ELEKTRONİK PAZARLARLARDA GÜVEN PROBLEMİ VE KRİMİNAL FAALİYETLER

Ramazan AKSOY[1], Hanifi SEVER[2]

Özet

Güven, internet ticaretinde oldukça önemli bir konudur ve özellikle önemli kararlar hakkındaki sosyal davranışın bir önkoşuludur. Genellikle internet ticaretinin tehlikeli olduğu ve müşterilerin kişisel bilgilerini, kredi kartlarının bilgilerini ve diğer varlıklarını tehlikeye attıkları sıklıkla ifade edilmektedir. Öte yandan, internet ticaretinin kullanımının arttırılması için çok sayıda proje ve uygulama vardır. İnternet kullanıcılarının sayısı gün geçtikçe artmaktadır ancak çoğu, internet üzerinden ticarete güvenmediği için Web sitelerine kişisel bilgilerini paylaşmaya gönülsüz olmaktadırlar. Bu çalışmada, ziyaretçilerin Web sitelerine olan güven duygusunun arttırılması için kullanılan anahtar elementlerin tartışılması yapılacaktır. Bunun için, ilk olarak literatürdeki güven kavramının çeşitli tanımlarının tahlili yapılacaktır. İkinci olarak, kriminal faaliyetler ve internetteki kriminal tehditlerin varlığı tanımlanmaya çalışılacaktır.

Anahtar Kelimeler: İnternet ticareti, Güven, Suç, Kriminal tehdit.

TRUST PROBLEMS ON INTERNET MARKETING AND CRIMINAL ACTIVITIES

Abstract

Trust is a major issue on internet commerce and a prerequisite of social behavior, especially regarding important decisions. It can be frequently expressed that internet commerce is generally danger and customers jeopardize their personel information, credit cards information and other properties by using internet. On the other hand, there are a number of project and application to elevate the using of internet commerce. The number of Internet users has increased dramatically, but many are reluctant to share their personal information to Web sites because they do not trust e-commerce security. In this study, it is discussed key elements that can be used to improve the visitors' sense of trustworthiness on Web sites. In doing so, we firstly examines the various definitions of trust in the literature. Secondly, it is tried to determine the criminal activites and the existence of criminal threats on Internet.

Keywords: Internet commerce, Trust, Crime, Criminal threat.

Giriş

Son yüzyılda özellikle internetin gelişimi sayesinde geleneksel pazarlama faaliyetlerini ötesinde internet yoluyla pazarlama bir sistem olarak gelişmektedir. Günümüz pazarlarında rekabet edebilmek için yeni açılımları hedefleyen firmaların temel güzergahları internet olmaktadır.

Modern pazarlama metotlarından biri olan internet ortamında satış işlemleri, pazarlama sürecindeki pek çok ara kademeyi ortadan kaldırdığı için hem tüketiciye hem de pazarlamacıya avantajlar sağlamaktadır. Bunun yanında, yaşanan çeşitli vakalar internet ticaretine olan güveni sarstığından bu alanda faaliyet gösteren firmalara da büyük zararlar verebilmektedir.

Yapılan çalışmalarda daha çok tüketicinin güvenini etkileyen faktörler araştırılmış (Jarvenpaa vd., 2000; Papadopoulou vd., 2001; Teo ve Lui, 2007; Vijayasarathy, 2004), bu faktörler arasında da tüketici için güvenlik kaygısının en üst seviyede olduğu ortaya konulmuştur (Atif, 2002; Culman, 1995; Goodwin, 1991; Han ve Suh, 2002; Hoffman vd., 1999; Liu, 2005; Peterson vd., 1997; Salam vd., 2005; Uzel ve Aydoğdu, 2010). Güvenlik kaygısı, yaşanmış kötü tecrübelerin yanı sıra internet ortamında faaliyet gösteren illegal yapılanmalar nedeniyle de yaşanabilmektedir. Bu çalışmada, tüketicinin güven ve güvenlik algısını etkileyen faktörlerin tanımlayıcı olarak belirlenmesi hedeflenmiştir. Bunun yanında internet üzerindeki kriminal faaliyetlerin çeşitliliğine değinilerek tüketici üzerindeki korkuya neden olan "en az sokaklar kadar tehlikeli" olan internetteki faaliyetlerinden bahsedilecektir.

İnternet Tüketicisinin "Güven" Sorunu

İnternet üzerinden pazarlama, geleneksel pazar uygulamalarını genişleterek organizasyonları çevresindeki şiddetli rekabet ortamına zorlayan ve sadakat ile uzun dönemli ilişki kurduğu müşterileri üzerine odaklanmaktadır (Papadopoulou vd., 2001: 322). İnternet üzerinden pazarlama, geleneksel pazarlama standartlarını değiştirerek tüketicilerin daha düşük ücretli ürünlere ulaşmasını sağlamaktadır (Liu vd., 2005: 289). Dahası, yeni girişimcilerin serbest pazara daha hızlı giriş yapabilmelerine yardımcı

[1] Yrd. Doç. Dr., Bülent Ecevit Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, aksoytr2001@yahoo.com
[2] Komiser, M.A., B.Sc., Bülent Ecevit Üniversitesi Doktora öğrencisi, hanifisever@yahoo.com

olmaktadır (Jarvenpaa vd., 2000:45). Yani, internet pazarlaması tüketicilere para, zaman, bilgi ve hizmet tasarrufu sağlamaktadır. İnternet teknolojisinin etkili bir şekilde kullanılması, büyük bir rekabetçi avantajın belirlenmesi, pazara dahil olma, yenilikçilik, teknoloji transferi ve yönetim bilimiyle yakından ilişkilidir (Torkzadeh ve Dhillon, 2002: 187).

Akademik çevreler yeni yüzyılda siber tüketicilerin aktiviteleri sayesinde büyük karların elde edileceğini belirtmelerine rağmen, sahadaki uygulayıcılar internet yoluyla satış gelirlerinin ve karın oldukça zayıf olduğunu belirtmektedirler (Kim vd., 2005; Hoffman vd., 1999). Oysaki, internet yoluyla alışveriş ABD'de 2003 yılında, B2C [3] açısından 95 milyar dolar, B2B [4] için ise, 2.6 trilyon dolar oranında gerçekleşmiştir (Liu vd., 2005). 2011 yılında yılbaşı haftasının ilk günü ABD'de online platformda yapılan harcama 825 milyon Amerikan Dolarıdır. 2010 yılında Türkiye'de 10.4 milyar pound'luk elektronik alışveriş yapılmış, bu rakam 2011 yılında 13,6 milyar pounda çıkmıştır (ZAK, 2012).

Güven, bir açıdan sosyal psikoloji ile ilgili bir kavramdır. Toplumların yaşamış oldukları olaylar nedeniyle güven duyma algılarında farklılıklar olabilmektedir. Pazarlama açısından da, tüketicilerin beklentileri ve satış işlemini gerçekleştiren kişilerin davranışları güveni oluşturmada en önemli etkendir (Jarvenpaa vd., 2000:45). Güven, özellikle önemli kararların alınmasındaki soysal davranışın bir ön koşuludur (Gefen, 2000: 725).

Pazarlama literatüründe güven, geleneksel olarak pazarlama karmasına olan güveni ifade etmektedir (Jarvenpaa vd., 2000: 46). Güven, bütün ticari işletmeler için hayati bir bileşendir. Tüketicinin, satıcının reklam kanalı ile sunduğu hizmetlere ve teminatlara güven duyması gerekmektedir (Grandison ve Sloman, 2000). Pazarlamadaki etkileşim, kişilerin kişilere, kişilerin firmalara ve firmaların firmalara güven duymaları yönünde ele alınmaktadır (Kim, vd. 2005).

İnternetin öncesi toplumlarda pazarlama, çoğu zaman müşterilerle yüz-yüze teması gerektirmekteydi (Vijayasarathy, 2004, 747-762; Papadopoulou vd., 2001: 322; Teo ve Lui, 2007: 22). İnternet üzerinden ticaretin başladığı ilk zamanlarda, güvenlik tüketicilerin davranışlarında belirgin bir engel oluşturmuştur. Özellikle kredi kartı bilgilerinin çalınması reel vakalar olarak karşımıza çıkmıştır. Güvenlik ihlali sorunları neticesinde tüketicilerin mali ve kişisel bilgilerinin (Suh ve Han, 2003: 136) hatta itibarlarının dahi çalınması mümkün hale gelmektedir. İnternet ortamında yaşanan bu güvenlik probleminin kısa dönemli teknolojik bir konu olduğu belirtilmiştir (Peterson vd., 1997, Atif, 2002). Aksoy (2006), tüketicilerin güven tutumları ile ilgili yapmış olduğu çalışmasında, müşterilerin elektronik alışverişten hoşlandıkları ancak güvenlik riskinden dolayı alışveriş yapmak istemediklerini saptamıştır. Uzel ve Aydoğdu (2010) da tüketicilerin güvenlik kaygıları nedeniyle internet üzerinden yapılan pazarlama eylemlerine temkinli yaklaştıklarını belirtmiştir. Öte taraftan, güven konusunun sadece teknolojik problemlerden kaynaklanmadığı da belirtilmelidir. Çünkü, internet ortamında yapılan ticarette, tüketici karşısındaki satıcıyı çoğunlukla reel olarak tanımamaktadır. Yani, tüketicinin marka, sponsor, işletme ya da reel birini tanıması oldukça güçtür. Ancak satış elemanının ortadan kaldırılması, tüketicide kendisine muhatap olarak alabilecek bir kişinin olmaması nedeniyle kaygı yaratabilmektedir (Jarvenpaa vd., 2000: 46). Burada karşımıza çıkan önemli bir nokta pazarlama açısından tüketicinin güven sorunu bireylere ya da sistemlere karşı olmaktadır.

Geleneksel pazarlamada güven, satıcının vermiş olduğu sözleri tutmasını, bir ürünü ya da hizmeti zamanında teslim etmesini tarif etmektedir. Bu aşamada, güven duygusunu yansıtan bir diğer konu ise, tüketicinin isim, adres, kredi kartı bilgileri ve aldığı ürünlerin gizliliği konusudur.

Güvenin tanımlanmasının güç bir kavram olması, risk ile arasındaki ilişkinin açıkça anlaşılmasındaki hatalar ve geçmişte yaşanan kötü deneyimler tüketicinin güven duygusunun karşısındaki en büyük engellerdir. Bu nedenle, internet üzerinden bir ticaret amaçlayan site yöneticileri öncelikle bu engelleri göz önüne alarak çözüm üreteci bir çaba içerisinde olmaları gerekmektedir.

İnternet pazarlayıcısı, tüketicilerin geçmişteki kötü deneyimlerinden ders çıkartarak kendilerine bir yol çizmektedirler. İlk olarak, piyasa ve kamuoyu araştırmaları neticesinde tüketicilerin güven ile ilgili tutumları belirlenmelidir. Geçmişte yaşanmış olan kötü deneyimlerin online işlemler esnasında ortadan kaldırılması gerekmektedir. Örneğin ikiz ya da sahte web siteleri müşterilerin güven duygusunu olumsuz yönde etkileyen bir durumdur. Online ticaretin başladığı ilk zamanlarda bankaların web sitelerinin sahtelerinin oluşturulması neticesinde pek çok kişi mağdur olmuştur. PandaLabs'ın 2010 raporuna göre; her

[3] **B2C**, ticari firmaların müşterilerine İnternet ortamından yaptıkları satış işlemleridir. Nihai tüketim yapılmaktadır. Amaç, mevcut ve potansiyel müşterilere daha kolay ve daha düşük maliyetle online satış imkanı sağlamaktır.

[4] **B2B**, şirketler için tedarik pazarı olarak kullanılmaktadır. Birçok şirketler İnternet üzerinden, mal ve hizmet üretim aşamasında ihtiyaç duydukları ürünlerini veya ara malların toptan satışlarını kolaylıkla yapabilme olanağına kavuşabilmektedirler.

hafta 57 bin sahte web sitesinin oluşturulduğu belirtilmektedir. Belirlenen sahte sitelerin %63,72'sinin bankaların, %26,81'inin ise online alışveriş yapılan tanınmış işletmelere ait olduğu belirtilmektedir.

Güven duygusunun oluşturulmasında ikinci adım, değişik pazarlar ve değişik ülkelerdeki tüketici davranışları üzerine yapılmış çalışmaların incelenmesi ve işletmenin bu araştırma sonuçlarını entegre etmesi gerekmektedir.

Son aşamada ise internet alışverişi için belirgin, herkes tarafından anlaşılabilir, süreçlerin her seferinde aynı şekilde işletildiği, piyasadaki diğer online ticarete izin veren sitelerden farklı bir hareket tarzı içselleştirilmelidir.

Han ve Suh (2002)'a göre, tüketicilerin bankaların web sitelerine karşı duydukları korku diğer web sitelerine göre daha yüksektir. Bunun gerekçesi ise, tüm mahrem bilgilerinin sahte siteler, ya da sistemden kaynaklanan açıklar yüzünden üçüncü kişiler tarafından çalınması korkusudur. Bunun yanında, tüketicilerin bu tür sitelere yönelik tutumlarında kullanışlılığın da ön planda olduğu belirtilmektedir. Bu tarzdaki çalışmaların farkına varan bankacılık sektöründeki işletmeler, online hizmet veren alanda dijital imza ve şifreleme gibi sistemlerle işlem güvenliğini arttırma yoluna gitmişlerdir.

Daha fazla büyüme arayışına giren işletmeler, yönelmiş oldukları internet pazarında karlarını arttırabilmek için, müşterilerini anlamaya çalışırken, müşterilerin kayıt, kişisel bilgileri, siparişleri veya anket formları ve "cookies"lerini (çerezleri) kullanarak müşterilerinin tercihleri konusunda bilgi sahibi olabilirler (Liu, 2005). Bu sayede tüketicinin ihtiyaçlarını belirleyen işletmeler, piyasadaki talebe göre ürün satışını gerçekleştirerek daha çok gelir elde edebilir. Ancak bu geliri elde ederken tüketicilerin kişisel bilgilerinin paylaşımındaki paradoks büyük sorun yaşanmasına neden olmaktadır. Bir işletmenin, bir tüketiciye ait adres, telefon gibi kişisel bilgilerine bir şekilde ulaşarak reklam amacıyla bile iletişime geçmesi, o tüketicide daha önceki alışverişlerine yönelik bir şüphe doğurmaktadır. Kendisine ait olan bu kişisel bilgilerin hangi yollarla diğer işletmelere sızdığı tüketici için kaygı verici bir durum oluşturmaktadır. Bu nedenle, tüketicinin kendisine yönelik algıladığı internet üzerindeki tehdit, onların tutum ve davranışlarında oldukça etkili olmaktadır (Teo ve Lui, 2007: 22)

Tüketicilerin algıladıkları güven, kişisel bilgilerinin başkaları tarafından erişilmesi gibi mahremiyetin ihlali sonucu maddi ve manevi zarar görme kaygısı olarak tanımlanabilir. Hoffman vd. (1999)'a göre, bu tip kaygılar "çevresel kontrol" ve "bilgi kontrolünün ikincil kullanımı" üzerindeki bilgi gizliliği etrafında dönmektedir. Çevresel kontrol doğrudan tüketicilerin online alışverişteki güvenlik algılarını doğrudan etkilemektedir. Reel dünyada, bir tüketici bir firmanın müşteri hizmetleri ile yaptığı telefon görüşmesi sonrası kredi kartı bilgilerini verirken kaygı duymaktadırlar. Ancak, öte taraftan bir tüketici herhangi bir ticari Web sağlayıcıya kredi kartı bilgilerini verirken korkmaktadır (Hoffman vd., 1999: 81; Salam vd., 2005: 73). Yani çevresel kontrolde internet ortamında yapılan alışverişler tüketicide psikolojik olarak kaygının ötesinde bir korku hali yaratabilmektedir. Çünkü bir nevi kimlik bilgisi olan kredi kartı bilgilerini tanımadığı kişilere verdiğini düşünmektedir. Bilgi kontrolünün ikincil kullanımı ise, tüketicinin vermiş olduğu bilgilerin işlemler sonrasında ikincil olarak kullanımını yansıtmaktadır. Yani, tüketici yapmış olduğu alışveriş sonrasında vermiş olduğu çeşitli kişisel bilgilerinin tüketicinin izni ya da bilgisi dışında başka firmalara satılması ya da başka firmalarca bu bilgilerin çalınması olarak tarif edilebilir (Goodwin, 1991; Culman, 1995). Online ticaret sonrası bir web sitesine vermiş olduğunuz tüm bilgilerin gizli kalması gerekirken, almış olduğunuz bir ürün sonrası diğer rakip firmalar cep telefonunuza sürekli mesaj göndererek ya da ev adresinize postalar yollayarak kişisel bilgilerinizi ele geçirdiklerini ispatlamaktadırlar.

Güven duygusu toplumsal kültürden etkilenmektedir. Bazı insanlar, bazı toplumlar doğası gereği diğer insanlardan daha fazla güvenebilirler. Sosyal normlar, değerler (Teo ve Liu, 2007: 22) ve sosyal düzen kuralları bir toplumdaki güven duygusunu tarif edebilmek için önemli özelliklerdir. Bu görecelilik, insanların içerisinde yaşadıkları toplumsal kültürle ilişkilidir. Örneğin, Çin ve Japon halkları kültürel boyutlar açısından birbirlerine oldukça yakın olmasına karşın Japonların güven duyguları Çinlilere nazaran daha gelişmiştir (Olson ve Olson, 2000: 43).

İnsanların güveni fiyat ve fayda açısından değerlendirmekte ve kırılganlıkları an be an değişebilmektedir (Olson ve Olson, 2000: 43). Bu nedenle, tüketicilerin güven duyguları yaşadıkları reel dünyadaki tecrübeleri ile farklılaşabilmektedir.

Pazarlamada yüz yüze ilişkiler güven sağlamada etkili bir yöntemdir. Yüz yüze ilişki sayesinde sosyal sınıf, tavır ve tabiyet hakkında çıkarım yapılabilir (Olson ve Olson, 2000: 43). İnternet ortamında yapılan ticaretin en büyük handikapı tüketicinin yüz yüze iletişime geçebileceği bir satış elemanının ya da mağazanın olmamasıdır (Chellappa ve Pavlou, 2002: 358). Online tüketiciler, bilgi kaynaklarının pek çoğundan elde ettikleri bilgiler sonrasında güvenilirliğe itibar ederler (Moore vd., 1999). Tüketicilerin

karşısında reel bir satış elemanını bulamadıkları web sitelerinde gerçekleşen ticarette güven unsuru web sitesinin büyüklüğü (Doney ve Cannon, 1997) ve şöhreti (Aksoy, 2009) ile tesis edilebilir.

Tüketicinin güveninden bahsederken için iki temel karakteristikten bahsedilebilir. Bunlar; tedarikçinin ve tüketicinin karakteristikleridir. Tedarikçinin karakteristikleri; şöhret, büyüklük, çok kanallı iletişim ve sistem güvencesidir. Bütün bu alt karakteristikler tüketicinin güvenini oluşturmada pozitif bir değer taşımaktadır. Şöhret, internet pazarlamasında yüzyüze iletişim olmadığı için tüketicilerin güven duygusunu oluşturmada oldukça etkili bir kavramdır. Örneğin yüzlerce online kitap satışı yapmakta olan web sitesi olmasına rağmen piyasada reklamını iyi yapabilen ve tüketicilerin birbirlerine tavsiye ettiği web siteleri, şöhretleri vasıtasıyla daha çok müşteri çekmektedir. Müşteri potansiyeli ve pazarlama hacmi ile büyüyen internet işletmesi daha kurumsal bir hale gelmektedir. Kurumsallaşma sürecine girmiş olan internet siteleri tüketicilere daha çok güven sağlayabilir.

Çok kanallı iletişim, bir işletmenin tutundurma çabalarında yaralanmış olduğu enformasyon kaynaklarıdır. Örneğin, yazılı veya sözlü reklamlar, kataloglar, e-mail reklamları ya da web sitelerine link verme, banner (düğme) atma gibi yöntemler tüketicide güven oluşturmak için önemlidir. Örneğin, toplumun çoğunluğu tarafından saygın olarak nitelendirilen web sitelerinde reklamlarını yayımlayan internet pazarlamacılar, bu sayede tüketicide dolaylı bir güven oluşturabilir.

Sistem güvencesi, tedarikçinin online alım satım sisteminin güvenliği ve güvenilirliği olarak tarif edilebilir. Örneğin, önceleri internet üzerinden bir alışveriş yapabilmek için sadece bir kredi kartı yeterli iken, bugünlerde pek çok alışveriş sistemi içerisine entegre edilmiş yan faktörler (kredi kartı kullanıcısına cep telefonu mesajı gönderilmesi, vatandaşlık numarası ile kredi kartı sahibinin bilgilerinin örtüştürülmesi, güvenlik kodlarının istenmesi vb.) tüketicideki güvenlik ve güvenilirlik duygularını arttırmaktadır.

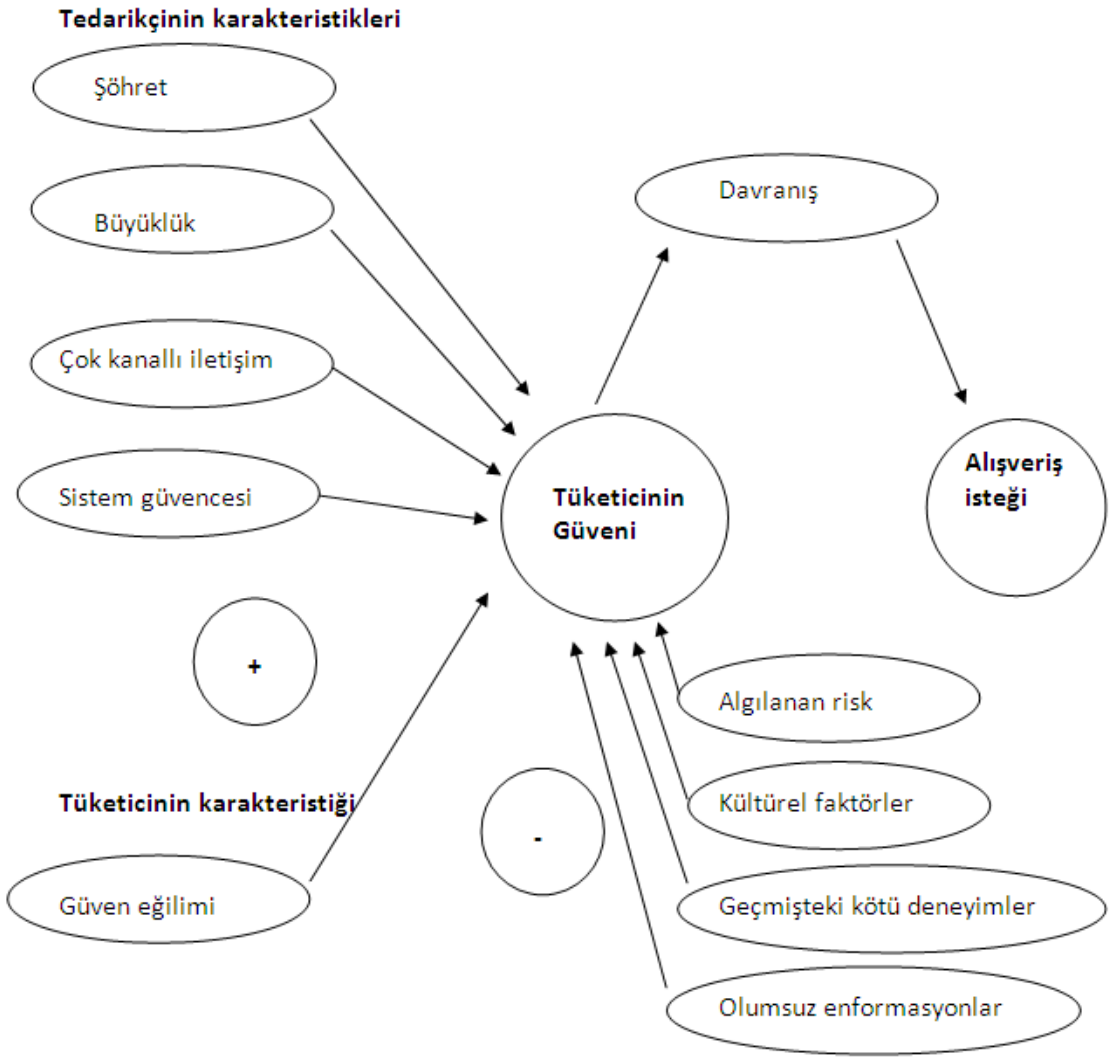
Tüketicinin karakteristiği açısından konuya baktığımızda, tüketicinin güven eğilimi göstermesi, internet pazarlamasındaki güven duygusu için pozitif bir etkiye sahiptir.

Tüketicinin güvenini olumlu yönde etkileyen bu faktörlerin yanında olumsuz etkileyen faktörler de bulunmaktadır. Olumsuz enformasyon, bir online satış yapan web sitesi ile ilgili reel dünyada tüketicilerin yaşamış oldukları sıkıntıları birbirleri ile paylaşmaları sonucu, toplumda yaygın olarak internet ticaretine ya da bahsedilen web sitelerine yönelik olumsuz bir tavır gelişebilir.

Tüketicilerin internet alışverişi esnasında ya da sonrasında yaşamış oldukları kötü deneyimler onların sonraki alışverişlerini etkilemektedir. Tüketici yaşamış olduğu sıkıntılar nedeniyle sadece sorun yaşadığı web sitesine değil, diğer web sitelerine karşı da bir direnç ya da önyargı geliştirebilir.

Kültür, güven duygusunun oluşmasında önemli bir etkendir. Toplumların kültürel yapıları, teknolojiye ve yeniliğe bakış açıları onların güven duygusunu da etkilemektedir. Dünyada internet alışverişinin gün geçtikçe yaygınlaşması kültürel açıdan toplumların teknoloji ile uyumlaşmaları sonucu oluşmaktadır. Kültürel faktörlere bağlı olarak; internet ortamında alışverişin risk olarak algılanması da bir diğer önemli boyutu oluşturmaktadır. Kültür ve risk algısı birbirini etkileyen kavramlardır. Yukarıda sayılmış olan faktörlerin tamamı tüketicinin güven duygusunu olumsuz yönde etkilemektedir. İşte bu noktada, online işletmeler için itme ve çekme anlayışından bahsetmekte fayda vardır. İtme, tüketicinin güven duygusunu olumsuz, çekme ise olumlu olarak etkilemektedir. Bu bakış açısından hareketle, tüketicinin zihninde oluşan negatif (itme) ve pozitif (çekme) kriterler onun internetten alışveriş yapma dürtüsünü eyleme geçirecektir. Tüketici bir davranış sergileyecektir ve neticede online alışveriş isteği gerçekleşmiş olacaktır.

Literatürde bahsedilen bütün bu bilgiler ışığında, internet pazarlamasında güven ile ilgili aşağıdaki gibi bir diyagram ortaya konulabilir.



Tüketicinin Güven Algısını Etkileyen Kriminal Eylemler

İş dünyasının teknolojiye ve internete olan bağımlılığı arttıkça, tüketicilerin de talepleri bu doğrultuda yönlendirilmeye başlanmıştır. İnternet üzerinden başlayan ticarette ilk başlarda oldukça iyimser bir hava olmasına rağmen internet üzerinde başlayan kriminal tırmanış tüketiciler üzerinde büyük bir baskı oluşturmuştur. Sadece tüketiciler değil, işletmeler dahi sahtecilik, hırsızlık ve dolandırıcılık suçlarından dolayı mağdur edilmiştir.

Bilgisayar sistemlerine yapılan iç ve dış sabotajlar öncelikle işletmelerin mağduriyetini doğurmuştur. İç sabotajlar, genellikle kurumların bünyesinde çalışmakta olan personel ile o işletmeden yeni ayrılmış olan kişilerce gerçekleştirilebilecek iken, dış sabotajlar çoğunlukla bilinmeyen, hatta okyanus ötesi ülkelerin küçücük bir kasabasından bile gerçekleştirilebilen sistem suikastlarıdır. Online işletmelere yapılan bu saldırılardaki temel amaç, rekabetin kırılması, saygınlık ve itibarın yitirilmesi, kötü şöhret oluşturulması, spekülasyon yaratılması, rakip organizasyonlara yönelik psikolojik harp, kişisel bilgilerin ele geçirilmesi, öç alma, şirket hesaplarının boşaltılması, suç geliri elde etmek gibi nedenlerle yapılmaktadır.

İnternet ortamında gerçekleştirilen kriminal aktiviteler tüketicinin güvenini doğrudan ya da dolaylı olarak etkilemektedir. Eğer tüketiciler doğrudan internet üzerinden işlenmiş bir suçun mağduru olmuşsa, doğrudan mağduriyetten bahsedebilmek mümkündür. Maalesef, bu tarz mağdur olan tüketicilerin yaşadıkları travmalar onların internet pazarına entegre olmasını neredeyse imkansız hale getirmektedir. Şehir efsaneleri sonucu yanlış bilgilenme, güvenilir şirketlere yapılan sabotajlardan haberdar olma, medyanın internet ticareti ile yaşanan bir sorunu sunarken olayı trajikomik bir şekilde sunması, internet

üzerinden teröre varan suçların işlenmesindeki kolaylık ve tüketicilerin bu durumlardaki farkındalığı gibi faktörler de tüketicilerin dolaylı olarak mağdur olmasına örnek olarak verilebilir.

Bilgisayar teknolojileri ve internetin yaygınlaşması sonrasında işlenmekte olan suçlar farklılık göstermektedir. Dolandırıcılık, sahtecilik, özel hayatın gizliliği ve iletişimin ihlali, hırsızlık, çalıntı mal satmak ve satın almak, pornografi, fuhuş, çocuk ticareti, insan ticareti, organ ticareti, örgütlü suçlar, narkotik suçlar ve terörizm suçları internette en yaygın işlenen suç tipleridir. Bu suç tiplerinin nasıl gerçekleştirildiğine dair kısa açıklamalara yer verilecektir.

İnternet üzerinden dolandırıcılık suçu sıklıkla ve çok çeşitli olarak işlenmektedir. Dolandırıcılık suçları işletmeler arası ve işletmelerden tüketiciye değil, özellikle tüketiciden tüketiciye yönelik gerçekleştirilen ticaret işlemlerinde karşılaşılmaktadır. Örneğin suçlular, zilyetlikleri kendisine ait olmayan ürünleri ilan ile satarken, tüketicilerden kaparo adı altında teminat parası yatırmalarını istemektedirler. Tüketici satın almak istediği bu ürüne karşılık teminatı dolandırıcının vermiş olduğu hesaba yatırdığında bir daha bu kişi ile iletişime geçememekte ve satın almak istediği ürüne de sahip olamamaktadır. Dahası yatırmış olduğu teminat parasını da kaybetmektedir.

Sahtecilik de internet ortamında yaygınlaşan bir suç tipi haline gelmiştir. İnternet kanalı ile bir tüketiciye ait kişisel bilgiler ele geçirilerek o kişi adına sahte kimlikler düzenlenerek bankacılık faaliyetlerine girişilebilmektedir. Böylelikle, başkaları adına şirket açma, vergi cezaları oluşturma, başkalarının adı üzerinden kara paranın aklanması gibi faaliyetler gerçekleştirilebilmektedir.

Özel hayatın gizliliği ve iletişimin ihlali suçları açısından incelendiğinde, kişisel verilerin güvenliği ilk olarak akla gelmektedir. Bir tüketicinin internet üzerinden gerçekleştirdiği faaliyetlerine ilişkin bilgilerin ele geçirilmesi, iletişiminin ihlali ve özel hayatının gizliliğinin ihlal edilmesine neden olur. Cinsel yaşam ve bebek üzerine bilgilendirici web sitelerinden alışveriş yapan tüketiciye ait kişisel bilgilerin çalınması neticesinde başka firmalar tarafından bu tüketicinin e-mailine, cep telefonuna mesajlar gelebilmekte, hatta evinin posta kutusuna reklamlar gönderilerek özel hayatının komşuları tarafından da öğrenilmesine neden olabilmektedir.

Kişisel verilerin çalınması, kişilerin online hareketlerinin takip edilmesi ve hırsızlık da internet ortamında mümkündür. Promis (Ersanel, 2001), Echelon (Gürdilek, 2001) ve Carnivore (Şen, 2007) gibi yazılımlar dünyada internet ortamında güvenli bir kale kalmadığını göstermektedir. Ersanel (2001)'e göre Promis bir istihbarat silahıdır. Bu yazılım kanalıyla bankaların, holdinglerin ve devlet dairelerinin gizli veri bankalarına, fark edilmeden girme ve istenilen bilgiyi çalma mümkün hale gelmiştir. Gürdilek (2001)'e göre, Echelon sistemi ile dünyada her gün gönderilmekte olan milyonlarca e postanın takibi, içeriklerinin incelenmesi mümkün hale gelmiştir. Carnivore sistemi de benzer şekilde kişisel bilgilerin, mahremiyetin çalınmasına ve ifşa edilmesine neden olmaktadır.

Fiziki dünyada çalınmış olan malların satılması da internet ortamında mümkün olabilmektedir. Örneğin bir otomobilden çalınan oto teybi, bir iş yerinden çalınan bilgisayar, televizyon ya da bir çalıntı otomobil vb. kıymetli bütün ürünler internet ortamında tüketicilere uygun fiyatlarla satılabilmektedir. Ülkemiz ceza kanunlarına göre çalıntı malın satılması bir suç iken, çalıntı malın satın alınması da ayrı bir suç olarak tüketiciyi de etkileyecektir. Böylelikle, tüketici de kriminal girdabın içerisine haberi olmaksızın çekilebilmektedir.

Pornografi, uluslararası evlat edinmeye aracılık, fuhuş, çocuk ticareti, insan ticareti ve organ ticareti gibi örgütlü suçlar da internet ortamında işlenmektedir. Özellikle yoksulluğun üst seviyelerde bulunduğu ülkelerde çocuklarına iyi bir gelecek sunma konusunda umutsuz ailelerin veya bekar annelerin çocuklarını genellikle iyi niyetli olarak uluslararası evlat edinilmesine razı oldukları, aynı zamanda da kendilerine belirli bir miktar maddi kazanç sağladıkları görülmektedir (Sever ve Harbigil, 2010). Çoğunluğu internet üzerinden gerçekleşen bu ticaret, günümüzde o kadar gelişmiştir ki; kişiler internetten beğendikleri bir çocuğu hiçbir yere gitmeden tacirler vasıtasıyla ayaklarına kadar getirtebilmekte, kısacası satın alabilmektedir. İnsan tacirleri, bu çocuk pazarında internet üzerinden dolandırıcılık da yapmaktadır. Kimi internet siteleri üzerinden aynı çocuğun birden fazla aileye satıldığı veya hiç evlat verilmeyecek çocukların bile bu internet

sitelerinde kayıtlarının bulunduğu belirlenmiştir (Sever ve Arslan, 2008) . FBI'ın araştırmasında 100.000'den fazla internet sitesinin çocuk pornografisi ve çocuk ticareti için hizmet verdiğini belirtmektedir (Poulopoulos, 2001). Kosova savaşından sonra çeteler ailelerinden 1000 Amerikan dolarına aldıkları çocukları İtalya ve Yunanistan'da internet üzerinden iki katı fiyatına satabilmişlerdir (Knaus vd. 2006).

İnternet üzerinden narkotik suçlar iki türlü işlenmektedir: sosyal paylaşım siteleri ve ayrı bir web sitesi kurulması. Özellikle son birkaç yılda büyük kullanıcı kitlesine sahip olan sosyal paylaşım sitelerinde kurulan gruplar üzerinde oluşturulan narkotik içerikli sitelerde "torbacılar" faaliyetlerini sokaklardan internet ortamına taşımışlardır. "Online torbacılar" müptezellerle girmiş oldukları ilişkiler sonrasında kredi kartı ile ödeme, havale, ptt posta çeki gibi yöntemlerle para transferleri gerçekleştikten sonra, narkotik madde kullanıcılarına özel kargo şirketleri kanalıyla kitap, CD ve giyim eşyası gibi ürünlere zulalamış oldukları narkotik maddeleri satmaktadırlar. İstanbul Emniyet Müdürlüğü Asayiş Şube Müdürlüğü Güven Tim Büro Amirliği görevlileri 2011 yılında yapmış oldukları 6 operasyonda toplam 12 "online torbacı"yı suçüstü yakalamıştır. Bir diğer yöntem ise, narkotik ticaretinin ayrı web siteleri üzerinden gerçekleştirilmesidir. Bu süreç de diğeri gibi işlemektedir.

Terörizm, modern dünyada yeni bir çatışma doğurmuştur. "Siber terör, siber savaş, siber saldırı" ya da önerilebilecek başka bir isim… Adı ne olursa olsun bu sanal tehdidin getirdiği risklerin ayrıntılı bir şekilde değerlendirilmesi gerekmektedir. Sanal savaş bilinmeyen5 bir düşmanın, bilgisayar ağları üzerinden yaptığı kötü amaçlı saldırılarla bir sihirbaz gibi elimizdeki bilgileri çalması, değişik teknikler kullanarak sistemlerimizi felce uğratması ve genel huzurun bozulması suretiyle karşımıza çıkar. Siber saldırılar, bir ülkenin mahremi olan kamu yararı ve ulusal güvenlik konularına kadar uzanmış ve karmaşık problemler oluşturmaya başlamıştır (Sever, 2006).

İnternet doğası gereği, terörist organizasyonların faaliyetleri için bulunmaz bir ortam yaratmıştır. Özellikle;

- Kolay giriş imkanı,
- Kural, sansür, daha başka idari kontrol yöntemlerinin yok ya da çok az olması,
- Dünya çapında büyük kitlelere hitap etmesi,
- Kimlik bildirme zorunluluğunun olmayışı,
- Bilgi akışının çok hızlı oluşu,
- Web ortamında bulunmanın, geliştirmenin ve tadilinin maliyetinin çok düşük olması,
- Yazılı eserler, grafik, ses, video gibi kullanım türleri yaratması ve kullanıcıların film, şarkı, kitap, poster ve benzerlerini bilgisayarlarına indirebilmesi,

İnterneti haber kaynağı olarak kullanan kitle iletişim araçlarını yönlendirebilme imkanı sunması internetin popülaritesini arttırmaktadır. Böylelikle psikolojik harp, tanıtım, propaganda, istihbari çalışma yapma, bilgi ve veri yönetimi, gelir elde etme, irtibat, planlama ve koordinasyon gibi eylemleri gerçekleştirmek rahatlıkla mümkün hale gelmiştir (Sever, 2006).

Siber suçlular, siber silahlarla internet ortamını terörize etmektedir. Siber silahları üç ana başlıkta toplamak mümkündür. Bu silahlar genel olarak sözdizimsel (syntactic), anlamsal (semantic) ve karışık (mixed) tipteki silahlar olarak adlandırılmaktadır (Brenner ve Goodman, 2002). Sözdizimsel silahlar DoS (Denial of Service) saldırılarını ve kötü niyetli yazılımları (Malicious Code, Spyware, Trojan Horses ve Worms) kullanarak bilgisayarların işletim sistemlerine zarar verirler. Anlamsal (semantic) siber silahlar ise bilgisayarda karşımıza çıkan bilgilerin doğruluğunu değiştirerek bilgisayar kullanıcılarına kendini fark ettirmeden yanlış bilgi edinmelerini sağlarlar. Karışık tipteki siber saldırı araçları ise hem sözdizimsel (syntactic) hem de anlamsal (semantic) silahların birlikte kullanılmasıyla oluşurlar ve sadece bilgisayarın işletim sistemlerine zarar vermekle kalmaz aynı zamanda bilgisayar kullanıcılarının elde ettiği bilgilerin doğruluğunu da değiştirirler (Gürkaynak ve İren, 2011).

Kriminal aktiviteler yönünden yukarıda bahsedildiği gibi en az sokaklar kadar tehlikeli olan internet ortamındaki vakalar tüketiciler üzerinde dolaylı bir mağduriyet oluşturmaktadır. "Hiçbir yerin güvenli

[5] Şüphelenilmeyen demek daha doğru olsa gerek, zira bilişim konularında kendi içimizden vurulma ihtimalini de asla göz ardı etmemek gerekir.

olmadığı" görüşünün toplumda hakim olması, tüketicide internet pazarlamasından ziyade geleneksel pazarlamaya yönelimi doğurabilmektedir. İşte internette kol gezen kriminal faaliyetlerin yoğunluğu tüketicideki güven duygusunu alt üst etmekte ve rekabet çağındaki online işletmeleri de hedeflerine ulaşmada engellemektedir.

Siber Suçlarla Mücadeledeki Politika

Sokaklarda yaşanan suç tiplerinin çok hızlı bir biçimde kriminal eğilimi olan kişilerce sanal ortama entegre edilmesi çok uzun sürmemiştir. Hemen her suç tipiyle karşılaşılan internet ortamındaki bu denetimsizliğin ortadan kaldırılabilmesi için çeşitli eylemlere girişilmiştir.

Devletlerin suç ve suçlulukla mücadelesi ancak ve ancak yasal yollarla yapılabilmektedir. Devletin suçla mücadelesindeki kolu olan adli mekanizmanın etkin bir şekilde çalışabilmesi için yetkilendirme gereklidir. Adli mekanizma gücünü kanunlardan ve elde ettiği teknolojiden almaktadır. Sahip olduğu teknolojiyi de kanunların sağladığı imkan doğrultusunda kullanabilmektedir.

İnternet aracılığı ile işlenen suçlarla mücadele internetin doğası gereği oldukça zordur. Sokakları, caddeleri, suçlulara ait eşkal bilgileri olmayan ve bölgesel değil küresel çapta düşünülmesi gereken bir yapıdır. Bu nedenle, internet ortamındaki güveni ve güvenliği sağlayabilmek için teknik imkan, mevzuat, işbirliği, uluslar arası kriterler, yetişmiş personel ve suçla mücadele kültürünün içselleştirilmiş olması gerekmektedir.

Ülkemizdeki internet suçları ile mücadeledeki politika, Avrupa Birliği'nin ayak izlerini takip etmektedir. İnternet suçları ile ilgili Avrupa Birliğinin attığı adımlara ilişkin bazı düzenlemelere bakmakta fayda vardır. 1 Eylül 2005'te Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) faaliyet başlamıştır. ENISA'nın görevi, bilgi ağlarının ve taşıdıkları verilerin güvenliğinin sağlanmasına yardımcı olmaktır. Bu, bütün AB vatandaşlarına, tüketicilere, işletmelere ve kamu sektörü kurumlarına yarar sağlamayı hedeflemiştir. Mayıs 2007 yılında, çevrim içi terörizmi gözlemlemek için Avrupa Polis Ofisi (EUROPOL) tarafından güvenlik portalı oluşturulmuştur. 29 Mart 2010 tarihinde çocuk pornografisini filtreleyecek öneriler masaya yatırılmıştır.

Türkiye'de 2005 yılında yapılan yargı reformu ile internet suçları ile mücadele hedeflenmiştir. Bu kapsamda; 5237 sayılı Türk Ceza Kanunu'ndaki düzenlemelere genel olarak değinilmelidir. Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu (m.243), bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme veya orada kalmaya devam etme" eylemini suç tipi haline getirmiştir (Dülger, 2004:212). Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi (m.244/1-2) de suç olarak tanımlanmıştır. Bir bilişim sisteminin işleyişinin engellenmesi, bozulması, sistemin içerdiği verilerin bozulması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi, erişilmez kılınması, değiştirilmesi ve yok edilmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlanması bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunu (m.244/4) oluşturmaktadır. Banka veya kredi kartlarının kötüye kullanılması suçu (m.245) da düzenlenmiş olan son yeniliklerden olmuştur.

Özel hayatın gizliliğine yönelik yapılan düzenlemelerde ise; Kişisel verilerin kaydedilmesi suçu (m.135) kişilerin siyasal, felsefi ve dinsel görüşlerinin, ırksal kökenlerinin, sendikal bağlantılarının, cinsel yaşamlarının ve sağlık durumlarının kişisel veri olarak yerleştirilmesi eylemleri suç tipi olarak düzenlenmiştir (Özel, 2001: 865; Değirmenci, 2002: 156). Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu (m.136) bu bilgilerin hukuka aykırı olarak üçüncü kişilere verilmesi, yayılması ya da bu verilerin üçüncü kişiler tarafından ele geçirilmesinin suç tipi olarak düzenlenmesi yerinde olmuştur. Verilerin yok edilmemesi suçu (m.138) yasal süresi dolmasına rağmen kişisel verileri sistem içinden yok etmekle görevli olan kişilerin bu görevlerini yerine getirmemeleri durumu suç haline getirilmektedir (Özel, 2001: 865; Değirmenci, 2002: 157).

İnternet ortamındaki güvenin sağlanmasında devletin elindeki yasal güç olan mevzuat oluşturma aşamasında Türkiye'nin önemli adımlar attığından bahsedilebilir.

Kriminal faaliyetlerin hızla yaygınlaştığı internet dünyasında fayda elde etmek isteyen şirketlere ve tüketiciye güven sağlama aşamasında polisin kabiliyetlerinin neler olabileceği merak konusudur. Türk

Emniyet Teşkilatı, siber suçlu ve suçlulukla mücadele edebilmek için ihtisas birimleri oluşturmuştur. Bu sayede internet ortamında korku salan kişilere karşı siber polisler iz sürmeye başlamıştır. "Her temas bir iz bırakır" prensibinden yola çıkarak "her tık bir iz bırakır" politikası geliştiren polis, işlenen her suçla ilgili bir delil araştırmaktadır. İnternette güvenli ortamın sağlanmasındaki (e-asayiş) temel aktör polisin profesyonelliğidir. Netice itibariyle, devletin, vatandaşların, işletmelerin, sermaye sahiplerinin itibarını koruyan en önemli husus siber suçluların yakalanmasıdır.

Sonuçlar

İnternet işletmeciliği, uzun dönemli rekabeti amaçlayan ve sadakate önem veren bir işletme mantığını yansıtmaktadır. Yoğun rekabet ortamındaki işletmeler, internet ticareti vasıtasıyla pazarlama sürecindeki ara kademeleri ortadan kaldırarak daha hızlı ve düşük maliyetli ürün tedariki sağlayabilmektedirler. Ancak bu kolaylığın yanında karşımıza çıkan en büyük engel internet ortamında karşılaşılan kriminal eylemlerdir.

İnternet pazarlamasındaki en önemli husus güven sorunudur. Geleneksel pazarlama anlayışının aksine yüzyüze pazarlamanın olmaması internet pazarlamasındaki en büyük handikaptır. Çünkü internet ortamındaki alışverişte tüketici reel olarak tanımadığı bir kimseye pek çok kişisel ve finansal bilgisini vermektedir.

İnternet ortamındaki yoğun kriminal aktiviteler bireylerin güven duygusunun zedelenmesinde büyük bir etkendir. Geçmişte yaşanmış kötü tecrübeler, sosyal öğrenme teorisi (İçli, 2007) ışığında öğrenilen tecrübeler, şehir efsaneleri, medyanın bir vakayı trajik olarak kamuoyuna sunması gibi pek çok faktörün yanında bireylerin internette kol gezen kriminal çetelerin hatta siber teröristlerin varlığından endişe duyması da gayet doğaldır. Gayet masum bir kişinin bilgilerinin siber teröristler tarafından ele geçirilmesi ve bu bilgilerin sanal ortamda suçta kullanılması bir kimsenin şahsiyetine, ticari şöhretine ve ailevi saygınlığına verilebilecek en büyük zararlardan bir tanesidir. Kişilerin ticari niyetlerinin suç işleyenler tarafından istismar edilmesi neticesinde pazarlama karmasındaki herkes zarar görmektedir.

İnternet ortamının güvenli bir kale haline gelmesinde ulusal ve uluslararası mekanizmaların üreteceği politikaların önemi büyüktür. Siber suç ve suçlulukla mücadele neticesinde daha güvenli bir sanal dünya, daha karlı bir ticaret sürecini de beraberinde getirecektir.

AB sürecindeki Türkiye, güvenli internetin sağlanabilmesi için pek çok politika geliştirmektedir. Uluslar arası hukuka uygun hareket eden kanun koyucunun çıkarmış olduğu yasalar ışığında hareket eden kolluk güçleri internet ortamında güvenli ve korunaklı alanlar oluşturmaya çalışmaktadır.

Kaynakça

Aksoy, R. (2006). Bir Pazarlama Değeri Olarak Güven ve Tüketicilerin Elektronik Pazarlara Yönelik Güven Tutumları. *ZKÜ Sosyal Bilimler Dergisi*, Cilt 2, Sayı 4, 79-90

Aksoy, R. (2009). *İnternet Ortamında Pazarlama*. Seçkin yay., Ankara.

Atif, Y. (2002). Building Trust in E-Commerce. *IEEE Internet Computing*, January-February 2002, 18-24.

Brenner, S.W., ve Goodman, M.D. (2002). In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks. *University of Illinois Journal of Law, Technology & Policy*

Chellappa, R. K. ve Pavlou, P.A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, Volume 15, Number 5/6, 358-368

Culman, M.J. (1995). Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing. *Journal of Direct Marketing* 9 (2) (Spring), 10-19.

Değirmenci, O. (2002). *Bilişim Suçları*. Yayınlanmamış Yüksek Lisans Tezi (Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı), İstanbul.

Doney, P.M. ve Cannon, J.P. (1997). An examination of the nature of trust in buyer–seller relationships. *Journal of Marketing*, 61 (April 1997), 35–51.

Dülger, M.V. (2004). *Bilişim Suçları*, Seçkin Yayıncılık, Ankara.

Ersanel N. (2001). *Siber İstihbarat*. ASAM Yayınları, Ankara.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *The International Journal of Management Science, Omega*, vol. 28, 725-737.

Goodwin, C. (1991). Privacy: Recognition of a Consumer Right. *Journal of Public Policy & Marketing,* 12 (Spring), 106-119.

Grandison, T. ve Sloman, M. (2000). A Survey of Trust in Internet Applications. *IEEE Communications Surveys and Tutorials*, Fourth Quarter, http://www.comsoc.org/pubs/surveys, (erişim tarihi: 12.12.2011)

Gürdilek, R. (2001). "Echelon", *Bilim Teknik Dergisi*, Ekim 2001, 36-37.

Gürkaynak, M. ve İren, A. A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, C.16, S.2, 263-279

Hoffman, D. L., Novak, T. P. ve Peralta, M. (1999). Building Consumer Trust Online. *Communications of the ACM*, Volume 42, Number 4, April, 80-85.

İçli, T. G. (2007). *Kriminoloji*, Seçkin yay., Ankara.

Jarvenpaa, S. L., Tractinsky, N. ve Vitale M. (2000). Consumer trust in an Internet store. *Information Technology and Management,* 1 (2000), 45–71.

Knaous, K., Kartosch, A. ve Reiter, G. (2000). *Combat of Trafficking in Woman For The Purpose of Forced Prostitution*, L.B.Ins.of Human Rights.

Kim, D. J., Song, Y.I., Braynov, S.B.; Rao, H.R. (2005). A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia / practitioner perspectives. *Decision Support Systems,* 40, 143– 165.

Liu, C., Marchewka J.T., Lu, J. ve Yu, C. (2005). Beyond concern-a privacy-trust-behavioral intention model of electronic commerce. *Information and Management*, 42, 289–304.

Moore, D. A., Kurtzberg, T. R., Thompson, L. L. ve Morris M. W. (1999). Long and short routes to success in electronically mediated negotiations: Group affiliations and good vibrations. *Organizational Behavior and Human Decision Processes,* 77, (1), 22–43.

Olson, J. S. ve Olson, G. M. (2000). i2i Trust in E-commerce. *Communications of the Acm*, December 2000/Vol. 43, No. 12, 41-44.

Özel, C. (2001). "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı. *İBD*, İstanbul, C: LXXV, S: 7-8-9, 858-872.

Pandalabs. (2010). *Annual Report 2010*, www.pandasecurity.com, erişim tarihi: 03.12.2011

Papadopoulou, P., Andreou, A., Kannelis, P. ve Martakos, D. (2001). Trust and relationship building in electronic commerce. *Internet Research: Electronic Networking Applications and Policy*, Volume 11, No:4, 322-332.

Poulopoulos, I.E. (2001). *Trafficking in Woman and Children: Greece, a Country of Destination and Transit*, http://www.mmo.gr, erişim tarihi:01.12.2012

Peterson, R.A., Balasubramanian, S. ve Bronnenberg, B. J. (1997). Exploring the implications of the Internet for consumer marketing. *Journal of the Academy of Marketing Science*, 25(4), 329–346.

Salam, A.F.N., Iyer, L., Palvia, P. ve Singh, R. (2005). Trust in E-Commerce. *Communications of the Acm*, Vol. 48, No. 2, 73-77.

Suh, B.ve Han, I. (2002). Effect of trust on customer acceptance of Internet banking. *Electronic Commerce Research and Applications*, 1 (2002), 247–263.

Suh, B. ve Han, I. (2003). The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. *International Journal of Electronic Commerce,* Vol. 7, No. 3, 135–161.

Sever, H. ve Arslan, S. (2010), *İnsan Borsası*, Adalet yayınları, Ankara.

Sever, H. ve Harbigil, T. (2011), Yeni Dünya Düzeninde Modern bir Kölelik: İnsan Ticareti. *Kriminoloji Dergisi*, sayı: 2, 41-69.

Sever, M. (2006). Bilişim Suçları ve Yeni Bir Çatışma: Siber Terörizm. *Suç Analizi-1* (Ed. Mustafa Kaygısız ve Hanifi Sever), Adalet Yayınları, Ankara.

Şen, B. (2007). *Elektronik Gözetim*, http://www.kom.gov.tr/Tr/KonuDetay.asp?BKey=64&KKey=121, erişim tarihi: 13.12.2011

Teo, T.S.H. ve Lui, J. (2007). Consumer trust in e-commerce in the United States, Singapore and China. *The International Journal of Management Science, Omega* 35, 22-38.

Torkzadeh, G. ve Dhillon, G. (2002). Measuring Factors that Influence the Success of Internet Commerce. *Information Systems Research*, Vol. 13, No. 2, 187-204.

Uzel, E. ve Aydoğdu, C. F. (2010). Çalışanların Elektronik Alışverişe Bakış Açıları Hakkında Kaltitatif Çalışma. *Organizasyon ve Yönetim Bilimleri Dergisi*, Cilt 2, Sayı 1, 19-25.

Vijayasarathy, L. R. (2004). Predicting Consumer Intentions to Use Online Shopping: The Case for an Augmented Technology Acceptance Model. *Information and Management*, 41: 747–762.

ZAK (Zirve Araştırma Komisyonu). (2012). Policy Paper, Dijital Ekonomik E-Ticaret Zirvesi ve Fuarı, İstanbul.