Bölüm 9

Elektronik Sivil İtaatsizlik Bağlamında Hacktivizmin Meşruluğu Üzerine

Özlem Çetin Öztürk[1]

Özet

Dijital araçların politikayı etkileme ve protestonun araçları olarak kullanılmasıyla birlikte kolektif eylemler için aktivistlerin eylem repertuarı dönüşmeye başlamıştır. Hack de aktivistlerin kullandığı eylem türlerinden biri olarak karşımıza çıkmaktadır. Politik bir motivasyonla hacki aktivist bir taktik olarak kullanmaya dayanan eylem biçimleri hacktivizm olarak nitelendirilmektedir. Ancak hack fiilinin yasal sınırları aşması nedeniyle hacktivzmin meşruluğunun ne olduğu ve hangi bağlamlarda kabul edilebilir bir aktivizm olarak kavranabileceği tartışmalıdır. Hacktivizmin meşruluğu bağlamında yürütülen çalışmaların bir kısmı hacktivizmin sivil itaatsizlik kavramıyla olan ilişkisini ortaya koymaktadır. Sivil itaatsizliğin yasaya politik ve sosyal bir nedenle bilerek uymamaya dayanan bir eylem türü olması; hackin yasadışı alana taşan yanının da dijital sistemlere izin giriş yasağına itaatsizlik şeklinde ele alınabileceğini gündeme getirmektedir. Bu durum, hacktivizmin politik bir motivasyona sahip bir hack eylemi olarak, elektronik sivil itaatsizlik olarak kavramsallaştırmasını beraberinde getirmiştir. Çalışmanın kapsamında hacktivizmin hangi bağlamda elektronik sivil itaatsizlik biçimi olarak kavranıp kavranamayacağı ve elektronik sivili itaatsizlik olarak meşruluğunu sorgulanmaktadır. Bu doğrultuda öncelikle hacktivizmin kavramsal olarak nasıl ele alındığı tarihsel örnekleriyle ele alınmakta ve sonrasında sivil itaatsizliğin nasıl teorize edildiğine meşruiyeti bağlamında tartışılmaktadır. Son olarak ise elektronik sivil itaatsizlik kavramı ve hacktivizmi meşru bir zeminde değerlendirmenin sınırları ortaya konmaktadır. Kavramsal olarak çalışma, meşru bir zeminde sivil itaatsizliğin sanal uzama taşınması olarak hacktivizmin, elektronik sivil itaatsizlik olarak ele alınmasının gerektiği savlamaktadır.

1 Dr. Öğretim Üyesi, İstanbul Gelişim Üniversitesi, İİSBF, Yeni Medya ve İletişim Bölümü, ozcetin@gelisim.edu.tr Orcid:0000-0002-4155-3352

https://doi.org/10.58830/ozgur.pub135.c742

1. Giriş

Dijital iletişim teknolojilerinin küresel düzeyde yaygın kullanılmaya başlamasıyla birlikte sanal uzamın politik olana açılması ve politik düzlemin bir parçası olarak işlemesi yeni aktivizm pratiklerini beraberinde getirmiştir. Sanal uzamda dijital teknolojiler kullanılarak ortaya çıkan aktivizm biçimleri, dijital aktivizm olarak nitelendirilmektedir. May Joyce'un da belirtiği gibi, dijital aktivizm denince akılda canlanan olgu, dijital teknolojiyi kullanan sosyal veya siyasi değişim hedefleyen aktivizm kampanyalarının tümünü kapsamaktadır. Dolayısıyla hem aktivistlerin kullandığı dijital teknolojiyi hem de bu kullanım sonucunda ortaya çıkan ekonomik, toplumsal ve politik bağlamı nitelendirmektedir (Joyce, 2010, 2,7). Bugün baktığımızda hashtag aktivizmi, kültür bozumu, elektronik imza kampanyaları gibi doğrudan sanal uzamın kolektif eylem alanına dönüştüğü aktivizm biçimlerini ve aynı zamanda tüm sosyal ve politik grupların reel hayattaki örgütlü yapılarını ve eylemlerini destekleyen sanal uzamdaki iletişim çabalarını görmekteyiz. Bir yandan dijital araçların reel hayattaki eylemler için kullanılması diğer yandan da sanal uzamın kendisinin eylem alanı olarak kullanılması söz konusudur. Dijital aktivizm, en genel anlamda reel politikayı etkileme ve dönüştürme amacıyla siber ortamda dijital iletişim kanalları kullanarak yapılan her türlü eylemselliği içermektedir. Bu bağlamda, politik ve sosyal motivasyona sahip tüm toplumsal aktörlerin hem dijital araçları motivasyonlarına uygun olarak kullanmaları hem de dijital uzamın kendisini doğrudan eylem alanı olarak kullanmaları söz konusudur. Dijital uzamın kendisini doğrudan eylem alanı olarak kullanan aktivizm biçimlerinden biri de hacktivizmdir.

Hacktivizm, en yalın anlamda hack ile aktivizmin birleşmesini ifade etmektedir (Denning, 2008, 407). Aktivizm artık somut olarak bireylerin sokaktaki eylemlere katılmasından ibaret değildir; "*zihinlerin ve sanal bedenleri çevrimiçi hale getirmeyi gerektiriyor. Hacktivizmin vaadi budur; aktivistin siyasi bilincinin hackerların teknik uzmanlığıyla birleşmesidir*" (Goodrum, Manion, 2000, 18). Dolayısıyla hacktivizm, sosyal ve siyasi amaçlarla aktivist bir araç olarak hackin kullanılmasını ifade etmektedir. Hackin siyasi amaçla kullanılması ise; hedeflenen siteye politik mesaj yerleştirme, sanal oturma eylemi, hizmet aksatma (Denial of Service) saldırıları, e-posta bombardımanı, bilgi sızdırma, web sitelerinin içeriklerinin değiştirilmesi, web sitesi yönlendirmeleri, web sitesine zarar verme, virüsler ve solucanlar, sanal sabotaj ve yazılım geliştirme gibi hackerların yaratıcılığına ve siyasi amaca yönelik olarak farklı eylemler şeklinde karşımıza çıkmaktadır (Baldi, vd., 2003, 24; Denning 2001; Samuel, 2004, 6). Hacktivistler, hedefleri ve istedikleri etkiyle ilişkili olarak farklı eylem biçimlerine başvurabilir veya yenilerini geliştirebilirler.

Hackleme yönteminden ziyade, herhangi bir hacki hacktivist eylemden ayırt edebilmek için odaklanılması gereken nokta, eylemin politik motivasyonudur. Hacktivizm diğer hackleme biçimlerinden, "*adaletsizliği protesto etmek gibi övgüye değer bir arzuyla*" politik olarak motive edilmesi bakımından ayrılır. Dolayısıyla hacktivizm, hackin aktivist bir amaçla "*siyasi veya ahlaki bir duruşu ifade etmek amacıyla izinsiz dijital müdahalede bulunma*" olarak tanımlanabilmektedir (Himma,2008, 200). Öte yandan, hacktivizm politik olarak motive olmuş bir eylem türü olarak "*yasadışı veya yasal olarak belirsiz dijital araçların siyasi amaçlar için şiddet içermeyen kullanımı olarak*" kavranmakta ve "h*acktivistler, kendi görüşlerini duyurmak ve yaymak için çok çeşitli erişim noktalarından*" yararlanmaktadırlar (Hampson, 2012; 514-515). Ancak bu bağlamda hackin *yasadışı veya yasal olarak belirsiz* konumu hacktivizmin meşruluğu sorunsalını ortaya çıkarmaktadır. Hackin kriminal yanı, hacktivizmi diğer tüm dijital aktivizm biçimlerinden farklı bir zeminde tartışılmasını beraberinde getirmektedir.

Bu bağlamda hacktivizmin, yasanın politik bir duruşla çiğnenmesini ifade eden sivil itaatsizlik kapsamında değerlendirilmesi söz konusudur: Sivil itaatsizlik, yasaya 'iyi bir nedenle' itaatsizlik etmek anlamına gelmektedir (Bedau, 1991, 8). Bu doğrultuda hacktivizm, "*çevrimiçi protestoları kolaylaştırmak, siber uzamda sivil itaatsizlik gerçekleştirmek ve küresel sermayenin ağlarına kasıtlı olarak müdahale ederek bilgi akışını bozmak amacıyla bilgisayar teknolojisinin yaratıcı bir şekilde kullanılmasına dayanmaktadır*" (Gunkel, 2005, 595). Motivasyonu yok sayılarak hack'in hukuken bir yasa ihlali olması nedeniyle, hacktivizmin geneleneksel sivil itaatsizlikle var olan bağını ve siber uzamda yeniden yaratılma biçimini vurgulamak için elektronik sivil itaatsizlik kavramı kullanılmaktadır (Denning, 2001, 2008; Gunkel, 2005; Himma, 2008; Jordan, Taylor, 2004; Manion, Goodrum, 2000; Wray, 1998). Elektronik sivil itaatsizlik kavramsallaştırmayla birlikte hacktivizmin meşru sayılmasının sınırlarının neler olduğu ve aktivizm açısından taşıdığı potansiyelin kapsamı ortaya konmaktadır.

Bu çalışma, hackin suç olarak kavranmasına karşın, hacktivizm kapsamında hackin meşru sınırlarını elektronik sivil itaatsizlik kavramı bağlamında tartışmayı amaçlamaktadır. Bu doğrultuda, hacktivizmin kavramsallaştırılması erken örnekleriyle de ilişkili olduğundan öncelikle hacktivizmin kısa tarihine ve kavramın hangi bağlamlarda tartışıldığına değineceğiz. Sonrasında ise sivil itaatsizliği kavramsal olarak açıklayarak; son bölümde de hacktivizmin elektronik sivil itaatsizlik olarak meşruiyetini sorgulayacağız.

2. Hacktivizm kavramsallaşması ve kısa tarihi

Hack, aktivizm amacıyla kullanılmadan önce ortaya çıkışı, aslında süregidene bir meydan okuma olarak yorumlanabilir. Zira hack öncelikle Massachusetts Institute of Technology'de (MIT) jargonunda öğrencilerin birbirine yaptıkları alışılmadık, yaratıcı ve sınırları zorlayan şakaları nitelendirmek için kullanılmaktayken; yine MIT'de, ancak bu kez bilgisayar laboratuvarlarında, hack bilgisayar sistemlerdeki sorunları çözmek için öğrencilerin buldukları olağandışı ve orijinal çıkış yollarını niteleyen bir anlama ulaşmıştı (Leibowitz, 2011, 5). Hack 1950'lerde, önce MIT, ardından Cornell ve Harvard üniversitelerindeki bilgisayar laboratuvarlarında teknoloji meraklısı öğrencilerin sistemlerdeki açıkları bulup daha kısa daha akılcı kodlar yazarak birbirlerine meydan okudukları; yazılım ve işletim sistemlerinin yaratılma amaçlarının çok ötesine geçmesini sağlayan yaratıcı çözümleri kapsayan bir anlama ulaştı. (Thomas, 2002; Graham, 2004; Levy, 2010). Dolayısıyla hack kavramı kampüste çatıya araba çıkarmak gibi sınırları zorlayıcı şakalardan (Williams, 2002, 151) kodlarda sınırları zorlamaya doğru evrilmiştir. Ancak hacktivizm kavramıyla birlikte hem kodların hem de politik söylemin sınırlarının zorlanması söz konusu olmaya başlamıştır.

Hackin aktivizm ile buluşmasını nitelendirmek için hacktivizm terimi ise ilk olarak dijital sanatın eleştirel yanını vurgulamak için 1995'te Jason Sack tarafından kullanılmıştır (Palmas, von Busch, 2015, 229). Sack'in Jason Logan mahlasıyla *InfoNation* isimli dergide *The Virtual Underground* başlıklı makalede, Shu Lea Cheang'in ekolojik sorunları eleştirel bir bakış açısıyla yansıttığı Fresh Kill (1994) filmini ve Bowling Alley (1995-1996) adını verdiği enstalasyon projesini kaleme almaktadır. Sack, makalesinde, kodu eserlerinde sanatsal bir araç olarak kullanan Cheang'İn andığımız çalışmalarını, hacktivizm olarak nitelendirir. Sack, hactivizm kelimesini; kodun kültürel kullanımın estetik, sosyal ve politik bir eleştiri amacıyla kullanılmasını açıklamak için kullanmıştır (Marino, 2014, 66). Dolayısıyla hacktivizm ilk kez, dijital sanat eserlerindeki eleştirel bakış açısını yansıtan ve sanatın konvansiyonel yollarını ters yüz eden bir anlamda, handiyse sanatı hacklemek anlamında kullanılmıştır.

Ancak hacktivizm terimi bu ilk kullanımının ötesinde politik doğrudan eylem biçimi olarak kavranmaktadır. Paul Taylor ve Tim Jordan, hacktivizmi, politik konumu ve söylemi belli olan, açık bir politik duruşla politik protestonun hack ile birleşimi olarak tanımlamaktadır (Jordan ve Taylor, 2004, 11; Taylor, 2005). Hacktivizmi, hack'in siyasi amaçlar doğrultusunda yasadışı veya yasal olarak dijital araçların şiddet içermeyen kullanımı olarak kavramak mümkündür (Samuel, 2004). Dorothy E. Denning, bu dijital araçların kul-

lanımını ise "*bilgisayarları alışılmadık ve genellikle yasadışı yollarla, tipik olarak özel yazılımlar yardımıyla kullanan operasyonlar*" (Denning, 2001, 15) Hacktivizmi kavramsal olarak nitelendirmek için ortaya konan yaklaşımlar genel olarak hacktivizmin ilk örnekleri üzerine duyulan bir gereklilikle; ancak ilk örneklerinden tarihsel olarak daha geç yapıldı. Zira hacktivizm bir politik eylem biçimi olarak kavramsallaştırılmadan çok daha önce ilk hacktivist eylem örnekleri yaşandı.

2.1. Dijital Politikalara İlişkin Hacktivizm

Literatürde ilk hacktivist eylem olarak farklı kabuller söz konusu olmakla birlikte bilinen en eski hacktivist eylem doğrudan politik bir amaç taşıyarak hacklemeye başlayan Chaos Computer Club'un (CCC / Kaos Bilgisayar Kulübü) eylemleri olarak değerlendirmek mümkündür. CCC, Almanya'da 1981 yılında Herwart Holland Moritz tarafından, World Wide Web'in ortaya çıkmasından ve kişisel bilgisayarların yaygınlaşmasından önce ve dolayısıyla internetin yaygın kullanımının henüz söz konusu olmadığı bir dönemde bir araya gelen hackerlarca 1986'da kâr amacı gütmeyen yasal bir organizasyon olarak kurulmuştur. Bu kurumsallaşmış zeminde ortaya çıkması, hem onu diğer hacktivist gruplardan ayırmakta hem de hacktivist bir oluşumun öncüsü kılmaktadır (Kubitschko,2018, 84; Mungo, Glough, 1993, 79). Bu nedenle CCC'i ilk hacktivist grup olarak kabul etmek ve ilk eylemlerini de ilk hacktivizm örnekleri olarak değerlenmek oldukça makuldür. Enformasyon toplumu teorilerinin popülerliğinin arttığı o dönemde, enformasyon toplumu için kaçınılmaz olan temel kriterin, dünya çapında enformasyon özgürlüğünün ve özgür iletişimin yeni insan hakkı olarak görülmesi olduğunu savunarak bir araya gelen grup (Jordan, Taylor, 2004, 14), günümüzde de aynı temel argümanla yasal sınırlar içerisinde kalarak faaliyetlerini sürdüren Avrupa genelinde bilinen en fazla üyeye sahip, Almanya'da siyasi partilere üyeleri tarafından danışmanlık verilen, Alman Anayasa Mahkemesi için bilirkişi raporları hazırlayan, hükümet komitelerine davet edilen, dijital haklar mücadelesini sürdüren yasal bir organizasyondur (Kubitschko,2018, 84). CCC'nin adını ilk duyurduğu eylemi, 1984'te telefon aracılığıyla anabilgisayara bağlanılabilen bir dijital ekran olan Bildschirmtext'i (Btx) güvenlik açıklarını göstermek için hacklemelesidir. Daha sonra, hükümet sistemlerini hackleyerek 1986'daki Çernobil felaketine ilişkin verileri yayınlamalarıyla medyanın ilgisini çekmeyi başararak daha fazla tanınır hale geldi. CCC'nin hacki kamuoyu gündemine taşıyan bu eylemleri, literatürde rastlanan en eski hacktivist eylem örnekleri olarak bilinmektedir. (Mungo, Glough, 1993, 79-80).

CCC, ilk eylemlerinden bu yana enformasyon özgürlüğü, sistem güvenliği ve kamusal şeffaflık vurgusuyla sistem açıklarını bulmak üzerine yoğunlaşmaktadır. CCC'nin kurumsallaşmış yapısı, enformasyon özgürlüğü için ortaya koyduğu duruş ve yasal sınırlar içerisindeki meşru yapısı günümüzde de bu hacktivist grubu, çoğu hacktivist gruptan ayıran önemli özellikleri olarak karşımıza çıkmaktadır. Ancak reel hayattaki kolektif eylemlerle ilişkisi oldukça sınırlı olmakla beraber dijital dünyanın kendisine yönelik politikalara ilişkin çabaları söz konusudur.

Benzer şekilde enformasyon özgürlüğünü temel bir insan hakkı olarak ele alan hacktivist grupların erken bir başka örneği de 1984'te kurulan Cult of The Dead Cow'dur (CDC / Ölü İnek Kültü). CDC, yazılımın ticarileşmesine karşı çıkarak kullanıcılar için sistem güvenliğinin önemini göstermeyi amaçladığı Back Orifice (BO) projesiyle ve enformasyonun koşulsuz özgür olması gerektiğini savunduğu *Hactivismo* bildirisiyle tanınmıştır (Klaus 1999; Thomas 2002; Jordan, 2002). BO ve sonrasında güncellenen sürümü BO2k, Windows 95 ve 98 işletim sistemine erişebilen bir backdoor (arka kapı) programıydı (Klaus, 1999). Bilişim dünyasında backdoor, üçüncü tarafların yazılım ve donanımlarını kullanmasına neden olan çok ciddi bir sorun olarak görülmektedir (Thomas, Francillon, 2018, 92). BO'nun Windows işletim sisteminde üçüncü taraf olarak çalışması, Windows'un çok önemli güvenlik açığına sahip olduğunu ortaya çıkardı. CDC bu eylemiyle, Microsoft'un kullanıcı mahremiyetini hiçe sayan, yüksek ücretlerle sattığı işletim sistemini hacklerken aslında genel olarak bilişim dünyasının hızla kapitalistleşen yapısını eleştirmekteydi. CDC'nin amacı daha güvenli ve kodları saklanmayan kullanıcılarının nasıl çalıştığını bilmelerini mümkün kılan işletim sistemlerinin yaratılması gerektiğini vurgulamaktı (Thomas, 2002, 98-100). Bu bağlamda CDC, bilişim dünyasının ticarileşmesine karşı çıkan açık kaynak/ özgür yazılım hackerlarının benimsediği fikirleri hacktivizmin meselesi haline getirmekteydi.

CDC, politik ve etik açıdan hacktivizmin, evrensel insan hakları bağlamında enformasyon özgürlüğünü savunması yönündeki görüşlerini açıkladığı *Hacktivismo Declaration*'ı (Hacktivismo Bildirisi, 2001) yayınladı. Bildiride, internet sansürü ve internetin sınırlandırılmasının, baskıcı rejimlerin kendilerine sorun yaratacağını düşündükleri, muhalif içerikli enformasyonları engellenmek amacıyla uyguladıklarını vurgulayarak; bu uygulamalara, insan hakkı olan enformasyona erişim özgürlüğünün engellenmesi olarak gördüklerini için karşı çıktıkları beyan edilir.[2]

2 Hacktivismo Declaration, Cult of the Dead Cow (04 Temmuz 2001), "International Bookburning In Progress", http://www.cultdeadcow.com/cDc_files/declaration.html

Hem CCC hem CDC'nin sistem açıklarını bulmak üzerine odaklandıkları, bilişim dünyasının hızla ticarileşen yapısını eleştirerek özgür bir dijital dünya için enformasyon özgürlüğünü insan hakkı olarak savundukları ve hacki dijital dünyanın kendi iç politikalarına ilişkin olarak politik bir amaçla kullandıkları görülmektedir. Jordan ve Taylor (2004), hacktivistlerin dijital haklar çerçevesinde enformasyon özgürlüğü temelinde şekillenen eylem ve çabalarını "*dijital olarak doğru hacktivizm*" olarak kategorize etmektedirler. Jordan ve Taylor'ın ortaya koyduğu dijital olarak doğru hacktivizm tanımlaması, CDC'nin ve CCC'nin yaklaşımlarında olduğu gibi, herkesin enformasyon özgürlüğü hakkına odaklanmaktadır. İkiliye göre, dijital olarak doğru hacktivizm, enformasyonun sınırlandırılması veya engellenmesinin kabul edilemez olduğunu ve aynı zamanda kişisel veri mahiyetindeki enformasyonun korunması gerektiğini hack aracılığıyla politik bir söyleme dönüştürmektedir. Dijital olarak doğru hacktivizmin mücadelesi, şirketlerin ve hükümetlerin interneti gözetim ve sansür mekanizması olarak kullanmalarına karşı, internette enformasyona güvenli erişimi sağlama amacı taşır. Dijital politikaların özgürlük ve güvenlik temelinde şekillenmesi için mücadele eden hacktivistler hem hackten hem de farklı yazılım türlerinden yararlanırlar (Jordan, Taylor, 2004, 98-114). İnterneti özgürlükçü bir uzam olarak yaratma mücadelesinde, hack çoğunlukla güvenlik açıklarına dikkat çekmek için kullanılırken farklı yazılım türleri de enformasyon erişiminin kesintisiz sağlanmasına yönelik geliştirilir. Bu nedenle de Jordan, dijital olarak doğru hacktivizmin enformasyona güvenli erişimi saylayacak internet altyapısının yaratılması için mücadele ettiğini ve böylelikle de dijital uzamda enformasyon özgürlüğünün hacktivizmin özel politikası olarak benimsendiğini belirtir (Jordan, 2007, 79-80). Dolayısıyla dijital ekosistemi yöneten ekonomi politik yapıya yönelik bir mücadele söz konusudur. Buradaki mücadeleden, kullanıcıların verilerinin dijital ekonominin bel kemiği haline geldiği ve Shoshana Zuboff'un nitelendirmesiyle kullanıcıların hammadde arz kaynağı olarak konumlandırıldığı gözetim kapitalizmin (Zuboff, 2019) bizzati kendisine yönelik antikapitalist bir vurgu olarak bahsedebiliriz.

2.2. Kolektif Eylemlere İlişkin Hacktivizm

Hacktivizm yukarıda andığımız üzere sadece dijital politikalar üzerine yoğunlaşarak şekillenmemiştir. Doğrudan kolektif eylemlere destek vermek amacıyla reel politikayı etkilemeye yönelik olarak da şekillenmiştir. Bu bağlamda ise Jordon ve Taylor'ın yaptığı ikinci hacktivizm kategorisi olan; hackin somut bir şekilde kitlesel bir eylem şeklinde yapıldığı ve reel kolektif eylem biçimleriyle doğrudan ilişkili olan kitlesel eylem hacktivizminde somutlaşmaktadır (Jordan, Taylor, 2004). Hackin reel hayyataki aktivizm

biçimlerine eklemlendiği bu hactivizm biçimin hacktivizm biçiminin ilk örneklerinden biri ise Wikileaks'in kurucusu Jullian Assage'ın en eski hacktivist eylem olarak gördüğü 1989'daki WANK solucanı (Worms Against Nuclear Killers / Nükleer Katillere Karşı Solucanlar) ile karşımıza çıkmaktadır (Assange, 2006). WANK solucanı, NASA'nın nükleer karşıtı gruplar tarafından protesto edildiği sırada, ABD Enerji Bakanlığı ve NASA SPAN sistemine saldırdı. WANK solucanıyla işgal edilen bilgisayarların giriş sayfasına "*Nükleer Katillere Karşı Solucanlar. Sisteminiz resmi olarak WANKlenmistir. Herkes için barış zamanlarından bahsediyorsunuz, sonra savaşa hazırlanıyorsunuz.*" şeklinde mesajlar yerleştirilmişti (Nazario, 2004, 42-43; Assange ve Dreyfus, 2001, 19-20, 25-26). Avustralyalı hackerlar bu solucanla, ABD'de meydanlarda düzenlenen nükleer karşıtı protestolarda döviz taşımak yerine sokaktaki aktivistlerin politik mesajlarını işgal ettikleri bilgisayarlara yaydılar (Friedman, Singer, 2014, 77).

Benzer şekilde reel hayattaki kolektif eylemlere destek olmak için yapılan hacktivist eylemlerin ilk örneklerinden bir başkası da Electronic Disturbance Theatre (EDT / Elektronik Rahatsızlık Tiyatrosu) adında üyeleri anonim olmayan hacktivist grubun 1998'de, NAFTA'nın (Kuzey Amerika Serbest Ticaret Anlaşması) neoliberal politikalarıyla mücadele eden Meksika'daki Zapatista hareketini desteklemek amacıyla gerçekleştirdiği eylemlerdi. EDT, Zapatista hareketine dikkat çekmek amacıyla NAFTA'ya taraf olan ve destekleyen ülkelerin resmi bazı kurumlarını hacklemek için FloodNet ismini verdikleri bir yazılım geliştirdiler. FloodNet, hedeflenen Meksika Cumhurbaşkanlığı, Frankfurt Menkul Kıymetler Borsası ve Pentagon'un sitelerine otomatik sayfa yenilenmesi komutu yolluyor ve böylelikle sunucuları yavaşlatarak siteye erişimi engelleniyordu. Bu eylem için katılımcıların FloodNet'i tarayıcılarında kendilerinin açmaları gerekiyordu (Stalbaum, 1998). Ancak katılımcı sayısının artmasıyla engellenebilen sitelerde *'bu servis sağlayıcıda insan haklan bulunamamıştır', 'bu servis sağlayıcıda demokrasi bulunamamıştır'* gibi mesajlar uyarı pencerelerinde çıkıyordu (Jordan, 2002, 120-121). EDT eylemleri; kolektif katılım, açık kaynak ve e-mail, javascipt gibi temel teknolojilerin yaratıcı bir buluşmasını ortaya koyan network art aktivizminin örnekleri olarak da kabul edilmekteyken (Lane, Domingueez, 2003, 131); FloodNet, botlar yerine gerçek katılımcılara sahip olan ilk sanal oturma eylemi ve ilk elektronik sivil itaatsizlik eylemi olarak kabul edilmektedir. (Wray,1999; Samuel, 2004, 130).

Kitlesel eylem hacktivzminin bir başka öncü örneği de 1999'da Seattle'daki küreselleşme karşıtı Dünya Ticaret Örgütü (DTÖ /WTO) protestoları sırasında, çevrimiçi protestolarda hackin kullanılmasıydı. Britanya'daki

Electrohippies Collective (E-hippies / E-hippiler) isimli hacktivist grup, hem WTO uzantılı mail adreslerine mail bombardımanı hem de FloodNet'e benzer ancak amacı siteyi yavaşlatmak değil sitenin işlevini tamamen durdurmak olan DDoS DDoS (Distributed Denial of Service/ Dağıtık Hizmet Reddi Saldırıları) saldırısında bulunan bir yazlım geliştirdi (Jordan, Taylor, 2004, 41; Jordan, 2002, 123). "WTO virtual sit-in" olarak isimlendirdikleri DDoS için zombi makineler kullanmıyorlar ve zombiler olmadan eylemin bunları gerçekleştirmeye istekli olanlar tarafından desteklenmesi gerekiyordu (Klang, 2004, 142). Katılımcıların saldırının gerçekleşmesi için yazılımı kendi bilgisayarlarına kurmaları gerekiyordu (Sauter, 2014, 40). Kitlesel bir katılım olmaksızın başarıya ulaşması olanaksız olan bu eylem ile sitenin işlevi durdurulması başarılmıştı.

Yukarıda örneklerini sıraladığımız Jordon ve Taylor'ın kitlesel eylem hacktivizmi olarak nitelendirdikleri eylem biçimlerinde hacktivizm, sokaktaki reel kitlesel eylemlerin bir uzantısı olarak sanal alanda hacktivistlerin yazdığı programlar kullanılarak ama yine ve mutlaka kitlesel katılım yoluyla gerçekleşmektedir. Kitlesel eylem hacktivizmi siyasetin ve sistem açıklarının birleşiminden oluşmaktadır. İkiliye göre, kitlesel eylem hacktivizmi hem istenilen sonuca en hızlı şekilde ulaşmayı hedefleyen boykot, grev, sivil itaatsizlik gibi reel hayattaki doğrudan eylemi hem de istenilen politik talep ve sosyal değişim konusunda insanları etkileme amacındaki reel hayattaki sembolik eylemin kombinasyonudur. Kitlesel eylem hacktivizminin temel amacının ise sivil itaatsizliği sanal alanda yeniden yaratmak olduğunu ve bu özelliği ile hacktivizmin diğer tüm eylem biçimlerinden ayrılmakta olduğunu vurgularlar (Jordan, Taylor, 2004, 68-69, 79, 81). Jordon, programlar aracılığıyla kitlesel olarak katılımın söz konusu olmasının hacktivist eyleme meşruluk kazandıran bir özellik olarak nitelendirmektedir (Jordan, 2002, 125; 2007, 75, 78). Ancak hem WANK solucanı örneğinde olduğu gibi hem de günümüzde Anonymous gibi hacktivist grupların eylemlerinde gördüğümüz örneklerde, eyleme kolektif bir katılım söz konusu değilken reeldeki kolektif eyleme verilen destek hacktivist eylemin temel özelliği olarak belirginleşmektedir. Bu özelliğiyle, özlüce eyleme kolekif katılım olsun ya da olmasın reel hayattaki kolektif eylemlerle ilişkisi bakımından kitlesel eylem hacktivizmi dijital olarak doğru hacktivizmden ayırmak daha yerinde görünmektedir. Ancak meşruluk sorunu kitlesel katılımın olmadığı bir hacktivist eylemde daha güçlü şekilde tartışmalı olacağı da açıktır. Hackin suçla olan ilişkisi ise diğer dijital aktivizm biçimlerinden oldukça uç bir noktada hacktivizmi meşruluk sorununa taşımaktadır. Bu bağlamda hacktivizmin sivil itaatsizlik olarak kavranıp kavranamayacağı önem taşımaktadır. Hacktivizmin meşruluğuna ilişkin açıklamalar sivil itaatsizlik kavramı ile açıklanmaktadır. Bu nedenle

öncelikle sivil itaatsizlik kavramına kısaca yer vererek; sonrasında elektronik sivil itaatsizlik biçimi olarak hacktivizm tanımlamalarını açıklayacağız.

3. Sivil İtaatsizlik

Sivil itaatsizlik, en yalın anlamıyla protesto amacıyla yasalara karşı gelmeyi ifade etmektedir. Belirli yasalara karşı meydan okuma niteliğine sahip olsa da suç işleme fiilinde ve isyandan ayrılmaktadır. Aynı zamanda kamusal, şiddet içermeyen, vicdanlı ve sınırlı eylemlerle, protestocular haksız yasalara, ayrımcı politikalara veya yaygın hak ihlallerine dikkat çekme amacıyla gerçekleşmektedir. John Rawls'un ifadesiyle sivil itaatsizlikte bulunan eylemci/ler "*yasa sadakati sınırları içinde*" kalma isteğini ifade etmektedir (Pineda, 2021, 5-6). Burada ortaya çıkan ayrım, yasanın ihlal edilirken yasanın ve yasa koyucunun varlığının kabul edilerek (– ki isyandan ayrılan yanı bu noktada siyasi sisteminin kabulü ile ortaya çıkmaktadır) politik bir söylem ve amaçla kamusal bir görünürlük içerecek şekilde çiğnenmesidir. Sivil itaatsizlik kavramı H. Adam Bedau'un deyimiyle "*iyi bir amaç için kanuna karşı gelmek*" olarak kavrandığında, "*Prometheus'un insanlara ateşi vermek için Zeus'a karşı gelmesi kadar eski*" bir geleneğe sahiptir (Bedau, 1991, 8). Ancak kavramın günümüzdeki siyasal aktivist bir taktik olarak kullanımının kökeni Henry David Thoreau'nun yaşadığı bir olayın sonucunda yaptığı kavramlaştırmaya dayanmaktadır. Thoreau'nun, ABD hükümetinin köleliği desteklemesi ve Meksika ile savaşını protesto etmek amacıyla zorunlu oy vergisini ödemeyi reddederek bir gece hapis cezasını kabul etmesine dayanmaktadır (Alton, 1992, 40-42). Bu olay sonrasında kaleme aldığı Sivil İtaatsizlik (On the Duty of Civil Disobedience) eserinde [3] Thoreau (2013) şöyle demektedir:

> Adaletsiz yasalar var: bunlara uymalı mıyız yoksa değiştirmek için çaba mı göstermeliyiz? Ya da yasa değişene kadar uymalı mıyız yoksa bir defada çiğneyip geçmeli miyiz? İnsanlar genellikle, böyle yönetimler varken, değişim için çoğunluğun ikna olması gerektiğini düşünür. Eğer tek başlarına direnişe kalkarlarsa, durumun daha kötü olacağını düşünürler. Ama durumun giderek kötüleşmesi, yönetimin suçudur. Reformu anlamak ve buna zemin hazırlamak daha uygun değil midir? Neden yönetimler çözüm sunan azınlığı[4] dikkate almazlar? (21) […] Eğer adaletsizlik, yönetim makinasında gereken sürtünmeyi yaratan parça ise, atın gitsin, atın gitsin: İşleyiş pürüzsüz olacak ve zaten makinaya hacet kalmayacaktır.. Adaletsizliğin kendi yayı, ipi, kasnağı

3 Thoreau'nun ilgili eseri *Resistance to Civil Government* ve *Civil Disobedience*, isimleriyle de basılmış; Türkçeye Sivil İtaatsizlik olarak kazandırılmıştır.

4 Thoreau, metnin orjinalinde 'wise minority' (*Eng*.) 'bilge azınlık'ifadesini kullanmaktadır: "*Why does it not cherish its wise minority?*" (Thoreau,1991:35) ifadesini kullanmaktadır.

> veya levyesi var ise, o zaman sonuçların çok da kötü olmayacağını düşünebilirsiniz; ama eğer bunların işlemesi için size ihtiyacı varsa, yani siz bir başkasına adaletsizlik getirecekseniz, o halde derim ki, o yasayı çiğnemelisiniz. Bırakın hayatınız işleyen makinayı durduracak karşı kuvvet olsun (22).

Thoreau'ya göre yasaya itaatsizlik hükümetin yanlış/haksız uygulamalarına yönelik "*bilge azınlığın*" uyarısının dikkate alınmamasına ve iktidarın adetsizliğine ortak olmaya karşı bir itiraz olarak kavramak mümkündür. Dolayısıyla sivil itaatsizlik, iktidarın yanlış uygulamalarına destek olmayı reddetmek için yasa ihlalini meşrulaştıran ve hatta gerekli gören bir noktadır. Thoreau'nun sivill itaatsizliği kavramsallaştırması var olan siyasi düzeleme bağlı kalan bireysel bir itiraz olarak karşımıza çıkmaktadır. Zira Stephen R. Alton'un da belirttiği gibi Thoreau oldukça "*bireyci ve özgürlükçü*" dür (Alton, 1992, 41); Thoreua'nun anarşizme varan çağrıları aslında yeni bir hükümet isteğinin ötesinde değildir ve Thoreau, "*hükümet karşıtı*" olmaktan kendisini ayırt ederek, "*hemen daha iyi bir hükümet*" talep eder (Alton, 1992, 42). H. Adam Bedau'ya göre, Thoreau'nun yazılarında sivil itaatsizliğin meşrulaştırılması ve bilimsel teorik bir zeminde kavramsallaştırması söz konusu değildir (Bedau, 1991, 10). Benzer bir durumu Hannah Arendt de Thoreau'nun sivil itaatsizliği ele alış biçimini, adaletsizliğe ortak olmama üzerinden bireysel vicdani bir itiraz olarak nitelendirir; ancak Arendt'e göre, vicdan apolitiktir (Arendt, 1972, 60). Bu yüzden Thoreau'nun sivil itaatsizliği bireysel vicdani bir reddediş ile suça ortak olmama temelinde, teorik değil olgusal olarak ele aldığı ortaya çıkmaktadır.

Arendt'in sivil itaatsizlik kavramsallaştırmasında ise eylemcinin genellikle bir grubun politik iradesine uygun olarak alenen yasayı çiğnemesi söz konusudur (Arendt, 1972, 76). Dolayısıyla, Arendt'te bireysel bir irade değil belli bir grubun politik itirazının yansıması söz konusudur. Ona göre sivil itaatsiz eylemi herhangi bir suçtan ayıran en önemli yan, gizli değil alenen kamusal alanda herkesin gözü önünde bir yasanın ihlalinin gerçekleşmesidir (Arendt, 1972, 75). Bu durumda kamusal görünürlük içerisinde yasa ihlali sivil itaatsizliğe meşruiyetini kazandırır. Arendt'in sivil itaatsizliğin meşruiyeti için vurguladığı bir diğer unsur ise sivil itaatsizliğin şiddet içermemesi ve barışçıl yolları kullanmasıdır. Ancak Arendt'e göre barışçıl yolları kullanmanın ve var olan siyasi sisteme bağlı olmanın, sivil itaatsizliğin var olan iktidar biçiminin meşruiyetini kabul etmek anlamına geldiği şekilde yorumlanamayacağını belirtir (Arendt, 1972, 76). Özlüce Arendt, bir grubun siyasi iradesine uygun olarak kamusal alanda ve aleni olarak yasanın çiğnenmesiyle

ortaya konan sivil itaatsizliğin, var olan siyasi sitemin de reddini içerebileceğini vurgulamaktadır.

Bedau'nun nitelendirmesiyle sivil itaatsizliği ve gerekçelendirilmesini liberal demokrasi ve sosyal adalet çerçevesinde teorize eden ilk düşünürlerden biri olarak John Rawls (Bedau, 1991:11), sivil itaatsizliğin temel unsurlarını sıraladığı şu tanımı yapar: " *İtaatsizlik, genellikle hükümetin yasalarında veya politikalarında bir değişiklik meydana getirmek amacıyla yapılan, kamuya açık, şiddet içermeyen, yasalara aykırı ancak siyasi bir eylemdir*" (Rawls, 1991, 104). Sivil itaatsizlik eyleminin kamunun önünde icra edilmesi, kamunun fikrini değiştirme amacını yansıtır ama aynı zamanda Arendt'in vurguladığı gibi sivil itaatsizliğin meşruiyetiyle de ilgilidir. Eylemin kamusal alanda icrası hem eyleme meşru bir zemin sağlamakta hem de tüm siyasal eylemlerin ortak amacı olan kamuoyunun dikkatini ilgili siyasi söyleme çekme amacı taşımaktadır. Rawls'ın sivil itaatsizlik teorisinin önemli başka bir noktası ise yasal sorunlar yaşansa da sivil itaatsizliğin ancak ve ancak demokratik anayasal bir toplum için geçerli olabilecek bir eylem türü olduğudur (Rawls, 1991, 103). Bu durum, Rawls'ın sivil itaatsizliği yasal sınırlar içinde kalan bir eylem olarak teorize edilebilmesinin önkoşulu olarak karşımıza çıkmaktadır; yasaya itaatsizlik edilmesini anlamlı kılacak olan şey yurttaşların demokratik bir devletteki anayasayı tanımalarıyla ilişkilidir (Rawls, 1991, 10). Zira sivil itaatsizliğin, hukukun işlerliğinin rafa kaldırıldığı herhangi bir başka yönetim biçiminde tartışılması anlamsız durumdadır. Bu nedenle sivil itaatsizliği ele alınış biçimi açısından Arendt'ten ayrılan yanı itaatsizliğin yöneldiği siyasi iktidarının meşruiyetinin kabulünün farklılığında yatmaktadır.

Diğer yandan Rawls, sivil itaatsizliğin amacı toplumun çoğunluğunun adalet duygusuna hitaben toplumsal işbirliği ilkelerine uyulmadığının kamuya duyurulması olarak değerlendirir (Rawls, 1991,105). Rawls'a göre, sivil itaatsizlik eylemleri kamusal prensiplere dayanan ve kamusal (aleni) bir eylem olarak kamuoyunu tarafından anlaşılabilecek şekilde derin bir siyasi ve vicdani çağrı içerir. Çağrının bu niteliğinin gereği olarak eylemin barışçıl olması önem taşımaktır çünkü şiddete başvuran bir eylem sivil itaatsizliğin kamuoyuna çağrısıyla uyuşmaz. Başkalarının sivil özgürlüklerine müdahale etmek, eylemin sivil itaatsizlik niteliğini muğlaklaştırır (Rawls, 1991, 106-107). Ayrıca Rawls'a göre sivil itaatsizlik eylemcisinin yasayı ihlal etmenin sonuçlarını üstlenmeye hazır olması yani onun yasaya sadakat sınırları içerisinde kalması, eylemin barışçıl olduğunun bir başka göstergesidir. Ancak sivil itaatsizlik yasaya sadakatin tam olarak sınırında yer alan nonkonformizm biçimidir (Rawls, 1991, 107). Bunun sonucunda da sivil itaatsizliğin uygulanma şekliyle ilgili bir sınır ortaya çıkmaktadır: *"Sivil itaatsizlik, bir çöküşe yol*

açmadan da gerçekleştirilebilir. Sivil itaatsizliğin hukuka ve anayasaya saygı çerçevesinde tanımlanması ve gerekçelendirilmesi, böylece herkes için talihsiz sonuçların ortaya çıkmasına yol açmaktadır" (Rawls, 1991, 110-11). Kamuoyunun da sivil itaatsizlik eylemi kabul edilebilir meşru bir şekilde algılaması yasaya ve anayasaya yani kurumsal siyasi sistemin işlerliğine de saygıyı tamamen yıkmamaya dayanmaktadır.

Dolayısıyla sivil itaatsizlik söz konusu olduğunda eylemin nasıl gerçekleştiği ve hangi yasal sınırlar içerisinde konumlandığı eyleme meşruiyetini kazandırmakta ya da kaybetmedir. Eylemin meşru ve haklı kabul edilebilmesi için 1) kamusal alanda aleni yani kamunun gözü önünde bir şekilde yasanın çiğnenmesi 2) şiddet içermeyen, barışçıl bir yapıda olması 3) kimseye zarara vermeyen diğer sivil özgürlüklere müdahale etmeyen bir sonucu yaratan 4) var olan yasal ve siyasi düzleme bağlı olmanın getirdiği ihlalin sonuçlarını kabul eden bir eylem olması gerekmektadir. Bütün bunlar reel alandaki sivil itaatsiz eylemin meşruluğu üzerine tartışmaların ana aksını şekillendirmektedir. Ancak sanal alanda sivil itaatsizliğin sınırları ve haklılığının neler olduğu tartışmaya açık bir konudur. Sivil itaatsizliğin sanal uzama taşınmasıyla eylemin haklılığı ve meşruiyetinin hangi bağlamda tartışabileceğini elektronik sivil itaatsizlik biçimi olarak değerlendirilen hacktivizm üzerinden sorgulayacağız.

4. Elektronik Sivil İtaatsizlik Olarak Hacktivizm

4.1. Kavramsal Temelleri: Critical Art Ensemble

Sivil itaatsizliğin hack aracılığıyla sanal uzaman taşınmasıyla ilgili ilk çağrı ve açıklama, sanatçı ve teorisyenler oluşan Critical Art Emsemble (CAE / Eleştirel Sanat Topluluğu) 1994 yılında yaptı (Meikle, 2008; Wray 1999). CAE siber uzama eklemlenen toplumsal koşulların akışkan hale geldiği bir zamanda, iktidarın ve hakimiyetinin, lokasyona bağlı kalmadan hedeflenebilir durağan noktalardan sanallık içerisinde göçebe bir varoluşa dönüştürdüğünü ve fiziki uzamdaki direniş ve protestonun da bu akışkanlık içerisinde etkisiz hale gelebildiğini iddia etmektedir. Bu nedenle CAE'e göre, "*göçebe iktidara*" karşı fiziki uzamda değil siber uzamda mücadele edilmelidir (1994, 11-15, 25). Bu noktada ise hackerların rolünü vurgulamaktadır:

> Göçebe iktidara fiziksel uzamdan ziyade siber uzamda direnilmelidir. (...) Küçük ama koordineli bir hacker grubu, otoritenin veri bankalarına, programlarına ve ağlarına elektronik virüsler, solucanlar ve bombalar sokabilir ve muhtemelen yaratacağı durgunluğun yıkıcı gücünü

> göçebe alana taşıyabilir. Uzun süreli durgunluk, göçebe otoritenin küresel düzeyde çöküşüne eşittir (1994,16).

CAE'ye göre, göçebe iktidar varlığını, hakimiyetini ağlara boyunca siber uzama yaymasına borçluysa ona karşı mücadele de ağlar boyunca yayılmalı ve ağı sekteye uğratarak geç kapitalizmin göçebe gücünü al aşağı etmelidir. CAE'nin temel vurgusu, siber uzamdaki direniş bu alanı en iyi bilen hackerlerla mümkün olduğudur. Topluluğa göre iktidar ile mücadele konusunda erken kapitalist dönemde sayıca kalabalık sınıfsal hareketlerinin yapamadığının, göçebe iktidara yönelik olarak siber uzamda küçük grupların sivil itaatsizlik eylemleriyle mümkün olmasıdır. Zira artık sivil itaatsizliğin biçimi değişmiş ve daha etkili daha kapsamlı somut sonuçları olacak eylemler mümkün hale gelmiştir (CAE, 1994, 141-142). CAE 1995'te solun geleneksel sivil itaatsizlik stratejilerini demode bulduğunu ve yeterince işlevsel bulmadığını belirterek merkezi olamayan iktidara elektronik seviyede yeni sivil itaatsizlik taktiklerinin ortaya konması gerektiğini savunur. Bu elektronik seviyedeki siber uzamda yaratılacak sivil itaatsizlik biçimlerini nitelendirmek için *elektronik sivil itaatsizlik* kavramını kullanır (CAE, 1995, 9-10). CAE aslında, elektronik sivil itaatsizliği taktiksel olarak sivil itaatsizliğin güncellenmiş ancak daha güçlü olması mümkün olan sanal bir versiyonu biçiminde görmektedir: "*Sivil itaatsizlikte olduğu gibi başlıca taktikler elektronik sivil itaatsizlikte de izinsiz girişler ve blokajdır*". Ancak bu kez "*etik dışı veya suç teşkil eden eylemlerde bulunan meşrulaştırılmış kurumlar üzerinde baskı oluşturmak*" amacıyla fiziksel mekanlar değil enformasyon kanallarında mücadele edilir (CAE, 1995, 18). Elektronik blokajın, mekana bağlı bir lokasyondaki blokajın yapamayacağı bir finansal stres yaratıp küresel etkilere neden olabilmesi gibi CAE, elektronik sivil itaatsizliğinin baskı oluşturma potansiyelini geleneksel sivil itaatsizlikten çok daha yüksek görmektedir. Topluluğa göre, devlet ve sermayenin değer siteminde enformasyon bireyin üstündedir ve elektronik sivil itaatsizliğin amacı bunu tersine çevirerek bireyi daha değerli hale getirme çabası olmalıdır (CAE, 1995, 17-18).

CAE'nin elektronik sivil itaatsizliğin meşruiyeti noktasında ortaya koyduğu temel kriterler ise ilk olarak, fiziksel bir karşılaşma söz konusu olmadığı için doğası gereği şiddet içermese de veri bloke ederken ya da rahatsızlık yaratmak için site engellemesi gibi eylemlerde bulunurken insani işlevlere sahip olan sitelerin ve verilerin engellenmemesinin gerekliliğidir. İkinci olaraksa kurumlara yönelik eylemlerde kurum çalışanları hedeflenmemelidir. Topluluk bu iki önemli noktada sıradan bilişim suçu ile elektronik sivil itaatsizlik arasındaki farkın ortaya çıktığını belirtmektedir (CAE, 1995, 18-19). CAE'ye göre, elektronik sivil itaatsizliğin önündeki engel meşruiyetinden

ziyade hackerlar ve aktivistler arasındaki işbirliğinin eksikliğidir. Sokaktaki aktivistler hack'i politik olarak doğru eylem olarak görme noktasında hackerlar ise apolitik oldukları için işbirliğinin zor hale geldiğini iddia etmektedirler. Ancak Topluluğa göre sokaktaki eylemlerin sanal uzama taşınmasının zorunluluğu iktidarın göçebe yapısıyla mücadelede elektronik sivil itaatsizliği zorunlu kılmaktadır (CAE, 1995, 20-23). Dolayısıyla CAE'nin ortaya koyduğu bakış açısı göçebe iktidar biçimiyle ancak elektronik sivil itaatsizlik ile mücadele edilebileceğidir. Topluluğun temel iddiası, iktidar ve kapitalizm biçim değiştirerek yer kürenin her yerine sermayenin hakimiyetini yayarken direnişin anlamlı ve en etkili aracı olarak elektronik sivil itaatsizlik olduğudur (CAE, 1994; 1995).

Wray ise CAE'in elektronik sivil itaatsizliği göçebe iktidara karşı zorunlu bir mücadele biçimi olarak görmesinden hareketle, sokaklardaki sivil itaatsizliğin hala önemli olduğunu anımsatarak geleneksel sivil itaatsizliğin elektronik sivil itaatsizlik ile tamamlandığı hibrit sivil itaatsizlik biçimlerinin ortaya çıkacağından bahsetmektedir. Ancak siyasi alan hızla dönüştükçe Wary'e göre de *"21. yüzyılda elektronik sivil itaatsizlik gerçekleşecektir"* (Wray, 1998). Wray'in ortaya koyduğu hibrit yapı, yukarıda andığımız Taylor ve Jordan'ın kitlesel eylem hacktivizmi olarak tarif ettiği bir hacktivizm biçimine işaret etmektedir. Kitlesel olarak ortaya konan, tam da CAE'in eksiklik olarak gördüğü ancak başarıya ulaşmış, FloodNet gibi aktivistlerin ve hackerların işbirliğinin ürünü olan hacktivist eylem biçimlerinden; bir grup hacktivistin elektronik sivil itaatsizlik eylemleriyle sokaktaki geleneksel sivil itaatsizliği desteklediği hibrit yapı bugün adı en fazla duyulan ve duyulmaya devam edilen hacktvist grup Ananonymous'un birçok eyleminde ortaya çıkmaktadır. Dolayısıyla elektronik sivil itaatsizliğe ilişkin tartışma, görece giderilen işbirliği eksikliğinden ziyade meşruiyetine yönelik belirmektedir.

4.2. Elektronik Sivil İtaatsizliğin Meşruluğu ve Sınırları

Hacktivizmi elektronik sivil itaatsizlik olarak değerlendirme çabasında ortaya çıkan tartışmanın en önemli yanı etik ve etik olabilmenin sağladığı meşruluk konusudur. Bu bağlamda hacktivizmin elektronik sivil itaatsizlik olarak kabul edilebilmesi için öncelikle etik olarak motive edildiğinin ortaya konması gerekmektedir. Kenneth E. Himma hackin ifade özgürlüğü olarak sivil itaatsizlik bağlamında moral olarak meşru değerlendirilebilmesi için politik olarak motive olmasına bağlamaktadır. Herhangi bir ticari ağa ya da hükümet ağlarına her türlü izinsiz giriş yasal ve moral olarak mahzurlu iken politik amaç taşıyan hacktivizm kabul edilebilir sınırlar içerisindedir (Himma, 2008, 196). Ancak Himma'ya göre, sivil itaatsizlik ifadeye değil davranışa

dayanan bir özgürlüktür. Bir yasayı çiğnemek davranışsal bir eylemdir. Meşru demokratik bir ülkede muhalefet edilen konuya ilişkin farklı ifade özgürlüğü biçimlerinin yolu açık olduğu için sivil itaatsizlik çoğunlukla, azınlıkta kalan bir fikrin bağlamında ortaya çıkan bir konudur (Himma, 2008, 197-198). Ancak meşru bir devletin yasaları zorla uygulama izninin sınırlarının olması fikri, sivil itaatsizliği moral olarak haklı kılabilmektedir. Bu noktada masum üçüncü kişilerin haklarının ihlal edilmemesi veya zarara uygulamaması esas olduğunu vurgulamaktadır. Sivil itaatsizliğin tüm bu özellikleri hacktivizm için de geçerlidir. Himma'nın hacktivizm açısından vurguladığı bir diğer önemli nokta ise eylemcinin yasal sonuçları kabul etmesi ve eylemin kamu barışını bozmaması hacktivist bir eyleme sivil itaatsizlik olarak meşruluk kazandırmaktadır (Himma, 2008, 198-199).

Mark Manion ve Abby Goodrum ise elektronik sivil itaatsizlik olarak hacktivizmin meşru sınırları sorgulamak için başlangıç noktasını hacktivizmin temel motivasyonu olarak işaret etmektedirler. İkiliye göre, bir hacktivistin motivasyonunun ne olduğunun anlaşılmasının yolunun kendi beyanına dayanmaktadır ve bu beyanın en somut kanıtı da genellikle hacklenen sitelere yerleştirilen politik mesajlarda görülmektedir. İkili, bir hackin ancak etik olarak motive olmuşsa yani kişisel kazanç ve/veya vandalizm amacı taşımıyor, şiddet içermiyor ve eylemin sonuçlarının yasal ve moral sorumluluğunu alıyorsa hacktivist bir eylem olarak sivil itaatsizlik niteliği taşıyabileceğini belirtir (Goodrum, Monion, 2000, 15). Hacktivizmin elektronik sivil itaatsizlik olarak değerlendirilmesi gerektiğini savunan Goodrum ve Monion'a göre, hacktivizm açıkça şiddet içermemesi nedeniyle sibervandallık ya da siberterör olarak değerlendirilemez. Hacktivizm basitçe ağır ceza ile sonuçlana hack eylemi kapsamında değil sivil itaatsizliğin politik eylem olduğu gerçeği göz önünde tutularak yasal zeminde değerlendirilmelidir (Goodrum, Monion, 2000, 16).

Başka bir açıdan hack ve suç ilişkisi bağlamında, Graham Meikle ise hacklemenin birçok insan için korkutucu, bilinmedik ve suçlu bir davranış olarak algılanmasının beraberinde getirdiği algının hacktivizmin meşruiyeti konusunda bir sorun yaratmasına dikkat çekmektedir. Hacktivizm kavramının kendisi hacklemenin suçla ilişkili anlamı nedeniyle, elektronik sivil itaatsizliğin marjinalleştirilmesini beraberinde getirmektedir. Meikle, hacktivizmi elektronik sivil itaatsizlik biçimi olarak değerlendirmenin hackin krriminal boyutu nedenliye ortaya çıkan sorunlu yanını vurgulamaktadır. Bu kriminal boyut ve bu boyutun yarattığı kamuoyu tarafından algılanış biçimi, hackin doğasını sorgulamayı beraberinde getirmektedir (Meikle, 2008,183). Ancak hack, tam da yasaya aykırılık teşkil etmesi açısından sivil itaatsizliğin

sanal uzama taşınması olarak kavramsallaştırılabilmektedir. Hacktivizmi suç bağlamında değerlendirilmesine kendisi karşı çıkan Meikle'in çabası, hackin olumsuz ve yanlı tüm anlamlarının yarattığı etkinin yükünden bu eylem biçimlerini arındırma çabası olsa da sivil itaatsizlik olarak kavranabilmesinin temel unsurunun yasayı ihlal etmeyle olan ilişkisini görmezden gelmektedir. Diğer yandan bir elektronik sivil itaatsizlik biçimi olarak hacktivizmin kriminalleştirilmesi hackin yaratabileceği etkinin iktidar ve sermaye bütünlüğünün dijital alandaki hegemonyası için tehdit olarak görülmesiyle de ilişkilendirilebilir.

Bu bağlamda, Goodrum ve Monion, hacktivistlerin suçlu olarak tanımlanmasının siyasi ve ekonomik elitler için işlevsel yanını vurgulayan çok kritik iki noktayı vurgularlar: (1) hukuk sisteminin, interneti tamamen ticarileştirmeye çalışan dev şirketlerin çıkaranlarını koruması, (2) vatandaşları hakkında geniş veri tabanları derleyen devletlerin kişisel mahremiyeti yok etmesi (Goodrum, Monion, 2000, 17). Hacktivizmin yasal zeminde sivil itaatsizlik olarak değil de doğrudan veri güvenliğine yönelik bir saldırı kapsamında terörle ilişkili olarak ve/ya siber tehdit, ulusal güvenlik tehdidi olarak değerlendirilmesini eleştiren ikili, elektronik sivil itaatsizlik olarak hacktivizmin devletler ve dev şirketler eliyle ihlal edilen veri mahremiyetinin ihlalinin yanında daha fazla meşru olduğunu savunmaktadır (Goodrum, Monion, 2000). Dolayısıyla hacktivizmin sistemlere izin giriş ve veri ihlaline ilişkin suçlarla ilişkilendirilmesi aslında her türlü dijital izimin kayıt altına alındığı ve veri mahremiyetimiz üzerinde sandığımızdan çok daha az söz hakkımızın olduğunu düşünürsek veri ihlalinin küresel dev dijital korporasyonlar üzerinden siyasi ve ekonomik elitler için meşruiyetini sorgulamayı gölgelemekte olduğu sonucu ortaya çıkmaktadır.

5. Sonuç

Hacktivistler ister dijital politikalara ilişkin olarak internetin sermaye ve iktidar gözetimine ve sansüre dayanan altyapısına karşı enformasyon özgürlüğü ve veri güvenliği politikalarına karşın daha özgür ve güvenli sanal alan için mücadele etsin ister reel kolektif eylemlere destek olmak ya da dijital kitlesel bir eylem ortaya koymak için aktivistlere FloodNet örneğinde olduğu gibi araçlar sunmak için mücadele etsin hacki kullanma amacı politik bir motivasyon taşımaktadır. Bir ceza suçu olan hack, sivil itaatsizliğin sanal alanda yeniden yaratılması bağlamında meşru bir zeminde değerlendirilebilinir. Reel hayattaki sivil itaatsizliğin meşruiyeti için yasa ihlalinin kamuoyunun önünde aleni bir şekilde işlenmesi, şiddet içermemesi, sonuçlarını yasal ve ahlaki olarak kabul etmesi ve kimseye zarar vermemesi koşulları söz konusu-

dur. Bu koşullar elektronik sivil itaatsizlik olarak hacktivizm için de geçerlidir. Ancak geleneksel sivil itaatsizlikten farklılaştığı noktalar söz konusudur. Hack zaten kamuoyunun dikkatini çekme amacıyla kamuya açık dijital alanda gerçekleştirilmektedir ve doğası gereği fiziksel bir temas söz konusu olmadığından barışçıldır. Ancak her ne kadar CCC ve EDT gibi hacktivistlerin kimlikleri bilinse de bugün baktığımızda, özellikle kolektif eylemlere destek veren Anonuymous gibi hacktivist grupların çoğu anonimdir. Dolayısıyla hackin moral sonuçlarından hacktivist grup olarak sorumlu olsalar da ancak kimliklerinin tespit edilebildiği ölçüde yasal olarak kabul etmeleri söz konusu olabilmektedir. Dolayısıyla geleneksel sivil itaatsizlikte eylemcinin kimliğinin bilinmesiyle aldığı risk ile elektronik sivil itaatsizlikteki aynı oranda karşımıza çıkmamaktadır. Ancak bu durum hacktivizmin meşruluğunu tartışmalı kılmanın ötesinde hackin motivasyonuna odaklanmayı önemli kılmaktadır. Kişisel çıkar sağlamamak, diğer kişisel hak ve özgürlüklere zarar vermemek ve vandalizm amacı taşımayarak politik olarak motive olması hackin elektronik sivil itaatsizlik olarak meşruiyetini göstermektedir.

Öte yandan elektronik sivil itaatsizlik kapsamında hackin sisteme izinsiz giriş ve veri mahremiyeti ihlali kapsamında suçla ilişkilendirilmesi ve hackin kriminal yanının inanılmaz tehlikeli olarak algılanması, aslında gözetim kapitalizmini meşrulaştırmaya hizmet etmektedir. Zira ağa bağlı her bir bireyin kişisel verileri dev dijital şirketlere tarafından ihlal edilmektedir. Gözetim kapitalizmi (Zuboff, 2019) veya platform kapitalizmi (Srnicek, 2016) olarak nitelendirelim, günümüz dijital ekonomi modelinin temeli, sermaye birikim modeli olarak veri birikimine (veriyi toplama, işleme ve ondan öngörülebilir yeni veriler üretmemeye) dayanmakta ve sıradan bireylerin veri mahremiyeti son derece yasal ancak meşruiyeti tartışmalı bir yolla aşılmaktayken; hacktivist bir eylemde verilerin ve sitemlerin tamamen tahrip edilmeden bir kuruma yönelik veri ihlali daha meşru görünmektedir. Dolayısıyla veri mahremiyetinin ihlali dev ulusüstü şirketler ve devletler eliyle olunca son derece meşruyken buna karşı mücadele eden hacktivizm – ve özellikle Jordon ve Taylor'ın andığımız dijital olarak doğru hacktivizm olarak nitelendirdikleri hacktivizm biçimi – için terör ve/veya vandallık olarak kavranması sorunlu görünmektedir. Ancak bu tartışma, başka bir çalışmanın kapsamında daha detaylıca irdelenerek ortaya koyulmalıdır.

Kaynakça

Alton, S. R. (1992) In the Wake of Thoreau: Four Morden Legal Philosophers and the Theory of Nonviolent Civil Disobedience, Loyola University Chicago Law Journal ,24 Loy. U. Chi. L. J. pp. 39-76.

Arendt, H. (1972), *Crises of The Republic,* A Harvest Book Harcourt Brace & Company, Florida.

Assange, J. (25 Kasım 2006), "The Curious Origins of Political Hacktivism", Counter Punch, http://www.counterpunch.org/2006/11/25/the-curious-origins-of-political-hacktivism/,

Assange, J. ve Dreyfus, S. (2001) *Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier,* Reed Books Australia.

Baldi, S., , Gelbstein, E., Kurbalija, J. (2003). Hacktivism, Cyber-Terrorism and Cyberwar: The Activities of The Uncivil Society in Cyberspace, Diplo-Foundation, Switzerland.

Bedau, H. A. (Ed.) (1991). Civil Disobedience in Focus. Routledge.

Critical Art Ensemble (CAE) (1994) The Electronic Disturbance, Autonomedia, http://www.critical-art.net/books/ted/

Critical Art Ensemble (CAE) (1995) Electronic Civil Disobedience & Other Unpopular Ideas, Autonomedia, http://www.critical-art.net/books/ecd/

Denning, D. E. (2001) Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, *Networks and Netwars : The Future of Terror, Crime, and Militancy* içinde, Arquilla, J. ve Ronfeldt, D. F. (Ed.), Santa Monica, CA: RAND, 239-288.

Denning, E. D. (2008) The Ethics of Cyber Conflict, *The Handbook of Information and Computer* içinde, Himma K. E. And Tavani H. T. (Ed.), New Jersey: John Wiley & Son., pp. 407-428.

Friedman, A. ve Sınger, P. W. (2014) *Cybersecurity And Cyberwar: What Everyone Needs To Know*, New York : Oxford University Press.

Goodrum, A. ve Manion, M. (2000) Terrorism or Civil Disobedience: Toward a Hacktivist Ethic, Computers and Society, Vol. 30 (2) June 2000, 14-19.

Goodrum, A. ve Manion, M. (2000) Terrorism or Civil Disobedience: Toward a Hacktivist Ethic, Computers and Society,Vol. 30 (2) June 2000, 14-19.

Graham, P. (2004) *Hackers and Painters*, Sebastopol, CA: O'Reilly and Associates

Gunkel, D. (2005) Editorial: Introduction to Hacking and Hacktivism, New Media & Society, vol. 7 no. 5, 595-597.

Hampson, N.C.N. (2012) Hacktivism: A New Breed of Protest in a Networked World, 35 B.C. Int'l & Comp. L. Rev. 511 http://lawdigitalcommons.bc.edu/iclr/vol35/iss2/6

Himma, K. E. (2008) Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking, *The Handbook of Information and Computer Ethics* içinde, Himma, K. E. ve Tavani, H. T. (Ed.), New Jersey: John Wiley & Son. 191-218.

Jordan, T. (2007) Online Direct Action: Hacktivism and Radical Democracy, *Radical Democracy and the Internet* içinde, Dahlberg, L. ve Siapera, E. (Ed.), New York: Palgrave Macmillan, 73-88.

Jordan, T. ve Taylor, P. (2004) *Hacktivism and Cyberwars,* London: Routledge.

Jordan. T. (2002) *Activism! Direct Action, Hactivism and the Future of Society,* London: Raktionbooks.

Joyce, M. (2010) Introduction: How to Think About Digital Activism, Digital Activism Decoded: The New Mechanics of Change içinde Joyce, M. (Ed.), New York: IDebate Press, 1-14.

Klang, M. (2004) Virtual Sit-Ins, Civil Disobedience and Cyberterrorism, *Human ights in The Dıgıtal Age* içinde, Murray, H. And Kalng M. (Ed.), The GlassHouse Press, London, pp. 135-145.

Klaus, C. (1999) An Introduction to the Back Orifice 2000 Backdoor Program, EDPACS, 27:6, 1-11.

Kubitschko, S. (2018) Chaos Computer Club: The Communicative Construction Of Media Technologies And İnfrastructures As A Political Category, *Communicative Figurations Transforming Communications in Times of Deep Mediatization* İçinde, A. Hepp, A. Breiter, U. Hasebrink (Ed.), Palgrave Macmillan, pp. 81–100.

Lane, J. ve Dominguez, R. (2003) Digital Zapatistas,TDR (1988-), Summer, 2003, Vol. 47, No. 2 (Summer, 2003), The MIT Press, pp. 129-144.

Leibowitz, B. (2011) Hack, Hacker, Hacking , Peterson, T. F.(Ed.) *Nightwork : A History of Hacks and Pranks at MIT* içinde, Cambridge, Massachusetts: MIT Press.

Levy, S. (2010) *Hackers: Heros of The Computer Revolution,* Sebastopol, CA: O'Reilly and Associates.

Marino, M. C. (2014) "Code" *The Johns Hopkins Guide to Digital Media* Ryan,M.L. Emerson,L., and Robertson B. J., (Ed.), Baltimore: Johns Hopkins UP, pp 64-69.

Meikle, G. (2008) Electronic Civil Disobedience and Symbolic Power, *Cyber-Conflict and Global Politics* Karatzogianni, A. (Ed.) London Routledge. pp. 177-187

Mungo, P. ve Glough,B. (1993) *Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, And Keyboard Criminals,* New York: Random House.

Nazario, J. (2004) *Defense and Detection Strategies Against Internet Worms,* Artech House, Boston.

Palmås, K. ve von Busch, O. (2006) *Abstract Hacktivism: The Making of a Hacker Culture,* Londoa: OpenMute.

Rawls, J. (1991) Definition and Justification Of Civil Disobedience, *Civil Disobedience in Focus* içinde, Bedau, H. A. (Ed.), Routledge, pp. 103-121.

Samuel, A. (2004) Hacktivism and the Future of Democratic Discourse, *Democracy Online : The Prospects For Political Renewal Through The Internet* içinde, Shane, P. M. (Ed.), New York: Routledge, 123-140.

Sauter, M. (2014) *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic.

Srnicek, N. (2016) *Platform Capitalism,* Cambridge, UK, Malden, MA, Polity.

Taylor, P. A. (2005) From hackers to hacktivists: speed bumps on the global superhighway?,, New Media and Society, London: Sage Publication, Vol7(5):625–646, (17 Nisan 2015).

Thomas, D. (2002) *Hacker Culture*, Minneapolis: University of Minnesota Press.

Thomas, S.L., Francillon, A. (2018). Backdoors: Definition, Deniability and Detection. In: Bailey, M., Holz, T., Stamatogiannakis, M., Ioannidis, S. (eds) *Research in Attacks, Intrusions, and Defenses*. RAID 2018. Lecture Notes in Computer Science, vol 11050. Springer, pp. 92–113.

Thoreau, H. D. (1991) Civil Disobedience, *Civil Disobedience in Focus* içinde, Bedau, H. A. (Ed.), Routledge, pp. 28-48.

Thoreau, H. D. (2013*) Sivil İtaatsizlik*, (Çev. Melis olçum), Kafekültür Yayıncılık, İstanbul.

Williams, S. (2002). *Free as in Freedom: Richard Stallman's Crusade for Free Software*, Sebastopol, CA: O'Reilly and Associates.

Wray, S. (1998) On electronic civil disobedience. Presented to the 1998 Socialist Scholars Conference, March 21–23. New York. https://www.thing.net/~rdom/ecd/oecd.html (17.06.2023)

Wray, S. (1999) Electronic Civil Disobedience and the World Wide Web of Hacktivism, Switch, Vol 4 (2).

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, Public Affairs.