Türkiye'de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri

Ahmet Çubukcu[1] Şahin Bayzan[2]

ÖZET

Dünyada bilişim ve iletişim teknolojilerinin her geçen gün hızlı artışı ve bu artışa paralel olarak çeşitlenen ve yenilikler sunan akıllı teknolojik araçların gerek Türkiye'de gerek dünyada özellikle dijital nesil olan çocuklarda ve gençlerde etkin bir şekilde kullanılması, günümüzde dijital vatandaşlık kavramının ortaya çıkmasına sebep olmuştur. Dijital vatandaş, bilgi ve iletişim kaynaklarını kullanırken eleştirebilen, çevrimiçi yapılan davranışların etik sonuçlarının farkında olan, teknolojiyi başkalarına zarar vermeyecek şekilde kullanabilen, internet ortamında iletişim hakkını kullanan, yaptığı paylaşımlarında ve işbirliğinde doğru tutumu sergileyen ve başkalarını da bu yönde teşvik eden vatandaştır. Dijital vatandaşlık ise en genel kapsamı itibariyle teknoloji kullanımına ilişkin hak ve sorumluluklar bütününde yer alan davranış normları olarak ifade edilmektedir.

Günümüz dünyasında iyi bir vatandaş olma algısı iyi bir dijital vatandaş olma yolunda hızlı bir şekilde ilerlemektedir. Çünkü vatandaşlar arası iletişim ve bilgi aktarımı teknolojik araçlar vasıtasıyla dijital ortamda gerçekleşmeye başlamıştır. Bu da sadece gerçek hayatta değil; en az gerçek hayat kadar etki yaratabilecek sanal ortamda teknolojik araçları kullanırken bilinçli, güvenli ve etkin hareket etme gerekliliğini doğurmaya başlamıştır.

Bu çalışmada, dijital vatandaşlık algısı ve dijital vatandaşlığın dokuz boyutunun (dijital erişim, dijital ticaret, dijital iletişim, dijital okuryazarlık, dijital etik, dijital kanun, dijital haklar/sorumluluklar, dijital sağlık ve dijital güvenlik) internetin bilinçli, güvenli ve etkin kullanımı ile sağlanabileceği üzerinde durulmuştur. Bu çalışmayla, birer dijital vatandaş olan etkin internet kullanıcılarına tavsiyeler sunulmakta, Türkiye'de ve dünyada mevcut düzenlemeler irdelenmekte ve bu düzenlemelerin yeni gelişmeler ve ihtiyaçlar doğrultusunda geliştirilmesi için özellikle Türkiye'de atılması gereken adımlardan bahsedilmektedir.

Literatürde internet riskleri; içerik riskleri, temas riskleri ve ticari riskler olmak üzere üç kategoride incelenmektedir. Bu risklerin bilinçli, güvenli ve etkin internet kullanımı konusunda yapılabilecek farkındalık çalışmaları ve gelinen noktada risklerin azaltılmasına yönelik ihtiyaçları karşılayabilecek internet düzenlemeleri ile en az düzeye indirgenebilmesi dijital vatandaş olma algısını güçlendirecektir.

Sonuç olarak, dijital vatandaşın çevrimiçi ortamda hak ve sorumlulukları, interneti etkin ve doğru kullanabilmesinin yanında ilgili diğer internet aktörlerinin de atması gereken adımlar çerçevesinde ele alınarak dijital vatandaşlığın dokuz boyutu, internet risklerinin üç boyutu ile eşleştirilerek mevcut durum ve ortaya konması gerekenler bu çalışma kapsamında sunulmaya çalışılmıştır.

1. Dijital Vatandaşlık Kavramı

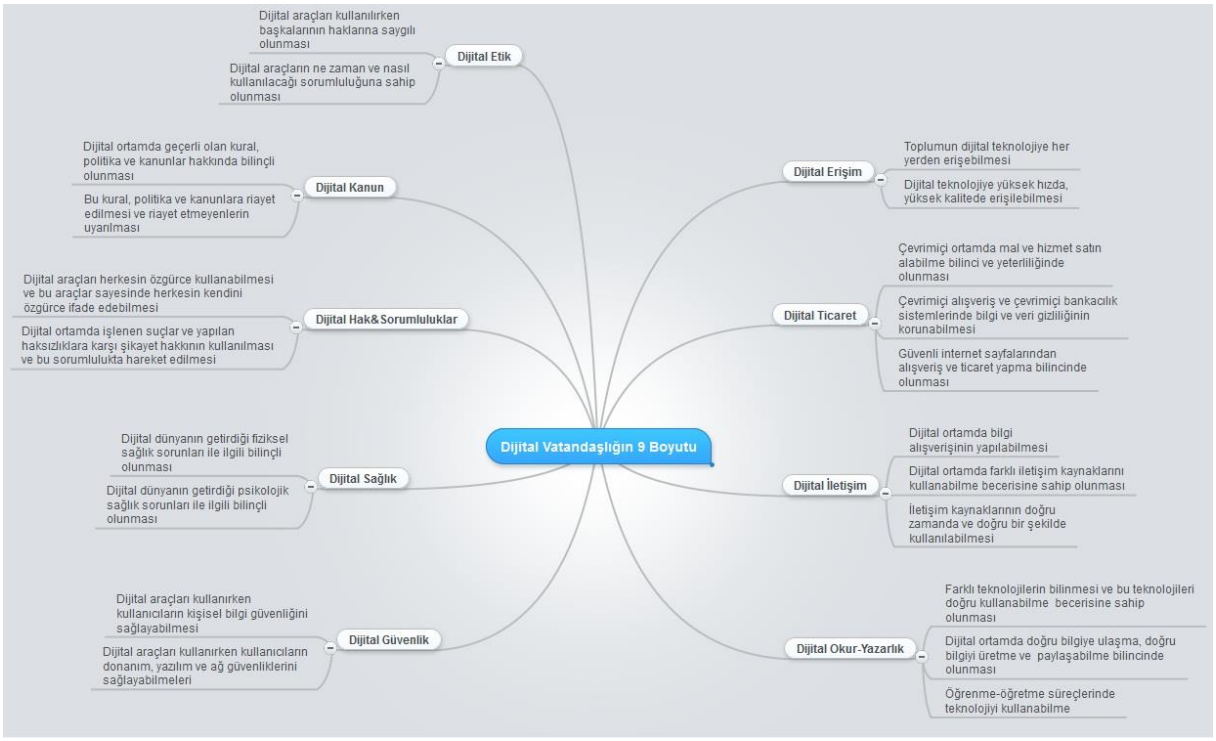
Anayasal ülkelerde, o ülkede yaşayanların devlet tarafından anayasada tanımlanmış haklardan yararlanmaları için o ülkeye vatandaşlık bağı ile bağlı kişilere vatandaş denilmektedir. Vatandaşlığa hak kazanma ve bu hakların bir parçası haline gelinmesi ise vatandaşlığı ifade etmektedir. Bu durumda vatandaşlık hakkı doğumdan itibaren kazanılabildiği gibi, günümüz dünyasında bir kişi başka bir ülkenin vatandaşlığını kazanabilmekte, kendi ülkesinin vatandaşlığından çeşitli nedenlerle ayrılabilmekte veya çifte vatandaş olabilmektedir. Bu durumda vatandaşlığın dijitalliğinin nasıl olduğu ve dijital vatandaşlık hakkının kazanılıp kazanılmayacağı, kazanılıyorsa nasıl kazanıldığı akla ilk gelen önemli sorulardandır.

Bilişim ve iletişim teknolojilerinin gün geçtikçe gelişmekte, bu teknolojilerin kullanıldığı araçlar yaygınlaşmaktadır. Bu gelişmelere paralel olarak bu araçlar sayesinde bilgiye her yerden ulaşılabilmekte ve her birey dünyanın farklı bir coğrafyasındaki ülke vatandaşı ile iletişim kurabilmektedir. Dijital vatandaşlık kavramı bu gelişmelerin bir sonucu olarak çıkmıştır. Diğer bir ifade ile internetin iletişim ve haberleşme noktasında ülke sınırlarını ortadan kaldırması, dünyayı küreselleştirmesi bu kavramın ortaya çıkmasına sebep olmuştur. Teknolojiyi ve teknolojiyle beraber hayatımıza giren dijital araçları doğru kullanmasını bilen, etik kurallara ve kişi haklarına dijital platformda da saygı duyan ve bu araçları güvenlik ve sorumluluk bilinciyle kullanmasını bilen kişiye dijital vatandaş denmektedir. Dijital vatandaşlık ise kısaca, teknoloji kullanımı ile ilgili dijital vatandaşların sorumluluk sahibi davranış normları olarak tanımlanmaktadır (Mossberger, Tolbert, & S. McNeal, 2007).

Dünyanın birçok noktasından dijital teknolojilerin kullanılabiliyor olması, bütün dünya vatandaşlarının eşit hak ve sorumluluklara sahip birer dijital vatandaş olabileceğini göstermektedir. Coğrafi sınırlara bağlı bir vatandaşlık algısının küreselleşmeyle ortadan kalkması, aynı dijital platformların tüm dünya vatandaşları tarafından kullanılabilir hale gelmesi gibi sebepler, dijital vatandaşlık kavramının ortaya çıkmasını neden olmuştur.

Dijital vatandaşlığın her açıdan anlamlarını ortaya koymaya çalışan ve dijital vatandaşlığı 9 boyutta incelemeye çalışan Mike Ribble, dijital araçları kullanım yaşının oldukça düşmesi ve yeni neslin aynı zamanda birer 'dijital yerli' olmasından dolayı dijital vatandaşlık algısının çocuk yaşlarda başlaması gerektiğini ve bu çağdaki çocuklara dijital araçların kullanımının öğretilmesi gerektiğini ifade etmiştir (Ribble, 2011). Çünkü bütün çocuklar vatandaşlık kimliğinden önce artık dijital vatandaşlık kimlikleri ile dünyaya gelmektedirler.

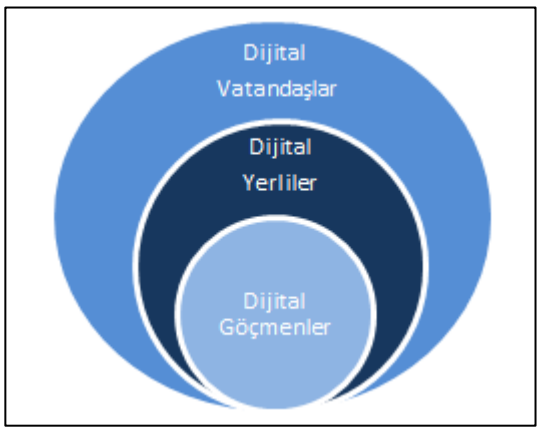
Şekil 1- Dijital Vatandaşlığın 9 Boyutu



Teknolojinin her gün biraz daha gelişmesi, farklı dijital araç ve gereçlerinin kullanımına fırsat tanımaya başlamış ve dijital vatandaşlığın daha fazla boyutlarda ele alınabileceğini göstermiştir. Ribble'in dijital vatandaşlık için önerdiği 9 boyuta bulut bilişim ie akıllı telefonlar, dizüstü bilgisayarlar ve tabletler gibi dijital araçların da eklenip dijital vatandaşlık, 11 boyutta incelenmeye başlamıştır (Alberta, 2012).

Dijital vatandaşlık ve yaklaşım alanları genellikle ilköğretim ve lise kademesindeki öğrencilerin teknolojik ihtiyaçları çerçevesinde özellikle çevrimiçi teknolojileri ve diğer dijital platformları bilinçli ve doğru kullanımı aşamasında öğrencilere, eğiticilere ve sektör temsilcilerine tavsiyeler sunan bir yöntembilim olarak literatüre dâhil olmuştur. Bununla birlikte, dijital vatandaşlığa sadece yeni yetişen genç neslin ihtiyaçları gözetilerek ortaya konması gereken yaklaşımlar olarak bakılmamalı; teknolojiyle sonradan tanışan ve dijital araçları kullanmaya yeni başlayan jenerasyonun da ihtiyaçları doğrultusunda ortaya konması gerekenler olarak ele alınmalıdır. Bunda, 'dijital yerli ve 'dijital göçmen' kavramlarının bundan yaklaşık 12 yıl önce yazar ve eğitimci Marc Prensky tarafından ortaya atılması etkili olmuştur. Prensky, dijital yerlileri 1980'ler ve sonrası doğan, teknolojinin odağında büyüyen bir nesil olarak tanımakla birlikte dijital göçmenleri de dijital dünya ile sonradan tanışan bir nesil olarak tanımlamaktadır (Prensky, 2001). Hatta bundan 10 yıl önce dijital yerli olarak adlandırılan 'Y Kuşağı (1977-1994 arası doğan nesil)' içinde bile dijital göçmenlerin oluşabileceği ve dijital yerlilik kavramının 21. Yüzyılda doğan 'Z Kuşağı' ile daha da boyut değiştirmeye başladığı aşikârdır. Z kuşağı, aynı anda birden fazla iş yapabilen, deneme-yanılma yolunu tercih eden, duyu yetenekleri daha da gelişmiş olan, internet teknolojisini Y Kuşağı ve daha da önce dünyaya gelen 'X Kuşağı (1965-1979 arası doğan nesil)' ve Boomers olarak adlandırılan 1964 öncesi arası doğan nesle tercih eden ve yazılı metinler yerine görselliğe daha fazla önem veren bir nesildir (Evran, 2012). Bu çerçevede dijital vatandaşlık yaklaşım olarak, hem dijital yerlilerin hem de dijital göçmenlerin ihtiyaçlarını kuşak farklılıklarını gözetecek şekilde ele alması gerekmektedir.

Şekil 2 - Dijital Nesiller



2. İnternetin Riskleri

Dijital vatandaşlık algısını en iyi belirleme yöntemlerinden biri hiç şüphesiz dijital vatandaşların çevrimiçi teknolojileri kullanım alışkanlıkları ölçmekten geçmektedir. Dijital vatandaşları çevrimiçi ortamda ne gibi risklerin beklediği ve bu risklere dijital vatandaşların ne ölçüde maruz kaldığı çeşitli araştırmalarla ortaya konmuştur. Bu bölümde de, internetin getirmiş olduğu fırsatlardan daha etkin yararlanmak için internet vasıtasıyla dijital vatandaşların karşılaşabileceği riskler ve yaşayabilecekleri mağduriyetler anlatılmaya çalışılmıştır.

Vanlanduyt ve De Cleyn, internet risk alanlarını beş başlıkta özetlemeye çalışmıştır. Bunlardan birincisi, sosyal hayatı ve sosyal ilişkileri olumsuz etkilemesi; ikincisi, pornografi, şiddet ve uygun olmayan bir dil üslubuna maruz kalınması; üçüncüsü, fiziksel sağlığa olumsuz etkiler yaratması; dördüncüsü, zamanı etkin planlayamamaya sebep olması ve son olarak da ticari istismar ve aşırı tüketim risklerine sebep olmasıdır (Valcke, Bonte , De Wever , & Rots , 2010).

Won Kim ve arkadaşları, internetin karanlık yüzü adlı makalelerinde internet risklerini teknoloji odaklı ve teknoloji olmayan odaklı olmak üzere iki grupta incelemiştir. Teknoloji odaklı olarak spam, malware, korsanlık (hacking) faaliyetleri, Dos atakları (Denial of service attacks: Bir servisi çalışmaz hale getiren siber saldırılar), oltalama (phishing) faaliyetleri, reklam dolandırıcılığı ve dijital hakların ihlalleri olarak sıralamışlardır. Teknolojik olmayan odaklı risklerde ise çevrimiçi hırsızlık ve dolandırıcılık, fiziksel şiddet (fuhuş, çocuk

istismarı vb.), siber zorbalık, gizlilik ihlalleri, suça yardım ve yataklık etme (uyuşturucu temini, bomba yapımı vb.) ve yasadışı kumar olarak sınıflandırmışlardır (Kim, Jeong, Kim, & So, 2011).

Türkiye'de bilişim ve iletişim sektörünü düzenleyen ve denetleyen üst kurul Bilgi Teknolojileri ve İletişim Kurumu (BTK)'na bağlı faaliyetlerin sürdüren Telekomünikasyon İletişim Başkanlığı (TİB) internetin bilinçli ve güvenli kullanımına yönelik yapmış olduğu bilinçlendirme faaliyetlerinde internetin risklerini dokuz başlıkta incelemiştir. Bunları, yanlış ve/veya zararlı bilgiye erişim, siber zorbalık, sanal dolandırıcılık, kişisel bilgilerin paylaşımı, zararlı yazılımlar, pornografi/çocuk istismarı/fuhuş, oyun ve internet bağımlılığı, yabancılarla çevrimiçi ve çevrimdışı iletişim ve şiddet/nefret/ırkçılık faaliyetleri olarak özetlemiştir.

İnternet riskleri sınıflandırmalarında genellikle internetteki kumar ve oyun bağımlılıkları göz ardı edilmektedir. Başka bir deyişle internetin fiziksel ve ruhsal sağlığa etkileri internetin riskleri sınıflandırmalarında çok fazla vurgulanmamaktadır. Bu durum, internet risklerinin daha çok internetin içerik olarak dijital vatandaşları etkilediği olumsuz yanlarının göz önünde bulundurulmasından kaynaklanmaktadır. İnternet risklerinin yanı sıra internet kullanımına bağlı oluşan risklere ilişkin çalışmalarda bulunan Cem Çuhadar, sorunlu internet kullanımına vurgu yapmıştır (Çuhadar, 2012). Yapılan çalışmada, sorunlu internet kullanımı daha önceden var olan psikiyatrik bozukluk semptomu olarak evde veya işte internet kullanım dürtüsünü kontrol edememe olarak tanımlanmıştır (Ceyhan, 2010)& (Kim & Davis, 2009). Bu bir süreç olarak, önce tercih, sonra sırasıyla alışkanlık, saplantı ve bağımlılığa dönüşme evrelerinden oluşmaktadır (Johnson, 2009). Sorunlu internet kullanım süreci, internet bağımlılığı, kumar ve madde bağımlılığı ile paralellik gösteren etki ve sonuçlara sahiptir (Doğan, Işıklar, & Eroğlu, 2008). Sorunlu internet kullanımı ve internet bağımlılığı aynı şey olmasalar da bir zincirin halkaları şeklinde değerlendirilmekte ve benzer şekilde, internette bilinçsizce harcanan vakit tüm bu sebeplerin başını çekebilmektedir (Çuhadar, 2012).

İnternetin riskleri sınıflandırılmalarında şimdiye kadar yapılmış en kapsamlı sınıflandırmalardan bir tanesi de De Moor ve arkadaşlarının yapmış olduğu çalışmadır. De Moor ve arkadaşları internetin risklerini Şekil-1'de de görüldüğü üzere 3 temel başlık altında inceleyip içerik, temas ve ticari riskler olmak üzere belirlemişlerdir (Valcke, Bonte , De Wever , & Rots , 2010). Bu çalışma kapsamında, De Moor ve arkadaşlarının belirlemiş olduğu 3 risk sınıflandırmasının alt başlıkları farklı açılardan bakılarak incelenmiştir.

2.1. İçerik Riskleri

İnternet içerik riskleri, web sitelerinin barındırdığı görsel ve yazılı negatif içeriklerdir. Bu içerikler farklı şekillerde internet kullanıcılarını olumsuz olarak etkileyebilmektedir. Kışkırtıcı şiddet söylemleri ve görselleri, nefret söylemleri ve görselleri, ırkçı söylemler ve görseller, cinsellikle ilgili içerikler, içeriğin derecesine göre kullanıcılar üzerinde olumsuz etkiler bırakabilmektedir. Bununla birlikte doğru olmayan yanlış ve zararlı bilgiler de, bu bilgilere ulaşan her internet kullanıcısı için ayrı bir risk oluşturmakta ve internette bilgi kirliliğine sebep olmaktadır. Bu tür doğru olmayan bilgiler büyük bir risk oluşturmakla birlikte, internet kullanıcılarının da doğru bilgiye ulaşmasını zorlu ve karmaşık hale gelmesine sebep olmaktadır.

2.2. Temas Riskleri

Temas riskleri, çevrimiçi ve çevrimdışı iletişimde riskler olmak üzere incelenmektedir. Çevrimiçi iletişim, siber zorbalık, çocukların cinsel istismarı ve gizlilik ihlalleri olmak üzere sınıflandırılmakla beraber tüm bu risklerin çevrimiçi ortamda özellikle çocukların tanımadığı insanlarla iletişime geçerek ve istismarcıların kendilerini olduğundan farklı göstererek ('grooming': kötü niyetli irtibat) çocuklarla iletişime geçmesi sonucu ortaya çıkmaktadır. Çevrimiçi bu temasın gerçek hayatta yüz yüze buluşma noktasına taşınması ise çevrimdışı iletişim olarak adlandırılmaktadır.

Siber zorbalık, bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme, kaba davranma ve kötü söz söyleme davranışlarının tümü olarak tanımlanmaktadır. Olayın daha çok teknik yönünü içeren elektronik zorbalık (electronic bullying) ve diğeri ise olayın daha çok psikolojik yönünü içeren elektronik iletişim (e-iletişim) zorbalığı (e-communication bullying) olmak üzer iki çeşit zorbalıktan bahsedilebilir (Arıcak, 2011).

Cinsel istismar, bir kişinin kendi rızası dışında cinsellik içeren bir eyleme maruz kalmasıdır. Eğer bu eylem internet üzerinden yapılıyor ise çevrimiçi (online) cinsel istismar olarak adlandırılmaktadır. Cinsel istismar, söz ile yapılabileceği gibi eyleme dönüştürülerek şiddet ve zorlama şeklinde de gerçekleştirilebilir. İnternet ortamında çevrimiçi iletişimle başlayıp, çevrimdışı buluşmayla noktalanan internet arkadaşlıkları cinsel istismarlara neden olabilmektedir. Çevrimiçi cinsel istismarın en büyük nedeni, internet ortamında kendini farklı

kişilik ve yaş gruplarında gösteren yabancı kişilerle bilinçsiz bir şekilde sonucunu düşünmeden kurulan arkadaşlıklardır.

Gizlilik ihlalleri, internetin anonim yapısı gerekliliği sonucu ortaya çıkan ihlalleri oluşturmaktadır (Valcke, Bonte , De Wever , & Rots , 2010). Ev adresi, kimlik numarası, telefon numarası, anne kızlık soyadı, aile bireylerinin adı ve diğer kişisel bilgilerin internet ortamında doğrudan veya dolaylı olarak paylaşılması sonucunda da gizlilik ihlalleri çok rahatlıkla kendine ortam bulabilmektedir.

2.3. Ticari Riskler

Ticari risklerin en büyük ayağını dijital vatandaşların kişisel verilerinin istismar edilmesi sonucu kimlik avı/oltalama (phishing) ve benzeri yöntemlerle dolandırılması vakaları oluşturmaktadır. Tüm bunları sosyal mühendislik veya kimlik hırsızlığı başlığı altında toplayabiliriz.

Kimlik hırsızlığı (identity theft), bir başkasına ait kişisel bilgilerin yetkisiz olarak kullanılması suretiyle işlenen dolandırıcılık yöntemidir. Kredi kartı ve internet bankacılığı bilgileri, şifre ve parolalar, elektronik posta ve diğer önemli kişisel bilgilerin bir başkası tarafından çıkar sağlamak amacıyla kullanıldığı bir dolandırıcılık türüdür. Kimlik hırsızlığında kullanılan en önemli yöntemlerin başında oltalama(Phishing) ve zararlı (casus) yazılımlar (keylogger, spyware) gelmektedir. Oltalama, dolandırıcıların banka, kredi kartı bilgilerini güncellemek amacıyla sahte e-posta göndererek kişileri sahte web sitesine yönlendirerek kişisel bilgilerin girilmesi sağlanarak ele geçirilmesi gibi yöntemleri kapsamaktadır. Gönderilen e-postanın gerçek kuruluştan geldiğini göstermek için kuruluşa ait logo, gerçek web sayfasının birebir kopyası ve diğer sahte bilgiler kullanılabilmektedir. Diğer bir yöntemde zararlı yazılım içeren siteler yoluyla kişilerin bilgisayarlarına keylogger, truva atı ve diğer casus yazılımları yüklemek için zararlı programların kullanıcının dikkatini çekmek için isminin değiştirilip bilgisayar indirilmesi sağlanarak yapılmaktadır.

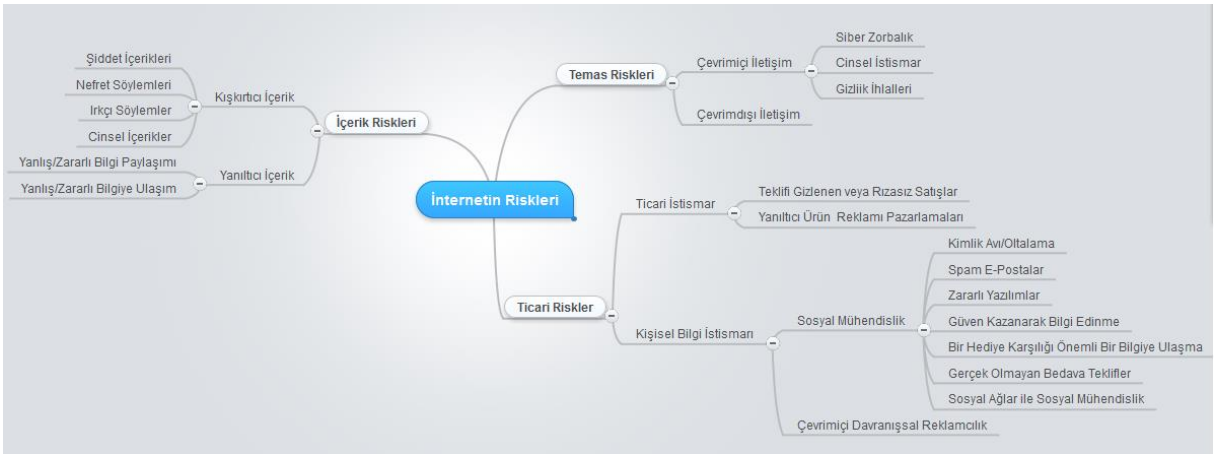
Diğer zararlı (casus) yazılımlar ise tanıtım, kişisel bilgi toplama veya kullanıcıların onayı almadan bilgisayarın yapılandırmasını değiştirme gibi belirli davranışları gerçekleştiren yazılımlar için kullanılan genel bir terimdir. Casus yazılımlar, genellikle başka bir program kurulurken, kullanıcının da onayı ile bilgisayara kurulan ve kurulduktan sonra kişinin internetteki gezme alışkanlıkları ilgili bilgi toplayan ve bu bilgileri internet üzerinden kötü niyetli kişilere iletebilen yazılımlardır.

Bunların dışında internet üzerinden yapılan gerçekliği olmayan bedava veya gerçekçi olmayan ticari teklifler de kullanıcıları farklı web sitelerine yönlendirmek suretiyle kişisel bilgileri elde etme amacı gütmektedir. İstenmeyen e-postaları (spam) da bu kategoride değerlendirmek gerekir. Bu tür e-postalarda kullanıcının hiçbir talebi olmadan e-posta adresine gönderilmiş zararlı ekler veya yazılımlar içeren e-postalardır. Bu e-postaların açılması kişisel bilgilerin bu e-postayı gönderenlerin eline geçmesine de aracılık edebilmektedir.

Sosyal mühendislik yöntemleri kullanıcıları kandırıp, mali kazanç sağlama amacıyla sıklıkla kullanılabilmektedir. Bunların dışında, dolandırıcılık amacı gütmeyip kullanıcılara teklifi gizlenmiş bir şekilde rızasız satışlar gerçekleştirebilme veya yanıltıcı ürün katalogları ile reklam ve pazarlama stratejileri izleme suretiyle de dijital vatandaşlar ticari risklerle karşı karşıya kalabilmektedir.

Her ne kadar bir risk unsuru olup olmadığı tartışmalı bir konu olsa da Çevrimiçi Davranışsal Reklamcılık (ÇDR) son zamanların popüler konu başlıklarından birini oluşturmakta ve bu konuda farklı görüşler ortaya konulabilmektedir. ÇDR, dijital vatandaşların ziyaret ettikleri web sitelerinin sınıflandırılması ve kişisel iletişimlerinin analizi sonucu vatandaşlara da çoğu zaman izlendiklerinin haberi doğrudan veya dolaylı yönden verilmeden internet ortamında vatandaşa özel ilgi alanlarına göre reklam ve pazarlama içeriklerinin sunulması yöntemidir. ÇDR uygulamaları asıl olarak kullanıcının bilgisayarına sunucular tarafından bırakılan çerezler (cookie) vasıtasıyla yürütülmekle birlikte birçok ÇDR uygulaması tarayıcıların kendi çerezlerini değil, flash programının çerezlerini de kullanılabilmektedir (Kırlıdoğ, 2013). 2002/58/EC sayılı Avrupa Birliği Direktifi ve bu Direktifi izleyen diğer çalışmalar ile web sitelerinin kişisel bilgileri toplaması ve çerez kullanımı ile bilgilendirme koyma zorunluluğu getirilmesine rağmen bunun uygulanabilirliği sektörde tam işlememektedir. Ayrıca Türkiye'nin de henüz kişisel verilerin işlenmesi ile ilgili Bilgi Teknolojileri ve İletişim Kurumu (BTK)'nun elektronik haberleşme sektöründe kişisel verilerin İşlenmesi ve gizliliğinin korunması hakkında yönetmeliği dışında herhangi bir yasası mevcut değildir.

Şekil 3 – İnternetin Riskleri



3. Dijital Vatandaşlık Algısında İnternet Risk Analizi

İnternetin riskleri çeşitli boyutlarda incelenmiş olsa da şimdiye kadar yapılan çalışmalar internette bir dijital vatandaşın karşı karşıya kalabileceği riskler belirli başlıklar altında incelenmeye çalışılmıştır. Dijital vatandaşlık ise literatürde farklı sınıflandırmalara şimdilik tabi olmadan birçok kaynak dijital vatandaşlığı Mike Ribble'ın belirlediği ölçülerde, dokuz alan içerisinde incelenmiştir. Bu çalışmada ise, dijital vatandaşlığın her bir boyutunun internet ortamındaki risklerle ne gibi bir bağlantısı olduğu ve her bir boyut içerisinde internet ortamında nelere dikkat edilmesi gerektiği özetlenmeye çalışılmıştır. Yapılan çalışma sonucunda da Tablo 1'de Mike Ribble'ın belirlediği 9 dijital vatandaşlık boyutunun De Moor ve arkadaşlarının belirlediği 3 temel internet risklerinden hangilerinin etkisi altına girebileceği analiz edilmeye çalışılmıştır.

Dijital Erişim Boyutu: Çevrimiçi ortamda zararlı bilgiye erişim internetin içerik ve ticari riskleri olmak üzere iki boyutta karşımıza çıkabilmektedir. Bir dijital vatandaş, kışkırtıcı bir içeriği de erişim sağlayacağı gibi yanıltıcı bir içeriği de erişim sağlayabilir. Ayrıca, bir dijital vatandaş zararlı erişim kaynaklarının kurbanı olarak ticari istismara uğrayabilir veya kişisel bilgi istismarı yöntemiyle başta dolandırıcılık, zararlı yazılım ve bilgi hırsızlığı olma üzere çeşitli senaryolara maruz kalabilir. Bu yüzden iyi bir dijital vatandaş çevrimiçi ortamda eriştiği bilgi hakkında iyi analiz yapabilmelidir.

Dijital Ticaret Boyutu: Çevrimiçi alışveriş ve bankacılık sistemlerinin kullanımı ve bu sistemleri kullanırken ticaret yapabilmek kadar bu işlemleri gerçekleştirirken kişisel verilerin korunumu ve güvenli sayfalardan işlem yapabilmek de önem arz etmektedir. Bir dijital vatandaşın herhangi bir veri kaybına sebebiyet vermeden güvenli sayfalardan ticari faaliyetlerini sürdürebilmesi ve çevrimiçi alışveriş ve bankacılık sistemlerini kullanırken güvenlik ilkelerine riayet edilebilmesi gerekmektedir. Aksi takdirde, çevrimiçi ortamda birçok ticari risk ile karşı karşıya kalınabilmektedir.

Dijital İletişim Boyutu: Dijital ortamda iletişimin büyük bir bölümünün internet teknolojisiyle çevrimiçi ortamda ve özellikle sosyal ağları kullanılarak yapılması internette çeşitli temas riskleriyle karşı karşıya kalınabileceğini göstermektedir. İletişim esnasında karşı tarafla özellikle tanımadığımız kişilerle, kişisel bilgilerin çok rahatlıkla paylaşılması büyük bir gizlilik ihlali olarak karşımıza çıkmaktadır. Ayrıca özellikle ergenler arasında popüler olan siber zorbalık vakaların dijital iletişim neticesinde ortaya çıkması ve literatürde 'grooming' olarak bilinen kişinin kendini farklı biri olarak göstererek internette özellikle çocukların güvenini kazanarak onlarla iletişime geçmesi cinsel istismarlara varacak sonuçları internette doğurabilmektedir.

Dijital Okur-Yazarlık Boyutu: Dijital ortamda okur-yazarlık dijital vatandaşlığın en önemli ayaklarından birini oluşturmakla beraber bu kavram, bilinen okur-yazarlıktan bile daha önemli bir hal almaya başlamıştır. Çünkü günümüz çağında bir çocuk, eğitim-öğretim faaliyetlerinden önce dijital araçları kullanmaya ve bu araçlar hakkında bilgi sahibi olmaya başlamaktadır. İnternet okur-yazarlığı ise internetin doğru kullanımı, doğru bilgiye ulaşma çabası ve internette doğruluğundan emin olduğumuz bilginin paylaşımı ve bu sayede doğru bir öğrenme-öğretme süreçleri gerçekleştirme aşamalarını kapsamaktadır. Aksi takdirde doğru bilgi etkileşiminin yapılamaması internete hem içerik hem temas hem de ticari risklerin oluşumuna kadar giden bir süreci başlatacaktır. İnternet risklerinin oluşmasındaki en büyük etken de, internette doğru olmayan veya başka bir tabirle istismar edici, aldatıcı veya yanıltıcı bilgilerin üretilmesi ve paylaşılmasından kaynaklanmaktadır.

Dijital Etik Boyutu: Dijital araçları doğru kullanmak kadar etik kullanmak da önemlidir. Çevrimiçi ortamda internet araç ve gereçlerini kullanırken başkalarının haklarına saygılı olacak sorumlulukta hareket etmek önemlidir. Örneğin, doğru bil dil üslubu ve ahlaki davranış normlarını çevrimiçi ortam da sürdürebilmek etik olgusu içerisinde gösterilebilir. Etik olgusuna internet üzerinde dikkat etmemek içerik riskleri içerisinde özellikle kışkırtıcı içeriklerin paylaşılması ve temas risklerinde de siber zorbalık vakalarının oluşumuna zemin hazırlayabilmektedir. İyi bir dijital vatandaşın internette de etik olgusuna dikkat etmesi gerekmektedir.

Dijital Kanun: Tüm dijital ortamda dikkat edilmesi gereken kurallar olduğu gibi özellikle internet ortamında da dikkat edilmesi gereken kurallar bütünü mevcuttur. Bir dijital vatandaşın, gerçek hayatta suç olan tüm davranışların internette de yapılmasının suç olduğu bilinciyle hareket etmesi ve internette suç işleyenleri ilgili mercilere şikâyet etmesi gerekmektedir. Bu bağlamda, internetin üç risk boyutuyla da içerikler üretmek ve bu içerikleri paylaşmak suç teşkil edebilmektedir.

Dijital Hak & Sorumluluklar: İnternet, dijital araçlar içerisinde önemli bir yere sahip olmakla beraber çoğu dijital araç, internet teknolojisini de sunmaya başlamıştır. İnternet, herkesin kendini özgürce ifade edebildiği bir mecra olabilmesinin yanı sıra bu ifade özgürlüğünün başkalarının kişisel haklarını ihlal etmeyeceği ölçüde sınırlı olabileceği, çevrimiçi ortamın hak ve sorumluluk çerçevesindeki denge noktasını oluşturmaktadır. Örneğin, internetten bir bilgi araştırırken alıntı yapılacak bilginin ne şekilde kullanılabileceği, o bilgi üstündeki fikri sınai haklar ve bu haklar çerçevesindeki mevcut olan çevrimiçi sorumlulukları mevcuttur. Benzer şekilde, internet ortamında yapılan haksızlıklar ve internet ortamının barındırdığı yasadışı içeriklere karşı bir dijital vatandaşın sorumlulukları mevcuttur. Bu noktada, internetteki bütün risk gruplarına karşı hak ve sorumluluklarımız mevcuttur.

Dijital Sağlık: Dijital ortamda sağlık faktörü genellikle olumsuz yönleriyle karşımıza çıkmaktadır. Dijital araçları ve özellikle çevrimiçi teknolojiler ve bilgisayarları kullanırken gerek fiziksel gerek psikolojik gerekse de ruhsal birçok hastalık türüne bir dijital vatandaş maruz kalabilmektedir. Bunların başında antropometri bilimi içinde incelenen kas-iskelet rahatsızlıklarından, internet ve oyun bağımlılığına ve hatta internetin içerik riskleri sonucu özellikle çocuklarda oluşan ruhsal bozukluklara kadar birçok sağlık problemi ile karşılaşılabilmektedir. Bu doğrultuda, internetin içerik ve temas riskleri dijital vatandaşlığın dijital sağlık boyutunu doğrudan etkileyen faktörler arasındadır.

Dijital Güvenlik: Dijital ortamda güvenlik en az gerçek hayat fiziksel güvenliği kadar önemli hale gelmeye başlamıştır. 2013 yılı itibari ile siber güvenlik, siber farkındalık gibi kavramların daha fazla konuşulmaya başlanacağı öngörülmektedir (Kıvırcık, 2013). Çünkü siber güvenlik açıklıkları ve dijital ortamda yapılan saldırıların ve istismarların her geçen gün artması ülkelerin teknolojik sistemlerini, bireylerin dijital cihazlarını ve dolayısıyla yapılan tüm faaliyetleri etkileyecek sonuçlar doğurabilmektedir. Dijital veya siber güvenlik kavramları internet boyutuyla ele alınacak olursa internet güvenliği ve güvenli internet kavramlarının her geçen gün daha da önemli hale gelmeye başlayacağı büyük olasılıktır. Bir dijital vatandaş ise kişisel bilgi güvenliğine internet üstünde oldukça dikkat etmeli ve internet ortamında gezindiği sayfaların güvenilirliğine dikkat etmelidir. Ayrıca, dijital vatandaşın bilgisayar ve internet ortamında çeşitli kurum ve kuruluşlar vasıtasıyla sağlanan filtreleme programları, güvenli internet paketleri ve anti-virüs programları içeren internet koruma paketlerine kendi güvenliği açısından sahip olması gerekmektedir. Aksi takdirde internet, hem içerik hem temas hem de ticari risk boyutlarıyla bir dijital vatandaş üstünde güvenlik açısından ciddi risk unsurları oluşturabilmektedir.

Tablo 1 - Dijital Vatandaşlık/İnternet Risk Analizi

	İçerik	Temas	Ticari
Dijital Erişim	*		*
Dijital Ticaret			*
Dijital İletişim		*	
Dijital Okuryazarlık	*	*	*
Dijital Etik	*	*	
Dijital Kanun	*	*	*
Dijital Hak & Sorumluluklar	*	*	*
Dijital Sağlık	*	*	
Dijital Güvenlik	*	*	*

4. Dijital Vatandaşlığın Çevrimiçi Boyutu

Dijital dünya, bilgiye daha hızlı ve etkin erişim, alternatif ve küresel dünyada başkalarını daha iyi anlama ve uzaktaki bir dijital vatandaş ile daha pratik ve basit bir şekilde iletişim kurma ve bilgi paylaşma imkânı doğurmuştur (Odabaşı, 2012). Dijital dünyada dijital vatandaşlık, dijital araçların kullanıldığı her durumda geçerli olan davranış normlarını tanımlamakla beraber günümüz dijital platformların kullanımının büyük bir çoğunluğu çevrimiçi teknolojiler yani internet aracılığıyla gerçekleşmektedir. Bu yüzden, dijital vatandaşlık algısını, çevrimiçi teknolojileri kullanım alışkanlıkları çerçevesinde değerlendirmek gerekmektedir.

4.1. Dünyada Dijital Vatandaşlık

Dijital vatandaşlık kavramı gün geçtikçe önem kazanmaya başlayan ve birçok önemli bilişim firması tarafından da gündeme getirilen bir kavram haline gelmeye başlamıştır. Örneğin, dijital vatandaşlığı çevrimiçi teknolojiler boyutuyla inceleyen Microsoft, çevrimiçi dünyanın hem risklerini hem fırsatlarını iyi bilerek bu çerçevede bir dijital vatandaşın uygun davranış normları oluşturmasının gerekliliğine değinmektedir. Bu konuda Microsoft özellikle çocukların çevrimiçi ortamda korunumuna ilişkin temelde 4 politika belirlemiştir. Bunlar: 1. Güvenlik araçları geliştirme 2. Eğitim ve rehber materyalleri üretme 3. Çevrimiçi ortamdaki ihlâlleri bildirecek güçlü ihbar mekanizmaları oluşturma 4. Kolluk kuvvetleri, devletler ve sektör ile işbirliği yapma. Bu çerçevede Microsoft, Windows işletim sistemindeki ebeveyn denetim ayarlarını devamlı geliştirmekte, internet koruma paketlerini kullanıcılarına sunmakta ve oluşturmuş olduğu güvenlik merkezi portalı üzerinden çeşitli tavsiyeler sunmakta ve bilinçlendirme faaliyetleri yapmaktadır. Ayrıca Microsoft, dijital vatandaşlık konsepti kapsamında bir eğitim rehber seti oluşturarak çevrimiçi teknolojiler konusunda hem ailelere hem çocuklara çeşitli tavsiyelerde bulunmaktadır (Microsoft, 2013).

Dijital vatandaşlık ile ilgili Google da, Youtube'un uygun kullanımına ilişkin interaktif bir dijital vatandaşlık rehberi yayımlamıştır (Google, 2013). İlgili rehberde, Youtube'un genel kullanım politikaları, olumsuz bir içeriğin Youtube'a ihbarı, siber zorbalık ve telif ihlalleri ile çevrimiçi gizliliğin korunmasına kadar birçok bilinçlendirici doküman yer almaktadır.

Dijital vatandaşlık kavramı literatüre daha tam olarak yerleşemese de konu ile paralel olarak çevrimiçi teknolojilerin güvenli ve doğru kullanımı hususunda özellikle çocukların korunumuna ilişkin çeşitli uluslararası kuruluşlar tarafından tavsiye kararları yayımlanmakta ve bu konuda çeşitli stratejiler oluşturulmaktadır. OECD(Ekonomik Kalkınma ve İşbirliği Örgütü), CoE (Avrupa Konseyi), ITU(Uluslararası Telekomünikasyon Birliği) ve Avrupa Birliği Komisyonu gibi birçok uluslararası önemli kuruluş konu ile ilgili birçok girişimde bulunmakta ve ülkelere çeşitli tavsiyeler sunmaktadırlar. Bunlardan en önemlisi ve günceli, çocukların internete daha güvenli bağlanabilmeleri için aralarında Microsoft, Samsung, Apple, Facebook ve Vodafone gibi önemli şirketlerin bulunduğu sektöründe lider 28 şirketin Avrupa Birliği Komisyonu önderliğinde toplanarak hazırladıkları ve 2011 yılı sonunda mutabık kaldıkları bir eylem planı olmuştur (DigitalAgenda, 2011).

Eylem planının öncelikli amaçları arasında, zararlı içeriklerin resmi kanallara kolay ihbarı, yaşa uygun gizlilik ayarlarının sağlanması, ebeveyn kontrollü internet içeriğinin filtrelenmesine ilişkin yazılım ve donanım araçlarının geliştirilmesi, çevrimiçi çocuk istismarı içerikleriyle mücadele ve giderek daha genç yaşta interneti kullanmaya başlayan bir kuşağın ihtiyaçlarının daha kolay karşılanabilmesine yönelik maddeler yer almıştır. Şu an, eylem planı dâhilinde 31 şirket mevcut olmakla beraber plan stratejisinde 5 çalışma grubu oluşturulmuştur.

Dünyanın en çok kullanılan sosyal ağı Facebook, oluşturulan plan çerçevesinde ve daha önceki çalışmalarına paralel, kapsamlı bir yardım merkezi portalı oluşturmuştur (Facebook, 2013). Portalda, çevrimiçi ortamda güvenlik ve gizlilikten, çalınan hesaplarla ilgili neler yapılabileceğinden ve paylaşılan olumsuz bir içeriğin ihbarına kadar birçok konuda Facebook kullanıcılarına tavsiyeler sunmaktadır.

Dijital vatandaşlık ile ilgili oluşturulan önemli bir standart, ISTE (The International Society for Technology in Education) organizasyonuna aittir. ISTE, dünyanın farklı noktalarından üyeleri olan ve teknolojiyi ilköğretim ve lise çağındaki öğrencilerin etkin bir şekilde kullanmaları için eğiticilerin ve öğrencilerin dijital ortamdaki eğitim-öğretim faaliyetlerinin geliştirebilmesine yardımcı olan bir organizasyondur. Bunun için ISTE, eğitimde NETS (The National Educational Technology Standards) standartlarını oluşturmuştur. NETS standartları, öğrenciler, öğretmenler, yöneticiler, eğitim koçları ve bilgisayar eğitimcileri için ayrı ayrı oluşturulmuştur. NETS, dijital çağda öğrenme ve öğretme kabiliyetlerinin geliştirilmesi ve dijital öğrenme ve öğretmenin tüm dünyada tanınır hale gelmesi için oluşturulan standartlar kümesidir. Dijital vatandaşlık ve teknolojide öğrenme-öğretme süreçleri ile ilgili detaylı açıklayıcı bilgiler sunmasa da NETS, küçük yaşlardan itibaren dijital vatandaşlığın yaratıcı

düşünce ile birleşip bilişim ve iletişim teknolojilerinde nasıl inovasyona dönüşebileceğine ilişkin bir şematik analiz sunmaktadır.

4.2. Türkiye'de Dijital Vatandaşlık

Türkiye'de dijital vatandaşlık algısına ilişkin yapılmış tek çalışma 8 ilden 20 pilot okul; 1848 çocuk ve genç (ortaokul ve lise) ile 1961 aile üzerinde uygulanmış ve önemli bulgularla karşılaşılmıştır. Yapılan çalışma çevrimiçi teknolojilerinin gelişimine paralel olarak dijital vatandaşlığın çevrimiçi boyutu olan internet üstünde yoğunlaşmış ve interneti kullanım alışkanlığına göre dijital vatandaşlık algısı ölçümlenmeye çalışılmıştır.

Çalışmaya göre, ailelerin %11'i son bir yılda internette en az bir zararlı eylemde bulunduklarını açıklamış, %66'sı interneti çocukları için faydalı gördüklerini açıklamış ancak yine ailelerin %67'si internetin aile ilişkilerini olumsuz etkilediklerini söylemişlerdir. Çocuğum benden daha iyi internet kullanıyor diyen ailelerin oranı %90 olmakla beraber çocuğunun internetten olumsuz etkilendiğini belirten aile oranı ise %48'i bulmuştur. Çocukların %26'sı ise internet bağımlısı olduklarını kabul etmekle beraber %81'i evlerinde herhangi bir internet filtreleme paketi olmadığını söylemişlerdir. Türkiye'de 2011 Kasım ayında devreye giren Güvenli İnternet Hizmeti'ni ise ailelerin %54,7'si yeterli bulmamaktadır (Ocak, 2013).

4.2.1. Dijitalleşen Dünyada Türkiye

Türkiye'de dijital vatandaşlık kavramından bahsedebilmek için öncelikli olarak Türkiye'nin internet tarihine göz atmak gerekir. Çünkü internet, dijital dünyanın en büyük buluşlarından ve en önemli araçlarından bir tanesini oluşturmaktadır.

1986 yılında ilk geniş alan ağı TÜVEKA (Türkiye Üniversiteler ve Araştırma Kurumları Ağı) kuruldu. Bunu 1991 yılında ODTÜ-TÜBİTAK işbirliğiyle kurulan TR.NET ilk İnternet servis sağlayıcı olarak, ICANN ve ODTÜ ".tr" alan adı dağıtımına başladı. 1992 yılında Hollanda'ya ilk deneysel bağlantı gerçekleştirildi. 1993 yılında ODTÜ'den 64Kbps kapasiteli ilk internet bağlantısı gerçekleşti. Türkiye'nin internete resmi bağlantısı 1993 yılı ile başlamıştır. 1994 yılında Ege Üniversitesi'nden internet bağlantısı gerçekleştirilerek, kurumlara ve firmalara ilk internet hesapları verilmesine başlanmıştır. 1995 yılında Bilkent ve Boğaziçi Üniversiteleri'nden internete bağlantı gerçekleştirildi. 1996 yılında İstanbul Teknik Üniversitesi'nden internete bağlantı gerçekleştirildi. Yine bu tarihte Türkiye'nin ilk internet altyapısı olan TURNET oluşturuldu. 1997 yılında akademik kuruluşların internet bağlantısını sağlayan omurga olan ULAKNET (Ulusal Akademik Ağ) oluşturuldu. 1998 yılında Ulaştırma Bakanlığı bünyesinde İnternet Üst Kurulu kuruldu. 1999 yılında TTNet, TURNET'in yerini alarak internet omurgasını oluşturdu. 2000 yılına kadar geçen süre içerisinde Türkiye'de internet kullanımının özellikle üniversitelerde kullanıldığı ve internet altyapısının Türkiye'de oluşturulmaya başlandığı gözlenmiştir.

Tüm bu gelişmeler radikal değişiklikleri de tetikleyen bir etmen olmuştur. Kurumların, şirketlerin, okulların, üniversitelerin, televizyon kanallarının, gazetelerin, dergilerin, hipermarketlerin, parlamentoların, şehirlerin, ülkelerin dijital ortama taşınmalarını gerekli kılmıştır. Günlük hayatta yapılabilecek birçok işlemlerin elektronik ortama aktarılması ve bunların kullanıcıların hayatını kolaylaştırması sebebiyle dijital ortam, birçok riskler barındırmasına rağmen dijital vatandaşları cezbetmekte ve hayatlarını olabildiğince kolaylaştırmaktadır (Bayzan, 2011).

Her geçen gün geniş kitleler tarafından internetin ulaşılabilir hale gelmesi ve buna bağlı olarak hızla yaygınlaşması, toplumsal gelişime önemli katkı sağlamaktadır. Özellikle genişbant internet, Web 2.0 teknolojileri, 3G ve şimdi de fiber internetten bahsetmeye başladığımız bir dünyada internet vazgeçilmez bir platforma dönüşmeye başlamıştır. İnternetin haberleşme, bilgi paylaşımı, habercilik ve medya, tanıtım ve reklam, seyahat ve tatil, kamu hizmetleri, bankacılık, ticaret, eğlence, sosyal ilişkiler ve kültürler arası etkileşim, çevre, sağlık ve eğitim gibi günlük yaşamı ilgilendiren pek çok alanda getirdiği olumlu getiriler, yenilikler ve faydalar bugün herkes tarafından kabul edilmektedir (Bayzan, 2011). Bu çerçevede, başta E-Devlet ve Eğitimde FATİH (Fırsatları Arttırma ve Teknolojiyi İyileştirme Hareketi) Projesi gibi önemli ulusal bilişim projeleri Türkiye'nin dijitalleşen dünyada teknolojiyi etkin, doğru kullanabilmesi ve üretken bir yapı çizebilmesinde önemli kilometre taşlarını oluşturmaktadır.

4.2.2. Dijital Ortamdaki İnternetin Risklerine Karşı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı

İnternet, son yüzyılın en önemli buluşlarından biri olarak insan hayatını kolaylaştıran en büyük araçlardan biri haline gelmeye başlamıştır. Günümüz dünyasının en kolay iletişim ağlarından biri olan internet ile insanlar arası

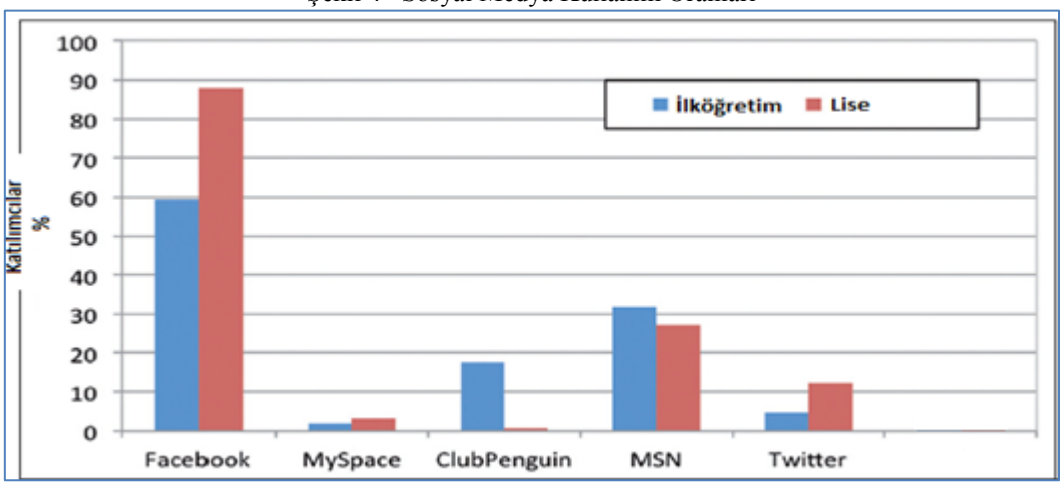
bilgi paylaşımı kolaylaşmış ve dünyanın herhangi bir noktasından doğan bilgiye çok rahatlıkla ulaşılabilir hale gelinmiştir. İnternetin hayatımıza girdiği 1990'ların başında, tek taraflı akmaya başlayan bilginin web 2.0 teknolojilerinin gelişimi ve özellikle sosyal ağların kullanılmaya başlanılması ile bilgi çok taraflı üretilip çevrimiçi ortamda kolay paylaşılır hale gelmiştir. Bu süreçte internet kullanıcıları aynı zamanda birer içerik üreticisi olmaya başlamaları interneti çok boyutlu hale getirmiş; çevrimiçi platformun hem fırsatlarının hem de risklerinin çabuk oluşmasına zemin hazırlamıştır.

4.2.2.1. Dünyada ve Türkiye'de İnternet Kullanım Eğilimleri

İnternet kullanım yaşının her geçen zaman daha da düşmesi ve dijital araçları aktif kullanan yeni bir neslin doğması dijital vatandaşlık algısının çocuk yaşlarda kazandırılmasının önemini bir kez daha göstermiştir. Dijital vatandaşlık algısında da internet kullanım eğilimlerinin ölçümlenmesi konu ile ilgili en büyük girdilerden birini oluşturmaktadır.

İngiltere'de The I In Online organizasyonu çevrimiçi oyunlar ve sosyal ağlara yönelik şimdiye kadarki en geniş kapsamlı çalışmayı yapacağını açıklamıştı (theiinonline.org, 2012). İngiltere, ABD, Kanada ve Avrupa'nın çeşitli yerlerinden 121 okuldan 31.000 öğrenci üzerinde yapılacak çalışmalarda çocuklara hem anket uygulanacağı hem de çevrimiçi ortamdaki bilgilerini korumalarına yönelik eğitimler verileceği belirtilmişti. Konu ile ilgili yayınlanan bir rapor veya haber henüz olmamakla beraber aynı organizasyonun 2011 Veri Koruma Günleri boyunca 4000 öğrenci (8-16 yaş) üzerinde yaptığı çalışmada sosyal ağlar üzerinde değişik bulgulara rastlanılmıştır. Sosyal ağ kullanımında Facebook'un ciddi bir üstünlüğü Şekil 4'de de gözükmektedir. Sosyal ağlar genellikle ana sayfalarından gizlilik politikalarına giden linkler vermekle beraber gizlilik politikalarının anlaşılırlığı ve okuma düzeyleri siteden siteye farklılık gösterebilmektedir. Bunda okuma konusundaki tembellik, gizlilik sözleşmelerinin karmaşıklığı ve anlaşılır olmayışı gibi etkenler gösterilebilmektedir. Gizlilik politikalarındaki kelime sayısına göre ise sosyal ağlar azdan çoğa doğru sırasıyla şöyle sıralanmaktadır: Twitter-Google-Club Penguin-MySpace-Bebo-MSN-LinkedIn ve Facebook (Furnell & Phippen, 2012).

Şekil 4 –Sosyal Medya Kullanım Oranları



Avrupa Birliği Güvenli İnternet Programı kapsamında desteklenen EU Kids Online projesi kapsamında ise 2006-2009 yılları arasında 25 Avrupa Birliği ülkesinde gerçekleştirilen anket çalışmasının 2. ayağına aralarında Türkiye'nin de bulunduğu 9-16 yaş aralığındaki 25.142 çocuk katılmıştır. İlgili projenin Ekim 2012'de yayınlanan diğer bir raporunda anket çalışmasına 8 Avrupa ülkesi daha katılarak ülke sayısı 33'e çıkmıştır (EUKidsonline, 2012).

Projenin 2011 yılında yayınlanan 2. ayağındaki 25 ülke ortalamasına göre, çocukların %60'ı her gün internete düzenli bağlanmaktadırlar (Livingstone, Haddon, & Ólafsson, 2011). İnternet erişimi ise en çok %87 ile evden ve %63 ile okuldan gerçekleşmektedir. İnternet kullanım amacı ise en çok %85 ile okul çalışmaları olmakla beraber bunu sırasıyla %83 ile oyun oynama ve %76 ile video izleme takip etmektedir. Çocukların, %59'unun bir sosyal ağ hesabının olmasıyla birlikte internet kullanım alışkanlıklarına bağlı olarak çeşitli risklerle de çocuklar çevrimiçi ortamda karşılaşabilmektedirler. Örneğin, çocukların %14'ü internette cinsellik içeren öğelerle karşılaşmıştır. Çocukların %6'sı kendilerini rahatsız eden mesajlar almış ve siber zorbalığa maruz

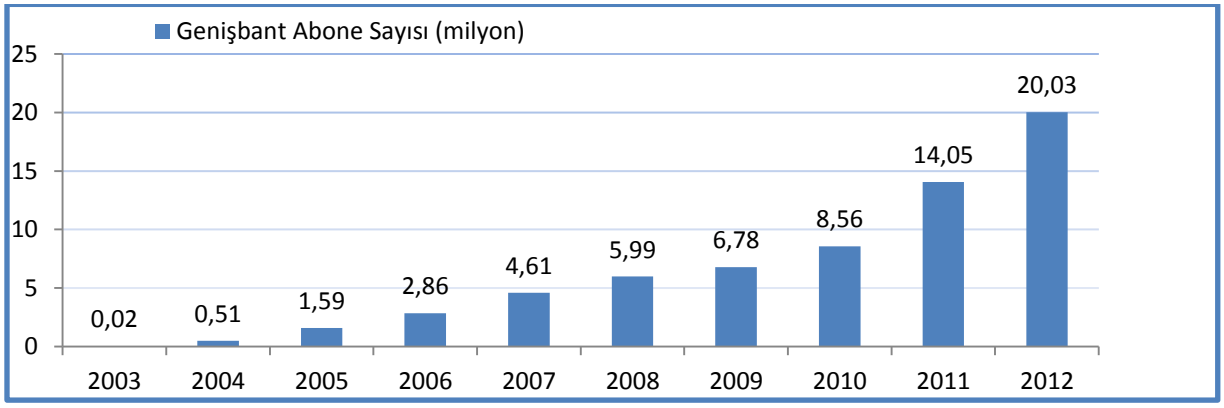
kalmışlardır. %30'u ise yüz yüze görüşmediği bir kişiyle çevrimiçi arkadaşlık kurmuştur. Katılımcıların %9'u tanıştığı çevrimiçi bir arkadaşıyla yüz yüze görüşmeye (çevrimdışı iletişim) gitmiştir.

Bu çalışmanın Türkiye'ye özgü bulgularına yönelik çalışmaya 1018 çocuk ve bir ebeveyni katılmıştır. Çocukların tümü internet kullanmakla birlikte ebeveynlerin sadece %29'u internet kullanmaktadır. Buna rağmen, ebeveynlerin %72'si internette karşılaştıkları olumsuz durumlara karşı çocuklarına yardım edebileceklerine inanmaktadırlar. Herhangi bir çevrimiçi risk ile karşılaşmış çocukların yarısı bu riski kimse ile paylaşmamıştır. Sosyal paylaşım sitelerine üyelik yaşı 13 olmasına rağmen, bu sitelere üyeliği bulunan katılımcıların 3'te biri 13 yaşın altındadır. Sosyal paylaşım sitesi kullanan çocukların %85'i Facebook hesabına sahiptir ve bu çocukların %42'si profil bilgilerini herkese açık tutmaktadır. Çocukların çevrimiçi risklerle ile karşılaşma oranı %25'tir ve bu oran %33 olan Avrupa ortalamasının altındadır. Çocukların %13'ü internette cinsel içerikli görseller gördüğünü bildirmiştir (Avrupa:%26). Bu çocukların %46'sı bu görsellerden rahatsız olduğunu raporlamıştır. Çocukların %9'u zorbalığa maruz kalmakla birlikte, sadece %3 siber zorbalığa maruz kalmıştır. Çocukların %14'ü yüz yüze tanışmadığı kişilerle internette görüşmekte ve sadece %2'si internette tanıştığı kişilerle yüz yüze görüşmektedir. Bu çalışma ile birlikte Türk çocuklarının interneti güvenli kullanım istatistiği maalesef tüm Avrupa ülkelerine göre en son sırada yer almıştır. Türk çocuklarının internet kullanım oranı ise düşük kullanım ve risk boyutu da orta düzey risk olarak nitelendirilmiştir.

Türkiye'de de şimdiki adı ile İnternet Geliştirme Kurulu olan İnternet Kurulu koordinesinde ve BTK'nın katkılarıyla düzenlenmiş olan 2010 yılı Şubat ayında düzenlenen "Güvenli İnternet Günü Etkinlikleri" kapsamında, "Ailelerin İnternet Algıları ve Eğilimleri" konulu bir araştırma yapılmıştır (BTK, Ailelerin İnternet Algıları ve Eğilimleri Araştırması, 2010). Bu araştırma kapsamında, 6–17 yaş aralığında İnternet kullanıcısı çocuğu olan 10.992 ebeveyn ve 12-17 yaş aralığındaki 2.816 çocuk üzerinde anket uygulanmış ve araştırmanın sonuçları Güvenli İnternet Günü'nde ele alınmıştır. Araştırmada, Türkiye'deki ebeveynlerin %90'ının çocuklarının internet kullanırken "müstehcen" ve "şiddet" içerikli görüntülere maruz kalabileceğini ya da bu tür sitelere girebileceğini düşünmektedirler. Ayrıca aileler çocuklarının, internete veya cep telefonuna bağımlı olabileceğini, kişisel ve özel bilgilerinin yabancıların eline geçebileceğini, internet üzerinden istismara ve tacize maruz kalabileceğini ve kötü niyetli kişilerle tanışıp arkadaşlık edebileceğini düşündükleri ortaya çıkmıştır (Güvenliweb, İnternetin Bilinçli, Güveni ve Etkin Kullanımı, 2013).

Türkiye İstatistik Kurumu verilerine göre Türkiye'de 2012 yılı itibari ile neredeyse her iki evden birinde internet bağlantısı bulunmakta ve BTK pazar verilerine göre de 2012 yılı itibariyle Türkiye genelinde 20 milyondan fazla internet abonesi bulunmaktadır (BTK, 2012). Veriler göstermektedir ki, Türkiye'de internet kullanımındaki orantısal artış çok hızlıdır. Bu durum aynı zamanda, hem dünyada hem de Türkiye'de üretilen çevrimiçi içerik ile ilgili bu platformu kötü amaçlı kullananların istismar alanı olarak da faaliyet göstermesine sebep olmaya başlamıştır. Bu yüzden, internet birçok faydasının yanında birçok riski de bünyesinde barındırmaktadır.

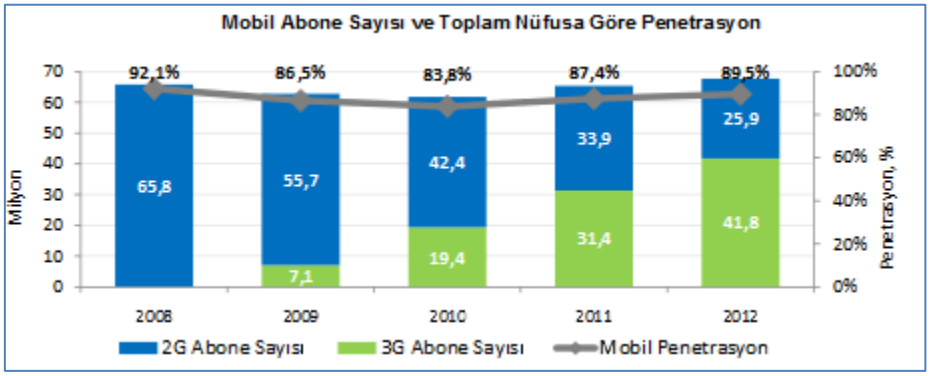
Şekil 5 –Türkiye'de Yıllara Göre Genişbant İnternet Abone Sayıları



Türkiye, her geçen gün internet teknolojisini kullanmaya adapte olan bir ülke olmakla beraber Türkiye'de internetin güvenli kullanımı bilinci maalesef alt sıralarda yer almaktadır. 2011 yılının son çeyreğinde Microsoft tarafından kişisel bilgisayarlara bulaşan malware sayılarına bakıldığında dünya sıralamasında Türkiye'nin 8. sırada yer aldığı gözlemlenmekte ve siber saldırılara yoğun maruz kalan ülkeler sıralamasında üst sıralarda yer aldığı gözlemlenmektedir (Güvenliweb, 2013).

Mobil ağlar üzerinden internet erişimi son zamanlarda internet kullanımında önemli bir yere sahip olmaya başlamıştır. Bunda tabletler, akıllı telefonlar ve özellikle de 3G teknolojisinin hem Türkiye'de hem dünyada yoğun bir erişim altyapısına bağlı olarak kullanımı ile izah edilebilmektedir. 2009 yılının Temmuz ayında 3G ile tanışan Türkiye'de Şekil 6'da görüldüğü üzere 3G abone sayısı 2012 yılı sonu ile 40 milyonu geçmiştir.

Şekil 6 – Türkiye'de Yıllara Göre Mobil Abone Sayısı Oranları



Öbür taraftan internet kullanımındaki payı git gide artan mobil ağlarla ilgili ABD'de Federal Ticaret Komisyonu'nun 2012 yılında yayınladığı raporlarda çarpıcı sonuçlara erişilmiştir. İlgili raporlarda, mobil uygulamaların sadece %20'si kullanıcılarına güvenlik politikaları hakkında uyardığı ve uygulamaların %60'ının kullanıcı bilgilerini reklam ağlarına, analisttik şirketlere ya da 3. şahıslara rahatlıkla verebildiği gözlemlenmiştir (MobileAppsforKids, 2012). Aileler ve çocukların ise tüm bunlardan habersiz bu uygulamaları rahatlıkla kullanabildiği yapılan çalışmalarda görülmüştür.

4.2.2.2. Türkiye'de İnternetin Güvenli Kullanımı ile ilgili yapılan Çalışmalar

İnternetin güvenli kullanımı ile ilgili çalışmalar, artık tüm dünyanın gündemini meşgul etmekle beraber Türkiye'de de konu ile ilgili bilinçlendirme çalışmaları yapılmaya başlanmıştır.

Dünya'da konu ile ilgili çalışmalara ilk örneklerden biri ABD'de 1992 yılında yürürlüğe giren ve okul ile kütüphanelerde internet kullanımını düzenleyen Children's Internet Protection Act (Çocukları Internette Koruma Yasası) olmuştur. Avrupa Birliği Komisyonu'nun 1999 yılında başlattığı Güvenli İnternet Programı ile internetin güvenli kullanımının teşvikine ve internet ortamındaki risklere karşı alınması gereken tedbirlere yönelik Avrupa'daki ilk çalışmalar başlatılmıştır. Avrupa Birliği Güvenli İnternet Programı tarafından desteklenen INSAFE ağı, Avrupa Birliği ülkeleri tarafından bir işbirliği ağı olarak kurulmuş olup, çevrimiçi teknolojilerin güvenli ve etkin bir şekilde kullanımına ilişkin çalışmalar yapmakta ve bu çalışmaların çoğu Avrupa ülkesinde faaliyete geçmiş Güvenli İnternet Merkezleri ve İnternet Yardım Hatları vasıtasıyla faaliyetlerini gerçekleştirebilmektedirler. Ayrıca Program kapsamında, Güvenli İnternet Günü(GİG) etkinlikleri her yılın Şubat ayında organize edilmektedir. GİG, özellikle tüm dünyadaki çocuklar ve gençler arasındaki çevrimiçi ve mobil internet teknolojisini daha güvenli ve sorumlu bir şekilde kullanımını destekleme amacındadır. 2004 yılında başlayan Güvenli İnternet Günü etkinliklerinin 10.su tüm dünyada 5 Şubat 2013 tarihinde kutlanmıştır. Türkiye'de de 2010 yılından bu yana kutlanan Güvenli İnternet Günü'nün 4.sü bu yıl gerçekleştirilmiştir. Ancak, Türkiye'nin Güvenli İnternet Programı'na katılımı henüz gerçekleşmemesine bağlı olarak Türkiye'de şu aşamada bir Güvenli İnternet Merkezi veya Yardım Hattı bulunmamaktadır.

Türkiye'de internetin bilinçli, güvenli ve etkin kullanımına ilişkin yapılan en önemli çalışmalardan biri Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde yürütülen çalışmalardır. TİB şimdiye kadar, Türkiye'nin 120'den fazla farklı noktasında farklı kademelerde 40.000'e yakın katılımcıya ulaşarak 300'e yakın eğitim semineri vermiş bulunmaktadır. Bu konuda bilinçlendirme amaçlı kitapçık, broşür, afiş ve benzeri çalışmalar yapan TİB aynı zamanda internetin güvenli kullanımına özgü yayın yapan ilk internet sitesi Güvenli Web (www.guvenliweb.org.tr) ve çocuklar için de Güvenli Çocuk (www.guvenlicocuk.org.tr) web portallarını hizmete açmıştır.

2007 yılında kabul edilen 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile verilen görevle TİB, internet ortamında işlenen suçlara ilişkin üretilen yasadışı içeriğe karşı işlem yapmakla yükümlendirilmiştir. Bu gayede Türkiye'de

kurulan İhbar Merkezi, İhbar Web (www.ihbarweb.org.tr) aracılığıyla vatandaşlar birer dijital vatandaş olma sorumluluğunda internet ortamında işlenen suça ilişkin içeriği İhbar Web'e şikâyet edebilmektedirler. Ayrıca, 5651 sayılı kanun kapsamında çevrimiçi ortamda kişi hakkı ihlal edildiğini düşünen bir dijital vatandaş, bireysel başvuru hakkını kullanarak içerik ve yer sağlayıcıya ulaşabilmekte, sonuç alınamaması halinde ise Sulh Ceza Mahkemelerine başvuruda bulunabilmektedirler.

Türkiye'deki özellikle çocuk ve gençlerin internet kullanımı sırasında zararlı içeriklere maruz kalmasını engellemek için Telekomünikasyon İletişim Başkanlığı'nın internet servis sağlayıcıları ile birlikte yaptıkları çalışmalar sonucunda Bilgi Teknolojileri ve İletişim Kurulu Kararı ile yürürlüğe giren "Güvenli Internet Hizmeti" ile dijital vatandaşlara tüm servis sağlayıcılar tarafından internet içerik filtreleme servisi sunulmaya başlanılmıştır. Güvenli Internet Hizmeti ile ilgili detaylı bilgilere www.guvenlinet.org.tr adresinden erişilebilmektedir.

İnternet kullanıcılarının çevrimiçi ortamda bilgilerinin korunması amacıyla TÜBİTAK tarafından Bilgi Güvenliği (http://www.bilgiguvenligi.gov.tr) ve Bilgimi Koruyorum (http://www.bilgimikoruyorum.org.tr) portalları hizmete açılmıştır. Bilgi Güvenliği portalında bilgi güvenliği ile ilgili güncel uyarılar, bilgilendirici rehberler ve teknik yazılar yayınlamaktır. Bu projenin bir alt projesi olarak hizmete giren Bilgimi Koruyorum portalında ise bilgisayar ve internet kullanıcılarının bilgi güvenliğiyle ilgili doğru kaynaklara etkin ve hızlı bir şekilde erişiminin sağlanması için e-öğrenme modülü oluşturulmuştur.

Türkiye'de konu ile ilgili yapılan çalışmalar içerisinde sivil inisiyatifin yeterince sürece dâhil olamaması ve sosyal sorumluluk kapsamında sorunların ele alınamaması ile internetin güvenli kullanımına ilişkin etkili kısa video filmlerin var olmaması en büyük eksikliklerin başında gelmektedir. Türkiye Cumhuriyeti Emniyet Genel Müdürlüğü'nün çekmiş olduğu güvenli internet filmi güzel bir örnek oluşturmakla beraber yine Emniyet bünyesinde internetin güvenli kullanımına ilişkin bilinçlendirme seminerleri verilmekte ve konu ile ilgili broşür ve afişler dağıtılmaktadır. Yalnız tüm bu çalışmalar yetersiz kalabilmektedir. Başta STK'ların süreç içerisinde daha etkin rol oynaması, Avrupa fonları başta olmak üzere çeşitli kanallar vasıtasıyla projeler üretilip öncelikli olarak Türkiye'de bir Güvenli İnternet Merkezi'nin kurulması gerekmektedir.

4.2.2.3. İnternetin Bilinçli, Güvenli ve Etkin Kullanımı

İnternet ortamında yoğun bilgi paylaşımı, web 2.0 teknolojilerine bağlı olarak yoğun içerik üretimi ve üretilen/ paylaşılan bilgilerin hem iyi niyetli hem de kötü niyetli olabilmesi internetin bilinçli, güvenli ve etkin kullanım ihtiyacını doğurmuştur. Bunun için internet ortamında bir internet kullanıcısının karşı karşıya kalabileceği risklere karşı bilinçli hareket etmesi gerekmektedir. İnternetin bilinçli, güvenli ve etkin kullanımı yukarıda da bahsedilen internetin risklerinden en az düzeyde etkilenecek şekilde interneti kullanabilme, fırsatlarından doğru bir şekilde yararlanabilme ve sorumluluk sahibi bir dijital vatandaş olabilmekten geçmektedir.

Bu konuda birer dijital vatandaş olan internet kullanıcılarının başlıca bazı tedbirler alarak internetin fırsatlarında doğru ve etkin bir şekilde faydalanmaları gerekmektedir. Alınması gereken bu tedbirleri şu şekilde özetlenebilir:

- Bilgisayarlara mutlaka güvenlik duvarı içeren bir anti-virüs programı yüklenmesi ve anti-virüs programlarının düzenli olarak güncellenmesi, Sosyal ağ profillerinin arama motorlarına, tanımadığımız kişilere ve 3. şahıslara reklam amaçlı verilmesi girişimleri vb. önem derecesi yüksek sayılabilecek durumlara karşı gizlilik ve güvenlik ayarlarını kullanarak kapalı tutulması,
- Web tarayıcıların gizlilik ayarlarından 'izlenmeme (do not track)' opsiyonunun seçilmesi ve özellikle farklı bilgisayarlardan internete bağlanıldığında bilinmeyen çerezlerin bu ayarlardan engellenmesinin sağlanması, Kişisel bilgilerin ve ileride pişman olabileceğimiz içeriklerin internette, özellikle sosyal ağlarda paylaşılmaması,
- Çevrimiçi bankacılık ve alışveriş sistemlerini kullanırken,
    - Site hakkında ön araştırma yapılması ve güvenilir sayfalardan işlem yapılması,
    - Https bağlantılarının internet sayfalarında varlığının adres çubuğundan kontrol edilmesi,
    - 3D Secure veya SMS onay kodlarının kullanımına dikkat edilmesi,
    - Sanal kart veya sanal limit kullanımına özen gösterilmesi,
    - Güçlü şifreler oluşturulması,
    - Satın alınacak ürünün fiyatının kontrol edilmesi ve alışveriş kaydının tutulması,
    - Küçük yazılara dikkat edilmesi,
    - Sanal klavye kullanılması, Farklı bilgisayarlardan ve toplu internet erişimi sağlanan bilgisayarlardan işlem yapılmaması,

- Arama motorları yerine sık kullanılanlara ilgili web sayfasını ekleyerek; ilgili sayfaya sık kullanılanlardan erişimin sağlanması,

- E-posta (özellikle spam) ve farklı bağlantılardan gelen web sayfalarının linklerini tıklayarak ve bilmediğiniz/güvenmediğiniz web sayfalarına giriş yapılarak işlem yapılmaması,
- İnternette karşılaşılan yasadışı içeriklerle ilgili ALO 166 veya www.ihbarweb.org.tr adresine ihbarda bulunulması,
- İnternetin zararlı içeriklerinden korunmak için çeşitli filtreleme programları, ebeveyn denetim ve aile koruması ayarları ile çocuk ve aile profillerinden oluşan Güvenli İnternet Hizmeti (www.guvenlinet.org.tr) gibi çeşitli teknik araçların kullanılması gerekmektedir. Ayrıca aileler, çocuklarının ve kendilerinin internet kullanım alışkanlıkları ile ilgili şu ilkeleri benimsemeleri gerekmektedir:

    - Kendinizi eğitin, interneti öğrenin, interneti oturma odanıza taşıyın; zaman sınırlaması yapın.
    - İnternet kullanımıyla ilgili kurallar belirleyin, çocuğunuzu uygun bir şekilde uyarın, çocuğunuzla bağlantıyı koparmayın.
    - Çocuğunuzun dolaştığı mecraları bilmeye çalışın, sosyal ağ üyeliklerini arkadaşı olarak inceleyin.
    - Oynadığı bilgisayar oyunlarına dikkat edin, çocuğunuza aşırı tepkiler vermeyin.
    - Her şeye inanmaması konusunda uyarın, kişisel ve ailevi bilgileri paylaşmamasını öğütleyin.

5. Türkiye'de Dijital Vatandaşlığın Çevrimiçi Boyutuyla SWOT Analizi

Dijital vatandaşlığın çevrimiçi boyutuyla SWOT (Strengths, Weaknesses, Opportunities, Threats - Güçlü yönler, Zayıf yönler, Fırsatlar, Tehditler) Analizi, dijital vatandaşlığın internet tarafıyla gelişmiş, gelişmekte olan ve henüz bu yönde kat edilmesi gereken yönlerini farklı açılardan ele alınması sonucu oluşmuştur. Tablo 2'de dijital vatandaşlığın dokuz boyutu SWOT Analizindeki 'S' ve 'W'ye karşılık gelen güçlü ve zayıf yönleri ile ele alınmıştır. Tablo 2 göstermiştir ki, dijital vatandaşlığın güçlü ve zayıf yanları daha çok dijital vatandaşların internet ortamından elde edecekleri kazanımlar, faydalanabilecekleri alanlar ve karşı karşıya kalabilecekleri riskler yönüyle doğrudan dijital vatandaşları ilgilendiren yönlerinden oluşmaktadır.

Bu çalışmada dijital vatandaşlık kavramı, internetin riskleri, internetin güvenli kullanımı ve internet kullanım eğilimleri ile ilgili bilgilere değinilerek konu ile ilgili ana paydaşın dijital vatandaşlar olduğu görülmüştür. Fakat dijital vatandaşlığın çevrimiçi boyutuyla SWOT Analizindeki 'O' ve 'T'ye karşılık gelen fırsat ve tehdit yönleri ile incelenmesiyle Tablo 3'de ortaya çıkan sonuçlar göstermiştir ki, Türkiye'de dijital vatandaşlık algısının geliştirilmesi için sektöre ve devlete önemli görevler düşmektedir. Örneğin; dijital güvenlik ile ilgili Bilgi Teknolojileri ve İletişim Kurulu'nun devreye soktuğu, Çocuk ve Aile Profillerinden oluşan Güvenli İnternet Hizmeti ve sektörde önemli sayıda filtreleme programları ve anti-virüs yazılımlarının mevcudiyeti dijital vatandaşlara dijital güvenlik boyutunda önemli fırsatlar sağlarken; Avrupa Konseyi Siber Suçlar Sözleşmesi'nin Türkiye'de imzalanmış olup henüz onaylanmamış olması ve aynı şekilde Kişisel Verilerin Korunması Hakkında Kanun Tasarısı'nın Türkiye gündeminde yıllardır olmasına rağmen tasarının henüz yasallaşamaması diğer taraftan önemli tehdit unsurlarını oluşturmaktadır.

Tablo 2 - Dijital Vatandaşlığın Güçlü ve Zayıf Yanları

	Güçlü Yanlar	**Zayıf Yanlar**
Dijital Erişim	3G ve fiber internet teknolojilerinin gelişmesi ve internet toplu kullanım alanlarının yaygınlaşması	İnternet kullanım ücretlerinin henüz istenilen seviyelerde olmamasına bağlı erişimlerin kısıtlanabilmesi
Dijital Ticaret	Alışveriş ve ticaretin internette yaygınlaşması ve bu alanda rekabetin doğması	Dijital vatandaşların çevrimiçi alışveriş ve bankacılık sistemlerini doğru ve güvenli kullanamamaları ve kişisel bilgilerini rahatlıkla paylaşabilmeleri

Dijital İletişim	Çevrimiçi teknolojiler vasıtasıyla iletişim imkânlarının oldukça kolaylaşması	Çevrimiçi ortamda iletişim araçlarının kötüye kullanılması, doğru dil üslubu ve doğru kimlik ile iletişime geçilmemesi
Dijital Okuryazarlık	İnternet üzerinden bilgiye kolay ulaşma ve bilgiyi kolay paylaşma imkânlarının doğması	İnternette doğru bilgiye ulaşmada bilinçsiz hareket edilmesi, paylaşılan bilginin çabuk doğru kabul edilebilmesi ve pozitif içerik üretimi konusunda yetersiz olunması
Dijital Etik	Çevrimiçi ortamın da etik değerler çerçevesinde kullanılma gereksiniminin oluşması	Çevrimiçi ortamda başkalarının haklarına saygılı olunması hususunda titiz davranılmaması
Dijital Kanun	Kanunların çevrimiçi ortamda da geçerli olması ve bu ortama ilişkin Türkiye'de düzenlemelere gidilmesi	Dijital vatandaşların çevrimiçi ortamda işlenen suçlarla mücadele konusunda bilinçsiz olması
Dijital Hak & Sorumluluklar	Dijital vatandaşların çevrimiçi ortamda kendilerini özgürce ifade edebilmeleri	Dijit vatandaşların haksızlıklara ve işlenen suçlara karşı şikâyet hakkını kimi zaman kullanmamaları
Dijital Sağlık	Sağlık sistemlerinin çevrimiçi ortamın fırsatlarından faydalanılarak kullanılabilmesi	Fiziksel ve ruhsal yönden aşırı ve bilinçsiz internet kullanımının getirmiş olduğu sağlık sorunlarının oluşabilmesi
Dijital Güvenlik	Dijital güvenlik cihazları ve internet koruma yazılımlarının üretilmesi ve dijital vatandaşların kullanımına açılması	İnternetin bilinçli, güvenli ve etkin kullanım oranının yapılan çalışmalarda düşük olması

Tablo 3 - Dijital Vatandaşlığın Fırsat ve Tehditleri

	Fırsatlar	**Tehditler**
Dijital Erişim	FATIH Projesi, 5809 Sayılı Elektronik Haberleşme Kanunu ve 5369 Sayılı Evrensel Hizmet Kanunu	İnternet trafiğinin her geçen gün artmasına bağlı altyapı sorunlarının zamanla oluşabilmesi
Dijital Ticaret	E-Ticaret Kanun Tasarısının gündemde olması	Çevrimiçi alışveriş ve bankacılık sistemlerinde her geçen zaman farklı dolandırıcılık ve kimlik hırsızlığı yöntemlerinin ortaya çıkması
Dijital İletişim	Dijital iletişim araçlarının kullanılabilir ve kolay ulaşılabilir olması	İletişim araçlarının kötüye kullanılması, zararlı içerik üretimi ve paylaşımının bu platformlarda artması
Dijital Okuryazarlık	FATIH Projesi'nin okullardaki eğitim sürecinde önemli bir yeri teşkil edecek olması ve okullarda Medya-Okuryazarlığı dersinin seçmeli verilmeye başlaması	Bilgisayar ve bilişim derslerinin okullarda etkin olarak verilememesi, güvenli internet kullanımı ve bilişim okuryazarlığı müfredatlarına ihtiyaç duyulması
Dijital Etik	Dijital dünyada da etik anlayışın oluşması	Zorbalık, nefret söylemi ve kişisel hakaret faaliyetlerinin çevrimiçi ortamda daha yaygın olması
Dijital Kanun	TCK'da bilişim suçlarının tanımlanması ve 5651 sayılı İnternet Kanunu'nun yürürlükte olması	Kanunların genel çerçevesinin ulusal olması ve internetin açık yapısı gereği internet ortamında işlenen suçlara karşı çoğu zaman yetersiz kalınabilmesi
Dijital Hak & Sorumluluklar	TİB Bilgi İhbar Merkezi'nin kurulmuş ve 5651 sayılı Kanun çerçevesinde kişi hakkı ihlal edilen vatandaşa bireysel başvuru hakkının verilmiş olması	Başkalarının eserlerinin kaynak belirtmeden veya izinsiz kullanımı neticesi intihal vakalarının oluşması ve internetin dinamik ve evrensel yapısı sonucu işlenen bunun gibi haksızlıklara karşı kimi zaman sonuçsuz kalınabilmesi

Dijital Sağlık	Sağlık hizmeti sistemlerinin çevrimiçi ortamda dijital vatandaşlara açılmaya başlanması ve ekranlı araçlarla çalışmalarda sağlık ve güvenlik önlemleri hakkında yönetmeliğin çıkmış olması	Yaşa uygun fiziksel araçların yeterince üretilmemesi, çevrimiçi platformun sadece fiziksel yönden değil psikolojik ve ruhsal yönden de özellikle çocukları etkileyebilmesi, internet üzerinden izinsiz birçok sağlığa zarar maddenin rahatlıkla satılabilmesi
Dijital Güvenlik	Birçok internet koruma paketinin ve güvenli internet hizmeti paketlerinin ücretsiz olarak dijital vatandaşlara sunulması	Siber saldırıların her geçen gün artması, Avrupa Konseyi Siber Suçlar Sözleşmesi'nin Türkiye'de henüz onaylanmamış olması, Kişisel Verilerin Korunması Hakkında Kanun Tasarısı'nın henüz yasallaşmaması ve güvenli internet kullanımı ile ilgili yeterince bilgilendirici eğitim, kamu spotu ve kısa film faaliyetlerinin olmaması

5. SONUÇ

İnternetin bilinçli, güvenli ve etkin kullanımına ilişkin yapılması gerekenler saymakla bitmez. Yaptığımız çalışmalar göstermiştir ki, çevrimiçi teknolojileri en doğru kullanabilme yöntemi çevrimiçi teknolojilerden doğru faydalanabilmeyi bilme ve fayda esasına dayalı bu platformları kullanmadan geçmektedir. Faydalanabilecek bilgiye çevrimiçi ortamda erişebilmek için de olabildiğince doğru bilgiye ulaştığımızdan emin olmak, bilgiye kaynağından erişmek, farklı web sayfalarından kaynak araştırması yapmayı ve arama motorları başta olmak üzere internette bilgi arama yöntemlerini bilmekten geçmektedir. Web 2.0 teknolojilerinin dinamik yapısı ve bu yapı çerçevesinde bütün internet kullanıcılarının çevrimiçi platformda aynı zamanda birer internet içerik üreticisi olmaları, doğru bilgiye ulaşmak kadar birer içerik üretici olan dijital vatandaşların da hak ve sorumlulukları çerçevesinde internette doğru ve faydalı bilgiler üretip paylaşmalarına özen göstermeleri gerekmektedir.

Günümüzün dijital çocukları veya dijital vatandaşları hatta daha özelde dijital yerlileri teknolojiyi içerik olarak kullanmayı yetişkinlere göre çok daha iyi bilmektedir. Burada gözden kaçırılan nokta ise, çocukların büyük bir bölümünü oluşturduğu dijital vatandaşlara teknolojiyi içerik olarak nasıl kullanılacağını öğretmekten ziyade teknolojiyi hak ve sorumlulukları çerçevesinde nasıl daha etkin ve doğru kullanılabilmelerini öğretilmesi gerekliliğidir. Dijital vatandaşlığın dokuz boyutu, teknolojiyi çocukların ayaklarına getiren dijital araçların bu gayede nasıl daha doğru ve sorumluk çerçevesinde kullanılması gerekliliğini öğütlemektedir. Dijital araçlar içerisinde çevrimiçi teknolojiler yani internet en önemli paylardan birine sahip olduğu için de internetin bilinçli, güvenli ve etkin kullanımının dijital vatandaşlara kazandırılması gerekmektedir.

Türkiye'de dijital vatandaşlık algısının güçlendirilmesi için internetin bilinçli, güvenli ve etkin kullanımı konusunda yapılacak işbirliği çalışmaları, kamuoyunun farkındalığını artıracak çalışmalar, projeler ve her şeyden önce de internette pozitif içerik üretme noktasında dijital vatandaşların teşvik edilmesi gerekmektedir. Dijital vatandaşlığın çocuk yaşlarda başladığı ve OECD'nin Mayıs 2011 tarihli 'Çocukların Çevrimiçi Korunması Raporu'nda belirtilen; pozitif içerikler ve çocuklara özgü kullanışlı ve eğitici alanlar yaratma ihtiyacı göz önünde bulundurulduğunda internetin güvenli kullanımının sadece dikkat edilmesi gerekenler ötesinde değerlendirilmesi gerekliliğini ortaya koymaktadır. Burada internette yasadışı, zararlı, yanlı veya yanlış içerikler üretmeden ziyade dijital vatandaşların istifade edebileceği doğru, güvenilir ve gündelik hayatta bir dijital vatandaşın işine yarayabileceği bilgiler üretilmesi gerekliliği ortaya çıkmaktadır. Burada hem devletlere hem Sivil Toplum Kuruluşlarına hem de sektör temsilcilerine önemli görevler düşmekle beraber en büyük görev ve sorumluk aynı zamanda birer içerik üreticisi olan internet kullanıcılarına yani dijital vatandaşlara düşmektedir.

Bu çalışmayla, dijital vatandaşlık kavramı internetin riskleri ile birlikte analiz edildikten sonra Türkiye'de ve dünyada dijital vatandaşlık algısı ve internetin güvenli kullanımına ilişkin yapılmış çalışmalar ve istatistiksel göstergeler eşliğinde irdelenmeye çalışılmıştır. Türkiye'de konu ile ilgili yapılan çalışmaların düşük seviyelerde olduğu ve yapılan çalışmaların büyük bir çoğunluğunun Telekomünikasyon İletişim Başkanlığı bünyesinde yürütüldüğü gözlemlenmiştir. Başta Avrupa'da ağırlıklı olarak Sivil Toplum Kuruluşları bünyesinde yürütülen

Güvenli İnternet Merkezleri ve Yardım Hatlarının yapılanmalarının Türkiye'de olmaması en büyük eksikliklerin başında gelmektedir.

Çalışma ile birlikte internetin bilinçli, güvenli ve etkin kullanımı ile dijital vatandaşlık kavramı birlikte incelenmeye çalışılmış ve bu süreçte dijital vatandaşlara düşen görevlere bakılmaya çalışılmışsa da dijital vatandaşlığın çevrimiçi boyutuyla SWOT Analizi göstermiştir ki, sektöre ve devletlere de önemli görevler düşmektedir. Bu çalışmanın devamında, Türkiye özelinde dünyada dijital vatandaşlık ve internetin güvenli kullanımı ile ilgili daha geniş perspektifte gerek hukuksal gerek sosyal mecralarda yapılması gerekenler ve süreç ile ilgili eksiklikler detaylıca incelenerek somut çıktılar ortaya konabilir.

Kaynakça

(2012). Mayıs 16, 2013 tarihinde EUKidsonline: http://eukidsonline.metu.edu.tr/ adresinden alındı

Alberta. (2012). *Digital Citizenship Policy Development Guide.* Edmonton, Canada: Alberta Education School Technology Branch.

Arıcak, O. T. (2011). *Siber Zorbalık: Gençlerimizi Bekleyen Yeni Tehlike*. 5 15, 2013 tarihinde Kariyer Penceresi: http://www.kariyerpenceresi.com/?yazarlarimiz,51,104/siber-zorbalik-genclerimizi-bekleyen-yeni-tehlike-.html adresinden alındı

Bayzan, Ş. (2011). *Dünyada İnternetin Güvenli Kullanımına Yönelik Uygulama Örnekleri ve Türkiye'de Bilinçlendirme Faaliyetlerinin İncelenmesi ve Türkiye İçin Öneriler.* Ankara: BTK.

BTK. (2010). *Ailelerin İnternet Algıları ve Eğilimleri Araştırması.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

BTK. (2012). Pazar Verileri 4. Çeyrek Raporu. Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Ceyhan, E. (2010). Problemli internet kullanım düzeyi üzerinde kimlik statüsünün, internet kullanım amacının ve cinsiyetin yordayıcılığı. *Educational sciences : theory & practice, 10*(3), 1323-1355.

Çuhadar, C. (2012). Exploration of problematic internet use and social interaction anxiety among Turkish pre-service teachers. *Computers & Education, 59*, 173-181.

DigitalAgenda. (2011). *Digital Agenda: Coalition of top tech & media companies to make internet better place for our kids.* Europa Press.

Doğan, H., Işıklar, A., & Eroğlu, S. (2008). Ergenlerin problemli Internet kullanımının bazı değişkenler açısından incelenmesi. *Kazım Karabekir Eğitim Fakültesi Dergisi*(18), 106-124.

Evran, B. (2012, 3 8). *Dijital Yerliler ve Dijital Yerlilerde Öğrenme.* 5 15, 2013 tarihinde blogspot.com: http://zkusagi.blogspot.com/ adresinden alındı

Facebook. (2013). Mayıs 16, 2013 tarihinde https://www.facebook.com/help/ adresinden alındı

Furnell, S., & Phippen, A. (2012). Online privacy: a matter of policy? *Computer Fraud & Security, 2012*(8), 12-18.

Google. (2013). *Google in Education.* Mayıs 16, 2013 tarihinde http://www.google.com/edu/teachers/youtube/curric/index.html adresinden alındı

Güvenliweb. (2013). Mayıs 16, 2013 tarihinde http://www.guvenliweb.org.tr/ adresinden alındı

Güvenliweb. (2013). Mayıs 16, 2013 tarihinde http://www.guvenliweb.org.tr/istatistikler/content/geni%C5%9Fbant-broadband-kullan%C4%B1m%C4%B1-2012 adresinden alındı

Johnson, N. (2009). *The Multiplicities of Internet Addiction: The Misrecognition of Leisure and Learning.* Burlington: Ashgate Publishing Company.

Kim, H.-K., & Davis, K. (2009). Toward a comprehensive theory of problematic Internet use: Evaluating the role of self-esteem, anxiety, flow, and the self-rated importance of Internet activities. *Computers in Human Behavior, 25*(2), 490-500.

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011, 5). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, 675-705.

Kırlıdoğ, M. (2013). Çevrimiçi Davranışsal Reklamcılık ve Kişisel Mahremiyet İhlalleri. *Akademik Bilişim 2013.* Antalya .

Kıvırcık, C. (2013, Şubat). *Telekom Dünyası*. 5 16, 2013 tarihinde Telekom Dünyası: http://www.telekomdunyasi.com/internet-gelistirme-kurulu-onculugunde-siber-guven-408.html adresinden alındı

Livingstone, S., Haddon, L., & Ólafsson, K. (2011). *Risks and safety on the internet.*

Microsoft. (2013). Mayıs 16, 2013 tarihinde http://www.microsoft.com/security/default.aspx adresinden alındı

MobileAppsforKids. (2012). *Current Privacy Disclosures are Disappointing.* Mayıs 16, 2013 tarihinde http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf adresinden alındı

Mossberger, K., Tolbert, C., & S. McNeal, R. (2007). *Digital Citizenship: The Internet, Society, and Participation.* London, England: The MIT Press.

Ocak, M. A. (2013). *Ailelerde ve çocuklarda dijital vatandaşlık algısının oluşturulması*. 2013 tarihinde Türkiye, www.guvenliweb.org.tr/egitimciler/files/aile_cocuk.pptx adresinden alındı

Odabaşı, F. (2012). İnternet ve Biz. Anadolu Üniversitesi Eğitim Bilimleri Enstitüsü.

Prensky, M. (2001). Digital Natives, Digital Immigrants. *On the Horizon, 9*(5), 1-6.

Ribble, M. (2011). *Digital Citizenship in Schools*, (Cilt 2nd Edition). Washington DC: The International Society for Technology in Education (ISTE).

theiinonline.org. (2012). Largest ever survey into children's use of online games and social networks launched by The i in online: http://www.theiinonline.org/2012/01/survey-by-the-i-in-online-largest-ever/ adresinden alınmıştır

Valcke, M., Bonte , S., De Wever , B., & Rots , I. (2010). Internet parenting styles and the impact on Internet use of primary school children. *Computers & Education, 55*(2), 454-464.