit etmeye çalışıyoruz" gibi ikna edici cümlelerin yanı sıra, "Operasyonun gizliliği var, kimsenin duymaması gerekiyor, herhangi bir şahsa söylerseniz, olayı deşifre ederseniz gözaltına alınırsınız" şeklinde insanları tehdit eden korku ve panik uyandıran ifadelerle inanılmaması yönünde uyarılar yapılmaktadır. Bilişim yoluyla işlenen suçlar açısından mail, mesaj, radyo ve televizyonlarda, kamu spotları ile kamuya açık alanlarda afiş, poster vs. ile halkın bilinçlendirilmesi özellikle önem taşımaktadır. Bununla birlikte, bilinçlendirme sadece dolandırıcılık kapsamında düşünülmemelidir. Bilişim yolu ile işlenebilecek her türlü suçta bu uygulamanın yaygınlaştırılmasına çalışılmalıdır. Örneğin; çocuğun cinsel istismar suçunda olduğu gibi sonuçları diğer suçlara göre daha ağır olan bazı suçlarda riskli grupların ayrıca ele alınarak bilgilendirilmelerine özen gösterilmesi gerekmektedir. Bunun haricinde diğer yasal eksikliklerin giderilmesi gerekmektedir. Türkiye 2010 yılında Siber Suçlar Sözleşmesi'ne imza atmış olmasına rağmen günümüzde halen bu sözleşmeye uygun ek düzenlemeler yapılmamıştır ya da tamamlanmamıştır.

Günümüzde her köşe başında neredeyse sorgusuz sualsiz bir şekilde, cep telefonu hattı satışının olmasının telefon aracılığı ile işlenen suçlarda artışa sebep olduğu düşünülmektedir. Bazen kişilerden habersiz adlarına hatlar açılabilir. Bunu önlemek için, Bilgi Teknolojileri İletişim Kurumu tarafından "Mobil Hat Sorgulama Sistemi" oluşturulmuştur. Kişiler internet üzerinden <http://hat-sorgulama.btk.gov.tr> adresine girerek kendi üzerlerine kaç tane hat açıldığını öğrenme imkanına sahiplerdir. Kişi adına habersiz hat açılması durumunda açılan hat hangi GSM şirketine ait ise o şirketin ortak sorumluluk altına gireceği belirtilerek caydırıcı önlemler

alınmaya çalışılmaktadır.

Bilişim aracı olarak cep telefonları yanında bilgisayarlar da suçun işlenmesinde önemli araçlardan biridir. İnternet ortamında kişilerin neredeyse tüm kişisel bilgilerini paylaştıkları sosyal iletişim ağlarına üyelik işlemlerinin daha kontrollü olmasının suç işlenmesini zorlaştıracacağı düşünülmüştür. Bu konuda özellikle ebeveynlerin çocukları üzerindeki kontrolleri büyük önem taşımaktadır. Bu tür iletişim araçları masum araçlar olarak görülmemelidir.

Sonuç olarak, bilişim yoluyla dolandırıcılık gibi asayiş suçları işlenmekte olup, asayiş suçları dışındaki diğer suçlarda da (örneğin, adli tıbbi uygulamada adli olguların önemli bir kısmını oluşturan cinsel istismar ve cinsel saldırı olgularında) bilişim araçlarının kullanımının arttığını görmekteyiz. Bu nedenle, gerekli önlemlerin alınması için bilimsel çalışmalar genişletilmeli, suç profilleri çıkarılmalıdır. Bu konuda hem yasal önlemler alınmalı, hem kurumlar arası işbirliği sağlanmalı, hem de halkın bilinçlendirilmesi konusu ihmal edilmemelidir.

TEŞEKKÜR (ACKNOWLEDGEMENT)

İzmir Cumhuriyet Başsavcılığı'na ve İzmir Emniyet Müdürlüğü Asayiş Şube Müdürlüğü Yankesicilik ve Dolandırıcılık Büro Amirliği'ne çalışmada sunulan olgularla ilgili verdikleri izin ve bilgiler için çalışmayı hazırlayan yazarlar olarak teşekkürü bir borç biliriz.

NOT (NOTICE)

Bu çalışma, 20-21 Mayıs 2013 tarihleri arasında Elazığ Fırat Üniversitesinde yapılan 1.Uluslararası Adli Bilişim ve Güvenlik Sempozyumunda sözlü sunum olarak sunulan çalışmanın hakemlik sürecinden geçirilmiş ve yeniden yapılandırılmış halidir.

KAYNAKLAR (REFERENCES)

1. Değirmenci, O., (2003). Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi. Legal Hukuk Dergisi, Volume: 11, ss.2750.
2. Çakır, H. ve Sert, E., (2011). Bilişim Suçları ve Delillendirme Süreci. II. Uluslararası Terörizm ve Sınırtaş Suçlar Sempozyumu (UTSAS 2010). Antalya, Bildiriler Kitabı, ss:143-171.
3. Perry, R.L., (1986). Computer Crime, New York, Franklin Watts.
4. Tanrıkulu, C. ve ark., (2007). Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu. TBD Kamu-BİB Kamu Bilişim Platformu IX. Antalya.
5. Dijle, H. ve Doğan, N., (2011). Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı. Bilişim Teknolojileri Dergisi, Volume:4, Number:2, ss: 43-53.
6. Hafızoğulları, Z., (2011). Türk Ceza Hukukunda Dolandırıcılık Suçları. Ankara, Ankara Üniversitesi Basımevi, ss: 405-440.
7. Türk Ceza Kanunu. Kanun Numarası: 5237, Kabul Tarihi:12.10.2004, Yayımlandığı Resmi Gazete Tarihi: 01.06.2005, Yayımlandığı Resmi Gazete Sayısı: 25611.
8. Çetin, B. ve Budak, S., (2011). İcra ve İflas Kanunu'na Muhalefet ve Dolandırıcılık Suçları (1997-2007). KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi, Volume:13, Number:21, ss. 95-102.
9. Atalığ Taş, K., (2010). Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi. Yüksek Lisans Tezi. Adana: Çukurova Üniversitesi Sağlık Bilimleri Enstitüsü.