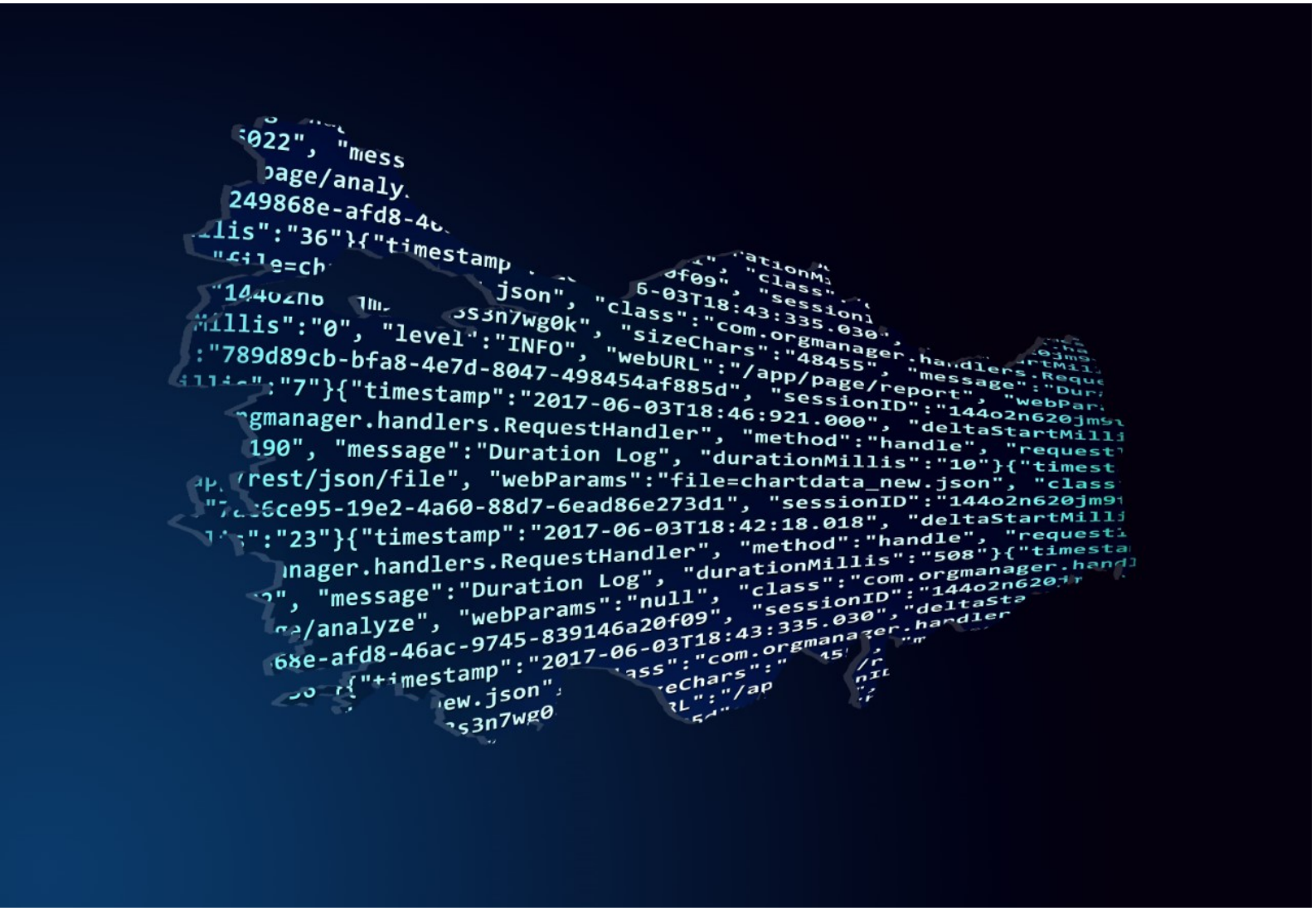
ULİSA12
2021 | Ocak



Mühendislik, Hukuk, İletişim & İktisat Perspektifinden

Siber Güvenlik

&

Sosyal Medya

ULİSA
28 Ocak 2021

ULİSA12
2021 | Ocak

Ankara Yıldırım Beyazıt Üniversitesi
Uluslararası İlişkiler ve Stratejik Araştırmalar (ULİSA) Enstitüsü
Institute for International Relations and Strategic Research

Kapak Dizaynı: İbrahim Demir & Cem İpek

Editörden

Bilgi güçtür. Bilgiye sahip olan güce de sahip olur. Bilgi dinamiktir ve değişime tabidir. Değişen bilgiye hakim olan değişimi yakalar ve değiştirir. Sosyal medya platformları, hükümetlerin dahi toplayamayacağı bilgi ve sosyal veriyi ticari faaliyet adı altında toplama, işleme (analiz) ve kullanma kapasitesine sahiptir. Sosyal medyanın etkin bilgi paylaşımından kaynaklanan refah artırıcı rolüne karşın bu durum, mücadele edilmesi son derece maliyetli bir güvenlik sorunudur. Kişisel veriler kanunla koruma altına alınmışken haberleşme ve eğlenceye dayalı ticari faaliyet adı altında toplanan 'sosyal veri' korunamamakta ve ülke dışı sunucularda depolanmaktadır.

Sosyal veri sayesinde bir toplumun reaksiyon fonksiyonu ve sosyal fay hatları istihbarat, suç ve terör örgütleri tarafından çıkarılıp manipüle edilebilir. Bu manada 'büyük verinin' hacmi kadar amacı da 'büyüktür'. Bu yüzden, 'sosyal veri' tanımlanıp yasal olarak düzenlenmelidir ve bu verinin ülke dışına çıkışı yasaklanmalıdır. Kişisel Verinin Korunması Kanunu (KVKK) sosyal verinin korunmasına ve sosyal verinin toplanıp ülke dışındaki sunucularda depolanmasından kaynaklanan yeni tehditlerle baş etmede yetersizdir. Bu yüzden KVKK'ya benzer bir yasal düzenleme sosyal verinin korunması için de yapılmalıdır.

ULİSA 12'nin bu sayısı da işte bu yeni tehdit ve fırsatlara odaklanmaktadır. Doç. Dr. Mikail Batu, sosyal medya kullanımını iletişim bilimi temelinde ele aldığı eserinde, ağ teknolojilerinin tarihi gelişimine kısaca değindikten sonra, birey ve grupların sosyal ağlara dahil olma ve bu ağlarda daha çok etkinlik gösterme itkilerini incelemektedir. Salgın dönemindeki tecrübelerin sosyal ağ kullanımına olan etkilerini de tetkik eden Batu, ilkokuldan başlayarak sosyal medya kullanımı eğitiminin ve bilincinin verilmesi gerektiğini savunmaktadır.

Dr. Öğr. Üyesi Mustafa Yeniad, sosyal ağların siber güvenlik konusuyla olan ilgisine eğildiği yazısında, önce sosyal ağların teknolojik ve ekonomik olarak ne anlama geldiğini anlatmakta ve konunun sosyal mühendislik boyutunu ön plana çıkarmaktadır. Konunun bilgi güvenliği gibi daha teknik alanlarına da değinen yazar, sosyal ağ ortamlarında dikkat edilmesi gereken hususlara da yer vererek, genel tüketici için önerilerde bulunmaktadır.

Dr. Hatice Kübra Ecemiş Yılmaz, siber uzay, siber güvenlik ve dijital egemenlik konularını uluslararası hukuk penceresinden ele aldığı yazısında, uluslararası hukukun siber uzayla ilgili eriştiği yaptırım ve düzenleme seviyesinden ve devam eden sorunlardan bahsetmekte, beynelmilel örneklerden bahsetmekte egemenlik kavramının dijital alandaki yansımalarını tartışmaktadır. Yılmaz, çalışmasını, uluslararası hukukun bu alandaki zafiyetlerinin giderilmesi için birtakım önerilerle neticelendirmektedir.

Doç. Dr. İbrahim Demir ve Doç. Dr. Fatih Cemil Özbuğday, siber güvenlik alanının endüstriyel organizasyonunu ele aldıkları çalışmalarında, konuya iktisadi açıdan yaklaşmakta ve kanunla korunan kişisel verilerin aksine, daha büyük ehemmiyet kesbetmekte olan sosyal verinin korunmasına ilişkin oluşan açığa dikkat çekmektedirler. Sosyal medya ve iletişim platformlarının iktisadi hayatta işgal ettikleri yeri ve bireylerin bu platformlara olan ilgisine dair pratik örnekleri, teorik mülahazalarla değerlendirmektedirler.

ULİSA 12'nin bu sayısının, kamuoyu gündeminde olan siber güvenlik ve sosyal medya tartışmalarına ışık tutabilmesini ve 'siber vatana' faydalı olmasını umuyoruz.

Sayı Editörü

Yönetici Özeti

- **Sosyal ağların web 2.0 ile etkileşim temelinde hizmet sunması; farklı eğitime, kültüre, ekonomik yapıya, yaşa, yaşam koşullarına sahip olan ve teknik bilgisi olmayan kişileri kolaylıkla kullanıcı haline getirmiştir.**
- Askeri amaçla ABD tarafından ARPA'nın (Advanced Research Projects Agency / İleri Araştırmalar Projeleri Ajansı) kurulması ve araştırmacıların birbirilerinin çalışmalarını görmelerinin istenmesi ve 1969 yılında sistemin bir ağla karşılıklı bağlanmasıyla ARPAnet adı verilen sanal ağların temeli atılmıştır.
- **Türkiye gibi birçok ülkede konunun sosyal ve iletişim boyutunun ilk başlarda pek üzerinde durulmamıştır. Çünkü yeni medyanın sunduğu imkânlar iş ve sosyal hayatı kolaylaştırmış ve bu "kolay hayatın" cazibesine kapılmak kaçınılmaz hale gelmiştir. Genel hayatını değiştirmek isteme, kişisel ve toplumsal sorunlardan sıkılma veya bunlardan kaçmaya çalışma gibi birçok farklı nedenle sosyal ağlar bir kaçış veya eğlence ortamı olarak görülebilmektedir.**
- Sosyal medya içerik üreticileri de hem gelecekte müşteri kazanmak hem de daha savunmasız olması nedeniyle çocukları hedef kitle olarak seçebilmektedir.
- **COVID-19 salgını sürecinde ise sosyal medya ağları kişisel ve toplumsal hayatta çok daha fazla yer bulabilmiştir. Her yaş grubunu, her mesleği diğer yandan her kurum ve sektörü doğrudan veya dolaylı yoldan etkileyen salgın, genel ve alışkın olunan hayat akışının dışına çıkılmasını zorunlu hale getirmiştir.**
- Sosyal medya hepimizin hayatında kaçınılmaz öneme sahip ve hayatımızdan çıkarmamız neredeyse mümkün olmayan bir ortam olarak tanımlanabilir. Bu önemli ortama yönelik sosyal medya okuryazarlığı eğitimlerine katılmak veya bu konuda ilkokuldan itibaren eğitim verilmesi gerektiğini ilgili birimlere duyurmak gerekmektedir.
- **Bireylerin günlük kullanımlarına ek olarak kamu ve özel sektör kurum ve şirketlerinin internet kullanımları artarak devam etmektedir**.
- Günümüzde siber tehditler ve sosyal mühendislik yöntemleri için en kullanışlı araç "sosyal ağlar"dır. İnternet tarihinin en eski ve en tehlikeli saldırı türlerinden biri olan sosyal mühendislik saldırılarının vereceği zararlar yetkisiz erişim elde etmek, itibar ve güven kaybı, veri hırsızlığı, sistemi çalışmaz hale getirme ve hedef kurum ya da kişilikleri yasal yaptırımlarla karşı karşıya bırakma şeklindedir.
- **"Siber güvenlik" bilişim sistemlerinde sürekliliğin ve veri bütünlüğün (değişmezliğin) sağlanması, gizliliğin (yetkisiz erişime karşı) korunması amacıyla yürütülen faaliyetleri ifade etmektedir. Siber güvenlik ihtiyacı ve endişeleri sebebiyle kamu kurumları hem özel şirketler bütçelerinin önemli bir kısmını bu alana ayırdıkları görülmektedir.**
- Sosyal ağlardaki içerikler, servisi sağlayan firmanın sisteminde -yedekleme gereği sunulan seçenekler sayesinde- depolandığından bu veriler üçüncü şahıs veya kurumlarla paylaşılabilir hale gelmektedir.
- **Siber alan, uluslararası toplumun geleneksel siyasi, sosyal ve ekonomik yapılarına meydan okumuştur.**
- Siber uzayın ortaya çıkışı, bireysel ve toplu güvenlik için büyük zorluklar ortaya çıkarmıştır. Kritik ulusal altyapı, siber saldırılara karşı savunmasız kalmış olup; dünya ekonomisi siber suç ve siber casusluk tarafından tehdit edilmeye ve bireyler ise bilgisayar korsanları tarafından terörize edilmeye başlamıştır.
- **Devletler siber saldırıların uluslararası hukukta var olan savaş hukuku kuralları içerisine dahil edilip edilemeyeceğini tartışmaya devam etmektedirler**.
- Siber uzaydaki hukuk konusu olabilecek aktörler devletlerden, internet şirketlerinden, büyük ya da küçük işletmelerden, bireylerden ve bunlara benzer çok çeşitli aktörlerden oluşabilirler. Her bir aktör siber uzay ile ilgili kendi ilgi alanlarına göre farklı sorunlara sahip olabilirler. Bu nedenle de siber uzayda uluslararası hukuk kurallarının yapılmasının kimler için meşru olacağının ya da hangi konuları içereceğinin tespit edilmesi son derece güç olacaktır. Siber alandaki aktörlerin

karmaşık yapısı uluslararası alanda bağlayıcı olacak kuralların konulmasına engel olmaktadır.

- **Hukuk kuralları açısından her ne kadar Budapeşte Sözleşmesinin siber uzay ile ilgili konuları içeren uluslararası antlaşma olduğu söylenebilse de anlaşmazlıkları çözmek adına bağlayıcı bir mekanizmasının olmaması, siber saldırılardan çok siber suçlara odaklanmış olması, genellikle devlet merkezli olması sözleşmeyi zayıf hale getirmektedir**.
- Gelişen teknoloji ve iletişim araçları sonucunda, siber savaşların geleneksel savaşlara nazaran daha cazip olduğu düşünülmeye başlanmıştır. 1) Maliyetin düşük olması, 2) tanınma veya tespit edilmenin zor olması, 3) sınır tanınmaması, 4) beklenmedik anda saldırıda buluna bilinmesi ve 5) geniş etki alanına rağmen can kaybının olmaması ya da çok az düzeyde olması siber savaşları daha cazip hale getiren nedenler arasında sayılabilecektir.
- **Son yıllarda devletler ile devlet dışı aktörler internet ile ilgili altyapı, veri ya da bilgi üzerine kontrolü daha fazla sağlamak amacı ile dijital egemenlik fikrini teşvik etmeye başlamışlardır. Ancak bu durum konunun daha karmaşık hale gelmesine, siber güvenliğe ilişkin ortak oluşturulabilecek uluslararası hukuk normlarının oluşturulmasının zora sokulmasına neden olmaktadır.**
- Sosyal medya platformları ekonomik manada 'etkin'dirler. Sosyal medyada birim bilgi paylaşım maliyeti tek tek bireylerle paylaşım maliyetlerine göre son derece düşüktür. Sosyal medya platformlarındaki iletişim ve dijital veri paylaşımı, piyasalardaki bilgi seviyesini artırmakta ve daha iyi kararlar alınmasını sağlayabilmektedir.
- **Bireyler kendilerine ilişkin veriyi aşağı-yanlı bir şekilde değerlemekte yani olduğundan daha değersizmiş gibi algılamaktadır. Bu yüzden bireyler kendilerine ait veriden çok düşük bir bedel karşılığında vazgeçebilmektedirler. Ancak tek başına bir birey için çok fazla anlam ifade etmeyen bilgi, diğer bireylerin bilgisi ile çok düşük bir maliyetle birleştirilebilmekte, istatistiki güç kazanabilmekte ve 'sosyal risk' hesaplamalarında kullanılır hale gelmektedir.**
- Sosyal medya hizmetleri karşılığında 'nakit' formunda ya da parasal bir ödeme olmaması bu hizmetlerin 'bedava' olduğu anlamına gelmez. Nakit ödeme olmasa da bir barter malın malla değiştirilmesi, yani bir trampa (barter) söz konusudur. Bireyler bu piyasalardan aldıkları hizmetin karşılığını tercih ve davranışlarına ilişkin veri yani 'kişisel bilgi' ile 'ayni' olarak ödemektedirler.
- **Sosyal medya platformlarının konu olduğu şebeke dışsallığı, bu platformların kullanıcı (abone) sayısı arttıkça bireysel bir tüketiciye sağladığı faydanın da artması anlamına gelmektedir. Bu da, tüketici sayısı fazla olan platformlardan vazgeçme eğilimini azaltmaktadır**.
- Sosyal medya platformlarının konu olduğu şebeke etkileri belli bir sayıda kullanıcının aktif olmasından sonra devreye girer. Şebeke etkilerinin görülmeye başlandığı kullanıcı büyüklüğü "kritik hacim" olarak adlandırılır.
- **Sosyal verinin toplanması, depolanması, işlenmesi ve kullanılması devletler için güvenlik sorunu arz edebilmektedir. Sosyal veri sayesinde bir toplumun 'toplumsal gen haritası' ya da reaksiyon formülü çıkarılabilir; bu formül toplumsal karmaşa/kargaşa, suç, terör, seçimler ya da siyasi manipülasyon gibi amaçlarla kullanılabilir**.
- Kişisel veriler kanunla koruma altına alınmışken haberleşme ve eğlenceye dayalı ticari faaliyet adı altında toplanan 'sosyal veri' korunamamakta ve ülke dışı sunucularda depolanmaktadır.

Sosyal Medya ve Dijital Toplumun Güvenliğine Yönelik Bir Tartışma

Mikail Batu, Ph.D.

Doç. Dr.,
İletişim Fakültesi, Halkla İlişkiler ve Tanıtım Bölümü
Ege Üniversitesi

Giriş

20.yüzyılda, yeni iletişim teknolojilerinin hızlı gelişmesi ile beraber sosyal ve gündelik hayat, iletişim türleri ve şekilleri bakımından farklı yönlerden doğrudan etkilenmiştir. Özellikle sosyal ağların Web 2.0 ile etkileşim temelinde hizmet sunması; farklı eğitime, kültüre, ekonomik yapıya, yaşa, yaşam koşullarına sahip olan ve teknik bilgisi olmayan kişileri kolaylıkla kullanıcı haline getirmiştir. "Yeni medya" kavramını yalnızca web 2.0 ile özdeşleştirmek doğru olmayacaktır. Çünkü her teknoloji getirdiği ve sahip olduğu yeni olanaklar ile "yeni medya" sayılabilir. Örneğin Telefon (1876), Radyo (1898) ve Televizyon (1923) icat edildiklerinde, dönemlerinin yeni medyası olarak görülmüşlerdir (Bat, 2012). Ancak günümüzde yeni medya daha çok akıllı uygulamalara sahip yeni iletişim teknolojileri ile etkileşimi sağlayan ve kullanımda karşılaşılan zorlukları en aza indiren sayısal uygulamalar için kullanılmaktadır.

Günümüzdeki anlamıyla yeni medya uygulamalarının temeli bilgisayarın icadına dayanmaktadır. Z1 adında ilk programlanabilir bilgisayar 1936-1938 yılları arasında Konrad Zuse tarafından, ilk dijital bilgisayar ENIAC Presper Eckert ve John Mauchly tarafından 1946 yılında (bazı kaynaklara göre ise ilk dijital bilgisayar Atanasoff-Berry Computer (ABC) John Vincent Atanasoff tarafından 1942 yılında bulunmuştur), ilk elektrikli programlanabilir bilgisayar Colossus ise 1943 yılında Tommy Flowers tarafından, İngilizlerin şifrelenmiş Alman mesajlarını çözmek amacıyla bulunmuştur. Ancak bilgisayarın en ilkel ve analog hali düşünüldüğünde, onun icadını 1600'lü yıllara kadar götürmek mümkündür (Dalan, 2018).

Bilgisayarın gelişimi ile beraber insanları sanal bir ağla birbirine bağlayan internetten bahsetmek kaçınılmazdır. Askeri amaçla ABD tarafından ARPA'nın (Advanced Research Projects Agency / İleri Araştırmalar Projeleri Ajansı) kurulması ve araştırmacıların birbirilerinin çalışmalarını görmelerinin istenmesi ve 1969 yılında sistemin bir ağla karşılıklı bağlanmasıyla ARPAnet adı verilen sanal ağların temeli atılmıştır. 1991 yılında (www/world wide web'in herkesin kullanımına açılması ile) kamusal hale gelen bu sanal ağ sistemi, günümüzde yeni medya denildiğinde düşünülen sosyal medyanın ilk adımları olmuştur. 1993 yılında TÜBİTAK & ODTÜ işbirliği ile Devlet Planlama Teşkilatı projesi çerçevesinde, Türkiye de internete bağlanmıştır. 2000'li yıllardan sonra Web 2.0 teknolojilerinin yarattığı olanaklar doğrultusunda, sosyal ağlar, ülkeleri adeta sınırları ortadan kaldırır gibi birbirine bağlamıştır (ODTÜ, 2020).

Sınırların sanal dünyada ortadan kalktığı süreçte, modern dünyanın tüketim olgusu içine, dijital dünyanın olanakları adapte edilmeye çalışılmıştır. Öyle ki, daktiloyu kullanmakta zorlanan insanlar bilgisayar başına geçmiş ya da yemeğini yiyemeyen çocuklar bilgisayarın karşısına oturtulmuştur. Türkiye gibi birçok ülkede konunun sosyal ve iletişim boyutunun ilk başlarda pek üzerinde durulmamıştır. Çünkü yeni medyanın sunduğu imkânlar iş ve sosyal hayatı kolaylaştırmış ve bu "kolay hayatın" cazibesine kapılmak kaçınılmaz hale gelmiştir. Saatlerce otobüs yolculuğu yaparken, son yılların filmlerini ekranda görmeyi ya da sosyal ağlardaki oyunlara takılmayı kim istemez ki!? Bir başka şehir ya da ülkede işe alınıp alınmayacağı bilinmeyeceğinden, dijital bir ağ üzerinden iş görüşmesi varken, saatlerce yolculuk /vize/ pasaportla kim uğraşır!? Çocuk büyütürken işten yorgun argın gelen ebeveynler için evde sessiz geçirilecek birkaç saat neden çekici olmasın!? Bunlar ve bunlara ek olarak sayılabilecek birçok nedenle yeni medya tabanlı sosyal medya yeni bir dünya yaratmıştır. Sosyolojik, psikolojik, kültürel ve iletişim temelinde değerlendirilmesi gereken çok yeni bir dünya. Bu yeni dünyanın, olanaklarını sunarken kendisini de kabul ettirmesi gerekmektedir. Öyle ki, çekici unsurlara sahip olması ve adeta bağımlılık derecesinde kendisini hayati bir unsura dönüştürmesi önemli bir ölçüttür. Genel hayatını değiştirmek isteme, kişisel ve toplumsal sorunlardan sıkılma veya bunlardan kaçmaya çalışma gibi birçok farklı nedenle sosyal ağlar bir kaçış veya eğlence ortamı olarak görülebilmektedir. Örneğin "İnternet Bağımlısı Erişkinlerde Sosyal Medya Oyunları Üzerine Vaka İncelemesi Candy Crush Oyunu" isimli çalışmada, internet bağımlısı yetişkinlerin Candy Crush oyununu tercih etme ve bu oyunun bağımlılık yaratma nedenleri bilimsel çerçevede araştırılmıştır (Bat ve Kayacan, 2016). Candy Crush oyununun dünyada 10 milyonun üzerinde

kişi tarafından oynanması, bu oyun üzerine araştırma yapılmasının ana nedenini oluşturmuştur. Çalışmanın sonunda Candy Crush oyununun bağımlılık derecesinde neden oynandığına yönelik derinlemesine görüşme ile saptanan nedenler aşağıda sıralanmaktadır (Bat ve Kayacan, 2016):

- Efekt ve seslerin beğenilmesi,
- Efekt ve seslerin oyun için motivasyon arttırması,
- Şekillerin şeker olmasının pozitif algı yaratması,
- Görsellerinin canlı ve güzel olması,
- Kişisel Facebook hesabından oynanmasının mümkün olması,
- Oyunu tek el ile bile oynamanın mümkün olması,
- Oyunun iş yeri, trafik, okul gibi farklı yerlerde oynanabilmesi,
- Oyunun oynanma şeklinin kolay olması,
- Oyuncuların etraflarında da oynayıcıların bulunması.

Yukarıdaki nedenlere bakıldığında, sosyal medya oyunlarını çekici kılan üç faktör üzerinde durulabilir. Birinci faktör "oyuna ilişkin çekici unsurlar". Bu konu ayrı bir çalışmanın ana teması olabilecek öneme sahiptir. Sosyal medya oyunları, kullanıcıların oyuna devam etmesi ve oyun motivasyonunu yüksek tutması için oyunlarını pazara sürmeden ön araştırmalar yapar ve oyunların kişisel etkilerini araştırırlar. Bu etkiler doğrultusunda eklenmesi ve çıkarılması gereken unsurlar üzerinde dururlar. Ayrıca bu araştırmalar oyunun piyasaya çıkmasından sonra da devam eder ve oyun üzerinde yeni değişiklikler için sürekli bir araştırma geliştirme çalışması (AR-GE) gerekir. İkinci faktör "oyuna ilişkin kolaylıklar". Medya üreticileri, pazara sürülen oyunlar için hedef kitleyi mümkün olduğunca büyük tutmaya çalışırlar. Böylelikle ürüne talep artacak ve daha fazla kar elde edeceklerdir. Üçüncü faktör ise konunun sosyolojik boyutu olan "çevreden etkilenme". Bilindiği gibi insan toplum içerisinde kendisini var eden bir canlıdır. Bu doğrultuda çevreden etkilenmemek mümkün değildir. Hele ki çevredekiler bir nesneyi öneriyor ya da o nesneye bağımlılık derecesinde sahip çıkıyorsa!

Sosyal medyanın özellikle çocuklara yönelik etkileri üzerinde durulması gereken bir diğer husustur. Yapılan birçok araştırma karakter ve alışkanlıklarımızın çocukluğumuzda şekillendiğini göstermektedir. Sosyal medya içerik üreticileri de hem gelecekte müşteri kazanmak hem de daha savunmasız olması nedeniyle çocukları hedef kitle olarak seçebilmektedir. Türkiye'de çocuk web sitelerindeki reklamlara yönelik "Dijital İletişim ve Çocuk: Türkiye'de Çocuk Web Sitelerindeki Reklamlara Yönelik Bir İçerik Analizi" isimli çalışmada (İplikçi ve Batu, 2018) sosyal medya ortamlarında 4-16 yaş grubunun reklamlara nasıl maruz kaldıkları ve risklerin neler olduğu araştırılmıştır. 27 ağ sayfasını 15 gün arayla dört kez ve her sayfa en az 10 kez yeniden gözden geçirilerek incelenmiştir. Ağ sayfalarının uygun olup olmadığının ölçüsünü ise Türkiye Reklam ve Haksız Ticari Uygulamalar Yönetmeliği'nin dördüncü bölümünde yer alan Reklamlarda Çocuklara İlişkin Düzenlemeler'e yönelik maddeler oluşturmuştur. Çalışma sonunda ulaşılan noktalar oldukça dikkat çekicidir:

- Çocukların özel bilgilerini elde etme,
- Üyelik yapılmasına ilişkin ödeme isteme,
- Özel mesaj bölümüne yönlendirme,
- Zararlı yiyecek ve içecekleri özendirme,
- Şiddet ve cinsel içerikli görüntülere sahip kişinin davranışlarını etkileyebilecek fotoğraf ve videoların olduğu görülmüştür.

Günümüzde yaşanan COVID-19 salgını sürecinde ise sosyal medya ağları kişisel ve toplumsal hayatta çok daha fazla yer bulabilmiştir. Her yaş grubunu, her mesleği diğer yandan her kurum ve sektörü doğrudan veya dolaylı yoldan etkileyen salgın, genel ve alışkın olunan hayat akışının dışına çıkılmasını zorunlu hale getirmiştir. Gerek tercihen, gerek yasal zorunluluk olarak dışarı çıkmama, eğitim, iş, yolculuk, sağlık, ekonomi vb. konularda belli zorunluluklar doğurmuştur. Dolayısıyla daha önceden birçok insanın hayatında olmayan bazı durumlar, adeta birer gereklilik haline gelebilmiştir. Adeta toplumsal anlamda alışık olunan düzen, yeni hayatın ihtiyaçlarına yanıt veremeyecek ve Weber'in bahsettiği toplumsal anominin (Taş, 2020) öncülü olabilecek bir süreç başlamıştır. Bu süreçte, hem günümüzde hem de gelecekte sorunların ve krizlerin oluşmaması için dikkatli ve bilinçli sosyal medya kullanımı gerekmektedir. Çünkü farklı ağlara girilen kişisel ve özel bilgilerin medya merkezlerinin arşivlerinde bulunması, ileriki dönemlerde güvenli olmayabilecek sorunlara yol açabilecektir. Bu durumun insan hayatındaki önemi nedeniyle güvenlik konusu her geçen gün daha çok önem kazanmaktadır. Güvenlik alanında üç farklı çalışma alanından bahsetmek mümkündür (Bilgisayar Kavramları, 2016):

Ağ güvenliği: Network cihazlarının kurulması bakımının yapılması ve network üzerinde belli bir politika dâhilinde yönetilmesini ifade etmektedir. Bunun için networking sistem yönetimi bilinmesi gerekmektedir.

Yazılım güvenliği: Sunucu ile ilgili uygulamaların ve kodlamanın bilinmesi gerekmektedir. Dolayısıyla uzmanlığa ihtiyaç vardır.

Siber güvenlik: Ülkemizde çok genel düşünülen bir konudur. Sosyal mühendislik, büyük veri, veri madenciliği, insanların eğitimi, bilinçlendirilmesini kapsamaktadır. Dünyada genelde devlet kurumlarının çalıştığı bir konu olarak düşünülebilir. Bu başlık sosyoloji, psikoloji, iletişim, finans gibi farklı alanları ilgilendirmektedir. Ayrıca uzmanlaşmanın gerektiği bir konudur. Siber güvenlik Türkiye'de ağ güvenliği olarak bilinmektedir.

Güvenlik konusu bazılarına göre abartılan bir kavram. Ancak bizler uyuduğumuzda bizim dışımızdaki hayatın devam etmesi gibi bilgisayarın fişini çektiğimizde veya sanal ortamdan çıktığımızda da sanal dünyadaki hayat devam etmektedir. Hem de teknolojinin baş döndüren hızı ile birlikte. Aşağıdaki örnekler sanal güvenlik konusunda farklı perspektiften bakıldığında uyarı özelliği taşımaktadır.

- 1979 yılında ilk katil robot, Amerika Ford fabrikasının deposunda 25 yaşındaki bir kişiyi öldürmüştür. Günümüzde robotlar üretim aşamasında yer alıyorlar, mayın temizliyorlar hatta Mars'ta yürüyorlar (Milliyet, 2010).
- 2011 yılında Güney Kore'de gardiyan robotlar denenmeye başlandı (Amerika'nın Sesi, 2012).
- Amazon prime air drone, ilk müşteri siparişini 2016 yılında teslim etti ve 2020 yılında da üretim için gerekli izinleri aldı (Eyidilli, 2016).
- 2017 yılında Facebook'un iki yapay zeka robotu, kendi aralarında belli nesnelerin ticaretini yapmaya programlandıklarında yeni bir dil kullandıkları saptandı ve fişleri çekildi (Öğütçü, 2017).

Bu sanal gerçekler gazete haberi gibi görünse de, günümüzde hayatın tam içinde yer almaktadır. Örneğin günümüzde buzdolapları, eksik olan şeyleri belirleyip bakkaldan sipariş verebilecek konuma ya da iş başvurularında tüm sağlık sorunlarımız sistem üzerinden görülebilecek duruma gelmiştir. Peki teknolojinin geldiği bu noktada bizler yeterli düzeyde nesnel davranabiliyor muyuz? Bu konuyu Halo Etkisi ile Amerikalı psikolog Edward Thrydike birinci dünya savaşında yaptığı deneyle açıklamak mümkün. Thrydike her komutana askerlerinin fiziksel yetenekleri, zekâları ve emirleri yerine getirme becerilerini sormuştur. Elde edilen sonuçlara göre üstün asker sıfatının sağlam yapılı ve yakışıklı olanlara yönelik kullanıldığı görülmüştür. Thrydike, buradan yola çıkarak dış görünüş pozitif algılandığında, gerçekte olmayan özelliklerin de bu pozitif algıya eklenebileceğini saptamıştır. Bu durumu, sadece insanlar için düşünmekten ziyade genel bakış açımızı da yansıtabilir. Sosyal medyada gördüğümüz insan veya nesne fotoğrafları veya videoları, algımızın nasıl şekillenebileceğine yönelik bazı özelliklere sahip olabilir. Dolayısıyla sosyal ağlarda kullanılan algı yönetmeye ilişkin propaganda tekniklerini bilmek ve bilinçli karar almak gerekmektedir. Algımızı etkileyebilecek bazı propaganda teknikleri aşağıda yer almaktadır (Bulut, 2017):

- Ad takma: Birinin özelliği olabilecek pozitif veya negatif bir sıfatla anılmasını ifade etmektedir. Şeytan Rıdvan, Kızıl Ordu, Baba, Karaoğlan, vb.
- Belirli tipler yaratma: Belirli grupları daha kolay ötekileştirebilmek veya belli çerçeveler kapsamında değerlendirmek / eleştirmek için kullanılmaktadır. Sendikacı, komünist, kapitalist, vb.
- Seçme / Sansür uygulama: Bir konunun/görselin manipüle edici şekilde paylaşılmasını ifade etmektedir. Örneğin fotoğrafın belli bir kısmının paylaşılması.
- Yalana başvurmak: Doğruları göz ardı ederek geçmiş veya yaratılmış algı ve tecrübelerle insanları yanlış şekilde yönlendirmeyi ifade etmektedir! Bilindiği gibi Irak'ta kimyasal kitle imha silahlarının olduğu yalanı, bölgesel bir savaşı başlatmıştı.
- Tekrarlama yoluyla inandırmak: Özellikle reklamcılık alanı gibi görsel alanlarda tekrarın kişilerin ikna edilmesinde etkili olduğu birçok alan araştırmacısı tarafından ispatlanmıştır (Bir kişiye kırk gün deli dersen deli olur atasözünü hatırlamak gerek).
- Ortak düşmana karşı birlikteliği kamçılamak: Günümüzde bunu uluslararası arenada bazı ülkeler bir araya gelerek ortak düşman üzerinden hareket edebilmektedir. Örneğin İran ve Rusya'nın ortak Amerika düşmanlığı noktasında güç birliği yapması.
- Sloganlar yaymak: Sözler akılda kalmayabilir ama etkili sloganlar çeşitli tekrarlarla hayatımızın merkezinde bile bulunabilirler. Örneğin, "alışverişin uğurlu adresi N11".
- İddia etmek: Gelecekte bir konunun olma ihtimallerini gündeme getirerek bazı iddialarda bulunmayı ifade etmektedir. Örneğin sosyal ağlarda günün sonuna kadar sürecek yüzde 50'leri geçen kampanyalar.
- Otoriteye sığınma / transfer aktarma: İddia edilen bir konuda uzman kişileri referans göstererek inandırıcılığı ve ikna etmeyi ifade eder. Birçok kampanyada bu nedenle fikir lideri olan kişiler kullanılmaktadır.
- Tanıklık: İkna etmek için inandırıcılığı yüksek olacak kişilerin sözlerinden alıntı yapmayı ifade etmektedir. Kullanılan sözlerin sonuna alıntı

yapılan kişilerin adları verilir. Ancak sosyal medyada aynı cümlenin sonuna farklı kişiler tarafından farklı isimlerin keyfi eklendiği daha önce birçok kez saptanmıştır.

- Kağıt derme: Bir konuda ikna etmek için belli amaçlar dâhilinde konunun istenilen yönlerinin seçilmesi ve izleyici / takipçilerin karşısına çıkarılması. Örneğin depremden sonra evlerin zarar gördüğünü ve insanların kötü durumda olduğunu göstermek için bir mahalleden zarar görmüş evleri sosyal ağlarda ardı ardına göstermek ve zarar görmemiş evleri hiçbir şekilde yansıtmamak.
- Herkes yapıyor psikolojisi, sürüleştirme çabası: Herkes yapıyor, sen de onların içinde ol mesajı ile insanları güdüleyerek belli konularda ikna etmeyi ifade etmektedir. Çoğunlukla birlikte hareket emek insanları rahatlatabilir.

Yukarıda bahsedilen ve ayrıca farklı ağların özelliklerine göre de eklenebilecek teknikler, günümüzde sosyal mühendisler tarafından profesyonelce kullanılmakta ve sosyal ağ kullanıcıları için krizler meydana gelebilmektedir.

"Sosyal mühendislik; etkileme, zorlama, aldatıcı ilişkiler geliştirme, sorumluluğu, etik değerleri, dürüstlüğü ya da bağlılığı azaltma amacını güden yöntemler kullanarak kişileri gizli bilgi vermeleri veya erişim sağlamaları için aldatma sürecidir. Ayrıca sosyal mühendislik; organizasyon güvenliğinin insanlarla etkileşime girilerek kırılmasıdır şeklinde tanımlandığı gibi, insanların ortak duygularındaki boşluklardan avantajlar elde etmek şeklinde de tanımlanmaktadır" (Bağcı, 2009).

Gerek sosyal mühendislik ve gerek diğer sosyal medya saldırı türlerine karşı dikkatli olmak gerekmektedir. Paylaşılan her bir içeriğin "birileri tarafından görüldüğünü", "kaydedildiğini" ve "birilerinin planına alet olabileceğini" unutmamak gerekmektedir. Bu kapsamda Türkiye'de de yasal düzenlemeler yapılmıştır. Bunların bazıları aşağıda yer almaktadır (Mevzuat, 2020):

- Banka kartları ve kredi kartları kanunu (2006)
- Kişisel verilerin korunması kanunu (2016)
- Tüketicilerin korunması hakkında kanun (2013)
- Mesafeli sözleşmeler yönetmeliği (2014)
- 6563 Sayılı elektronik ticaretin düzenlenmesi hakkında kanun (2014)

Sonuç olarak sosyal medya ortamlarının etkileşim özelliği sebebiyle, kişilerin tecrübesizliğinden yararlanılarak kötü niyetle kullanıldıkları söylenebilir. Bu noktada "bilinçli kullanıcı / hesap sahibi" esas konudur. Bilinçli kullanıcı olmak için birçok önemli noktadan bahsedilebilir. Eğer sosyal medya ortamlarını iş amaçlı kullanmıyorsak kendimize günlük saat sınırlaması koymak, özelden gelen tanımadığımız kişilere ait mesajları uygunsuz olarak bildirip yanıtlamamak, farklı ağlar için isim, doğum tarihi gibi basit olan şifreler kullanmamak, güncelliği olmayan antivirüs programlarını kullanmamak, her linke tıklamamak, beğenileri abartmamak, her gruba üye olmamak, özel ve mahrem hayatımızı ifade eden yemek masası, ev içi ortamlarını paylaşmamak, kaynağından emin olmadığımız bilgileri yaymamaya çalışmak, savaş görüntülerinden uzak durmak, din, dil, ırk, cinsiyet gibi hassasiyete sahip unsurlar hakkında açıklama yaparken dikkatli olmak, bağımlılık seviyesinde sosyal medyanın cazibesine kapılmamak için gerekirse terapi almak bunlardan bazıları. Sosyal medya hepimizin hayatında kaçınılmaz öneme sahip ve hayatımızdan çıkarmamız neredeyse mümkün olmayan bir ortam olarak tanımlanabilir. Bu önemli ortama yönelik sosyal medya okuryazarlığı eğitimlerine katılmak veya bu konuda ilkokuldan itibaren eğitim verilmesi gerektiğini ilgili birimlere duyurmak gerekmektedir.

Kaynaklar

Amerika'nın Sesi, (2012) Robot Gardiyanlar Güney Kore'de Deneniyor https://www.amerikaninsesi.com/a/robot-gardiyanlar-guney-korede-devriye-testinde--148327155/1206640.html Erişim Tarihi: 18.01.2020.

Bağcı, H. (2009). Sosyal Mühendislik ve Denetim, Denetişim, (1). 42-51.

Bat, M. & Kayacan Ş. (2016). "İnternet Bağımlısı Erişkinlerde Sosyal Medya Oyunları Üzerine Vaka İncelemesi: Candy Crush Oyunu" Karadeniz Teknik Üniversitesi İletişim Fakültesi Elektronik Dergisi, 3(12). 20-45.

Bat, M. (2012). Dijital Platformda Sosyal Medyanın Stratejik Kurumsal İletişime Etkisi, Ege Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Doktora Tezi.

Bilgisayar Kavramları (2016). https://www.youtube.com/watch?v=nzVzvqBq1sQ Erişim Tarihi: 20.01.2020.

Bulut, Y.H. (2017). Büyük Dizayn Algı Savaşları, İstanbul: Yeniyüzyıl Yayınları.

Dalan M.C. (2018). İlk Bilgisayarı Kim Yaptıhttps://medium.com/5bayt/i%CC%87lk-bi%CC%87lgi%CC%87sayari-ki%CC%87m-yapti-a38dc077c4eaErişimTarihi: 22.01.2020.

Eyidilli, S. (2016) Amazon Prime Air Drone ile İlk Müşteri Teslimatını Gerçekleştirdi https://webrazzi.com/2016/12/15/amazon-

prime-air-drone-ile-ilk-musteri-teslimatini-gerceklestirdi/ Erişim Tarihi: 16.01.2020.
İplikçi H. & Batu, M. (2018). "Dijital İletişim ve Çocuk: Türkiye'de Çocuk Web Sitelerindeki Reklamlara Yönelik Bir İçerik Analizi". Akdeniz İletişim Dergisi, (29 Özel Sayı). 238-252.
Mevzuat https://www.eticaret.gov.tr/mevzuat Erişim Tarihi: 22.01.2020.
Milliyet Gazetesi (2010) Dünyanın İlk Robotu https://www.milliyet.com.tr/teknoloji/dunyanin-ilk-katil-robotu-1193368 Erişim Tarihi: 20.01.2020.
ODTU Bilgi İşlem Daire Başkanlığı https://bidb.metu.edu.tr/tarihce Erişim Tarihi: 22.01.2020.
Öğütçü H. (2017). İki Facebook Robotu Kendi Aralarında Bilinmeyen Bir Dil Geliştirince Fişleri Çekildi https://egirisim.com/2017/08/09/iki-facebook-robotu-kendi-aralarinda-bilinmeyen-bir-dil-gelistirince-fisleri-cekildi/Erişim Tarihi: 18.01.2020.
Taş, S. (2020). "Emile Durkheim'ın Sosyolojik Anlayışında Toplumsal İşbölümü, Sosyolojik Yöntemin Kuralları, Din, Anomive İntihar", Motif Akademi Halkbilimi Dergisi, 13(29). 442-449.

Siber Güvenlik Bağlamında Sosyal Medya Platformları Ekonomisi ve Endüstriyel Organizasyonu

İbrahim Demir, Ph. D.
Doç. Dr.,
Ulisa & İktisat Bölümü
Ankara Yıldırım Beyazıt Üniversitesi

&

Fatih Cemil Özbuğday, Ph. D.
Doç. Dr.,
İktisat Bölümü
Ankara Yıldırım Beyazıt Üniversitesi

Giriş

Dijital ve mobil teknolojilerdeki hızlı gelişmeler, özellikle son yirmi yıllık zaman diliminde sosyal medya sektörünün gelişmesi ve genişlemesiyle sonuçlanmıştır. Sosyal medya platformlarının kurulup pazar gücü elde etmesi ya da piyasadan silinmeleri, anlaşılması gereken birtakım ekonomik ve endüstriyel organizasyon dinamikleri barındırmaktadır. Bu dinamiklerin anlaşılması, bu platformlara talebi, bu platformların faaliyet gösterdikleri endüstriyi ve siber güvenlik endişelerini anlamakta faydalı olacaktır. Bu çabayla politika yapıcılar ve genel toplum bu platformları daha iyi anlamlandırıp fayda/kar maksimizasyonu ya da güvenlik endişeleri için kendilerini daha iyi konumlandırabileceklerdir.

Sosyal medya platformlarının enstrümanı dijital veri formundaki bilgidir. Bilgi her zaman olduğu gibi günümüzün de en önemli güç kaynağıdır. Bu sektördeki pazar yoğunlaşması ve faaliyet gösteren işletmelerin özellikle birkaç ülkede kümelenmesi, ticari faaliyetin ötesinde son derece hassas ve değerli bilgi ve veriyi dünya genelinden çok düşük bir maliyetle toplama operasyonuna dikkatleri çekmektedir. Sosyal medya platformları aracılığı ile devletlerin dahi başaramayacağı bir ölçekteki "sosyal veri" birkaç ülkedeki sunuculardaki depolanmaktadır. Bu "büyük verinin" (big data) işlenip yeri geldiğinde ekonomik, siyasi ve uluslararası ilişkiler çıkarları için kullanılabileceğine ilişkin ciddi endişeler bulunmaktadır. Bir topluma ait sosyal verinin yabancı ülke sunucularında sürekli bir şekilde depolanması çok ciddi bir güvenlik sorunudur. Bu endişeler nedeniyle kişisel verinin korunması için önemli hukuki düzenlemeler yapılmış olmasına rağmen, sosyal verinin korunması ihmal edilen ve gözden kaçan bir alan olmuştur. Asıl tehlikeli olan sosyal verinin yabancı sunucularda depolanıp işlenmesi ve kullanıma hazır halde tutulmasıdır. Bu güvenlik sorununun anlaşılması için önemli adımlardan biri de meselenin iktisadi analizidir.

Bu çalışmada ele alındığı üzere, sosyal medya endüstrisinin bugünkü yapısının oluşturduğu güvenlik sorununu iktisadi açıdan ele almak, ekonomik, hukuki ve idari çözümlerin ya da doğrudan kamu müdahalesi formlarının etkililik sınırlarını anlamaya yarayacaktır. Uluslararası ticaret kuralları ve uluslararası hukuk gereği küresel düzeyde ticari faaliyet yürüten bu girişim ve firmaları engellemek, sunulan hizmetin ikamesi bulunmayan ekonomik bir değerinin bulunması ve toplumun bu değer karşılığında ödeme istekliliği göstermesi nedeniyle çok zordur ya da arzu edilir değildir. İdari ya da hukuki engellemelerin kaçakçılığı özendirdiği ya da daha etkinsiz kaynak ayrımına yol açabileceği bilinmektedir. Bu yüzden pansuman ve hatalı sonuçlar doğurabilecek tedbirler yerine, sosyal medya platformları ihtiyacını iyi anlamak, bu ihtiyacın doğurduğu ödeme istekliliğini ve sosyal medya sektörünün endüstriyel organizasyonunu iyi analiz etmek gerekmektedir. Bu analizlerden öğrendiğimiz şey bireysel talebin, günün ihtiyaçlarına ve teknolojisine göre etkin ve güvenli yöntemlerle karşılanması gerektiğidir. Sosyal medya hizmetlerine duyulan temel ihtiyaç ve talebi, dijital verinin kontrol zorluğunu ve sosyal medya sektörünün endüstriyel organizasyonunu göz ardı eden idari/hukuki tedbirler tek başına yeterli olmayacaktır ve istenmeyen sonuçlara yol açacaktır. Diğer taraftan, bilinmelidir ki özellikle şebeke dışsallıkları, hesap geçiş maliyetleri ve kilitlenme etkileri nedeniyle geniş halk kitlelerinin pazar gücüne sahip platformları terk etmesi ekonomik gerekçelerle zordur. İdari/hukuki önlemlerin yetersizliği ve ekonomik gerekçeler politika yapıcıları en iyi çözüm konusunda zorlamaktadır. Yapılması gereken, yerlileştirme, eğitim ve farkındalık oluşturma yanında ekonomik, idari ve hukuki müdahalelerin entegre ve birbirlerini tamamlayıcı bir şekilde geliştirilip uygulanmasıdır.

1. Sosyal Medya Hizmetlerine Talep

Sosyal medya ve şebekeler, günümüzün görsel ve işitsel dijital bilgi iletişim, etkileşim ve paylaşım ortamlarıdır. Özellikle doksanlı ve ikibinli yıllarda dijital ve mobil teknolojilerdeki hız, depolama, miktar ve kalite gelişmeleri, görsel ve işitsel bilgi paylaşım maliyetlerini ciddi oranda düşürmüştür. Aktarılan ve paylaşılan veri aynı zamanda depolandığı için dijital veri depolama

maliyetleri, veri aktarım ve paylaşım maliyetleri için bir fikir verebilir. Yapılan bir çalışmaya göre 1980-2009 yılları arasında bir gigabyte hard disk fiyatı her 14 ayda bir yarıya inerek 1980'lerdeki 100 bin dolar civarından 2009'da 10 dolar-sente düşmüştür (https://mkomo.com/cost-per-gigabyte). Maliyetlerdeki düşüş, arz-talep yasaları gereği görsel ve işitsel bilgi üretim ve kullanımında ciddi bir artış ve bu alanda hızla gelişen bir endüstri doğurmuştur. Bireylerin dijital bilgi aktarımı ve paylaşımına sağladıkları fayda karşılığında atfettikleri değer ve bu değer karşılığında oluşan ödeme istekliliği de aynı şekilde sosyal medya ve şebeke piyasalarının doğmasında ve gelişmesinde etkili olmuştur. Bu piyasadan elde edilen dijital bilgi aktarım ve paylaşımının bireysel faydaları başlıca mesajlaşma, görüntü ve ses paylaşımı, konum bildirme/öğrenme, görünürlük (bilinme, tanınma, ünlenme), eğitim/öğretim (tarım, sağlık, hobi, finans), ticaret (alım, satım), istihdam (iş ve işçi bulma), ilan ve tanıtım (idari, siyasi, dini, endüstriyel reklam), eğlence, sosyalleşme vb. şeklinde sıralanabilir. Bu faydalara atfedilen değer ve bu değerle gelen talep, sosyal medya endüstrisini doğurmuştur.

Sosyal medya platformları ekonomik manada 'etkin'dirler. Sosyal medyada birim bilgi paylaşım maliyeti tek tek bireylerle paylaşım maliyetlerine göre son derece düşüktür. Sosyal medya platformlarındaki iletişim ve dijital veri paylaşımı, piyasalardaki bilgi seviyesini artırmakta ve daha iyi kararlar alınmasını sağlayabilmektedir. İletişim işbirliğine, işbirliği de verimlilik ve fayda artışına yol açma potansiyeline sahiptir. Bu bağlamda sosyal medya platformlarında tarım, inşaat, sağlık, imalat, hizmetler, hobicilik ve rekreasyon gibi bir çok alanda paylaşılan eğitsel ve doğruluğu kanıtlanmış bilgi ya da şebekeleşme, genel sağlık ve refah seviyesini hiç görülmedik şekilde artırma potansiyeline sahiptir. Ancak, etkinlik (birim paylaşım maliyeti) abone sayısı tarafından belirlendiği için sosyal medya platformları aşırı büyüme ve tekelleşme eğilimindedir.

Bu bağlamda sosyal medya endüstrisinin gelişimi ve günümüzde geldiği nokta, iktisat bilimine konu birtakım soruları da beraberinde getirmiştir. Bireylerin hangi sosyal medya platformunu tercih edeceği, bu tercihi belirleyen faktörlerin neler olacağı, bu platformlarda ne kadar zaman harcayacağı, kimlerle etkileşim içinde olacağı, kimleri engelleyeceği, hangi gruplara katılacağı, hangi gruplardan çıkacağı, veri güvenliğinin sağlanıp sağlanamayacağı gibi sorular talep yönüne ilişkin sorulardan sadece bazılarıdır. Bu sorulara verilebilecek ekonomik cevaplar birey tercihlerinin fayda ve maliyetler tarafından motive edildiği varsayımına dayanan rasyonel davranış hipotezi temellidir. Arz yönünde ise sosyal medya endüstrisi ile alakalı endüstriyel organizasyon soruları da bu piyasaların sınırlarının ne olduğu, firma büyüklüklerinin ne kadar olacağı, rekabet (pazar gücü, giriş ve çıkışlar ve yoğunlaşma vb.) yapısının ne olacağı gibi sorular önemli sorulardandır. Sosyal medya piyasasının hem arz hem de talep yönündeki bu sorulara cevap verilmeden bu endüstrilere ilişkin politikaların etkililiği ve veri güvenliği meselesinin anlaşılması imkânsızdır.

2. Bireysel Veriden Sosyal Veriye Değer Asimetrisi

Bireyin kendisine ait bilginin hem kişisel hem de toplumsal faydasına (ve değerine) ilişkin algı sorunludur. Bireyler kendilerine ilişkin veriyi aşağı-yanlı bir şekilde değerlemekte yani olduğundan daha değersizmiş gibi algılamaktadır. Bu yüzden bireyler kendilerine ait veriden çok düşük bir bedel karşılığında vazgeçebilmektedirler. Ancak tek başına bir birey için çok fazla anlam ifade etmeyen bilgi, diğer bireylerin bilgisi ile çok düşük bir maliyetle birleştirilebilmekte, istatistiki güç kazanabilmekte ve 'sosyal risk' hesaplamalarında kullanılır hale gelmektedir. Sigorta mekanizmasındaki bilgi ve risk havuzuna benzer bu oluşum, veri toplama, depolama, birleştirme ve analiz maliyetlerinin düşük oluşunun bir sonucudur. Bu manada sosyal veriyi mümkün kılan şey ölçek ekonomileridir. Kişinin kendisi için değeri olduğundan düşük algılanan kişisel veri sosyal veriye dönüştüğünde değeri katlanarak artmaktadır. Bireysel veri ve sosyal veri arasındaki bu değer asimetrisi bireylerin kişisel verilerinden kolay bir şekilde vazgeçmelerine neden olmaktadır. Tek tek bireylerin hem kişisel hem de sosyal veriye talebi son derece düşük iken, reklam ve pazarlama şirketleri, hükümetler, istihbarat, terör ve suç örgütlerinin bu verilere olan talebi son derece yüksektir.

Sosyal Medya ve Modern Trampa

Kişisel veri ve toplumsal veri arasındaki değer asimetrisi ve sosyal medya hizmetlerinin 'sözde' bedava oluşu, sosyal medya hizmetleri tüketiminin yaygınlaşmasının nedenlerinden biridir. Ancak, bütün ekonomik kaynaklar için söz konusu olduğu üzere sosyal medya platformlarında sunulan hizmetler bedava değildir. Sosyal medya hizmetleri karşılığında 'nakit' formunda ya da parasal bir ödeme olmaması bu hizmetlerin 'bedava' olduğu anlamına gelmez. Nakit ödeme olmasa da bir barter malın malla değiştirilmesi, yani bir trampa (barter) söz konusudur. Bireyler bu piyasalardan aldıkları hizmetin karşılığını tercih ve davranışlarına ilişkin veri yani 'kişisel bilgi' ile 'ayni' olarak ödemektedirler. Sosyal medya platformlarına abone olunduktan itibaren bireyin yaşı, cinsiyeti, lokasyonu, alışkanlıkları, satın aldığı ve merak ettiği ürünler, tercihleri, sağlık durumu, duygu durumu vb. gibi özellikleri satın aldıkları hizmetin

bedelinin ayni karşılığı haline gelmektedir. Burada kimin kime ödeme yapması gerektiği sorunu söz konusudur. Cheung (1973) benzer bir sorunu arı petekleri sahipleri ile elma bahçesi sahipleri arasındaki problem etrafında ele almıştır. Yazları arı sahipleri arıların elma çiçeklerinden bal toplaması karşılığı elma bahçelerine ödeme yaparken kışları da elma bahçesi sahipleri polenleme karşılığı arı sahiplerine ödeme yapmaktadır.[1]

Sosyal medya platformları esasen "ilgi aracısıdır". Kullanıcılarının ilgisini toplayarak bunu reklam verenlere satarlar ve "ilgi" için rekabet ederler (Prat ve Valletti, 2018). Sosyal medya platformları çok-taraflı piyasalardır ve şebeke etkileri/dışsallıkları tarafından karakterize edilirler.

Çok taraflı ya da çift taraflı piyasalarda fiyat yapısı asimetriktir (Rochet ve Tirole, 2003). Bu pazarlarda faaliyet gösteren teşebbüsler, pazarın fiyata duyarlı tarafında maliyet altı hatta sıfır fiyatlama yaparak şebekelerini genişletmek isterler. Öte yandan bu teşebbüsler, sıfır veya düşük fiyatlama yoluyla katlandıkları zararları pazarın fiyat duyarlılığı daha düşük olan kesimlerinde daha yüksek bir fiyat koymak suretiyle telafi ederler (Evans ve Schmalensee, 2005). Örneğin, Twitter standart kullanıcılarından herhangi bir bedel talep etmez. Bedeli olmayan bir hizmeti almak için çok sayıda kullanıcı Twitter'da aktif olur. Twitter diğer teşebbüslerden reklam geliri elde ederek tüketici tarafında yaptığı sıfır fiyatlamadan ötürü katlandığı zararı telafi eder. Bir başka ifadeyle, çok taraflı bir piyasanın bir tarafında katlanılan zarar, aynı piyasanın başka tarafında yapılan kâr ile çapraz desteklenir. WhatsApp ise kullanıcılarından herhangi bir bedel istemezken elde ettiği veriyi işleyerek pazarlama analitikleri oluşturmakta ve bu verileri aynı ekosistem içinde yer alan gelir getirici ürünlerde kullanılan yapay zekâların eğitiminde kullanır.

3. Sosyal Medya Sektöründe Pazar Gücü

Sosyal medya platformlarının pazar gücü elde etme eğiliminde oldukları bilinmektedir. Bu platformların nasıl pazar gücü elde ettikleri ve bu gücü nasıl sürdürdükleri merak edilen konulardan biridir. Benzer hizmetleri sunan çok sayıda platform olduğu halde bazı sosyal medya platformlarının pazar gücü elde edip sürdürmeleri başlıca şu faktörler tarafından belirlenmektedir:

- **Orijinal fikir, konsept ve mülkiyet hakları**: Tescil edilmiş orijinal fikir ve konsept, sahibine pazar gücü bahşedebilmektedir. Konsept, sosyal medya platformu formatının genel bir ihtiyaçla yerindelik ve zaman bakımından örtüşmesi ya da kendi kavramsal ihtiyacını doğurmasını ifade eder. Twitter, örneğin, zaman maliyeti nedeniyle uzun mesajların okunmaması nedeniyle kısa mesajlaşma konseptine dayalıdır. Tescil edilmiş bu konsept Twitter'a pazar gücü vermektedir ve orijinal konsepte sahip diğer sosyal medya platformları için de aynı durum söz konusudur.

  Orijinal fikirlerin korunması için gelişmiş bir mülkiyet hakları koruma geleneği ve bunu destekleyen bir yargı sistemi bulunmalıdır. Bu yüzden, orijinal fikirler mülkiyet haklarının korunduğu ekonomilere doğru hareket etme eğilimindedir. Zihninde orijinal bir fikir taşıyan bir bireyin bunu fikri mülkiyet haklarının daha iyi korunduğu bir ekonomide tescil ettirmesi daha olasıdır. Fikri mülkiyet hakları ve bu hakların korunması kopyalanmayı engellediği için giriş engeli oluşturmakta ve pazar gücü bahşetmektedir.
- **Sermaye ve fikir fonlaması:** Yeni bir ürüne giden yolda fikir ve sermaye aynı kişi veya ekonomik birimde bir araya gelmeyebilir. Fikirden ticarileşmeye yeni ürünler sermayeye ve reklam harcamalarına ihtiyaç duyarlar. Sermaye ihtiyacını hızlı bir şekilde giderecek yerleşmiş bir sermaye piyasası fikirlerin kısa sürede fonlanmasını sağlamaktadır. Yatırım kararına dayanan bu süreç etkindir ve daha iyi fikirlerin daha yüksek bir sermaye gücüne ulaşmasıyla sonlanır. Sermaye piyasaları gelişmemiş toplumlarda elde daha iyi bir fikir bulunsa bile sermaye birikimini sağlamak mümkün değildir. Bu yüzden yenilikler, yeni ürünler ve ticarileşme sermaye piyasalarının ve fikir fonlaması mekanizmalarının daha gelişmiş olduğu ekonomilerde ortaya çıkma eğilimindedir. Birçok yeni ürünün Amerika Birleşik Devletleri'nden çıkıp yayılmasının sebeplerinden biri budur. Fonlama bulunur bulunmaz ilgili fikir ciddi bir piyasa avantajı kazanmakta ve bunu sürdürmektedir.
- **Arayüz özellikleri:** Pazar gücü bulunan sosyal medya işletmelerinin sahip olduğu arayüzlerin renk, dizayn, logo, hız, platform uyumu gibi özellikleri kodlama ya da yazılım etkinliklerini yansıtabilir. Bu özellikler, geniş nüfus kitlelerinin zevk ve kullanım kolaylıklarına hitap ederek pazar gücü kazanmalarının sebeplerinden biridir.
- **İlk davranan avantajı:** Bir yeniliği ilk olarak piyasaya süren pazar gücü elde edebilir ve sürdürebilir. Schumpeter (1942) bu süreci 'yaratıcı yıkım' kavramı etrafında ele almıştır.
- **Geçiş maliyetleri ve abone kilitlenmesi:** Şebeke etkileri dolayısıyla elde edilen pazar gücünü destekleyen unsurlardan biri de geçiş/transfer

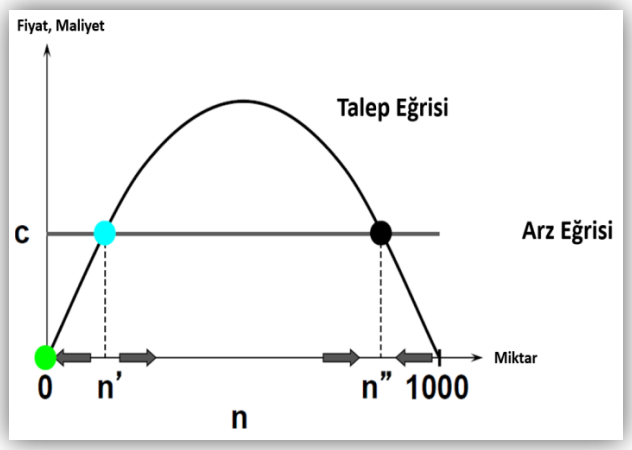
[1] Sosyal medya platformlarının bir kısmı, yayımlanan materyalin izlenme sayısına göre parasal telif öderken birçoğunda ise yerleşik bir ödeme mekanizması mevcut değildir.

maliyetleri ve kilitlenme etkisidir. Gerek doğrudan gerekse dolaylı şebeke etkilerinden ötürü tüketicilerin bir sosyal medya platformundan başka bir platforma geçişi sınırlı olacaktır. Bunun nedeni şebeke dışsallıklarının bir platform üzerinde çok güçlü olmasının bir platformdan başka bir platforma geçişi oldukça "maliyetli" kılmasıdır. Bu duruma tüketici kilitlenmesi adı verilmektedir. Şebeke dışsallıkları ve tüketici kilitlenmesi söz konusu olduğunda, piyasaların çalışması klasik iktisat kuramının anlattığından oldukça farklıdır. Standart iktisat teorisi bize der ki aynı ürünün daha ucuzu piyasaya çıktığında veya aynı fiyata daha kaliteli bir ürün piyasaya sunulduğunda tüketiciler diğer ürüne geçiş yapar. Hâlbuki şebeke dışsallıkları ve tüketici kilitlenmesi söz konusu olduğunda tüketicilerin başka ürünlere veya hizmetlere geçişi bu kadar basit değildir. Örneğin, bir sosyal medya platformunun pazar payının çok yüksek olduğu durumda, bir tüketici grubunun başka bir platforma geçmeye ikna olması için aslında kullanıcıların büyük kısmının toplu halde rakip bir platforma geçmesi gerekmektedir. Ve yine biliyoruz ki sosyal medya platformlarında tüketicinin karşılaştığı fiyat sıfırdır. Bir başka deyişle, tüketicilerin başka bir platforma toplu bir halde göçünü sağlayacak stratejik değişken fiyat değildir. Kullanıcıların bir platformdan başka bir platforma geçişinde bütün mesaj, resim, video, paylaşım, hatıra ve etkileşimlerinin hepsini taşıması son derece maliyetlidir. Diğer taraftan, bu taşıma tek bir kullanıcıyı ilgilendiren bir sorun değildir ve aynı kişisel faydaya ulaşması için kullanıcının ilgilendiği diğer kullanıcıları ikna etmesi ve onların da dijital materyallerini yeni platforma taşıması gerekmektedir. Bu çok zor olduğu için aradaki fayda farkı rekabeti engellemektedir. Böylesi bir toplu geçişin sağlanması ancak radikal bir teknolojik dönüşüm ya da rakip platformun tüketicilere büyük bir fayda sağlayan yıkıcı bir inovasyonu pazara sunması ile mümkündür. Örneğin, 2004-2006 yılları arasında Türkiye'de oldukça popüler olan sosyal networking sitesi Yonja, 2006'dan itibaren yerini Facebook'a bırakmış ve sonrasında Yonja'nın esamesi okunmamıştır. Bunun nedeni, Facebook'un daha önce kullanıcıların hayal edemeyeceği çok daha zengin bir tüketici deneyimi sunmuş olmasıdır.

- **Şebeke Dışsallıkları:** Sosyal medya platformlarının konu olduğu şebeke dışsallığı, bu platformların kullanıcı (abone) sayısı arttıkça bireysel bir tüketiciye sağladığı faydanın da artması anlamına gelmektedir. Doğrudan ve dolaylı olmak üzere iki şebeke etkisinden bahsetmek mümkündür. Örneğin, Twitter'ı daha fazla sayıda kişi indirip kullandıkça bir bireyin Twitter kullanmaktan sağladığı fayda (Twitlerin daha fazla kişi tarafından görülmesi, paylaşılması vb.) artış göstermektedir. Bu doğrudan şebeke etkisidir.

Varian'ın (2014) şebeke dışsallıklarını aşağıdaki grafikle izah etmiştir. Grafikte 1000 bireyli bir pazarda n kişinin, şebeke dışsallıkları ile karakterize edilen ürünü tükettiği bir örnek ele alınmıştır. Bu pazarda toplam talep n=1000−v olup (v, bireyin ürünü değerlemesini göstermektedir) ters talep fonksiyonu p=n(1000−n) olarak yazılabilmektedir. Ürünün satıcılarının hepsinin aynı marjinal üretim maliyetine (c) sahip olduğu varsayımı altında söz konusu ürün için yatay bir arz eğrisi çizilebilir. Bu pazar için, arz eğrisi ile talep eğrisinin kesiştiği üç farklı denge noktası değerlendirilebilir. Birinci durumda hiçbir satıcı ürünü satmaz ve hiçbir alıcı ürünü almaz (yeşil renkle gösterilen denge noktası). İkinci durumda, n' ile gösterilen, az sayıda tüketici ürünü alır (açık mavi renkle gösterilen denge noktası). Üçüncü durumda, n" ile gösterilen, fazla sayıda tüketici ürünü alır (siyah renkle gösterilen denge noktası). Peki, bu üç denge noktasından hangilerinin ortaya çıkması en muhtemeldir? Açık mavi renkle gösterilen denge noktası durağan değildir: zira tüketicilerin ödeme eğilimi (talep eğrisi ile gösterilmektedir), marjinal üretim maliyetini aştığı sürece söz konusu pazarın büyüklüğü değişme eğilimindedir. Böylece, sadece yeşil ve siyah renkle gösterilen iki denge noktaları durağandır. Bunun anlamı, şebeke dışsallıklarının söz konusu olduğu bir ürünün satıldığı pazarda ya hiçbir satış işleminin gerçekleşmeyeceği ya da pazarın büyük çoğunluğunu oluşturan bir tüketici grubunun ürünü satın alacağıdır.

Şekil 1. Şebeke Dışsallıklarıyla Karakterize Edilen Bir Pazarda Arz-Talep Dengesi



Bir başka ifadeyle, şebeke dışsallıklarının söz konusu olduğu bir ürünü ya hiçbir tüketici kullanmayacak ya da pazarı oluşturan tüketicilerin büyük bir kısmı kullanacaktır. Bu iki uç durumun arası pek muhtemel olmayıp, günlük hayatta yapılan gözlemlerimiz de bu kuramsal öngörü ile tutarlıdır. Örneğin sosyal medyada, bir platformu ya tüketicilerin büyük bir kısmı kullanmakta ya da bu platformu neredeyse hiçbir tüketici kullanmamaktadır.

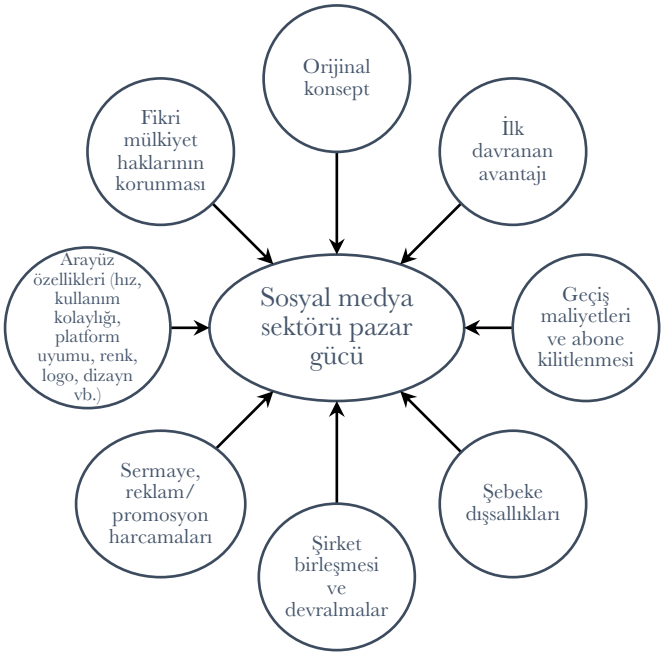
Sosyal medya platformlarının sunduğu hizmetlerinin doğrudan şebeke etkilerinin yanı sıra dolaylı şebeke etkilerinden/dışsallıklarından da söz etmek mümkündür. Buna göre, pazarın bir tarafında daha fazla sayıda kullanıcının olması, pazarın diğer tarafında yaratılan değerin/faydanın artışını sağlamaktadır. Örneğin, daha fazla sayıda kullanıcı Twitter kullandıkça Twitter pazarın diğer tarafındaki firmalardan daha fazla miktarda reklam geliri elde edebilmektedir. Twitter daha fazla reklam geliri elde ettikçe, daha fazla tüketiciyi bünyesine katacak şekilde hizmetlerini genişletmektedir. Bu şekilde Twitter örneğinde çift-taraflı dijital platformlar için doğrudan ve dolaylı şebeke dışsallıklarının yol açtığı kendi kendini güçlendiren geri besleme etkilerinden söz etmek mümkündür.

Sosyal medya platformlarının konu olduğu şebeke etkileri belli bir sayıda kullanıcının aktif olmasından sonra devreye girer. Şebeke etkilerinin görülmeye başlandığı kullanıcı büyüklüğü "kritik hacim" olarak adlandırılır. Böylece, bir sosyal medya platformunda kritik hacme ulaşılmasının ardından kendi kendini güçlendiren geri besleme etkileri devreye girer ve bu geri besleme etkileri, kritik eşiğin geçilmesine ve pazarın "kaymasına" yani tek bir teşebbüsün pazara hâkim olmaya başlamasına yol açar. Bu durum, daha önce ifade ettiğimiz bir sosyal medya platformunu ya tüketicilerin büyük bir kısmının kullandığı ya da bu platformu hiçbir tüketicinin kullanmadığı şeklindeki kuramsal tahminlerden ilkine karşılık gelmektedir.

- **Şirket Birleşmeleri:** Sosyal medya platformlarının ve genel olarak dijital ekonominin yoğunlaşması sadece çok taraflı piyasa olma özelliği, şebeke etkileri ve yaptıkları inovasyon ile alakalı değildir. Kısaca GAFAM olarak adlandırılan dijital ekonomi devleri (Google, Apple, Facebook, Amazon, Microsoft) son 20 yılda toplamda neredeyse 1.000 adet firmayı satın almış (Cabral, 2020) ve bu satın alma ve devralmaların hiçbiri dünyanın büyük ekonomilerindeki rekabet otoriteleri tarafından engellenmemiştir (Valletti, 2021). Satın alınan bu firmalardan bazıları GAFAM'ın doğrudan rakibiyken pek çoğu önemli potansiyeli olan teknoloji teşebbüsleriydi. Şimdi ise zaman içinde devasa büyüklüklere ulaşan GAFAM'ın yol açtığı rekabet problemlerinin nasıl ele alınacağı ve çözüleceği bilinmemektedir. Bu teşebbüsler öylesine bir pazar gücüne sahip olmuşlardır ki bir ülkede beğenmedikleri bir kararla karşılaştıklarında sundukları hizmeti kullandırtmama aşamasına bile geldikleri görülmektedir. Google'ın Avustralya'da elde ettiği gelirlerden haber kuruluşlarına da pay verilmesini şart koşan yasal düzenlemenin yürürlüğe girmesi halinde hizmet vermeyi durduracağını açıklaması bunun bir örneğidir (Hürriyet, 2021). Keza, son günlerde Facebook'un sahibi olduğu WhatsApp'ın kullanım koşullarını tek taraflı olarak değiştirmesi ve bu koşulların kabul edilmemesi durumunda sunduğu hizmetlerden yararlanılamayacağını ifade etmesi, bir başka deyişle, işine gelirse (*take it or leave it*) tarzı bir yaklaşım göstermesi aslında pazardaki güçlü yerleşik konumundan ve WhatsApp'ın bu konumun zayıflamasının çok zor olduğunu bilmesinden kaynaklanmaktadır.

Sosyal medya sektöründe pazar gücüne yol açan ve pazar gücünü sürdürmeye yarayan faktörlerin büyük çoğunluğunu aşağıdaki şekilde göstermek mümkündür:

Şekil 2. Sosyal Medya Sektöründe Pazar Gücü



Bu faktörlerden her biri tek başına güçlü ve sürdürülebilir bir pazar gücü oluşturmak için yeterli değildir. Ancak bu faktörlerden büyük çoğunluğundan ya da tamamından kaynaklanan bir pazar gücü güçlü ve kalıcıdır. Bu faktörlerden kaynaklanan küresel pazar

gücü hükümetlerin dahi baş edebileceği boyutu aşmış durumdadır. Bu faktörlerin kazandırdığı avantajlar yenilik veya rekabet tarafından ortadan kalkmadan bu platformları ekonomik olarak durdurmak mümkün değildir. Bu durumda geriye sadece normatif ve idari çözümler kalmaktadır. GAFAM incelendiğinde bu faktörlerin neredeyse tamamına sahip oldukları görülmektedir. Bu durum GAFAM'ın faaliyet gösterdiği sektörün bu gözle irdelenip değerlendirilmesini gerekli kılmaktadır.

Çoklu Erişim ve Rekabet

Sosyal medya platformları arasındaki rekabeti değerlendirirken dikkate alınması gereken kavramlardan biri de çoklu erişimdir. Çoklu erişim, kullanıcıların aynı anda birden fazla rakip sosyal medya platformunu kullanması olarak ifade edilebilmektedir. Eğer, kullanıcıların rakip sosyal medya platformlarına aynı anda erişimi söz konusuysa, bu durumda pazar kaymasının yol açacağı anti-rekabetçi endişelerin dengelendiği söylenebilmektedir. Zira çoklu erişimin olduğu durumda hem rakip platformlar kullanıcı sayılarını artırabilirken hem de pazara yeni platformlar girebilmektedir. Böylece, çoklu erişimin pazar yoğunlaşmasını azaltıcı bir etkiye sahip olduğu, bunun da şebeke etkilerinin ve tüketici kilitlenmesinin olduğu pazarlarda kritik öneme sahip olduğu öne sürülebilmektedir.

Sosyal medya platformları, günümüzde şebeke dışsallıklarının olduğu çift-taraflı piyasa yapısından başka bir yapıya evirilmeye devam etmektedir. Buna göre, sosyal medya platformlarının pek çoğunun çift-taraflı bir piyasadan N-yüzlü pazarlara dönüştüğü öne sürülebilir (Biancotti ve Ciocca, 2018). Örneğin, sosyal networking ile ticaret hayatına başlayan Facebook bugün yüz tanıma teknolojisi, kredi skoru hesaplama, yeni ödeme yöntemleri gibi pek çok alanda faaliyetlerini sürdürmektedir. Bütün bu faaliyetlerde kullanılan temel girdi kullanıcı verisidir.

Dolayısıyla, bütün bu tartışmaları birlikte değerlendirdiğimizde şebeke dışsallıklarından, bağlantılarımızdan ve alışkanlıklarımızdan ötürü başka bir mesajlaşma uygulamasına geçişimizin oldukça maliyetli ve zor olduğunu, WhatsApp'ın zorunlu tuttuğu yeni kullanım koşullarının aslında bir rekabeti problemini işaret ettiğini; bu koşullara karşı bireysel tüketici olarak oldukça korunmasız olduğumuzu, yeni koşulları biz kabul etmesek bile istatistiksel açıdan bize çok benzeyen birinin kabul etmesi durumunda mahremiyetimizin korunamayacağını, WhatsApp için ise "atı alanın Üsküdar'ı geçtiğini" söylemek mümkündür.

Peki, sosyal medya devlerinin ve genel olarak data-opolilerin (Stucke, 2018) sahip oldukları muazzam pazar güçleri karşısında rekabet otoriteleri ne yapabilir? Burada evveliyatla yapılması gereken GAFAM gibi teşebbüslere artık başka firmaları –ölçek olarak ne kadar küçük ve ihmal edilebilir olursa olsun- devralma olanağının verilmemesidir. Birleşme-devralma kontrolünün tek başına data-opolilerin pazar gücünü dizginleyeceğini öngörmek doğru mudur? Elbette hayır. Birleşme-devralma kontrolüne ilaveten data-opolilerin rakipleri ve piyasaya yeni giren teşebbüsleri dışlayıcı eylemleri de rekabet otoriteleri tarafından hızlı bir şekilde engellenmelidir. Rekabet otoritelerinin yapacaklarının yanı sıra data-opolilerin pazar gücünü dizginlemek için başka kamu kurumlarının yapacağı yasal ve teknik düzenlemelerin de etkin olması esastır.

4. Güvenlik Maliyetleri ve Sosyal Medya

Sosyal verinin toplanması, depolanması, işlenmesi ve kullanılması devletler için güvenlik sorunu arz edebilmektedir. Sosyal veri sayesinde bir toplumun 'toplumsal gen haritası' ya da reaksiyon formülü çıkarılabilir; bu formül toplumsal karmaşa/kargaşa, suç, terör, seçimler ya da siyasi manipülasyon gibi amaçlarla kullanılabilir. Sosyal medyada oluşan bilgi havuzu bir toplumun anlık, saatlik, günlük, haftalık ve aylık duygu, düşünce ve reaksiyon fonksiyonunun elde edilmesine yarayabilir. Bu fonksiyon elde edilip doğrulandığında hedef kitlelerin manipüle edilmesi kolaylaşır. Bütün bunlarla mücadele etmek ve siber güvenliği sağlamak, ciddi kaynak kullanımı gerektiren maliyetli bir iştir.

Sosyal medya platformları, devletlerin hatta bireyin kendisinin dahi fark edemeyeceği bilgilere sahip olabilme kapasitesine sahiptir. Sosyal medyada toplanan verinin analizi sayesinde bir bireyin sağlık, aile ve finans sorunları tahmin edilip siyasi eğilimleri tespit edilebilir. Aynı şekilde bir toplumu 'kırılgan' yapan 'sosyal fay hatları' da sosyal veri ile tespit edilebilir. Geriye kalan zamanı geldiğinde bu bilginin satılmak ya da doğrudan kullanılmak suretiyle 'kâra' ya da 'etkiye' dönüştürülmedir. Örneğin, bir toplumsal kargaşa çıkarılmak istendiğinde bunun için günün en uygun saatinin ya da haftanın hangi gününün bunun için en uygun zaman olduğu öğrenilebilir. Geniş halk kitlelerinin abone olduğu platformlar haber ve paylaşımları belli algoritmalar dâhilinde yönlendirebilmektedirler. Belli bir abone grubuna belli mesajları sınırlanırken, seçilmiş diğer gruplarda aynı mesaj veya bilgi sürekli bir şekilde paylaşılabilir. Bu, tarlasını sulayan bir çiftçinin vananın başına geçip tarlasının neresini sulayacağını kontrol etmesine benzer bir şekilde sosyal veriyi kontrol edenlerin hangi tür veriyi nereye ne zaman yönlendireceklerini seçmeleri ve sonucu manipüle etmesidir. Örneğin, Facebook'un yüklenen ve paylaşılan dijital materyalin kimlere ulaşacağını bir algoritma ile sınırlandırıp manipüle edebildiği bilinmektedir. Bu, sadece ticari sonuçlara sahip olacak kadar 'masum' bir kapasite değildir. Ticari ürünler için

yaygın bir şekilde kullanılan bu stratejinin siyasi veya uluslararası ilişkiler amaçları için de kullanıldığı bilinmektedir. Akar vd. (2015) tarafından yapılan ampirik çalışmada; yapısal eşitlik modeli sonuçları, sosyal etkinin en çok alternatiflerin değerlendirilmesini etkilediğini, sosyal etkinin sosyal etki kaynaklarından ve sosyal platform aktivitelerinden anlamlı şekilde etkilendiğini ve sosyal platform aktivitelerinin etkisinin daha yüksek olduğunu göstermiştir. Bu yüzden, sosyal veri ticari işletmeler kadar hükümetler, istihbarat örgütleri, suç ve terör örgütleri için son derece değerlidir. Özellikle ülke dışı kaynaklarda depolanan bu etkileme ve manipülasyon gücünün kontrolü son derece maliyetlidir ve bu güç kontrol edilemediğinde tehlikelidir. Reklam geliri için sosyal medya şirketlerinin veri toplaması ve bu veriyi kullanmasının sadece bir pazarlama aracı olarak görülmesi ve kanıksanması bir masumlaştırma ve uyuşturma çabasının ürünüdür. Bu yüzden 'big data' sadece toplanan verinin hacminin değil 'amacının' da 'big' olduğunu ima eden bir kavram olarak algılanmalıdır. Sosyal veri topladığı aşikar yabancı sosyal medya şirketlerinin faaliyetleri konusunda toplumsal bilinç artırılmalı, bu faaliyetler çok sıkı bir şekilde denetlenmeli ve uygun yasal düzenleme çok geç olmadan yapılmalıdır.

Sosyal medya platformlarının topladığı 'büyük verinin' boyutu ve kapsamı, hükümetler tarafından uygun bir maliyetle kontrol edilemeyecek kadar karmaşık ve derindir. Bunun bir sebebi toplanan verinin genelde ülke dışı sunucularda depolanmasıdır. Diğer bir zorluk ise bu alanda istihbarat ve ticari faaliyetin iç içe geçmiş olmasıdır. Sosyal medya platformlarının kontrol zorluğu gereği 'verileri paylaşmayacağı' önermesi inandırıcı ve yeterli değildir. Sosyal medya platformlarının veri toplama/depolama süreç ve teknolojileri bir asimetrik bilgi sorunudur. Hükümetlerin ve tek tek bireylerin bu platformların kullandığı teknolojiyi ve faaliyetlerinin hukuki boyutunu anlık bir şekilde anlamaları devasa yatırımlar gerektireceği için son derece maliyetlidir. Diğer taraftan, sosyal medya platformları hükümetlerin ihtiyaç duyduğu acil durumlarda iş birliği yapmayı reddedebilirler. Bu, hem insani hem de siyasi sonuçlar doğurabilir.

Bir kalite parametresi olarak güvenlik

Bu yazının kaleme alındığı dönemde, WhatsApp'ın kullanım koşullarını değiştirmesi ve kullanıcı bilgilerinin Facebook ve iştirakleriyle paylaşılmaya zorlanması güvenlik ve kalite bağlamında irdelenmelidir. Böylesi bir zorlama "tüketiciyi koruma ve gizlilik" odaklı hukuki bir problem gibi ele alınabilir. Ancak, ortada aslında bir rekabet problemi vardır. Tüketici mahremiyeti, WhatsApp'ın sunduğu hizmet için bir kalite parametresi olarak görülebilir. Burada WhatsApp edindiği pazar gücünü kötüye kullanarak tüketiciye sunduğu ürünün "kalitesini" düşürmektedir. Tüketicinin kendini güvende hissetmesini sağlayan mahremiyet politikası WhatsApp tarafından kötüleştirilmiştir. Her ne kadar tipik bir kullanıcı WhatsApp'a herhangi bir fiyat ödemese de yeni koşulları kabul etmesi halinde kullandığı hizmetin kalitesi düşecektir. Burada temel olarak hatırlanması gereken husus rekabetin pek çok parametre üzerinden gerçekleştiği; fiyatın bunlardan sadece biri olduğu; tüketici seçimi, kalite, yenilik gibi pek çok parametrenin dijital platformlarda fiyattan çok daha önemli olduğu, bu parametrelerde bir sınırlama olursa bunun esasında bir rekabet problemi olduğudur.

Bu noktada, mahremiyet ve güvenlik endişesi taşımayan, yani kalite duyarlılığı düşük olan WhatsApp kullanıcılarının aklına şu soru gelebilir: "benim verilerim başkalarıyla paylaşılsa ne olur paylaşılmasa ne olur?" Eğer bir kullanıcı, verilerinin Facebook ve iştirakleri ile paylaşılmasına izin verirse, aslında istatistiksel olarak pek çok açıdan kendisine benzeyen ama mahremiyet tercihleri daha katı olan kullanıcıların da verisini bir anlamda paylaşmış olmaktadır. İktisadi terminolojide ifade edildiğinde, bir kullanıcının WhatsApp'ın yeni koşullarını kabul etmesi, kendisine benzeyen diğer kullanıcılar için bir negatif dışsallık oluşturmaktadır (Valletti, 2021; Acemoğlu vd. 2019).

WhatsApp meselesinde akıllara gelen bir başka soru da şu olabilir: "WhatsApp zaten benden alacağını almamış mıdır?" Yani, WhatsApp hâlihazırda tüketicilere hiper-hedeflenmiş reklamlar sunmasına olanak tanıyan istatistiksel içgörüleri, daha önce topladığı kullanıcı verilerini işleyip yapay zekâ algoritmalarını eğiterek elde etmemiş midir? Bu soruya verilecek kanıt-temelli kesin bir yanıtımız olmamakla beraber cevap muhtemelen evettir. Demek ki bir kullanıcıyı eski kullanım koşullarında WhatsApp'ta tutmanın sağladığı marjinal gelir/fayda, o kullanıcıyı WhatsApp'ta tutmanın marjinal maliyetinden yüksek değil ki, WhatsApp bir "işine gelirse" teklifini kullanıcılarına sunuyor. Bir başka ifadeyle, bütün kullanıcılar WhatsApp'ı bugün terk etse bile bu platformun elinde arzu edeceği hedeflemeleri yapabilecek yeterlikte toplumsal veri mevcut olabilir.

Sonuç

Bilgi güçtür ve bilgiyi elinde tutan güce sahip olur. Diğer taraftan, bilgi dinamiktir ve değişime tabidir. Değişen bilgiye hakim olan değişimi yakalar ve değişimi değiştirir. Sosyal medya platformları, hükümetlerin dahi toplayamayacağı bilgiyi ve sosyal veriyi ticari faaliyet adı altında toplama ve kullanma kapasitesine sahiptir. Bu durum, mücadele edilmesi son derece maliyetli bir güvenlik sorunudur. Kişisel veriler kanunla koruma altına alınmışken haberleşme ve eğlenceye dayalı ticari faaliyet

adı altında toplanan 'sosyal veri' korunamamakta ve ülke dışı sunucularda depolanmaktadır. Sosyal veri sayesinde bir toplumun reaksiyon fonksiyonu ve sosyal fay hatları istihbarat, suç ve terör örgütleri tarafından çıkarılıp manipüle edilebilir. Diğer taraftan, sosyal medya platformları haberleşme, sağlık ve eğitim gibi alanlarda refah artırıcı etkilere de sahip olabilir. Bu yüzden, 'sosyal veri' tanımlanıp yasal olarak düzenlenmelidir ve bu verinin ülke dışına çıkışı yasaklanmalıdır. Kişisel Verinin Korunması Kanunu sosyal verinin korunmasına yetmeyebilir ve bu kanuna benzer bir yasal düzenleme sosyal verinin korunması için de yapılmalıdır.

Ekonomik prensipler gereği sosyal medya platformları ciddi pazar gücü elde etme eğilimindedir. Bu çalışmada açıklanan sebepler nedeniyle bu platformların pazar gücünü kırmak son derece zordur. Diğer taraftan, ekonomik ve endüstriyel organizasyon prensipleri gereği sosyal medya platformları bir veya birkaç ülkede kümelenme eğilimindedir. Bu yüzden sosyal medya işletmeleri finans kurumları, sağlık kurumları ya da hava ulaşımı işletmeleri gibi yoğun bir şekilde düzenlenmeli ve denetlenmelidir. Düzenleme ve denetlemeler; pazar gücüne (tekelleşme, tröstleşme) karşı müdahaleler, idari/hukuki müdahaleler ve eğitim/farkındalık müdahalelerini tamamlayıcı bir çerçevede ele almalıdır.

Kaynakça

Acemoglu, D., Makhdoumi, A., Malekian, A., & Ozdaglar, A. (2019). Too much data: Prices and inefficiencies in data markets (No w26296). National Bureau of Economic Research.

Akar, Erkan & Hale Fulya Yüksel & Zeki Atıl Bulut. (2015). "The Impact of Social Influence on the Decision-Making Process of Sports Consumers on Facebook". Journal of Internet Applications and Management. 6(2). Pp. 5-27.

Cabral, Luis M. B (2020). "Merger Policy in Digital Industries", *CEPR Discussion Paper No. DP14785*, 28 Mayıs 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3612854.

Cheung, Steven N. S. 1973. "The Fable of the Bees: An Economic Investigation". The Journal of Law & Economics. Vol. 16. No. 1. (Apr.). pp. 11-33.

Evans, D. S., & Schmalensee, R. (2005). The industrial organization of markets with two-sided platforms (No. w11603). National Bureau of Economic Research.

Hürriyet (2021). "Google yasaya sinirlendi! O ülkede hizmet vermeyi durduracağını açıkladı", *Hürriyet*, 22 Ocak, 2021, https://www.hurriyet.com.tr/ekonomi/google-yasaya-sinirlendi-o-ulkede-hizmet-vermeyi-durduracagini-acikladi-41721785.

Rochet, J. C., & Tirole, J. (2003). Platform competition in two-sided markets. Journal of the European Economic Association, 1(4), 990-1029.

Schumpeter, J. 1942. Capitalism, Socialism, and Democracy. New York: Harper & Bros.

Stucke Maurice E. (2018). "Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data", Harvard Business Review, 27 Mart, 2018, https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data.

Valletti, Tommaso (2021). ""An Offer We Can't Refuse": How We Gave Away Our Data and Made Big Tech What It Is Today, *Promarket*, 18 Ocak 2021, https://promarket.org/2021/01/18/facebook-whatsapp-terms-of-service-ads-data-privacy/.

Sosyal Ağlar ve Siber Güvenlik

Mustafa Yeniad, Ph. D.

Dr. Öğr. Üyesi
Bilgisayar Mühendisliği Bölümü
Ankara Yıldırım Beyazıt Üniversitesi

1. Sosyal Ağların Günlük Hayatımızdaki Yeri

Günlük yaşamımızın önemli bir bölümünü sanal ortamlarda yaşıyor durumdayız. Günümüzde yalnızca bireyler değil, kamu kurumları ve özel şirketler de hizmet ve ürünleri için interneti birincil araç olarak kullanmaktadırlar.

Yıllara göre internet kullanıcısı istatistiklerini incelediğimizde, karşımıza sürekli artış gösteren bir eğilim çıkmaktadır. Örneğin wearesocial.com platformundan elde edilen bilgilere göre, 2020 yılında dünyadaki internet kullanıcı sayısı, önceki yıla oranla %7 artarak 4,54 milyar kişiye ulaşmış; sosyal medya kullanıcı sayısı ise %9,2 artışla 3,80 Milyar kişiye yükselmiş; sosyal medyada geçirilen günlük ortalama süre ise yine önceki yıla oranla %1,4 artarak ve 2 saat 24 dakikaya çıkmıştır. Ülkemizde toplam 62 milyon internet kullanıcısının 54 Milyonu sosyal medya platformlarında aktif hesabı olan kişilerden oluşmaktadır.

Geçtiğimiz yıl dünya genelinde en sık ziyaret edilmiş ilk 7 web sitesinden 3 tanesi sosyal ağdır. Hal böyle olunca, siber tehditler ve sosyal mühendislik yöntemleri için en kullanışlı aracın "sosyal ağlar" olduğu gerçeği ile karşılaşıyoruz. Sosyal ağlar "*tekilden çoğula*" doğru kullanıcıların içerik paylaşımı yapmalarını sağlayan araçlar sunmanın yanında, bünyelerindeki harici oyunlar ve uygulamalar ile üçüncü parti servisler üzerinden de insanların birbirleriyle iletişim kurmalarını sağlamaktadır.

2. Siber Güvenlik Bağlamında Sosyal Ağlar ve Sosyal Mühendislik İlişkisi

Uygulandığı alana göre farklı tanımları yapılıyor olsa da "siber güvenlik" terimini bilişim sistemlerinde sürekliliğinin ve veri bütünlüğünün (değişmezliğinin) sağlanması, gizliliğinin (yetkisiz erişime karşı) korunması amacıyla yürütülen faaliyetler şeklinde tanımlayabiliriz. Siber güvenlik ihtiyacı ve endişelerinin bir sonucu olarak hem kamu kurumları hem özel şirketler bütçelerinin yüksek bir kısmını bu alandaki faaliyetler ve ürünler için ayırmaktadırlar ancak yapılan araştırmalar, donanım ve yazılım tabanlı güvenlik ürünlerinin, özellikle sosyal mühendislik teknikleri kullanılarak yapılan saldırılarda yetersiz kaldığını göstermiştir. Bu durumun doğal bir sonucu olarak da siber güvenlik alanındaki en zayıf halkanın "insan" olduğu kabul edilebilir.

Sosyal ağlardaki kullanıcı sayısının artması, bu alandaki güvenlik tehditlerinin çeşitlenmesine ve risklerin de yüksek oranda artmasına neden olmuştur. Sosyal mühendislik tekniklerine yenik düşen, gizlilik ve güvenlik ilkelerini göz ardı etmiş bilinçsiz kullanıcılar hem kendileri zarar görebilmekte hem de çalıştıkları kurumlar için telafisi güç zararlara neden olabilmektedir.

Sosyal mühendislik saldırılarının amacı, saldırganın sistem içerisindeki bir kullanıcı aracılığıyla hassas verileri sızdırmasını veya sisteme yetkisiz erişimini sağlamaktır. Sosyal mühendislik bir anlamda insan aldatma sanatı olarak da ifade edilmekte, insanları istemedikleri şeyleri kendi rızaları ile yapmaya ya da gizli bilgilerini vermeye ikna eylemi olarak tanımlanmıştır. Bu ise genellikle personelin iyi niyetinin veya zaafının kötüye kullanılması şeklinde olmaktadır.

Sosyal mühendislik saldırıları internet tarihinin en eski ve en tehlikeli saldırı türlerinden biridir ve saldırgan için hedef sistemin kullanıcısıyla iletişim kurabilmek için sosyal ağlar oldukça etkili imkanlar sağlar. Sosyal mühendislik saldırılarında ilk aşama hedefin belirlenmesi ve kurbanın seçilmesi olup, genel olarak da en zayıf halkayı bilgisiz ya da dikkatsiz kullanıcılar oluşturur. Sosyal mühendislik yöntemlerinin başarısı genellikle acele etme duygusuna bağımlı olduğundan, saldırganlar kurbanın ne olup bittiği hakkında çok fazla kafa yormamasını bekler. Kurban hakkında bilgi toplanarak ikinci aşamaya geçiş yapılır. Bilgi toplama, sosyal mühendislik saldırılarında en önemli aşama olup bu esnada saldırganlar toplanacak verinin değerini önemsemez ve kurban hakkındaki her türlü veriyi özellikle de sosyal ağlar aracılığıyla elde etmeye çalışır. Üçüncü aşamaya gelindiği zaman sistemdeki zafiyet tarama süreçleri devreye girer. Zafiyet tarama bunun için hazırlanmış özel yazılımlar kullanılarak genellikle otomatik şekilde gerçekleştirilir. Aktif (hedef sistemle doğrudan etkileşime geçilerek veri toplanmaya çalışılır) ve pasif (hedef sisteme ilişkin dolaylı sorgulamalar arama motorları, sosyal medya hesapları, bloglar, forumlar ve kariyer siteleri üzerinden) tarama şeklinde iki ayrı metotla yürütülen bu sürecin sonunda elde edilen veriler sonraki aşamalar için destek sağlamaktadır. Elde edilen veriler saldırgana hedef sistemle ilgili kullanılan işletim sistemleri, veri tabanları, sunucu servisleri ve sürümleri, ağ mimarisi, alan adları, açık portlar ve daha pek çok konuda bilgi sağlar. Risk modellemesi ve bu konuda kapsamlı analizlerin ihmal edilerek önlemlerin alınmamış olduğu sistemler, saldırganlar için kolay lokmadır. Son aşama ise hedefe ulaşma ve sonrasında kanıtların ortadan kaldırılması sürecidir. Sosyal mühendislik

saldırılarının vereceği zararlar yetkisiz erişim elde etmek, itibar ve güven kaybı, veri hırsızlığı, sistemi çalışmaz hale getirme ve hedef kurum ya da kişilikleri yasal yaptırımlarla karşı karşıya bırakma şeklindedir.

Sosyal ağlarla ilgili bir diğer risk unsuru kullanılmayan hesaplardır. Güvensiz parolalar atanmış ve kullanılmayan hesaplar, oyunlar ya da üçüncü parti uygulamalar aracılığıyla saldırganlar hesap sahibi adına paylaşımlar yapabilmekte ve bağlantılı olduğu kişilerden çeşitli taleplerde bulunabilme, içerik paylaşımı, mesajlaşma, yorum yazma ve daha farklı çeşitli yasadışı aktiviteler yapabilmektedir.

Fotoğraf, video, yer ve konum bilgisi ile her türden kişisel verinin paylaşılabildiği sosyal ağ ortamlarında güvenlik ve gizlilik ayarlarına yeteri kadar önem vermeyen ve varsayılan seçeneklerden ötürü nelere izin verdiğinden habersiz kullanıcılar, farkında olmadan çok yönlü risklerle karşı karşıya kalmaktadır. Örneğin sosyal ağlar aracılığıyla bağlantıları paylaşılan ve genellikle kaynağı bilinmeden indirilen uygulamalar gereğinden fazla kişisel veri talep edilmekte, arkadaş listelerine ve açık profil bilgilerine erişmekte, kullanıcı adına paylaşım veya beğenide bulunma, kamera, mikrofon ve veri erişimine izin vermekte, mesajlarının okunması ve konuşmalarının dinlenmesi gibi istenmeyen durumlar yaşatabilmektedir. Öte yandan paylaşıldığında kişileri zor durumda bırakabilecek kişisel veriler, konum ve yer bilgisi, aile ve arkadaşlara ait özel bilgiler sosyal ağlarda ve özellikle bilgi talep eden uygulamalarda ciddi potansiyel sorunlara da davetiye çıkarılmaktadır.

Akıllı telefonlar ya da diğer cihazlar ile çekilen resimlere çoğu zaman coğrafi konum bilgisi bir meta veri (EXIF) (fotoğrafın çekildiği tarih, yer, boyut, cihaz bilgileri ve çekim ayarlarına kadar birçok bilgiyi barındırır) kullanıcıdan habersiz ve genellikle otomatik olarak eklenmektedir. Örneğin, dijital fotoğraf makineleri veya akıllı cep telefonları ile çekilen bu türden bir resim dosyasına, o fotoğrafın nerede çekildiğine dair coğrafi konum bilgileri de işlenmiş olduğundan, bunları sosyal ağlara yüklediğiniz andan itibaren, o ağların veri ayıklama servisleri otomatik olarak bu resimlerin meta verilerine erişerek bunları kendi veri tabanlarına kaydetmektedir. Bunun yanı sıra, paylaşılmış aynı resimlere ulaşabilen başka herhangi bir sosyal ağ kullanıcısı da bu içerikleri kendi bilgisayarına indirip, EXIF meta veri görüntüleme araçları ile içeriklerin meta verisinde yer alan coğrafi konum verilerine kolayca ulaşabilmekte ve bu verileri Google Maps veya Google Earth benzeri araçlara girilerek fotoğrafın çekildiği yerin adresini saniyeler içerisinde elde edilebilmektedir.

3. Sosyal Ağlar ve Bilgi Güvenliği

Sosyal ağlardaki içerikler, servisi sağlayan firmanın sisteminde -yedekleme gereği sunulan seçenekler sayesinde- depolandığından bu veriler üçüncü şahıs veya kurumlarla paylaşılabilir hale gelmektedir.

Anlık mesajlaşma yazılımlarında silinen mesaj ya da içerikler genellikle anlık olarak silinmek yerine uygulama veri tabanında veya dosya sisteminde mantıksal olarak silinmiş şeklinde işaretlenerek yaşlandırma veya boyut arttığında yeni mesajların eskilerin yerine kaydedilmesi ile sonradan silindiğinden, içerikler en azından bir süre daha cihazlarda yaşamakta ve erişilebilir de olmaktadır.

SMS *(Short Message Service)* olarak bildiğimiz kısa mesaj hizmeti, mesajların tamamen şifresiz olarak gönderildiği bir hizmettir. SMS ile gönderilen mesajlar alıcısına ulaştırılmak üzere salt metin olarak olduğu gibi mobil hizmet operatörünün sunucularına iletilir. Mobil hizmet operatörünün sunucularına gelen mesaj, buradan alıcının telefonuna gönderilir. Tüm bu iletişim sırasında gönderilen mesaj içeriği, salt metin biçiminde olduğundan, istenildiğinde herkes tarafından okunabilir durumdadır.

Anlık mesajlaşma yazılımlarının sunmaya başladığı "Uçtan Uca Şifreleme / End-to-end Encryption (E2EE)" özelliği, temelinde "Simetrik Şifreleme (Symetric Encryption)" yöntemine dayanır ve bu yöntem şifreleme algoritmaları içindeki en eski ve en iyi bilinen tekniktir. Simetrik şifreleme adından da anlaşılacağı üzere, tek / aynı şifreleme anahtarına dayanan şifreleme türüdür. Veriyi şifrelemede gönderici tarafında kullanılan aynı anahtar, aynı zamanda alıcı tarafında da veriyi çözümlemek amacıyla kullanılır. Yani hem gönderici hem alıcı aynı gizli anahtarı kullanmaktadır. Gizli anahtar, rastgele üretilmiş bir sayı veya kelime dizisi olabilir. İşlem süresinin hızlı olması simetrik şifreleme algoritmalarının en önemli avantajlarındandır fakat aynı anahtara sahip olan üçüncü bir taraf şifrelenmiş içeriklere kolayca erişebildiğinden, daha sürecin başında şifreleme anahtarının kim tarafından ve hangi algoritmik yöntem(ler)le üretildiği burada hayati önem kazanır. Ayrıca şifreleme ve çözümlemede kullanılan algoritmaların kapalı tutulması, alanda standart kabul edilen algoritmaların *(örneğin AES, DES, 3DES, RC4, RC5, IDEA vb.)* kullanılmaması ya da kullanılan algoritmaların bağımsız kuruluşlarca onaylanarak güvenirliğin akredite edilmemiş olması durumu, hatta bir ana-anahtar / master-key varlığından emin olunamaması, tüm şifreleme sürecini güvenilmez kılar. Bunun yanında simetrik şifreleme sürecinin birtakım zorlukları da mevcuttur. Örneğin şifreleme anahtarının güvenli olarak saklanması ve diğer ağdaki diğer kullanıcılarınkinden

benzersiz anahtarların üretilmesi şarttır. Kimlik doğrulama (authenticity) sağlanmadığından anahtara sahip olma potansiyeli bulunan herhangi bir üçüncü taraf burada ciddi risk oluşturur. Ayrıca veri bütünlüğü (integrity) desteklenmediğinden, iletim ortamında araya girme yöntemi ile verinin manipülasyonu da söz konusu olabilmektedir. Ek olarak, anlık mesajlaşma platform sahibi şirketler sistemlerinde kendileri ile anahtar paylaşımını zorunlu kılan gerekçeler oluşturabilir, hatta sistemlerinde şifrelemeyi atlatan arka kapılar da bulundurabilirler. Benzer durumun, kaynak kodları kapalı olan ya da bağımsız otoritelerce kaynak kodları incelenerek ilgili akreditasyonu onaylanmamış tüm yazılımlar (işletim sistemleri, veri tabanları, ağ güvenlik yazılımları, e-posta sistemleri, çevrim içi iletişim ortamları vb.) için de söz konusu olduğu unutulmamalıdır.

4. Sosyal Ağ Ortamında Nelere Dikkat Etmeliyiz?

Sosyal ağlarda dikkat edilmesi gereken genel hususlardan bahsedecek olursak;

- Sosyal ağ platformlarının kullanım politikası ve gizlilik sözleşmelerini dikkatle okuyarak, gizlilik ve güvenlik ayarlarının gözden geçirilmesi, varsayılan güvenlik ve gizlilik ayarları yerine sıkılaştırılmış ayarların kullanılması ve bunları incelemek için zaman ayrılması,
- Herhangi bir ön işlemden geçmeyip doğrudan sosyal ağa eklenen fotoğraf ve videoların meta verileri ile EXIF bilgileri gibi konum tanımlayıcı ve ayırt edici veriler, içerik üretim aşamasında engellenmeli,
- Farkındalığı artıracak eğitimlerin alınması ve dokümantasyonun incelenmesi,
- Mesajlaşma uygulamaları kullanılırken -mutlak bir güvenlik sağlayamasa da- uçtan uca şifreleme sunan uygulamaların tercih edilmesi,
- Dijital parmak izi olarak nitelendirilebilecek hangi kişisel verilerin hangi internet ortamlarında paylaşıldığının tekrar gözden geçirilmesi (örneğin özgeçmişlerdeki bilgiler),
- Kritik hesaplar için iki faktörlü kimlik doğrulama sisteminin (2FA) (böylece tek başına parola yeterli olmayacağından tek kullanımlık kod, ses tanıma, elektronik imza, parmak izi veya SMS onay kodları ek doğrulama amaçlı) kullanılması,
- Hesap erişim izninin tanınan ve güvenilen kişilerle sınırlandırılması,
- Kişisel bilgilerin mümkün olduğunca paylaşılmaması,
- Farklı hesaplar için aynı parolanın kullanılmaması,
- Cihaz konum verisinin kapalı tutulması,
- Kolay tahmin edilebilir parolalar yerine, yüksek sayıda karakterden oluşan hem küçük hem büyük harfler, rakamlar ve içinde özel karakterler içeren tahmin edilmesi zor güçlü parolalar belirlenmesi,
- Kaynağından emin olunamayan bağlantılara tıklanmaması, bağlantı veya mesaj ekindeki yazılımların kurulmaması,
- Sosyal ağlara telefon aracılığıyla erişiliyorsa, uygulamalara verilen erişim izinlerinin gözden geçirilmesi ve gereksiz veya riskli olduğu düşünülen izinlerin kaldırılması,
- Kişisel olmayan bir bilgisayarda mümkünse bir sosyal ağ hesabına giriş yapılmaması,
- Ses kaydı aracılığıyla mesajlaşma yerine, yazışma yönteminin kullanılması (ses çözümleme teknikleri aracılığıyla kurbanın sesi kolayca taklit edilebilmektedir),
- Sosyal ağlara giriş yapılan bilgisayarlarda mutlaka internet güvenlik yazılımları (antivirüs, güvenlik duvarı vb.) kullanılmalı,
- Toplu kullanıma açık kablosuz ağların mecbur kalınmadıkça sosyal ağ hesaplarına erişim için kullanılmaması şeklinde özetlenebilir.

Siber Uzay, Siber Güvenlik, Dijital Egemenlik Kavramlarının Uluslararası Hukuk Bağlamında Değerlendirilmesi

Hatice Kübra Ecemiş Yılmaz, Ph. D.

Öğr. Gör. Dr.,
Hukuk Fakültesi-Milletlerarası Hukuk
Ankara Yıldırım Beyazıt Üniversitesi

Öz

Siber uzayda etkili uluslararası hukuk kurallarının olmaması, teorik ve politik tartışmalarda konunun büyük ölçüde gündeme gelmesine yol açmıştır. Çünkü siber alandaki karmaşıklıklar aktörlerin anlaşma yapmalarını zorlaştırır ve bu da devletler tarafından kabul edilebilecek bağlayıcı kuralların konulmasına engel olmaktadır. Akademik platformlarda yapılan tartışmalarda siber uzay üzerinde uluslararası hukuk kurallarının oluşturulmasında devletlerin etkin rolünün olması gerektiğine inananlar ile siber uzayın devletlerden bağımsız özgür bir alan olarak kalması gerektiğine inananlar farklı kutuplara ayrılmıştır. Yine akademik alanın dışında da, siber uzayla ilgilenen uluslararası kurumlarda yapılan tartışmaların çoğu siber uzayda aktörlerin karmaşık yapısından dolayı uluslararası hukuki düzenin, yargılama yetkisinin olmamasından kaynaklanmaktadır. Son birkaç yılda, başta devletler olmak üzere birçok uluslararası aktörün, internet ile ilgili bilgi, iletişim, veri ve altyapı üzerindeki kontrolünü sağlama konusundaki ilgilerini artırmak için dijital egemenlik fikrini teşvik etmesi konuyu daha da karmaşık hale getirmiştir. Ayrıca bu durum, siber güvenliğe ilişkin gelecekte oluşturulabilecek uluslararası hukuk normları için ede daha fazla zorluklar yaratmaktadır. Cevap aranması gereken konular devletlerin dijital egemenliklerini öne sürdüğü siber uzaydaki davranışları üzerinde uluslararası hukuk kurallarının geçerliliğinin olup olmadığı, siber uzayda kontrol ve denetimin mevcut uluslararası hukuk kuralları ile zorluğunun nasıl çözülebileceği, siber uzay ve dijital egemenlikte uluslararası hukuk kurallarının nasıl yer bulabileceğidir.

Giriş

Özellikle son yıllarda, siber uzay kavramı genişlemiş ve insan yaşamının birçok yönünü etkilemiştir. Devletler, örgütler ve bireyler, siber uzayın sunduğu fırsatlardan kapsamlı bir şekilde yararlanmıştır. Siber alan, uluslararası toplumun geleneksel siyasi, sosyal ve ekonomik yapılarına meydan okumuştur. Bu, iletişimin hızını, hacmini ve kapsamını radikal bir şekilde artırıp devletlerin yönetim biçimini, şirketlerin hizmet ve kamu mallarını sunma stilini, bireylerin çevrimiçi sosyal ağlarla etkileşime girmesini ve vatandaşların sivil topluma katılma şeklini büyük ölçüde değiştirmiştir (Betz & Stevens 2011). Bu gelişmelerle birlikte, siber uzayın ortaya çıkışı, bireysel ve toplu güvenlik için de büyük zorluklar ortaya çıkarmıştır. Kritik ulusal altyapı, siber saldırılara karşı savunmasız kalmış olup; dünya ekonomisi siber suç ve siber casusluk tarafından tehdit edilmeye ve bireyler ise bilgisayar korsanları tarafından terörize edilmeye başlamıştır. Siber alanda, siber saldırılar ulusal sınırları aşmakta hem sivil hem de askeri ağları etkileyebilmektedir. Devletler açısından ise, bunların izlenmesi ve takibi zordur. Askerler, terörist gruplar ve hatta bireyler artık sadece askeri bağlantılara karşı değil, aynı zamanda bilgisayar ağlarına bağlı kritik altyapılara karşı da siber saldırılar başlatma yeteneğine sahiptir (Liaropoulos 2011b). Haberler, özel ve kamusal iletişimin kesintiye uğradığı, bankacılık sistemlerinin manipüle edildiği ve hatta askeri iletişim sistemlerinin tahrip edildiği vakalarla doludur. İlgili duruma sosyal medya şirketlerinin içerisinde yer aldığı seçim manipülasyonları örnek olarak verilebilecektir. Bu manipülasyonlar uluslararası platformlarda artık devletler için güvenlik sorunu haline gelmeye başlamıştır. *Cambridge Analytica* adındaki danışmanlık şirketi, 2015 yılı içerisinde çok sayıda *Facebook* kullanıcısının verilerini izin almadan elde etmiş, seçim çalışmalarında da ele geçirdiği bu bilgileri kullanmıştır. *Facebook* tarafından üyelerinin verilerinin kullanılmış olduğu bu nedenle de sorumlu olunacağı kabul edilmiştir. Yine 2016 yılındaki Amerika Başkanlık Seçimlerinde sosyal medya mecraları üzerinden müdahale edildiğine dair ortaya çıkan haberler devletlerin karşı karşıya kaldıkları güvenlik riskini daha çok gözler önüne sermektedir. Bunun sonucunda, kaçınılmaz olarak bir dizi soru ortaya çıkmaktadır. Devletler siber uzaya nasıl uyum sağlayacaktır? Devletlerin sınırsız bir dünyada yetkilerini ve kontrollerini kullanmaları mümkün müdür? Bu soruların doğru şekilde cevaplanabilmesi için, devletlerin uluslararası hukuk düzenini koruyacak şekilde hareket etmesi gerekmektedir. Çünkü uluslararası düzenin korunamaması devletlerin gelecekte kendi çıkarlarını da olumsuz yönde etkileyecektir. Bu nedenle devletlerin

siber uzayda da uluslararası düzeni sağlamak için çalışmalara başlaması gerekmektedir.

Siber Uzayda Uluslararası Hukuk ile ilgili Süregelen Sorunlar

Siber uzay devletlerin ya da insanların faydalanabileceği, olumlu faaliyetlerin yer alacağı bir alan olarak karşımıza çıkabileceği gibi, silahlı saldırı boyutuna ulaşabilecek siber saldırıların oluşabileceği, insanlara ve devletlere zarar verebilecek bir alan olarak da karşımıza çıkabilir.

Devletler siber saldırıların uluslararası hukukta var olan savaş hukuku kuralları içerisine dahil edilip edilemeyeceğini tartışmaya devam etmektedirler. Bu nedenle de, siber uzayın uluslararası hukuk kuralları ile düzenlenmesi fikri 1996'dan bu yana, hukuk uzmanları, iş aktörleri ve devletler tarafından sürekli gündeme gelmiştir. Bazı devletler bu durumu kendi iç hukuklarına uygun olarak tek başlarına yürütmeye çalışmıştır. Örneğin 2017 yılının Ekim ayında Almanya'da kabul edilip 2018 yılında yürürlüğe giren Sosyal Medya Alanlarındaki Hukuki Uygulamaların İyileştirilmesi yasası Avrupa içerisindeki ilk sayılabilecek düzenlemelerden bir tanesidir. Bazı devletler ise ortak karar verilebilmesini sağlamak amacıyla örgütler kurup yasal düzenlemeler ya da regülasyonlar yapmaya başlamışlardır. Örneğin, Amerika Birleşik Devletleri (ABD)'nde, bu amaçla oluşturulan Siber Savaş Komutanlığı, siber saldırıların askeri amaçlı kullanımını resmi olarak tanımlamıştır. Bu tanıma göre, bir siber saldırı düşmanca hareket ederek hedef alınan devletlerin siber alandaki sistemlerine zarar verilmesidir (Hathaway vd; 2012: 825). Diğer bir tanım ise, Şangay İşbirliği Örgütü tarafından yapılmıştır. Şangay İşbirliği Örgütü ülkeleri arasında Uluslararası Bilgi Güvenliğini Sağlamaya Yönelik İş Birliği Anlaşmasında yapılan tanımda ise siber saldırılar için, yeni iletişim ve bilgi edinme sistemleri üzerindeki teknolojik gelişmeler nedeni ile sivil hatta askeri nitelikte düzeni bozabilecek derecede uluslararası güvenlik sorunlarına neden olabileceği ifade edilerek bu nedenle de siber saldırılara karşı uluslararası mücadelenin ulusal mücadeleye tercih edilmesi gerektiği belirtilmiştir. Örgütün siber saldırılara ilişkin tanımlama yaparken, daha kapsamlı bir tanım yaparak siyasi istikrarı da içine aldığı görülmektedir. Sonuç olarak, ulusal ve uluslararası yapılanmalar tarafından ortaya atılan siber saldırı tanımlarında ortak ifadeye ulaşılamamasından kaynaklanan uygulama zorluğu ve karmaşıklığı çıkmaktadır. (Hathaway vd; 2012: 826-828).

Uluslararası hukuk açısından siber saldırıların değerlendirilmesini gerekli kılan sebeplerin başında siber uzayda kimlik tespitinin veya saldırının gerçekleştiği mekanının neresi olduğunun anlaşılıp tespit edilmesinin zor olmasıdır. Örneğin saldırının gerçekleştiği merkez yurtdışında olabilmekte, devletlerin ulusal sistemleri içerisinde de irtibat merkezleri ya da temsilcilikleri olmadığı için yapılan saldırıların tespiti, sona erdirilmesi ya da delillerin temini konusunda zorluklar çıkabilmektedir. Yine bu durumlara karşı devletler ulusal bazda karar almış olsalar da, alınan kararların uygulanması konusu yine problem oluşturmaktadır.

Uluslararası hukuk bakımından uygulanabilen kuvvet kullanma yasağına siber saldırılar açısından da başvurulabileceği görüşünü ABD, Çin, Rusya, İran, İtalya, Hollanda, Macaristan devletleri ile Avrupa Birliği ve BM gibi uluslararası örgütler savunmaktadırlar. (Roscini, 2014). Resmi olarak en iyi örnek 2013 ve 2015 yılında BM Uzmanlar Heyeti tarafından yayımlanan raporlarda, uluslararası hukuk kurallarının siber uzay için de uygulanabileceğinin belirtilmiş olmasıdır.

Ancak siber uzayla ilgili bağlayıcı ve iyi işleyen uluslararası hukuk kuralları ilgili alanda devam eden tartışmalar nedeni ile hala mevcut değildir. Bu tartışmalar, siber uzayda uluslararası kamu hukukunun temel ilkeleri ve özellikleri nedeni ile yargılamada, tahkimde ve uluslararası hukuk normlarının formüle edilmesinde yaşanan zorlukların merkezinde yer edinmektedir. Devlet egemenliği ile ilişkili olarak doğan yargı yetkisi ülkesel olmasına rağmen uluslararası hukukta aksine bir kural yoksa devletler, yargı yetkilerinin kullanım alanlarını serbestçe genişletebileceklerdir. (Rabinovitch, 2004: 505). Ancak belirtilmesi gereken husus, uluslararası hukuk normlarındaki yargı yetkileri genel olarak hukuk kurallarının uygulanabileceği bölge ile ilgilidir. Siber uzaydaki hukuk konusu olabilecek aktörler devletlerden, internet şirketlerinden, büyük ya da küçük işletmelerden, bireylerden ve bunlara benzer çok çeşitli aktörlerden oluşabilirler. Her bir aktör siber uzay ile ilgili kendi ilgi alanlarına göre farklı sorunlara sahip olabilirler. Bu nedenle de siber uzayda uluslararası hukuk kurallarının yapılmasının kimler için meşru olacağının ya da hangi konuları içereceğinin tespit edilmesi son derece güç olacaktır. Siber uzay kavramı düşünüldüğünde ilgili davranışların nerede, kim tarafından, nasıl yürütüldüğünün tespiti de giderek zorlaşmaktadır. Özellikle siber saldırıyı gerçekleştiren bir devlet ise, bu davranışın devlete atfedilebilmesi (isnat edilebilmesi) sorunu akademik alanda pek çok kez tartışılmıştır. (Rid ve Buchanan, 2014). Siber uzayda siber saldırıların etki alanı açısından, uluslararası aktörler, siber uzayın durumu konusunda bir anlaşmaya varamamışlardır.

(Liaropoulos, 2017). Sonuç olarak, siber uzayda uluslararası hukukun yargı yetkisini belirleyebilmek büyük zorluklar yaratmaktadır.

Siber uzayda aktörlerin karmaşık durumu uluslararası hukuk içerisindeki tahkim yoluna başvurmayı da zorlaştırmaktadır. Siber uzaya uygulanabilecek hukuk kurallarında, aktörlerinin çeşitliliği nedeniyle, uyuşmazlık çözüm mekanizmalarının ve tahkim yetkisini kimin alması gerektiği konusunda ulaşılan, evrensel olarak kabul edilmiş bir yasal norm hâlâ yoktur. Lahey' de bulunan Uluslararası Daimi Tahkim Mahkemesi, halihazırda uzay, enerji ve çevre davalarına bakmakla yetkilidir. Bu nedenle de siber uzayda hüküm veren taraf olabilme ihtimali vardır. Bununla birlikte, bu tür yetkileri ve otoriteleri siber uzay kullanabilmek ve verilen kararları bağlayıcı kılmak için tarafların en başta uzlaştıkları tahkim sözleşmesinde hakemlerin verecekleri karara uymayı taahhüt etmeleri gerekmektedir. Yine siber uzay ile ilgili içtihatların oluşmasının zorluklarının da dikkate alınması gerekmektedir.

Hukuk kuralları açısından her ne kadar Budapeşte Sözleşmesinin siber uzay ile ilgili konuları içeren uluslararası antlaşma olduğu söylenebilse de, anlaşmazlıkları çözmek adına bağlayıcı bir mekanizmasının olmaması, siber saldırılardan çok siber suçlara odaklanmış olması, genellikle devlet merkezli olması sözleşmeyi zayıf hale getirmektedir.

Siber Uzayda Güvenlik

Gelişen teknoloji ve iletişim araçları sonucunda, siber savaşların geleneksel savaşlara nazaran daha cazip olduğu düşünülmeye başlanmıştır. 1) Maliyetin düşük olması, 2) tanınma veya tespit edilmenin zor olması, 3) sınır tanınmaması, 4) beklenmedik anda saldırıda buluna bilinmesi ve 5) geniş etki alanına rağmen can kaybının olmaması ya da çok az düzeyde olması siber savaşları daha cazip hale getiren nedenler arasında sayılabilecektir. İlgili avantajlar göz önünde bulundurularak gerçekleştirilen siber savaşlara örnek olarak Estonya(2007) ile Gürcistan(2008) Savaşları gösterilebilinir. (O'connell, 2012: 188; Ashmore, 2009). Estonya'nın Tallinn şehrinde 2007 yılında gerçekleşen savaş, Bronz Asker adı verilen anıtın bulunmakta olduğu Tallinn Meydanından kaldırılıp yerinin değiştirilmesi kararı ile ortaya çıkmıştır. Siber saldırılar, hükümeti, gazeteleri, cep telefonlarını, acil müdahale sistemlerini ve bankaları hedef alarak Estonya iletişim ağlarını geçici olarak bozmuştur. Hedefler Estonya cumhurbaşkanlığını, parlamentosunu ve birçok hükümet Bakanlığını içermiştir. Estonya Hükümeti gerçekleşen saldırının Rusya kaynaklı olduğunu ileri sürmüştür. Ancak bu iddia Rusya tarafından kabul edilmemiştir. Devlete atfedilme sorunu nedeni ile Estonya misilleme de bulunamamıştır (Tsarougias 2012; O'connell, 2012: 192). Estonya'nın siber savaştan korunması için siber savaş birimi faaliyete geçirilmiştir. Rusya'nın Estonya saldırısını gerçekleştirdiği isnat edilmesinin zorluğu yüzünden ispat edilememiş, sadece iddia seviyesinde kalmıştır. Ancak bu durumun NATO devletleri ile, ABD gibi Batılı ülkeler açısından gelecekte tehdit unsuru oluşturabileceği düşünülmüştür. NATO üyesi olan Estonya'nın maruz kaldığı bu saldırılardan sonra, NATO üyesi diğer devletler bir yandan ulusal siber güvenlik stratejilerini kendi kendilerine kurmaya çalışırken, diğer yandan Siber Savunma Mükemmeliyet Merkezi, Tallinn'de kurulmuştur. NATO müttefiki olan devletlerin siber savaşın uluslararası hukuktaki yerini anlamaları, ayrıca böyle saldırılara karşı uygulayabilecek kuralların belirlenebilmesi için Tallinn El Kitabı yazılmıştır.

2008 yılına gelindiğinde ise Gürcistan, ülkenin toprak bütünlüğünü korumak amacı ile Güney Osetya'ya yönelik operasyonlara başlamıştır. Ardından, Rus güçleri de Osetya'ya gelmiş, Gürcistan'ı işgal amacı ile saldırı başlatmıştır. Bunun akabinde, Rusya geleneksel savaşın yanında Gürcistan'a karşı siber saldırılarda bulunmaya başlamıştır (O'connell, 2012: 192- 193). Rusya başlattığı siber savaş ile Gürcistan hükümetinin web sitelerine, medya ve iletişim hizmetlerine siber saldırılar düzenlemiştir. Estonya davasında olduğu gibi, bu saldırıların arkasında kimin olduğuna dair bir kanıt bulunamamıştır. Rusya, saldırıların arkasında olduğuna ilişkin ileri sürülen iddiaları kabul etmemiştir.

Siber savaşlarla ilgili olarak, İran Nükleer tesislerine yönelik ABD tarafından gerçekleştirildiği ileri sürülen Stuxnet isimli virüsün neden olduğu zararlara değinmek gerekecektir. Bu siber saldırıda İran Nükleer tesislerinde virüs sisteme bulaşmıştır. Virüs tüm sistemi etkisi altına almış, nükleer tesiste fiziksel zararlara neden olmuş, tesisin belli kısımlarını işlemez hale getirmiştir (O'connell, 2012: 194 vd.; Çelik, 2013: 137- 175). İnternetin var olmasına bağlı kalınmaksızın bilgisayarların veri girişi yapılabilen araçlarla ele geçirebileceğini göstermesi açısından öneme sahiptir. Ayrıca, Stuxnet saldırısından önce siber saldırılar ile sadece yazılımlara veya ağlara zarar verildiği görülürken, Stuxnet ile beraber siber saldırılar ile fiziki olarak da zararların da meydana gelebileceği ortaya çıkmıştır. Bahsi geçen olaylar, devlet ve devlet dışı kötü niyetli kişilerin hükümetlere, özel kuruluşlara ve sıradan vatandaşlara ait milyonlarca bilgisayarı ele geçirme ve kontrol etme yeteneğine sahip olduğunu göstermektedir.

Bu gelişmeler nedeni ile uluslararası hukuk alanında da tanımlamalar yapılmaya çalışılmıştır. (Hughes 2010; Tikk, Kaska & Vihul 2010; Schmitt, 2013; Zeng, et.al., 2017; Woods, 2018)) Siber alan ile ilgili pek çok konuyu derinlemesine ele alan büyüyen bir literatür vardır, ancak sonuç bulmak açısından yeterli değildir.

Siber uzayın karmaşıklıklarını çözmeye çalışan biri egemenlik kavramını görmezden gelemeyecektir. Sonuçta, devlet egemenliği büyük ölçüde mevcut uluslararası düzeni tanımlar. Birleşmiş Milletler, tüm üyelerinin egemen eşitlik ilkesine dayandığını kabul etmektedir. Devlet egemenliğinin korunması hem uluslararası kuruluşlar hem de bireysel devletler için en önemli önceliktir (Franzese 2009). Egemenlik kavramına odaklanmanın iki nedeni vardır: Birincisi, bölgesel bir varlık olan devletin siber uzay gibi bölgesel olmayan ve sınırsız bir alanda egemenliği, dolayısıyla otorite ve kontrolü nasıl uygulayabileceğini keşfetmek; ikincisi, siber uzayda egemenlik tartışmasını çerçeveleyerek, siberle ilgili diğer sorunları ele almak için yararlı bir çerçeve geliştirmek. Bununla birlikte, bu tartışmanın bir başlangıcı olarak, "siber uzay" ve "egemenlik" terimlerinin tanımlanıp, yorumlanmasına ihtiyaç vardır.

Siber saldırılar ile ilgili olarak uluslararası hukuk kuralları oluşturulmaya çalışılırken, konulacak kuralların ya da yapılacak tanımların ilgili devletin ulusal sınırlarında oluşabilecek siber saldırıların yanısıra uluslararası platformda ortaya çıkabilecek hukuka aykırı saldırı veya hareketleri de kapsaması gerekmektedir. Yapılacak tanımlamalarda, gelişen teknolojiler göz önünde bulundurulmalı ve çerçeve hükümler oluşturulmalıdır. Bu çerçeve hükümlerin ilk olarak devletlerin hangi tür saldırılarının siber saldırı olarak nitelendirilebileceğini, devletlerin gerçekleştireceği hangi hareketlerin siber savaşa neden olabileceğini içermesi gerekmektedir. Yine siber saldırı ya da siber savaş kavramlarının belirlenmesi için çerçeveler çizildikten sonra, devletlerin iç hukuk düzenlemeleri ile gerçekleştirmiş olduğu hareket ya da davranışların sorumluluklarından kurtulamayacağının belirtilmesi gerekmektedir. Bu durumda uluslararası hukukta devletlerin ortak olarak oluşturacağı yeni sözleşmeye uyum açısından devletlerin iç hukuklarında gerçekleşebilecek siber saldırı düzenlemeleri yapması gerekecektir. Ayrıca yeni düzenlemelerde siber saldırıların devletlere atfedilebilmesi sorununun çözümlenebilmesi için devletlerin işbirliği içerisinde hareket ederek, devletlerin ilgili siber saldırıların devletlere atfedilme sorununa da çözüm önerisi getirmesi gerekmektedir.

Siber Uzayda Dijital Egemenlik

Siber uzay, tüm iletişim ağlarının, veri tabanlarının ve bilgi kaynaklarının küresel bir sanal sistemde birleştirilmesi anlamına gelir. Kara, deniz, hava ve uzay ile keskin bir tezat oluşturan siber uzay, doğanın bir parçası değildir; insan yapımıdır ve bu nedenle yapılmayabilir ve düzenlenebilir (Herrera 2007, Gourley, 2014, 279-286). Her ne kadar sınırsız gibi gözükse de, siber uzay, mevcut fiziksel yapılarla sınırlıdır. Siber uzayı oluşturan şeylerin çoğu, devletlerin egemen topraklarında yer almaktadır. (Betz &Stevens 2011).

Siber uzayın çalışması için fiziksel bir altyapıya ihtiyaç duyduğu açıktır. Bu altyapı karasaldır ve bu nedenle devlet egemenliğinden muaf değildir (Gourley, 2014, 279-286, Von Heinegg 2012). Siber uzay düzenleme ve gözetim gerektirir. Siber uzayda faaliyet gösteren şirketler, işlerini yürütmek için devletlerin kurallarına ihtiyaç duyar (Gourley, 2014; Carr, 2016;Wu 1997). Son olarak, devletlerin siber uzayda yer almaları için ve ulusal güvenlik nedenlerinden dolayı bu alanda denetim uygulamalarını sağlamaları gerekmektedir. Devletler, egemenliği başarılı bir şekilde tesis etmek ve dolayısıyla siber uzayda düzeni sağlamak için hem teknik hem de siyasi nitelikte bir dizi kritik sorunu çözmek zorundadır. Siber uzayda oluşan siber saldırıların devlete atfedilememe, isnat edilememe problemi egemenliğin uygulanmasında büyük bir engeldir. Devletler, aktörleri belirleme ve siber saldırıları geri izleme yeteneği kazanmadıkça, siber uzayda güç kullanma iddiaları zor olacaktır.

Dijital egemenlik, uluslararası aktörler tarafından dijital alanda erişim, bilgi, iletişim, ağ ve altyapıyı kontrol etme ve yönetme fikridir. (Couture & Toupin, 2019). Son yıllarda Çin ve Rusya'nın dijital egemenlik üzerine siber ittifak yapması ; Snowden ve Wikileaks davaları; ve Google-Apple-Facebook-Amazon 'un yükselişi nedeni ile konu daha da popüler olmuştur. Bu durumlar, devlet aktörleri için elverişli olan siber alanla ilgili uluslararası hukukun yeni iklimini açık bir şekilde belirlemiştir. Bu dijital egemenlik gelişmeleri, siber uzayda özgürlük ve özgürlük ile ilgili sorunlar ortaya çıktıkça, özellikle devlet dışı aktörleri ve internet tarafsızlığını potansiyel olarak zayıflatmakla kalmayacak, aynı zamanda siber güvenliğe ilişkin olası kabul edilebilir uluslararası hukuk kurallarının uygulanmasını da engelleyecektir. Sonuç olarak, uluslararası aktörlerin siber alanla ilgili etkili ve bağlayıcı uluslararası hukuku formüle etmek için anlaşmaya varma olasılığını zorlaştırabilecektir. Dijital egemenlik, devlet aktörlerinin siber alan ihlal davaları ile ilgili yargılama ya da tahkime başvurma olasılığını daha da azaltacaktır.

Bu dijital egemenlik fikri, devlet aktörlerini uluslararası siber hukuku formüle etmek için bir anlaşmaya varmak üzere bir araya getirirse o zaman faydalı olabilecektir. Böylece, hukukun kendisi, ticari şirketler, bireysel vatandaşlar ve sivil toplumlar gibi devlet dışı aktörler pahasına dijital egemenlik konusundaki tartışmalı fikirleriyle devlet aktörlerinin çıkarları tarafından yönetilecek ve belirlenecektir.

Sonuç

Siber uzay kavramı incelendiğinde şu an için bu alanla ilgili etkili uluslararası hukuk kurallarının var olmaması sürekli tartışmalar çıkmasına ve sürekli bu tartışmaların gündeme gelmesine neden olmaktadır. Siber alandaki aktörlerin karmaşık yapısı da uluslararası alanda bağlayıcı olacak kuralların konulmasına engel olmaktadır. Uluslararası hukuk kurallarının siber uzay kavramlarına uygun olarak oluşturulabilmesinde devletlerin etkin rolünün olması gerektiği görüşü ile siber uzay alanının devletlerden bağımsız bir platform olarak kalması gerektiği görüşleri sürekli çatışma halindedir. Son yıllarda devletler ile devlet dışı aktörler internet ile ilgili altyapı, veri ya da bilgi üzerine kontrolü daha fazla sağlamak amacı ile dijital egemenlik fikrini teşvik etmeye başlamışlardır. Ancak bu durum konunun daha karmaşık hale gelmesine, siber güvenliğe ilişkin ortak oluşturulabilecek uluslararası hukuk normlarının oluşturulmasının zora sokulmasına neden olmaktadır. Siber uzayla ilgili uluslararası hukukun karmaşıklığı ve zorlukları nedeni ile dijital egemenliğe teşvik çalışmaları gündemde tutulmamaktadır. Dijital egemenlik üzerine akademik literatürün gelişimi hala büyük ölçüde devlet merkezli anlatımlar ile güvenlik politikaları konularının hakimiyetindedir. Dijital egemenliğin kavramsallaştırılması, mevcut eksikliklerin üstesinden gelinmesi için hala daha yapıcı çabalara ihtiyaç duyulmaktadır.

Dijital egemenlik fikri siber güvenliğe ilişkin muhtemel kabul edilebilir uluslararası hukuk kurallarını da zayıflatabilecektir. Bunun nedeni, dijital egemenliğin, bölgesel bazda devletler tarafından derinlemesine düzenleneceği için potansiyel olarak parçalanmış siber alanı yaratmasıdır. Dijital egemenlik fikri, şu anda var olan küresel internet bağlantısını kesecektir. Uluslararası aktörlerin siber uzay konusunda etkili ve bağlayıcı uluslararası hukuku formüle etmek için anlaşmaya varma olasılığını azaltmış olacaktır. Ayrıca, dijital egemenlik müdahale etmeme ilkeleriyle iç içe olduğundan, siber alanda oluşan ihlal vakalarının devlet aktörlerince yargılama olasılığını da güçleştirecektir. Sonuç olarak, uluslararası hukukun devletlerin siber uzay üzerindeki davranışları için yeterli olmadığı söylenebilecektir. Bu nedenle de şimdiden devletlerin iş birliği ile yeni anlaşmalar üzerine görüşmelere başlaması gerekmektedir.

Kaynaklar

Ashmore, W. (2009). Impact of Alleged Russian Cyber Attacks https://www.bdcol.ee/files/files/documents/Research/BSDR2009/1_%20Ashmore%20-%20Impact%20of%20Alleged%20Russian%20Cyber%20Attacks%20.pdf (s.e.t. Ocak 2021)

Betz, DJ & Stevens, T. (2011). Cyberspace and the state: toward a strategy for cyber-power, Routledge, International Institute for Strategic Studies, Oxon.

Carr, M. (2016). US Power and the Internet in International Relations: The Irony of the Information Age. New York: Palgrave

Couture, S & Toupin, S. (2019). What Does the Notion of "Sovereignty" Mean When Referring to the Digital?, New Media & Society, 21(10):2305-2322.

Çelik, Ş. (2013). Stuxnet Saldırısı ve Abd'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 15(1), 137-175.

Franzese, P.W. (2009). Sovereignty in cyberspace: can it exist?, Air Force Law Review, vol. 64, pp. 1-42.

Gourley, S. K. (2014). "Cyber Sovereignty", in Conflict and Cooperation in Cyberspace: The Challenge to National Security. Ed. Panayotis A. Yannakogeorgos & Adam B. Lowther. Boca Raton: Taylor & Francis.

Hathaway, O., Crootof, R., Levitz, P., Nix, H. (2012). The Law of Cyber-Attack, California Law Review, 100 (4), 817-886

Herrera, G. (2007). "Cyberspace and sovereignty: thoughts of physical space and digital space", Power and security in the information age: investigating the role of the state in cyberspace, Ashgate, Burlington.

Hughes, R. (2010). A treaty for cyberspace, International Affairs, vol. 86, no. 2, pp. 523-41.

Liaropoulos, A . (2011). "Power and security in cyberspace: implications for the Westphalian state system", in Panorama of global security environment, Centre for European and North American Affairs, Bratislava.

Liaropoulos, A. (2017). "Cyberspace Governance and State Sovereignty", in Democracy and an Open-Economy World Order, ed. George Bitros & Nicholas Kyriazis. Cham: Springer.

O'Connell, M. (2012). Cyber Security without Cyber War, Journal of Conflict and Security Law, 17 (2),187-210.

Rabinovitch, R. (2004). Universal Jurisdiction In Abstentia. Fordham International Law Journal , 500-530.

Rid, T. and Buchanan, B. (2014). Attributing Cyber Attacks, Journal of Strategic Studies, 38(1-2), pp.4-37.

Roscini, M, (2014). Cyber Operations as a Use of Force .Nicholas Tsagourias and Russell Buchan (eds.), Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, 2015, 233-254, U. of Westminster School of Law Research Paper No. 16-05.

Schmitt, M (ed.) (2013). Tallinn manual on the international law applicable to cyber warfare, Cambridge University Press, Cambridge.

Tikk, E Kaska, K & Vihul L (eds.) (2010). International cyber incidents: legal considerations, NATO CCD COE Publications, Tallinn

Tsarougias, N. (2012). Cyber attacks, self-defense and the problem of attribution, Journal of Conflict & Security Law, vol. 17, no. 2, pp. 229-44.

Von Heinegg W. (2012). Legal implications of territorial sovereignty in cyberspace, Proceedings of the 2012 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn.

Woods, A. K.. (2018). Litigating Data Sovereignty, Yale Law Journal, 128(2):328-406

Wu, T. (1997). Cyberspace sovereignty?, the internet and the international system, Harvard Journal of Law & Technology, vol. 10, no. 3, pp. 647-66.

Zeng, J., et.al. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty", Politics and Policy, 45(3):432-464.

ULİSA12, Ankara Yıldırım Beyazıt Üniversitesi Uluslararası İlişkiler ve Stratejik Araştırmalar (ULİSA) Enstitüsü'nün aylık politika notu yayınıdır. Her konu bir sayı editörü rehberliğinde ele alınmaktadır. Yazarların görüşleri kendilerini bağlar. Ankara Yıldırım Beyazıt Üniversitesi ve ULİSA yazarların görüşlerinden dolayı sorumlu tutulamaz.

Adres: Güvenevler Mah.
Cinnah Cad. No: 16
Çankaya/ANKARA
Tel : 0(312)906-1313
e-posta : ulisa@ybu.edu.tr
Web Sayfası : www.ybu.edu.tr/ulisa/