BİLİŞİM SİSTEMLERİ ÜZERİNDE ARAMA VE EL KOYMA TEDBİRİ

Murat Volkan Dülger*

I. GENEL OLARAK

1. Ülkemizde ve yabancı ülkelerde bilişim suçları konusunda yapılan özellikle ceza hukuku alanındaki yasal düzenlemelerin tek başına bu suçların önlenmesinde yeterli olmadığı görülmektedir. Ceza normları hiçbir zaman tek başına suçun önlenmesi açısından caydırıcı ve suçu yok edici bir etken olmamıştır. Gelişen teknolojiyle birlikte özellikle bilişim alanında her gün yeni suç işleme modellerinin ortaya çıkması, yapılan ceza hukuku düzenlemelerinin de eksik ve yetersiz kalmasına neden olmaktadır.

2. Ülkemiz açısından ise durum daha da kötü bir tablo çizmektedir. Teknoloji ithal eden bir ülke olmamızın yanı sıra hukuksal düzenlemeler de ithal eden bir ülke olduğumuz için her ikisini birleştiren bir alan olan bilişim suçlarının hukuksal düzenlemesi konusunda hataların ve yetersizliklerin olması kaçınılmazdır. Tüm hukuk kuralları toplumsal düzenin ve ihtiyaçların birer yansımasıdır; bu nedenle hukuk kuralları uygulanmaya konuldukları toplumun bünyesine uymalı ve toplumun gerisinde kalmamalıdır. Bunun yanı sıra bu kurallar o toplumda bulunan diğer hukuk kurallarıyla ve özellikle "küreselleşen" dünyada toplumun ilişki içinde bulunduğu diğer toplumların hukuk kurallarıyla uyum içinde olmalıdır.

3. Uzun zamandır onaylanması gerektiğini belirttiğim, 10.11.2010 tarihinde ülkemiz tarafından imzalanmış olan Avrupa Siber Suç Sözleşmesi, 22.4.2014 tarih ve 6533 sayılı *"Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun"* ile onaylanarak uygun bulunmuş, 2.5.2014 tarihli ve 28988 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Dolayısıyla Avrupa Siber Suç Sözleşmesi iç hukukumuzun bir parçası haline gelmiştir. Bundan sonra bu Sözleşmeye uyum için iç hukukumuzda da bazı değişikliklerin yapılması ve özellikle soruşturma ve kovuşturma makamlarının Sözleşmeye uygun işlem yapmalarının, yani Sözleşmenin uygulanmasının sağlanması gerekir. Ancak bu konuda, özellikle ceza muhakemesi koruma tedbirleri açısından önemli eksiklerin olduğu ve bu konuda hareket edilmediği görülmektedir.

4. Bilişim suçlarının çok ciddi bireysel ve toplumsal sonuçları bulunur. Bu nedenle bu suçlarla yürütülecek mücadele de çok boyutlu olmalıdır. Ceza normlarıyla sağlanmaya çalışılan koruma, bilişim suçlarıyla mücadelenin yalnızca bir boyutudur. Bu mücadelenin diğer bir boyutu da bilişim sistemi kullanan kişilerin, kurumların ve hatta devletlerin bu konuda almaları gereken tedbirler ve ceza hukuku dışında özellikle sanal alanın hukuksal bir alan haline getirilmesi için yapmaları gereken düzenlemelerdir. Ayrıca bilişim suçlarının soruşturulması ve kovuşturulması da ayrı bir teknik uzmanlık bilgisi ve deneyimi gerektirmekte ve bunların yapılabilmesi soruşturma makamlarına

* Doç. Dr., İstanbul Aydın Üniversitesi Hukuk Fakültesi Ceza Hukuku, Ceza Muhakemesi Hukuku ve Bilişim Hukuku Anabilim Dalı öğretim üyesi, volkan.dulger@dulger.av.tr.

yetki veren özel muhakeme kurallarının bulunmasını gerekir. 5271 sayılı CMK'nın 134. maddesiyle bu alanda düzenleme yapılmış, ayrıca bir de yönetmelik çıkarılarak, bu soruşturmalar hukuk kurallarıyla düzenlenmeye çalışılmıştır. Ayrıca CMK'nın 135. maddesi akış halindeki veriler için dikkate alınması gereken diğer bir düzenlemedir.

5. Ancak bilişim teknolojilerinin ilerlemesi ve hayatın her alına girmesi; büyük veri, yapay zekâ, nesnelerin interneti, blok zincir kavramların günlük hayatımızın bir parçası olması; kamusal ve öze pek çok hizmetin bilişim sistemleri aracılığıyla internet üzerinden gerçekleştirilmesi, klasik suçların da bilişim sistemleri aracılığıyla ve özellikle internet üzerinden işlenmesi yol açmaktadır. Dolayısıyla bilişim sistemleri üzerinde gerçekleştirilecek arama ve el koyma tedbiri yalnızca bilişim suçlarında değil, klasik suçlarda da kullanılmaktadır. Nitekim ülkemizin 15 Temmuz 2016'da maruz kaldığı darbe girişimi sonrasında FETÖ/PYD terör örgütüne yapılan soruşturma ve kovuşturmaların büyük bölümünde dijital deliller kullanılmaktadır. Darbe girişimi gibi klasik bir suçta dahi dijital delillerin ana ispat aracı olması konunun önemini göstermesi açısından son derece önemlidir. Dolayısıyla bu çalışmada yapacağım açıklamalar yalnızca bilişim suçları bakımından değil, dijital delillerin kullanıldığı her türlü suça ilişkin soruşturma ve kovuşturma açısından dikkate alınmalıdır.

II. BİLİŞİM SİSTEMLERİNE YÖNELİK CEZA MUHAKEMESİ KORUMA TEDBİRLERİ

A. Bilişim Sistemlerinde Arama, Kopyalama ve El Koyma

1. Yasal Dayanak

6. Bilişim sistemlerine karşı veya bilişim sistemleri kullanılmak suretiyle bir suç işlendiğinde yapılması gereken en önemli işlemlerden biri söz konusu sistem üzerinde inceleme yapılmasıdır. Bu sistem suçun failine ait olabileceği gibi mağdura ya da üçüncü bir kişiye de ait olabilir. Ancak bu arama işleminin, aynen evde ya da iş yerinde yapılan aramalar gibi, bir yasa normuna dayanılarak yapılması gerekir; zira bu temel hak ve özgürlükleri kısıtlayan bir işlemdir. Aksi takdirde keyfi ve hukuksuz uygulamaların gerçekleşmesi kaçınılmazdır. Bu ise hem maddi gerçeğin ortaya çıkarılmasına zarar verir hem de elde edilen deliller gerçeği yansıtsa da hukuka aykırı elde edildiği için yasak delil olur ve soruşturmada ve kovuşturmada kullanılamaz[1]. İşte bu nedenlerle 5271 sayılı CMK'nın 134. maddesinde *"bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* başlığı altında bilişim sistemlerinde yapılacak delil araştırması yöntemi düzenlenmiştir. Ayrıca *Adli ve Önleme Aramaları Yönetmeliği*'nin[2] 17. maddesinde de yasa maddesindeki aynı başlıkla düzenleme yapılmıştır. Ancak birkaç ifade dışında yönetmelikte CMK'nın 134. maddesi aynen tekrar edilmiştir. Ayrıca günümüzde iletişim, aslında bir bilgisayar olan cep telefonlarıyla yapıldığı için, dijital verilerin iletimi yöntemiyle ve yalnızca sesli değil, görsel veya yazılı metinlerin anlık paylaşımı yöntemiyle de yapılmaktadır. Dolayısıyla bilişim sistemlerini üzerindeki durağan (depolanmış) veriler için CMK'nın 134. maddesi uygulanırken, akış halindeki

---

[1] Hukuka aykırı deliller ve bunların uzak etkisi (zehirli ağacın meyvesi öğretisi) hakkında ayrıntılı bilgi için bkz: **Murat Volkan Dülger**, Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi), Ankara, Seçkin Yayıncılık, 2014, s. 33 vd.

[2] Resmi Gazete, 1.6.2005, S. 25832.

(iletişim esnasındaki) veriler için telekomünikasyon araçları üzerindeki koruma tedbirlerini düzenleyen CMK'nın 135. maddesinin uygulanması gerekir[3].

2. Somut Delillere Dayanan Kuvvetli Şüphe Sebeplerinin Varlığı

7. CMK'nın 134. maddesinin 1. fıkrasında *"Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkanının bulunmaması halinde, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin haline getirilmesine karar verilir. Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hakim onayına sunulur. Hakim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hakim tarafından aksine karar verilmesi halinde çıkarılan kopyalar ve çözümü yapılan metinler derhal imha edilir"* denilmektedir[4].

8. Böylelikle daha önce 668 sayılı KHK[5] ile olağanüstü hal süresiyle sınırlı olmak üzere getirilen ve CMK'daki birçok koruma tedbiri için genel formül olan *"gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından"* karar verilebilmesi hali, olağan dönemler için de geçerli olmak üzere bu tedbir bakımından da getirilmiştir. Bu değişikliğin gerekçesinde, gecikmesinde sakınca bulunan hallerde 134. maddede belirtilen tedbirlere Cumhuriyet savcısı tarafından da karar verilebilmesine imkân sağlamak suretiyle, delillerin bir an önce elde edilebilmesi ve suçla etkin mücadele edilebilmesinin amaçlandığı belirtilmektedir. Savcının vereceği karar için yirmi dört saat içinde yargıç onayının gerekmesi bu konuda bir teminat oluşturmaktadır. Bu tedbire doğası gereği genellikle soruşturma aşamasında karar verileceğinden, denetim mercii de sulh ceza hakimlikleri olacaktır.

9. Maddede özellikle "şüphelinin kullandığı" ifadesine yer verilmiştir; zira üzerinde arama ve kopyalama işlemi yapılacak bilişim sisteminin şüpheliye ait olması gerekmez. Şüphelinin maliki olduğu, kiraladığı, ödünç aldığı ya da ortak kullanıma açık bir bilgisayarı eylemini gerçekleştirirken kullanması bu tedbirin uygulanması için yeterlidir. Ancak delile ulaşmak için sadece failin kullandığı bilişim sisteminde arama yapılması yeterli değildir. Bazı durumlarda failin kullandığı sistemle birlikte söz konusu kişilerin hatta yalnızca üçüncü kişilerin bilişim sistemlerinde bu tedbirin uygulanması gerekebilir. Yasanın bu durumu

---

[3] Bilişim sistemlerinde arama ve el koyma tedbiri hakkında ayrıntılı bilgi için bkz: **Olgun Değirmenci**, Ceza Muhakemesinde Sayısal (Dijital) Delil, Ankara, Seçkin Yayıncılık, 2014, s. 309 vd.; Telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenilmesi ve kayda alınması vb. tedbirler hakkında ayrıntılı açıklama için bkz: **Seydi Kaymaz**, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, 4. Bası, Ankara, Seçkin Yayıncılık, 2015, s. 25 vd.

[4] 25/7/2018 tarihli ve 7145 sayılı Kanunun 16'ncı maddesiyle, bu maddenin birinci fıkrasında yer alan *"Cumhuriyet savcısının istemi üzerine"* ibaresi *"hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından"* şeklinde değiştirilmiş, fıkrada yer alan *"hâkim tarafından"* ibaresi madde metninden çıkarılmış, ikinci fıkrasına *"bilgilere ulaşılamaması"* ibaresinden sonra gelmek üzere *"ya da işlemin uzun sürecek olması"* ibaresi eklenmiştir.

[5] 27/07/2016 tarihli ve 668 sayılı KHK'nin 3'üncü maddesinin birinci fıkrasının j bendine göre; 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun İkinci Kitap Dördüncü Kısım Dördüncü, Beşinci, Altıncı ve Yedinci Bölümünde tanımlanan suçlar, 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu kapsamına giren suçlar ve toplu işlenen suçlar bakımından, olağanüstü halin devamı süresince; Kanunun 134'üncü maddesi uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılacak arama, kopyalama ve elkoyma işlemlerine, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da karar verilebilir. Bu karar, beş gün içinde görevli hakimin onayına sunulur. Hakim, kararını elkoymadan itibaren on gün içinde açıklar; aksi halde elkoyma kendiliğinden kalkar. Kopyalama ve yedekleme işleminin uzun sürecek olması halinde bu araç ve gereçlere elkonulabilir. İşlemlerin tamamlanması üzerine elkonulan cihazlar gecikme olmaksızın iade edilir.

düzenlememiş olması bize göre önemli bir eksikliktir ve yapılacak bir düzenleme ile bu eksiklik giderilmelidir.

10. Bilişim sistemlerinde delil elde etmek için araştırma yapılabilmesi için öncelikle *"somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı"* ve *"başka surette delil elde etme imkanının bulunmaması"* gerekir. Somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı şartı bu maddenin ilk halinde bulunmamaktaydı. 21.2.2014 tarih ve 6526 sayılı "Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun"un 11. maddesiyle CMK'nın 134. maddesinde yapılan değişiklik ile bu ifade maddeye eklenmiştir[6].

11. Buna göre bilişim sistemlerinde arama (veya elkoyma) koruma tedbirinin uygulanabilmesi için öncelikle iki şartın birlikte bulunması gerekir. Bunlardan ilki yasa değişikliği ile fıkraya eklenen *"somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı"*dır.

12. CMK'da ya da öğretimizde *"somut delil – soyut delil"* ayrımı yapılmamıştır, mantıksal olarak böyle bir ayrımın yapılması da anlamsızdır. Delil, yargılama konusu olayı temsil etsin ve ister beyana, ister belgeye ister ise belirtiye dayansın somut bir olgudur; dolayısıyla bana göre maddede somut delil kavramı soyut delil kavramının karşıtı olarak kullanılmamıştır. Öte yandan Anglosakson hukuk sisteminde *"somut (gerçek) delil – ikrar delili"* ayrımı yapılmaktaysa da[7], ülkemizin de dahil olduğu Kıta Avrupası hukuk sisteminde böyle bir ayrım bulunmamaktadır. Nitekim ülkemiz ceza muhakemesi hukuku sisteminde yukarıda belirttiğim üzere ikrarı da kapsayan beyan delilleri, somut delil niteliğindedir. O halde bana göre geriye kalan tek seçenek, bu kavramın, ulaşılabilir, gerçekçi (rasyonel – akılcı) delillerin karşılığı olarak kullanılmasıdır. Ancak bunların ayrıca belirtilmesine gerek yoktur, zira bunlar zaten ceza muhakemesinde kullanılabilecek delillerin bir özelliği olup, delil kavramının içinde yer alırlar, zaten bu belirtilen özellikler olmaksızın bir beyan, belge ya da belirtinin delil olarak kabul edilmesi ve ceza muhakemesinde ispat aracı olarak kullanılması mümkün değildir.

13. Kuvvetli şüphe ise, genellikle koruma tedbirleri için bir ön şart olarak aranan şüphe türüdür. Örneğin CMK'nın 100. maddesinde tutuklama kararı verilebilmesi için *"kuvvetli suç şüphesinin varlığını gösteren olguların ... bulunması halinde, şüpheli veya sanık hakkında tutuklama kararı verilebilir"* denilerek bu tür bir şüphenin varlığı aranmıştır. Kuvvetli şüphe, şüphelinin/sanığın suçu işlediği konusunda, somut olaylarla desteklenmiş, dayanağı olan delille mahkûmiyet kararı verilebilmesinin kuvvetle muhtemel olduğu şüphedir. Yasaya göre failin yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe var ise, şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir (CMK m. 116). Eldeki delillerle yapılacak muhakeme sonucunda, sanığın mahkûm olması olasılığı, beraat etmesi olasılığından daha fazla ise "yeterli şüphe (delil)" söz konusudur. Kamu davasının açılabilmesi için "yeterli şüphe" aranmıştır (CMK m. 170/2)[8].

---

6 21.2.2014 tarihli ve 6526 sayılı Kanunun 11'inci maddesiyle, bu maddenin birinci fıkrasında yer alan "soruşturmada," ibaresinden sonra gelmek üzere "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve" ibaresi eklenmiş ve dördüncü fıkrasında yer alan "İstemesi halinde, bu" ibaresi "Üçüncü fıkraya göre alınan" şeklinde değiştirilmiştir.

7 Bu konuda bkz: **Kerri Mellifont**, Fruit of the Poisonous Tree – Evidence Derived from Illegaly or Improperly Obtained Evidence, Sydney, The Federation Press, 2010, s. 7, 8.

8 **Nur Centel/Hamide Zafer**, Ceza Muhakemesi Hukuku, 14. Bası, İstanbul, Beta Yayıncılık, 2017, s. 92.

İşte kuvvetli şüphe, bunların da üstünde, mahkumiyetin çok yüksek bir ihtimalle gerçekleşeceği durumlarda söz konusu olur. Dolayısıyla madde metnine yapılan ekleme ile inceleme konusu koruma tedbirinin uygulanması zorlaştırılmak istenmiştir. Bundan sonra söz konusu tedbir talep edilirken ve karar verilirken çok dikkatli ve titiz olunması gerekir. Aksi takdirde deliller hukuka aykırı olarak elde edilmiş olur ve ispat aracı olarak kullanılmaları mümkün olmaz.

3. Başka Surette Delil Elde Etme İmkanının Bulunmaması

14. Yukarıda da belirttiğim üzere, *"somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı"* inceleme konusu arama (ve elkoyma) tedbirine karar verilmesi için yeterli değildir. Bunun yanı sıra *"başka surette delil elde etme imkanının bulunmaması"* da gerekir. İki ifadenin arasında *"ve"* bağlacı bulunduğu için somut olayda tedbire karar verilmesi için her iki ön şartın birlikte bulunması gerekir.

15. Yürürlükte bulunan hukuk açısından bu şartlar gerçekleşmeden karar verilmesi hukuka aykırıdır ve bu şekilde verilen karar neticesinde elde edilen deliller de *"hukuka aykırı delil"*dir ve Anayasa m. 38 ve CMK m. 217/2 gereğince hükme esas alınmaları mümkün değildir.

16. Somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ile başka surette delil elde etme imkanının neden bulunmadığı ve bu nedenlerle bu yola başvurulduğu hem savcılığın kararında hem de hakimin onayında açık ve gerekçeli bir şekilde belirtilmelidir. Ancak şu ana kadarki uygulamada, bazı istisnalar dışında, buna hemen hemen hiç uyulmadığı, yalnızca "yasa maddesi tekrar edilerek" karar verildiği görülmektedir. *Dolayısıyla verilen kararların büyük çoğunluğu hukuka aykırıdır.* Beklentim bu konuda hassasiyet gösterilmesi, kararların ve onayların yasanın şartlarını karşılar şekilde gerekçelendirilmesidir.

17. Ayrıca ön koşul niteliğindeki *"başka surette delil elde etme imkanının bulunmaması"* halinin soruşturma evresinin hangi aşamasında belirleneceği de belli değildir. Ancak 134. maddenin normatif yapısı gereği, soruşturmaya konu yapılan suçla ilgili olarak belirli bir delil araştırmasının yapılmış olması, bu araştırmanın sonucunda bir delil elde edilememiş olması ve bunun da açıkça tutanağa bağlanması gerekir.

18. Olması gereken hukuk açısından ise bana göre bu şartın aranması özellikle bilişim suçları ve bilişim sistemleri aracılığıyla işlenmiş suçlar için yapılacak soruşturmalar açısından son derece hatalıdır. Zira bilişim sistemlerine karşı ya da bilişim sistemleri aracılığıyla işlenen suçlarda yapılması gereken ilk iş, sistemin yapısı ve veri bütünlüğü bozulmadan içindeki verilerin ve bağlantılarının tespit edilmesidir. Bu suçlar hakkında yapılan soruşturmalarda genellikle başka şekilde delil elde etme imkânı da bulunmamaktadır. Başka şekilde delil elde etmeye çalışıldıktan sonra en son çare olarak bilişim sistemlerinde araştırma yapılmaya girişildiğinde ise çok geç kalınmış olacak faillere ve delillere ulaşmak son derece güçleşecektir. *Nitekim bu maddenin sanki böyle bir şart yokmuş gibi uygulanmasının altında yatan gerekçe de budur*. Ancak ifade etmeliyim ki, teknolojinin ve dijital çözümlerin hayatımızın her alanına girmesi nedeniyle artık klasik olarak adlandırdığımız suçların da pek çoğunun aydınlatılmasında dijital materyallere başvurulması bir zorunluluktur. Dolayısıyla yukarıda bilişim suçları açısından söylemiş olduğum hususlar pek çok olayda klasik suçlar açısından da geçerlidir.

20. Bu görüşüme karşın, her suç soruşturması için ilk olarak bilişim sistemlerinde arama ve elkoyma koruma tedbirinin uygulanması halinde kişisel verilerin güvenliğinin ve özel hayatın gizliliğinin kalmayacağı şeklinde içinde haklılık payı olan bir karşı görüş de ileri sürülebilir. Ancak bu eleştirinin de CMK'nın 134. maddesiyle eklenen *"somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı"* şartının gerçek anlamda uygulanması suretiyle karşılanması mümkündür.

21. Ancak bilişim suçu soruşturmalarının gerektirdiği hız dikkate alınarak, 134. maddenin 1. fıkrasına getirilecek bir istisna hükmüyle, *"TCK'nın bilişim alanında suçlar bölümünde ve 135, 136, 138, 142/2-e 158/1-f maddelerinde yer alan suçlar için başka surette delil elde etme imkanının bulunmaması şartı aranmaz"* denilmek suretiyle kısmen hatalı olan norm ve yanlış uygulama düzeltilebilir. Ancak bugünkü haliyle hem madde düzenlemesi hatalıdır, hem de uygulama ve bu yöntemle elde edilen deliller hukuka aykırıdır.

22. Madde metninde *"bilgisayar, bilgisayar programları ve bilgisayar kütükleri"* terimleri yerine kısaca *"bilişim sistemi"* denmesi yeterli olurdu. Maalesef TCK'da günümüze uygun bir terminoloji kullanılması rağmen CMK'da aynı yöntem izlenmemiştir. Bilgisayar kütüğü terimiyle ifade edilmeye çalışılan, sabit, taşınabilir ya da bulut formunda her türlü veri taşımaya ve depolamaya yarayan araçlar ya da sistemlerdir.

4. Arama ve Kopyalama Tedbiri

23. 134. maddenin 1. fıkrasının metninde açıkça anlaşıldığı üzere bu tedbir kural olarak; şüphelinin kullandığı bilişim sistemlerinde arama yapılması, sistemdeki verilerin kopyasının çıkarılması ve kayıtların çözümünün yapılarak metin haline getirilmesini içerir. Yani kural olan *arama tedbiridir*; şüphelinin kullandığı bilişim sistemi olduğu yerde bırakılacak ve kopyalama işlemi sistemin bulunduğu yerde yapılacaktır. Ayrıca kolluk güçleri sistemin ya da veri taşıma aracının aslını almayacaktır. Kural olan budur ve öncelikle bu tedbirlerin uygulanması gerekir!

24. CMK'nın ilk halinde, şüphelinin veya müdafiin talebi halinde alınan yedeklemelerin bir kopyasının talepte bulunana verileceği düzenlenmişti. Ben de, kitabın önceki basılarında bu hususun talebe bırakılmış olmasına rağmen, uygulamada delilin sağlamlığının kontrol edilebilmesi için bu yedeğin mutlaka talep edilmesini önermiş idim.

25. Yasa koyucu, öğreti ve uygulamadan gelen bu ve benzer eleştirileri dikkate almış olacak ki, 21.2.2014 tarih ve 6526 sayılı Yasanın 11. maddesiyle CMK'nın 134. maddesinde değişiklik yaparak[9], 4. fıkrada yer alan "istenmesi halinde" ifadesinin çıkartarak yerine "Üçüncü fıkraya göre alınan" ifadesini getirmiştir. Böylelikle arama tedbiri sonucu çıkartılan yedeğin bir kopyasının şüpheli veya müdafine verilmesi isteğe bağlı olmaktan çıkartılmış ve zorunlu hale getirilmiştir. Bu değişikliği olumlu karşılıyorum, ancak bazı hallerde bunun olumsuz sonuçlarının da bulunduğu açıktır, bu konuya aşağıda ayrıca değineceğim.

5. Elkoyma Tedbiri

26. 134. maddenin 2. fıkrasında ise 1. fıkranın istisnası olarak el koyma tedbiri düzenlenmiştir. Buna göre *"Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun*

[9] RG., 6.3.2014, 28933.

sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir."[10]

27. Bu fıkra çok açık biçimde bir istisnayı düzenlemesine rağmen, ülkemiz mevzuatında yer alan pek çok istisna hükmünün uygulamada kural haline getirilmesinde olduğu gibi, bilişim sistemlerinde yapılan aramalarda "el koyma tedbirinin uygulanması" kural haline getirilmiştir. Kolluk güçleri CMK'nın 134. maddesine göre yaptıkları aramaların tamamında 2. fıkradaki istisna hükmünü işletmekte, bunun için arama yapacakları bilişim sisteminde şifre olduğuna ilişkin işleme katılan diğer kolluk güçleriyle birlikte bir tutanak tutmakta ve böylelikle yasayı dolanmak suretiyle görünüşte de olsa yasaya uygun davrandıkları düşüncesiyle görevlerini yerine getirmektedirler. Bunun gerekçesi olarak ise *"yeterli personellerinin olmadığını, eğer sistemin olduğu yerde arama ve kopyalama yapmaya kalkarlarsa hiçbir işi yetiştirmeyeceklerini"* beyan etmektedirler. Aslında içinde büyük oranda gerçeklik payı olan bu bahane yasa maddesini değiştirme hakkını vermediği gibi bu şekilde elde edilen delili de hukuka uygun hale getirmemektedir. Zira tutulan tutanaklarda ne tür bir şifrenin ya da gizli verinin bulunduğu, bunun işin uzmanı olan bilişim polisi tarafından neden etkisiz kılınamadığına ilişkin herhangi bir kayıt ya da son yapılan eklemeyle getirilen neden işlemin uzun süreceğine ilişkin bir bilgi, yer almamaktadır. Dolayısıyla bu tutanağın gerçekle bir ilgisi ve denetlenebilir bir tarafı olmadığı gibi, hukuken hiçbir değeri de bulunmamaktadır. Bu işlem açıkça yasanın arkasına dolanmaktadır ve hukuka aykırıdır. Söz konusu işlemin yapılış şekli hukuka aykırı bir delil elde etme yöntemi olduğu gibi bu yolla elde edilen deliller de yasak delil niteliğindedir ve yargılamanın hiçbir aşamasında kullanılmamaları gerekir.

28. 134. maddenin 3. fıkrasında *"Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır."* denilmek suretiyle 2. fıkradaki istisna hükmünün uygulanması halinde yapılması gerekenlere yer verilmiştir. Bununla bağlantılı olarak 4. fıkrasında 6526 sayılı Yasa ile değişiklik yapılarak *"Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır."* denilmek suretiyle el koyma tedbirinin uygulanması halinde çıkarılan yedeğin bir kopyasının şüpheliye veya müdafiine verilmesi bir zorunluluk halinde getirilmiştir. Bu değişikliği genel anlamda olumlu bulmakla birlikte, sakıncalı ve dolayısıyla olumsuz yönlerinin bulunduğunu da belirtmeliyim. Özellikle çocuk pornografisi ve kredi kartı bilgileri gibi başkalarına ait kişisel verilerin ya da terör örgütüne ait bilgi ve belgelerin bulunduğu bir depolama aygıtının imajının bir örneğinin şüpheliye verilmesi yeni suçların işlenmesinin önünü açabilecek niteliktedir. Maddede bunlar açısından bir istisna getirilmemesi bana göre bir eksikliktir. Uygulamada ise bu tür içeriklerin bulunması halinde CMK'nın 123. maddesinde düzenlenen suç eşyasına el koyma tedbiri gereğince el konulmakta ve şüpheli ve/veya müdafiine verilmemektedir. Bana göre burada bir ayrım yapılmalı, müdafi görevini yerine getiren avukatın suç işlemeyeceği ve sır saklama yükümlülüğü düşüncesinden hareketle, bu görevi yapanlara imajın yedeği verilebilir ve sınırlama yalnızca şüphelinin kendisiyle sınırlı

---

[10] 25/7/2018 tarihli ve 7145 sayılı Kanunun 16'ncı maddesiyle, bu maddenin birinci fıkrasında yer alan *"Cumhuriyet savcısının istemi üzerine"* ibaresi *"hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından"* şeklinde değiştirilmiş, fıkrada yer alan *"hâkim tarafından"* ibaresi madde metninden çıkarılmış, ikinci fıkrasına *"bilgilere ulaşılamaması"* ibaresinden sonra gelmek üzere *"ya da işlemin uzun sürecek olması"* ibaresi eklenmiştir.

tutulabilir. Böylelikle hem yeni suçların işlenmesinin önüne geçilmiş hem de delilin doğruluğunun teyit edilmesi sağlanmış olur. Ancak ülkemizin gerçekleri karşısında bu çözümün ne kadar doğru olacağı tartışmalıdır.

29. Düzenlemeler bu şekilde olmakla birlikte uygulama böyle olmamaktadır. Kolluk güçleri bilişim sistemleri üzerinde arama, kopyalama ve elkoyma tedbiri için bilişim sisteminin bulunduğu yere gittiklerinde yukarıda da belirttiğim üzere yasayı dolanarak doğrudan elkoyma tedbirini uygulamakta ve yedek alma işlemini de kendi çalıştıkları merkezlerde yapmaktadırlar. Yedekleme için gerekli olan veri depolama araçlarını da şüpheliden istemektedirler. Bu uygulama tamamen hukuka aykırıdır. Çünkü el koyma koruma tedbiri uygulandığında yedekleme soruşturmanın güvenilirliği, tarafsızlığı ve adil yargılanma hakkına uygunluğu açısından son derece önem taşımaktadır. Şöyle ki:

30. Üzerinde tedbir uygulanan bilişim sisteminin sabit diski ya da veri taşıma aracı örneğin 320 GB veri taşıma kapasitesine sahiptir. Ancak bunun tamamı hiçbir zaman kullanılmamaktadır. Örneğin; bu diskte 100 GB veri olduğunu kabul ettiğimizde geri kalan 220 GB boştur. Yalnızca veri bulunan kısımlar yedeklendiğinde boş kalan 220 GB'lık kısma daha sonra başka verilerin yazılması mümkündür. Dolayısıyla dolu ve boş kısımlarıyla tüm diskin olduğu gibi yedeklenmesi teknik tabiriyle *"imajının alınması"* ve bunun sonucunda HASH değerinin alınması yani işlem yapıldıktan sonra diskin bir nevi mühürlenmesi gerekir. İşlemlerin şüpheli ve müdafi önünde yapılmaması halinde, imaj alınmadan önce veri yerleştirildiği ve daha sonra imaj alındığı şüphesi ve iddiaları daima söz konusu olacaktır. Bu durum doğru ve adilane yürütülen soruşturmaların da güvenilirliğini etkileyecektir. Oysa adil yargılanma hakkının ihlal edilmemesi için hem görünüşte hem de içerikte tüm soruşturma ve yargılama işlemlerinin tarafsız ve hukuka uygun şekilde yerine getirilmesi gerekir. Ayrıca bilişim sistemleri üzerinde yapılan adli bilişim incelemeleri daima bu yedekler üzerinde yapılmaktadır; delilin aslının saklanması ve ileride söz konusu olabilecek itirazlarda incelenmek üzere bozulmamış halde muhafazası için aslı üzerinde hiçbir işlem yapılmaması gerekir. Uygulamada ise bilişim sistemleri kolluk güçleri tarafından yasa maddesi dolanılmak suretiyle olduğu yerden alınarak kolluk merkezlerine götürülmekte, yedekleme ve HASH değerlerinin alınması şüpheli ve/veya müdafiinin olmadığı ortamda yapılmaktadır. *Bu uygulama kesinlikle hukuka aykırıdır!* Bu yöntemle delil elde edilmesi hukuka aykırı olduğu gibi, elde edilen deliller de yasak delildir; kullanılması ve hükme esas alınması mümkün değildir. Ne yazık ki; bugün ülkemizde yürütülen "kamuoyunda en çok yer alan soruşturma ve kovuşturmalar da dahil olmak üzere" davaların hemen hepsinde bu tür deliller kullanılmakta ve adil yargılanma hakkı ihlal edilmektedir.

31. 134. maddenin son fıkrasında ise *"Bilgisayar ve bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kağıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır."* denilmek suretiyle yukarıdaki düzenlemelerle çelişki yaratan bir fıkraya yer verilmiştir. Çünkü yukarıda belirttiğimiz üzere bilişim sistemlerinden delil elde edilmesinde kural, bilişim sisteminin olduğu yerde arama yapılması ve sistem verilerinin kopyalanmasıdır; el koyma ise istisnadır. Oysa bu fıkradaki düzenlemede sanki el koyma kural, bu tedbir uygulanmadan sistemin olduğu yerde kopyasının alınması ise istisna imiş gibi bir anlam

çıkmaktadır. Dolayısıyla bu fıkra, gereksiz yere maddede yer alan ve anlam karışıklığına yol açan bir düzenlemedir.

6. CMK m. 134 Özel Bir Düzenlemedir

32. CMK'nın 116. ve 123. maddelerindeki genel nitelikteki arama hükümlerine rağmen 134. maddeye yer verilmesi bunun özel nitelikte bir düzenleme olduğunu göstermektedir. Dolayısıyla 116. maddeye dayanılarak şüphelinin işyeri ya da konutunda yapılan bir arama sırasında ayrıca 134. maddeye göre arama yapılmasına ilişkin bir karar alınmamışsa, şüphelinin kullandığı bilgisayarlar üzerinde arama yapılması mümkün değildir. 116. maddeye dayanılarak yapılan aramada şüphelinin üzerinden çıkan cep bilgisayarında arama yapılması için dahi 134. maddeye göre karar alınması gerekir. Buna uyulmaksızın yapılan aramalar hukuka aykırı yöntemle delil elde etmektir ve elde edilen delil de yasak delil niteliğindedir.

7. Uygulamadaki Eleştiriler ve Uygulanan Yöntem

33. Dikkat edilirse ne CMK'nın 134. maddesinde ne de yönetmelikte "imaj alma"dan ya da "HASH değeri"nden bahsedilmemektedir. Bunun yerine "yedek alma" ve "kopyalama" terimleri kullanılmaktadır. Oysa yukarıda açıkladığımız üzere, bir veri taşıma aracının yedeğinin ya da kopyasının alınması ile imajının alınması ve bunun sonucunda hash değerinin elde edilmesi çok farklı işlemlerdir. Yedekleme ve kopyalamada boş sektörler kopyalanmadığı gibi, veri bütünlüğü ve güvenliği de sağlanamaz. Bu ise dijital verilerin "güvenilir delil" olma özelliğini ortadan kaldırır. Bu yöntemlerin CMK'da ve yönetmelikte düzenlenmemesi büyük bir eksikliktir.

34. Uygulamada ise soruşturma görevlileri "tamamen kendi iyi niyetleri ve görevi düzgün yapma istekleriyle", bu alandaki uluslararası standartları takip ederek her soruşturmada imaj ve hash değerini almaktadırlar. Ancak bu işlemi yapmasalar, kendilerine neden bu standardı kullanmadıklarını sorgulayacak bir yasal dayanak mevzuatımızda bulunmamaktadır. Bu büyük eksikliğin bir an önce hem CMK'da hem de yönetmelikte yapılacak değişiklikler ile giderilmesi gerekir.

35. Yukarıda da belirttiğim üzere soruşturma görevlilerine yapılan önemli bir eleştiri, arama (imaj alma) işleminin veri taşıma aracının bulunduğu yerde değil, el koyma tedbiri uygulanmak suretiyle soruşturma görevlilerinin bulunduğu merkezde yapılması, istisna olan el koyma tedbirinin kural haline getirilmesidir. Söz konusu görevliler bunun gerekçesi olarak haklılık payı olan bazı gerekçeler ileri sürmekte ve çözüm yolları da üretip uygulamaktadırlar. Söz konusu gerekçelerden bazıları şunlardır:

a. Yeterli sayıda ve nitelikte adli bilişim uzmanı ve olay yeri inceleme ekibinin bulunmaması,

b. Çoğunlukla şifrelerin çözülmesinin ya da gizlenmiş verilerin bulunmasının uzun zaman ve özel ekipman gerektirmesi,

c. Uzun zaman alan arama faaliyeti sırasında, üzerinde arama yapılan bilişim sisteminin bulunduğu, ev ya da iş yerinde bulunan kişilere rahatsızlık verilmesi ya da bu yerlerin çalışmaya uygun ve/veya hijyenik olmaması,

d. Bilişim sisteminin imajının alınacağı yerde, veri bütünlüğünün sağlanması için kesintisiz güç kaynağının bulunmaması, özellikle veri kurtarma yapılması gereken durumlarda toz olmayan ve özel ekipmanların bulunduğu ortamlarda bu işlemlerin yapılması gerekliliği.

36. Bu listeyi daha uzatmak mümkündür ve bunlarda haklılık payının olduğu da bir gerçektir. Soruşturma görevlileri, hem yukarıda anılan olumsuzluklardan kurtulmak hem de delillerin hukuka aykırı olarak elde edildiği –haklı– itirazını engellemek için şu şekilde bir yöntem uygulamaktadırlar:

37. CMK'nın 134. maddesine göre arama ve el koyma tedbirinin uygulanmasına ilişkin kararı aldıktan sonra, tedbirin uygulanacağı yere gitmekte ve şüphelinin kullandığı tüm veri taşıyabilen araçları usulünce fişten çektikten sonra bunları özel yapılmış torbalara koymakta ve ağzını mühürlemektedirler. Bu esnada yapılan tüm işlemleri tutanağa bağlamaktadırlar. Merkeze götürülen bu araçlar üzerinde inceleme yapılacağı zaman duruma göre şüpheli ve/veya müdafii incelemenin yapılacağı merkeze çağrılmakta ve bu işlem için hazırlanmış özel yere alınmaktadırlar. Adli bilişim uzmanları tozdan arındırılmış özel yerlerinde araçlar üzerinde inceleme yaparlarken, buraya yerleştirilmiş kameralar sayesinde, şüpheli ve/veya müdafii kendilerine ayrılan yerde kameralardan aktarılan bu görüntüleri monitörlerden canlı olarak izlemektedirler. Böylelikle bir yandan araçların olduğu yerde inceleme zorunluluğundan kurtulup kendi laboratuvarlarında inceleme yaparlarken, bir yandan da verilere müdahale edildiği ve hukuka aykırı delil elde edildiği itirazından kurtulmaya çalışmaktadırlar.

38. Bu sadece soruşturma görevlilerinin oluşturduğu ve uyguladığı bir yöntemdir. Bunun bir benzerinin ya da daha gelişmişinin bir an önce yasal bir zemine oturtulması ve uygulamaya geçirilmesi gerekir. Aksi takdirde ülkemizde hem "hukuka aykırı delil" elde edilmeye devam edilecek, hem de bilişim suçları ve bilişim sistemleri aracılığıyla işlenen suçlar hakkında "olması gerektiği şekilde" soruşturma yapılamayacaktır.

B. Soruşturma ve Kovuşturmada Mevzuat Kaynaklı Yenilikler ve Eksiklikler

1. ASSS'nin İç Hukukumuzun Parçası Haline Gelmesi

39. Yukarıda da belirttiğimiz üzere ASSS'nin onaylanması uygun bulunarak Resmi Gazete'de yayınlanmış ve iç hukukumuzun bir parçası haline gelmiştir. Sözleşmenin "Usul Hukuku" başlıklı II. Kısmının 14-22. maddeleri arasında soruşturma ve kovuşturmayı kolaylaştıracak tedbirler, "Uluslararası İşbirliği" başlıklı 23-35. maddelerinde arasında soruşturma ve kovuşturmaları kolaylaştıran ve hızlandıran işbirliği kuralları düzenlenmiştir[11].

40. Bu hükümlerin ülkemizde de artık işler hale gelmesi sebebiyle, bugüne kadar aydınlatılamayan ya da delillendirilemeyen pek çok soruşturma ve kovuşturmanın kısa sürede ve olumlu şekilde sonuçlanacağını düşünüyorum. Ancak ASSS'de yer alan soruşturma tedbirlerinin ülkemiz iç hukukuna aktarılması gerekir; çünkü bu sözleşmenin doğrudan uygulanma özeliği yoktur, bu aktarma ise henüz gerçekleştirilmemiştir. CMK'nın 134 ve 135. maddelerinde yer alan tedbirler ise ASSS'de

[11] Sözleşmenin çevirisi için bkz: **Murat Volkan Dülger**, Bilişim, Kişisel Verilerin Korunması ve İnternet İletişimi Mevzuatı, 6. Bası, Ankara, Seçkin Yayıncılık, 2020, s. 33 vd.

yer alan tedbirleri tam olarak karşılamamaktadır. Dolayısıyla bu Sözleşme'ye taraf olmakla uluslararası yükümlülüklerden kaynaklanan zorunluluktan dahi olsa bu değişiklerin yapılması gerekir. Ancak bu konuda henüz bir talep bulunmamaktadır.

41. Öte yandan Sözleşmenin imzaya açıldığı tarih 2001 olup üzerinden oldukça uzun bir süre geçmiştir. Bu süre bilişim hukuku açısından daha da uzun bir süredir. Bilişim alanında yeni teknolojiler, gelişmeler, fırsatlar, çözümler ve suç işleme modelleri ortaya çıkmıştır. Buna bağlı olarak, bu yeniliklere karşı veya bunlar vasıtasıyla işlenen suçları soruşturmak için de yeni adli bilişim ve soruşturma teknikleri söz konusu olmaktadır. Dolayısıyla CMK ve ilgili yönetmeliklerde değişiklik yapılacağı zaman yalnızca ASSS'nin hükümleriyle sınırlı kalınmamalı bu konudaki güncel gelişmeler de takip edilerek mevzuata yansıtılmalıdır[12].

2. 5651 sayılı Yasanın 3/4. Maddesi ile Soruşturma Açısından Getirilen Değişiklik ve AYM'nin 4. Fıkrayı İptalinden Sonraki Durum

42. 5651 sayılı Yasanın 3. maddesine, 26.2.2014 tarihli ve 6527 sayılı Yasanın 16. maddesi ile eklenen 4. fıkra gereğince *"Trafik bilgisi ancak bir suç soruşturması kapsamında mahkemelerce talep edilmesi halinde Başkanlık tarafından içerik sağlayıcı, yer sağlayıcı ve/veya erişim sağlayıcıdan alınarak verilir"*.

43. Bu fıkra ekleninceye kadarki uygulamada, soruşturmayı yürüten savcılar doğrudan TİB'den (şimdi ise BTK) bu bilgileri istemekteydiler. Hatta TİB bunun için soruşturma görevlilerinin kullanması için bir panel açmıştı ve söz konusu bilgiler bu panel üzerinden rahatlıkla elde edilebilmekteydi.

44. Bu yöntem bilişim suçu soruşturmasında gerekli olan "hızı" sağlamakla birlikte, maalesef ülkemizde yaygın olan kötüye kullanımları da teşvik etmekteydi. İşte yasa koyucu bu kötüye kullanımları önlemek amacıyla hızlı hareket etmeyi ikinci plana itmiş ve bu bilgilerin ister soruşturma ister kovuşturma sırasında ancak bir mahkeme kararı ile TİB'den istenebileceğini, TİB'in de ancak hakim kararına dayanarak söz konusu bilgileri verebileceğini düzenlemiştir. Yapılan bu düzenlemenin haklılığı zaman içinde ortaya çıkmışsa da, karar verenlerin birçoğunun da örgütsel bağlantısı bu düzenlemenin de boşa çıkmasını sağlamıştır.

45. Bu düzenlemeden sonra soruşturma görevlilerinin ya da savcılığın doğrudan TİB'den bu bilgileri alması halinde bunlar hukuka aykırı delil olacak ve muhakemede kullanılmaları mümkün olmayacaktır. Öte yandan mahkeme kararı olmadan bu bilgilerin talep edilip kullanılması ve verilmesi ilgilileri açısından TCK'nın ilgili hükümleri gereğince suç oluşturacaktır.

46. Ancak söz konusu düzenleme Anayasa Mahkemesi'nin, 1.1.2015 tarih ve 29223 sayılı R.G.'de yayımlanan, 2.10.2014 tarihli, 2014/149 E. ve 2014/151 K. sayılı kararı ile iptal edilmiştir. AYM'nin iptal kararından sonra bu konuda bir yasal boşluk oluşmuştur. Zira iptal üzerine değişiklikten önceki düzenlemenin ihya olması yani yeniden yürürlük kazanması mümkün değildir. Dolayısıyla boşluk oluşmuş ve hiçbir düzenlemenin

---

[12] ASSS'nin de yer alan koruma tedbileri, bu tedbirlerin Türk Hukukundaki karşılıkları ve karşılaştırması hakkında ayrıntılı bir inceleme için bkz: **Yavuz Erdoğan**, Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbileri Ve Bu Tedbirlerin Türk Hukukundaki Yeri, İstanbul, Legal Yayıncılık, 2018, s. 92 vd.

olmadığı ilk hale dönülmüştür. Bu durumda mahkemelerin ve savcılıkların yargılamaya veya soruşturmaya ilişkin taleplerinin herkes tarafından karşılanması yasal bir zorunluluk olduğundan artık mahkemelerin ve savcılıkların bu bilgileri ilgili kurumlardan bir hakim ya da mahkeme kararı olmaksızın doğrudan istemeleri mümkündür. Kovuşturma ya da soruşturma aşamasında mahkemelerin ya da hakimlerin bir kararla bunları istemesinde bir sorun bulunmamakla beraber, soruşturma aşamasında kolluk güçlerinin ya da savcılık makamının bir hakim kararı olmaksızın bu önemli verilere ulaşması sorun yaratabilecek niteliktedir. Sorunun çözümü AYM'nin iptal kararındaki gerekçeleri de dikkate alınarak en kısa zamanda yapılacak bir düzenleme ile söz konusu boşluğun giderilmesidir.

3. CMK m. 134'e Göre Alınan İmajların Muhakeme Sonucunda Ne Yapılacağına İlişkin Belirsizlik Giderilmelidir

47. Uygulamada karşılaştığım ve tarafıma soru olarak yöneltilen önemli bir sorun da CMK m.134'e göre alınan imajların muhakeme sonucunda ne yapılacağıdır. Öncelikle ifade etmeliyim ki burada "muhakeme sonu" ile kastım soruşturma sonucunda verilen kovuşturmaya yer olmadığı (takipsizlik) kararı, ilk derece mahkemesince verilen kararlar ya da denetim muhakemesi (istinaf ve/veya temyiz) sonucu verilen kesinleşmiş kararlardır.

48. Üzerinde arama ve el koyma tedbirine karar verilen dijital veri taşıyıcıların, failin mahkumiyeti halinde bu kararla birlikte iadesine ya da suç unsuru barındırması halinde TCK m. 54 gereğince bir güvenlik tedbiri olarak müsaderesine karar verilebilir. Kovuşturmaya yer olmadığına ve beraat halinde de şüpheliye/sanığa iadesine karar verilebilir. Burada kastettiğim ise, arama ve/veya el koyma neticesinde bu dijital veri taşıyıcılardan alınan imajların ne olacağı sorunudur. İşte bunlarla ilgili yürürlükteki mevzuatımızda bu delillerin ne yapılacağına ilişkin açık bir düzenleme bulunmamaktadır.

49. Bazı mahkemeler ya da savcılıklar bu verileri elinde bulunduran adli emanete ya da emniyet birimlerine bunların imha edilmesine ilişkin karar ya da emir gönderdikleri bilinmektedir. Ancak iyi niyetle yapılan bu uygulamaların hukuka aykırı olduğunu düşünmekteyim.

50. Söz konusu imajların CMK m.134'e göre bir ceza muhakemesi koruma tedbiri neticesinde alındıkları açıktır. Ceza muhakemesi koruma tedbirleri ise temel hak ve özgürlüklere ilişkin düzenlemeler olup Anayasanın 13. maddesine göre bunların sınırlanması ancak yasa ile olur. Nasıl ki imajların alınması temel hak ve özgürlüklerin kısıtlanması ile oluyorsa bunların imhası da adil yargılanma hakkı gibi temel hak ve özgürlüklerin kısıtlanmasına yol açabilir. Dolayısıyla bunların imhası da ne zaman, nerede, kim ya da kimler tarafından ve ne şekilde yapılacağını detaylı bir şekilde gösteren bir yasal düzenleme ile olmalıdır. Yasal bir düzenleme olmadan mahkeme kararı ya da savcılık emriyle bunun yapılması Anayasanın 13. maddesinin ve TCK'nın 257. maddesinin ihlali anlamına gelir.

51 Bu imajların sonsuza kadar adli emanette ya da ilgili kolluk birimlerinde tutulması da gerçekçi değildir. Zira bunun için ne yer ne de gereklilik vardır. Ancak imhaları için de düzenleme olmadığı için bu konuda yasal boşluk bulunmaktadır. O halde yukarıda

belirttiğim üzere bu konuda CMK'nın 134. maddesine eklenecek bir ek fıkra ile düzenleme yapılarak söz konusu imajların ana hatlarıyla nasıl imha edileceği düzenlenmeli, teknik ayrıntılar da yönetmelikle açıklığa kavuşturulmalıdır.

4. CMK m. 135'te Bilişim Suçlarının Belirtilmemesi Soruşturmaların Eksikliğine veya Hukuk Aykırı Delil Elde Edilmesine Yol Açmaktadır

52. Soruşturma görevlileri tarafından CMK'nın 134. maddesine dayalı olarak arama tedbiri uygulandığında, eğer arama esnasında açık bilişim sistemleri var ise, bunlar kapatılmaksızın "canlı" haldeyken incelenmektedirler. Zira sistem kapatıldığında uçucu bellekteki veriler silinebilmekte, monitörde görüntülenen veriler kaybolmakta ve o anda üçüncü kişilerle yapılan iletişim de sonlandırılmaktadır. Bu ise soruşturmanın amacı açısından istenilen bir durum değildir.

53. Bilindiği üzere, bilişim sistemleri veri depolama ve işlemeye yaradıkları gibi anlık iletişim kurmayı da sağlayan araçlardır. Bunun için skype, messenger, ChatOn ya da WhatsApp gibi sayısız yazılım geliştirilmiş ve geliştirilmektedir. Hatta bugün kullandığımız cep telefonlarının çoğu hem bir bilişim sistemi hem de iletişim aracıdır. Dolayısıyla bu cihazlar ya da yazılımlar üzerinde arama ve el koyma tedbirinin hukuka uygun şekilde uygulanabilmesi için hem CMK'nın 134. maddesi hem de 135. maddesi gereğince karar alınması gerekir. Oysa 135. maddede sayılan, haklarında iletişimin tespiti kararı verilebilecek katalog suçlar arasında "bilişim suçları" bulunmamaktadır.

54. CMK'nın 135. maddesinde 21.2.2014 tarihli ve 6526 sayılı Yasanın 12. maddesiyle değişiklik yapılana kadar maddenin 8. fıkrasında *"Suç işlemek amacıyla örgüt kurma (iki, yedi ve sekizinci fıkralar hariç, madde 220)"* ifadesi bulunmakta ve buna dayanılarak bilişim suçlarının örgüt çerçevesinde işlendiği varsayılmak suretiyle adeta yasa dolanılarak iletişimin tespiti kararı alınmakta idi. Yasa koyucu iletişimin tespiti, dinlenmesi ve kayda alınması tedbirinin kötüye kullanımlarının çok artması, bunların basına ve sosyal medyaya düşmesi ve politik yaşamı ve seçimleri etkilemeye çalışması üzerine, bu tedbirin alınmasını zorlaştırmak amacıyla maddede değişikliğe gitmiş ve bu değişiklikler çerçevesinde yasayı dolanmak için sıklıkla kötüye kullanılan 8. fıkrayı da yürürlükten kaldırmıştır. Ancak (asla olmaması gerektiği halde) politik nedenlerle yapıldığını düşündüğüm bu düzenlemeden dönülmüş ve 24.11.2016 tarihli ve 6763 sayılı Yasanın 26. Maddesiyle "Suç işlemek amacıyla örgüt" düzenlemesi getirilmiştir. Ancak bu düzenlemenin olması durumu hukuka uygun hale getirmemektedir. Hala bilişim suçları katalog suçlar içinde yer almamakta ve örgüt çerçevesinde işlendikleri gerekçesiyle zaman zaman yasa dolanılarak bu koruma tedbirine konu olmaktadırlar.

55. Ancak bilişim sistemlerinin yapısı gereği bunlar üzerinde arama ve elkoyma tedbiri uygulandığında ister istemez iletişimin tespiti ve kayda alınması da söz konusu olmaktadır. Bu işlem yapılmadığında bilişim suçlarının ve suçlularının tespiti ve faillerin yakalanması çok zorlaşmaktadır, bu yapıldığında ise CMK'nın 135. maddesindeki katalog suçlar arasında bilişim suçları bulunmadığından elde edilenler hukuka aykırı delil olacak ve muhakemede kullanılamayacaktır. Dolayısıyla bu alandaki yasal boşluğun giderilmesi amacıyla acilen CMK'nın 135. maddesine TCK'nın 243, 244 ve 245. ve 158/1-f maddesindeki suçlar eklenmelidir.

C. IP Numarası Tek Başına Faili Göstermez

56. Öncelikle IP'nin ne olduğuna kısaca değinmek istiyorum. IP adresi, internete bağlanmak isteyen bilgisayarlara internet servis sağlayıcıları tarafından atanan kimlik numarasıdır. Dolayısıyla IP adresi, bilgisayarın internet ortamında birbirleriyle iletişim kurmaları için bağlantı sağlamaktadır. Bunlar 0 ile 255 sayıları arasında değişen, genellikle noktalı onluk (desimal) formatta gösterilen 32 bitlik adreslerdir. Örneğin, 155.212.56.73. Şu an *"Internet Protocol Version 4 (IPv4) Standard"* denilen bir standart kullanılmaktadır. Bu standart ile yaklaşık dört milyar IP adresi kullanılabilmektedir. Ancak nüfusun artması, teknolojinin ilerlemesi ve her türlü elektronik eşyanın internete girmesi için olmazsa olmaz olan IP adreslerin adedinde sıkıntı yaşanıldığından IPv6 standardı üzerinde çalışılmaktadır. Bu standardın gerçekleşmesi halinde, kullanılabilir 16 milyar adet IP adresi olacaktır[13].

57. IP adresleri, dinamik ve statik olmak üzere ikiye ayrılır. İnternet servis sağlayıcı tarafından internete bağlanmak isteyen bilgisayara geçici olarak atanan IP adresleri dinamiktir. Statik IP adresleri ise, değişmeyen adreslerdir. Sunucu bilgisayarlarda statik IP kullanılır. Bir de Özel IP adresi (Private IP Adress) şeklinde adlandırılan yalnızca Yerel Ağ (LAN) da kullanılabilen IP adresleri vardır. Özel IP adreslerine örnekler: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0. - 192.168.255.255. Bu IP adreslerini kullanarak Geniş Ağ'a erişmek mümkün olmadığından, Geniş Ağ'a erişmek istenildiğinde *"Network Address Translation (NAT)"* Ağ Adresi Dönüştürme ile Özel IP adresi değiştirilerek bilgisayarın internete çıkışı sağlanır.

57. Soruşturma ve kovuşturma esnasında yapılan en büyük hatalardan birisi herhangi bir eylemin gerçekleştirildiği şüphesiyle bir IP numarası elde edildiğinde, bu numarayı kullanan kişinin doğrudan şüpheli, sanık ve suçlu yapılmasıdır. Oysa bu tamamen yanlış ve kolaycılıktan kaynaklanan bir algıdır. Yargıtay'ın da isabetli bir şekilde belirttiği üzere, IP numarası kullanılan bilgisayarı göstermeyip internetle olan bağlantıyı göstermektedir[14].

58. Pek çok soruşturma sonuna kadar hakkıyla yürütüldüğünde IP numarasını kullanan kişinin ya da kurumun gerçekleştirilen hukuka aykırı eylemden haberinin dahi olmadığı ortaya çıkmaktadır. Özellikle birçok bilgisayarın Truva atları ya da diğer programlar sayesinde "zombi bilgisayar"[15] haline getirildiği günümüzde IP numarası soruşturma için bir sonuç değil olsa olsa soruşturmanın ilerlemesi için bir başlangıç olabilir. Nitekim

---

[13] **Michael Cross**, Scene of The Cybercrime, 2. Ed., Syngress, 2008, s. 195.

[14] "Sanığın kullandığı bilgisayar üzerinde usulünce imaj alma işlemi yapılarak sonucunda çıkan veri bütünlük (hash) değerlerinin tesbit edilmemiş bulunması, IP numarasının kullanılan bilgisayarı göstermeyip internetle olan bağlantıyı göstermesi, sanığın bilgisayarlarında yapılan incelemede, bu bilgisayar kütüğünden m. -k12.com adresine bağlantı yapıldığının tespit olunamaması "hack" programına rastlanmasının şikayetçiye ait siteye müdahale edildiğini göstermeyeceği, kesin delil bulunmadan varsayımlarla hüküm kurulamayacağı cihetle tebliğnamedeki bozma düşüncesine katılınmamıştır. .. beraat kararı usul ve yasaya uygun bulunduğundan... ONANMASINA karar verildi." 8. CD. 24.10.2013, E. 2012/21817, K. 2013/25428.

[15] Zombi bilgisayar, (genelde yalnızca zombi olarak kısaltılır) genel ağa (internet) bağlı, bir kırıcı (hacker) tarafından bilgisayar virüsü veya truva atı ile tehlikeye atılmış bilgisayardır. Daha geniş bir şekilde ifade etmek gerekirse Zombiler, programların içlerine gizlenmiş ya da bizzat uygulama dosyası olarak indirilir ve çalıştırılır. Program çalıştığı andan itibaren sizin internet bağlantınızı kullanarak istenilen hedeflere saldırı düzenler. Böylelikle Hacker yakalanma riskine kendisini değil Zombi Bilgisayarları atmış olur. Diğer bir avantajı ise saldırıyı güçlü hale getirmektir. Tek bir saldırı komutu ile binlerce saldırı gücüne sahip olunmuş olur.

Yargıtay da IP adreslerinin doğru ve gerektiği gibi araştırılmamasını bozma nedeni yapmaktadır[16].

59. Bu konuda dikkat edilmesi gereken önemli bir husus ve soruşturmalarda gerçek faillere ulaşılması için soruşturma makamlarının önüne çıkan önemli bir engel yaygın şekilde kablosuz internet kullanımı nedeniyle hatta kullanıcısı abone haricindeki kişilerin de internet bağlantısını ortak şekilde kullanmalarının oldukça yaygın olmasıdır. Ayrıca tüm abonelere yetecek sayıda IP numarası olmadığından yukarıda söz etmiş olduğum NAT uygulaması yapılmakta, böylelikle faillerin, IP adresi kullanılmak suretiyle belirlenmesi olanaksızlaşmaktadır[17].

D. IP Numarası Olmadan Faile Ulaşılamaz

60. Her ne kadar yukarıda belirttiğim üzere, IP tek başına failin kim olduğunu göstermezse de, IP numarası olmadan da faile ulaşılması bilişim suçları bakımından imkansıza yakındır. Dolayısıyla IP numarası, eldeki ilk ve en önemli ipucunu oluşturur. Soruşturma esnasında faillere ulaşabilmek için IP adresini kullananlara ulaşılmaya çalışılır. IP adresleri dağıtılırken sistematik ve hiyerarşik bir yapı kullanıldığı için[18], bunun internet üzerinden sorgulanarak yapılması mümkündür[19].

---

16 "...Sanığın, ... elektronik posta adresini kullanarak mağdur adına bir internet sitesine verdiği ilanda, mağdura ait olduğu anlaşılan telefon numaralarını yayımlayarak TCK'nın 136. Maddesinde tanımlanan kişisel verileri hukuka aykırı şekilde yaymak suçunu işlediği iddiasıyla açılan davada...; mağdura ait kişisel verileri içeren elektronik posta gönderisinin, sanığa ait internet kafeden gönderildiğinin IP adresi ile tespit edilmesi, aynı elektronik posta adresi hesabının oluşturulması sırasında elektronik posta hizmeti veren şirkete beyan edilen bilgilerin de doğru olmadığının anlaşılması karşısında; elektronik posta adresi oluşturulurken kullanılan IP adresinin ve bu adresi kullanan kişinin, elektronik posta adresinin aktive edilmesi için ...net adli internet sitesinin yedek elektronik posta adresi isteyip istemediğinin, istemişse bu adresin ne olduğu, hangi IP adresini kullandığı ve sahibinin kim olduğu ... adındaki elektronik posta adresinin gerçek kullanıcısının, gerekirse bu adresten elektronik posta alan kişiler Türkiye İletişim Kurumu Başkanlığından sorulup, tespit edilerek dinlenilmek suretiyle belirlenmesinden sonra sanığın hukuki durumunun takdir ve tayini gerekirken eksik inceleme ile beraat kararı verilmesi Yasaya aykırı görüldüğünden HÜKMÜN BOZULMASINA..." 4. CD. 13.12.2010, E. 2010/19559, K. 2010/20604

"Osmaniye Valiliği Bilgi İşlem Şubesi servis sağlayıcılarının İsim Tescil İnternet Teknolojileri A.Ş olduğu ve yapılan araştırmada söz konusu şirketin www.osmaniye.gov.tr web sitesine 31.03.2012 günü saat 19:38'de siber saldırı düzenleyen ve www.osmaniye.gov.tr web sitesine erişim yapan bilgisayarların IP numaralarının tespiti istenildiği ve İsim tescil İnternet Teknolojileri A.Ş'nin cevabı yazısında 31.03.2012 günü saat 19:38'den 19:39'a kadar 88.252.161.194 IP numarası ile 31.03.2012 günü saat 19:38:02'de Mehmet Demirdağ isimli şahsa ait sabit telefonla bağlantı sağlandığından bahisle açılan davada; yapılan soruşturma ve kovuşturma yetersiz olup olaya ilişkin deliller toplanmadan mahkumiyet hükmü kurulmuştur. Sanığın suçlamayı kabul etmeyerek kullandığı modemin şifreli olduğunu, kötü niyetli kişiler tarafından şifresinin kırılıp kullanılabileceğini savunması karşısında, sanığın internet hattına izinsiz giriş yapan olup olmadığının sanığın internet hattının bağlı bulunduğu internet sağlayıcısından sorulması, dosya içinde suça konu valiliğe ait siteye giriş yapan IP numaralarının ilgili birim tarafından bildirildiği ancak sitenin erişilmez hale getirilip getirilmediği, veri değiştirme, yok etme veya yeni veri yerleştirme yapılıp yapılmadığına ilişkin bir tespite rastlanmadığı anlaşılmakla, erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde siteye erişimin ne zaman engellendiği sanık veya servis sağlayıcı tarafından bildirilen diğer IP numaralarından hangisi ile girişin yapıldığı araştırılmalı, siteye yapıldığı iddia olunan siber saldırının ne şekilde gerçekleştiği, niteliği, sitenin geçici veya daimi olarak erişilmez kılınıp kılınmadığı yahut mevcut verilerin yok edilip edilmediği veya varsa yerleştirilen resim, yazı v.s. nin neler olduğunun tespit edilip önekleri de alınmak suretiyle dosya içine konulmalı, sanığın bilgisayarına el konulup hard diski incelenerek suça konu siteye ait bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanmalıdır. Bu itibarla yukarıda açıklanan eksiklikler yerine getirilerek sonucuna göre tüm deliller birlikte değerlendirilip sanığın hukuki durumunun takdir ve tayini gerekirken eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması, (BOZULMASINA)" 8. CD. 14.05.2014, E. 2014/3415, K. 2014/12298.

17 **Ahmet Gül**, Doğrudan ve Dolaylı Bilişim Suçları, 2. Bası, Ankara, Seçkin Yayıncılık, 2018, s. 42.

18 IP adresleri tüm dünyada RIR olarak adlandırılan beş farklı bölgesel kayıt merkezi tarafından dağıtılmaktadır. Bunlar bölgelere göre IP dağıtım işlemlerini yaparak, ülkelerdeki servis sağlayacılara bu numaraların verilmesi görevini üstlenmişlerdir.

19 **Gül**, (2), s. 29.

61. Ülkemizde yapılan soruşturma ve kovuşturmalarda en önemli sorunlardan birini de bu son derece önemli bilginin elde edilmemesi oluşturur. Özellikle yurt dışında merkezi bulunan internet siteleri, kendi ülkelerinde suç oluşturmayan hakaret ya da ifade özgürlüğüne ilişkin suçlarda bilgi paylaşamında bulunmaktan kendi yasalarını gerekçe göstererek "haklı olarak" kaçınmaktadırlar. Bu eylemler ülkemizde (olmaması gerektiği halde) suç olarak düzenlendiği için, yapılan soruşturma ve kovuşturmalar akamete uğramaktadır.

62. Ülkemizde hizmet veren ve ülke içinde hukuki temsilcisi olan Microsoft gibi şirketlerden sınırlı da olsa bilgi akışı sağlanabilir iken; ülke dışında bulunan ve yurt dışından hizmet veren web sitelerinden ve yer sağlayıcılardan bilgi almak için istinabe (uluslararası adli yardımlaşma) yoluna başvurmak gerekir[20]. Bunun ise işlemi son derece uzatıcı, bilişim suçları açısından bir karşılığı olmayan ve genellikle de amaca hizmet etmeyen bir yöntem olduğu herkesin bildiği bir konudur.

E. Soruşturma ve Kovuşturmada Yapılması Gerekenler

63. Bu başlık altında belirtmem gereken ilk husus, adli bilişim incelemelerinin bilişim suçları hakkında yapılabileceği gibi, diğer klasik suçların ortaya çıkarılması ve/veya delillendirilmesi esnasında kullanılmasının mümkün ve gerekli olmasıdır. Dolayısıyla adli bilişim incelemesinin yalnızca bilişim suçlarına ilişkin olduğu bir söylem doğru değildir ve gerçeği yansıtmamaktadır.

64. İkinci husus ise, bilişim suçlarının izlenmesi, ortaya çıkarılması ve delillendirilmesinin kendine özgü yöntemler gerektirmesi, bunun da üst düzey bir uzmanlık seviyesi gerektirmesidir. Üzülerek ifade etmeliyim ki, Yargıtay da bunun farkındadır ve aşağıda örneklerini göreceğimiz üzere, pek çok mahkeme kararını eksik soruşturma veya kovuşturma nedeniyle bozmakta hatta gelinen aşamada zaman kaybı söz konusu olduğu ve deliller karartıldığı için istemediği ve hukuka aykırı olduğunu bildiği halde beraat kararı vermek zorunda kalmaktadır. Bu haksızlıkların ve hukuksuzlukların önüne geçilebilmesi ancak pek çoğunun Yargıtay kararlarında ve bu alana özgü uluslararası rehberlerde (özellikle Avrupa Konseyi'nin rehberlerinde) belirtilen suç soruşturma ve delil elde etme yöntemlerinin yerine getirilmesi gerekir.

65. Örneğin internette yer alan ve suç oluşturan bir içeriğe ilişkin soruşturma ve kovuşturmada, içeriğin oluşturulmasına ilişkin log kaydı, erişim yapan IP numarası, erişim tarih ve zamanı, abonelik gerektiren sistemlerde kayıt bilgileri (hesap oluşturulma zamanı, IP numarası, hesap sahibi bilgileri, erişim tarih ve zamanı) gibi bilgiler yer sağlayıcıdan sorularak bir sonuca ulaşılabilir[21].

66. Banka veya kredi kartlarının kötüye kullanılması suçundan güzel bir örnek ise, sanığın savunmasına karşın, başkaca bir delil de olmadığı ve sanığın savunması da bu yönde olduğu için sanığın iletişiminin tespite ilişkin kayıtlarının çözümünün yapılarak "yer bilgisi kullanılmak suretiyle" savunmanın doğru olup olmadığının tespit edilmesidir:

> *"Katılana ait kredi kartını rızasına aykırı olarak alıp, kullanarak 1000 TL'lik harcama yapıp nakit para da çekerek atılı hırsızlık ve kredi kartını kötüye kullanma*

[20] **Gül**, (2), s. 28.

[21] **Gül**, (2), s. 28.

suçlarını işlediğinden bahisle açılan davada; sanığın, katılanla 2012 yılı Haziran ve Temmuz aylarında birlikte İzmir'de olduğunu, atılı suçları kabul etmediğini savunması, bankanın ATM görüntülerini süresi dolduğundan göndermemesi karşısında, sanığın 2012 yılı Ağustos ayında İzmir'de bulunduğuna dair iletişim tespitine ilişkin CD'nin çözümlenerek tespit edilen baz istasyonları ile para çekimi yapılan ATM'lerin bulundukları yerlerin aynı mevkide olup olmadığının tespiti ile sonuca göre hukuki durumun tayini ve takdiri gerekirken yazılı şekilde hüküm kurulması, Yasaya aykırı..."[22].

67. BDDK tarafından yayınlanan *"Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ"*in[23] 32. maddesinin 10. bendi uyarınca para çekimine ilişkin kamera kayıtları "iki ay" süre ile saklanmakta, bu süre geçtikten sonra eski kayıtların üzerine kayıt yapılmaktadır. Soruşturma esnasında ilgili kurumlar ile yapılan yazışmalar uzun süre aldığı için genellikle bu süre geçmiş olduğu için suç anına ilişkin görüntülere ulaşılması mümkün olmamaktadır. Bunun yanı sıra banka içinden gerçekleşen bilgi sızıntılarının denetlenmesi, belirlenmesi ve delillendirilmesi çeşitli zorlukları ortaya çıkarmaktadır[24]:

"*İlgili banka tarafından havale edilen tutarın ne şekilde kullanıldığının bildirilmemesi karşısında; suça konu paranın ne şekilde kullanıldığının tespiti ile; öncelikle suça konu paraların ATM'lerden çekilmiş ise; hangi banka şubesi ya da yerdeki ATM'lerden çekildikleri, kamera görüntüsü olup olmadığı tespit edilip ATM'lerden çekildikleri ana ilişkin kamera görüntülerinin temin edilerek görüntülerdeki kişinin kimliğine dair araştırma yoluna gidilmesi, işyerlerinde alışveriş sırasında kullanılmış ise, bu işyerlerinin tespiti ile işlem anında kamera görüntüsü bulunup bulunmadığının sorularak, varlığı halinde, kamera kaydında görüntüsü bulunan kişinin sanıklar veya başkaca bir kişi olup olmadığının değerlendirilmesi, kamera kaydının bulunmaması ya da elde edilen görüntülerin kimlik tespitine elverişli olmaması halinde ise alışveriş yapılan işyerlerinden alım-satım işlemine ait fatura, fiş veya benzeri bir belgenin bulunup bulunmadığının, faturanın kimin adına tanzim edildiğinin tespitinin yapılması, (bozma)..."*[25].

68. Banka ve kredi kartlarının kötüye kullanma suçlarında ortaya çıkan diğer bir eksik incelemeye dayalı bozma nedeni ise aslında bir suç soruşturmasının temelinde yer alan şüphelilerin ifadelerinin aşamalarda alınmamasıdır:

"...sanık K.Ş.'nin suçlamayı kabul etmeyerek, hesabına para gönderildiğinden haberi olmadığını ve para çekmediğini beyan ettiği, dosya içerisinde mevcut 25/11/2010 tarihli teşhis tutanağında kredi kartını kullanarak dolandırıcılık yapan şahısların sonradan isimlerini öğrendiği diğer sanıklar M.T. ve B.K. olduğunu beyan ettiği, ancak bununla ilgili hiçbir aşamada ifadesinin alınmadığı, diğer sanıklar M.T. ve B.K.'nın ise suçlamayı kabul etmediklerinin anlaşılması karşısında; sanık K.Ş'nin, kendisine ait suça konu kredi kartının diğer sanıklar tarafından ne şekilde ele

---

[22] 8. CD. 24.02.2016, E. 2015/10508, K. 2016/2141. Akt: **Gül**, (2), s. 141.

[23] RG. 14.09.2007, 26643.

[24] **Gül**, (2), s. 42.

[25] 13. CD. 07.04.2015, E. 2014/20932, K. 2015/6394.

geçirilerek kullanıldığı hususunda ayrıntılı savunması alınması suretiyle sanıkların hukuki durumunun tayini gerekirken, delillerin nelerden ibaret olduğu gösterilmeden, tartışılmadan ve gerekçelendirilmeden eksik araştırma ile yazılı şekilde hüküm kurulması, (bozma)..."[26].

III. SONUÇ

69. Bu çalışmaya özellikle bir sonuç yazılmamıştır. Çalışmadaki bilimsel yorumlar dışındaki uygulamaya yönelik bölümler tamamen bugüne kadar hakimler, savcılar ve siber suçlar alanında çalışan emniyet mensuplarından, bu tür toplantılar ya da birebir görüşmeler esnasında alınan bilgiler çerçevesinde oluşturulmuştur. Dolayısıyla özellikle uygulamaya yönelik kısımlarda eksik, güncelliğini yitirmiş ya da hatalı bilgiler olabilir.

70. Yazarın amacı, bu çalışmanın yazılmasına vesile olan toplantı sonrasında, değerli katılımcıların bilgi, görgü ve eleştirilerini derlenmek suretiyle hem çalışmanın güncellenmesi hem de ayrıntılı bir sonuç bölümü yazılarak daha iyiye ulaşmak için atılması gereken adımlara ve tavsiyelere yer verilmesidir.

[26] 13. CD. 07.04.2015, E. 2014/20932, K. 2015/6394.