BYLOCK HAKKINDA YAZILAN ALGI RAPORLARI

(Bilimsel ve Hukuki Gerçekler)

Önsöz

ByLock ve FETÖ; hem hukuki hem teknik değerlendirmelerin bir araya gelmesi gereken çok yönlü bir konudur. Bu nedenle basit bir blog yazısı olarak düşündüğüm aşağıdaki I. içeriğe uzun yıllardır dostum olan Av. Süleyman BOŞÇA'dan hukuki değerlendirmelerini yazmasını istedim. Kendisi beni kırmayarak II. Bölümün oluşturulmasında çok değerli katkılarını esirgemedi. Ben I. Bölümde teknik tarafı daha çok halkın anlayabileceği bir dil ile ele alarak konuya değinirken, arkadaşım ise bu rapor mahkemelere referans olabileceği için II. Bölümdeki hukuki değerlendirmelerini yalın bir hukuk diliyle ifade ederek rapora eklemiştir. Dostum Av. Süleyman BOŞÇA'ya ve Av. Olcay ENLİOĞLU'na verdikleri sonsuz destek için teşekkürlerimi sunarım.

Dr. Öğr. Üyesi. Uraz YAVANOĞLU
Gazi Üniversitesi
Bilgisayar Mühendisliği
Bölüm Başkan Yrd.

I. BİLİMSEL GERÇEKLER

Öncelikle yazılarımı takip etmeye başlayan dostlarıma teşekkürlerimi sunarım. Arkadaşlarım, ilk olarak kaleme aldığım CITIZENLAB Aldatmacası başlıklı yazımla ilgili olumlu ve olumsuz görüşlerde bulundular, yazının daha uluslararası düzeyde kaldığı öncelikli olarak ülkeye daha kısa vade içerisinde katkı sağlayabilecek bir içeriğin daha yararlı olabileceğini ilettiler. Bende önerileri doğrultusunda yaptığım araştırmalarda çok sayıda Türkçe teknolojik blog, haber portalı, sosyal medya vb. içerikler bulunduğunu görmekle birlikte bilimsel olarak tartışılabilecek konuları ararken, biraz da uzun yıllar bilirkişi olarak görev yaptığımdan olsa gerek ByLock konusunda halkın her kesimine fayda sağlayabileceğim bilimsel bir tartışma yazısı yazabileceğimi düşündüm. Teknik olmayan kişilerin de kolaylıkla anlayabilmelerini sağlamak adına, konu hakkındaki bilimsel gerçekleri açık, anlaşılır ve sade bir dille ve kişilere doğrudan hitap ediyormuşçasına kaleme almanın doğru bir yöntem olacağını düşünüyorum. Çünkü internette aynı çevrelerce hazırlandığını müşahede ettiğim bilirkişi raporlarında,

okuyucunun birçok teknik terim ile bilgiye boğulduğunu, kullanım amacı ve yerine göre farklılık arz eden kavramların -yine bilinçli olduğunu düşündüğüm anlatım tarzıyla- birbirine girmesine sebebiyet verildiğini gördüm ve bu durum karşısında şaşkınlığımı gizleyemedim.

Bu alanda uzman biri olarak akademisyen olarak bu ülkenin yarınlarını yetiştiren bir bilim adamı olarak halkı kin ve düşmanlığa sevk eden algı raporlarını ele almayı ve bunlar üzerinde tek taraflı doğruymuş gibi sunulan yalan/yanlış noktaları çok yönlü tartışmayı ve doğruların ortaya konulması gerektiğini düşünüyorum. Bu yazı içerisinde ByLock'a taraf olan sanıklar ve mahkemeler arasındaki süreci değil algı raporları ile konuyu tek taraflı olarak ele alan kişilerin düşünceleri hakkındaki yorumlarımı yazmaya çalışacağım. Sanıklar ve Mahkemeler arasındaki süreçler sanıkların bilirkişilerden alacağı özel raporlar ve mahkemelerin bu süreçte atadığı veya atacağı bilirkişiler vasıtasıyla zaten çözüme kavuşacaktır.

Bir konuya dair bilirkişi raporlarını ve uzman görüşünü mahkemeler talep etmelidir; şöyle ki bir dava görülürken hakim bilirkişi yorumuna başvurabilir, bu bilirkişi ve/veya bilirkişi heyetini seçerken yetkinliğini ispat edebilen kişilerden oluşan bölge adalet komisyonu bilirkişi listesi baz alınır. İnceleme alanıyla ilgili listeye kayıtlı bilirkişi bulunmaması halinde ilk aşamada bu talep üniversitelere yazılır ve akademisyenlerden bilirkişi ataması yapılır. Bir de bilimsel mütalaa konusu vardır, davanın tarafları kurumlara veya bilirkişi vasfına haiz kişilere başvuru yaparak özel rapor alabilir ve bunları mahkemelere sunabilir.

ByLock ile karşılaştığım dikkat çekici husus, kişilerin herhangi bir yargı makamının ve doğrudan etkilenen şahsın talebi olmaksızın, bırakın tarafsızlığı, 'devlete karşı taraf' olarak bilimsel bakış açısının dışında ByLock mütalaası vermeleridir. Bir kişi bir gün oturup hadi ben bugün devletin ve Milli İstihbarat Teşkilatının (MİT) ByLock konusunda geldiği noktayı eleştiren bir rapor yazacağım diyorsa; böyle bir davranışın içerisinde kesinlikle bu işte olmaması gereken birileri var demektir. Taraflardan birinin olması elbette tarafsızlık açısından sorun teşkil etmez ancak bu incelemeyi isteyen tarafın belli olmaması, raporlar içerisinde devletin gizli bilgilerine olmadığı şekliyle yer verilmesi, konuların her yönüyle tartışılmadan tek taraflı bir bakış açısıyla ele alınması, dahası bilimsel/akademisyen kişilerin değil ben yaptım oldu mantığı olan kişilerce yazılmış olması, halkın gözünde devleti değersizleştirme ve siyasileştirme çabaları olduğunun göstergesidir.

Yaptığım araştırmalar neticesinde üzülerek ifade ediyorum; MİT'in GİZLİ ibareleri bir raporunun internette yayınlandığını, çok sayıda kişi ve grubun bu rapor üzerinde hatalı senaryolar ile çok uç noktalarda ve bilimsel tartışma ortamından uzak karşıt algı raporları hazırladıklarını gördüm. Benim rastladığım tüm raporlar tek bir kalemden çıkmışçasına konuyu bilimsel olarak ispat edilemeyecek bir noktaya taşıyan ve taraf olunarak hazırlanmış içeriklerden oluşmaktaydı. Eminim MİT tarafından yazılan raporu ve içeriklerini tarafsız bir tartışma ortamında kaleme alan kişilerde olacaktır ancak Linç Kültürü maalesef toplumun her kesimini sarmış ve bizleri olduğumuzun ötesinde büyük bir kuşkuculuk, şüphecilik ve komplo teorisyenliğine götürmüş durumdadır. Bir an için şapkamızı önümüze koyarak düşünmemiz gerekmektedir, Nasreddin Hocanın dediği gibi "Hırsızın hiç mi suçu yoktur?".

Bazı kesimler toplumun algısını yönetmek için devlet eliyle yapılan tüm işlerin şaibeli olduğu yönünde kamuoyu oluşturmaya çalışarak hareket etmektedir. Geçmişten günümüze devleti ele geçirmeye çalışan silahlı terör odaklarının kullandıkları yöntemler değişmiş olsa da devlet geleneğini yıkamayacağını anlayan destekçileri halkın yanında görünerek devlete karşı hareketlerin ortaya çıkmasını amaçlayan çalışmalarda bulunmaktadır.

Ben bilim adamı ve akademisyen kimliğim ile adli bilişim uzmanı kimliğini bir arada kullanabilen bir kişiyim. Ama hayatta her zaman benden daha bilgili ve deneyimli kişiler olduğunu ve her zaman bir başkasından yeni şeyler öğrenebileceğimi kabul etmiş bir insanım. Hayatta her zaman mütevazi olmayı korumak ve her zaman yeni bir fikri, manayı ve hayatın bizleri sunacağı deneyimleri kabul etmeyi, ben oldum demeden insanın kendisini geliştirmesini, eğitmesini bilmesi gerektiğine inanan kişilerdenim. Burada x kişisi y kişisi şöyle yazmış böyle davranmış demem beni bu kişilerle aynı kefeye koyar. Amacım kimseyi hedef göstermek olamaz. Ama güzel ülkemin geldiği noktada artık birilerinin taşın altına elini koyarak gerçekleri söylemesi ve gerçekten tarafsız olarak tartışmaya katılması gerekmektedir; çünkü yazılan çizilen raporlarda kendisini adli bilişimci olarak tanıtan kişiler bilişim hukukçusu olarak tanıtan kişiler çamur at izi kalsın mantığı ile hareket etmektedir. Bu ayak oyunlarının doğrusunu yanlışını biri söyleyecekse bu kişinin işine yıllarını vermiş doktorasını yapmış halen ülkesinde ve yurtdışında akademik çalışmalarını sürdüren biri olmasından gurur duyduğumu belirtmek isterim.

ByLock meselesi 15 Temmuz tarihi ile hayatımıza giren çok yeni bir olgudur, halkın büyük bir kesimi tarafından değil sadece silahlı terör örgütü mensuplarınca bilinmektedir. ByLock basit bir mesajlaşma uygulaması değildir. Toplumun her kesimi tarafından kullanılan WhatsApp gibi bir yapısı olduğunu düşünmek yanlıştır. ByLock programını kullanmak için kayıt olmaktan fazlası gerekmektedir. Diğer bir ifadeyle ByLock kullanmadan önce birbirlerinin örgüt içindeki kod adını bilmeyen kişi yada grupların haberleşmesi mümkün değildir. Uygulamanın kripto haberleşme yazılımı olarak anılmasının en büyük nedeni basit bir yöntem ile haberleşecek tarafların birbirlerini görememesi bu isimlerin örgüt içi imamlar vasıtasıyla taraflara bildirilmesidir. Bu noktada bir anti parantez açarsam; 6 yılı aşkın süredir üniversitede farklı kesimlerden öğrencilerim ile sayısız mobil uygulamalar geliştirdik. Android ve iOS sistemler için halen uygulama mağazalarında özellikle mesaj gönderme, konum bildirme, adres defteri eşleştirme, siber güvenlik vb. özellikleri olan akademik uygulama paketleri üretiyoruz. Benim yada en azından öğrencilerimden birinin “Uraz hocam bakın hem mobil hem de siber güvenlik çalışıyoruz, ByLock adında bir kripto haberleşme yazılımı varmış” demeleri gerekirdi diye düşünüyorum. Bizim yazdıklarımızla aşağı yukarı aynı kategorilerde olan ve on binlerce kişi tarafından yüklenmiş bir yazılımın bu kadar genç arkadaşımın ve benim gözümden kaçmış olmasını anlamam mümkün değildir. Ben bu yazılımı bulamıyorken on binler nasıl bulmuş, yüklemiş ve kullanmış benim için halen anlamakta güçlük çektiğim bir husustur. Bu bile özünde ByLock uygulamasının FETÖ/PDY mensuplarının gizli haberleşmelerini sağlamak amacıyla geliştirildiğini ve kullanıma sunulduğunu ortaya koymak için yeterli bir delildir. Ancak bilim, kişisel düşüncelerimden fazlası demektir. İsterseniz biraz bunlar üzerine konuşalım.

Bugüne kadar mütalaa verdiğim sayısız bilişim suçu davasında her zaman bilimsel gerçekleri yazan biriyim. Çünkü bilim adamı, tartışmaya duygularını dışarda bırakarak sadece aklıyla dâhil olmalıdır.

Yazımın hukuki ve insani sonuçları ne olabilir bilmediğim için MİT tarafından yazılan GİZLİ ibareli raporu kullanıp kullanmama noktasında bazı endişelerim bulunmaktadır. Sonuç olarak MİT raporunda yazılan tüm içeriklere güvenim tam olmakla birlikte, devlet sırrı olabilecek bir içeriği ifşa etmek sadece devlete değil devleti oluşturan bireylerden biri olarak bana da zarar verecektir. Gördüğünüz gibi endişem devlete duyduğum güvenle alakalı değildir, Türkiye bir hukuk devletidir. Bu gerçeği yıkmak için kamuoyu oluşturarak bu güveni yıkmaya çalışan terör odakları bulunmaktadır. Dolayısıyla A

kişisine B kişisine değil ayrılmaz bir bütün olan vatanıma, milletime ve devletime güvenim tam olarak bu yazıyı ele almam gerektiğini düşünüyorum.

Bu noktada ani öfkelenip ani durulan bir milletiz, bazen olaylara bakarken bir anlık öfkeyle ve heyecanla hareket ederek bizi yönlendirmeye çalışan kişilerin oyunlarına gelebiliyoruz, hayatta her zaman sakin kafayla düşünerek, tartışarak farklı görüşleri de dikkate alarak hareket etmek gerektiğine olan inancımı koruyorum.

Bu nedenle direkt olarak MİT raporunu değil, MİT raporunu bilimsel temelden uzak bir şekilde ele alan diğer kişilerce veya gruplarca yazılmış raporlar üzerinden tartışmalarda bulunarak aslında bilimin nasıl suiistimal edildiğini sizlerle paylaşmak istiyorum. Bu sayede her konu da olduğu gibi 'Linç Kültürünün' bize ve devlete nasıl bir hasar verdiğini anlatmak istiyorum.

Tekrar ve tekrar söylüyorum; amacım belirli bir kişi yada grubu hedef göstermek değil ama ByLock uygulamasını sanki kendisi/kendileri yazmış ve her yönüyle konuya hakim olmuş gibi bilim adamı olmayan kişi yada kişilerin 'ByLock Tespitleri ve Yargılamaya Etkileri' başlıklı bir yazıyı kaleme aldıklarını görmek beni gerçek anlamda derinden üzmektedir. ByLock yargılamasının belirsizliklerle dolu olduğunu ifade eden 'MİT Raporuna İnceleme Raporu' adı altında sürekli olarak devleti şaibe içerisinde göstermeyi hedefleyen dokümanlar internet ortamında dolaştığından, bu yazı içerisinde son yayınlananlardan bir kaçını tarafsız bir dille ele almak istiyorum.

Konuya taraf oldukları anlaşılan kişilerce yazılan son raporlara bakılacak olursa; konu, hukuki ve teknik boyuttan oldukça uzaklaşmış durumdadır. Gerçekten konuya çok hakim olması gereken kişilerce yazılması, çizilmesi ve tartışılması gereken çok sağlam bir bilgisayar ağları ile telekomünikasyon mühendisliği, bilgisayar bilimleri ve mühendisliğinin kabiliyetlerini gerektiren konularda, hangi lisans dalından mezun oldukları belli olmayan, eğitimlerini nereden aldıkları belli olmayan internet kafe işleterek mi adli bilişim uzmanı oldukları anlaşılamayan, bir de üstüne kendilerini dünyada adli bilişim otoritesi olarak gören kişilerin saydığım yeteneklerde rapor vermeleri doğru değildir.

Burada olması gereken, bu ülkenin yetiştirdiği çok değerli bilim insanlarına başvurulması zorunluluğudur. Belli ki bahsettiğim taraf olan kişilerin görmezden geldikleri bir husus bulunmaktadır, kendileri de bazı konuların bilincinde değildir, görmezden gelmektedir veya teknik çizgiden uzakta kendilerine söylendiği gibi hareket etmektedir. Ülkemin sayısız akademisyeni bugüne kadar görülen tüm bilişim suçu davalarında birey ve heyet olarak sayısız kereler mahkemelere rapor, ek rapor ve

mütalaa vermiş ve vermeye devam etmektedir. Bugüne kadar ByLock veya herhangi bir bilişim suçuyla ilgili kapıma her kim geldiyse her kim bana ulaştıysa onlara hiçbir maddi kaygı gözetmeden yardımcı oldum ve olmaya devam ediyorum. Böyle bir tablo içerisinde kendini bilime adamış insanların değil de algı yöneticilerinin ülkemin kurumlarını siyasileştirmelerini ve bundan nemalanmalarını hazmedemiyorum.

Ayrıca, bilirkişi makamı yaptığı iş dolayısıyla bir kamu görevlisidir, bir diğer ifade ile görevini ifa ederken aslında kamu görevlisi olmasa bile bilirkişilik yaparken kanun kişiyi kamu görevlisi olarak kabul etmektedir. Dolayısıyla akademisyen olsun veya olmasın, düşünce özgürlüğü içinde, listeye kayıtlı olsun yada olmasın bilirkişi şartlarına haiz veya kendini haiz gören her tarafsız bireyin kendisine verilen sorumluluğu da gerçekten bağımsızlık ve adalet ilkelerini gözeterek kamu vicdanına bağlı kalarak bilimsel gerçekler ışığında yapması büyük bir önem taşımaktadır.

Gerçek olmayan bilgiler ile toplum nazarında bir algı operasyonu yapmak için Disinformation ve Misinformation kavramlarının uygulanması gerekmektedir. Disinformation sahte bilgileri, Misinformation ise eksik bilgileri ifade etmektedir. Kişilere öncelikli olarak gerçek bilgilerin bir kısmını sunmak kalanı ise sahte bilgiler ile tamamlamak en sık kullanılan algı yönetme tekniklerinden birisidir. Bahsi geçen raporlarda şu şekilde yapılmaktadır. Örn: İlgili raporun bir sayfasında "*27 Aralık 2017 tarihinde Ankara Cumhuriyet Başsavcılığınca 11.480 kişinin iradeleri dışında ByLock sunucularının kullandığı IP'lere yönlendirildiğinin tespit edildiği açıklaması söz konusu tespitimizi doğrulayan bir husustur."* cümlesine yer verilmiştir. İçinde geçen tüm bilgiler doğru ama eksiktir; arkasından gelen "*Kamuoyunda Morbeyin uygulamaları veya ByLock zokası olarak bilinen tuzaklar bitmemiştir ve geride hala çok sayıda mağdur olduğu değerlendirilmektedir*." cümlesi ise eksik verilen bilgiyi tamamlayan sahte bilgi cümlesidir. Kişilerce hatalı veya kendileri tarafından da doğrulanması teknik açıdan bir diğer ifade ile bilimsel kıstaslar ile mümkün olmayan ifadeler gerçek bilgi içeren cümlelere eklenerek algı yönetimi yapılmaktadır. Kamuoyu hatalı bir şekilde yönlendirilerek devlete duyulan güvenin ve sevginin ortadan kaldırılması amaçlanmaktadır.

Çoğunlukla devletin yaptığı işlere şaibe katmayı amaçlayan raporlar içerisinde gördüğüm husus teknik detayları, kanunları, farklı farklı teknik bilgileri ve unsurları bir araya getirerek karmaşa yaratmak ve okuyucuları sonuç bölümüne yönlendirerek "bakın 60 sayfa anlattık işte şu 2 sayfayı okursanız" her şey oturmuş olur fikrini yansıtmaktır. Ben böyle yapmadan raporlarda sunulan büyük resmi görerek devam etmeyi daha doğru buluyorum. Bahsi geçen algı raporlarında beni yani bilimi ilgilendiren

bölümler şöyle sıralanabilir; sayısal delil, veri kaynağı, zaman damgası, özetleme algoritması, üst veri, VPN, NAT kayıtları ile bugüne kadar NAT teknik olarak yeteri kadar sorgulanıp elle tutulur bir husus bulunamadığından son raporlarda karşımıza çıkmaya başlayan Deterministik NAT'lı CGNAT sistemi ve problemleridir.

Bu algı raporlarını yazan ve hedeflerinde MİT tarafından kaleme alınmış ByLock raporu olan kişilere prim vermemek adına yazdıkları raporlardan çok sayıda alıntılar yapmak yerine bilimsel olarak ölçülebilir tespitlerim üzerinden gitmek istiyorum. Yazımı halkın her kesimine hitap eder nitelikte yazmak istiyorum ancak bilim insanı yolunda olan biri olarak şuna değinmeden geçmem mümkün değildir. Söz konusu raporların yazarları telekomünikasyon mühendisliği alanında yazılmış Deterministik NAT-CGNAT kavramını anlatan rehber dokümanı (RFC) yazı içerisinde vermişlerdir. RFC7422 olarak ifade edilmiş ve yayın tarihi Aralık 2014 senesidir. Ancak, ilgili algı raporu içerisinde F5 firması adında AVEA'ya bazı sistemler satmış bir firma 23 Temmuz 2013'te yayınlanan ve 13 Mart 2017'de güncellenen "*CGNAT Sanal Sunucuları için Deterministik NAT Adres çevrimlerinde hata olabilir*" şeklinde kendi yazdığı sistemler için bir bug kaydı oluşturmuştur. Algı raporunu kaleme alan içlerinde ne bir telekomünikasyon mühendisi ne bir akademisyen ne bir GSM operatörü ne de teknik ve bilimsel altyapısı olan kişiler, ne de Türk operatör sistemlerinin F5 firmasıyla teknik altyapı ve iş ilişkisine hâkim olmayan kişilerden oluşan heyet, dünyanın en zorlama yargısına ulaşarak "*Özetle, F5 firması demektedir ki, bahsedilen koşullar gerçekleştiğinde sistemde bir problem (bug) oluşur ve yanlış eşleştirmeler olabilir. Bunun da anlamı açıktır. Genel IP Adreslerinden Özel IP Adreslerine yapılan çevrimlerde, hatalar oluşabilmektedir.*" demişlerdir. İşte bilimin de tekniğin de gerçekliğinde bittiği nokta, tüm raporun özeti ve ne kadar saçma ve mesnetsiz iddiaların olduğu tek bir cümlenin içinde saklıdır. Bir sistemde oluşabilecek ve "bug" diye tabir edilen standart dışı bir çalışmadan koca bir dünya yaratılmıştır. Bunun nedeni tartışmamın ilerleyen bölümlerinde verilecektir.

Elbette yazımı burada bırakarak algı raporcuları gibi polemik ortamı yaratmak doğru bir davranış olmayacaktır. İnternet ortamında dolaşan algı raporlarında geçen çoğu ifadenin üzerinden teknik olarak geçmek gerekmektedir.

Raporların bazı bölümlerinde IP adresinden suçluya gitmenin mümkün olmadığı ve tüm dünyada tartışmalı olduğu vurgulanmaktadır. Bu doğru değildir hatta yalandır. Hiçbir teknik ve bilimsel karşılığı yoktur. IP adresi gerçek veya NAT'lanmış olsun, noktadan noktaya iletişim için gerekli olan en temel hukuki delildir. Bugün dünya geneline bakıldığı zaman siber suçlar ile mücadelede ilk tespit ve dayanak noktasıdır. Suçluya

direkt olarak işaret etmediği söylenen durumlar, akıllı telefonları değil sadece masaüstü ve dizüstü gibi bilgisayarlardan yapılan işlemlerin bir kısmı için söylenebilir. Bir hane içerisinde kullanılan modem bağlantısı, bir IP adresini hane içerisindeki bilgisayar, tablet, telefon vb. cihazlara NAT üzerinden kullandırmaktadır. Hane içerisinde kullanılan bir bilgisayarı kimin kullandığını tespit etmek inkar korumasına başvuran suçlular için teknik tespitin yapılmasında çözümsüzlük yaratmaktadır. Ancak ByLock davalarında örgüt üyeliği ile suçlanan kişiler ByLock uygulamasını bilgisayarlarından değil kendi şahsi cep telefonları üzerinden kullanmaktadır. Hane içerisinde ve dışında kişiye ait telefon ile yapılacak özel yazışmaları hanenin başka bir üyesinin yapması hayatın olağan akışına aykırı olduğu için IP adresinden hattın kayıtlı olduğu kişiye, bu kişiden ise suçluya ulaşmak teknik açıdan anlamlı ve mümkündür. Bu hane içerisinde kullanılan DSL modemlerden elde edilen verilerin açıklamasıdır, BTK tarafından elde edilen IP adresleri ise direkt olarak akıllı telefon, operatör, NAT vb. kaynaklardan elde edilmiştir. Dolayısıyla bu şekilde elde edilen IP adresleri internet bağlantı paylaşımının olabileceği hane ortamının dışında olduğundan IP adresinin kişinin şahsına ve özel kullanımına ait hangi cihaz ile eşleştirildiği bilgisi tartışılmaz bir örgüt üyeliği delilidir.

Algı raporunun bir bölümünde AVEA ve o tarihte Türkiye'de mevzuat gereği henüz kullanılmayan Deterministik NAT kapasitesi kullanımıyla alakalı bir bölüm göze çarpmaktadır. Yazarların, İngilizce dilini hatalı bir şekilde ele almalarından dolayı sanki D-NAT sisteminin AVEA tarafından kullanıldığı tarzında bir anlam oluşmaktadır. Ancak yazının orijinalinde "Another feature that Avea benefits from is F5's deterministic NAT capability." denmektedir. Bir diğer ifade ile hatta Google Translate ile de "Avea'nın fayda sağlayacağı bir diğer özellik ise F5'in Deterministik NAT yeteneğidir." denmektedir. Dolayısıyla AVEA'da kullanıldığı anlaşılan sistemin D-NAT özelliğinin de olduğu, bu özelliğin AVEA'ya fayda getireceği, ancak kullanılıp kullanılmadığına yönelik bir yorumun olmadığı görülmektedir.

Bir de şu açıdan değerlendirirsek A firmasının ürettiği bir ürünün bir kurum tarafından kullanıldığını ve A firmasının bunu öven hem haber hem reklam niteliğinde bir yazı kaleme aldığını düşünelim. A firması, bakın kurumun şöyle yetenekleri de var mı olarak yazar yoksa bu yetenek sayesinde kurum şöyle kazandı böyle gelişti olarak mı yazar. Keza yazı içerisinde sistemin güvenlik (DDoS) koruması ile ilgili bir özelliğini firma şu şekilde ele almaktadır; "Avea was pleased to employ this functionality to help it protect its critical network and deliver an optimal service for customers." Google Translate karşılığı "Avea, bu işlevselliği kritik ağını korumasına ve müşteriler için en uygun hizmeti sunmasına yardımcı olmaktan memnuniyet duymuştur." denilmektedir. Bir diğer ifade

ile; şayet AVEA, F5 firmasının D-NAT özelliğini aktif halde kullanıyor olsaydı firma bunu aynı DDoS önleme özelliği gibi reklam malzemesi yapmak için kullanırdı. Ancak görüyoruz ki F5 firması AVEA'ya sattığımız sistemde D-NAT özelliği de var gelin sizin firmaya da bu gelişmiş sistemi satalım demek istemiştir. Aynı şekilde F5 firmasının haberi içerisinde şöyle denilmektedir. "VIPRION also helps Avea to ease its transition to IPv6 by supporting both IPv6 and IPv4 protocols simultaneously." Google Translate karşılığı "VIPRION, Avea'nın aynı anda hem IPv6 hem de IPv4 protokollerini destekleyerek IPv6'ya geçişini kolaylaştırmasına yardımcı oluyor." denilmektedir. Bir diğer ifadeyle; algı raporuna göre D-NAT neyse bu cümle de aynı yapıda olduğundan algı raporcularının mantığına göre AVEA IPv6 kullanmaktadır anlamı oluşmaktadır. Ancak 2018 senesinde dahi henüz AVEA, IPv6 adreslerine geçiş yapamamıştır. Bu demek değildir ki AVEA sistemleri IPv6 uyumlu değildir. Bilakis uyumludur ama o yetenek 2018 tarihinde dahi kullanılmamaktadır.

AVEA, D-NAT özelliğini veya IPv6 özelliğini kullanıyor olsaydı o iş ürün tanıtımının ötesine geçer, F5 firması bunu hunharca reklam malzemesi yapmak için haberler yayınlıyor olurdu, başka ülkelere ve GSM operatörlerine bu sistemi ve yeteneklerini anlatan bloglar hazırlardı, kısaca ticaret neyi gerektiriyorsa öyle davranırdı. Mevzuat o tarihte buna izin vermezken AVEA'nın D-NAT özelliğini kullandığına kanaat getirmek algı raporunda yer alan çok zorlama bir çıkarımın ötesinde delilsiz yalan/yanlış bir ifadedir. Yazı içinde geçen bölüm güvenlik log kayıtlarıyla ilgilidir ve kullanılan güvenlik sistemiyle ilgili haberden sonra AVEA'nın kazanımları, adli bilişimcilerde bir sistemin güvenlik sorunları nedeniyle para kaybedeceğini bilmektedir.

Bu sayede algı raporlarında iddia edilen AVEA'nın ByLock kullanılan tarihlerde Deterministik NAT kullandığına yapılan atıfların bir firma tarafından yapılan reklam malzemesi olarak kullanılan bir ürün tanıtımına dayandırıldığı ve bu özellik üzerine kurulu tüm senaryoların çökeceği anlaşılmaktadır. Zira, algı raporlarında bahsi geçen NAT ve CGNAT sistemleri üzerine ByLock kullanıcısı örgüt üyelerini aklama senaryoları; AVEA'nın Deterministik NAT özelliğini aktif olarak kullandığı üzerinedir. Ancak AVEA bu yetenekte sistemlere sahip olsa da D-NAT özelliğini kullanmamıştır.

Bir an için D-NAT-CGNAT sisteminin kullanıldığını ve algı raporunda bahsedildiği gibi F5 firması tarafından AVEA'ya satılan sistem üzerinde bir bug (istenmeyen durum) oluştuğunu varsayalım. Bu hususu anlamak için öncelikle bug dediğimiz; hata ortaya çıkartabilecek yazılımsal yada donanımsal aykırı durumu anlamak gerekmektedir. Bug olarak tabir edilen durum sistem ilk tasarlandığı anda değil sistem kullanılmaya başlandıktan sonra aşırı yüklemelerde, korsanlarca yapılan saldırılar neticesinde, yeni

gelişen donanımlara uyum noktasında, normalde sistemden beklenmeyen bir davranışın yönetici tarafından sisteme girilmesi sonucu oluşan durumlarda sistemin çalışmasını engelleyen veya hatalı sonuçlar üretmesini tetikleyen durumların genel adıdır. Bu nedenle, sistem ilk tasarlandığı zaman ne iş yapması gerekiyorsa ona göre tasarlanır üzerinde bug yoktur denebilir çünkü standart bir kullanımda sistem tamamen bug-sızdır ve tasarlandığı işi kusursuz bir şekilde yapmaktadır. Diğer türlü olsaydı temel kullanım için bir ürün seçtiğinizde kimse bug'lı ürünü yani yaptığı standart işlem sonucunda hatalı sonuçlar üreten sistemleri satın almak istemezdi. Bug'lar genel olarak müşterinin sistemden beklentilerinin ürün geliştiricilerince öngörülemediği hallerde ortaya çıkmaktadır.

Algı raporu halkın aklında yanlış bir akış şeması oluşturmak için hep örnekler üzerinden gitmiştir, bende sizlere şöyle bir örnek vereyim. Araba sizi A noktasından B noktasına taşımak için tasarlanmıştır. Araba lastikler üzerinde gider ve her lastik her araca takılamaz, bizler için en önemli unsur aracın ve parçalarının kaliteli ama ucuz olmasıdır. Aracı aldıktan sonra kış mevsimine kadar sorunsuz kullandınız. Kış lastiği alacağınız zaman 195/55R16 lastiğin 600 TL 205/55R16 lastiğin ise 300 TL olduğunu gördünüz. Bunu hangi lastikçiye sorarsanız size 195/55 lastiğin ara ölçü olduğundan çok pahalıya geldiğini söyleyecektir. Sizde insani bir durum olarak 205 taban olan lastiği aldınız, arabanın jantları bu lastiği kabul etti ve kullanmaya başladınız. Ancak arabanın yol bilgisayarının ayarları 195 taban lastik için yapılmış olduğundan sizin standardın dışında bir lastik takmanız yol bilgisayarının hatalı okumalar yapmasına sebep olmaya başladı. Hız ibresi normalde 100 KM/Saat gösterirken standart dışında taktiğiniz lastik nedeniyle gerçek hızınız 102 KM/Saat olmaya başladı. İŞTE BU BİR BUG'dır. Bir diğer ifade ile standardın dışında yaptığınız her kullanım sistem de bir BUG oluşmasını tetikleyebilir veya sistem bunu görmezden gelerek sorunsuz çalışabilir. AMA STANDART kullanımda sistemde BUG oluşmaz. Bu tip BUG'lar sistem henüz satış reyonuna konulmadan yapılan testlerde düzeltilerek son ürün üzerinde ortaya çıkmaması için çalışılır. Diğer türlü son ürün stabil olmaz ve kimse satın almak istemez. Sıfır aldığınız aracın muayeneden geçemediğini hayal edin, o aracı iade edersiniz.

Algı raporunda F5 firmasının CGNAT'ta ortaya çıkan BUG tarifinde AVEA'nın hiç kullanmadığı bir özelliği kullandığı ve bunu da standart dışı şekilde kullanmış olduğundan yola çıkılarak şu ifadeye yer verilmiştir. "*Genel IP Adreslerinden Özel IP Adreslerine yapılan çevrimlerde, hatalar oluşabilmektedir. bir IP'nin gerçekte kime ait olduğu Avea'ya sorulduğunda, Deterministik NAT sisteminde oluşabilen çevrim hatalarından ötürü, Avea yanlış kişileri ByLock IP Adresi ile eşleştirebilmektedir."* denilmektedir.

Algı raporunun bazı bölümleri şaka gibi sürmektedir; sürekli Europol yani Avrupa Polis Teşkilatı raporlarına atıf yapılan sayfalar konulmuştur. Deterministik NAT-CGNAT özelliği daralan IP Versiyon 4 uzayı nedeniyle IP Versiyon 6 uzayına geçiş sırasında yaşanacak sorunları minimize etmek amacıyla RFC7422 ile önerilmiştir. Dünya üzerinde bulunan hiçbir sistem yöneticisinin bir anda bir başka yöntemi kullanmaya geçmesi hadi sil baştan bu özelliği kullanmaya başlıyoruz demesi mümkün değildir. Bu geçişin yumuşatılması maksadıyla önerilen Deterministik NAT sistemlerine de RFC dokümanı içerisinde 2014 senesinde yer verilmiştir. Dolayısıyla bir operatörün 2014 yılında hadi bu sene bunu kullanmaya başlayalım tüm sistemleri kaldıralım demesi de ne teknik ne de mali anlamda mümkün ve mantıklı değildir. Avrupa Birliği operatörleri dahi Deterministik NAT sistemini yeni yeni kullanmaya başlamıştır. Buna paralel olarak Europol endişesini dile getiren yazıları henüz 2017'de yayınlamıştır. Tarihler belgeleriyle internet ortamında mevcuttur. Amaç sürekli bahsettiğim doğru bilgileri takip eden hatalı bilgiler ile algı yönetimi yapmaktır. Ama öyle bir şey yazılmıştır ki ne mahkeme kayıtlarında ne MİT raporunda geçen bir ifade önümüze çıkmaktadır, sanki birileri oraya özel olarak ekletmiş yazarlarda verilen emir gereği oraya bu ifadeyi yazmışlar gibi, şöyle denmiştir "*bu sistemlerin kayıtlarını tek başına yeterli delil olarak kabul etmemiz büyük bir problemdir*." Yargısı eklenmiştir. Madem tek delilin bu olduğu ortaya çıkmış durumda ki o durumda mahkeme evraklarında D-NAT kullanan CGNAT ile elde edilen kayıtlar adında bir bölüm olması gerekirdi o halde algı yönetmenlerinin sundukları yalanlara da gerek olmazdı. BTK tarafından mahkemelere gönderilen tüm kayıtların, tüm tarihlerin, dökümlerin, IP adreslerinin hepsinin gerçek ve tutarlı olduğu açıktır. Zira, algı raporculari D-NAT kullanan CGNAT yoksa her şey tamam demişlerdir. Bunu keşke 60-70 sayfa safsata rapor yazmadan tek bir sayfada tek bir cümle olarak vermiş olsalardı. O zaman halkın devletin ne kadar haklı olduğunu anlaması kolaylaşırdı.

Bu sözde adli bilişimci arkadaşların yazdığı ama daha önce de değindiğim gibi adli bilişim tutarsızlıkları olduğundan yazarlar harici kişilerinde kaleminin dokunduğu belli olan yazı içerisinde öyle bir bölüm var ki insan nasıl olur da teknik detaylar böyle çarpıtılabilir anlamıyor.

Bahsettiğim kısım elbette kayıtlarda yer alan tarih ve saat bilgileridir. Her adli bilişimci mesleğe başladığı ilk andan itibaren zamanın ne kadar önemli bir delil olduğunu bilmektedir. Türkiye'de ve dünyada neredeyse her adli bilişim bilirkişisi siber suçlar kapsamında kendisine ev yada işyeri internet IP adresi bağlantı dökümlerinin, E-Posta dökümlerinin, SMS ve Çağrı dökümlerinin vb. sayısız sayfalarca farklı dökümlerin nasıl elde edildiğini ve nasıl analiz edilmesini gerektiğini öğrenmektedir. Saat farklarından suça konu olan eylemi gerçekten sanık mı işlemiş yoksa aynı saat içerisinde farklı bir hesap mı bağlantı yapmış bunu anlayabilmektedir. İlk defa ByLock'ta bir adli bilişimcinin yaptığı işten şüphe duyulmasını sağlamaya çalışma girişimi görüyorum. İnternete bağlanan tüm sistemler ki ticari sistemlerin %95 kadarı UNIX işletim sistemi tabanlıdır. Ayrıca, UNIX veya WINDOWS fark etmez, tüm bağlantı sistemleri aralarındaki tarih, saat, dakika ve saniye koordinasyonunu sağlamak zorundadır. Bu nedenle NTP dediğimiz protokol geliştirilmiştir. NTP üzerinde çalışan tüm sistemler dünya atom saatine göre senkron edilir. Bugün uçaklar düşmüyor trenler çarpışmıyor ve bugüne kadar siber suçluların IP adreslerinden kullandıkları hatlar tespit edilebiliyorsa hepsi NTP sayesindedir. Algı raporunda yaz saati uygulamasından Windows Server 2016'da NTP gecikmelerine kadar sayısız safsata yazılmıştır. O ifadeyi kullanmak istemiyorum ama tüm dünyada sistemlerin NTP ile zaman senkronlaması sorunu olduğunu ifade etmek cahilliktir. Yaz saatine geçtiğimizde uçağımızı nasıl kaçırmıyorsak, 5 dakika önce aynı raydan geçen trene nasıl çarpmıyorsak, dünyanın öbür yanında olan maçı nasıl canlı izliyorsak NTP'den dolayı "*Zaman Damgası hatası olur kişiler doğru tespit edilemez*" demek, ne Türkiye'de ne dünyada bilişim suçunun delili olmaz demekle aynı şeydir. Bunlara kesinlikle itibar edilmemeli, bilimden ve fenden uzaklaşılmamalıdır. İşin üzücü tarafı ise algı raporunun ilgili bölümü gerçek bir ifade ile bitirilerek "*Fakat bütün bu problemlerin yanında, ByLock gibi FETÖ üyelerinin tespitinde ve örgütün çözülmesinde büyük rol oynayan bir bulgunun göz ardı edilmesi de doğru değildir*." Denilmektedir. İşte size çok kullanılan bir algı yönetme tekniği daha sunuyorum; gerçek bilgi, yalan bilgi, gerçek bilgi verip arada geçen yalan bilginin doğru kabul edilmesini sağlamaya çalışmaktır. Keşke kendisine adli bilişim uzmanı diyebilen arkadaşlar burada bahsettikleri bulgu hakkında dokümanlar oluşturup inceleme raporları yazabilselerdi. ByLock kim tarafından yazılmış kaç kullanıcısı varmış kimler buraya bağlanıp vatan haini olmuşlar bunlar hakkında da senaryoları ve gerçekleri

yazabilmeleri önemlidir. Ancak ısmarlama algı raporları ile halkı devlete karşı kullanamayacaklarını, bu işin olmayacağını anlamaları da şarttır.

Algı raporlarına genel olarak bakıldığında yukarıda bahsi geçen bilimden, fenden ve o tarihlerde mevcut mevzuattan uzakta zorlama iddialar ile hazırlanan sözde teknik senaryolar MİT raporuna atıfta bulunarak doğrulanmaya çalışılmaktadır. CGNAT ve Deterministik NAT ile ilgili senaryoları teknik olarak yukarıda çürütüldü. Ancak algı raporları içerisinde kablosuz internet ortak kullanımı ve paylaşımı başlıklı bir bölüm de bulunmaktadır. Bir adli bilişimcinin senaryolar üzerinden konuyu her yönüyle tartışmak varken daireler interneti paylaşırsa herkes aklanır demesi bilimsel olmadığı kadar komik ve cahilce bir yaklaşımdır. İnternetin paylaşıldığı iddia edilen daireler arasında da kişi sorguları gerçekleri kısa sürede ortaya çıkartacaktır. Bu ByLock değil çocuk pornosu da olabilirdi. Zaten yıllardır benzer suçlar davaların konusu olmakta, yargılamalar ve cezalandırmalar da sorunsuz yapılmaktadır.

Çok tartışılan başka bir senaryo ise 2 hane arasında paylaşılan internete veya sadece tek bir hanede bulunan internete 3. bir kişinin ortadaki adam saldırısı veya şifre kırma yöntemleri ile girmesi durumudur. Bu durumun gerçekleşmesi için 3. Kişinin saldırı için hedef seçilen haneye ait kablosuz modem şifrelerini yani WPA2 gibi şifreleme tekniklerini kırması gerektiğinin bilinmesi gerekir. Bu yöntem 5 dakikalık bir süreç değildir. Şifre kırabilen özel işletim sistemleri, bu konuda ciddi bir teknik bilgi ve deneyim gerektirmektedir. Zaten şifrenin kırılması ve sonrasında modeme yakın olunması gerektiğinden ByLock'cuların apartman apartman gezip bozacı gibi kamu personeli oturan hane aradığını düşünmek safsatadır. Bir ByLock'cunun tanımadığı kamu görevlisinin internet hattını kırarak o hane içerisindeki kişilerin internetinden ByLock kullanmasını düşünmek hayatın olağan akışına aykırıdır. Ayrıca 7-8 katlı bir apartmanda katlarda gezinerek yapılması da gerekebilir. Bu yöntemle giren olmuşsa bile zaten GSM hatlarından elde edilecek lokasyon bilgilerinin eşleştirilmesi şifre kırılıncaya kadar geçen sürede 3. Kişileri ortaya koyacaktır.

Sonrasında ise mahrumiyet bölgelerinde asker ve polislerin hotspot ile internet paylaşımı yaptığı iddiası yer almaktadır. Adli bilişimci arkadaş maalesef kağıt üzerinde düşünerek sebep-sonuç ilişkisi kurmuştur; gerçek olana baktığımızda operatörler asker, polis ve genel olarak kamu personellerine yüksek konuşma, mesaj ve internet paketli genellikle aile bazlı kampanyalar yapmaktadır. Aynı coğrafi bölgede yaşayan polisin ne kadar mahrumiyeti varsa interneti o kadar mahrum kullanabilir. Zaten mahrum kullanabildiği interneti hotspot yaparak aynı internet paketine sahip arkadaşıyla paylaşması mantıklı değildir. Burada mahrumiyet kavramı da açık değildir.

Dağ da operasyonda zaten kimsenin telefonu çekmeyecektir. İlçe de karakol da bir kişinin telefonu çekerken diğeri de çekecektir, neden insanlar hotspot yapsınlar. Ayrıca hotspot telefon şarjını çok hızlı bir şekilde tüketen bir özelliktir. Mahrumiyet bölgesinde aynı operatör paketine sahip 2 veya daha fazla sayıda kişi neden hotspot yaparak telefon bataryasını bitirsin, sonra arkadaşı ailesiyle görüşürken o da bitmiş bataryası ile cephe de düşman mı gözlesin. Dolayısıyla şu söylenebilir, devletin polisi internet paketi alamayan çoban arkadaşa hotspot yaparak internete çıkartmış, bu tamamdır. Ama aynı polis aynı asker aynı operatör aynı internet paketi aynı batarya aynı karakol kısaca aynı mahrumiyet bölgesi içinde olan kişiler neden hotspot yaparak internet paylaşsınlar, algı operasyonu yapan arkadaşların dediği gibi oraya "*oldukça yaygın olduğu da bilinen bir başka hususdur*" yazmakla olmamaktadır. Hotspot iddiası silahlı terör örgütü üyelerince hemen kullanılan bir argümandır. Esasen hotspot iddiaları 3 gün kuralı sebebiyle ekarte edilmektedir. Bu şekilde ByLock kullanıldığı düşünülürse paylaşımın kimin interneti üzerinden yapıldığı ve bu kişinin hotspot yaptığı kişilerin belirlenmesi kolay bir süreçtir.

Algı raporcularının dediğine göre kamuoyuna ortak internet kullanımı nedeniyle çok sayıda kişinin ByLock kullanıcı listelerinde olduğu yansımıştır. Yalanın ve iftiranın bir dozu olmalıdır. Ben araştırdım kamuoyuna bilim ve fen ışığında yansıyan bir tane olay bulunmamaktadır. Keşke onlar da ısmarlama rapor yazarken iddialarını gerçekten araştırarak yapmış olsalardı karanlıkların olmadığını her konunun aydınlık olduğunu göreceklerdi.

Bir başka iftira ise "*cep telefonlarının mobil erişim noktasının etkin hale getirilmesi, yani WiFi-HotSpot özelliğinin açılması durumunda, internete bağlantı kuran diğer cihazların tespiti çoğu zaman mümkün olamamaktadır*." denilmektedir.Türkiye'de sınırsız data paketli internet olmadığından telefon ister hotspot yapsın ister direkt interneti kullansın önemli değil ama sanmayın ki telefonunuzun hotspot yaptığı anlaşılamıyor, buna özgü analiz yöntemleriyle hotspot yapanlara dair tespit ve değerlendirmelerde bulunulabilmektedir. O sebeple burada detay çok bilinmediğinden halkı kandırmaya gerek yok, hotspot yapıldığı teknik olarak anlaşılabilir.

Ancak yukarıda tartıştığım gibi benimle aynı mahrumiyet bölgesinde olan ve benimle aynı internet paketi yani kurum hattı, kamu aile hattı olan arkadaşıma neden bataryamı su gibi içecek hotspot yapma ihtiyacım oluşsun yargısı hayatın olağan akışına aykırıdır, zaten bu husus algı raporcularının cevap veremediği, delil göstermeden kabul ettikleri bir durumdur. Dolayısıyla bu husus üzerinden şahsın değil de hotspot yaptığı arkadaşının ByLock kullanıcısı olması da şahsın suçunu örtbas etme çabasından başka bir şey değildir.

Algı raporunun bir bölümünde ise VPN (Sanal Özel Ağ) sistemlerinden bahsedilmektedir. VPN sistemleri ve yöntemleri bilişim suçlarının çözülmesinde ve suçluya ulaşmada çok büyük bir engeldir. Bağlantı gerçekleştirmek isteyen IP adresi VPN bağlantısı kullanması halinde suçun işlendiği uzak bilgisayar sisteminde kişiye GSM Operatörü veya ADSL IP adresi değil hangi VPN sistemine bağlantı kurulduysa o VPN sunucusunun IP adresini göndermektedir. Dolayısıyla, suçun işlendiği uzak bilgisayar üzerinde suçu işleyen şahsa ait gerçek IP adresine dolayısıyla gerçek şahsa ulaşmak kullanılan VPN kayıtları incelenmeden mümkün olmamaktadır. Bir senaryo ele alırsak bu yazıyı yazdığım ve evde adıma kayıtlı Türk Telekom ADSL hattım üzerinden bir bankanın bilgisayarına korsanlık yöntemleriyle sızmaya çalışırsam banka benim IP adresimi mahkeme yoluyla Türk Telekom üzerinde sorgulayarak bana kısa sürede ulaşabilir. Ancak evde adıma kayıtlı Türk Telekom ADSL hattım üzerinden önce ABD'de olan bir VPN bağlantısı açar ve açtığım VPN üzerinden bir bankanın bilgisayarına korsanlık yöntemleriyle sızmaya çalışırsam banka benim IP adresimi değil ABD'de bir VPN firmasına ait IP adresini görecek ve dolayısıyla ABD'de faaliyet gösteren VPN firmasının tuttuğu kayıtlara erişmeden benim Türk Telekom ADSL IP adresime erişemeyecek bir diğer ifade ile bana ulaşamayacaktır. Ancak, çeşitli sebeplerle bağlantının kopması anında, aboneye ait IP bilgileri operatör kayıtlarına yansımaktadır

ByLock için durum daha farklıdır. Mahkemelerde ByLock'cuların VPN kullanmış olduklarına dair bir delil bulunmamaktadır. Ancak algı raporcuları VPN kullanmış olabileceklerini ifade ederek bunu hatalı bir şekilde MİT raporuna bağlamaktadır. VPN konusunda iddia, ByLock yazılımını işleten kişilerin MİT raporuna göre VPN güvenlik katmanının örgüt genelinde uygulanması için Ortadoğu kisvesi altında Türkiye IP adreslerini engellemeleri sonucu tespitlerin nasıl yapıldığıdır. MİT raporunda yazıldığı üzere 15 Kasım 2014 tarihinden önceki log kayıtları silinmiştir ancak IP bloklarının kiralık sunuculardan engellenmesi için kullanılan blok atama log kayıtları erişilebilir durumda kalmıştır. Engellenen IP blok adresleri ise halihazırda MİT raporunun ekler bölümünde sunulmuştur. ByLock uygulamasını yönetenler Türkiye IP adreslerini toplu halde engellenmeye çalışmışlar ancak Türkiye'de kullanılan çok sayıda IP bloğunu engellemek zor olduğundan uygulamanın sadece VPN üzerinden erişilebilmesi noktasında başarısız olmuşlardır.

Mahkemelere sunulan ByLock raporlarından VPN kullanan şahıslar arasından Bylock kullanıcısı tespitinin bulunmadığı görülmektedir. Dolayısıyla VPN kullandığı için ByLock kullanıcısı olmakla suçlanan hiç kimse bulunmadığı anlaşılmaktadır. VPN kesilme anında uygulamaya VPN siz gitme girişimin bağlantı verilerine yansımıştır.

Algı raporlarında dikkate değer başka bir husus ise Kiralık Sunucu (Dedicated Server)'a ait IP adresi karmaşasıdır. İnternet dünyasında ticari maksatlı 2 tip sunucu kullanılmaktadır. Bir tanesine Kiralık Sunucu diğerine ise Paylaşımlı Sunucu denilmektedir. Kiralık sunucular müşteriler tarafından özel bir hizmet sunmak amacıyla tek bir sanal yada fiziksel bilgisayar olarak yüksek ücretlere kiralanırken, paylaşımlı sunucular genellikle web sitelerinin yayınlanması için aynı IP adresi üzerinden erişilen sunucu sistemleri olarak düşük meblağlara kiralanmaktadır. Kiralık Sunucu size aittir ve üzerinde bulunan tüm bellek ile işlem gücü gibi özellikleri yazdığınız uygulamalar için atanmıştır. Paylaşımlı Sunucu'da ise sisteme ait tek bir IP adresi, bellek ile işlem gücü herhangi bir anda o sunucu üzerinde faaliyet gösteren yüzlerce kullanıcı tarafından paylaşılmaktadır. Algı raporlarında Baltic Server bilgisayarlarının paylaşımlı sunucu olduğu algısı oluşturulmaya çalışılarak aslında ByLock'cuların başka bir siteye bağlanırken istemsizce ByLock IP adresine kayıtlarının düşmüş olabileceği söylenmektedir.

Bu husus teknik olarak mümkün değildir. Bir akış üzerinden gidilecek olursa; Paylaşımlı Sunucular tek bir IP adresi üzerinden İsim Sunucuları kullanarak (Name Servers) bir alan adına(domain) bağlanmak isteyen kullanıcıları paylaşımlı IP sunucusunda o alan adı için ayrılmış olan alana yönlendirirler. Böylece bizler farkında olmadan sahipleri farklı 2 siteyi ziyaret ederken aslında her iki site içinde aynı IP adresinin kullanıldığı gerçeği ile karşılaşabiliriz. Öte yandan siteye ait alan adını değil de IP adresini yazarak erişmeye çalışırsanız içinde mesela 2000 web sitesi olan sunucunun hata sayfası ile karşılaşırsınız çünkü siz alan adını değil de sunucuya ait tek IP adresini yazdığınızda sunucu firması sizi hangi alan adına yönlendirmesi gerektiğini bilemez. ByLock delillerine baktığımız zaman uygulamanın bir alan adına değil direkt olarak sunucu IP adresine bağlanmaya çalıştığını görmekteyiz. Örn: https://46.166.164.181:443 uygulama içinde bağlantı yapan adreslerden biridir. Bu, ByLock sunucusunun paylaşımlı olmayan bir sunucu üzerinde çalıştığını gösterir bir diğer ifade ile bunun bir Kiralık Sunucu (Dedicated Server) olduğunun teknik olarak ispatıdır. Yani 46.166.164.181 IP adresli sunucu üzerinde sadece ByLock uygulaması çalışmaktadır. Başka bir siteye bağlanmak mümkün değildir.

Dolayısıyla, algı raporlarında sunulduğu üzere ByLock IP adresinin bir başka sistem tarafından kullanılmış olabileceği fikri bilime ve fenne aykırıdır. Algı raporlarında bu husus üzerinde çok fazla durularak sürekli yalan, safsata ve konuyu teknik bakış açısından uzak tartışmalara çekerek ByLock uygulamasının kullanıldığı Kiralık Sunucu'yu Paylaşımlı Sunucu gösterme çabası ortaya konmuştur. Burada yalan denilebilecek yazıların adli bilişimci arkadaşlar tarafından alan adı, web barındırma ve alt sistemleri, paylaşımlı sunucu üzerinde tek IP adresinden sunucuda barındırılan diğer web sitelerine Reverse DNS Lookup yapmadan ulaşılamayacağı gibi konseptlere hakim olmadıklarından kendilerine gelen talimatlar doğrultusunda günü kurtarmak amacıyla yazdıklarını düşünüyorum.

ByLock uygulamasının bazı sürümlerinde IP adresi direkt olarak Kiralık Sunucu'ya işaret etse de bazı sürümlerinde domain adresine işaret etmektedir. Ancak, ByLock yazılımının hep aynı sunucu üzerinde faaliyet göstermiş olması, kullanımda 443 nolu tek bir portun kullanılmış olması aynı port aynı anda başka bir uygulamaya atanamayacağı için ByLock uygulamasının Kiralık Sunucu üzerinde faaliyet gösterdiğini kanıtlar niteliktedir. ByLock adreslerinde IP olduğundan teknik açıdan başka web siteleri ile karışabilecek paylaşımlı yapıda değildir. ByLock sunucuları ile bağlantı da olup bu nedenle hukuk önünde olduğunu düşünen kişilerin ByLock nedeniyle değil bunun silahlı terör örgütüne üyelik suçu için bir delil olmasından kaynaklandığını unutmamaları gerekir.

Algı raporlarıyla ilgili öngördüğüm teknik ve bilimsel bakış açısıyla derlenmiş hususlar şöyle sıralanabilir:

- Yazar veya yazarlarca ele alınan teknik detaylar ByLock kullanıldığı dönemlerde GSM operatörlerinde kullanılan yazılım sürümleri, NAT sürümleri, şebeke ve ağ mimarileri göz ardı edilerek teknik bilgiden yoksun ve sadece tahminler üzerine kurulu yazılmıştır, bilimsel olarak ispat edilemeyecek bir hususta varsayımlar ile tartışma ortamı yaratmak adli bilişim kıstaslarıyla bağdaşmamaktadır, Adli bilişim uzmanı kendisine teslim edilen adli emanete göre hareket eder, ben böyle öngördüm kesin öyledir mantığı kamuoyunu yanlış yönlendirmekten başka bir şeye hizmet etmeyecektir.
- Direkt alanım olmamakla birlikte ilgili tarihlerde mevzuat incelenirse şunu çok açık bir şekilde görebilirsiniz;
    - İşletmecilere ait NAT sistem kayıtları bir kopyası işletmecide kalmak üzere gerçek zamanlı olarak BTK'ya gönderilmektedir. Ayrıca NAT kayıtları oluştuğu sistemler üzerinde yöneticiler dahil olmak üzere tüm işlemler

zaman damgalı olarak saklanmaktadır. Dolayısıyla elle tutulur bir bilgi vermeksizin sadece varsayımlar üzerine hareket ederek tüm NAT mimarisini ve telekomünikasyon altyapısını sorgulamaya, dahası bu kurumlarda çalışan tüm personeli itham ederek istenilen kişilere ait istenilen kayıtların hukuksuz bir şekilde oluşturulabileceğine yönelik bir girişimde bulunmak doğru ve anlamlı değildir.

Sen nerden biliyorsun derseniz; 2009-2011 yılları arasında müşteri kurumun BTK olduğu Ulusal IPv6 Projesi Tasarımı ve Geçişi projesinde bulundum, aynı zaman da BTK ile 2006 yılından bu yana bu sene 11.'si yapılacak olan Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansını (ISCTURKEY) düzenliyoruz. Sizleri de yaptığımız etkinliklere bekleriz. Bu ülkenin STK'ları ve üniversiteleri, kendisini geliştirmeyi amaçlayan herkese açıktır. Bu bağlamda etkinliklerimizi de halkın katılımı için ücretsiz yapmaya devam ediyoruz.

Notlarıma dönecek olursak;

- NAT mimarisi sadece ByLock uygulamasının tespitinde değil her gün tüm dünyada sayısız operatör tarafından kullanılmaktadır. NAT mimarisinde yaşanacak bir güven bunalımı dünya genelinde bilişim suçlarının artık tespit edilemeyeceği veya sorgulanabileceği anlamına gelecektir. Anlaşılacağı üzere NAT mimarisi sadece Türkiye'de değil IP havuzunun tükendiği tüm ülkelerde sorunsuz bir şekilde çalışmakta ve halen siber suçlu tespitinde en güvenilir yöntemlerden biri olarak çalışmaktadır. NAT kayıtlarında ilgili operatör kayıtları ilgili müşteri ve bağlantı sağlanan IP adresi kayıtları ile eşleştirilerek suçluya ulaşılmaktadır. Dolayısıyla sadece dış IP adresleri üzerinden eşleştirilme yapılması ve tespit gerçekleştirilmesi mümkün olmadığı gibi ne MİT raporunda ne de mevcut mahkemelere sunulan kayıtlarda bundan bahsetmek algıyı yönlendirmekten başka bir şey değildir.
- Bildiğim kadarıyla GSM operatörlerinin şebeke içerisinde NAT donanımları NTP sistemiyle zaman senkronlu olarak çalışmaktadır. Dolayısıyla zaman senkronlaması ve buna bağlı ortaya çıkabilecek saat farkları yargılama içerisinde problem değildir. Bu sadece ByLock için değil bilişim suçu kavramı ilk ortaya çıktığı günden bu yana tüm dünyada suçlu tespitinde sorunsuz bir şekilde kullanılan bir yöntemdir. Bunun çalışmayacağını ifade etmek başta ABD yargı sistemi olmak üzere tüm dünyada bilişim suçlarında bu sistemin kullanılamayacağını ifade etmektir. Bunun ByLock'a kadar ve sonrasında sorunsuz çalıştığını bilerek sadece ByLock'a özel hatalar ortaya çıkmıştır varsayımının bilimsel ve teknik kabul görebilecek hiçbir şartı sağlamadığı anlaşılmaktadır.

Uzun yıllardır akademinin ve telekomünikasyon sektörünün içerisinde olan biri olarak algı raporlarını yazan kişilere kötü bir haberim bulunmaktadır. ByLock aboneliklerinin tespit edildiği dönemlerde operatörler tarafından Deterministik NAT özelliği kullanılmamaktaydı, arkadaşlarda güzel güzel açıklamışlar "*Deterministik NAT işleminde kullanıcılara belli zaman da bir genel IP ve port tahsis edilmektedir*" yazmışlar. Kendilerine şu soruyu sormaları gerekir; hangi mahkemeye sunulan hangi kayıtlarda bu özelliğin kullanıldığına dair somut delil bulunmaktadır. Hatta şöyle talihsiz bir ifade kullanmışlar

"*Bunlar arasında Avea'nın (ve muhtemelen diğer operatörlerin de) Deterministik NAT kayıt tekniklerini kullandığı ve bundan ötürü Genel IP / Özel IP kayıtlarını algoritmik olarak tuttuğu ve bu algoritmaların çözümlenmelerinde problemler yaşadığı açıktır.*"

Ben bilim adamı olarak bu tam yargı içeren ve AVEA'nın D-NAT kullandığını kanun gibi ortaya koyan cümleyi bir adli bilişim uzmanına kim yazdırmış olabilir diye merak ediyorum. En azından olduğu düşünülmektedir yazılabilirdi. Bu algı raporunu ortaya koyarak büyük emekler harcayan arkadaşların şunu bilmesi gerekir; bilirkişi yemini yapılırken onlarda benimle birlikte tekrar ederlerse "*Bilirkişilik görevimi sadakat ve özenle, bilim ve fenne uygun olarak, tarafsız ve objektif bir biçimde yerine getireceğime, namusum, şerefim ve kutsal saydığım bütün inanç ve değerlerim üzerine yemin ederim*" denilmektedir. Bunu kendilerine hatırlatmak gerektiğini düşünmekteyim.

- NAT sistemi kullanıcılara 1000 kadar port tahsisi yapmaktadır. Bu kayıtlarda kaynak port bilgileri de bulunmaktadır. Dolayısıyla sorgusu yapılan kullanıcıya tahsis edilen portlar dışında bir portun atanmış olması teorik olarak mümkün değildir ve bu tip bir iddia basit bir kayıt incelemesi ile ortaya konabilecek bir hususdur, konuyu olmadığı bir yere taşıyarak anlam karmaşası yaratmak bilimsel temelden uzak bir sav olmaktan öteye geçememiştir.
- Halen bu alanda yaptığımız bilirkişilik çalışmalarından gördüğüm kadarıyla NAT kayıtlarında hangi abonenin hangi tarih ve zaman içinde ByLock sunucusu ile iletişime geçtiği bilgisi mevcuttur.Ayrıca operatörler nezdinde çalışan CGNAT kayıtlarını tutan sistemler, algı operasyonu yapmayı hedefleyen raporlarda yazdığının aksine aynı NTP zaman sunucusundan hizmet alarak senkronlu hale gelmektedir. Bunun yanında IP bilgileri ve NAT kayıtları operatör üzerinde saklandığından bu verilerde yer alan zaman bilgisi ile kullanılan mobil cihazın zaman bilgisi arasında teknik bir ilişki olması beklenemez. Bu raporları yazan arkadaşlar bir telekomünikasyon mühendisiyle bunları tartışarak raporlarını yazma

zahmetinde bulunsalardı zaten bunu bir problem gibi yansıtmamaları gerektiğini öngörebilirlerdi.

- Bir kullanıcıya ait binlerce log kaydının bulunabileceği gibi az sayıda bağlantı kaydı da bulunabilir. Her kullanıcı aynı ByLock uygulamasını kullanmış olsa dahi VPN kullanımı, SESLİ görüşme, E-POSTA gibi farklı işlem türleri değişken tür ve boyutta bağlantı verisi oluşturacaktır. Dolayısıyla NAT kayıtları ve VPN bağlantı ve kopma anları gibi kayıt sayısının log kaydının büyüklüğüne göre ByLock kullanıp kullanılmamasında belirleyici bir faktör olmadığı anlaşılmalıdır. Bu noktada BTK'dan gelen kayıtlar tarafsız bir gözlem ile değerlendirilmelidir.
- Algı raporu yazarlarının gözünden kaçan bir diğer nokta ise GSM mimarisine hakim olmamalarından kaynaklanan unsurlardır. GSM şebekesi SES ve VERİ olarak iki kısımdan oluşmaktadır. Bu iki kısma ait lokasyon güncelleme yöntemleri farklıdır.
    - Şöyle ki; SES hizmeti alındığında yapılan konum güncellemesi ile VERİ hizmeti alınan IP santrali üzerinde VERİ iletişim zamanına göre yapılan konum güncellemesi farklıdır. Dolayısıyla ByLock kullanıldığında alınan konum bilgisi ile öncesinde veya sonrasında SES iletişimi alındığında tespit edilen konum bilgisinin farklı olması son derece teknik, bilimsel ve normal bir durumdur.

Algı raporcuları tarafından ifade edilen "*MİT, bir kullanıcının gerçekten örgüt üyesi olup olmadığını, kullanıcının kullanım frekansı ve sıklığına göre değerlendirmiştir*" ithamı MİT'in teknik inceleme sonucunu yansıtması karşısında haksızdır.

- ByLock kayıtları 443 nolu nolu TLS/SSL portu üzerinden yapılan haberleşmeleri esas almaktadır. BTK'dan gelen CGNAT kayıtları da en az 3 farklı gün kuralı ile ByLock sunucusu IP adresleri ile 443 nolu port bağlantısının kurulduğuna ve başka bir port bilgisine yer verilmediğine işaret etmektedir. Dolayısıyla algı raporlarını hazırlayan ekipler mahkemelere ulaşan delilleri dikkate almadan başta söz ettiğim karmaşıklığı arttırmaya yönelik girişimlerde bulunarak "*BTK kayıtlarından abonenin ilgili sunucu IP adreslerine 443 numaralı (HTTPS) porta bağlantı kurulup kurulmadığının*," demişlerdir ki zaten bu bilgi mevcuttur. Yazarlar, raporun genelinde varsayımlar üzerine kurulu bir senaryo oluşturduklarından, 5651 sayılı kanunda saklanması emredilen bilgilerin mevcut olmadığı yönünde bir görüş bildirmişlerdir. İronik olarak bir görüşten başka bir görüş üretme noktasında öncekini gerçekten olmuş kabul ederek başka bir görüş üretme yöntemiyle son gelinen örneği teknik açıdan anlamlı ve genel ifadeyle her bilişim sisteminde her gün yaşanan temel bir sorunmuş gibi göstermişlerdir. Gündemin sıcak konusu

olduğundan MorBeyin tuzağına atıfta bulunarak çarpıtılan gerçekleri akılda kalıcı bir ifade ile yaşanabilecek senaryolar içerisine almışlardır.

ByLock basit bir mesajlaşma uygulaması değildir. Toplumun her kesimi tarafından kullanılan WhatsApp gibi bir yapısı olduğunu düşünmek yanlıştır. ByLock programını kullanmak için kayıt olmaktan fazlası gerekmektedir. Bir diğer ifadeyle ByLock kullanmadan önce birbirlerinin örgüt içindeki kod adını bilmeyen kişi yada grupların haberleşmesi mümkün değildir. Uygulamanın kripto haberleşme yazılımı olarak anılmasının en büyük nedeni basit bir yöntem ile haberleşecek tarafların birbirlerini görememesi bu isimlerin örgüt içi imamlar vasıtasıyla taraflara bildirilmesidir. ByLock uygulamasının kullanılabilmesi için kayıt işlemi gerekmektedir ancak kayıt işlemi sırasında kişilerin belirlenmesini mümkün kılacak özel bir bilgi talep edilmemektedir, öte yandan uygulamaya kayıt olunması uygulamanın kullanılmasını da mümkün kılmamaktadır. Uygulama cihaz üzerinde kayıtlı telefon defteri ile ByLock sistemine bağlı olan kişiler arasında eşleştirme yapılmasına izin vermemektedir. Dolayısıyla, ByLock kullanacak bir kişinin haberleşeceği grup veya kişiye ait kod adını bilmesi, görüşeceği kişini kod ismini karşılıklı olarak Bylock uygulamasına eklemesi gereklidir. Kullanıcılarının hücre tipi örgütsel yapılanmaya özgü mesajlaşabilmelerine imkan verildiği ve otomatik mesaj silinmesi gibi özelliklerin olduğu anlaşılmaktadır. Çünkü mesajlaşmak için iki ve/veya daha fazla kişinin birbirlerini eklemesi gerekmektedir. Bunun anlamı kod adını bildiğiniz biriyle sizin sistem de kod adınız yoksa yazışma yapamayacağınız gerçeğidir.

Algı raporlarında ByLock sunucularının IP adreslerini de özel bir yer verilmiştir fakat atlanan noktalar kendi içinde çelişmektedir. Baltic Server üzerine kayıtlı bu IP adresleri Dedicated Server(Hizmete/Şahsa Özel Sunuculara) aittir. Dolayısıyla Shared Hosting denilen paylaşımlı internet sitelerine verilmesi mümkün değildir. Farz edelim mümkün olsun ByLock bir web sitesi değildir Dedicated Server üzerinde çalışan bir mobil uygulamanın veri-tabanı operasyon ve yönetim ara-yüzüdür.

Şahsen bende oluşan izlenim her ne kadar 4-5 kişinin adıyla yayınlanan raporlar olsa da ifadeler, cümle yapıları, teknik bilgi birikimi gibi alanlar değerlendirildiğinde yazar olarak görünen kişilerden de fazla sayıda kişinin bir araya gelerek zorlama senaryolar ile bilimden, teknikten ve fenden uzak raporlar yazdığı gerçeğidir.

Bu tip algı operasyonlarını yöneten kişilere naçizane tavsiyem altına imza atmanız gereken bir işi yaparken;

1. Alanınız olmayan bir konuda zorlama senaryolar ile rapor yazmayın, alan uzmanı akademisyen veya alan uzmanı sektör önderlerinden kişilerle çalışın,
2. Dünya siber suç literatüründe kabul görmüş yöntemleri sorgulanır hale getirecekseniz lütfen bunu varsayımlar ile değil dünya yargı örnekleri üzerinden yapın,
3. Bir konuda kesin yargı bildirecekseniz 2 sayfa önce verdiğiniz öneriye atıf yaparak değil bilimsel ve teknik olarak ispatlanabilir, ölçülebilir ve yeniden oluşturulabilir test kriterleri kullanarak ifade etmeniz gerektiğini unutmayın,
4. Elinizde olmayan teknik bilgileri sanki varmış gibi anlatmayın veya var olmayan delilleri öngörülerinize göre sanki varmış gibi kullanmayın,
5. Ve en önemlisi teknik bir rapor hazırlarken her zaman bilirkişi olduğunuzu hatırlayın, raporunuza başlamadan şu yemini tekrarlayın,

"*Bilirkişilik görevimi sadakat ve özenle, bilim ve fenne uygun olarak, tarafsız ve objektif bir biçimde yerine getireceğime, namusum, şerefim ve kutsal saydığım bütün inanç ve değerlerim üzerine yemin ederim*"

Son olarak okuyucularımdan bir istirhamım olacak;

Lütfen Troll/Aldatmaca raporları, bilimi ve tekniği siyasileştiren mağdurum söylemlerini bir anlık heyecan ile kabul etmeden önce çok sesliliğe destek verin farklı düşünce, fikir ve deneyimlere açık olun, konuyu her yönüyle tartışan gerçekten bilim adamı kimliği olan yaptığı işin alaylısı değil mekteplisi olan insanların söylediklerine kulak verin, iftiralara kulak tıkayın.

Bu ülke hepimizin, bu devleti oluşturan halk bizlerden başkası değil, bayrak hepimizin bayrağı ve o bayrağa güven duymaktan başka çaremiz yok,

Son sözüm ise Algı Raporcularına;

Ismarlama raporlar yazarken tüm senaryoları ele alarak konuyu tartışırsanız bilime ve fenne bağlı kalarak doğruları ve gerçekleri yazmış olursunuz, devletin haklı olmasından endişe ederseniz belki mahkemelere verdiğiniz imzalı raporlarda olduğu gibi "kanaati oluşmaktadır" veya "düşünülmektedir" gibi doğru ifadelerle yazar; yargı ve karar cümlelerini sağduyulu bir şekilde mahkemelere bırakırsınız.

II. HUKUKİ GERÇEKLER: TÜRK CEZA YARGILAMASINDA ELEKTRONİK DELİL KAVRAMI ve BYLOCK UYGULAMASI

Yukarıda I. Kısım'da gerek ByLock uygulamasına, gerekse algı raporları ile CGNAT kayıtları hakkındaki yanlış yönlendirme girişimlerine karşı verilen cevap, konunun daha anlaşılabilir olması bakımından sade bir dil ile aktarılmaya çalışıldı.

Bu kısımda ise ByLock uygulamasına dair verilerin hukuka aykırılığı iddiaları incelenmektedir.

Bu anlamda ByLock uygulamasına dair verilerin elektronik delil niteliği göz önüne alınarak Türk ceza yargılamasında elektronik delil kavramına değinilmesi, esasen bundan da önce ceza yargılamasında "delil" kavramına değinmekte fayda görülmektedir.

1. Türk Ceza Yargılamasında Delil Kavramı

Ceza yargılamasının temel amacı ceza muhakemesine konu olan olayın araştırılarak maddi gerçeğin kuşkuya yer bırakmayacak şekilde ortaya çıkarılmasıdır. Maddi gerçeğin ortaya çıkartılması ise akla ve mantığa uygun, gerçekçi deliller ile mümkündür.

Türk Ceza Kanununda delil kavramı tanımlanmamıştır. Bununla birlikte Türk ceza yargılamasında delil kavramına farklı tanımlar getirilmiştir. Örneğin, yazarlardan bazıları delili "ceza uyuşmazlığının konusu olan olayı temsil eden olayın mahkeme önünde canlandırılmasına yarayan araç"[1] olarak tanımlarken, bir başka yazar delili "anlaşmazlık konusu olan bir fiilin, hukukî bir olayın veya hareketin, suç olup olmadığı konusunda hâkimin bir kanaate varmasını sağlayan ve usul hukukunun kullanılmasına izin verdiği her türlü ispat vasıtası"[2] olarak tanımlamıştır.

Delil, Polisin Adlî Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmelikte ise "Meydana gelen bir suçun aydınlatılması ve suç sanıklarının tespitine yarayan her türlü ispat vasıtası" olarak tanımlanmıştır[3].

Ceza yargılamasında delillerin ispat vasıtası olarak kullanılabilmesi için bazı özelliklere sahip olması gerekmektedir. Aksi halde bu vasıtaların delil olarak değerlendirilmesi mümkün değildir. Bu bağlamda değerlendirildiğinde deliller;

---

[1] Nur Centel/Hamide Zafer, Ceza Muhakemesi Hukuku (10. Bası) İstanbul, 2013, s. 201.
[2] Şenocak, Cengiz, Maddi Suç Delilleri ve Ateşli Silahlar 3. Baskı, Ankara, 1997, s. 27
[3] Resmi Gazete, Tarih: 17.02.1983, Sayı: 17962

a) Ceza uyuşmazlığını oluşturan olayın bir parçasını ispat edebilecek nitelikte ve elde edilebilir olmalı,

b) Ulaşılamayacak ve dolayısıyla mahkemeye sunulamayacak durumda olmamalı,

c) Mahkemede tartışılabilir olmalı,

d) Hukuka uygun yollardan elde edilmiş olmalı,

e) Sağlam ve güvenilir olmalı, sonradan uydurulmuş veya tahrif edilmiş olmamalıdır.

2. Türk Ceza Yargılamasında Elektronik Delil Kavramı

Elektronik delil, elektronik bir cihaz üzerinde saklanabilen veya elektronik cihazlar aracılığıyla iletilebilen ve yargılama bakımından değeri olan bilgi ya da veriler olarak tanımlanmaktadır[4].

Elektronik deliller ile ilgili karşılaşılan sıkıntıların başında somut bir yapıya sahip olmamaları gelmektedir. Bundan dolayıdır ki elektronik delillerin elde edilmesinde ve muhakeme öncesinde ya da sonrasında değerlendirilmesinde çeşitli cihazlara ihtiyaç duyulmaktadır. Bu cihazlar sayesinde elektronik ortamdan edindiğimiz veriler duyularımızla algılanabilecek bir hale getirilmektedir. Somut bir yapıya büründükten sonra elektronik veriler yargı makamlarınca temas edilebilir bir hale gelmekte ve bir delil niteliği taşımaktadır.

Elektronik ortam hususunda elektronik delillerin klasik delillerden farklı olarak soyut bir yapıya sahip olmaları sebebiyle delil niteliğini haiz olan, bilginin bilgisayar ya da ekran çıktısı değil, elektronik ortamdaki bilginin kendisidir. Bu durum bizi muhakeme açısından esas delil niteliğini haiz olanın, donanım ya da yazılım vasıtalarının kendisinin değil, içerisinde bulunan elektronik nitelikteki bilginin olduğu sonucuna da götürecektir.

Elektronik deliller ile ilgili diğer bir sıkıntı da güvenilirliği hakkındadır. Elektronik deliller soyut yapılarından kaynaklı olarak müdahale edilmeye ve güvenilirliğinin yitirilmesine müsaittir. Bu sebepler de elektronik delillerin delil olma niteliğinin tartışılır hale gelmesine neden olmaktadır.

Elektronik delillerle ilgili diğer bir husus ta elde edilme ve ortaya çıkarılma aşamasında dikkat edilmesi gereken bir çok teknik unsurun olmasıdır. Bu sebepten dolayıdır ki

---

[4] Keser Berber Leyla, Adli Bilişim (Computer Forensic), s. 46; Özocak, s. 114; Değirmenci, s. 127; Osman Gazi Ünal, Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Ceza ve Ceza Usul Hukuku Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara 2011, s. 16.

elektronik delilin sıhhatinin korunması için teknik bilgilere sahip uzmanlarca uğraş konusu edilmelidir.

Elektronik delillerin Türk ceza hukukunda düzenlenen delil türlerinden hangisine dâhil olduğu hususu tartışmalıdır. Şahsi kanaatimiz elektronik delillerin niteliğine göre her türlü delil yapısına sahip olabileceğidir. Bu konuda önemli olan husus elektronik delillerin bu muhakeme içerisindeki maddi olaya tam olarak uygunluk göstermesi ve güvenilir bir yapıda olmasıdır.

3. Elektronik Delillerin CMK 134 Kapsamında Değerlendirilmesi

Bilişim sistemlerinin kullanılması suretiyle işlenen suçlarda yahut klasik suçlara ilişkin delillerin bilgisayar sistemlerinde bulunma ihtimalinin söz konusu olduğu durumlarda, bilgisayarlarda yapılacak arama CMK m. 134'te özel olarak düzenlenmiş olup, bu hallerde arama kararının yalnızca hâkim tarafından verilebileceği öngörülmüştür.

CMK m. 134 uyarınca;

> *(1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.*
>
> *(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.*
>
> *(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.*
>
> *(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.*
>
> *(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.*

CMK m. 134 de, bilgisayarlarda ve bilişim sistemlerinde arama ve el koyma tedbirinin uygulanabilmesi için birtakım şartlar düzenlenmiştir. Bu şartların tamamı ceza hukukunun kanuniliği ilkesine uygun olarak ilgili tedbirin düzenlendiği maddede mevcuttur. CMK m. 134'ün uygulanabilmesi için kanunda düzenlenen şartlardan biri hali hazırda mevcut olan bir suç soruşturmasının varlığıdır. Bu husus ilgili tedbirin en temel şartıdır. Kanunda yer verilen diğer bir şart ise başka surette delil elde etme imkânının bulunmamasıdır. Bu husus CMK da birçok yerde bulunmaktadır. Başka surette delil elde etme imkânının bulunmaması konusu doktrinde tartışmalıdır. Bu kavramdan, tedbir öncesinde her türlü delil elde etme yönteminin uygulanmış ancak hiçbir delil elde edilememiş olmasını anlamak gerekir. Bir başka ifadeyle CMK m. 134'ün uygulanması maddi gerçekliğin ortaya çıkarılması için başvurulacak son yöntemdir. Diğer bir şart ise bu tedbirin uygulanması kararının ilgili sulh ceza hâkimi tarafından verilmiş olmasıdır.

CMK m. 134 uygulanırken dikkat edilmesi gereken unsurlardan biri de işlemler yapılırken izlenecek usuldür. Soruşturmaya konu olan bilgisayarlarda öncelikle yerinde inceleme yapılmalıdır. Yerinde inceleme yaparak delil elde etme imkânı olmazsa bilgisayarlara veya diğer bilişim sistemlerine el koyulmalıdır.

Sonuç olarak, delil araştırmasında CMK'da öngörülen usule eksiksiz bir biçimde uyulması, delillerin ceza yargılamasında verilecek hükme esas teşkil edebilmesi açısından son derece önemlidir. Zira ceza muhakemesinde, ancak hukuka uygun yollarla elde edilmiş deliller soruşturma ve yargılamaya konu edilebilir, aksi halde, kanunda öngörülen usullerden birine dahi uyulmaması durumunda, elde edilen delil "kanuna aykırı delil" olacak ve herhangi bir hukuki anlam içermeyecektir. CMK'nın birçok hükmünde, ceza yargılamasında isnadın ancak kanuna uygun elde edilmiş deliller ile ispatlanabileceği, aksi halde, kanuna aykırı bir delile dayanılarak verilmiş bir hükmün mutlak bir biçimde bozulacağını düzenlemiştir.

4. CMK M. 134'te Düzenlenen Tedbirin Hak ve Özgürlükler Açısından Değerlendirilmesi

Temelde bilgisayar ve diğer bilişim sistemlerinde arama ve el koyma tedbiri, temel hak ve özgürlüklere yönelik bir tedbirdir. Bilgisayarlarda ve bilgisayar kütüklerinde arama yapılması ve bunlara el konulması da, kişilerin özel hayatlarının gizliliğinin ihlali

sonucunu doğurmaktadır. Temel hak ve özgürlükler, insanların sadece insan olmalarından kaynaklanan ve doğuştan kazandıkları dil, din, ırk, aidiyet fark etmeksizin sahip oldukları temel değerlerdir. Devlet tarafından bu hakların uygulanmasında veya sınırlandırılmasında usulsüz bir şekilde ayrım yapılması veya bu haklara haksız bir müdahalede bulunulması durumunda da, Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) ihlali söz konusu olacaktır[5].

Bu sebepledir ki, söz konusu koruma tedbirinin uluslararası hukuk normlarına ve Anayasa'ya uygun olması için CMK m. 134'teki hükümler düzenlenmiştir. Çünkü ilgili koruma tedbirinin uygulanması sonucunda ihlal edilen temel insan hakkı özel hayatın korunmasıdır. Bu hak AİHS'nin 8. maddesinde güvence altına alınmıştır. Buna göre, söz konusu hak bir insan hakkı olup, bu hakkın ancak istisnai hallerde ve kanun ile sınırlandırılabilmesi mümkündür.

Bu bağlamda, CMK m. 134 genel arama ve el koyma hükmünden ayrılarak, özel hayatın gizliliğine kanuni müdahalenin şartlarını düzenlemiş, bunu hakim kararı şartına bağlamış, temin edici kimi usuller öngörmüş ve istisnai bir durum olarak yalnızca suç şüphesi olması durumunda ve başka surette delil elde edilemediğinde bu tedbire başvurulacağını ifade etmiştir[6].

5. Silahlı Terör Örgütüne Üye Olma Suçu

Örgüt kurma suçu çok failli bir suçtur. Türk Ceza Kanununun 220. maddesine göre; en az üç kişinin, suç işlemeye elverişli araç ve gerece sahip olarak, hiyerarşik bir ilişki ve iş bölümü içerisinde amaç suçları işlemek için süreklilik arz edecek şekilde bir araya gelmesiyle suç işlemek amacıyla örgüt kurma suçu meydana gelir.

"FETÖ/PDY, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasi, hukuki, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türkiye Devletini ve varlığını tehlikeye düşürmek, Devlet otoritesini yıkmak ve daha sonra ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini bozmak amacıyla kurulmuş bir terör örgütüdür. Bu örgüt kuruluşundan 15 Temmuz sürecine kadar örgüt lideri Fethullah Gülen tarafından belirlenen ideolojisi doğrultusunda amaçlarını gerçekleştirmek üzere eylem ve fikir birliği içinde hareket etmiştir. Sahip olduğu yada mensuplarının tasarrufunda bulunan

[5] Şen, Ersan / Özdemir, Bilgehan; Tutuklama – Uygulamada Şüpheli ve Sanık Haklarının Korunması, Ankara, 2011, s. 50.
[6] Özbek, Kanbur, Doğan, Tepe: Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Eylül 2014, s. 380

araç gereç bakımından 5237 Sayılı TCK'nın 314/1-2 maddesi kapsamında silahlı bir terör örgütü olduğu anlaşılmıştır." (Yargıtay 16. CD., 2017/1443 E. ve 2017/4758 K.).

Bu bağlamda değerlendirildiğinde ByLock uygulamasının silahlı terör örgütüne üye olma suçunun bir delili olduğunu hatırda tutmak gerekir. Zira Bylock uygulaması sadece FETÖ/PDY terör örgütü üyeleri arasında gizli haberleşme için kullanılan bir uygulamadır ve örgütsel bir iletişim sistemidir. Keza, 15 Temmuz 2016 tarihinde gerçekleştirilen askeri darbe girişimi sonrasında adli soruşturma işlemlerine tabi tutulan FETÖ/PDY silahlı terör örgütü mensupları, ByLock uygulamasının 2014 yılının başından itibaren FETÖ/PDY silahlı terör örgüt üyeleri tarafından örgütsel haberleşme aracı olarak kullanıldığını beyan etmişlerdir. ByLock uygulamasının global bir uygulama görüntüsü altında münhasıran FETÖ/PDY silahlı terör örgüyü mensuplarının kullanımına sunulduğu artık soruşturma dosyalarındaki örgüt üyelerinin beyanları ile de sabit hale gelmiştir. Bu beyanlar ve ByLock uygulamasının elektronik/mobil cihazlara kurulma yöntemleri dikkate alındığında bu hususun hala bir delil olamayacağı iddiası bir hezeyandan ibarettir.

Yargıtay 16. Ceza Dairesinin kararında da belirtildiği üzere; "Bir kişinin mobil telefon cihazında veya bilgisayarında, özel bir iletişim ağına dahil olduğuna dair bir program kullanılabilir.

Bu özel iletişim ağını sadece belirli kişilerin kullanabilmesi ve bu ağa girebilmesi için, ağı kullanan bir veya birçok kişinin referansına gerek bulunması, başlı başına suç oluşturmaz. Ancak, bu iletişim ağının suç işlemek amacıyla oluşturulmuş ve münhasıran bir suç örgütünün mensupları tarafından kullanılmakta olan bir ağ olduğunu somut delillere dayanması halinde, kişinin, suç örgütünün mensupları tarafından kullanılmakta olan bir ağa bu özelliğini bilerek dahil olması ve hatta bu ağın iletişim için kullanılması, iletişim içerikleri tespit edilmese bile, suç örgütü ile bağlantısını gösterir bir delil olarak kabul etmek gerekir."

Anayasa Mahkemesinin 2016/22169 Başvuru Nolu bireysel başvuru üzerine vermiş olduğu kararda "Bunların yanı sıra başvurucular B.G ve A.Y'nin, FETÖ/PDY üyelerinin kendi aralarındaki iletişimi sağladığı ifade edilen "ByLock" uygulamasının kullanıcısı oldukları tespit edilmiştir. Anılan uygulamanın özelliklerine ilişkin olarak soruşturma ve kovuşturma mercilerinde yapılan tespit ve değerlendirmeler gözönüne alındığında kişilerin bu uygulamayı kullanmalarının veya kullanmak üzere elektronik/mobil cihazlarına yüklemelerinin soruşturma makamlarınca FETÖ/PDY ile olan ilgi bakımından bir belirti olarak değerlendirilmesi mümkündür. Bu belirtinin derecesi elbette söz konusu uygulamanın ilgili kişi tarafından kullanılıp kullanılmadığı, kullanım

şekli, kullanım sıklığı, haberleşme yapılan kişilerin FETÖ/PDY içindeki konumu ve önemi, haberleşmenin içeriği gibi hususlara bağlı olarak her somut olayda farklı olabilir. Bununla birlikte darbe teşebbüsüyle veya FETÖ/PDY ile ilgili olarak yürütülen soruşturmalarda, soruşturma makamlarınca veya tutuklama tedbirine karar veren mahkemelerce, "ByLock"un kullanılmasının ve/veya kullanılmak üzere elektronik/mobil cihazlara yüklenmesinin somut olayın koşullarına göre suçun işlendiğine dair "kuvvetli belirti" olarak kabul edilmesi, anılan programın özellikleri itibarıyla temelsiz ve keyfî bir tutum olarak değerlendirilemez. Dolayısıyla "ByLock" kullanıcısı olduğu belirtilen başvurucular Burhan Güneş ve Aydın Yavuz bakımından bu yönüyle de suç şüphesine ilişkin kuvvetli bir belirtinin bulunduğu sonucuna varmak gerekir." görüşüne yer verilmiştir.

Ceza yargılamasında deliller, çoğunlukla beyan, belge ve belirti delilleri olmak üzere üçe ayrılmaktadır. Belirti delili, fiilin ardında kalan ve suçun dolaylı olarak ispatına yarayan doğal veya yapay iz ve emareleri ifade etmektedir[7]. Belirti delili, ceza muhakemesinde soruşturma ve kovuşturma makamlarınca incelenebilecek ve maddi gerçeğin araştırılması ve ispatlanmasında yararlanılabilecek vasıtalar olmasından dolayı maddi deliller olarak da adlandırılmaktadır[8]. Dolayısıyla gerçeğin ispatlanmasında maddi delil olan "belirti" delilinin, hukuki temeli bulunan hiçbir açıklamaya yer verilmeksizin delil olmadığı izlenimi veren algı raporlarının ByLock uygulamasının delil niteliğini tamamen ortadan kaldırmayı amaçlayan art niyetli bir bakış açısıyla yazıldığı görülmektedir.

Kararda, Bylock uygulamasının özelliklerine ilişkin olarak soruşturma ve kovuşturma mercilerince yapılan tespit ve değerlendirmeler göz önüne alındığında (ki bu tespit ve değerlendirmeler bu uygulamanın gerek mobil cihazlara yüklenme, gerekse kullanıcı ekleme vs özellikler nedeniyle sadece örgüt üyeleri arasında kullanıldığına ilişkindir) kişilerin bu uygulamayı kullanmalarının veya kullanmak üzere elektronik/mobil cihazlarına yüklemelerinin soruşturma makamlarınca FETÖ/PDY ile olan ilgi bakımından bir belirti olarak değerlendirilmesi mümkündür. Dolayısı ile uygulamayı elektronik/mobil cihazlarına yükleyenler bakımından haberleşmenin içeriği tespit edilemese dahi bunun FETÖ/PDY silahlı terör örgütü ile bağlantısını ortaya koymaktadır. Haberleşmenin içeriğinin tespiti, uygulamanın kullanım sıklığı vs, sadece bu kişilerin FETÖ/PDY içindeki konumu ve önemini ortaya koymaktadır. Bir başka ifade ile bu durum sadece, ByLock kullanıcılarını örgüt üyeliği, örgüt yöneticiliği ve varsa

[7] Kunter/Yenisey/Nuhoğlu, No. 86.2, s. 1345-1346; Toroslu/Feyzioğlu, s. 177 vd.
[8] Parlar Ali/Hatipoğlu Muzaffer/Yüksel Erol Güngör, a.g.e., s.468

diğer suçlar bakımından ayırt etme hususunda değerlendirilebilir. Haberleşme içeriği bulunmayan ByLock kullanıcılarının aklanması anlamına gelmeyecektir.

Netice olarak Anayasa Mahkemesi kararındaki belirti/kuvvetli belirti yaklaşımını, ByLock uygulamasının delil niteliğini ortadan kaldıran bir unsur olarak öne süren iddiaların mesnedi bulunmamaktadır. Bu yöndeki iddia ile soruşturma ve kovuşturma makamlarını etkilemeye ve kamuoyunun yönlendirilmeye çalışıldığı görülmektedir.

6. ByLock Uygulamasına Ait Veriler ve Delil Niteliği

ByLock uygulamasının FETÖ/PDY terör örgütü mensupları tarafından kullanılan bir örgütsel iletişim sistemi olduğunun öğrenilmesi üzerine, Milli İstihbarat Teşkilatı tarafından teşkilata özgü teknik istihbarat usul araç ve yöntemleri kullanılmak suretiyle ByLock uygulamasına ait sunucular üzerindeki veriler ile uygulama sunucusunun ve IP adreslerinin, e-posta adreslerinin içerikleri başta olmak üzere muhtelif veriler elde edilmiş, düzenlenen teknik analiz raporu ve dijital materyaller Ankara Cumhuriyet Başsavcılığına ve Emniyet Genel Müdürlüğüne ulaştırılmıştır. ByLock verilerinin elde ediliş şeklini eleştiren ve hiçbir maddi delile yer verilmeksizin verilerin tahrip edildiği iftirasında bulunan algı raporlarının hukuki dayanağının olmadığı ortadadır.

Türkiye Cumhuriyeti Anayasası'nın 20. maddesine göre;

> *"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*
>
> *Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.*

Keza Türkiye Cumhuriyeti Anayasası'nın 22. maddesine göre de;

> *"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.*
>
> *Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı*

olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

Yukarıda zikredilen Anayasa'nın 20. ve 22. maddelerinde temel haklardan olan özel hayatın gizliliği ve haberleşmenin gizliliği güvence altına alınmıştır. İlgili maddelerin içerisinde bu hakların milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakla başkalarının hak ve özgürlüklerinin korunması amacıyla sınırlandırılma halleri de sayılmıştır. Bu anayasal haklar için ilgili sınırlama sebeplerinin varlığı bu hakların mutlak hak olmadıklarını göstermektedir.

Bu bağlamda, 15 Temmuz Hain Darbe Girişimi öncesinde hiç duymadığımız ve sonrasında FETÖ/PDY'nin örgüt için iletişim uygulaması olduğu ortaya çıkan "ByLock: Chat and Talk" adlı uygulamaya ve bu uygulamanın ceza yargılaması bağlamında delil olma özelliğine değinmekte fayda görmekteyiz.

Anayasa'da istisnaların uygulanacağı kamu kurum ve kuruluşlarının kanunla belirtileceği düzenlenmiştir. Bu düzenleme Milli İstihbarat Teşkilatının (MİT) kendi kanunundan doğan hakkının aynı zamanda anayasal bir dayanağı olduğunu da göstermektedir. Bu çerçevede değerlendirdiğimizde, 2937 sayılı Devlet İstihbarat Hizmetleri Ve Milli İstihbarat Teşkilatı Kanununun 4. maddesine göre Milli İstihbarat Teşkilatının görevleri şunlardır:

a) *Türkiye Cumhuriyetinin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak.*

b) *Devletin milli güvenlik siyasetiyle ilgili planların hazırlanması ve yürütülmesinde; Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamak.*

c) *Kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için Cumhurbaşkanı, Başbakan ve Milli Güvenlik Kuruluna tekliflerde bulunmak.*

d) Kamu kurum ve kuruluşlarının istihbarat ve istihbarata karşı koyma faaliyetlerine teknik konularda müşavirlik yapmak ve koordinasyonun sağlanmasında yardımcı olmak.

e) Genelkurmay Başkanlığınca Silahlı Kuvvetler için lüzum görülecek haber ve istihbaratı, yapılacak protokole göre Genelkurmay Başkanlığına ulaştırmak.

f) Milli Güvenlik Kurulunda belirlenecek diğer görevleri yapmak.

g) İstihbarata karşı koymak.

*h) **(Ek: 17/4/2014-6532/1 md.)** Dış güvenlik, terörle mücadele ve millî güvenliğe ilişkin konularda Cumhurbaşkanınca veya Bakanlar Kurulunca verilen görevleri yerine getirmek.*

*i) **(Ek: 17/4/2014-6532/1 md.)** Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak.*

*j) **(Ek: 17/4/2014-6532/1 md.)** İstihbarat kapasitesini, niteliğini ve etkinliğini artırmak amacıyla çağdaş istihbarat usul ve yöntemlerini araştırmak, teknolojik gelişmeleri takip etmek ve uygun görülenleri temin etmek.*

2937 sayılı Devlet İstihbarat Hizmetleri Ve Milli İstihbarat Teşkilatı Kanununun 6. maddesine göre de Millî İstihbarat Teşkilatı bu Kanun kapsamındaki görevlerini yerine getirirken aşağıdaki yetkileri kullanacağı hüküm altına alınmıştır.

> *Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilir ve bunlarla irtibat kurabilir. Bu kapsamda talepte bulunulanlar, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamazlar (2937 s. Kanun m. 6/1-b).*
>
> ***Telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilir** (2937 s. Kanun m. 6/1-g).*

2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 6. maddesinin 1. fıkrasının g bendi hükmü gereği MİT'in ***telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplama yetkisi açık şekilde mevcuttur.***

Bu çerçevede MİT'in, ana sunucusu (server) yurt dışında bulunup mobil cihazlara kurulan, internet üzerinden yazışma imkanı veren ve kriptolu iletişimde münhasıran FETÖ/PDY silahlı terör örgütü ile bu örgüt mensuplarınca kullanılan ByLock iletişim sisteminde bulunan verileri temin etme yetkisi ve bu verileri adli makamlara ulaştırma görev ve yükümlülüğünü tartışmak abesle iştigaldir ve hukuk abesle iştigal etmez.

Ceza Muhakemesi Kanununa göre suçun öğrenilmesi ile birlikte delillerin toplanmasının başlanması gerekmektedir. Türk ceza hukukunda suçun öğrenilme çeşitleri vardır. Suçun öğrenilmesi ihbar, şikâyet veya yetkili makamların tesadüf etmesiyle gerçekleşir. Bu nedenle MİT'in suça ilişkin olarak edindiği bilgileri, delilleri ve yasal yetkileri çerçevesinde elde ettiği ByLock iletişim sistemine içerikleri adli makamlara teslim etmesi zorunludur. Teslim ettiği makamların da yine CMK hükümlerine göre derhal hareket etmesi gerekmektedir.

ByLock uygulaması, kullanılması için sadece indirilmesi yeterli olmayan, özel bir kurulum gerektiren, güçlü bir kriptolama yoluyla internet bağlantısı üzerinden iletişim sağlamak üzere, gönderilen her bir mesajın farklı bir kripto anahtarıyla şifrelenerek iletilmesine dayanan bir tasarıma sahiptir. Bu şifreleme sisteminin, kullanıcıların kendi aralarında bilgi aktarırken üçüncü kişilerin bu bilgiye izinsiz şekilde (hack) ulaşmasını engellemeye yönelik bir güvenlik sistemi olduğu da ayrıca tespit edilmiştir. 2014 yılı başlarında işletim sistemlerine ait uygulama mağazalarında yer alıp bir süre herkesin ulaşımına açık olan ByLock'un, bu mağazalardan kaldırılmasından sonra örgüt mensuplarınca harici bellek, hafıza kartları ve bluetooth yoluyla yüklenildiği yürütülen soruşturma ve kovuşturma dosyalarındaki ifadeler, mesaj ve e-postalardan anlaşılmıştır. Nitekim Yargıtay Ceza Genel Kurulunun 26.09.2017 T., 2017/16-956 E. ve 2017/370 K. sayılı kararı da bu yöndedir.

ByLock uygulamasının FETÖ/PYD'nin örgüt içerisinde özel iletişim amacı ile kullanılan bir uygulama olduğunu ortaya koyan teknik değerlendirmeler yine sözü edilen Yargıtay Ceza Genel Kurulu kararında ve MİT ve EGM-KOM Daire Başkanlığı tarafından düzenlenen raporlarda detaylı olarak ortaya konulmuştur. Uygulamanın deşifre edilmesi ve elde edilen sonuçların rapora konu edilmesi bu meselede önem arz eden hususlardandır. Çünkü yasal yetki çerçevesinde gerçekleştirilen bir işlem uygulamanın teknik açıdan analizi, daha da önemlisi söz konusu uygulamanın kullanıcı kitlesine ilişkin

veriler şüphenin ispatına (bu uygulamayı FETÖ/PDY mensuplarının kullandığının somutlaştırılmasına) vesile olmuştur.

CMK m. 135'e göre "Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, **(Değişik ibare: 6763 - 24.11.2016 / m.26)** "hâkim" veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi (...)**(*)** dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir."

Ancak, ByLock uygulamasının kullanımı sonucunda oluşan verilerin tespiti, CMK. m. 135 kapsamında değerlendirilemez. Bu durum CMK'nın "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlıklı 134. maddesinin birinci fıkrası kapsamındadır. Zira yukarıda da belirtildiği üzere CMK m. 134/1 maddesi bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilmesini düzenlemektedir.

Bu sebeple 2937 Sayılı Kanunun 4. maddesinin birinci fıkrasının (i) bendi ile 6. maddesinin birinci fıkrasının (b) ve (g) bentlerine uygun şekilde elde edilen ByLock uygulamasına ilişkin dijital materyaller hakkında verilen tespit kararları, bağlantı verisi kaynaklı bir dijital materyalin delil teşkil edebilmesi için "yeniden erişilebilir" ve "doğrulanabilir" olma özelliğini teyit maksatlıdır. Bu bağlamda söz konusu tespit kararlarında hukuka aykırılık bulunmamaktadır.

Diğer taraftan dijital verilerin hassas oldukları, dışarıdan müdahaleye açık oldukları ve bu nedenle güvenilirliklerin tartışma konusu olduğu iddialarının ve yine bununla birlikte verinin elde ediliş aşamasında uygulanacak usullerin verinin bozulmasını engellememesi için yasada belirtilen usule göre elde edilmesi gerektiği yönündeki iddiaların hukuken de doğru bir yaklaşım olmadığı ortadadır. Yukarıda izah edildiği üzere ByLock verilerinin elde edilmesi aşamasında bir hukuka aykırılık söz konusu değildir. ByLock verilerinin elde ediliş şeklini eleştiren ve verilerin çözümlenmesinde verilerin tahrip edildiğini iddia eden rapor ve söylemler somut değerlendirmelerden uzak olan, gerçekte kamuoyunu yanlış yönlendirme amacı güden rapor ve söylemlerdir. Temeli olmayan bu tür iddia ve söylemlerin kabulü dijital delillerin inkarı anlamına gelir ki, siber suçların ve olayların

giderek arttığı göz önüne alındığında, bu yöntemle işlenen suçların cezasız kalacağı anlamına gelecektir.

Ayrıca, kişilerin internet trafik verileri Bilgi Teknolojileri Kurumu (BTK), GSM operatörleri ve internet servis sağlayıcıları nezdinde bulunmaktadır. Bu nedenle bağlantı verilerinin büyüklüğü, bu çapta bir verinin bütün bu kurumların tamamından aynı yöntemlerle aynı şekilde müdahale edilmesini gerektirir ki böyle bir yöntem ve işlem mümkün değildir.

Diğer taraftan NAT uygulamasına dair dezenformasyon maksatlı iddia ve söylemlerin dayanaksız olduğu görülmektedir. Zira, dünyanın bir çok ülkesinde bir çok GSM operatörü kısıtlı sayıdaki IP sebebiyle müşterilerini NAT uygulaması kullanarak ayrıştırmaktadır. Bu uygulamaya itiraz da esasen bu zamana kadar yapılmış bilişim suçları tespitlerinin de inkarı anlamına gelmektedir.

Sadece FETÖ/PDY Örgüt üyelerinin kendi aralarında kriptolu şekilde haberleşmeleri amacıyla kullanıldığı teknik raporlar ve sunucudan elde edilen içerikler ile ByLock uygulamasını kullanan kişilerin tespit edilmiş olması karşısında hukuka uygun olarak elde edilen ve çözümlenen verilerin hukuka aykırı olduğu yönündeki iddialara itibar edilmemesi hukukun bir gereğidir.

Netice olarak Bylock uygulaması kullanmayan kişilerin bu uygulamayı kullandıkları yönünde bir veri tahrip işlemi yapılabilmesi de söz konusu değildir.

Dr. Öğr. Üyesi. Uraz YAVANOĞLU & Av. Süleyman BOŞÇA & Av. Olcay ENLİOĞLU

KAYNAKÇA

- Özbek, Kanbur, Doğan vd., Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Eylül 2014
- Centel ve Zafer, Ceza Muhakemesi Hukuku, Beta Basım Yayın, Kasım 2016
- Prof. Dr. Muharrem Özen-Gürkan Özocak Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki rejimi (CMK M.134),Ankara Barosu Dergisi. 2015/1,
- Osman Gazi Ünal, Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Ceza ve Ceza Usul Hukuku Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara 2011
- Keser Berber Leyla, Adli Bilişim (Computer Forensic), Yetkin Yayınları, Ocak 2004
- Eryılmaz, Mesut Bedri; Ceza Muhakemesi Hukuku Dersleri, Ankara, 2012
- Şen, Özdemir, Tutuklama – Uygulamada Şüpheli ve Sanık Haklarının Korunması, Ankara, 2011