

UZMAN GÖRÜŞÜ

GSM OPERATÖR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDİALARI ÜZERİNE DEĞERLENDİRMELER

İşbu uzman görüşü, 5271 sayılı Ceza Muhakemeleri Kanununun 67. Maddesi 6. Fıkrası uyarınca, tarafımıza ulaştırılan ve devam eden soruşturmalarda/kovuşturmalarda şüpheli/sanık (Danışan) olan çok sayıda kişi ya da vekillerince yöneltilen soruların teknik ve hukuki açıdan incelenmesi ve değerlendirilmesi suretiyle hazırlanmıştır.

“GSM operatörlerince tutulan kayıtlar kullanılarak ByLock uygulaması kullanımının tespit edildiği” iddiaları içerikli soruşturma/kovuşturma dosyalarında değerlendirilmek üzere tarafımıza iletilen sorular, değerlendirilmesi talep edilen hususlar:

i. Yargıtay 16. Ceza Dairesinin ByLock isnatlı kovuşturma dosyalarına yönelik bozma kararlarında ***“ByLock kullanıcısı olduğunu kabul etmeyen sanığın, ByLock uygulamasını kullandığının kuşkuya yer vermeyecek şekilde teknik verilerle tespiti halinde, ByLock kullanıcısı olduğuna dair delilin atılı suçun sübutu açısından belirleyici nitelikte olması karşısında, ilgili birimlerden ayrıntılı ByLock tespit ve değerlendirme tutanağının getirtilip, ByLock tespit değerlendirme tutanağının temin edilememesi halinde gerekirse teknik olarak programı kullandığının tespiti açısından HIS (CGNAT) kayıtları ve HTS üzerinden uzman bilirkişi incelemesi yaptırılıp rapor alınması”*** şeklinde veya benzeri ifadelerin yer aldığı ancak incelemenin nasıl yapılacağına detayının belli olmadığı, dolayısıyla bu incelemenin nasıl yapılacağına değerlendirilmesi,

ii. HIS (CGNAT) kayıtlarının internet trafik kaydı niteliğinin değerlendirilmesi ile kayıtlarda yer alan hangi verilerin CGNAT sisteminden, hangi verilerin diğer (HTS-İletişim, HTS-GPRS vb.) kayıt sistemlerinden temin edildiğinin açıklanması,

iii. Bozma kararları sonrasında ilk derece mahkemelerince alınan bilirkişi raporlarında ve raporların değerlendirilmesinde farklılıklar olduğu, dolayısıyla GSM operatör kayıtlarının incelenmesi ve farklı kayıtların (CGNAT, HTS-İletişim veya HTS-GPRS) birbirleriyle kıyaslanması yoluyla ByLock uygulamasının kullanımının kuşkuya yer vermeyecek şekilde tespitinin mümkün olup olmadığının teknik olarak değerlendirilmesi,

iv. Soruşturma/kovuşturma dosyalarına dahil edilen BTK kaynaklı sayısal verilerin teknik olarak herhangi bir şüpheye yer vermeyecek bilgi niteliklerinin olup olmadığı,

v. GSM operatörlerinin konum/baz verilerini nasıl kayıt aldığının, baz verilerinin teknik olarak herhangi bir şüpheye yer vermeyecek şekilde kesin bilgi niteliklerinin olup olmadığının, CGNAT kayıtları ile HTS-İletişim veya HTS/GRPS kayıtları baz verileri kıyaslanarak ByLock uygulamasının kullanımının kuşkuya yer vermeyecek şekilde tespitinin mümkün olup olmadığının değerlendirilmesi,

vi. GSM operatör kayıtlarının adli bilişim uzmanlığı kapsamında incelenmesi yoluyla ByLock uygulamasının kullanımının teknik olarak herhangi bir şüpheye yer vermeyecek şekilde tespit edilebildiği bir örneğin bulunup bulunmadığı,

vii. ByLock uygulaması kullanımının teknik olarak herhangi bir şüpheye yer vermeyecek şekilde tespiti için gerekenlerin değerlendirilmesinden ibarettir.

Uzman görüşü kapsamında sorular/talepler teknik ve hukuki çerçevede cevaplanmış/değerlendirilmiştir.

Bu rapor her ne kadar uzman görüşü sunan bir çalışma olsa da, yapılan inceleme bir bilirkişi raporuna denk olacak şekilde tarafsızlıkla yapılmıştır ve verilen teknik bilgiler somut gerçekleri yansıtacak şekilde sunulmuştur.

Tarafımızca hazırlanan işbu uzman görüşü, soruşturma/kovuşturmalarda şüpheli/sanık olanlar veya vekilleri tarafından sunulması halinde Sayın Mahkemelerin/Dairelerin takdirlerine arz olunur.

Saygılarımızla.

02 Haziran 2021

Berker KILIÇ

Adli Bilişim Uzmanı
Veri Bilimci

T. Koray PEKSAYAR

Adli Bilişim Uzmanı
Bilgi Teknolojileri Y. Lisans

Dr. Levent MAZILIGÜNEY¹

Adli Bilişim Uzmanı
Y. Mühendis

¹ Dr. Levent MAZILIGÜNEY avukatlık mesleğinin yanı sıra yüksek mühendis ve adli bilişim uzmanıdır. İşbu uzman görüşünü adli bilişim uzmanlığı kapsamında diğer uzmanlarla birlikte hazırlamış ve imzalamıştır. GSM OPERATÖR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDİALARI ÜZERİNE DEĞERLENDİRMELER

Teknik Değerlendirme

A.1. Yargıtay 16. Ceza Dairesinin ByLock isnatlı kovuşturma dosyalarına yönelik bozma kararlarında “ByLock kullanıcısı olduğunu kabul etmeyen sanığın, ByLock uygulamasını kullandığının kuşkuyla yer vermeyecek şekilde teknik verilerle tespiti halinde, ByLock kullanıcısı olduğuna dair delilin atılı suçun sübutu açısından belirleyici nitelikte olması karşısında, ilgili birimlerden ayrıntılı ByLock tespit ve değerlendirme tutanağının getirtilip, ByLock tespit değerlendirme tutanağının temin edilememesi halinde gerekirse teknik olarak programı kullandığının tespiti açısından HIS (CGNAT) kayıtları ve HTS üzerinden uzman bilirkişi incelemesi yaptırılıp rapor alınması” şeklinde veya benzeri ifadelerin yer aldığı ancak incelemenin nasıl yapılacağının detayının belli olmadığı, dolayısıyla bu incelemenin nasıl yapılacağının değerlendirilmesi.

1. HTS (Historical Traffic Search) ses veya veri CDR²lerinin kaydı olarak tanımlanabilecek bir çatı kavramdır. Ancak HTS kavramı genellikle abonelerin telefonlarıyla gerçekleştirdikleri görüşmelerin arayan, aranan, arama zamanı, arama süresi ve **sinyal alınan baz istasyonları** gibi verilerini kapsayan kayıtlar anlamında kullanılmaktadır. Bu tür HTS'ler (ses/mesaj iletimi trafiği) bu rapor kapsamında **HTS-İletişim** olarak adlandırılmıştır.

2. İnternet üzerinde veri iletimi trafiği olarak adlandırılacak diğer bir HTS türü ise Kaynak IP, Hedef IP, Erişilen Sayfa, Gönderilen ve İndirilen Veri Miktarları, Bağlantı Süresi gibi verileri kayıt altına alan GPRS (General Packet Radio Service) kayıtlarıdır ve bu rapor kapsamında **HTS-GPRS** olarak adlandırılmıştır.

3. HIS (Historical Internet Search) (CGNAT – Carrier Grade Network Address Translation) kayıtları Genel IP adres sayısının yetersiz olması nedeniyle aynı Genel IP adresinin farklı Özel IP'ler ile birden çok kullanıcıya paylaştırılması işleminde Genel ve Özel IP, Genel ve Özel Port, Hedef IP, Hedef Port gibi verilerin kayıdır.

4. Yargıtay 16. Ceza Dairesinin “**teknik olarak programı kullandığının tespiti açısından HIS (CGNAT) kayıtları ve HTS üzerinden uzman bilirkişi incelemesi yaptırılıp rapor alınması**” şeklinde belirtilen karar ifadeleriyle nasıl bir inceleme talep ettiği tarafımızdan bilinmemektedir.

5. HIS (CGNAT) kayıtları ile HTS-İletişim kayıtlarının kıyaslanabileceği ortak veri yakın zamanlı kayıt bulunması durumunda hizmet alınan baz istasyonu konum verisidir. Ancak HIS (CGNAT) ve HTS-İletişim kayıtlarındaki baz istasyonu konum verilerinin kıyaslanması ile ByLock veya başka bir uygulamanın kullanımının teknik olarak herhangi bir şüpheye yer vermeyecek şekilde tespiti mümkün değildir. Konunun detayları diğer soruların cevapları kapsamında açıklanmıştır.

6. HIS (CGNAT) kayıtları ile HTS-GPRS kayıtlarının kıyaslanabileceği ortak veriler HIS (CGNAT) kaydındaki Özel IP ile HTS-GPRS kaydındaki Kaynak IP, her iki kayıttaki Hedef IP,

² Doğru açılımı “Call Detail Record”dur ancak zaman zaman Charging Data Record veya Customer Data Record olarak da kullanıldığı görülmüştür.
GSM OPERATÖR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDİALARI ÜZERİNE DEĞERLENDİRMELER

baz istasyonu konum verisi ve bazı yaklaşımlarla ve kesinlik içermeyecek şekilde süre verileridir. Ancak HIS (CGNAT) ve HTS-GPRS kayıtlarındaki verilerin kıyaslanması ile ByLock veya başka bir uygulamanın kullanımının teknik olarak herhangi bir şüpheye yer vermeyecek şekilde tespiti mümkün değildir. Konunun detayları diğer soruların cevapları kapsamında açıklanmıştır.

7. Yargıtay 16. Ceza Dairesince uzman görüşünde değerlendirilen hususlar haricinde bir inceleme talebinin açıklanması halinde belirtilecek husus ayrıca değerlendirilebilecektir.

A.2. HIS (CGNAT) kayıtlarının internet trafik kaydı niteliğinin değerlendirilmesi ile kayıtlarda yer alan hangi verilerin CGNAT sisteminden, hangi verilerin diğer (HTS-İletişim, HTS-GPRS vb.) kayıt sistemlerinden temin edildiğinin açıklanması.

8. Av. Gizay DULKADİR, Av. Ali AKTAŞ, Adli Bilişim Uzmanı T. Koray PEKSAYAR ile Yüksek Mühendis, Hukukçu ve İktisatçı Levent MAZILIGÜNEY tarafından **“ByLock Kullanıcı Tespitleri ve Yargılamalara Etkisi Üzerine Değerlendirmeler”** isimli ve uzman görüşü niteliğinde kapsamlı bir rapor 30 Mart 2018 tarihinde internet ortamında yayınlanmıştır³. Söz konusu rapor kapsamında genel hususlara yönelik detaylı teknik ve hukuki açıklamalar yer aldığından işbu uzman görüşüne EK-1 olarak sunulmaktadır.

9. EK-1 raporun 3. Bölümünde “CGNAT Sistemi ve Gerçek Kullanıcılara Ulaşmada Karşılaşılan Problemler” başlığı altında CGNAT kayıtları kullanılarak teknik olarak herhangi bir şüpheye yer vermeyecek şekilde gerçek kullanıcılara ulaşmanın mümkün olmadığı açıklanmıştır. EK-1 raporun 4. Bölümünde “Geniş Ölçekli Ağ Dönüştürme (CGNAT) Tekniği ve 5651 Sayılı Kanun” başlığı altında HIS (CGNAT) kayıtlarının 5651 sayılı kanunda tarif edilen anlamlı bir internet trafiği tanımı da dikkate alındığında tek başına ByLock kullanım delili olamayacağı açıklanmıştır. Bu uzman görüşü kapsamında ilave bazı hususlara değinilecek ve EK-1 raporda yer alan önemli hususlar tekrar edilecektir.

10. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun”un (İnternet Kanunu) 2. Maddesi j bendinde internet trafiği,

“j) Trafik bilgisi: İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerleri,” şeklinde tanımlanmıştır.

Anlamlı bir internet trafik kaydında, kanunda belirtilen ve aranan bilgilerin yer alması gerektiği anlaşılmaktadır. Kanunda yer alan tanımdan anlamlı bir internet trafiğinin aşağıdaki sorulara cevap vermesi gerektiği değerlendirilmektedir.

- i. Karşılıklı iletişim talebi yapılan IP bilgileri nelerdir?
- ii. Bağlantı noktaları (Mobil cihaz, sunucu, vb.) nedir?
- iii. IP bilgilerini kullanan taraflar (Erişilen Sayfa) kimlerdir?
- iv. Bağlantı süresi ne kadardır?

³ <https://koray.peksayar.org/bylock-kullanici-tespitleri-ve-yargilamalara-etkisi-uzerine-degerlendirmeler/>
GSM OPERATÖR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDİALARI ÜZERİNE DEĞERLENDİRMELER

v. Bağlantıda ne kadar veri aktarımı gerçekleşmiştir?

11. **HIS (CGNAT) kayıtları tek başına anlamlı bir internet trafik kaydı oluşturamaz.**
12. EK-1 olarak sunulan raporda detaylı bir şekilde açıklandığı şekilde, operatör kayıtları verinin kendisi değil, üst veridir (özet veri veya metadata). Raporda belirtildiği şekliyle;

“Bu konu farklı açılardan tartışılabilir olmakla birlikte, önemli olan CGNAT kayıtlarının üst verilerde olduğu gibi özet veri olması dolayısıyla neticede bir iz veya belirti olduğudur. Ayrıca müdahaleye açık olup olmadığı ve orijinalliğinin ve veri bütünlüğünün nasıl kontrol edilebileceği konusu da problemlidir, tartışılmalıdır. Nihayetinde özet veri olan kayıtlar doğru tutulmuş olsa dahi, operatör, TİB/BTK veya erişebilecek/müdahale edebilecek başka kurum ve kuruluşlarda görevli art niyetli kişilerin bulunması veya kurumlar dışından bu alanlarda uzman olan başkaca art niyetli kişilerce kayıtlara müdahale edilip edilmediği, edildiyse bunun kontrolünün nasıl sağlanabileceği konusu tartışılmalı ve şüpheyi yer vermeyecek şekilde netleştirilmelidir.

CGNAT başta olmak üzere operatör kayıtları, herhangi bir şekilde ilgili uygulama ile gerçekleştirilen iletişime ait içerik bilgisine işaret etmez. Bu nedenle nihayetinde bir iz veya belirti olarak kabul edilebilir. İliyet bağı açısından da kesinliği bulunmamaktadır. Teknik olarak müdahaleye açık olan ve veri bütünlüğü ve doğruluğu açısından hatalı olduğu örnekleri ile bilinen operatör kayıtlarının delil niteliğinin bu açıdan da tartışılması gereklidir.”

13. Dolayısıyla, operatör kayıtlarının bu açıdan değerlendirilmesi gereklidir. Kayıtların doğruluğu veya öncesinde veya çözümleme aşamasında müdahale olup olmadığı hususları ilgili operatör ve yetkili kurumca netleştirilmelidir

14. EK-1 olarak sunulan raporda CGNAT kayıtlarının güvenilirliği ve herhangi bir uygulamaya yönelik kullanım gösterip göstermeyeceği hususu detaylı bir şekilde açıklanmıştır. Raporda, **Avea firmasına CGNAT sistemini satan Amerikan F5 firması, CGNAT ile gerçek kullanıcıya ulaşmanın imkânsız yakın olduğunu kurumsal internet sitesinde belirtmektedir. Avrupa Polis Teşkilatı (Europol), Avrupa genelinde İSS'lerin %90 oranında CGNAT kullandığını ve CGNAT kayıtları üzerinden suçluya ulaşmak istediklerinde %80 oranında problemle karşılaştıklarını, suçsuz kişilerin suçlanabildiğini belirtmekte ve tarafları internet üzerinde hesap verebilirliği artırmak için CGNAT sisteminden vazgeçmeye davet etmektedir. Telekomünikasyon ve internet alanında uzman İngiliz Ofcom/Inter-Connect firmaları CGNAT üzerinden kullanıcıya ulaşmanın neden imkânsız yakın olduğunu geniş bir raporla bilimsel olarak ve örnekler üzerinden açıklamıştır.**

15. **CGNAT verileri bağlantı değil, bağlantı talebi bilgileridir. Bağlantının gerçekleşip gerçekleşmediğinin tam olarak tespiti CGNAT kayıtları üzerinden yüzde yüz kesinlikle tespit edilememekle birlikte, bağlantı olamayacak kayıtların tespiti ise mümkündür.**

16. GSM operatörün tuttuğu kayıtlara göre belirtilen zaman diliminde GSM hattınca kullanılan Genel IP adresinden, ByLock sunucusunca kullanılan Genel IP adresine bağlantı talebi oluşmasının muhtemel nedeni yalnızca telefonda yüklü ByLock uygulamasının bağlantı talebinde bulunması olmayabilir. Diğer muhtemel nedenler (başka nedenler de olabilir) şunlardır:

ii. Başka uygulamalar ve/veya internet sitesi ve/veya reklamlar ByLock sunusuna irade dışında yönlendirme yapabilir. Bunun örneği Morbeyin genel isimlendirmesiyle bilinen uygulamalardır.

iii. ByLock sunucunun kullandığı Genel IP adresleri başka uygulamalar ve/veya internet sitelerince de kullanılıyor olabilir.

iv. Bağlantı talebi oluşmadığı halde operatörlerin kayıt hatası olabilir.

v. GSM operatörü aynı Genel IP adresi ile birden çok kullanıcıya (aboneye) internet bağlantı hizmeti sunarken, kullanıcı trafiklerini ayırıştırma konusunda hataya düşmüş olabilir.

17. Kamuoyuna yansıyan Morbeyin tuzak uygulamaları bilinmektedir. Tarkan'dan "kuzu kuzu" şarkısını dinlemek isteyen bir kişinin tuzak uygulamalar nedeniyle nasıl ByLock sunucusuna bağlandığı ve bu tespit sonrasında gelişen olaylarla söz konusu tuzak uygulamaların devletin ilgili ve yetkili birimlerince de tespit edildiği ve 11.480 kişinin ByLock sunucusuna iradeleri dışında yönlendirildiği anlaşıldığından kullanıcı listelerinden çıkarıldığı Ankara Cumhuriyet Başsavcılığınca 27 Aralık 2017 tarihinde açıklanmıştır. Morbeyin uygulamalarına benzer şekilde, Namaz Vakitleri ve Kible Pusulası uygulamalarının da ByLock sunucusuna kullanıcısının isteği dışında bağlantı oluşturduğuna yönelik bilgiler kamuoyu ile paylaşılmıştır. **Morbeyin uygulamaları nedeniyle mağdur olduğu Devletin yetkili birimlerince ilan edilmiş 11.480 kişinin tamamının CGNAT kayıtlarının bulunduğu hususu CGNAT kayıtlarının güvenilir olmadığı konusunda önemli bir veridir.**

18. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2. Maddesinde yapılan tanımlar ve erişim sağlayıcının saklamakla yükümlü olduğu bilgi "İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerleri," olarak tanımlanmakta, trafik bilgisinin ayrıntılarının saklanması gerektiği açıkça belirtilmektedir/emredilmektedir. Uygulamaya ait işlemlere işaret eden adreslerin ve oluşan trafik hacminin (yani transfer edilen verinin miktarının) noksanlığı durumunda, bu noksan bilgiye sahip dökümün doğruluğu ve tamlığından, dolayısıyla anlamlı bir internet trafik bilgisinden bahsedilemeyeceği değerlendirilmektedir.

19. MİT'ten Ankara Cumhuriyet Başsavcılığı'na gönderilen 09/12/2016 tarihli, 10.2.001.01.000.390.1960.249-2236/691-92452/57 sayılı "Müsteşar a. Hukuk Müşaviri" sıfatıyla imzalanmış yazı ekinde gönderilen açıklama, kullanıcı listelerinin genellikle operatör verileri esas alınarak hazırlandığını doğrulamaktadır. Açıklama sayfasının ilgili bölümü aşağıda sunulmuştur.

Gerçekleştirilen tüm çalışmalar, eldeki veri, bilimsel ve istihbari analiz metotları ile işletmecî kaynaklı veriler kullanılarak gerçekleştirilmiştir. Elektronik haberleşme sektöründe hizmet veren operatörlerin, öncelikle tabi oldukları Bilgi Teknolojileri ve İletişim Kurumu mevzuatı kapsamında vermeleri gereken bilgi ve belgeyi “doğru” ve “noksansız” şekilde vermeleri gerekmektedir. Operatör verileri esas alınarak ve bir takım veri doğrulama/tutarlılık yöntemleri imkanlar nispetinde kullanılarak, bu aşamada, söz konusu uygulamanın kullanıldığı değerlendirilen abonelik bilgilerine ulaşılmıştır. Söz konusu uygulamaya, farklı en az üç günde erişen abonelikler listeye dahil edilmiştir. Bu kapsamda 102.192 farklı kimlik numarasına (ki bazı kimlik numaralarının yanlış ve sahte olduğu görülmektedir.) ait 123.115 GSM aboneliği ve 6748 ADSL aboneliği listesi Ek-1’de sunulmuştur. GSM aboneliklerine ait kayıt bilgilerinde yer alan kimlik bilgileri ile söz konusu GSM numarasının gerçek kullanıcısının bazı durumlarda farklılık arz edebileceğinin, ADSL aboneliklerinde ise aynı abonelik üzerinden birden fazla kişi tarafından bağlantı sağlanmış olabileceğinin göz önüne alınmasına ihtiyaç bulunmaktadır.

Resim 1: MİT Raporu Açıklama Sayfası İlgili Bölümü

Ekran resmi sunulan metinde kullanıcı listelerinin **operatör verilerinin tam ve eksiksiz olduğu ön kabulü** ile hazırlandığı açıkça belirtilmektedir ancak HIS (CGNAT) kayıtlarının açıklanan özellikleri nedeniyle operatörlerin teknik olarak herhangi bir şüpheye yer vermeyecek şekilde kullanıcıyı tespit etmeye imkân sağlayan kayıt tutamayacakları değerlendirilmektedir.

20. HIS (CGNAT) sistemi bir telefon santraline benzetilebilir. Telefon santrali tek bir harici telefon hattını çok sayıda dahili hat tarafından kullanılabilir hale getirebilir. HIS (CGNAT) sistemi de tek bir Genel IP adresini Özel IP’ler vasıtasıyla çok sayıda kullanıcıya paylaştırabilir. Bu paylaşımı EK-1 raporda ve rapor kaynaklarında/atıflarında açıklandığı şekilde gerçekleştirirler.

21. HIS (CGNAT) sistemi işleyişi nedeniyle GSM numarası, Genel IP, Özel IP, Genel Port, Özel Port, Hedef IP, Hedef Port ve Oturum Başlama Tarihi (GSM kullanıcısından karşı sunucuya bağlantı talebinin gönderildiği tarih ve saat verisi) verilerini tutabileceği değerlendirilmektedir. HIS (CGNAT) kayıtları kapsamında yer alan IMSI, IMEI ve BAZ verilerinin HIS (CGNAT) sistemi kapsamında kaydedilmediği, GSM operatörlerinin HTS-İletişim veya HTS-GPRS sistemlerinden veya veri bankalarından temin edildiği değerlendirilmektedir. İlerleyen bölümlerde açıklanacağı şekilde BAZ verisinin HTS-GPRS sistemi verilerinden alındığı değerlendirilmektedir.

22. HIS (CGNAT) satırlarının her biri bağlantı değil bağlantı talebi verileridir. Çok sayıda satırın peş peşe yer almasının nedeni HIS (CGNAT) kayıt sistematüğinden kaynaklanmaktadır. **Bağlantının gerçekleşip gerçekleşmediğinin tam olarak tespiti CGNAT kayıtları**

GSM OPERATÖR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDİALARI ÜZERİNE DEĞERLENDİRMELER

üzerinden yüzde yüz kesinlikle tespit edilememekle birlikte, kesinlikle bağlantı olamayacak kayıtların tespiti ise mümkündür.

A.3. Bozma kararları sonrasında ilk derece mahkemelerince alınan bilirkişi raporlarında ve raporların değerlendirilmesinde farklılıklar olduğu, dolayısıyla GSM operatör kayıtlarının incelenmesi ve farklı kayıtların (CGNAT, HTS-İletişim veya HTS-GPRS) birbirleriyle kıyaslanması yoluyla ByLock uygulamasının kullanımının kuşkuyla yer vermeyecek şekilde tespitinin mümkün olup olmadığının teknik olarak değerlendirilmesi.

23. HIS (CGNAT) ve HTS-GPRS kayıtlarının kıyaslanarak ByLock uygulamasının kullanımına yönelik değerlendirmelerin yer aldığı bilirkişi raporlarına sıklıkla rastlanmaktadır. Bunlardan ilki baz/konum verilerinin kıyaslanması şeklindedir. HIS (CGNAT) ve HTS-İletişim veya HTS-GPRS kayıtlarının konum/baz verilerinin kıyaslanmasına yönelik değerlendirmeler bir sonraki soru cevapları kapsamında yer almaktadır. Diğer sık karşılaşılan kıyaslama ise HIS (CGNAT) satır kaydının olduğu zaman diliminde HTS-GPRS kaydının bulunup bulunmadığının incelenmesi şeklindedir. Bilirkişi raporlarında sıklıkla karşılaşılan kıyaslamalar ile ByLock veya başka bir uygulamanın kullanımına yönelik, teknik olarak herhangi bir şüpheye yer vermeyecek şekilde tespit yapılamayacağına yönelik değerlendirmelerimizin gerekçeleri ilerleyen paragraflarda açıklanmıştır.

24. HIS (CGNAT) kayıtları ile HTS-GPRS kayıtlarının kıyaslanabileceği ortak veriler HIS (CGNAT) kaydındaki Özel IP ile HTS-GPRS kaydındaki Kaynak IP, her iki kayıttaki Hedef IP, baz istasyonu konum verisi ve bazı yaklaşımlarla ve kesinlik içermeyecek şekilde süre verisidir. Ancak bu kıyaslamalar HTS-GPRS kayıtlarının oluşturulma sistematığı ve HTS-GPRS kayıtlarındaki gecikme nedeniyle bir anlam içermemektedir.

25. 5651 sayılı kanunda tanımlanan internet trafik bilgilerinin tamamı HIS (CGNAT) kayıtları ile GPRS/WAP kayıtları birlikte değerlendirilerek incelenebilir görüşü tartışma konusudur. Çünkü Hedef IP ve HIS (CGNAT) kayıtlarında eksik olan Erişilen Sayfa, bağlantı süresi, gönderilen ve indirilen veri boyutu gibi veriler HTS-GPRS sistemi ile kayıt altına alınmaktadır. Ancak bugüne kadar tarafımızdan **incelenen HTS-GPRS kayıtlarının tüm satırlarında Hedef IP ve Erişilen Sayfa bilgilerinin boş olduğu görülmektedir. Bu bilgiler eksik olduğunda internet trafiği bilgisinin tamlığından bahsetmek veya HIS (CGNAT) veya HTS-GPRS kayıtlarını tam olarak kıyaslayabilmek mümkün olmamaktadır.**

26. HTS-GPRS kayıtları sağlıklı tutulduğunda, kişilerin internete bağlantı tarih ve saatlerini, bağlandıkları hedefi (erişilen sayfayı) ne kadar süre bağlandıklarını ne boyutta veri alışverişi yaptıklarını gösterirler. İnternete bağlanan her kullanıcı bir şekilde veri alışverişi yapar ve her bağlantıda bu kayıt oluşur. Ancak operatörler arasında GPRS/WAP kaydının tutulması yönteminde farklılıklar ve belirsizlikler olduğu bilinmektedir. **Uzman görüşü kapsamında HIS (CGNAT) ve HTS-GPRS kayıtlarının bir arada değerlendirilmesi halinde anlamlı bir internet trafik kaydına ulaşılabilirliği incelenmiştir.**

27. 5651 sayılı kanun kapsamında aranan tüm kıstasları karşılayabilecek HTS-GPRS kaydı ancak her bir müstakil (her bir site veya uygulama) bağlantı için ayrı kayıt satırı oluşturulması ile mümkündür. Ancak incelenen HTS-GPRS kayıtlarında her bir müstakil

bağlantı için ayrı kayıt satırı bulunmadığı, internet servis sağlayıcıların (GSM operatörlerinin) daha çok faturalandırma amaçlı kayıt tuttıkları gözlenmiştir.

28. HTS-GPRS kayıtları 5651 sayılı kanun çerçevesinde tutulmakla birlikte Hedef IP ve Erişilen Sayfa bilgilerinin eksik olması nedeniyle anlamlı bir internet trafik kaydından bahsedilememektedir. Anılan eksikler nedeniyle HTS-GPRS kayıtları HIS (CGNAT) kayıtları ile eşleştirilememektedir. **Soruşturma/kovuşturma dosyalarına eklenen BTK kaynaklı HTS-GPRS kayıtlarının tüm satırlarında Hedef IP ve Erişilen Sayfa bilgilerinin boş olduğu görülmektedir. Bu bilgiler eksik olduğunda internet trafiği bilgisinin tamlığından bahsetmek veya HIS (CGNAT) veya HTS-GPRS kayıtlarını tam olarak kıyaslayabilmek mümkün olmamaktadır.**

29. HIS (CGNAT) kaydı müstakil oluşan bir kayıt değildir. HIS (CGNAT) kaydı oluşabilmesi için teknik olarak HTS-GPRS kaydı da oluşmalıdır. HTS-GPRS kaydı olmaksızın CGNAT kaydının var olması teknik olarak mümkün değildir. HIS (CGNAT) satırı olan zaman diliminde HTS-GPRS kaydının da bulunması teknik bir zorunluluk olmakla birlikte, bu zorunluluğun bulunup bulunmadığının iki kayıt kıyaslanarak kontrol edilmesi ByLock veya başka bir uygulamaya bağlantı konusunda bir veri oluşturmamaktadır.

30. Mobil cihaz ve mobil internet açık ancak kullanıcı tarafından aktif olarak herhangi bir internet işlemi gerçekleştirilmezken, sosyal medya ve iletişim için olanlar başta olmak üzere, izin verilen birçok uygulama arka planda internet üzerinde veri alışverişi yaparlar ve HTS-GPRS kaydı oluşmasına neden olurlar. Dolayısıyla hayatın olağan akışında, mobil cihaz ile WiFi bağlantısı yapılmamış ve mobil internetin kullanıldığı tüm zaman dilimlerinde, aktif internet işlemi yapılmamış olsa da HTS-GPRS kayıtlarının oluştuğu gözlenmektedir. Mobil cihazlarda genellikle aynı anda birden fazla iletişim uygulaması, sosyal medya platformu vb. bağlantısı arka planda çalışabildiğinden, Hedef IP ve Erişilen Sayfa verileri olmadan HIS (CGNAT) ve HTS-GPRS kayıtlarının kıyaslanması anlamlı olmamaktadır.

31. Operatörler, her bir ayrı bağlantı için ayrı HTS-GPRS kayıt satırı tutmak yerine cep telefonu kullanıcısı ilk internet bağlantısını gerçekleştirdiğinde GRPS çizelgesini zaman belirterek kayıt altına almaya başlamakta ve internet bağlantısı kesilinceye kadar kaç farklı uygulamaya bağlanılırsa bağlanılsın aynı kaydı genellikle devam ettirmektedir. Başlatılan kayıt ancak bağlantının kesintiye uğraması veya operatör tarafından belirlenen kayıt yenileme süresi dolunca yenilenmektedir. Operatörler kayıt yenileme sürelerini yaygın olarak 3600 sn., 5400 sn., 7200 sn. olarak belirleyebilmektedir. Ancak, böyle bir durumda anlamlı bir internet trafiği kaydından söz etmek mümkün olmamaktadır. Anılan türdeki kayıtlar operatörlerin faturalandırma/muhasebe amaçlı tuttıkları kayıtlardır.

32. Anlamlı bir internet trafiği bilgisi için GPRS/WAP kaydında Erişilen Sayfa ve Hedef IP haneleri dolu olmalı ve CGNAT verileri ile kıyaslanabilmelidir. CGNAT verilerinde görülen ve bağlantı talebi olduğu iddia edilen Genel IP adreslerinin GRPS/WAP verilerinde Hedef IP olarak yer alması ve Erişilen Sayfa hanesinin de dolu ve uyumlu olması; bunlarla birlikte bağlantı süresi ve konum uyumunun da olması halinde tutarlı kayıtlar yoluyla herhangi bir

internet sitesi veya uygulamanın kullanım iddiasında bulunulabileceği değerlendirilmektedir. Bu hususların birlikte sağlanabildiği bir kayda tarafımızdan rastlanmamıştır.

33. HIS (CGNAT) ve HTS-GPRS kayıtlarının kıyaslanarak ByLock kullanımı tespiti konusu **Adli Tıp Kurumunca** (ATK) da incelenmiştir. ATK incelemesi daha önce basında paylaşılmıştır⁴. İzmir 2. Ağır Ceza Mahkemesinde 207/269 E. Sayılı kovuşturma kapsamında ATK'ya BTK'dan getirilen HIS (CGNAT) ve HTS-GPRS kayıtlarını içeren GSM operatör kayıtları iletilmiş ve sanığın ByLock kullanıcısı olup olmadığının tespiti talep edilmiştir. ATK tarafından hazırlanan raporun başlangıç bölümü ekran resmi aşağıda paylaşılmıştır. İzmir 2. Ağır Ceza Mahkemesinin ATK'dan talebinin Yargıtay 16. Ceza Dairesinin uzman görüşüne konu karar metinleriyle benzer olduğu görülmektedir.

T.C. ADALET BAKANLIĞI Adli Tıp Kurumu		
Adli Bilişim İhtisas Dairesi Veri İnceleme Şubesi Rapor No: 66560527-101.04-2019/22383/654/67V		AB-0273/T
		2019/22383
		23/05/2019

RAPOR

1. **İNCELEMİYİ 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
3. **TALEP EDİLEN İNCELEME:** Sanık E. B. 'a ait CGNAT ve HTS kayıtları yazı ekinde gönderilmiş olup mevcut verilerin sanığın bylock kullanıcısı olduğunu gösterip göstermediği konusunda düzenlenecek raporun Mahkemenize gönderilmesi talep edilmektedir.

Resim 2: ATK raporu başlangıç bölümü

34. ATK'nın ilk raporu 23 Mayıs 2019 tarihlidir ve HIS (CGNAT) ile GPRS (HTS) kayıtlarını inceleyen Adli Bilişim İhtisas Dairesi Veri İnceleme Şubesi tarafından düzenlenmiştir. Biri daire başkanı 4 uzman tarafından imzalanan raporda önce HTS-GPRS kayıtlarındaki boş olan Hedef IP sütunu vurgulanmıştır. ATK raporunda boş olduğu vurgulanan Hedef IP sütununun yer aldığı ekran resminin bir bölümü kişisel veriler yer aldığından netliği giderilerek aşağıda sunulmuştur.

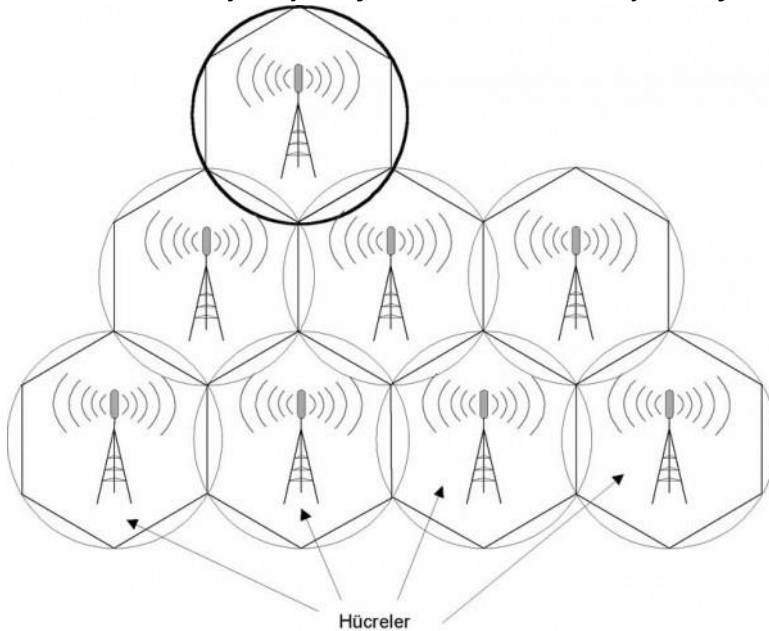
⁴ <https://www.meridyenhaber.com/bylock-operator-atk-pilot-makale,44859.html> ve <https://www.meridyenhaber.com/operator-kayıtlarından-bylock-cikmaz-makale,44862.html>

36. HTS-GPRS kayıtları operatörlerin genellikle muhasebe/faturalandırma amacıyla tuttukları kayıtlardır. **HIS (CGNAT) ve HTS-GPRS verilerinden anlamlı bir internet trafiği bilgisine ulaşmanın mümkün olmadığı, bu verilerin birbirleriyle kıyaslanmasından ByLock veya başka bir uygulamanın kullanımına yönelik teknik olarak herhangi bir şüpheyne yer vermeyecek şekilde tespit yapılamayacağı anlaşılmaktadır.**

A.4. GSM operatörlerinin konum/baz verilerini nasıl kayıt aldığının, baz verilerinin teknik olarak herhangi bir şüpheyne yer vermeyecek şekilde kesin bilgi niteliklerinin olup olmadığının, CGNAT kayıtları ile HTS-İletişim veya HTS/GRPS kayıtları baz verileri kıyaslanarak ByLock uygulamasının kullanımının kuşkuya yer vermeyecek şekilde tespitinin mümkün olup olmadığının değerlendirilmesi.

37. GSM operatörlerinin konum/baz verilerini nasıl kayıt altına aldığına yönelik detaylı inceleme tarafımızdan hazırlanarak imzalanan “GSM Hatlarının Ortak Baz (Konum) Kaydı Vermesine Yönelik Sorular Üzerine Değerlendirmeler”⁶ başlıklı uzman görüşünde yer almaktadır ve anılan uzman görüşü EK-2 olarak sunulmuştur. İşbu uzman görüşü kapsamında önemli görülen bazı hususlara tekrar değinilmekle birlikte EK-2 uzman görüşünde daha kapsamlı değerlendirme mevcuttur. Mevzuatta belirtilen koşullarla tutulan HTS-İletişim veya HTS-GPRS kayıtlarında yer alan baz bilgileri tek bir baz istasyonundan alınan verilerdir. Ancak bu verinin abonenin noktasal konumunu belirtme ihtimali bulunmamaktadır.

38. GSM operatörleri kesintisiz iletişimi devam ettirebilmek için genellikle aşağıdaki resimde gösterilen petek modelini kullanmaktadır. Baz istasyonlarının yerleşiminin, şehir içi veya dışında olma gibi koşullara bağlı olarak 35 km. mesafeleri bulan bir çap dâhilinde herhangi bir konumu işaret edebileceği anlaşılmaktadır. Bu durum baz istasyonlarının kullandıkları teknoloji ve yerleşim mimarileri nedeniyle oluşmaktadır.



Resim 5: Baz istasyonları petek modeli yerleşimi

⁶ <https://www.patreon.com/posts/gsm-hatlarinin-38097243>

GSM OPERATÖR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDİALARI ÜZERİNE DEĞERLENDİRMELER

Bir baz istasyonunun hizmet kapasitesi dolduđu anda veya kapsama alanı dıřına ıktıđında veya herhangi bir nedenle sinyal gc zayıfladıđında komřu istasyonlar devreye girmektedir. Mobil cihazlar da sinyal gc en iyi olan baz istasyonundan hizmet alacak řekilde tasarlanmıřtır. Abone hangi baz istasyonundan hizmet aldıđını bilemez. GSM firmaları ise HTS kayıtlarında baz bilgisi olarak nihai olarak hizmet veren baz istasyonunun konumunu kaydederler.

Sonuç olarak, **HTS kayıtlarında yer alan baz (konum) bilgileri noktasal konum deđildir. Abonenin nihai olarak hizmet aldıđı baz istasyonunun konum verisidir. Abonenin hizmet alınan baz istasyonunda deđil, komřu baz istasyonlarının birine daha yakın olması da mmkndr.**

39. GPRS (General Packet Radio service) baz istasyonları da benzer řekilde konum tespiti yaparlar. Ancak GPRS istasyonları, ses verisi iletimi amacıyla kurulmuř baz istasyonları kadar yaygın deđildir. Birlikte veya ayrı olabilirler.

40. GPRS internet zerinde veri trafiđi oluřtuka kayıt tutar. Ancak gnmzde internet trafiđi sesli iletiřim trafiđine gre daha yođun ve devamlılık arz eder niteliktedir. zellikle sosyal medya ve iletiřim uygulamaları srekli veri alıřveriři sađlarlar ve mobil cihazların hcresel veri iletimi zellikleri aık olduđu srece (kablosuz WiFi hatlarına bađlı deđilse) GSM operatrlerince sađlanan GRPS hizmeti zerinden veri alıřveriři devamlılık gsterir. Bu nedenle GPRS verilerinin kaydında GSM operatrlerince belirlenen kayıt yenileme sreleri bařında konum/baz verisi kaydedilir. GSM operatrlerin GPRS/WAP kayıtlarında belirledikleri kayıt yenileme (yeniden bařlatma) sreleri bitiminde, yeni kayıt bařladıđında konum bilgisinin de gncellenmesi gereklidir. **Konum bilgisinin gncellenmemiř olması sistemin sađlıklı kayıt yapmadıđı řeklinde yorumlanabilir.** Turkcell ve Trk Telekom (Avea) operatrlerinin 7200 saniyelik, Vodafone operatrnn ise 3600 saniyelik kayıt yenileme sresi kullandıđı gzlenmektedir ancak bu sreler operatrlerce deđiřtirilebilir.

41. CGNAT, baz/konum verilerini kaydetmek iin tasarlanan bir sistem deđildir. HIS (CGNAT) kayıtları kapsamında yer alan baz/konum verileri HTS-İletiřim veya HTS-GPRS kayıtlarından alınabilir. İncelene kayıtlardan yapılan ıkarım HIS (CGNAT) kayıtlarında yer alan baz/konum verilerinin HTS-GPRS kayıtlarından alındıđı řeklindeydir. Dolayısıyla **HIS (CGNAT) kayıtları ile HTS-GPRS kayıtları baz/konum verilerinin uyumlu olması olađan bir durumdur. HIS (CGNAT) kayıtları ile HTS-İletiřim kayıtları baz/konum verilerinin uyumlu olması da uyumsuz olması da ařađıda deđinilecek gecikmeli kayıt problemleri nedeniyle olađan durumlardır. Ancak baz/konum verilerinde uyum ya da uyumsuzluk, ByLock veya bařka bir uygulamanın kullanımına ynelik teknik olarak herhangi bir řpheye yer vermeyecek řekilde bir tespite imkn sađlamayacaktır.**

42. Yukarıda aıklanan hususlara ilave olarak HTS-GPRS kayıtlarında gecikme sz konusu olabilmektedir. HTS-İletiřim kayıtları baz istasyonunun kayıt sisteminin ayarlandıđı saate uygun olarak hizmetin alındıđı yani arama/aranma/mesaj alma/mesaj atma iřleminin bařlangı saatinde kayıt tutar. GSM operatrlerinin iřleyiři řeffaf olmamakla birlikte, HTS-İletiřim kayıt sistemlerinde TBİTAK UME tarafından sađlanan atomik saat hizmetini kullanmadıkları deđerlendirilmekte ve incelenen ok sayıda kayıttan gzlenmektedir. Ancak HTS-İletiřim kayıt sisteminin saat ayarında bir hata yoksa kayıt saatinde de hata

GSM OPERATR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDİALARI ZERİNE DEđerLENDİRMELER

beklenmemektedir. Hata oranının hayatın olağan akışında (± 5 dakika gibi) kabul edilebilir makul mertebelerde olacağı değerlendirilmektedir. Ancak saat ayarında hata yapılması nedeniyle ya da yaz-kış saati ayarlaması yapılmaması nedenleriyle bir saati bulan farkların gözlemlendiği de olmuştur.

43. GSM operatörlerinin kayıt sistemleri şeffaf (kamuoyuna açık) olmadığından HTS-GPRS kayıtlarındaki gecikme miktarı konusunun net olarak bilinebilmesi mümkün olmamaktadır. Ancak ByLock isnatlı çok sayıda kovuşturma dosyasında mahkemelerce atanan bilirkişilerin düzenledikleri raporlarda atıf yaptıkları bir yazı ve yazıda geçen azami gecikme süresi bilgisi yer almaktadır. Avea İletişim A.Ş.'nin 04.04.2017 tarih ve TT.504444811-856.02-73238 sayılı yazıları ile BTK'nın "Baz Tutarsızlıkları" ile ilgili resmi cevap verdiği, bu yazı içeriğinde 2015 yılı öncesinde GPRS kullanımlarında baz (lokasyon) bilgisinin, GPRS kullanımının ilk başında okunduğu ve abonenin bağlantısının açık kaldığı sürece GPRS CDR'larının hep ilk baz bilgisinin basıldığına belirtildiği, 2015 yılı itibarıyla "Konum Ara Güncelleme İşlevi"nin devreye alınarak uzun GRPS kullanımlarında baz (lokasyon) bilgilerinin 8 (sekiz) saatte bir güncellenerek CDR'lara yazıldığı ifade edilmiştir. Anılan bilgi çok sayıda kovuşturma dosyasında ve farklı bilirkişi raporlarında yer almaktadır.

44. Avea İletişim A.Ş.'nin yukarıda atıf yapılan yazısından anlaşılan 2015 yılı öncesinde GPRS hizmeti başlangıcında konum bilgisinin kaydedildiği ve hücresel veri özelliği kapatılmadığı sürece ilk baştaki konum bilgisinin kayıt yenileme süresi dolsa ve yeni kayıt başlasa dahi değişmediğidir. Değişmeyen konum hali günlerce devam edebilir. Bu durumun örnekleri incelenen çok sayıda HTS-GPRS kaydında görülmüştür. 2015 yılı sonrasında ise konum bilgilerinin hücresel veri hizmetinin kesilmesi ve yeniden başlatılması halinde veya 8 (sekiz) saatte bir güncellendiğidir.

45. Avea İletişim A.Ş.'nin yukarıda atıf yapılan yazısından anlaşılan 2015 yılı öncesinde GPRS hizmeti başlangıcında konum bilgisinin kaydedildiği ve hücresel veri özelliği kapatılmadığı sürece ilk baştaki konum bilgisinin kayıt yenileme süresi dolsa ve yeni kayıt başlasa dahi değişmediğidir. Değişmeyen konum hali günlerce devam edebilir. Bu durumun örnekleri incelenen çok sayıda GPRS kaydında görülmüştür. 2015 yılı sonrasında ise konum bilgilerinin hücresel veri hizmetinin kesilmesi ve yeniden başlatılması halinde veya 8 (sekiz) saatte bir güncellendiğidir.

46. Benzer bir husus kovuşturma dosyalarına dahil edilen ve Adli Bilişim Uzmanı T. Koray PEKSAYAR tarafından kişisel internet sitesinde yayımlanan⁷ "HTS Kayıtlarının GPRS/WAP Bölümüyle CGNAT Kayıtlarının Kıyaslanması" başlıklı makalesinde ve makale kapsamında sunulan Avea (Türk Telekom A.Ş.) tarafından Bilgi Teknolojileri ve İletişim Kurumuna yazılan 25.10.2017 tarihli yazıda açıklanmıştır. Söz konusu yazının ekran görüntüsü aşağıda tekrar

⁷ <https://koray.peksayar.org/hts-kayitlarinin-gprs-wap-bolumuyle-cgnat-kayitlarinin-kiyaslanmasi/>
GSM OPERATÖR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDİALARI ÜZERİNE DEĞERLENDİRMELER

sunulmuştur.

SAYI : TT.50444811 - 576.18 - 198406
KONU : Abone Bilgisi

25.10.2017

T. C. BİLGİ TEKNOLOJİLERİ ve İLETİŞİM KURUMU'NA
(Bilgi Sistemleri Dairesi Başkanlığı)

İlgi: 21.09.2017 tarih ve 2017.565257 sayılı yazınız.

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 bulunduğu tespit edildiğine, söz konusu hususun teknik olarak incelenerek bilgi verilmesine ilişkin ilgi yazınız alınmıştır.

Ses ve veri (internet) şebekeleri benzerlikler gösterebilir 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.

Data şebekesinde abone her lokasyon değişikliği yaptığı anda CDR'a yazılan ilgili lokasyon verisi güncellenmemektedir. Bu verinin güncellenmesi, abone erişim tipinin değişmesi (2G-3G-LTE), abonenin bağlı olduğu SGSN'in değişmesi gibi değişik teknik şartlar gerektirmektedir.

Abone farklı lokasyonlar arasında seyahat ederken erişiminde kopma yaşanmaz ve erişim tipinde değişiklik olmaz ise data oturumuna başladığı andaki lokasyon verisi CDR'da sabit kalacaktır.

Ortalama SES oturum süreleri DATA oturum sürelerine göre daha kısa olduğu için SES CDR'ları DATA CDR'larına göre daha doğru lokasyon verisi içerecektir.

Ayrıca, 2014 yılında bahsi geçen CDR'lar IT'de işlenirken, ilk parçalı CDR 12 saate kadar bekletilip, son gelen parçalı CDR ve aralarındaki tüm parçalı CDR'lar tek CDR olarak konsolide edilip Kurumunuza tek CDR şeklinde gönderiliyordu. Bu yapıda Kurumunuza gönderilen abone CDR'ında, ilk parçalı CDR'da gelen lokasyon verisi gönderilmiştir. Bu nedenle yukarıda da açıklandığı gibi, internet kullanımları ses CDR'ları kadar güncel lokasyon bilgisini içermemektedir. 2016 yılının Nisan ayında Kurumunuzdan alınan onay sonrasında, Kurumunuzun CDR'ları daha hızlı alma talebi doğrultusunda CDR konsolidasyonu kaldırılmıştır.

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.

"Bu belge, 5070 sayılı Elektronik İmza Kanununun 5. maddesi gereğince güvenli elektronik imza ile imzalanmıştır.
Evrak bilgisine <http://www.turktelekom.com.tr/editis-belge-dogrulama> sayfasından "nyqt368C00E1" Belge Doğrulama No ve evrak tarihi ile erişebilirsiniz.
www.evra.com.tr İşletme Merkezi Sicil no/Mersis no:

Resim 6: Türk Telekom A.Ş. yazısı ekran görüntüsü

Adli Bilişim Uzmanı T. Koray PEKSAYAR tarafından makalesinde "CGNAT ile HTS kayıtlarının kıyaslamasının yapılması teknik açıdan hatalıdır. Bunun nedeni aşağıda GSM OPERATÖR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDİALARI ÜZERİNE DEĞERLENDİRMELER

ayrıntılıdır” denildikten sonra detaylı açıklamalar yapılmış, sonuç olarak aşağıdaki cümlelere yer verilmiştir.

“Yazıda da veri CDR bilgilerinin ses CDR bilgilerine göre gecikmeli aktarıldığı doğrulanmaktadır.

Sayıli teknik nedenlerle, CGNAT dökümünün HTS dökümüyle kıyaslanması doğru sonuç vermeyecektir.”

47. Sonuç olarak HTS-İletişim baz/konum verilerinin kayıt sisteminin saat ayarı ile uyumlu olduğu, HTS-GPRS konum verilerinin ise 8 (sekiz) saate kadar fark içerebileceği anlaşılmaktadır. HIS (CGNAT) kayıtları baz/konum verilerinin HTS-İletişim baz/konum verileri ile 8 (sekiz) saate kadar fark içermesi de olağandır. Ne kadar zaman farkı olduğu ise her bir kayıtta farklılık gösterebilmektedir ve zaman farkı olan kayıtların baz/konum verilerinin kıyaslanması anlamlı değildir. HIS (CGNAT) kayıtları baz/konum verileri ile HTS-İletişim veya HTS-GPRS kayıtları baz/konum verileri kıyaslanması, ByLock veya başkaca bir uygulamanın kullanımının teknik olarak herhangi bir şüpheye yer vermeyecek şekilde tespitine imkân vermemektedir.

A.5. Soruşturma/kovuşturma dosyalarına dahil edilen BTK kaynaklı sayısal verilerin teknik olarak herhangi bir şüpheye yer vermeyecek bilgi nitelikleri var mıdır?

48. BTK kaynaklı HTS kayıtları ham veri değildir. Ham veriler kullanılarak metin haline getirilen veya tablolaştırılan kayıtlardır. Ham verilerin anlaşılır metin ya da tablo halinde kayıtlara çevrilmesi genellikle yazılımlar aracılığıyla yapılır. Ham verilerden metin ya da tablo haline getirilen veriler de sayısal verilerdir.

49. Sayısal ortamda depolanan veriler, istenilen şekilde; istenilen zamanı gösterecek, istenilen bilgiyi içerecek, istenilen içeriğe sahip olacak, istenilen kişi tarafından oluşturulduğu izlenimini verecek şekilde, herhangi bir kişi veya kişiler tarafından oluşturulabilir. Bu durum mahkemelere yansımış çok sayıda örneği mevcuttur.

50. Adli bilişimde delil bütünlüğünün sağlanabilmesi için delilin toplama aşamasından inceleme aşamasının sonuna kadar değişmezliğinin sağlanması gereklidir. Sayısal imza, zaman damgası ve özüt değeri kullanılarak verinin değişmezliği ve bütünlüğünün korunduğu ispatlanabilir.

51. Delilin bütünlüğünün, değişmezliğinin dolayısıyla güvenliğinin sağlanması açısından yalnızca imaj alınmasında değil, HTS vb. verilerin de kullanılmasında özüt değeri hesaplanmalı ve kopyalar özüt değeri kontrolüyle çoğaltılmalıdır.

52. HTS verilerinin BTK veri tabanlarında depolandığı değerlendirilmektedir. Ancak BTK veri tabanlarına da operatörler yoluyla gelmektedir. Öncelikle operatörlerden BTK veri tabanlarına aktarım sırasında verilerin değişmezliğinin (güvenliğinin) sağlanması ve ilerleyen zamanlarda da kontrol edilebilmesi amacıyla sayısal imza, zaman damgası ve özüt değeri kullanılmalıdır.

GSM OPERATÖR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDIALARI ÜZERİNE DEĞERLENDİRMELER

53. Uzman görüşü kapsamında açıklanan hususlar ile EK-1 ve EK-2 uzman görüşleri kapsamlarında açıklanan hususlar birlikte değerlendirildiğinde BTK kaynaklı sayısal verilerin teknik olarak herhangi bir şüpheyeye yer vermeyecek şekilde bilgi niteliklerinin olmadığı anlaşılmaktadır.

A.6. GSM operatör kayıtlarının adli bilişim uzmanlığı kapsamında incelenmesi yoluyla ByLock uygulamasının kullanımının teknik olarak herhangi bir şüpheyeye yer vermeyecek şekilde tespit edilebildiği bir örneğin bulunup bulunmadığının değerlendirilmesi.

54. İşbu uzman görüşünü hazırlayan ve imzalayan uzmanlar tarafından (üç uzmanın ayrı ayrı incelediği toplam kayıt sayısı) yaklaşık 2.000 (ikibin) farklı dosyada HIS (CGNAT) başta olmak üzere GSM operatör kayıtları incelenmiştir. İncelenen kayıtlar arasında 5651 sayılı kanunda tanımlandığı şekliyle anlamlı bir internet trafik kaydı ile ByLock uygulamasının kullanımını teknik olarak herhangi bir şüpheyeye yer vermeyecek şekilde tespitine imkân sağlayabilecek kayda rastlanmamıştır.

A.6. ByLock uygulaması kullanımının teknik olarak herhangi bir şüpheyeye yer vermeyecek şekilde tespiti için gerekenlerin değerlendirilmesi.

55. Adli Bilişim Uzmanı T. Koray PEKSAYAR tarafından kişisel internet sitesinde “Yargıtay 16. Ceza Dairesi Kararına Teknik Bakış: CGNAT Neden Tek Başına Delil Olamaz?-Bölüm 1” başlıklı makalede⁸ bu husus açıklanmıştır.

56. ByLock adlı uygulamanın kullanıldığından teknik olarak herhangi bir şüpheyeye yer vermeyecek şekilde söz edilmesi için sırayla;

- i. ByLock uygulamasının cep telefonu veya uygun özelliklerde bir akıllı cihaza kurulması,
- ii. Bu uygulama kullanılarak kullanıcı kaydı oluşturulması,
- iii. Kullanıcı kaydı oluşturulduktan sonra iletişim kurulacak kişilerin kullanıcı numaralarının (user ID) adres defterine eklenmesi,
- iv. Uygulama kullanılarak haberleşme yapılması adımlarının gerçekleştirilmesi ve bu adımların eksiksiz olarak gerçekleştirildiğinin tespit edilmesi gereklidir.

Bu adımların gerçekleştirilerek ByLock uygulaması kullanılarak ByLock sunucusuna gerçekten bağlantı kurulduğunun ve kullanıma devam edildiğinin eksiksiz tespitinin yapılması için gerekli akıllı cep telefonu incelemesinin, gerekli bağlantı kayıtları incelemesinin ve ByLock sunucusundan elde edilmiş verilerden yapılan içerik ve kullanıcı kaydı sorgulamasının yapılması gereklidir.

Bu unsurların birlikte varlığında ve aralarında çelişki olmaması durumunda ByLock uygulaması kullanılarak ByLock sunucusuna gerçekten bağlantı kurulduğundan ve kullanıma devam edildiğinden bahsedilebilir.

⁸ <https://koray.peksayar.org/yargitay-16-ceza-dairesi-kararina-teknik-bakis-cgnat-neden-tek-basina-delil-olamaz-bolum-1/>

GSM OPERATÖR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDİALARI ÜZERİNE DEĞERLENDİRMELER

SONUÇLAR VE DEĞERLENDİRMELER

Yukarıda ayrıntıları ile izah etmeye çalıştığımız, bilimsel gerekçelerle aşağıda belirtilen sonuçlar ve değerlendirmelere ulaşılmıştır.

MİT'in ByLock raporunda yer alan ve ekran resmi sunulan metinde kullanıcı listelerinin **operatör verilerinin tam ve eksiksiz olduğu ön kabulü** ile hazırlandığı açıkça belirtilmektedir ancak HIS (CGNAT) kayıtlarının açıklanan özellikleri nedeniyle operatörlerin teknik olarak herhangi bir şüpheye yer vermeyecek şekilde kullanıcıyı tespit etmeye imkan sağlayan kayıt tutamayacakları değerlendirilmektedir.

HIS (CGNAT) sistemi işleyişi nedeniyle GSM numarası, Genel IP, Özel IP, Genel Port, Özel Port, Hedef IP, Hedef Port ve Oturum Başlama Tarihi (GSM kullanıcılarından karşı sunucuya bağlantı talebinin gönderildiği tarih ve saat verisi) verilerini tutabileceği değerlendirilmektedir. HIS (CGNAT) kayıtları kapsamında yer alan IMSI, IMEI ve BAZ verilerinin HIS (CGNAT) sistemi kapsamında kaydedilmediği, GSM operatörlerinin HTS-İletişim veya HTS-GPRS sistemlerinden veya veri bankalarından temin edildiği değerlendirilmektedir. HIS (CGNAT) kayıtlarında yer alan BAZ verisinin HTS-GPRS sistemi verilerinden alındığı değerlendirilmektedir.

HIS (CGNAT) ve HTS-GPRS verilerinden anlamlı bir internet trafiği bilgisine ulaşmanın mümkün olmadığı, bu verilerin birbirleriyle kıyaslanmasından ByLock veya başka bir uygulamanın kullanımına yönelik teknik olarak herhangi bir şüpheye yer vermeyecek şekilde tespit yapılamayacağı anlaşılmaktadır.

HTS baz/konum verileri kullanıcının noktasal konumunu değil, hizmet alınan baz istasyonunun konumunu göstermektedir. İlgilinin noktasal konumu baz istasyonunun hizmet verdiği kapsama (petek yapısı) alanı içinde olabileceği gibi komşu baz istasyonu kapsama alanları içinde de olabilir. HTS ve GPRS baz verileri kullanılarak noktasal konumunun teknik olarak herhangi bir şüpheye yer vermeyecek şekilde tespiti mümkün değildir.

CGNAT, baz/konum verilerini kaydetmek için tasarlanan bir sistem değildir. HIS (CGNAT) kayıtları kapsamında yer alan baz/konum verileri HTS-İletişim veya HTS-GPRS kayıtlarından alınabilir. İncelene kayıtlardan yapılan çıkarım HIS (CGNAT) kayıtlarında yer alan baz/konum verilerinin HTS-GPRS kayıtlarından alındığı şeklindedir. Dolayısıyla HIS (CGNAT) kayıtları ile HTS-GPRS kayıtları baz/konum verilerinin uyumlu olması olağan bir durumdur. HIS (CGNAT) kayıtları ile HTS-İletişim kayıtları baz/konum verilerinin uyumlu olması da uyumsuz olması da aşağıda değinilecek gecikmeli kayıt problemleri nedeniyle olağan durumlardır. Ancak baz/konum verilerinde uyum ya da uyumsuzluk, ByLock veya başka bir uygulamanın kullanımına yönelik teknik olarak herhangi bir şüpheye yer vermeyecek şekilde bir tespiti imkân sağlamayacaktır.

HTS-İletişim baz/konum verilerinin kayıt sisteminin saat ayarı ile uyumlu olduğu, HTS-GPRS konum verilerinin ise 8 (sekiz) saate kadar fark içerebileceği anlaşılmaktadır. HIS (CGNAT) kayıtları baz/konum verilerinin HTS-İletişim baz/konum verileri ile 8 (sekiz) saate kadar fark içermesi de olağandır. Ne kadar zaman farkı olduğu ise her bir kayıta farklılık gösterebilmektedir ve zaman farkı olan kayıtların baz/konum verilerinin kıyaslanması anlamlı değildir. HIS (CGNAT) kayıtları baz/konum verileri ile HTS-İletişim veya HTS-GPRS kayıtları

baz/konum verileri kıyaslanması, ByLock veya başkaca bir uygulamanın kullanımının teknik olarak herhangi bir şüpheye yer vermeyecek şekilde tespitine imkân vermemektedir.

HTS kayıtları ham veri değildir. Ham veriler kullanılarak metin haline getirilen veya tablolaştırılan kayıtlardır. Ham verilerden metin ya da tablo haline getirilen veriler de sayısal verilerdir.

Uzman görüşü kapsamında açıklanan hususlar ile EK-1 ve EK-2 uzman görüşleri kapsamlarında açıklanan hususlar birlikte değerlendirildiğinde BTK kaynaklı sayısal verilerin teknik olarak herhangi bir şüpheye yer vermeyecek şekilde bilgi niteliklerinin olmadığı anlaşılmaktadır.

Uzman görüşünü hazırlayan ve imzalayan uzmanlar tarafından (üç uzmanın ayrı ayrı incelediği toplam kayıt sayısı) yaklaşık 2.000 (ikibin) farklı dosyada HIS (CGNAT) başta olmak üzere GSM operatör kayıtları incelenmiştir. İncelenen kayıtlar arasında 5651 sayılı kanunda tanımlandığı şekliyle anlamlı bir internet trafik kaydı ile ByLock uygulamasının kullanımını teknik olarak herhangi bir şüpheye yer vermeyecek şekilde tespitine imkân sağlayabilecek kayda rastlanmamıştır.

ByLock uygulaması kullanılarak ByLock sunucusuna gerçekten bağlantı kurulduğunun ve kullanıma devam edildiğinin eksiksiz tespitinin yapılması için gerekli akıllı cep telefonu incelemesinin, gerekli bağlantı kayıtları incelemesinin ve ByLock sunucusundan elde edilmiş verilerden yapılan içerik ve kullanıcı kaydı sorgulamasının yapılması gereklidir.

Bu unsurların birlikte varlığında ve aralarında çelişki olmaması durumunda ByLock uygulaması kullanılarak ByLock sunucusuna gerçekten bağlantı kurulduğundan ve kullanıma devam edildiğinden bahsedilebilir

İşbu uzman görüşü, şüpheli/sanık veya vekili tarafından sunulması halinde Sayın Mahkemenin/Dairenin takdirlerine arz olunur.

Saygılarımızla.

02 Haziran 2021

Berker KILIÇ

Adli Bilişim Uzmanı
Veri Bilimci

T. Koray PEKSAYAR

Adli Bilişim Uzmanı
Bilgi Teknolojileri Y. Lisans

Levent MAZILIGÜNEY

Adli Bilişim Uzmanı
Y. Mühendis, Hukukçu

EKLER :

EK-1 ByLock Kullanıcı Tespitleri ve Yargılamalara Etkisi Üzerine Değerlendirmeler (internet ortamında yer aldığından fiziki olarak sunulmamıştır)

EK-2 GSM Hatlarının Ortak Baz (Konum) Kaydı Vermesine Yönelik Sorular Üzerine Değerlendirmeler (internet ortamında yer aldığından fiziki olarak sunulmamıştır)

GSM OPERATÖR KAYITLARI KULLANILARAK BYLOCK UYGULAMASI KULLANIMI İDDIALARI ÜZERİNE DEĞERLENDİRMELER