CGNAT ve HTS Kayıtlarının Karşılaştırılması Neticesinde Elde Edilen Sonuçların Hukuki ve Teknik Değerlendirmesi

CGNAT ve HTS Kayıtlarının Karşılaştırılması Neticesinde Elde Edilen Sonuçların Hukuki ve Teknik Değerlendirmesi

Dr. Berker KILIÇ
Adli Bilişim Uzmanı
Veri Bilimci

www.adlibilisimci.com
berker.kilic@gmail.com
05069302199

Gizay DULKADİR
Avukat

gizay.dulkadir@gmail.com

Ekim 2022

CGNAT ve HTS Kayıtlarının Karşılaştırılması Neticesinde Elde Edilen Sonuçların Hukuki ve Teknik Değerlendirmesi

15 Temmuz 2016 tarihi sonrasında başlayan ve ByLock kullanıcısı olmak iddiası kapsamında devam etmekte olan yargılamalar, başladığı günden bu yana ceza hukuku ve adli bilişim temelinde pek çok noktada tartışma konusu olmuştur. Bugün dahi bu hususta tartışmalar devam etmektedir.

Sürmekte olan bu tartışmalar, ByLock isimli uygulamaya ilişkin verinin elde ediliş biçiminin hukuka uygun olup olmadığından, söz konusu programı kimlerin kullandığına ilişkin yapılan tespitlerin doğruluk oranına ve neticeten yalnızca bu programı kullanmış olmanın silahlı terör örgütü üyeliği suçunun işlendiğinin kabulü bakımından yeterli bir eylem olup olmadığına kadar uzanmaktadır.

Yüksek yargı, süreç içerisinde tüm bu tartışmalara ilişkin çeşitli kararlar vermiş ve bu kararlar birer içtihat halini almıştır. Hal böyle olmakla birlikte, yüksek yargı kararlarının bugün dahi ByLock isimli uygulamayı kullanmak iddiasıyla yürütülen yargılamalara ilişkin süren hukuki tartışmayı bitirebildiğini söylemek mümkün değildir. Öyle ki, yüksek yargı kararlarının her biri gerek ceza hukuku ve gerekse adli bilişim temelinde yeni tartışmaların doğmasına neden olmaktadır.

Yüksek yargının ByLock kullanıcısı olmak iddiasıyla yürütülen yargılamalar kapsamında verdiği güncel kararlarında değinilen "*CGNAT kayıtları ve HTS sonuçları karşılaştırılıp belirtilen hat üzerinden ByLock kullanan kişinin sanık olup olmadığı*

doğrultusunda bilirkişiden teknik rapor alınması" hususu yargılamalar bakımından yeni bir tartışma konusu haline gelmiştir.

Yargıtay'ın ilgili kararları akabinde, yerel mahkemeler tarafından yaptırılan bilirkişi incelemelerinde sıklıkla, HTS ve CGNAT kayıtlarının uyumluluğunu tespite ilişkin raporlarla karşılaşılmıştır. Bu incelemelerin bir kısmının yanlış verilerin karşılaştırılması bir kısmının ise uyumluluğu kesin olması gereken verilerin karşılaştırılmasına dayandığı görülmektedir. Karşılaştırmalarda iletişim kayıtları içerisinde yer alan ilgili Baz İstasyonu bilgisinin kullanıldığı görülmektedir.

Bu gelişmeler ışığında, yukarıda kısaca özetlenen ByLock kullanım iddiasına konu yargılamalarda hala devam eden tartışmaların beraberinde yeni bir değerlendirme yapmak ihtiyacı doğurmuştur. Bu çalışma yukarıda da ifade edilen tartışmalara ilişkin kamuoyuna deklare edilmiş görüşlerin yanında, ortaya çıkan bu yeni tartışma bakımından görüşleri ifade etmek maksadıyla hazırlanmıştır. Bu nedenle çalışmanın kapsamı ByLock kullanım iddiasına konu yargılamalardaki diğer hukuki ve teknik tartışmalardan bağımsız olarak yalnızca CGNAT ve HTS kayıtlarının karşılaştırılması ile bir kimsenin ByLock kullanıcısı olup olmadığının tespiti yönündeki Yargıtay kararlarına ilişkin değerlendirmeleri kapsamaktadır.

Dr. Berker KILIÇ
Adli Bilişim Uzmanı
Veri Bilimci

Gizay DULKADİR
Avukat

0. İçindekiler

1. Giriş

Ülkemizde yaşanan 15 Temmuz 2016 tarihli askeri darbe girişimi ve beraberinde ilan edilen olağanüstü hal neticesinde, Türk Ceza Kanunu ve Terörle Mücadele Kanunu kapsamında düzenlenen silahlı terör örgütü kurmak, yönetmek ve bu örgütlere üye olmak suçu kapsamında yapılan yargılamaların sayısında, ülkemiz tarihinde görülmemiş bir artış yaşandığı ve sayıları yüz binleri bulan yurttaşın işbu suçlar kapsamında yargılandığı bilinen bir gerçektir.

Bu yargılamaların önemli bir kısmı -soruşturma makamlarının anlatımı ile- 15 Temmuz 2016 tarihli askeri darbe girişiminin sorumlusu olarak kabul edilen -soruşturma makamlarının tanımlaması ile- Fettullahçı Terör Örgütü/Paralel Devlet Yapılanması (FETÖ/PDY) isimli oluşuma üye ya da yönetici olmak suçlaması ile yürütülmektedir.

Bahsi geçen yargılamalarda bir kısım –soruşturma makamlarının tanımlaması ile- kriterler belirlendiği ve bu kriterlere haiz olan kimselerin FETÖ/PDY isimli yapının üyesi ya da yöneticisi oldukları iddiası ile haklarında mahkumiyet kararları verildiği de bilinen bir gerçektir. Soruşturma makamları ile Milli İstihbarat Teşkilatının çalışmaları neticesinde FETÖ/PDY isimli yapının üyesi ya da yöneticisi olmak hususunda, "ByLock" isimli uygulamanın kullanıcısı olmak şeklinde bir kriter kabul edilmiştir. Soruşturma makamları "ByLock" isimli uygulamanın "münhasıran" FETÖ/PDY isimli yapının üyesi ya da yöneticisi olan kimselerin aralarında haberleşmek maksadıyla kullandığını iddia etmiş, bu görüş Yargıtay kararlarında büyük ölçüde kabul görmüştür. Bununla birlikte pek çok hukukçu, soruşturma makamlarının bu iddiasının maddi hakikati ortaya koymadığını

ve “ByLock” isimli uygulamaya ait olduğu iddia olunan yazışma vb. içeriklerin elde ediliş biçiminin, istihbari faaliyet kapsamında olması ve dijital verilerin elde edilmesine ilişkin usul kurallarına riayet edilmemiş olması nedeniyle hukuka aykırı olduğu görüşünü belirtmiştir.

Soruşturma makamları ByLock kullanım iddiasını zaman zaman yalnızca CGNAT kayıtlarına, zaman zamansa bu CGNAT kayıtları da kullanılarak oluşturulduğu iddia olan Tespit ve Değerlendirme Tutanağı başlıklı detaylı kullanıcı profili ve kullanım içeriği bilgisi içeren bir kısım evraklara dayandırmaktadır. Bu noktada soruşturma makamlarının iddiası ile Yargıtay kararları arasında bir yeknesaklık olmadığı, Yargıtay kararlarında CGNAT verilerine dayandırılan ByLock kullanım iddiasının “mahkumiyete yeterli delil” olarak değerlendirilmediği anlaşılmaktadır. Bu noktada Yargıtay 16. Ceza Dairesi 2018/187E. 2018/1462K. sayılı 27.03.2018 tarihli kakarında CGNAT kayıtlarına ilişkin şu içtihat kararı verilmiştir; “*Ayrıntıları Yargıtay Ceza Genel Kurulunun 26.09.2017 tarih, 2017/16.MD-956 E, 2017/370 sayılı kararı ile onanarak kesinleşen Dairemizin ilk derece mahkemesi sıfatıyla verdiği 24.04.2017 tarih, 2015/3 Esas, 2017/3 sayılı kararında açıklandığı üzere; ByLock iletişim sistemi FETÖ/PDY silahlı terör örgütü mensuplarının kullanmaları amacıyla oluşturulan ve münhasıran bu suç örgülünün bir kısım mensupları tarafından kullanılan bir ağ olması nedeniyle; örgüt talimatı ile bu ağa dahil olunduğunun ve gizliliği sağlamak için haberleşme amacıyla kullanıldığının, her türlü şüpheden uzak, kesin kanaate ulaştıracak teknik verilerle tespiti halinde, kişinin örgütle bağlantısını gösteren bir delil olacaktır. ByLock uygulaması programını indirmek, mesajlaşmak/haberleşmek için yeterli değildir. Öncelikle kayıt esnasında kullanıcının bir kullanıcı adıyla parola üretmesi,*

mesajlaşma için ise kayıt olan kullanıcılara sistem tarafından otomatik olarak atanan ve kullanıcıya özel olan ID (kimlik) numarasının bilinmesi ve karşı tarafça onaylanması gerekmektedir. Karşılıklı ekleme olmaksızın iletişime geçme imkanı bulunmamaktadır. ByLock iletişim sisteminde bağlantı tarihi, bağlantıyı yapan IP adresi, hangi tarihler arasında kaç kez bağlantı yapıldığı, haberleşmelerin kimlerle gerçekleştirildiği ve içeriğinin ne olduğu tespit edilebilmektedir. Bağlantı tarihinin, bağlantıyı yapan IP adresinin tespit edilmesi ve hangi tarihler arasında kaç kez bağlanıldığının belirlenmesi, kişinin özel bir iletişim sisteminin bir parçası olduğunun tespiti için yeterlidir. Haberleşmelerin kimlerle yapıldığı ve içeriğinin ne olduğunun saptanması ise kişinin örgüt içindeki konumunu tespit etmeye yarayacak bilgilerdir. ByLock kullanıcı tespitleri ByLock sunucusunda kayıtlı IP adresleri üzerinden tespit edilebilmektedir. ByLock sunucusunda kaydı olan kullanıcıların User-ID(Kullanıcı No) tespiti yapılabilmekte ve mesaj içeriklerinin çözümü gerçekleştirilebilmektedir. Bu nedenle ByLock tespit değerlendirme tutanağında yer alan User-ID(Kullanıcı No), şifre ve gruba kayıtlı kişilerin tespiti bu kişilerin birbirleriyle olan ilişki ve irtibatlarının ortaya konulması sanığın hukuki durumunun belirlenmesi bakımından önemlidir. ByLock kullanıcılarının tespitleri açısından operatörler tarafından tutulan CGNAT (HIS)kayıtları bir çeşit üst veridir. CGNAT kayıtları özet veriler olması nedeniyle bir iz ve emare niteliğinde olduğundan tek başına kişinin gerçek ByLock kullanıcısı olduğunu göstermez. Kişiler iradeleri dışında ByLock sunucularına yönlendirilmiş olabilirler. Nitekim Ankara Cumhuriyet Başsavcılığı nezdinde yürütülen ve BTK tarafından yapılan teknik çalışmalar sonucunda iradeleri dışında ByLock sunucularına yönlendirildikleri saptanan 11.480 kişinin tamamının CGNAT kayıtlarının olduğu ve tespit

edilen CGNAT kayıtlarına göre ByLock uygulamasının IP'lerine bağlantıya yönlendirildikleri belirtilmektedir. Kişinin User-ID ve şifrelerinin belirlenememesi ve fakat CGNAT kayıtlarıyla ByLock sunucusuna bağlantı yaptığının tespit edilmesi halinde, kişinin gerçek ByLock kullanıcısı olduğu ancak henüz User-ID ve şifresinin tespit edilemediği anlaşılabileceği gibi; ByLock sunucularına tuzak yöntemlerle (Morbeyin vb.) yönlendirilmiş olabileceği sonucuna da ulaşılabilir. Bu nedenle ancak operatör kayıtları ve User-ID eşleştirmesi doğru yapılabilen kişilerin gerçek ByLock kullanıcısı olduklarının kabulü gerekeceğinden, kişinin örgütsel gizliliği sağlamak ve haberleşmek amacıyla ByLock sistemine girdiğinin ve bu sistemi kullandığının, User-ID, şifre ve grup elemanlarını içerir ByLock tespit değerlendirme tutanağı ve CGNAT kayıtlarını içeren belgeler ile kesin olarak kanıtlanması zorunludur."

Görüldüğü üzere Yargıtay, bu kararı ile Yargıtay Ceza Genel Kurulu'nun "ByLock isimli uygulamanın münhasıran FETÖ/PDY yapılanması üye ve yöneticileri arasında kullanılmak amacıyla oluşturulduğu" yönündeki soruşturma makamının teorilerine dayanan görüşüne ilişkin bir istisna getirmiştir. Yargıtay, morbeyin hadisesine atıf yaparak CGNAT kayıtlarının bir kimsenin ByLock kullanıcısı olduğunu göstermeye yetecek delil niteliği taşımadığına hükmetmiştir.

Yargıtay'ın bu görüşü, başta savunma görevini ifa eden Avukatlar olmak üzere pek çok hukukçunun "ByLock" isimli uygulamaya ait olduğu iddia olunan yazışma vb. içeriklerin elde ediliş biçiminin istihbari faaliyet kapsamında olması ve dijital verilerin elde edilmesine ilişkin usul kurallarına riayet edilmemiş olması nedeniyle bu verilerin kullanılmasının hukuka aykırı olduğu, buna rağmen soruşturma makamlarınca

dosyalara kazandırılan pek çok yazışma içeriğinin silahlı terör örgütü üyeliği suçlamasına konu edilebilecek mahiyette olmadığı, yönündeki görüşlerini tartışılabilir olmaktan uzaklaştırmıştır. Gelinen aşamada ByLock kullanım iddiası kapsamındaki yargılamalar, teknik gerçeklikler bakımından bir kimsenin ByLock kullanıcısı olup olmadığının tespiti özelinde yürütülmektedir. Bunun istisnası olarak kabul edilebilecek Yargıtay kararı, Yargıtay 16. Ceza Dairesinin 2019/11650E. 2020/3039K. sayılı 25.06.2020 tarihli kararıdır. Kararda, hakkında ByLock kullanıcısı olduğu gerekçesiyle mahkumiyet kararı verilmiş sanıklardan S.O. bakımından yapılan temyiz incelemesi neticesinde "*Yargıtay Ceza Genel Kurulu tarafından onanarak kesinleşen dairemizin ilk derece mahkemesi sıfatıyla verdiği 24.04.2017 tarih, 2015/3 esas, 2017/3 karar sayılı kararında, "Bylock iletişim sisteminin FETÖ/PDY silahlı terör örgütü mensuplarının kullanmaları amacıyla oluşturulan ve münhasıran bu suç örgütünün bir kısım mensupları tarafından kullanılan bir ağ olması nedeniyle; örgüt talimatı ile bu ağa dahil olunduğunun ve gizliliği sağlamak için haberleşme amacıyla kullanıldığının, her türlü şüpheden uzak, kesin kanaate ulaştıracak teknik verilerle tespiti halinde, kişinin örgütle bağlantısını gösteren delil olacağı"nın kabul edildiği dikkate alınarak, somut dosyada sanık S.'in kullandığını kabul ettiği 168979 ID numaralı Bylock'ta sadece diğer sanık Ö.'ın ekli olması ve yazışma içeriklerinin örgütsel nitelikte olmadığının anlaşılmasına rağmen hatalı değerlendirmeyle sanığın, örgüt talimatı ile bu ağa dahil olunduğunun ve gizliliği sağlamak için haberleşme amacıyla kullanıldığının kabul edilerek yazılı şekilde mahkumiyetine karar verilmesi, Kanuna aykırı, sanık müdafiinin temyiz itirazları bu nedenlerle yerinde görülmüş olduğundan hükmün bu sebepten dolayı CMK'nın 302/2.*

maddesi uyarınca BOZULMASINA" şeklinde bir bozma kararı verilmiştir.

Bu gibi istisnai kararlar dışında Yargıtay, CGNAT kayıtlarının tek başına kişinin ByLock kullanıcısı olduğunu göstermeyeceği yönündeki görüşünü uzun süre devam ettirmiştir. Bu görüş kapsamında, yalnızca CGNAT kayıtları gerekçe gösterilerek ByLock kullanıcısı olduğu iddiasıyla haklarında TCK 314/2 kapsamında mahkumiyet kararı verilmiş sayısız sanık bakımından yapılan temyiz incelemelerinde BOZMA yönünde kararlar verilmiştir. Bu kararlar gerekçe edilerek, ilk derece mahkemeleri ile Bölge Adliye Mahkemelerince verilmiş beraat kararları da mevcuttur. Hal böyle olmakla birlikte, soruşturma makamları, yalnızca CGNAT kayıtlarına dayanarak kişilerin ByLock kullanıcısı olduğu yönündeki iddialar kapsamında iddianame düzenlemek hususundaki tutumlarında değişikliğe gitmemiştir.

Yargıtay, bir kimsenin ByLock kullanıcısı olarak kabul edilebilmesi için, Tespit ve Değerlendirme Tutanağı isimli kolluk evrakının varlığını zorunlu gören görüşüne zaman içinde bir istisna getirmiştir. Bu istisna kapsamında verilen pek çok kararda matbu şekilde şu ifade yer almaktadır; "*Dairemizin 20.02.2018 tarih ve 2017/3618 Esas, 2018/705 sayılı kararı ile "ByLock iletişim sisteminin" FETÖ/PDY silahlı terör örgütü mensuplarının kullanmaları amacıyla oluşturulan ve münhasıran bu suç örgütünün bir kısım mensupları tarafından kullanılan bir ağ olması nedeniyle; örgüt talimatı ile bu ağa dahil olunduğunun ve gizliliği sağlamak için haberleşme amacıyla kullanıldığının, her türlü şüpheden uzak, kesin kanaate ulaştıracak teknik verilerle tespiti halinde, kişinin örgütle bağlantısını gösteren delil olduğunun kabul edildiği dikkate alınarak, somut dosyada sanığın üzerine kayıtlı*

bulunan hatlar bakımından ByLock kullanıcısı olup olmadığının atılı suçun sübutu açısından belirleyici nitelikte olması karşısında; ByLock "Tespit ve Değerlendirme Tutanağı"nın dosyaya getirtilmesi, değerlendirme ve tespit tutanağının temin edilememesi halinde, operatör kayıtları ile eşleştirmesi yapılmak üzere ***Bilgi Teknolojileri ve İletişim Kurumundan getirtilen CGNAT kayıtları ve dosya içerisindeki HTS sonuçları karşılaştırılıp belirtilen hat üzerinden ByLock kullanan kişinin sanık olup olmadığı doğrultusunda bilirkişiden teknik rapor alınarak yargılamaya devamla bir hüküm kurulması gerekirken eksik araştırma ile yazılı şekilde hüküm kurulması,***" (Yargıtay 3.C.D. 2021/6372E. 2021/10700K.)

Pek çok kararda aynen ya da eş anlama gelecek şekilde yer alan yukarıdaki değerlendirme neticesinde, yerel mahkemelerde, Yargıtay'ın CGNAT ve HTS kayıtları üzerinde yapılacak bilirkişi incelemesini, Tespit ve Değerlendirme Tutanağı başlıklı kolluk evrakına eş değer gördüğü ve Tespit ve Değerlendirme Tutanağının mevcut olmadığı durumlarda "ByLock kullanan kişinin sanık olup olmadığı" hususunun tespiti bakımından bu teknik incelemenin yapılmasının zaruri olarak değerlendirdiği kanaati oluşmuştur.

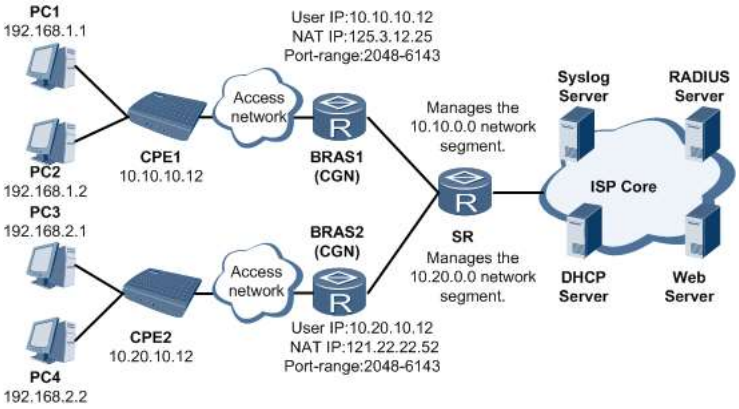
Yargıtay'ın bu kararlarının akabinde, yerel mahkemeler tarafından yaptırılan bilirkişi incelemelerinde sıklıkla, HTS ve CGNAT kayıtlarının uyumluluğunu tespite ilişkin raporlarla karşılaşılmıştır. Bu incelemelerin bir kısmının yanlış verilerin karşılaştırılması bir kısmının ise uyumluluğu kesin olması gereken verilerin karşılaştırılmasına dayandığı görülmektedir. Karşılaştırmalarda iletişim kayıtları içerisinde yer alan ilgili Baz İstasyonu bilgisinin kullanıldığı görülmektedir.

Bu gelişmeler ışığında, yukarıda kısaca özetlenen ByLock kullanım iddiasına konu yargılamalarda hala devam eden tartışmaların beraberinde yeni bir değerlendirme yapmak ihtiyacı doğurmuştur. Bu çalışma yukarıda da ifade edilen tartışmalara ilişkin, kamuoyuna deklare edilmiş görüşlerin yanında, ortaya çıkan bu yeni tartışma bakımından görüşleri ifade etmek maksadıyla hazırlanmıştır. **Bu nedenle çalışmanın kapsamı ByLock kullanım iddiasına konu yargılamalardaki diğer hukuki ve teknik tartışmalardan bağımsız olarak yalnızca CGNAT ve HTS kayıtlarının karşılaştırılması ile bir kimsenin ByLock kullanıcısı olup olmadığının tespiti yönündeki Yargıtay kararlarına ilişkin değerlendirmeleri kapsamaktadır.**

2. CGNAT Nedir?

CGNAT yapısını anlatmak için öncelikle NAT yapısını anlamalıyız. NAT bir ağda bulunan bilgisayarın, telefonun, vb. kendi ağı dışında başka bir ağa veya internete çıkarken farklı bir IP adresi kullanabilmesi için geliştirilmiş bir internet protokolüdür. NAT kullanılması ve ortaya çıkması IPv4 ile yetersiz IP adresinden kaynaklanır. İnternette bazı adresler yerel ağlarda kullanılmak amacıyla özel olarak ayrılmışlardır. Bu IP adresleri aşağıdaki gibidir.

10.0.0.0/8 yani 10.0.0.0 ile 10.255.255.255 arasındaki IP adresleri, 172.16.0.0/12 yani 172.16.0.0 ile 172.31.255.255 arasındaki IP adresleri ve 192.168.0.0/16 yani 192.168.0.0 ile 192.168.255.255 arasındaki IP adresleri alt ağ oluşturmak için özel olarak ayrılmıştır. NAT protokolünün çeşitleri vardır. NAT44, NAT444, NAT64 gibi. Normal NAT, NAT44 olarak geçer. Sonda bulunan 44 numarası iki tane IPv4 ile çalıştığını belirtir. Yani iç ağda bir IP adresi dış ağda ayrı bir IP adresi. CGNAT yani NAT444 ise 3 tane IPv4 adresi kullanır. Aşağıdaki şeklideki örneklemek gerekirse.



Internet Servis Sağlayıcılar CGN IP kullanımına neden olarak iPv4 adreslerinin yetmediğini gösteriyor.Dünyadaki cihazların artması ve internet abonelerinin hızla çoğalması neticesinde IPv4 adres sınırı olan 4 milyar sayısına yaklaşılmıştır. Internet Servis sağlayıcılarda bu nedenle tek bir IP adresini birden fazla abonesine tahsis edebilmek için kullanabilmektedirler.

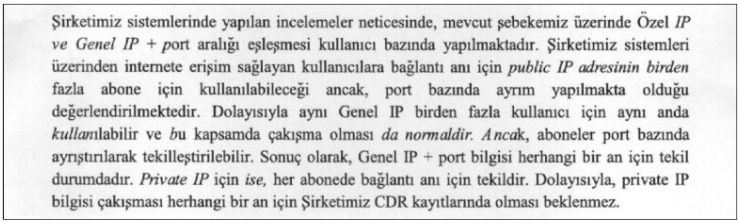
Bir kısım davalarda, sanık ve sanık avukatlarının IP adreslerinin operatörler tarafından birden fazla aboneye tahsis edilmiş olması nedeni ile IP adresine bağlı olarak kişinin ByLock kullanıcısı olduğuna dair bir tespit yapılamayacağı, ByLock kullanan bir başka kişi ile IP adreslerinin çakışması, yani operatör tarafından aynı IP adresinin hem bir ByLock kullanıcısına hem de ByLock kullanmayan kişiye tahsis edilmesi nedeni ile kişinin ByLock kullanmış gibi göründüğü yönünde savunmalar geliştirildiği görülmektedir.

Ancak ne var ki, operatör açısından bir abonenin tespiti yalnızca IP adresine değil bununla birlikte aboneye tahsis edilen Port bilgisi ile birlikte yapılmaktadır. Bu nedenle evet kişinin yalnızca CGNAT kaydının varlığına dayalı olarak ByLock kullandığı yönünde bir tespitte bulunabilmek mümkün değildir ancak bir başka kişi ile aynı IP adresine sahip olmak da kişinin ByLock kullanıcısı olup olmaması ile ilgili değildir.

IP adresi çakışması olarak ifade edilen, birden fazla aboneye aynı IP adresinin tahsis edilmesi nedeni ile ByLock kullanmayan kişilerin olmadığı halde CGNAT kaydının var olmasına dayalı bu savunmanın herhangi bir teknik geçerliliğe sahip olamayacağı açıktır.

Bu konu Avea İletişim Hizmetleri A.Ş. tarafından Bilgi Teknolojileri ve İletişim Kurumuna yazılan 05/06/2017 tarihli

yazıda açıklanmış abonelerin IP adresi ve Port bilgileri ile ayrıştırıldığı açık bir şekilde ifade edilmiştir.



Şirketimiz sistemlerinde yapılan incelemeler neticesinde, mevcut şebekemiz üzerinde Özel *IP ve Genel IP + port* aralığı eşleşmesi kullanıcı bazında yapılmaktadır. Şirketimiz sistemleri üzerinden internete erişim sağlayan kullanıcılara bağlantı anı için *public IP adresinin birden* fazla abone için kullanılabileceği ancak, port bazında ayrım yapılmakta olduğu değerlendirilmektedir. Dolayısıyla aynı Genel IP birden fazla kullanıcı için aynı anda *kullan*ılabilir ve *b*u kapsamda çakışma olması *da normaldir. A*ncak, aboneler port bazında ayrıştırılarak tekilleştirilebilir. Sonuç olarak, Genel IP + port bilgisi herhangi bir an için tekil durumdadır. *Private IP* için *ise,* her abonede bağlantı anı için tekildir. Dolayısıyla, private IP bilgisi çakışması herhangi bir an için Şirketimiz CDR kayıtlarında olması beklenmez.

CGNAT Sisteminin kullanımı ve adli vakalarda delil niteliği hakkında daha fazla bilgi için https://www.adlibilisimci.com/ortak-raporlar/adresinde yer alan "ByLock Uygulaması, Gerçek Kullanıcıların Tespiti" başlıklı yazımızı okumanız önerilir.

3. CGNAT Kayıtları İle HTS İletişim Kayıtlarının Karşılaştırılması

Bu noktada öncelikle bahsi geçen verilerin nasıl elde edildiği, saklandığı ve soruşturma dosyalarına hangi usul ile kazandırıldığını anlamak gerekmektedir. Zira, bir ceza yargılamasında temel amaç maddi gerçekliğe ulaşmaktır. Maddi gerçekliğe ulaşabilmenin öncelikli yolu ise, hukuka uygun olarak elde edilmiş, hiçbir şüpheye yer bırakmayacak şekilde maddi gerçeği ortaya koyabilen delillerin elde edilebilmesidir.

Bilindiği üzere iletişim verileri işbu hizmeti sunan operatörler tarafından üretilmektedir. Operatör şirketleri söz konusu verileri saklamakla yükümlüdür. Bununla birlikte saklama süresine sınırlama getirilmiştir. Konuya ilişkin yasal düzenlemenin yapıldığı Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği md.19/f'de 11.06.2016 tarihinde yapılan değişiklikle HTS ve CGNAT kayıtlarına ilişkin verilerin 2 yıl süreyle operatör şirketleri tarafından saklanması öngörmüştür. Bu çalışma bakımından dikkat edilmesi gereken husus yönetmeliğin ilgili maddesinin 11.06.2016 tarihinde değiştirilmiş olmasıdır. Öyle ki, değişiklik öncesi bu süre bir yıldır ve değişikliğe kadar erişim sağlayıcılar ve işletmeciler sadece "kullanıcı sayısı, kimlik bilgileri, görüşme süreleri ve altyapısı üzerinden gerçekleşen görüşmelere ait trafik bilgilerini" saklamakla yükümlüdürler. Başka bir ifadeyle, değişiklikle Yönetmeliğe eklenen "IP adresi, port aralığı, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü ve aktarılan veri miktarı" yani CGNAT kayıtlarını oluşturan verilerin, erişim sağlayıcıları ve telefon hizmeti sunan işletmeciler tarafından saklanması

mümkün değildir. Özetle, ByLock programının kullanılabilir olduğu tarih aralığında (Nisan 2014-Şubat2016) CGNAT kayıtlarını oluşturan verilerin saklanabilmesi için yasal bir dayanak mevcut değildir. HTS kayıtları ise operatör şirketleri tarafından bir yıl süreyle saklanabilmektedir.

Uygulamada, bu verilerin operatörler tarafından saklanmasının akabinde BTK'ya gönderildiği anlaşılmaktadır. Verinin BTK tarafından ne kadar süreyle saklanabileceğine ilişkin yasal mevzuatta bir açıklık bulunmamakla birlikte, esasen, bu verinin BTK tarafından operatörden temin edilebileceğine ilişkin bir düzenleme de mevcut değildir. Öyle ki, Anayasa Mahkemesi (AYM), 5651 sayılı Kanun'un 5/5. maddesinde yer alan; "Yer sağlayıcı, Kurumun talep ettiği bilgileri talep edilen şekilde Kuruma teslim etmekle ve Kurum tarafından bildirilen tedbirleri almakla yükümlüdür" ifadesi ile erişim sağlayıcıların; "Kurumun talep ettiği bilgileri talep edilen şekilde Kuruma teslim etmekle ve Kurum tarafından bildirilen tedbirleri almakla" yükümlü olduklarını belirten 6/1-d maddesindeki ifadeyi; "…bu çerçevede iptali istenilen kurallarda, TİB'in (BTK) hangi koşullarda ve hangi gerekçelerle istediği bilgilerin içerik, yer ve erişim sağlayıcılar tarafından Başkanlığa teslim edileceğine ya da verilen bilgilerin ne kadar süre ile TİB'de saklanacağına, talep edilen bilgilerin mahiyetine, içerik, yer ve erişim sağlayıcılara bildirilecek tedbirlere ilişkin herhangi bir belirlilik bulunmamaktadır. Kurallar bu yönleriyle belirli ve öngörülebilir değildirler. Anayasa'da yer alan güvenceye rağmen, kişilere ait her türlü kişisel veri, bilgi ve belgelerin konu, amaç ve kapsam bakımından yeterli sınırlamaya tabi kılınmaksızın koşulsuz olarak TİB'e verilmesine imkân tanımakta, böylece kişiler idareye karşı korumasız hale getirilmektedirler. Dolayısıyla iptali istenilen kurallar, belirli ve öngörülebilir olmadığından kişilerin kişisel verilerin korunması

hakkını ölçüsüzce sınırlandırmakta ve Anayasa'nın 20. maddesine aykırılık teşkil etmektedir. Açıklanan nedenlerle kurallar, Anayasa'nın 2., 13. ve 20. maddelerine aykırıdır" demek suretiyle iptal etmiştir. Bu yönüyle HTS ve CGNAT kayıtlarının BTK tarafından operatörlerden temin edilmesi ve depolanması uygulaması tamamen yasal dayanaktan yoksun kalmıştır.

Tüm bunların yanında, AİHM geçmişten beri vermiş olduğu kararlarda, kişilerin iletişim verilerinin kamu kurumları tarafından süresiz olarak saklanmasının ya da saklanma süresine ilişkin yasal mevzuatta açıklık bulunmamasının AİHS md. 8'de düzenlenen özel yaşam ve aile hayatının korunması hakkına aykırı olduğuna hükmetmiştir. Bu kapsamdaki güncel kararlardan Ekimdzhiev ve Diğerleri/Bulgaristan (B. No: 70078/12, 11/01/2022) kararında "Yetkililer tarafından erişilen iletişim verilerinin saklanması, erişilmesi, incelenmesi, kullanılması, iletilmesi ve imha edilmesi konusunda kamuya açık kurallar mevcut değildir" denmek suretiyle yasal mevzuatın yeterli açıklıkta olmaması hak ihlali kararına gerekçe edilmiştir. Türkiye mevzuatı bakımından da benzer durumun yaşandığı aşikardır.

Tüm bunların yanında, söz konusu verilerin yalnızca bir kamu kurumu olan Bilgi Teknolojileri Kurumunda saklanmasının ve soruşturma makamlarınca bu kaynaktan temin edilmesinin, şüpheli ve/veya sanıkların silahlı terör örgütü üyeliği ile suçlanması bir arada değerlendirildiğinde şüpheli ve/veya sanıkların Avrupa İnsan Hakları Sözleşmesinde adil yargılanma hakkının bir parçası olarak düzenlenmiş silahların eşitliği ilkesinin ihlaline neden olduğu aşikardır.

Hal böyle olmasına ve bu hususta itirazların başta savunma görevini ifa eden Avukatlar olmak üzere pek çok hukukçu tarafından dile getirilmesine rağmen, Yargıtay bu kayıtların saklanması ve soruşturma dosyalarına kazandırılmasını hukuka uygun kabul etmektedir. Bu nedenle işbu çalışmanın konusu olan HTS ve CGNAT kayıtları üzerinde bilirkişi incelemesi yaptırılması yönündeki kararları vermiştir.

Uygulamada, Yargıtay kararlarında bahsi geçen bilirkişi incelemesinin CGNAT kayıtlarına yer alan baz istasyonu bilgisi ile HTS kayıtları içerisinde iletişim (mesaj ve görüşmeler) kayıtlarında yer alan baz istasyonu bilgilerinin karşılaştırılması suretiyle yapıldığı anlaşılmaktadır.

CGNAT kayıtlarının birbiri ardına gelen belirli bir dizi niteliğinde olması, HTS/İletişim Kayıtlarının ise iletişimin türüne göre belirli bir anda gerçekleşen kayıtlar olması nedeni ile zamansal olarak, eş zamanlı kayıtların görülmesi pek mümkün olmasa da, yakın zamanlı kayıtların karşılaştırılması veya CGNAT ve HTS/İletişim kayıtlarının tek bir listeye dönüştürülüp, zamansal olarak sıralanmasının yapıldığı görülmektedir.

Bu durumda, birbiri ardına yakın zamanlı CGNAT ve HTS/İletişim Kayıtlarına ait baz istasyonu bilgilerinin aynı veya farklı olup olmadıkları belirlenmektedir.

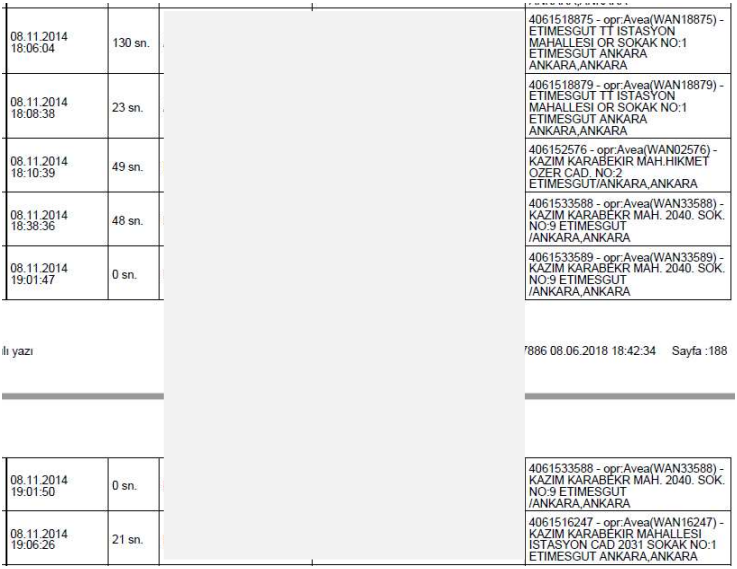
Bu kıyaslama sonucu her ne olursa olsun, kişinin aleyhine yorumlanmakta, uyumlu ise kişinin ByLock kullandığı, uyumsuz ise uyumsuzluk da olabileceği ifade edilmektedir.

Baz istasyonu bilgisinin farklı olabileceğine örnek olarak aşağıdaki 08.11.2014 18:08:21 ile 08.11.2014 19:07:05 zaman

aralığında CGNAT kayıtlarında yer alan baz istasyonu bilgisi "(4062539259 - opr:Avea(WAN39259)" olarak görülmektedir.

08.11.2014 18:08:21	46.166.164.177	443	4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA
08.11.2014 18:08:22	46.166.164.177	443	4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA
08.11.2014 18:08:22	46.166.164.177	443	4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA
08.11.2014 18:08:26	46.166.164.177	443	4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA
08.11.2014 19:06:52	46.166.164.177	443	4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA
08.11.2014 19:06:54	46.166.164.177	443	4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA
08.11.2014 19:06:55	46.166.164.177	443	4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA
08.11.2014 19:06:57	46.166.164.177	443	4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA
08.11.2014 19:07:00	46.166.164.177	443	4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA
08.11.2014 19:07:02	46.166.164.177	443	4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA
08.11.2014 19:07:05	46.166.164.177	443	4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA

Aynı zaman aralığında HTS/İletişim Kayıtlarında yer alan baz istasyonu bilgilerinin sırası ile "1) 4061518875-opr:Avea(WAN18875), 2) 4061518879-opr:Avea(WAN18879), 3) 406152576-opr:Avea(WAN02576), 4) 4061533588-opr:Avea(WAN33588), 5) 4061533589-opr:Avea(WAN33589), 6) 4061533588-opr:Avea(WAN33588) ve 7) 4061516247-opr:Avea(WAN16247)" olduğu görülmektedir.



08.11.2014 18:06:04	130 sn.		4061518875 - opr:Avea(WAN18875) - ETIMESGUT TT ISTASYON MAHALLESI OR SOKAK NO:1 ETIMESGUT ANKARA ANKARA,ANKARA
08.11.2014 18:08:38	23 sn.		4061518879 - opr:Avea(WAN18879) - ETIMESGUT TT ISTASYON MAHALLESI OR SOKAK NO:1 ETIMESGUT ANKARA ANKARA,ANKARA
08.11.2014 18:10:39	49 sn.		406152576 - opr:Avea(WAN02576) - KAZIM KARABEKIR MAH.HIKMET OZER CAD. NO:2 ETIMESGUT/ANKARA,ANKARA
08.11.2014 18:38:36	48 sn.		4061533588 - opr:Avea(WAN33588) - KAZIM KARABEKR MAH. 2040. SOK. NO:9 ETIMESGUT /ANKARA,ANKARA
08.11.2014 19:01:47	0 sn.		4061533589 - opr:Avea(WAN33589) - KAZIM KARABEKR MAH. 2040. SOK. NO:9 ETIMESGUT /ANKARA,ANKARA

lı yazı

7886 08.06.2018 18:42:34 Sayfa :188

08.11.2014 19:01:50	0 sn.		4061533588 - opr:Avea(WAN33588) - KAZIM KARABEKR MAH. 2040. SOK. NO:9 ETIMESGUT /ANKARA,ANKARA
08.11.2014 19:06:26	21 sn.		4061516247 - opr:Avea(WAN16247) - KAZIM KARABEKIR MAHALLESI ISTASYON CAD 2031 SOKAK NO:1 ETIMESGUT ANKARA,ANKARA

Yani CGNAT kayıtlarında yer alan baz istasyonu bilgisi ile HTS/İletişim Kayıtlarında yer alan baz istasyonu bilgisinin birbirinden farklı olması olağan bir durumdur.

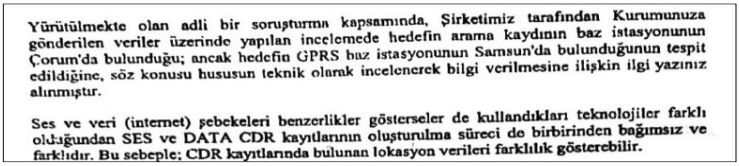
Bu nedenle de, kayıtlar arasındaki baz istasyonu uyumluluğu veya uyumsuzluğu herhangi bir kişinin ByLock uygulaması kullandığına dair bir tespit niteliği taşımamaktadır.

Uyumsuzluk tespit edilmişse, bunun anlamı, kişinin Internet bağlantısı kesilmeksizin baz istasyonları arasında hareket halinde olduğu, bu hareketlilik sırasında CGNAT kayıtlarının ilk bağlantı kurulan baz istasyonu bilgisini gösterirken HTS/İletişim Kayıtlarının her bağlantıda uygun en yakın baz istasyonu bilgisini göstermesidir. Uyumluluk ise, kişinin hareket halinde olmaması durumunda ortaya çıkacaktır.

Bu konu Avea İletişim Hizmetleri A.Ş. tarafından Bilgi Teknolojileri ve İletişim Kurumuna yazılan 25/10/2017 tarihli yazıda açıklanmıştır.

Yazının ilk paragrafında talebin hedef arama kaydında yer alan baz istasyonunda yer alan şehir ile GPRS kayıtlarında yer alan şehir bilgisinin birbirinden farklı olmasının nedeninin sorulduğu görülmektedir.

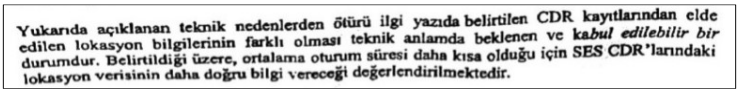
İkinci paragrafta ise, SES (HTS/İletişim Kayıtları) ile DATA (HTS/GPRS Kayıtları) CDR (Call DetailReporting-Arama Detayı Raporlama) kayıtlarının oluşturulma süreçlerinin farklı olması nedeni ile lokasyon verilerinin farklılık gösterebilir açıklamasının yapıldığı görülmektedir.



Yürütülmekte olan adli bir soruşturma kapsamında, Şirketimiz tarafından Kurumunuza gönderilen veriler üzerinde yapılan incelemede hedefin arama kaydının baz istasyonunun Çorum'da bulunduğu; ancak hedefin GPRS baz istasyonunun Samsun'da bulunduğunun tespit edildiğine, söz konusu hususun teknik olarak incelenerek bilgi verilmesine ilişkin ilgi yazınız alınmıştır.

Ses ve veri (internet) şebekeleri benzerlikler gösterseler de kullandıkları teknolojiler farklı olduğundan SES ve DATA CDR kayıtlarının oluşturulma süreci de birbirinden bağımsız ve farklıdır. Bu sebeple; CDR kayıtlarında bulunan lokasyon verileri farklılık gösterebilir.

Yazının son paragrafında ise, CDR kayıtlarından elde edilen lokasyon bilgilerinin farklı olmasının teknik anlamda beklenen ve kabul edilebilir bir durum olduğundan bahsedildiği görülmektedir.



Yukarıda açıklanan teknik nedenlerden ötürü ilgi yazıda belirtilen CDR kayıtlarından elde edilen lokasyon bilgilerinin farklı olması teknik anlamda beklenen ve ***kabul edilebilir bir*** durumdur. Belirtildiği üzere, ortalama oturum süresi daha kısa olduğu için SES CDR'larındaki lokasyon verisinin daha doğru bilgi vereceği değerlendirilmektedir.

CDR kayıtları içerisinde lokasyon bilgisini gösterir verinin baz istasyonu bilgisi olduğu bilinmekle birlikte, yazıdan da anlaşılacağı üzere, HTS/İletişim Kayıtlarına ait baz istasyonu ile, HTS/GPRS kayıtlarında yer alan baz istasyonunun farklı

şehirlerde olması dahi olağan bir durumdur. İzah edildiği üzere önemli olan kişinin baz istasyonları arasında herhangi bir bağlantı kesilmesi (baz istasyonları arasında kapsama alanı boşluğu veya bağlantı sağlanamayan asansör gibi bir kapalı alana girme) olmadığı sürece, zaman aşımı süresi dahilinde (genellikle 7200 saniye) kişinin HTS/İletişim Kayıtları ile HTS/GPRS Kayıtları arasındaki baz istasyonu uyumluluğu da uyumsuzluğu da olağan bir durumdur.

4. CGNAT Kayıtları İle HTS/GPRS Kayıtlarının Karşılaştırılması

Bir diğer karşılaştırma ise CGNAT kayıtlarına yer alan baz istasyonu bilgisi ile HTS kayıtları içerisinde GPRS (internet bağlantısı) kayıtlarında yer alan baz istasyonu bilgilerinin karşılaştırılması yapılmaktadır.

CGNAT kayıtlarının birbiri ardına gelen belirli bir dizi niteliğinde olması, HTS/GPRS Kayıtlarının ise belirli bir başlangıç zamanı ve süresi ile birlikte kaydedildiği bilinmektedir.

HTS/GPRS kayıtları, kişinin Internete bağlanması ile operatörü tarafından kendisine tahsis edilen bir IP adresi ile Internet hizmetlerinden faydalanabilmesi için ön koşuldur.

CGNAT kayıtları ise, kişinin Internete bağlanması sonrasında, faydalandığı belirli bir IP adresi ile olan veri iletişimleridir.

Bu durumda CGNAT kayıtlarının var olabilmesi için önce buna bağlı HTS/GPRS kayıtlarının olması gerekmektedir. Yani, HTS/GPRS kaydı olmaksızın CGNAT kaydının var olması imkansızdır.

Zamansal olarak, bir CGNAT kayıt dizisinin başlangıç zamanının, herhangi bir HTS/GPRS kaydının başlangıç zamanından sonra, CGNAT kayıt dizisinin bitiş zamanının ise, HTS/GPRS kaydının bitiş zamanından önce olması gerekmektedir. Bu koşul sağlandığında, CGNAT kayıt dizisinin belirli bir HTS/GPRS kaydının bağlantı süresi içerisinde olduğu tespit edilebilecektir.

Ancak karşılaştırma işlemlerinde, zamansal tutarlılıklar yerine baz istasyonu bilgilerinin aynı veya farklı olup olmadıklarının incelendiği görülmektedir.

CGNAT kayıtlarının, HTS/GPRS kayıtlarına bağımlı olması nedeni ile bu kıyaslama sonucunda baz istasyonlarının farklı olduğu bir durumla karşılaşmak mümkün değildir. Eğer ki bir farklılık tespit edilmişse, bunun sebebi, ilgili operatörün kayıt hatası olduğundan ve kayıtların veri bütünlüğü ve doğruluğunun sağlanamıyor olması nedeni ile dijital delil olarak kullanılmasının sakıncalı olacağından bahsedebilmek mümkündür.

Baz istasyonu bilgisinin aynı olması gerekeceğine örnek olarak, önceki başlık altında yer alan aynı CGNAT kayıtları bu sefer HTS/GPRS kayıtları ile karşılaştırılmıştır. Yukarıda08.11.2014 18:08:21 ile 08.11.2014 19:07:05 zaman aralığında CGNAT kayıtlarında yer alan baz istasyonu bilgisi "(4062539259 - opr:Avea(WAN39259)" olarak görülmektedir.

HTS/GPRS kayıtları incelendiğinde CGNAT kayıtları ile ilgili olabilecek 2 adet GPRS kaydına ait, baz istasyonu bilgilerinin sırası ile "1) (4062539259 - opr:Avea(WAN39259) ve 2) (4062539259 - opr:Avea(WAN39259)" olduğu ve bu baz istasyonu bilgilerinin de CGNAT kayıtlarında yer alan baz istasyonu ile bire bir aynı olduğu görülmektedir.

Gprs	08.11.2014 17:06:53	7199 sn.		4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA
Gprs	08.11.2014 17:12:37	6855 sn.		4062539259 - opr:Avea(WAN39259) - BATIKENT ANDORA IS MRK.,ANKARA

Bu tespitin anlamı, kişinin HTS/GPRS kaydının başladığı zaman (Internet bağlantısının başladığı zaman veya bağlantının güncellendiği zaman) bağlantı kurulan baz istasyonu bilgisi ile

bu bağlantı sırasında oluşan CGNAT kayıtlarının uyumlu olmak zorunda olduğudur.

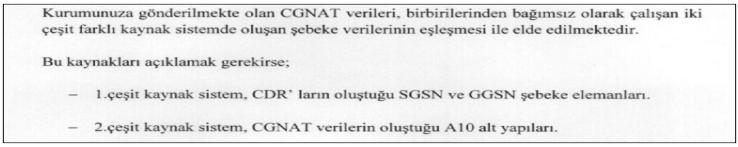
Yani CGNAT kayıtlarında yer alan baz istasyonu bilgisi ile HTS/GPRS Kayıtlarında yer alan baz istasyonu bilgisinin birbirinin aynısı olağan, hatta zorunlu bir durumdur.

Ancak, bu uyumluluk durumu, iletişim sürecinin teknik bir zorunluluğu olup, CGNAT kayıtları kişinin ByLock uygulaması kullandığına dair bir tespit niteliği taşımamaktadır.

CGNAT baz istasyonu bilgisi ile HTS/GPRS baz istasyonu bilgisinin uyumlu olması gerekmekle birlikte, önceki kıyaslama ile birlikte değerlendirildiğinde, HTS/İletişim Kayıtları ile HTS/GPRS Kayıtları arasında baz istasyonu bilgileri karşılaştırılacak olursa, uyumlu olmaları veya uyumsuz olmaları olağan bir durum olacaktır.

Bu konu Turkcell İletişim Hizmetleri A.Ş. tarafından Bilgi Teknolojileri ve İletişim Kurumuna yazılan 13/06/2017 tarihli yazıda ve Vodafone Telekomünikasyon A.Ş. tarafından Bilgi Teknolojileri ve İletişim Kurumuna yazılan 29/09/2017 tarihli yazıda açıklanmıştır.

Turkcell tarafından yazı içerisinde BTK' ya gönderilen HTS (CDR) ve CGNAT kayıtlarının kaynaklarının açıklandığı, CDR kayıtlarının kaynağının SGSN ve GGSN şebeke elemanları olduğu, CGNAT kayıtlarının kaynağının ise A10 alt yapıları olduğunun ifade edildiği görülmektedir.



Kurumunuza gönderilmekte olan CGNAT verileri, birbirilerinden bağımsız olarak çalışan iki çeşit farklı kaynak sistemde oluşan şebeke verilerinin eşleşmesi ile elde edilmektedir.

Bu kaynakları açıklamak gerekirse;

- 1.çeşit kaynak sistem, CDR' ların oluştuğu SGSN ve GGSN şebeke elemanları.
- 2.çeşit kaynak sistem, CGNAT verilerin oluştuğu A10 alt yapıları.

Yazının devamında, ise SGSN ve GGSN şebeke elemanlarından elde edilen veriler içerisinde, bir aboneye Özel IP adresi tahsis edildiği zamanında da CDR kayıtları içerisinde yer aldığının CGNAT kayıtları içerisinde ise oturum başlama tarih saat bilgisi ile beraber Özel IP/Özel Port, Gerçek IP/Gerçek Port eşleşmesi ve Erişilen IP/Erişilen Port bilgilerinin yer aldığının ifade edildiği görülmektedir.

(Burada ifade edilen Gerçek IP/Gerçek Port bilgisinin CGNAT kayıtları içerisinde Genel IP/Genel Port ve Erişilen IP/Erişilen Port bilgilerinin CGNAT kayıtları içerisinde Hedef IP/Hedef Port bilgisi olduğu bilinmektedir.)

Temelde,

- SGSN ve GGSN CDR' larında, Özel IP adresin bir kullanıcıya tahsis edildiği zaman aralığı bilgileri yer almaktadır.
- CGNAT verilerinde ise oturum başlama tarih ve saat bilgisi ile beraber, özel IP/özel Port, gerçek IP/gerçek Port eşleşmesi, erişilen IP/erişilen Port bilgileri yer almaktadır.

Bu noktada paragraf içerisindeki önemli olan ifade, CGNAT kayıtları içerisinde Özel IP/Özel Port bilgisi ile Gerçek IP/Gerçek Port eşleşmesinin yapılmış olduğunun ifade edilmiş olmasıdır. Çünkü bir operatör açısından abonesini tanımlayabilmesi ve ağ içerisinde hizmet verebilmesi için bu tanımlamayı yapabilmesi gerekeceği açıktır. Bu ifadenin bir diğer açıklaması da önceki sayfalarda değinilen Avea İletişim Hizmetleri A.Ş. tarafından Bilgi Teknolojileri ve İletişim Kurumuna yazılan 25/10/2017 tarihli yazıda yer almaktadır.

Operatör açısından bu eşleşmenin nasıl yapıldığı Turkcell İletişim Hizmetleri A.Ş. tarafından Bilgi Teknolojileri ve İletişim Kurumuna yazılan 13/06/2017 tarihli yazısının ikinci sayfasında daha detaylı olarak açıklanmıştır.

Açıklamalar öncesinde iki farklı kaynaktan yani SGSN ve GGSN şebeke elemanlarından gelen CDR veriler ile A10 alt yapılarından gelen CGNAT kayıtları arasında her bir oturuma ilişkin açıklanan tüm koşulların sağlanmasının gerektiği vurgulanmıştır.

> Birbirinden bağımsız olarak çalışan iki kaynaktan gelen verilerin eşlemesi için CGNAT alt yapılarında oluşan her oturum kaydına ilişkin aşağıdaki **tüm koşulların tam olarak sağlanması** gerekmektedir;

Sağlanması gereken birinci koşulda SGSN ve GGSN CDR' larında yer alan Özel IP ve CGNAT kayıtlarında yer alan Özel IP bilgilerinin birbirinin aynısı olması gerektiği ifade edilmiştir.

Bunun anlamı CGNAT kayıtları ile HTS/GPRS kayıtları içerisinde yer alan Özel IP bilgisinin aynı olmasının zorunlu bir durum olduğudur.

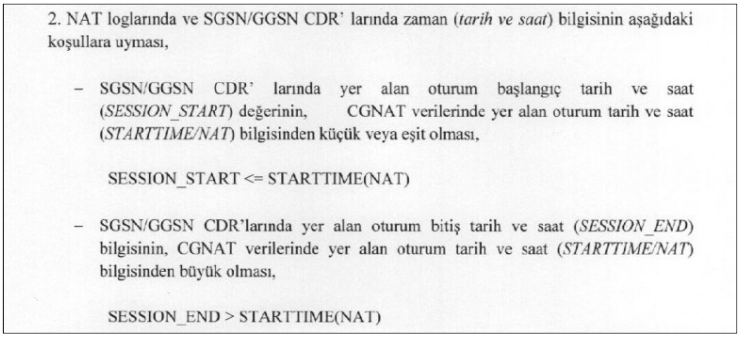
> 1. SGSN/GGSN CDR' larında yer alan Özel IP (*SERVEDPDPADDRESS*), CGNAT loglarında yer alan Özel IP (*PRIVATE_IP/NAT*) bilgisine eşit olması,
>
> SERVEDPDPADDRESS = PRIVATE_IP(NAT)

Sağlanması gereken ikinci koşulda ise SGSN ve GGSN CDR' larında yer alan oturum başlama tarih ve saati ile CGNAT kayıtlarında yer alan tarih saat bilgisi karşılaştırıldığında CGNAT kayıtlarında yer alan tarih saat bilgisinin daha büyük veya eşit olmaları gerektiği, aynı şekilde SGSN ve CGSN CDR' larında yer alan oturum bitiş tarih saati ile CGNAT kayıtlarında yer alan tarih saat bilgisi karşılaştırıldığında CGNAT kayıtlarında yer alan tarih saat bilgisinin daha küçük veya eşit olmaları gerektiği ifade edilmiştir.

Bunun anlamı ise HTS/GPRS kayıtlarında yer alan bir kayıtlar için herhangi bir CGNAT kaydının oturum başlangıç ve bitiş zamanları aralığında olması gerektiğidir.

HTS/GPRS kayıtları içerisinde oturum başlama ve oturum süresi bilgileri yer almakta oturum bitiş zamanlarının ise hesaplanması gerekmektedir.

Yalnızca buradaki basit nedenle dahi, oturum bitiş zamanları hesaplanmamış incelemelerde her ne kadar bu inceleme teknik olarak her zaman uyumlu olmak zorunda olsa da, eksik inceleme yapıldığından bahsedebilmek mümkündür.



2. NAT loglarında ve SGSN/GGSN CDR' larında zaman (*tarih ve saat*) bilgisinin aşağıdaki koşullara uyması,

- SGSN/GGSN CDR' larında yer alan oturum başlangıç tarih ve saat (*SESSION_START*) değerinin, CGNAT verilerinde yer alan oturum tarih ve saat (*STARTTIME/NAT*) bilgisinden küçük veya eşit olması,

  SESSION_START <= STARTTIME(NAT)

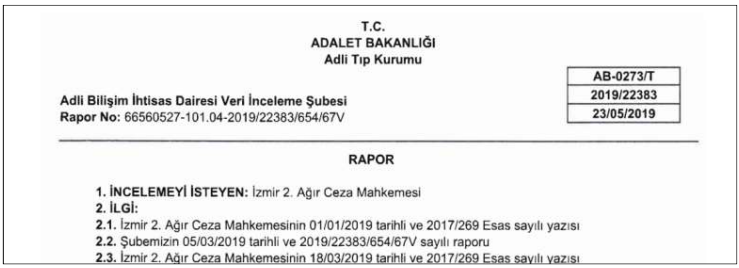
- SGSN/GGSN CDR'larında yer alan oturum bitiş tarih ve saat (*SESSION_END*) bilgisinin, CGNAT verilerinde yer alan oturum tarih ve saat (*STARTTIME/NAT*) bilgisinden büyük olması,

  SESSION_END > STARTTIME(NAT)

Buradan özetle, HTS/GPRS ve CGNAT kayıtlarının karşılaştırılması sonucunda herhangi bir uyumsuzluk tespitinin söz konusu olamayacağı, bu kıyaslamanın teknik bir zorunluluk olması nedeni ile yapılmasının dahi anlamsız olduğu açık bir şekilde anlaşılmaktadır.

5. Adli Tıp Kurumunun CGNAT ve HTS Kayıtlarının İncelenmesi Konusundaki Görüşü

Adli Tıp Kurumunun İzmir 2. Ağır Ceza Mahkemesinin talebi ile 23/05/2019 tarihli Raporunda CGNAT ve HTS Kayıtları arasındaki uyumluluğu incelemiş olduğu görülmüştür.



T.C.
ADALET BAKANLIĞI
Adli Tıp Kurumu

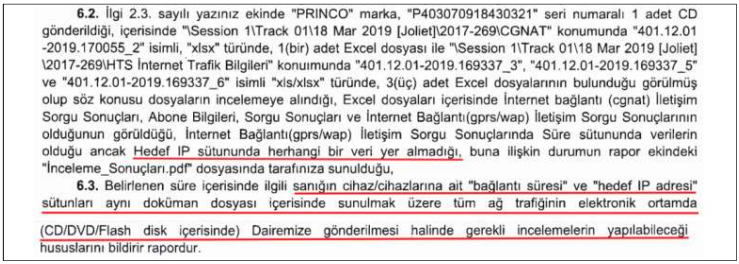
AB-0273/T
2019/22383
23/05/2019

Adli Bilişim İhtisas Dairesi Veri İnceleme Şubesi
Rapor No: 66560527-101.04-2019/22383/654/67V

RAPOR

1. İNCELEMEYİ İSTEYEN: İzmir 2. Ağır Ceza Mahkemesi
2. İLGİ:
2.1. İzmir 2. Ağır Ceza Mahkemesinin 01/01/2019 tarihli ve 2017/269 Esas sayılı yazısı
2.2. Şubemizin 05/03/2019 tarihli ve 2019/22383/654/67V sayılı raporu
2.3. İzmir 2. Ağır Ceza Mahkemesinin 18/03/2019 tarihli ve 2017/269 Esas sayılı yazısı

Adli Tıp Kurumunun Raporunun Bulgular ve Sonuç kısmında GPRS kayıtları içerisinde Hedef IP herhangi bir veri olmaması nedeni ile inceleme yapılamadığının ifade edildiği görülmüştür.



6.2. İlgi 2.3. sayılı yazınız ekinde "PRINCO" marka, "P403070918430321" seri numaralı 1 adet CD gönderildiği, içerisinde "\Session 1\Track 01\18 Mar 2019 [Joliet]\2017-269\CGNAT" konumunda "401.12.01-2019.170055_2" isimli, "xlsx" türünde, 1(bir) adet Excel dosyası ile "\Session 1\Track 01\18 Mar 2019 [Joliet]\2017-269\HTS İnternet Trafik Bilgileri" konumunda "401.12.01-2019.169337_3", "401.12.01-2019.169337_5" ve "401.12.01-2019.169337_6" isimli "xls/xlsx" türünde, 3(üç) adet Excel dosyalarının bulunduğu görülmüş olup söz konusu dosyaların incelemeye alındığı, Excel dosyaları içerisinde İnternet bağlantı (cgnat) İletişim Sorgu Sonuçları, Abone Bilgileri, Sorgu Sonuçları ve İnternet Bağlantı(gprs/wap) İletişim Sorgu Sonuçlarının olduğunun görüldüğü, İnternet Bağlantı(gprs/wap) İletişim Sorgu Sonuçlarında Süre sütununda verilerin olduğu ancak Hedef IP sütununda herhangi bir veri yer almadığı, buna ilişkin durumun rapor ekindeki "İnceleme_Sonuçları.pdf" dosyasında tarafınıza sunulduğu,

6.3. Belirlenen süre içerisinde ilgili sanığın cihaz/cihazlarına ait "bağlantı süresi" ve "hedef IP adresi" sütunları aynı doküman dosyası içerisinde sunulmak üzere tüm ağ trafiğinin elektronik ortamda (CD/DVD/Flash disk içerisinde) Dairemize gönderilmesi halinde gerekli incelemelerin yapılabileceği hususlarını bildirir rapordur.

Halbuki, HTS/GPRS Kayıtları içerisinde yer alan oturumların başlangıç zamanı ve süresi ile tanımlanması nedeni ile belirli bir zaman dilimini kapsadığı açıktır. Bu süre içerisinde ise kişinin, oturum süresine bağlı olarak yüz binlerce CGNAT

kaydı (yalnızca ByLock değil tüm iletişimlerine ait) olmasının mümkün olması ve bu yüzbinlerce CGNAT kaydının ise HTS/GPRS kayıtları içerisinde tek bir oturumda, yani tek bir satırda gösterilmesinin mümkün olmaması nedeni ile Adli Tıp Kurumunun bu gerekçesinin yersiz ve teknik uygulama ile de uyumsuz olduğu görülmüştür.

Tek bir GPRS oturumu yüzbinlerce hatta milyonlarca CGNAT kaydı ile ilişkili olabilmektedir. Burada CGNAT kayıtlarının yalnızca ByLock Uygulaması ile ilişkili olmadığı, bir kullanıcının Internet üzerindeki tüm iletişim etkinliklerinin CGNAT kaydı oluşturduğu unutulmamalıdır.

6. Sonuç

Bilindiği üzere, bir ceza yargılamasının temel amacı maddi hakikate ulaşmaktır. Maddi gerçekliğe ulaşması gereken yargıç, uyuşmazlık konusunda doğrudan bilgi sahibi olmayan kimsedir. Kısacası yargıç, yargılama konusu olayın tanığı ya da tarafı olmayan kimsedir. Bu yönüyle yargıç maddi gerçekliğe yalnızca deliller aracılığıyla ulaşabilecektir. Bu noktada maddi gerçekliğe ulaşabilmenin temel şartı delilleri doğru değerlendirmek ve anlamlandırmaktır. İşbu çalışmanın ortaya çıkmasına neden olan Yargıtay değerlendirmesinde detaylarıyla izah olunduğu üzere, yargılamada delil olarak kullanılan HTS-CGNAT ve GPRS verilerinin teknik gerçekliklerine uygun şekilde yorumlanmamaktadır. Bu yönüyle söz konusu değerlendirme ile maddi gerçeklikten uzaklaşıldığı, HTS-CGNAT ve GPRS verileri üzerinde yapılan değerlendirmenin bilimsel gerçeklikten uzak olduğu aşikardır.

Netice itibariyle CGNAT-HTS/İletişim Kayıtları, HTS/İletişim Kayıtları-HTS/GPRS Kayıtları ve CGNAT-HTS/GPRS Kayıtları arasındaki baz istasyonu bilgilerinin uyumluluğu ya da uyumsuzluğu tespitinden edinilebilecek, bilimsel ve dolayısıyla maddi gerçekliğe uygun tespitler şunlarla sınırlıdır:

1. CGNAT-HTS/İletişim Kayıtları uyumluluk da uyumsuzluk da olağan ve beklenen bir durumdur.

2. HTS/İletişim Kayıtları-HTS/GPRS Kayıtları uyumluluk da uyumsuzluk da olağan ve beklenen bir durumdur.

3. CGNAT-HTS/GPRS Kayıtları arasında uyumluluk olmak zorundadır. Bu uyumluluğun sebebi CGNAT kayıtlarının (yani bir IP adresine erişimin) var olabilmesi için HTS/GPRS

Kayıtlarının (Internet bağlantısının yapılmış olması) var olmasının gerekmesidir.

4. Bu zorunluluk tıpkı bir telefon görüşmesi yapılmak istenen kişinin önce aranmasının gerekmesi kadar temel bir zorunluluktur.

5. Ancak, bu kıyaslamaların hiç birisi, CGNAT kayıtlarının ne yolla ortaya çıktığını, (yani ByLock veya Mor Beyin uygulamalarının kullanılmış olması veya bilinmeyen başka sebepler) açıklayabilir nitelikte değildir. Bu nedenle kişinin ByLock uygulaması kullandığına dair tespit niteliği olan bir delil olabilmesi de mümkün değildir.

6. Yalnızca operatör tarafı verilerin incelenmesi ile kişilerin ByLock uygulamasını kullandıklarına dair kesin bir tespit teknik olarak mümkün değildir.

7. CGNAT Kayıtları ile HTS/GPRS kayıtları arasındaki uyumluluğun ByLock kullanımı için yeterli görülmesi CGNAT kayıtlarının varlığının yeterli görülmesi ile aynı anlama gelmektedir.

İlgili Diğer Hususlar Açısından;

1. CGNAT-HTS/İletişim Kayıtları, HTS/İletişim Kayıtları-HTS/GPRS Kayıtları ve CGNAT-HTS/GPRS Kayıtları arasındaki baz istasyonu bilgilerinin uyumluluğu ya da uyumsuzluğu tespitinden edinilebilecek tespitlerin herhangi bir kişinin ByLock Uygulamasını kullanıp kullanmadığı yönünde bir tespit niteliği olmadığı kesin olmakla birlikte atıf yapılan evrakların yazıldığı tarihler incelendiğinde;

- Avea İletişim Hizmetleri A.Ş. tarafından Bilgi Teknolojileri ve İletişim Kurumuna yazılan 05/06/2017 ve 25/10/2017 tarihli yazılar,
- Turkcell İletişim Hizmetleri A.Ş. tarafından Bilgi Teknolojileri ve İletişim Kurumuna yazılan 13/06/2017 tarihli yazı
- Vodafone Telekomünikasyon A.Ş. tarafından Bilgi Teknolojileri ve İletişim Kurumuna yazılan 29/09/2017 tarihli yazı,

mevcut olması nedeni ile konunun esasen 2017 yılının ikinci yarısında çözümlenmiş veya çözümlenebilir olduğu açık bir şekilde görülmektedir.

2. Bu konuda bir kısım Yargıtay kararlarında sanıklara ait CGNAT ve HTS kayıtlarının karşılaştırılmamış olmasının bozma nedeni olarak değerlendirildiği görülse de bu nedenin kişinin ByLock kullanıcısı olup olmaması yönünde tespit niteliği olmayan bir karşılaştırmaya bağlanması teknik olarak anlamsız olduğu görülmektedir.

3. Alt mahkemelerde sanıkların CGNAT-HTS kayıtları arasında uyumluluğa bağlı verilen cezalarda teknik olarak tespit niteliği olmaması nedeni ile aslen delil olamayacak bir durumun delil niteliğinde değerlendirildiği görülmektedir.

4. Adli Tıp Kurumunun HTS/GPRS Kayıtları içerisinde Hedef IP bilgisinin var olmaması nedeni ile inceleme yapılamamış olmasının teknik uygulama ile uyumsuz olduğu, CGNAT sistemi içerisinde GPRS kayıtları içerisinde Hedef IP sütununun boş olmasının zaten olması gereken durum olması nedeni ile Adli Tıp Kurumunun bu konuda yetersiz olduğunun değerlendirilebilir olduğu görülmektedir.

5. Bir kısım Bilirkişi Raporlarında CGNAT-HTS/GPRS kayıtlarının uyumlu olması nedeni ile sanığın ByLock kullanıcısı olduğuna dair tespitte bulunulduğunun ifade edilmesi bundan daha kötüsü kişinin CGNAT-HTS İletişim Kayıtlarının karşılaştırılarak büyük oranda uyumlu oldukları görülmüştür gibi aslen kıyaslanması mümkün olmayan verilerin kıyaslanmasına bağlı ifadelerin kullanılmasının sanıklar aleyhine yetersiz değerlendirmeler olduğu, incelemeyi yapanların uzmanlıklarının ve iyi niyetlerinin sorgulanması gerektiği görülmektedir.

6. Bir kısım Özel Bilirkişi Raporlarında, CGNAT kayıtlar ile HTS/GPRS kayıtlarının zamansal olarak karşılaştırılırken yalnızca CGNAT kayıt zamanı ile HTS/GPRS oturum başlangıç zamanının kullanılarak zaman bilgilerinin farklı olması nedeni ile uyumsuzluk olduğu yönündeki inceleme ve değerlendirmelerin, teknik olarak uyumlu olan kayıtların uyumsuz olarak tespit edilmiş olmasının özel incelemeyi yapan kişilerin uzmanlıklarının veya sorgulanması gerektiği görülmektedir.

Netice itibariyle, CGNAT baz istasyonu bilgisi ile HTS/GPRS kayıtlarının karşılaştırılması sonucu, ByLock kullanıcısı olan bir kişi ile CGNAT kayıtları ByLock Uygulaması kullanımı sonucu dışında ortaya çıkan bir kişinin birbirinden ayrıştırılabilmesi imkansızdır. Bu nedenle bu kıyaslama, kullanıcı tespiti açısından teknik ve hukuki bir niteliğe sahip değildir.

7. Özgeçmiş

Gizay Dulkadir

Avukat, Ankara Barosu, Ceza Hukuku, İnsan Hakları Hukuku, İdare Hukuku ve adli bilişim alanlarında çalışmaktadır.

Dr.Berker KILIÇ

Adli Bilişim Uzmanı, Adli Bilişim ve Veri Bilimi alanlarında yüksek lisans, Adli Bilişim Mühendisliği alanında doktora yapmış resmi ve taraf bilirkişiliği yapmaktadır.