SİBER ÂLEM: YENİ MEDYA VE DİJİTAL YURTTAŞLIK

Serhat BEKAR* Murat SAĞLAM**

CYBERSPACE: NEW MEDIA AND DIGITAL CITIZENSHIP

Özet

İletişim teknolojilerindeki gelişmeler, kitle iletişim araçlarının çeşitlilik göstermesini ve toplumsal yaşamda kullanılmalarını sağlamıştır. Medya ortamlarının geleneksel ortamlar olarak, basılı ve görsel işitsel araçlar şeklinde uzun bir süre hükmü devam ederken; yeni medya, internetin sivillerin kullanımına sunulması ile toplumları değiştirmiş ve dönüştürmüştür. Bireyler de yeni medya ortamı olarak dijital ortamlarda birer dijital vatandaş haline gelmiştir. Dijital vatandaşlar dijital hakları, çevrimiçi güvenliği, etik kuralları bilen ve bu haklarını savunan özellikler sergilemiştir. Dijital çağda ağ toplumunun bir üyesi olarak bireyler sürekli çevrimiçi olma ihtiyacı içerisindedir. Bu ihtiyaçlar dijital vatandaşların gerçekleştirdikleri işlemlerde birtakım izleri bırakmalarına neden olmuş ve bırakılan izler dijital yurttaşların verilerini barındırmıştır. Siber alanda yurttaşların korunması gereken unsurlarını ise verileri oluşturmuştur. Bu nedenle çalışmanın amacını kişilik haklarının ihlali gibi yasalara aykırı tutum ve davranışların sergilenmesi durumlarında; dijital yurttaşların dijital haklarını, siber farkındalıklarını ve internet ilkelerinin oluşturulmasının gerekliliği oluşturmuştur. Literatür taraması yapılarak geçmişte ve günümüzde dünyanın farklı bölgelerinde gerçekleşen önemli siber saldırılar çerçevesinde çalışma konusu incelenmiştir. Bu hususta her geçen gün siber ortamlarda artan kullanıcı sayısı dikkate alındığında, güvenlik konusunun önemi daha iyi anlaşılmıştır. Sonuç olarak bireysel ve kurumsal olarak verilecek eğitimler ile yeni medya ortamlarında dijital yurttaşların maruz kalacakları siber saldırılardan korunmalarının artacağı düşünülmektedir.

Anahtar sözcükler: Yeni medya, dijital yurttaşlık, siber güvenlik

Abstract

Developments in communication technologies have enabled mass media to diversify and be used in social life. While media environments continue to dominate as traditional media in the form of printed and audio-visual tools for a long time; New media has changed and transformed societies with the introduction of the internet to civilians. Individuals have also become digital citizens in digital environments as the new media environment. Digital citizens have demonstrated characteristics of knowing digital rights, online security, ethical rules and defending these rights. As a member of the network society in the digital age, individuals need to be constantly online. These needs have caused digital citizens to leave some traces in their transactions, and the traces left contain the data of digital citizens. The elements that citizens need to protect in the cyberspace are their data. For this reason, the aim of the study is to investigate the display of illegal attitudes and behaviors such as violation of personal rights; It has created the necessity of establishing digital rights, cyber awareness and internet principles of digital citizens. By scanning the literature, the subject of the study was examined within the framework of important cyberattacks that took place in different parts of the world in the past and today. In this regard, considering the increasing number of users in cyber environments every day, the importance of security is better understood. As a result, it is thought that the protection of digital citizens from cyberattacks they will be exposed to in new media environments will increase with individual and institutional training.

Keywords: New media, digital citizenship, cyber security

* *Dr. Öğr. Üyesi, Tokat Gaziosmanpaşa Üniversitesi, Erbaa Meslek Yüksekokulu, Pazarlama ve Reklamcılık Bölümü, serhat.bekar@gop.edu.tr, Orcid: 0000-0002-3322-4559.*
** *Doç. Dr., Karamanoğlu Mehmet Bey Üniversitesi, Uygulamalı Bilimler Fakültesi, Yeni Medya Bölümü, murat4081@hotmail.com, Orcid: 0000-0001-8036-7942.*

Giriş

İletişim teknolojilerinde yaşanan hızlı gelişimler, medya alanına da yansımıştır. Geleneksel medyada mesajlar tek taraflı olarak izleyiciye, okuyucuya ve dinleyiciye ulaşırken; yeni medya da ise karşılıklı, etkileşimli olarak içerikler kitleye ulaşmaya başlamıştır. Yeni medyanın en önemli özelliklerinden olan etkileşim, eş-zamansızlık ve kitlesizleşme; değişen ve dönüşen teknoloji ile mümkün kılınmıştır. Geleneksel medya içeriklerinin kitlelere ulaşmasında teknolojinin büyük bir rolü olmakla beraber; internet bu süreçte daha fazla pay sahibi olmuştur. İçeriklerin dijital ortamda sayısal bir form almasıyla birlikte yeni medya ortaya çıkmıştır (Şeberoğlu, 2020: 29).

Yeni medya, farklı öğelerle ve sosyal medya platformları ile birlikte içeriklerin iletilmesidir. Bu iletim sürecinde geliştirilen ses, fotoğraf, video, metin, hareketli görüntü gibi öğeler birçok bilgi ve özelliği içinde barındırmaktadır (Gökçe, 2022). İnternet çeşitli sosyal medya platformları ile yeni medya içeriklerinin hızlı bir şekilde paylaşılmasını, yayılmasını ve daha kolay ulaşılmasını sağlamıştır.

Bu bağlamda yeni medya ortamının oluşmasında yeni iletişim teknolojileri ön plana çıkmıştır. Birçok sektörün bilişim, telekomünikasyon, bilgi-işlem, enformasyon ve ağ teknolojilerinde birleşmesi yeni medyayı oluşturmuştur (Gürcan ve Kumcuoğlu, 2017: 67). Dinamik bir özellik sergileyen yeni medya, internet ortamında içerik üreterek siber ortama adapte olmuştur. Kitlenin, yeni medya içeriklerine ulaşması ve enformasyon ihtiyacını karşılaması için dijital ortamda yer alınmasını gerektirmiştir. Değişen teknoloji, medya ortamının yeni medya ve kitlenin dijital yurttaş olarak lanse edilmesi; yeni medya ekosisteminde dijital alan ve siber ortamların önemine dikkat çekmiştir.

Yeni İletişim Teknolojileri ve Kitle İletişim Araçlarının Dönüşümü

1980'li yıllarda teknolojideki gelişmeler, kitle iletişim araçlarının gelişmesini sağlamıştır. Geleneksel kitle iletişim araçlarının mesajlarını anında ulaştırabilmesi ve kitlesizleştirme özelliği, bireylerin dış dünyayla olan etkileşimlerini artırmıştır. Radyo, televizyon ve gazete gibi geleneksel kitle iletişim araçlarının mesajları kitlenin geneline yönelik üretirlerken; internet ile birlikte mesajlar daha özel ve daha kişisel olarak üretilmeye başlanmıştır (Öztürk, 2010).

Kitle iletişim araçlarındaki içeriklerin kişiselleştirilebilir olması, hedef kitlelerdeki değişimleri kaçınılmaz kılmıştır. Gazete içeriklerinin dijitale eklemlenmesi, dijital olarak yayımlanması, geri bildirim hızının geleneksel araçlara göre hızlı ve anında olması, içerik sürecine dâhil olan kitlenin iletişim biçimini belirlemesi yeni iletişim teknolojilerinin bir sonucu olmuştur. Ayrıca televizyon içeriklerinin kişiselleştirilebilir olması, kaydedilip daha sonra izlenebilmesi, durdurma özelliğinin olması, reklamsız bir süreci etkin kılması kitle iletişim araçlarının yeni medyaya adapte olma sürecini ortaya çıkaran diğer etmenler arasında yer almıştır (Castells, 2005: 452).

Bireyler evden çıkmadan banka işlemlerini, alışverişlerini, fotoğraf çekme, eğlenme ve bilgi ihtiyacının giderilmesi gibi birçok eylemi cep telefonu veya bilgisayar gibi cihazlarla gerçekleştirmektedir. Bu cihazların birçok eylemi gerçekleştirebilmeleri internet tabanlı olmaları ve yeni medya ortamlarına adapte olabilmeleri ile sağlanmıştır. Ayrıca kitle iletişim araçlarının bir kısmının geleneksel olarak anılmasının herhangi bir olumsuz sonuç doğurmadığı belirtilmekle beraber; eskinin yeniye uyumu ve dönüşümüyle ilgili bir durumdur (Bayraktar, 2018).

1980 ve 1990'lı yıllarda televizyon gibi birçok kitle iletişim aracının bağımsız şebekesi ve istasyon sayısının artmasıyla birlikte dünya çapında ismini duyuran kanallar ve yayımcılar olmuştur. Farklılaşan ve çoğalan yayımcılık, daha farklı kitle iletişim araçları ile yayılmaya başlamıştır. Kitle iletişim araçlarının çeşitlenmesiyle içeriklerin her kesimden kitleye ulaşabilmesi, yeni medyanın kendi kitlesini oluşturmasını sağlamıştır (Lister, Dovey, Giddings, Grant ve Kelly, 2003: 31).

İletişim teknolojilerindeki hızlı gelişimle beraber bilginin yayılma hızı, kontrolü ve enformasyonun ulaştırılma süreci ivme kazanmıştır. Yeni iletişim teknolojileri bilginin uzaktan, yakına gelmesini sağlamıştır. Dünyanın bir ucundan diğer bir ucundaki olup bitenin öğrenilmesi ve haberdar olunması yeni iletişim teknolojilerinin hızı ile ilgilidir. Bu durum

dünyadaki geleneksel toplumların dönüşümü olarak da anlaşılabilir (Poster, 2021: 123). Bu süreçte etkin rol oynayan internet ile ağ haline gelen toplumların ve toplumun enformasyona ulaşımında yeni medyanın etkisini ortaya çıkarmıştır. Enformasyon ve bilgi çağının hedef kitlesi, yeni medya içerikleri ile donatılmaktadır. Bu içerikler internet ile dağıtılmakta ve elektronik cihaz ve yazılım kullanabilen, alanında uzman ve dijital içerik üretiminde yeteneği olan kişiler tarafından üretilmektedir. Üretilen içerikler dijital ortamda yayımlanmakta ve hedef kitleye bu kanaldan ulaştırılmaktadır. Yeni medya içeriklerinin üretilip dijitale dönüştürülmesi internet ortamında gerçekleştirilmektedir. Dolayısıyla kitle iletişim araçlarının ve geleneksel medyanın dönüşümünde yeni medya teknolojileri ön plana çıkmıştır (Askeroğlu ve Karakulakoğlu, 2019).

Yeni medya ve geleneksel medya arasındaki ayrımın net çizgilerle belirlendiği söylenememektedir. Yeni bir kitle iletişim aracı olarak internet, gelenekseli içinde barındırmak zorunda ve eskiyle birlikte bir dönüşüme tabi olmaktadır. Fidler (1997: 22-23) bu dönüşümü "medyaformoz" olarak ifade etmiştir. Yeni medyanın kullanım biçimi, teknolojiyi içerisinde barındıran yapısı ile gerçekleşmektedir. Yeni iletişim teknolojileri ile daha da hızlı bir ivme kazanan yeni medya Jan Van Dijk'e göre; link, metin, görüntü ve ses gibi öğeler türlerine göre farklı aygıtlarla, birlikte entegre olabilmektedir (Akt. Downing, 2004: 6-7). Yeni medyanın güçlü bir teknolojik alt yapıyla yükselişe geçmesi iletişimin; internette bilgisayar ve ağlar ile kurulması, içeriklerin dijital ortamlarda üretilmesi, dijital yeteneklerin ortaya çıkarılmasını sağlamıştır. Kitlelerin ve içeriklerin yeni medyada dijitale geçişle birlikte, içeriklerin dijitalleştiği ve kitlelerin dijital yurttaşlara dönüştüğü birtakım gelişmeler yaşanmıştır.

Yeni Medya ve Dijital Alan

Etkileşimli bir alan olan dijital medya oldukça yeni bir kavram olarak karşımıza çıkmaktadır. Dijital medyanın tarihsel süreci incelendiğinde ilk denemelerin etkileşimli televizyon programı üretiminde denendiği görülmüştür. Canlı görüntü ve sesin ilk denemesi 7 Nisan 1927'de Washington, D.C. - New York City arasında kurulan telefon hatları üzerinden gerçekleştirilmiştir. Bu görüşme Amerikan Telefon ve Telgraf Şirketi olan AT&T şirketinin Başkanı Walter Gifford ve ABD Ticaret Bakanlığı sekreteri Herbert C. Hoover'ın konuşmalarının iletilmesiyle gerçekleşmiştir (Einav, 2015: 1-2). 1927'de yapılan bu ilk deneme ticari kaygılar ve olanakların eksikliği sebebiyle çok fazla benimsenmemiştir.

Teknolojiyi benimseme hızı arttıkça, kullanım alanlarının da genişlediği ve yeni teknolojilere adapte olma süresinin kısaldığı bir çağda yaşanması interaktifliği ve dijital cihazları daha çok bir meta haline getirmiştir. Küresel mobil kullanıcılar verisi 2022 yılında cep telefonu kullanıcılarının 5,31 milyara ulaştığını; internet kullanıcılarının 4,95 milyara yükseldiğini, toplam nüfus içinde %62,5'i kapsadığını; sosyal medya kullanıcılarının ise 4,62 milyara yükselerek toplam nüfusun %58,4'lik bir orana sahip olduğunu ortaya koymuştur (We are social, 2022). Teknolojiyi benimseme hızı artıkça teknoloji öngörüleri daha zor ve yaratıcı olmayı gerektiren bir hâl almaya başlamıştır. Bu süreçte üretilen teknoloji ile medyanın ve kitle iletişim araçlarının dönüşümü, adaptasyonu gittikçe daha kolay bir hâl aldığını göstermiştir. Eskinin yeniye adaptasyon süreci, hızlı bir ivme kazanarak sürekli güncel halini korumaktadır.

İnsanlığın gelişim süreci içerisinde toplumlar, avcı toplumdan tarım toplumuna geçmiş ve ardından sanayi devrimi sonucunda makineleşme, fabrikalaşma ve Fordist üretim gibi süreçlerle yapısal bir dönüşüme uğramıştır. Özellikle bilgi toplumunda dijital araçların kendi içerisinde iletişim ortamı oluşturması ve bilgi toplumlarında bireye her zaman her yerde aktif olma imkânının sunulduğu bilişim toplumlarına dönüştürmüştür (Sağlam ve Topsümer, 2019: 487). Son dönemlerde bilgi ve iletişim teknolojileri gelişerek bilgi toplumunu oluşturduğu gibi ağ toplumuna dönüşen yeni yapıları meydana getirmiştir. Ağ toplumu gibi toplumsal dönüşümlerin temelinde yer alan yeni iletişim teknolojileri ve yeni medya araçları bilgi alışverişinde toplumu şekillendirmiştir (Hazer, 2020: 92-93). Toplumun bilgi ihtiyacının karşılanmasında kitle iletişim araçlarının etkisinin bulunması ayrıca medyanın ve içerik üretiminin gelişmesinde yeni iletişim teknolojilerinin etkisinin büyük olduğunu göstermektedir.

Yeni medyadan önce geleneksel medya da içerikler analog yöntemler ile üretilmiştir. Geleneksel medya iletişim araçlarının gelişen teknolojiye uyumlanması, internet ve bilgisayar teknolojisiyle gerçekleşmiştir. Yeni medya da içerikler dijital olana endekslenebilen '1' ve '0' kodları üzerinden bilgilerin depolanması süreçleridir (Yanık, 2016: 898). Geleneksel medya içeriğinin sayısallaştırılması, 'dijite' edilmesi; bu dönüşümün sağlanmasında en önemli kavramı temsil etmektedir. Bilginin hızla erişilebilir olması ve dağıtılması, bilgiye ulaşım konusundaki sınırlamaları da ortadan kaldırmıştır. Gazetedeki bilginin, televizyondaki programın internete taşınması; radyo programının internetle dağıtımının yapılabilmesi yeni medyanın dijital veri olarak sunulması en somut örneklerini oluşturmaktadır. Genel olarak yeni medyanın özelliklerini; dijite olabilmesi, multimedya katmanı, interaktiflik, zaman ve mekândan bağımsızlık şeklinde dijital alana geçişini ve uyumunu göstermektedir.

Dijitalleşme terimi ilk kez 1971 yılında bilgisayar destekli beşerî araştırmalara yönelik yazılmış bir makalede kullanılmıştır (Brennen ve Kreiss, 2014). Geleneksel medyada yazılı olanın doğrudan dijital ortama eklenmesi ve var olan verinin aynı şekilde aktarılması değildir. Dijital olan, birçok farklı multimedyayı bir arada kullanabilen medya ortamlarıdır. Yazının, içeriğin her türlü gösterge ile desteklenebilmesidir. Dijitalde sayısallaştırılmış veri; ses, fotoğraf, video, animasyon, hareketli görüntü, grafik, tablo ve şekiller ile desteklenebilmektedir. Verinin, işlenerek enformasyona dönüştürülmesi ise bilişim ile iletişim teknolojilerinin bütünleşmiş bir şekilde çalışmasıyla ilgilidir (Karaduman, 2019).

Enformasyon ve bilginin dijital olana uyumlaşmasıyla birlikte yeni bir döneme kapı açan iletişim teknolojileri, dijital çağda kitlelerin içeriklere erişmesinde mekân kavramını değiştirmiş; dijital ortamda içerik üreten dijital yurttaşlar oluşmuştur.

Dijital Alanda Kimlik: Dijital Yurttaşlık

McLuhan'ın "media is the message" (medya mesajdır) ifadesi dönüşen medyada yer edinen bireylerin kimlikleri haline gelen medya, insan bedenini betimleyen bir olgu haline gelmiştir (Erdoğan ve Alemdar, 2005: 444). Yeni sistemde kuşak farkı gözetilmeksizin bütünleşik bir yapı görülmektedir. Bireyler ve dijital yerliler olarak tüm dijital yurttaşlar, sosyal ağlar aracılığıyla sürekli olarak bağlı ve çevrimiçi oldukları bir dünyada yer almaktadırlar.

Dijitalleşme ile çevrimiçi izleme, mobil bağlantı gibi uygulamaların yükselişte olması, kitlelerin içerikleri istedikleri yerlere taşıyabildiklerini göstermektedir. Lisa Hsia (NBCUniversal Medya - Başkan Yardımcısı), içerik üretiminin dijital süreçte birden fazla medyaya yayılmış bir süreç olduğundan bahsederek, transmedya vurgusunu yapmaktadır (Comcast, 2022). Yeni medya emekçileri bu bağlamda içerik üretim sürecinde kollektif bir şekilde etkileşim yaratarak, ağlar oluşturmaktadır. Dijital medya ile mesafeler ve mekânların önemini kaybettiği bir döneme girilmesi, sanıldığı kadar her yerde aynı anda gerçekleşmemiştir.

Dijital alan; uzak, ulaşılabilir, etkileşimli, anında geri bildirim alınabilen bir alan haline gelmekle beraber dünyanın her yerindeki bireylerle iletişim halinde olunabilmektedir. Bilişim ve iletişim teknolojileri ile bu gelişmelere şahit olan dijital yurttaşlar bu süreçle birlikte ortaya çıkmıştır. Geleneksel yurttaşlık kavramı, internet ve toplumsal ağ ile farklı şekilde yorumlanmıştır. Dijitalde var olan, teknolojiyi kullanabilen yurttaşlar oluşmuştur (Alberta, 2012). Küreselleşme ile sınırların ortadan kalkması, dijital teknolojileri kullanabilen her bireyi dijital yurttaş yapmaktadır. Çünkü dijital haklara ve erişime sahip birey sayısının fazlalığı; dijital hakları, çevrimiçi güvenliği, etik kuralları bilen ve kişi haklarını dijitalde de savunan tüm bireylerin dijital yurttaş olduğu ifade edilmektedir (Buluş, 2017: 108-109).

21. yüzyılın iletişim teknolojileri ile yükselen bir çağ olması, teknolojinin kolay erişilebilir bir yönünü de ortaya koymuştur. Ağ toplumu olan ve bilgi çağında yaşayan tüm bireylerin dijital erişilebilirlik seviyelerinin yüksekliği, dijital çağda doğan yerlilerin sayısıyla hızla artmıştır. Bu çağda doğan bireyler dijital içeriklere, dijital teknolojilere kısacası dijital olana yatkın bir şekilde dünyaya gelmiştir. Bu bireyler dijital yerliler olarak adlandırılırken; eski kuşakların da dijitale erişim olanaklarının bulunmasıyla bu çağa taşınan dijital göçmenler olarak yerlerini almıştır (Ribble, 2011: 16-17).

Dijital yurttaşlık, önerilen dokuz (9) boyutu farklı dijital araçların kullanılmasıyla günlük hayatta yerleşikleşmiştir. Ribble ise bu boyutları şu şekilde sıralamıştır:

a. Dijital kanun,
b. Dijital hak ve sorumluluklar,
c. Dijital sağlık,
d. Dijital güvenlik,
e. Dijital erişim,
f. Dijital ticaret,
g. Dijital iletişim,
h. Dijital okuryazarlıktır (Çubukçu ve Bayzan, 2013).

Teknolojilerin kullanımı ile belirlenen dijital yurttaşlık algısı yeni teknolojilerin insan hakları doğrultusunda kullanımıyla daha da ön plana çıkmıştır.

Dijital Yurttaş ve Çevrimiçi Haklar

Dijital çağda var olmak, ağa bağlı ve sürekli çevrimiçi olmayı gerektirmiştir. Dijital yurttaşların oluşturdukları dijital kimlikler, dönüşüm sürecinde değişen medyanın siber ortamlarda yer almasının bir sonucudur. Dijital yurttaşlar ekosistemleri olan dijital alanlarda var oldukları sürece çevrimiçi olarak her zaman ağa bağlanılabilir olacaktırlar (Bozkurt, Kaban, Taşçı, Aykul ve Hamutoğlu, 2021).

Dijital ortamda yapılan tüm işlemlerde dijital yurttaşların izleri kalmaktadır. Bu izler beraberinde, yurttaşların internet ortamlarında belli başlı haklarını gündeme getirmiştir. İnternet ortamındaki dijital yurttaş hakları incelendiğinde:

a. Özel hayatın gizliliğinin korunması hakkı,
b. Kişilik haklarının ihlal edilmemesi hakkı,
c. Kişisel verilerin korunması hakkı,
d. İfade özgürlüğü hakkı,
e. İnternet üzerinden yönetime katılma hakkı,
f. İnternet üzerinden şikâyet hakkı,
g. İnternette lekelenmeme hakkı, şeklinde ifade edilmiştir (Bayzan, 2019).

Dijital ortamda haklarını bilmek ve bu hakların gereği doğrultusunda bilinçli bir şekilde internet kullanımını gerçekleştirmek ancak dijital eğitimle ve farkındalık ile gerçekleştirilebilir. Bu süreçte teknolojik eylemler, çevrimiçi haklar her dijital yurttaşın ve dijital yerlinin aktif katılımının sağlanarak; toplumda dijital hakların, siber farkındalığın ve internet ilkelerinin varlığını zorunlu kılmıştır.

İnternetin İlkeleri

İnternet bugünün dünyasında enformasyona ulaşmada hem kitlesel hem de bireysel olarak ilk sırada yer alan önemli bir kaynaktır. İnternette enformasyon edinmenin yanı sıra enformasyon bolluğu ve kirliliği de söz konusu olmuştur. Bugünün bilişim ve iletişim teknolojileri bireylerin hayatlarını ve toplum içerisindeki hayat kalitelerini sürdürmelerine olanak sağlayan büyük bir kamu hizmeti araçlarıdır. Bireyler bu eylemlerin birçoğunu siber ortamda, dijital olarak gerçekleştirmektedir.

İletişim teknolojilerinin hızlı gelişimi ve dönüşümü ile birey elinde bulunan tek bir cihazdan tüm sosyal ihtiyaç ve eylemlerini gerçekleştirebilecek duruma gelmiştir. Bir cihazdan tüm işlemlerini yapabilen birey, medyanın yöndeşmesi ile karşı karşıya kalarak belli bir süreçte gerçekleştirmektedir. Bilgisayar, telekomünikasyon ve yeni iletişim teknolojileri sayesinde yeni medyada; her yerde her türlü medya aracıyla iç içe kullanılabilecek bir döneme geçilmiştir (Jenkins, 2021). Tehlikelerin ve fırsatların bulunduğu siber alanların, aslında insan odaklı bilgi toplumu oluşturma yönündeki ilk adımlarının atıldığı bir gerçeklik haline almıştır.

Sanal olana yönelen eylemler eşliğinde insan hakları, gündelik hayattaki insan hakları kadar önemli bir yer kaplamıştır. Devletlerin, insan haklarını anayasaları ile uyumlaştırmayı başarabilmeleri önemli görevleri arasında yer almıştır. Özel, kamu teşebbüsleri ya da politik aktörlerin neden olabileceği insan hakları ihlallerine karşı yurttaşların korunmalarının sağlanması önemli bir konu olarak ele alınmıştır. Bu ihlallerin siber ortamlarda yer alabileceği gerçeği ile hareket edilmesi dijital yurttaşlık haklarında önemli bir tartışma konusu yaratmıştır.

Dijital eylemlerin gerçekleştiği internet ortamlarında insan haklarını odağına alan birçok internetin ilkeleri geliştirilmiştir. Bu ilkeler:

a. Evrensellik ve eşitlik,
b. Haklar ve sosyal adalet,
c. Erişilebilirlik,
d. İfade ve örgütlenme,
e. Özel hayatın gizliliği ve veri koruması,
f. Yasa, hürriyet ve güvenlik,

g. Çeşitlilik,
h. Ağ eşitliği ve tarafsızlığı,
i. Standartlar ve düzenlemeler ve
j. Yönetim, şeklinde ifade edilmiştir (Franklin, Bodle ve Hawtin, 2014).

Siber Güvenlik ve Dijital Farkındalık

Siber ortamda, artan kullanıcı sayısı gereği dijital yurttaş hakları önemli hale gelmiştir. Güvenliğin, ne tür saldırılara karşı alınması gerektiği ve bu saldırı türlerinin açıklanması, alan terminolojisinin iyi bilinmesi ile gerçekleşmektedir. Korunması gereken dijital yurttaş, korunanın ne veya neyi olduğu konusunda bir soru sormakla başlamasını gerektirmiştir. Dijital yurttaşın korunacak en değerli şeyi ise verisidir. Dijital ortamda bıraktığı izler, dijital yurttaşın rızası olsun ya da olmasın şartlı bir şekilde sunduğu verileridir. Bu nedenle aşağıda sıralanan kavramların ne anlama geldiğinin bilinmesi gerekmektedir. Bu kavramlar:

- *Veri:* dijital ortamda bulunan, taşınan, sinyallerdir. Uygun ortamlarda yapılandırılarak depolanma özellikleri vardır. Gizlilik, bütünlük, erişilebilirlik, doğrulama, yetkilendirilme, inkâr edilemez bilgiler ve temeller üzerinde oluşur (Kara, 2019: 53).
- *Bilgi:* verinin işlenmiş, değerlendirilip analiz edilmiş halidir. Bilişim terimi olarak uygun görülen tanımıdır (TDK, 2022).
- *Siber:* genel olarak elektronik ortamların ismidir. Fakat bilişim alanında verinin işletildiği ortamlar olarak ele alınması nedeniyle bilgisayar, sunucu, cihaz, donanım, algoritma, işlem vb. alanları da içermektedir (Sağıroğlu, vd., 2018: 24).
- *Siber saldırı:* Elektronik veya dijital ortamda dolaşımda olan bireyin, devletin, kurumun bilgisayar ağlarına yapılan zafiyet uygulamaları ve güvenlik duvarlarının suistimal edilmesidir. Dijital sistemler devre dışı bırakılıp veriler çalınmaktadır (Hatipoğlu ve Tunacan, 2021: 431).
- *Siber güvenlik:* bilgisayar ya da ağların siber saldırı sonucunda güvenlik tedbirlerini içeren kavramdır.
- *Siber alan* ise birbiriyle ilişkili sistem, yazılım, donanım ve insanların iletişim ve etkileşimde bulundukları soyut ve somut alanlardır (Aslay, 2017: 25).

Siber Alanda Görülen Saldırılar

Elektronik ve dijital ortam olarak atfedilen siber alanda, yurttaşların maruz kalabilecekleri güncel saldırıların terminolojideki örneklerinden bahsedilmesinde yarar bulunmaktadır. Yurttaşların dijital ortamda farkında olmadan teknik saldırılar ile karşı karşıya kalması bu saldırıların isim ve içeriğinin bilinmesinin bu konuda büyük farkındalık kazandıracağı ön görülmektedir. Bu konuda bazı kurumların ve bireylerin uğradığı siber saldırılar aşağıdaki gibidir:

- *Wikileaks CIA Vault 7 Saldırısı:* ABD Merkez Haber Alma Teşkilatı (CIA)'nın elektronik gözetimi ve siber hareketi gerçekleştirme, etkinlik ve yeteneklerini açıklayan bir dizi belgedir. 2013-2016 tarihli dosyalar, teşkilatın yazılım yetenekleri hakkındaki ayrıntılarda akıllı telefon işletim sistemlerinden, internet tarayıcılarından, Windows işletim sistemlerinden veri ve bilgi çekme olayıdır.
- *Macron Campaign Hack:* Fransa Cumhurbaşkanlığı seçimleri sırasında Emmanuel Macron'un 9 GB boyutundaki özel bilgilerini içeren dosyaların, bilgisayar korsanları tarafından sızdırılmasını konu edinen bir siber saldırıdır.
- *Rampant Veri Sızıntısı:* 2017 ve 2018 yılları arasında özellikle gündeme gelen bir durumdur. Yaklaşık 340 milyon veri herkese açık bir sunucu üzerinde güvenlik ve gizlilik önlemi alınmadan sosyal güvenlik numaraları, kredi kart bilgileri vb. kişisel bilgiler sızdırılmıştır.
- *Veri Teşhiri:* İnternet üzerindeki verilerin herkese açık hale gelmesidir. Bulut kullanıcılarının yanlış yapılandırdığı veri tabanlarından dolayı böyle bir teşhir ortaya çıkmıştır. Dolayısıyla herhangi bir prosedüre gerek duymadan Exactis isimli firma neredeyse 340 milyon veri kaydını genele açık bir şekilde korunaksız bırakmıştır. Veri içeriklerinde güvenlik numaraları ve kredi kartı gibi bilgiler olmasa da yüzlerce Amerikalıya ait bilgiler yer edinmiştir (Sağıroğlu, vd., 2018: 98).

Belirtilen siber saldırılar günlük hayatta çokça karşılaşılabilecek örneklere benzemese de oldukça basit ve dalgınlık sonucu gerçekleşen siber olaylardır. Bu tür olayların en temel taşı olan insan, aynı zamanda en zayıf bileşenini de teşkil etmiştir.

Siber Saldırı, Dijital Ortamlarda Nasıl Fark Edilir?

Siber alandaki tehdidin farkında olunmasında ister kişisel ister kurumsal, isterse de ulusal ya da uluslararası olarak bilginin her şekilde tehdit olarak görülmesi mümkündür. Bu tehditler kimi zaman bilinçli bir saldırı olabilirken, kimi zamansa bilinçsiz şekilde gerçekleşebilmektedir. Aynı zamanda siber saldırılara kaynaklık eden birçok unsur, güncellenerek artmaya devam etmektedir. Yabancı devletlerin tehdidi, siber casuslar, hackerler, siber suçlular, siber ordular vb. bu kaynakların içinde yer almaktadır (Sağıroğlu, vd., 2018: 114).

Her siber saldırının içeriğinde kötü amaçlı yazılım bulunmaktadır. Bu nedenle bilinen kötü amaçlı yazılım çeşitleri ise:

a. *Küresel tehditler:* e-posta ve internet tarayıcılarındaki savunmasızlıklardır.
b. *Gelişmiş kalıcı tehditler:* saldırı hedefindeki belirli kurumların finansal popülerliklerine kalıcı zarar vermektir.
c. *Hizmeti engelleme saldırıları:* saldırı yapılan sisteme sürekli kesintisiz veri gönderimi sağlanarak sistemin cevap vermesini engellemektir.
d. *Virüsler:* kötü amaçlı kod parçacıkları içeren programlardır.
e. *Solucanlar:* bilgisayar ağları kullanılarak, bir sistemden diğerine izinsiz girişlerin olmasıdır.
f. *Truva atları:* normal bir program gibi görünen kötü amaçlı kodlar içeren programlardır.
g. *Arka kapılar:* geleneksel güvenlik duvarlarını atlayıp kullanıcısının bilgisi dışında sisteme uzaktan erişilmesidir.
h. *Fidye yazılımları:* bulaştığı sistemin belirli bir kısmını veya tümünü şifreleyerek kullanıcı tarafından kendi verilerinin görülememesidir.
i. *Korsan amaçlı kullanılan yazılımlar:* bilgisayar komutuna yönetici izni sağlayarak, dosyalara erişilmesi ve yönetici kimliğini gizleyerek sistemde kalınmasıdır.
j. *Robotlar:* savunmasız bilgisayar ağlarının bulunup belirlenen kurbana yapılan saldırılardır.
k. *Casus yazılımlar:* kullanıcı ve şirket bilgilerini gizlice toplayarak üçüncü kişilere gönderen yazılımlardır (Sağıroğlu, vd., 2018).

Bahsedilen siber saldırılara karşı gerekli önlemler; siber farkındalık düzeyleri ve eğitimlerle sağlanmalıdır. Kurumlar açısından çalışanın eğitimini sağlamak, kurum güvenlik kurallarına uyumunu kişisel sorumluluk düzeyine çıkarmak ve denetlenebilirliğin sağlanması bir gereklilik halini almıştır (Arda, 2020: 18). Bireylerin farkındalığı ne kadar yüksekse siber saldırı o derece önlenebilir olmaktadır. Farkındalık, bireylerin kendi sorumlulukları kapsamında ve sahalarında değiştirip dönüştürülebilir olmalıdır. Bu dönüşümler ise eğitim ve güvenlik politikaları ile gerçekleştirilmelidir.

Bireylerin siber saldırılara karşı farkındalık kazanmaları, saldırganlar tarafından seçilen kurbanlar olmalarını engelleyecektir. Bu durumun sağlanabilmesi için eğitim ve farkındalık kazandırılmasını, yapılması gerekenlerde ilk sıraya alınmasını gerektirmiştir. Farkındalık kazanma süreci uzun ve yeteneklerin kazanılması bakımından kolay değildir. Fakat burada üzerinde durulması gereken konu, temel farkındalık eğitiminin bireylere kazandırılması üzerinedir ve bilgi güvenliğini artırmada birtakım yöntemlerin uygulanması gerekmiştir.

Bilgi güvenliği farkındalığının ölçülmesinde kullanılan bazı yöntemler:

a. *Uzman geri beslemeleri:* kullanıcılara verilecek eğitim sonrasında bakış açılarının nasıl değiştiği ve bazı güvenlik olaylarının tartışılması,
b. *Kişisel değerlendirme:* bireylerin kendi güvenliğini anlama ve gelecek planları,
c. *Bilgi testleri:* bilgi güvenliği sorularından oluşan anket veya yazılı sorularla güvenlik seviyesinin ölçülmesi,
d. *Seçici görüşme:* önceden belirlenmiş kriterlere göre on veya daha az kişi ile belirli bir konu üzerinde konuşarak sonrasında geri besleme alma,
e. *Güvenlik programı kıyaslaması:* iki farklı kurumun, durum üzerinde yapmış oldukları kıyaslamalardır (Sağıroğlu, vd., 2018: 127-128).

Bireyler içinse eğitim müfredatlarında ve yükseköğrenim derslerinde alanı fark etmeksizin farkındalık eğitimi verilmelidir. Bu faaliyetleri gerçekleştirmek adına bazı kuruluşlar dijital içerikler hazırlamaktadır. Bu içeriklerden bazılarına aşağıda yer verilmiştir.

Akıllı cihazlar için önerilen güvenlik yöntemlerinden bilgisayarlar için öneriler:

1. Cihazlarda güçlü bir şifre, PIN kullanılmalı ve periyodik olarak değiştirilmelidir.
2. Cihaza oyun ve uygulama yüklemeden önce söz konusu programın, hangi süreçlerde erişim izni istediği belirlenmelidir.
3. Zararlı yazılımlara karşı virüs temizleme programları kullanılarak cihaz periyodik olarak taratılmalıdır.
4. Kullanılmadığı zaman cihazı otomatik kilitleyecek zamanaşımı koyulmalıdır.
5. Kullanılmadığı zamanda Wi-Fi, Bluetooth gibi özellikler kapalı tutulmalıdır.
6. Kamusal ağlarda VPN kullanılmalıdır.
7. Bluetooth kullanırken kimliği doğrulanmamış cihazlara karşı cihaz görünmez kılınmalıdır.
8. Cihaz içi verilerin bir kopyasının alınması ihmal edilmemelidir.
9. Cihaz kaybolduğunda eğer varsa uzaktan silme özelliği etkinleştirilmelidir (Bilgi Teknolojileri ve İletişim Kurumu - BTK, 2014).
10. Kişisel veriler mümkün oldukça HTTPS kullanan sitelere girilmelidir.
11. İstenmeyen e-postalarla gelen bağlantılara tıklanmamalı ve ekleri cihazda açılmamalıdır.
12. Cihazlarda mümkün oldukça son sürüm kullanılmalı ve sürekli olarak güncellemeleri kontrol edilmelidir (Dijitalgüvenlik, 2019).

Telefonlar için öneriler:

a. *Ekran koruyucu şifre:* telefonların ansızın kaybolması durumunda telefon ekranlarına şifre/pin gibi giriş koruması yapılmalıdır.
b. *Temel güvenlik ayarları:* telefonun fabrika ve işletim ayarlarının değiştirilmesi gibi işlemler, telefonu siber saldırılara karşı daha duyarlı yaparken işletmeci ve telefon tarafından sunulan güvenlik özelliklerini zayıflatmaktadır.
c. *Telefon yedeklemesi ve veri güvenliği*: telefonda yer alan fotoğraf, rehber ve diğer belgelerin hepsinin yedeğinin alınması tavsiye edilmektedir. Bu veriler, kişisel bilgisayarlarda ve bulut ortamlarında saklanmalıdır.
d. *Uygulamaların erişim yetkinliklerini kontrol etmek:* indirilen uygulamalar ve var olan uygulamaların çeşitli erişim yetkinliklerinin olduğu kontrol edilmelidir. Örneğin, uygulamaların kullanıcı izni almadan konum üzerinden işlem yapılabilir. Bu nedenle her bir uygulama için izinler tek tek kontrol edilmelidir.
e. *Güvenilir kaynaklardan uygulama indirilmeli:* uygulamanın yasal ve güvenilir olduğundan emin olmak gerekmektedir. İşletim sistemlerinin uygulama mağazaları tercih edilmelidir.
f. *Uzaktan etkileşim ile silmeyi gerçekleştiren uygulamaları açmak:* bu uygulama ile telefonun GPS özelliği kapalı olsa bile telefondaki verilere uzaktan erişilip söz konusu verilerin silinmesi mümkündür.
g. *Açık Wİ-Fİ bağlantıları:* ücretsiz ve şifresiz ağ hizmetlerine girişlerde hizmet sağlayıcıları tarafından denetlenmelidir.
h. *Yazılım güncellemeleri:* otomatik güncellemeler açık tutularak işletim sisteminde operatörlerden gelen sürüm güncellemeleri kabul edilerek siber tehditler azaltılmalıdır.
i. Çalınan telefonun bildirilmesi: hattı kapatmak için telefon operatörüne başvurmak gerekmektedir. Telefonun ülkedeki kullanımını engellemek içinse BTK'ya bildirimde bulunulmalıdır (USOM, 2014: 16-18).

Sonuç

Dijital yetkinlikler ve içerikler günümüzde vazgeçilmez bir araç haline ve iletişim yöntemine gelmiştir. Dijital içerikler internetle birlikte oldukça kolay bir şekilde ulaştırılmakta, dağıtılmakta ve paylaşılmaktadır. Dijital çağdaki yaşam pratikleri içerisindeki toplumsallaşma süreçlerinde, dijital teknolojiler ve internet ağları süreci yeniden dizayn etmiştir (Demirel ve Durgeç, 2022: 32). Günümüzde dijital alanda internet ve diğer kitle iletişim araçları olmadan hedef kitlelere ulaşmak kolay değildir. Fakat günümüz toplumları dijitalleşme ile hızlıca gelişme göstermiş; teknolojinin hızlı evrimi ve yüksek orandaki dönüşümü ile bilgi toplumları, ağ toplumlarına evrilerek iş süreçlerini bir networke dönüştürmüşlerdir.

Toplumların enformasyon ihtiyacı hiçbir dönem yeterli görülmemiş ve enformasyona duyulan ihtiyaç her geçen gün artış göstermiştir. Üretilen enformasyonun mikta-

rı internet ile birlikte kapsamlı bir şekilde artmaya devam etmiştir. Yeni medya ise dönüşümün başat rollerinden birini üstlenmiştir. Bilgiye ve enformasyona ulaşımda internet her ne kadar önemli olsa da içeriklerin oluşturulması, kullanıcıların yeni medya ortamlarındaki içeriklere erişebilmesi; bu alanların işlevselliğini ve güvenlik konularında bir takım soru işaretlerini beraberinde getirmiştir. İnternet ve dijital içerikler bağlamında sınırsız ortam, siber alan olarak ifade edilmiştir. Siber alanda tehdit ve güvenlik konuları giriş seviyesinde verilecek eğitimler, güvenlik problemlerine karşı olumlu sonuçlar doğuracağı varsayılmaktadır.

Siber güvenliğin gün geçtikçe çok önemli hale gelmesi Türkiye'de siber suçların önlenmesine yönelik Bilim, Sanayi ve Teknoloji Bakanlığının koordinatörlüğünde Bilgi Teknolojileri ve İletişim Kurumu (BTK) ile sivil toplum kuruluşları ve kurumlar tarafından 2012 yılına kadar sürdürülmüştür. Bu tarihten sonra ise "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" ile yürütülmeye başlanmıştır (STM, 2023). Türkiye'nin Ulusal Siber Güvenlik Stratejisi, 2013-2014 dönemi ile 2016-2019 dönemleri gözden geçirilmiş ve iyileştirmeler yapılmasını gerektirmiştir. Bu konuda belirlenen stratejiler çerçevesinde amaçlar 8 ana başlık altında toplanmıştır: kritik altyapıların korunması ve mukavemetin artırılması, ulusal kapasitenin geliştirilmesi, organik siber güvenlik ağı, yeni nesil teknolojilerin güvenliği, siber suçlarla mücadele, yerli ve milli teknolojilerin geliştirilmesi ve desteklenmesi, siber güvenliğin milli güvenliğe entegrasyonu, uluslararası iş birliğinin geliştirilmesi başlıklarından oluşmuştur. Gerçekleştirilmesi planlanan 8 adet stratejik amaçla ilişkilendirilen 40 adet eylem ve 75 adet uygulama adımı Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) kapsamında yer almıştır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2023).

Bilgi ve iletişim teknolojileri bir yandan bireylerin hayatlarını kolaylaştırırken diğer yandan ise haberleşme, enerji, finans, ulaştırma ve su yönetimi gibi önemli alanlarda siber riskler hem bireysel hem de toplumsal güvenliği tehlikeye atmıştır. Bu nedenle ortaya çıkan güvenlik riskleri, siber güvenliğin bireysel ve toplumsal boyutta değerlendirilmesini gerekli kılmıştır. Dünyada bu çerçevede sıralama yapan 2019 Uluslararası Telekomünikasyon Birliği Global Siber Güvenlik Endeksi'nde Türkiye bir önceki yıla göre 23 sıra birden yükselerek 2018 yılında dünyada 20'nci sırada, Avrupa'da ise 11'inci sırada kendisine yer bulmuştur (Global Cybersecurity Index, 2021). Dijital dönüşümün gerçekleştirilmesinde kamu ve özel sektöre yönelik faaliyetlerde bulunan GlassHouse, 10-11 Şubat'ta düzenlenen Güvenli İnternet gününde siber saldırıları ve oluşabilecek zararların azaltılması konusunda Genel Müdür Alp Bağrıaçık, veri güvenliğine yönelik 10 öneride bulunmuştur:

- Siber güvenlik uzmanıyla çalışılması
- İşletme içinde siber güvenlik eğitimleri verilmesi
- Küçük işletmelerin de siber saldırıya uğradığı
- Verilerin şifrelenmesi
- Yedeklemenin önemi
- Güncellemelerin sıkı takibi
- Yeni teknolojilerden yararlanılmasının gerekliliği
- Bulut sistemlerin gerekliliği
- Güvenlik konusuna yatırım yapılması
- Felaket ve tehlikelerde kriz yönetimi çalışılmalıdır (Bağrıaçık, 2020).

Siber saldırıların etkilerinin hem kurumlar hem de bireyler tarafından tespit edilmesi her zaman kolay değildir. Burada güvenlik politikaları devletler tarafından kanunlar ve yasal düzenlemelerle yürütülmelidir. Yanı sıra özellikle bireylerin farkındalık düzeylerini artırmada eğitim kurumları ve sivil toplum örgütlerine önemli görevler düşmektedir. Kurum içi ve kurumlar arasında siber farkındalık eğitimleri ve uygulamaları sağlanmalıdır. İnternet ve siber ortamda tüm insanlar için temel hak ve özgürlüklerin, demokrasinin, kalkınmanın ve sosyal adaletin tam anlamıyla uygulanabilmesi temel bir ihtiyaç haline gelmiştir (Franklin, Bodle ve Hawtin, 2014: 12). Siber âleme yönelik yapılacak güncel çalışmalar, farkındalık yaratılması adına oldukça önem taşımaktadır.

Extended Abstract

II. After the World War II, the transition to a period of digitalization movements began with the internet. The emergence of digitalization began in the 1980s. Thus, there has

been a process in which the transition from traditional mass media to new mass media has begun. With the digitizing – digitalizing communication environment, in which the weight of the Internet is felt, it has ensured that mass communication is personalized and individual users can be reached. Printed media, especially newspapers and magazines, have begun to be integrated into the digital environment. Radio and television; It has made it possible to watch and record it again and again in the online environment. People have been able to meet their needs such as banking transactions, shopping, taking photos, recording videos, listening to music, having fun and getting information from devices such as phones, tablets and PCs connected to the internet. The concepts of time and space become history; Users were able to access information at any time and in any environment online. Usage habits and the duration of being connected to the network have become an indispensable tool of life, increasing day by day.

The content produced could be delivered to millions of people in a few seconds in the digital environment where the borders called globalization disappeared. With the transformation of media into digital; new situations have emerged such as the digital, digital content and the transformation of the masses to become digital citizens. Digital media, which is an interactive field, is a fairly new concept. The characteristics of new media in general; it has features such as being digitized, multimedia layer, interactivity, being independent of time and space, and adapting to the digital space. McLuhan's "media is the message" expression, which has become the identities of individuals in the transformed media, has become a phenomenon that depicts the human body (Erdoğan and Alemdar, 2005: 444). Digital space; although it has become a remote, accessible, interactive area where immediate feedback can be obtained; can communicate with individuals all over the world. Digital citizens, who witness the developments with information and communication technologies, are emerging. The disappearance of borders with globalization makes every individual who can use digital technology a digital citizen. Because the high number of individuals with digital rights and access, it is stated that all individuals who know digital rights, online security, ethical rules and defend personal rights digitally are digital citizens (Buluş, 2017: 108-109).

The perception of digital citizenship determined by the use of technologies has come to the fore even more with the use of new technologies in line with human rights. Existing in the digital age has required being connected and constantly online. The digital identities created by digital citizens are the result of the changing media taking place in cyber environments during the transformation process. In all transactions made in the digital environment, traces of digital citizens remain. These traces bring up certain rights of citizens on the internet. Among these rights: the right to protect the privacy of private life, the right to the protection of personal data, the right to freedom of expression took place. Realizing the conscious use of the internet in line with the requirements of these rights and knowing their rights in the digital field can only be realized with digital education and awareness. In this process, online actions and online rights ensure the active participation of every digital citizen; the existence of digital rights, cyber awareness and internet principles in society has become mandatory. These rights include: universality and equality; privacy and data protection; law, liberty and security, etc. principles are included. In the cyber environment, digital citizens' rights have become more important due to the increasing number of users. The digital citizen who needs to be protected should start by asking a question about what or what is being protected. The most valuable asset of a digital citizen to be protected is his data. The traces left in the digital environment are the data that the digital citizen provides conditionally, with or without the consent of the digital citizen. Among the types of attacks that citizens can be exposed to in cyberspace, which is attributed as electronic and digital media, in terminology: "Wikileaks CIA Vault 7 Attack, Macron Campaign Hack, Rampant Data Leak, …" etc. can be expressed as.

In being aware of the threat in the cyber field, it is possible to see it as a threat in every way, whether it is personal, institutional, national or international. While these threats

can sometimes be a conscious attack, sometimes they can happen unconsciously. Every cyberattack contains malware. So among the known malware variants: global threats, advanced persistent threats, viruses, trojans, backdoors, etc. (Sağıroğlu, et al., 2018).

Necessary measures against the mentioned cyberattacks; cyber awareness levels and training should be provided. The higher the awareness of individuals, the more preventable a cyberattack is. Awareness of individuals against cyberattacks will prevent them from being the victims chosen by the attackers. For individuals, awareness training should be given in education curricula and higher education courses, regardless of the field. In addition, each digital citizen should consciously carry out learning activities on his own. In order to carry out these activities, it is seen that a number of institutions and organizations prepare informative digital content.

Kaynakça

Alberta. (2012). *Digital citizenship policy development guide.* Edmonton: School Technology Branch Alberta Education.

Arda, E. (2020). Siber Uzay Ortamında Saldırı Tehditlerinin Farkındalığı, Tespiti Ve Önlenmesi Üzerine Bir Gerçek-Zaman Sistem Önerisi. Yüksek Lisans Tezi. Ankara: Başkent Üniversitesi.

Askeroğlu, E. D., Karakulakoğlu, S. E. (2019). Geleneksel Medyadan Yeni Medyaya Geçiş Sürecinde Değişen Gaztececilik 'Yurttaş Gazeteciliği': Kuşaklar Üzerine Bir Araştırma. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi,* 7(1), 508-536.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1), 24-28.

Bağrıaçık, A. (2020). Siber Saldırıdan Korunmanın Yolları – Basın Bülteni https://www.glasshouse.com.tr/list/haberler/siber-saldiridan-korunmanin-yollari-basin-bulteni. (E.T.: 15.11.2023).

Bayraktar, G. (2018, Temmuz). Türkiye'de Veri Gazeteciliği: Medya Profesyonellerinin Veri Gazeteciliği Algısı Üzerine Bir Araştırma. https://www.voyd.org.tr/tr/blog/204/turkiyede-veri-gazeteciligimedya-profesyonellerinin-veri-gazeteciligi-algisi-uzerine-bir-arastirma/ adresinden edinilmiştir.

Bayzan, Ş. (2019, Kasım 6). Dijital Hak ve Sorumluluklarımız Nelerdir?. https://www.guvenliweb.org.tr/haber-detay/dijital-hak-ve-sorumluluklarimiz-nelerdir adresinden edinilmiştir.

Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı. (2014, Kasım). Taşınabilir Cihaz Kullanımına İlişkin Riskler. UR.RHB.006. https://dsy.usom.gov.tr/usom/19/02/190211084314_Tasinabilir%20Cihaz%20Kullanimina%20Iliskin%20Riskler.pdf adresinden edinilmiştir.

Bozkurt, A., Hamutoğlu, N. B., Kaban, A. L., Taşçı, G., Aykul, M. (2021). Dijital Bilgi Çağı: Dijital Toplum, Dijital Dönüşüm, Dijital Eğitim Ve Dijital Yeterlilikler. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 7(2), 42-44.

Brennen, S., Kreiss, D. (2014, September 8). Digitalization and Digitization. https://culturedigitally.org/2014/09/digitalization-and-digitization/ adresinden edinilmiştir.

Buluş, B. (2017). Yetişkin Yeni Medya Okuryazarlığı: Avrupa Birliği ve Türkiye Örnekleri. Yüksek Lisans Tezi. Ankara: Hacettepe Üniversitesi.

Castells, M. (2005). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür* (Cilt 1) (Çev. E. Kılıç) İstanbul: İstanbul Bilgi Üniversitesi.

Comcast. L. H. Leading the Digital Revolution. https://corporate.comcast.com/news-information/news-feed/lisa-hsia adresinden edinilmiştir (E.T.: 08.01.2023).

Çubukçu, A., Bayzan, Ş. (2013). Türkiye'de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. *Middle Eastern & African Journal of Educational Research,* 7, 148-174.

Demirel, S. D., Durgeç, P. (2022). Dijital Medyada Deprem Haberlerini İnfografikler Üzerinden Okumak: Anadolu Ajansı ve TRT Haber Örneği. *Journal of Communication, Sociology and History Studies,* 2(2), 27-44.

Dijitalgüvenlik. (2019). Saldırganlar Kişisel Verilerinizin Peşinde: Onlara Engel Olun! https://www.dijitalguvenlik.org/kisisel-veriler/saldirganlar-kisisel-verilerinizin-pesinde-onlara-engel-olun/ adresinden edinilmiştir.

Downing, J. (2004). *The SAGE Hand book of Media Studies*. In J. D. H. Downing (Ed.) California: Sage Publications.

Einav, G. (2015). *The New World of Transitioned Media Digital Realignment and Industry Transformation.* G. Einav (Ed.) New York: Springer International Publishing.

Erdoğan, İ., Alemdar, K. (2005). Marshall McLuhan Araç İnsanın Uzantısıdır. İ. Erdoğan, ve K. Alemdar (Ed.) Öteki Kuram *Tarihsel ve Eleştirel Bir Değerlendirmesi* içinde, (s. 440-444). Ankara: Erk.

Fidler, R. (1997). *Mediamorphosis:Understanding New Media.* U.K.: Sage Publications.

Franklin, M., Bodle, R., Hawtin, D. (2014, Ağustos). İnternette İnsan Hakları ve İlkeleri Şartı. B. S. Bakioğlu (Ed.), (Çev.: S. Kaledelen). İnternet Hakları ve İlkeleri Dinamik Koalisyonu (İHİDK) Birleşmiş Milletler İnternet Yönetimi Forumu.

Global Cybersecurity Index – 2021. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (E.T.: 15.11.2023).

Gökçe, M. (2022). *Yeni Medya İletişim, Kültür, Toplum ve Dijital Değişim.* https://www.academia.edu/30800642/Yeni_Medya_%C4%B0leti%C5%9Fim_K%C3%BCl%C3%BCr_Toplum_ve_Dijital_De%C4%9Fi%C5%9Fim. adresinden edinilmiştir.

Gürcan, H. İ.,Kumcuoğlu, İ. (2017). Medya Profesyonellerinin Gözüyle Yeni Medya Sektörünün Yapısı ve Sorunları. *e-Kurgu Anadolu Üniversitesi İletişim Bilimleri Fakültesi Uluslararsı Hakemli Dergisi*, 25(1), 65-76.

Hatipoğlu, C., Tunacan, T. (2021). Türkiye'de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması. *BŞEÜ Fen Bilimleri Dergisi*, 8(1), 430-445.

Hazer, O. (2020). Yeni Medya ve İletişim Teknolojileri: Ailede Sosyal Etkileşim. Gençlik ve Dijital Çağ. *Hacettepe Gençlik Araştırmaları ve Uygulama Merkezi*, 92-93.

Jenkins, H. (2021). Medya Yöndeşmesinin Kültürel Mantığı. F. Aydoğan (Ed.), *Yeni medya kuramları* içinde (ss. 33-44). İstanbul: Der Yayınları.

Kara, İ. (2019). Dijital Verilerin İmha Süreçlerinin Tanımlanması ve Uygulama Yönünden Değerlendirilmesi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimler Dergisi*, 3(2), 53-58.

Karaduman, S. (2019). Yeni Medya Okuryazarlığı: Yeni Beceriler/Olanaklar/Riskler. *Erciyes İletişim Dergisi*, 6(1), 683-700.

Lister, M., Dovey, J., Gıddıngs, S., Grant, I., Kelly, K. (2003). *New Media A Critical Introduction Second Edition* . New York: Routledge.

Öztürk, T. A. (2010). 1990 Yılı Ve Sonrası Türkiye'de Kitle İletişim Araçları Ve Müzik-Medya Üzerindeki Etkisi. Yüksek Lisans Tezi. İstanbul: İstanbul Teknik Üniversitesi.

Poster, M. (2021). Postmodern Gerçeklikler. F. Aydoğan (Ed.), (Çev.: Ö. Aydınlıoğlu). *Yeni medya kuramları* içinde (ss. 122-123). İstanbul: Der Yayınları.

Ribble, M. (2011). Digital Citizenship in Schools. Copyright ISTE (International Society for Technology in Education).

Sağlam, M., Topsümer, F. (2019). Üniversite Öğrencilerinin Dijital Oyun Oynama Nedenlerine İlişkin Nitel Bir Çalışma. *Akdeniz İletişim Dergisi*, 32, 485-504.

Sağıroğlu, Ş., Alkan, M., Samet, R., Ulutaş, G., Yalman, Y., Şengül, G., . . . Urfalıoğlu, R. (2018). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık.* Ankara: Grafiker Yayınları.

STM .(2016). Temmuz Eylül Dönemi Siber Tehdit Durum Raporu. Mühendislik Teknoloji Danışmanlık. https://afyonluoglu.org/PublicWebFiles/Reports-TR-SG/2016%20T%C3%BCrkiye%20Siber%20Tehdit%20Durum%20Raporu-STM.pdf (E.T.: 16.11.2023).

Şeberoğlu, A. (2020). Yeni Medya ve Etkileşimli Yeni Sinema. *Yeni Medya Hakemli, Akademik, E-Dergi*, 8, 77-85.

T.C. Ulaştırma ve Altyapı Bakanlığı. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023. https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf. (E.T.: 15.11.2023).

TDK. https://sozluk.gov.tr/ (E.T: 24.11.2022).

Ulusal Siber Olaylara Müdahale Merkezi (USOM). (2014, Temmuz). Akıllı Telefonlarda Güvenlik. Türkiye.

We are social. (2022, Mart 10). Digital 2022: Another Year Of Bumper Growthhttps://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/ adresinden edinilmiştir.

Yanık, A. (2016). Yeni Medya Nedir Ne Değildir? Uluslararası Sosyal Araştırmalar Dergisi, 9(45), 898-910.