Kırıkkale Üniversitesi
Sosyal Bilimler Dergisi (KÜSBD)

ISSN 2146-2879 Kirikkale University Journal of Social Sciences E-ISSN: 2717-6231

Makale Bilgisi/Article Info
Geliş/Received: 03.03.2021 Kabul/Accepted: 08.06.2021
Araştırma Makalesi/Research Article, s./pp. 649-667

BİLİŞİM SUÇLARINDA CEZA MUHAKEMESİ KANUNUNUN 134. MADDESİNDEKİ HÜKÜMLERİN UYGULANMASINDA YAŞANAN AKSAKLIKLAR

Salih KESKİN [i]

Öz

Bilgisayar, bilgisayar programları ve bilgisayar kütüklerinde arama ve el koyma yapılabilmesi için CMK 134 gereğince şüphelinin bir suç işlediğine dair kuvvetli şüphe ve başkaca delil elde etme imkânının bulunmaması gerekir. Madde metni her ne kadar arama ve el koymaya ilişkin bir düzenleme olsa da CMK 116 ve CMK 123'te düzenlenen arama ve el koymadan konusu ve uygulanış şekli olarak farklı ve özel olarak tek madde halinde düzenlenmiştir. Bilişim materyallerinde yapılacak arama ve el koyma ile ilgili yasal düzenleme, çalışmada maddeler halinde gösterilen nedenlerden dolayı uygulamada bazı aksaklıklara neden olmaktadır. Bu çalışmada CMK 134 kapsamında elektronik verilerin depolandığı cihazlara yapılan arama ve el koyma işlemlerinde yaşanan sıkıntılar ve bu sıkıntılara çözüm aranmaya çalışılmıştır.

***Anahtar Kelimeler*:** CMK 134, Bilgisayarlarda Arama, Bilgisayarlara El Koyma, Elektronik Veri.

The Problems in The Enforcement of The Provısıons of The Turkish Criminal Procedure Code Artıcle 134 in Cyber Crime

Abstract

In order to search and seize computers, computer programs and computer logs, there should be strong suspicion that the suspect committed a crime in accordance with TCPC 134 and no other evidence should be available in accordance with TCPC 134. Although the article text is a regulation on search and seizure, it is different and specially arranged as a single article in terms of the subject and application of search and seizure regulated in TCPC 116 and TCPC 123. The legal regulations on search and seizure of informatic materials cause some problems in practice due to the reasons shown in the study as articles. İn this study, the difficulties experienced in the search and seizure of the devices where electronic data is stored within the scope of TCPC 134 and the solutions to these problems were tried to be sought.

***Keywords**: TCPC 134, Search On Computers, Seizing Computers, Electronic Data.*

[i] Doktora Öğrencisi, Ankara Sosyal Bilimler Üniversitesi, Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, e-posta: salihkeskin2004@hotmail.com, ORCID ID: 0000-0001-7039-0831.

Giriş

Ceza muhakemesinde delil elde etme yöntemleri; ifade alma, olay yeri inceleme, arama ve el koyma gibi klasik uygulamalarla yapılmaktayken bilişim suçlarının ortaya çıkmasıyla klasik yöntemlere ek koruma tedbirlerine ihtiyaç doğmuştur. Çünkü bilişim sistemleriyle işlenen suçların delillerini oluşturan elektronik veriler beş duyu organımızı kullanarak farkına varabileceğimiz türden değildir (Özen ve Özocak, 2015, s. 59). Bu sebeple elektronik verilerin ortaya çıkarılması önemli hale gelmekte, bu verilerin delil niteliği kazanması için teknolojik aletler kullanılması mecburiyeti ortaya çıkmaktadır. Özetle; artık klasik yöntemlerin yanında çok daha farklı teknolojik yöntemlerin koruma tedbiri olarak uygulanması gerekmektedir.

Beş duyu organımızla tespit edilemeyen ve elektronik devrelerden oluşan bilgisayar girdilerinin maddi gerçeğin ortaya çıkmasında delil olarak kullanılması, yeni bir yöntem olarak karşımıza çıkmaktadır. Elektronik verilerin tespit edilebilmesi için arama ve el koymayı düzenleyen genel hükümler niteliğindeki CMK m. 116 vd. ve m. 123'deki koruma tedbirlerinden daha özel ve daha sıkı şartlara bağlanmış arama ve el koyma kararının uygulanması gerekmektedir. Çünkü dijital materyallerin içerisinde ve bu materyallerin birbirleriyle veri akışının sağlandığı ağların bağlı olduğu sistemlerde suç delili araştırılması ve bu delillere el koyulması, adli arama ve el koyma tedbirinden hem nitelik olarak hem de delil tespiti yöntemi açısından farklı uygulamalardır. CMK 116 ile CMK 133. Maddeleri arasında düzenlenen arama ve el koymaya ilişkin koruma tedbirleri; şahıs, araç, ev, iş yerlerinde yapılırken CMK 134 kapsamında yapılan tedbirin konusunu bilişim sistemleri oluşturmaktadır (Kunter, Nuhoğlu ve Yenisey, 2013, s. 331-332).

Adli aramanın düzenlendiği CMK'nın 116. maddesinde şahısların üzerinde, evinde ve iş yerinde arama yapabilmek için makul şüphe yeterliyken CMK 134 kapsamında bilgisayar ve bilgisayar kütüklerinde yapılacak aramada suç işlendiği yönünde makul şüphe yetmemekte makul şüpheden daha yoğun bir şüpheyi içinde barındıran kuvvetli şüphenin varlığı aranmaktadır.

5271 sayılı CMK'da düzenlenen "gözlem altına alma", "iletişimin tespiti, dinlenmesi ve kayda alınması", "tutuklama", "bilgisayar ve bilgisayar kütüklerinde arama", "gizli soruşturmacı ve teknik araçlarla izleme" gibi koruma tedbirleri bir suç işlendiğine dair şüphenin kuvvetli olduğu temel hak ve özgürlüklere müdahale gerektiren olaylarda uygulanmaktadır.

CMK 134'te geçen kuvvetli şüpheyi, soruşturma evresinde sadece bir suçun işlendiği yönünde somut delillerle desteklenmiş bir şüpheyi değil; aynı zamanda üzerinde arama ve inceleme yapılacak bilgisayar, bilgisayar programları ve kütüklerinde suç delillerinin bulunacağı yönünde yoğun bir şüpheyi içinde barındırdığı şeklinde algılamak gerekir (Değirmenci, 2014, s. 352-353).

Bu çalışmanın birinci bölümünde CMK 134'ün uygulanmasında yaşanan aksaklıklar ile ilgili madde metnindeki beş fıkra, tek tek ele alınarak açıklanmıştır. İkinci bölümde CMK 134 kapsamındaki olaylara CMK 116 ve devamındaki hükümlerin uygulanması halinde yaşanan aksaklıklar değerlendirilmiştir. Üçüncü bölümde CMK 134'te olmayıp düzenlenmesini düşündüğümüz, madde metnine eklenmesi gereken hususlardan bahsedilmiştir. Dördüncü bölümde bilişim suçlarıyla mücadelede başat rol oynayan uygulayıcıların yeterince eğitilmemesi nedeniyle yapılan hatalardan bahsedilmiştir. Beşinci bölümde CMK 134 kapsamında elde edilen kopyaların ve çözümü yapılan metinlerin imha edilme prosedüründeki belirsizliklere değinilmiştir. Altıncı bölümde ise CMK 134 maddesinin uygulanmasında görülen diğer aksaklıklar incelenmiştir. Sonuç bölümünde ise aksaklıklar ile ilgili değerlendirmelerde bulunulmuştur.

CMK 134'ün Uygulanmasında Yaşanan Aksaklıklar

CMK 134/1'in Uygulanmasında Yaşanan Aksaklıklar

CMK 134'ün uygulanmasında yaşanan aksaklıklara değinmeden önce madde metninde geçen bilgisayar, bilgisayar programları ve bilgisayar kütüklerinin tanımı açıklığa kavuşturulmalıdır. Bilişim sistemleri denilince ilk akla gelen bilgisayarın "çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin" şeklinde tanımı yapılmaktadır (TDK, 2021).

Bilgisayar programları sayesinde bilgisayar içindeki dijital veriler, fail ve delil arasındaki köprüyü kuracak ispat bağına dönüşmektedir. Ayrıca suçun aydınlatılmasında son çare olarak icra edilen dijital delil arama faaliyeti, bilgisayar programları ile maddi gerçeğin ortaya çıkarılmasını mümkün kılmaktadır. Bu nedenle "Bilgisayar programı" nın kısa ve öz bir tanımını yapmak gerekir: Bilgisayar programına, bilgisayarın çalışır ve anlaşılır hale gelmesini sağlayan düz metin komutlarıdır, diyebiliriz. (Tanrıkulu, 2014a, s. 318).

CMK 134'te geçen "bilgisayar kütükleri" kelime grubunda geçen kütük kelimesi İngilizce "log" kelimesinin karşılığıdır. Bilişim alanında "log" denilince akla "kayıt" kelimesi gelmektedir. Bu sebepten CMK 134'te geçen bilgisayar kütüğü aslında bilgisayar veri tabanlarını ifade etmektedir. Her ne kadar böyle bir yorumla bu kavramlar açıklansa da mevzuatta bahsi geçen terimlerin; dijital sistemlerin, elektronik veri kavramlarının tanımı yapıldıktan sonra kullanılması daha uygun olurdu (Doğanay, 2020, s. 16,17). Bu açıdan bakılırsa bilgisayar ve bilgisayar kütüklerinin tanımları beraber düşünüldüğünde kaydetme özelliği bulunan tüm elektronik cihazları, bilgisayar kütüğü olarak değerlendirebiliriz.

Madde metninde geçen verilerin kâğıda yazdırılarak yazılı metin haline dönüştürülmesi, çoğu durumda kolluk kuvvetlerini sıkıntıya sokacak mahiyette bir düzenleme olarak görünmektedir. Şöyle ki el koyulan elektronik cihazdaki verilerin Office Word formatında depolandığı varsayıldığında 120 GB (Giga Byte)'lık bir hard diskin yaklaşık olarak 400'er sayfalık 25500'den fazla kitap alabileceği düşünüldüğünde bu kadar çok çıktının

alınması, kanunun emrettiği bir zorunluluk olarak görünmektedir. Bu itibarla "metin haline getirilmesi" şeklinde düzenlenen kanun metninin "tespit edilen bulgu verinin raporlanmasına" şeklinde değiştirilmesinin sorunun çözümü olacağı düşünülmektedir (Doğanay, 2019, s. 16).

Bir suç şüphesi nedeniyle yapılan soruşturmada şüphelinin CMK 134 gereğince bilgisayar kütükleri, bilgisayar programları ve bilgisayarlarında arama ve inceleme yapılırken aynı özellikteki cep telefonu, kamera kayıt cihazları, fotoğraf makineleri, hafıza kartları, LCD televizyon, taşınabilir bellekler, akıllı kartlar, bilgisayar yazıcısı(okuyucu, tarayıcı dahil) gibi elektronik cihazlarda arama ve inceleme yapılması durumunda bu arama faaliyetinin CMK 134 kapsamında olması gerektiği yukarıda fıkra incelendiğinde görülecek olsa da CMK 134'ün bu gibi elektronik delilleri kapsayacak şekilde yeniden düzenlenmesi kanunilik ilkesi açısından önem arz etmektedir. Mevzuat bu haliyle kaldığı sürece kanaatimizi belirttiğimiz düşüncenin aksine CMK 134'ün sadece bilgisayarlarla ilgili olduğu, diğer elektronik cihazların bu kapsamda değerlendirilemeyeceği gibi düşüncelerin bu hükmün uygulama alanını daraltacağı gözden kaçırılmamalıdır (Aydoğan, 2009, s. 19).

Bilişim suçları kapsamında düzenlenen ilk uluslararası sözleşme olan Avrupa Siber Suçlar Sözleşmesi, Macaristan'ın Budapeşte şehrinde 2001 yılında taraf devletlerce imzalanmış ve 23 Mart 2004 tarihinde yürürlüğe girmiştir. Bu sözleşme, Türkiye tarafından 10 Kasım 2010'da Strazburg'da imzalanmış ve 9 Ağustos 2014 tarihli 29083 sayılı resmi gazetede "Sanal Ortamda İşlenen Suçlar Sözleşmesi" başlığı altında yayımlanmıştır (Aliusta ve Benzer, 2018, s. 37,38). Avrupa Konseyi Siber Suç Sözleşmesi'nde tanımlar başlıklı birinci maddesinde "bilgisayar verisi", "bilgisayar sistemi", "hizmet sağlayıcı" ve "trafik verisi" gibi bilişim suçlarında kullanılan birtakım kavramların tanımı yapılarak bilişim suçlarıyla mücadelede kavramsal kargaşaların önüne geçilmeye çalışılmıştır. Örneğin; sözleşmede bilgisayar sisteminin tanımı "bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder." şeklinde yapılmıştır (Sanal Ortamda İşlenen Suçlar Sözleşmesi, 2014). Tanımda, bilgisayar sisteminin sadece bilgisayarlardan ibaret olmadığı bir program sayesinde dijital materyal içindeki verileri anlamlandırabilen tüm elektronik cihazların bu kapsama girdiği açık bir şekilde düzenlenmiştir. Adli ve Önleme Arama Yönetmeliği'nin 17/3'teki "Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır." hükmü aramanın yapıldığı yerde şüphelinin kullandığı bilgisayar ve bilgisayar kütüklerinin yanı sıra veri depolaması için kullandığı kompakt diskler, blu-ray diskleri, taşınabilir ve sabit hafıza diskleri gibi elektronik cihazlarında CMK 134 kapsamında yedeklenebileceğini ifade etmektedir (Aydoğan, 2009, s. 23). Kanuni metindeki boşluk, yönetmelikle doldurulmaya çalışılmaktadır. Ancak bu hususun CMK 134'te düzenlenmediği, Adli ve Önleme Arama Yönetmeliği'nin 17. maddesiyle düzenlendiği hususunun kabulü durumunda bu yönetmelik hükmü, Anayasa 13. maddesi "Temel hak ve hürriyetler, özlerine

dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir." hükmü ile kanunilik ilkesi gereğince Anayasaya aykırı olacaktır.

CMK 134/1'de arama kararı vermeye asıl yetkili hakimin olduğu, gecikmesinde sakınca bulunan halde ise cumhuriyet savcısının da yetkili olduğu düzenlemesi karşısında Adli ve Önleme Arama Yönetmeliği'nin 17/1. bendinde cumhuriyet savcısının istemi üzerine hakimin arama kararında yetkili olduğu görünmektedir. Bu yönüyle yönetmeliğin, gecikmesinde sakınca bulunan halde cumhuriyet savcısının da arama kararı verebileceği şeklinde düzenlenmesi gerekmektedir.

CMK'nın 134/1'de şüpheliye ait bilişim sistemlerinde arama ve inceleme yapabilmek için bir cürüm işlendiğine dair somut kanıtlarla desteklenmiş kuvvetli şüphenin mevcudiyeti tek başına yeterli görülmemekte, kuvvetli şüphenin yanında ayrıca suça ilişkin başka bir koruma tedbiri ile kanıt elde etme ihtimalinin olmaması koşulunun da varlığı aranmaktadır. Bu iki unsurdan birinin eksik olması durumunda elde edilen kanıt, bu madde gereğince kanuna aykırı olacaktır. "Başka bir yöntemle kanıt elde etme ihtimalinin olmaması" ibaresi soruşturma evresinde bu tedbirin son çare (ultima ratio) olarak kullanılmasını zorunlu kılmaktadır (Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma, 2021; Değirmenci, 2018, s. 147). Ayrıca bu iki şartın gerçekleştiği durumlarda bilişim sistemlerinde arama ve inceleme yapabilmek için öncelikli olarak hakim kararı, gecikmesinde sakınca bulunan hallerde ise cumhuriyet savcısı kararı gerekmektedir. Eğer böyle bir karar yoksa kolluk tarafından yapılan incelemenin hukuka aykırı bir soruşturma tedbiri olacağı gözden kaçırılmamalıdır. Bu duruma, Yargıtay 17. Ceza Dairesi'nin 15.02.2017 tarihli ve 2015/27517 E., 2017/1716 K. sayılı kararı örnek olarak gösterilebilir:

"Cumhuriyet Savcısının talimatıyla yapıldığı belirtilen, telefon inceleme tutanağının 20.04.2014 saat 14.10'da düzenlendiği, bu saatten daha önceki bir saatte saat 12.57'de düzenlenen 'fotoğraf teşhis tutanağına' göre şüphe üzerine durdurulan sanığın cep telefonunun Cumhuriyet Savcısının emri ya da mahkeme kararı olmadan kolluk görevlileri tarafından incelendiği ve telefonda, müştekiye ait çalıntı motosikletin fotoğrafının telefonda K ismiyle kayıtlı bir kişiye gönderildiğinin tespiti üzerine sanık hakkında mahkumiyet kararı verilmiş ise de; işlevi itibarıyla bilgisayar niteliğinde olan cep telefonu üzerinde inceleme yapılabilmesi için CMK'nın 134. maddesi uyarınca hakim kararı alınması gerektiği bu kararın alınmaması nedeniyle arama ve incelemenin yasaya aykırı olduğu ve bu delilin mahkumiyete esas alınmayacağı…"

Bu davada Yargıtay, hakim kararı olmadan kolluk tarafından cep telefonu üzerinde yapılan incelemenin hukuka aykırı olduğunu tespit etmiş olup elde edilen delil ile hüküm kurulamayacağına karar vermiştir. Cep telefonunun CMK 134'te arama yapılabilecek elektronik cihazlardan olduğu açık bir şekilde düzenlenmemiş olsa da bu kararda Yargıtay, bizim de savunduğumuz düşünce ile aynı doğrultuda cep telefonunu bilgisayar niteliğinde eş değer görmüş ve kararını CMK 134'teki hükümlere göre vermiştir. Her ne kadar biz de Yargıtay da bu şekilde düşünsek de CMK'nın cep telefonu gibi veri depolamada kullanılan

diğer elektronik cihazları da kapsayacak şekilde yeniden düzenlenmesi Anayasa 38/3 ve kanunilik ilkesi gereğince uygun olacaktır.

Cmk 134/2'nin Uygulanmasında Yaşanan Aksaklıklar

CMK 134/2 el koymaya ilişkin bir düzenlemedir. Şöyle ki madde metninde bilgisayar, bilgisayar programları ve bilgisayar kütüklerinin içindeki verilerin kopyalarının alınması ve çözümünün yapılabilmesi için üç durumda bu elektronik cihazlara el koyulabilir. İlki bilgisayarın içindeki verilere ulaşımın şifreli olması ve bu şifrelerin çözülememesi durumu, ikincisi bilgisayar içindeki gizlenmiş verilere ulaşılamaması ve son olarak da 25 Temmuz 2018 tarihli 7145 sayılı kanunun 16. maddesiyle CMK 134/2'ye eklenen bilgisayar içindeki verilere ulaşmada işlemin uzun sürecek olması durumudur (Parlak, 2019, s. 75). Bahsi geçen üç durumda şüphelinin kullandığı bu elektronik cihazlara el koyulabilmektedir.

CMK 134 kapsamında arama yapılan yerde bilgisayar içindeki verilerin şifreli olduğu, verilerin gizlenmiş olduğu ya da verilere ulaşmanın uzun zaman alacağı canlı inceleme yapılarak tespit edilebilir. Türkiye'de adli makamlar, uygulamada çoğu zaman canlı inceleme yapmaktansa verisine ulaşmak istediği şüphelinin kullandığı bilgisayar içinde bulunan harddisk, ssd gibi bilgisayar kütüklerini bilgisayardan sökmekte ve çıkarılan bu cihaz incelenmek üzere polis laboratuvarlarına götürülmektedir. Adli makamların para ve zaman kaybına neden olan bu uygulaması yerine suç delili sayılacak resimlerin, videoların, kelime listelerinin; bir süzgeçten geçirilerek el koyulan cihaz içinde aranması, suçla ilgili verilerin kopyasının alındığı diğer verilerin ayıklandığı aramanın amacına yönelik dünya standartlarında geçerliliği bulunan bir yöntemin uygulanması gereklidir. Bahsedilen bu yöntemle sadece suçla ilgili olan dosyalar incelenerek zaman tasarrufu sağlanacaktır. Ayrıca adli makamlarca yapılan suçun aydınlatılması süreci kısalacak, bu sayede soruşturma evresinde yapılan parasal masrafların azalacağı gibi adaletin tesis edilme süresi de kısalacaktır.

Burada şu hususa da vurgu yapmakta fayda vardır: CMK 134/2 kapsamında el koyulması gereken nesnenin, verinin içinde bulunan donanım olmalıdır. Yoksa içinde veri bulunmayan elektronik donanımlara el koymanın suçun aydınlatılmasında işe yaramayacağı ortadadır. Bunun yerine örneğin bilgisayara el koyulmaktansa içindeki elektronik verinin bulunduğu çıkarılabilir harddisk, ssd gibi veri depolarının bilgisayara zarar vermeden çıkarılarak el koyulmasının kanun amacına daha uygun olacağı düşünülmektedir.

Bilişim cihazlarında kopyalama işlemi tesis edilirken delil zincirinin bozulmaması ve suçun aydınlatılmasında kullanılacak elektronik verilerin güvenilirliğinin sağlanmasına önemli bir katkısı olan "hash değeri" kavramının incelenmesi gerekmektedir. Hash "belli bir verinin tanımlanmış algoritmalar ile tek yönlü olarak matematiksel işleme sokulması sonucu elde edilen özet veridir" (Doğanay, 2019, s. 22). Hash değeri ise dijital verilerin bulunduğu dosyalar üzerinde herhangi bir, en ufak bir değişiklik yapıldığında bile tamamen değişebilen, bundan dolayı dijital verinin bütünlüğünü garanti altına alan tabiri caizse dijital dosyaların parmak izi olarak adlandırılmaktadır (Özen ve Özocak, 2015, s. 53). Bilişim suçlarında delil

zincirinin güvenilirliğini sağlayan dijital verilerin hash değerinin hesaplanmasında en çok kullanılan algoritmalar SHA256, MD5 ve SHA1'dir. Dijital verinin çok küçük boyutlarda 1 bit veri dahi değişse hash değerinin değişecek olması hash algoritmalarının bilişim suçlarında güvenilir bir yöntem olduğunu göstermektedir (Doğanay, 2019, s. 85-86). CMK 134 kapsamında usulüne uygun verilmiş bir kararla suç mahallinde yani dijital verinin bulunduğu yerde imaj alma işlemine geçilmeden önce imajı alınacak elektronik cihazların yukarıda bahsedilen algoritmalarla hash değerinin hesaplanması ve imaj alındıktan sonra alınan imajlı dosyanın da hash değerinin hesaplanması gerekmektedir. Bu hash değerlerinin aynı olması, yapılan bu işlemlerle beraber hash değerinin tutanakla kayıt altına alınıp bir nüshasının müdafiye ya da şüpheliye verilmesi; kararda belirtilen adreste alınan veri ile adli emanette ve polis laboratuvarlarında incelemeye alınan verinin birebir aynı olmasına vesile olacak ve imaj alma işleminin usulüne uygun, doğru, güvenilir bir şekilde yapıldığını kanıtlayacak aynı zamanda imaj alma işleminde veri ekleme ya da veri çıkarma şüphelerinin ortadan kalkmasını sağlayacaktır (Değirmenci, 2018, s. 153). Polis laboratuvarlarında bilirkişi incelemesinden önce hash değerinin hesaplanarak bilirkişi raporunda belirtilmesi ve bu değer ile olay yerinde imaj alma işleminde hesaplanan hash değerinin aynı olup olmadığı davanın yetkili makamları tarafından kontrol edilmelidir. Suçun aydınlatılmasında kullanılacak imajı alınan dijital verinin, yukarıda bahsi geçen prosedürün uygulanmasıyla güvenilir bir delil vasfına kavuşacağı değerlendirilmektedir.

Cmk 134/3'ün Uygulanmasında Yaşanan Aksaklıklar

Bilgisayar ve kütüklerine arama ve el koyma koruma tedbiri uygulanırken şüphelinin kullandığı sistemdeki bütün verinin yedeklemesinin yapılması mevzuat gereği bir zorunluluk olduğu kanun metninden anlaşılmaktadır.

Veri yedeklemesi "Backup (Yedekleme) genel anlamı ile bilgisayar sisteminin işlevsel olmasını sağlayan temel birimlerini, depolanan verilerin ve çalışan yazılımların hata, hasar ve arıza durumunda kesintiye uğramaması ve geri dönülemez bir biçimde kaybolmasını önlemek için birçok kopya halinde saklanmasını amaçlayan dosyalar bütününün adıdır." Ş-şeklinde tanımlanmaktadır (Veri Yedekleme Nedir ve Gerekli midir?, 2021). Veri yedeklemedeki gaye, yedeklemesi yapılacak verinin birebir kopyasının elde edilmesidir. Adli bilişimde de suçla ilgisi olduğu yönünde kuvvetli şüphe bulunan verinin yedeği alınarak yedek üzerinde inceleme yapılması amaçlanmaktadır. Her ne kadar kanun bütün sistemin yedeğinin alınmasını şart koşsa da böyle bir uygulama şüpheli kişinin dışındaki kişilerin yaşantılarını ya da özellikle de ticari faaliyet gösteren gerçek kişiler ile ticari şirketlerin faaliyetlerini sekteye uğratabilir. Bu sebeple sistemdeki bütün verilerin yedeklerinin yapılması yerine sadece suçla ilgili verilerin bulunduğu bölümlerin yedeğinin alınmasını sağlayacak şekilde bir kanuni düzenlemenin yapılmasının, daha uygun olacağı düşünülmektedir (Doğanay, 2019, s. 20).

CMK 134/3'te geçen bilgisayar, bilgisayar programları ve bilgisayar kütüklerine el koyma işleminin gerçekleştirilmesi hükmü göz önüne alındığında; CMK 134 kapsamında

yapılacak bir el koymanın niteliği itibariyle CMK 123'te bahsi geçen el koymadan farklı olduğundan el koymanın gerekçelerinin ayrıntılı bir şekilde düzenlenmemiş olması önemli bir eksiklik olarak görülmektedir (Kunter vd., 2010, s. 339-340). Şöyle ki CMK 123'te zilyedinin rızası olması durumunda suç eşyası muhafaza altına alınabilmektedir. Muhafaza altına alma işlemi için zilyedin rızası yeterli olmakta ayrıca bir hakim kararı ya da başka bir merciin iznine ihtiyaç duyulmamaktadır (Göktürk ve Şahin, 2019, s. 341). Ancak CMK 134 incelendiğinde muhafaza altına alma ile ilgili bir düzenlemenin olmadığı görülecektir. Bu sebeple bilgisayar ve bilgisayar kütüklerine, şüphelinin rızası olsa bile muhafaza altına alma işleminin yapılması mümkün gözükmemekte dijital materyallere zilyedinin rızası olduğu halde bile yapılacak muhafaza altına alma işleminin hukuka aykırı olacağı değerlendirilmektedir.

CMK 134/2 ve CMK 134/3 madde metinleri karşılaştırıldığında bu madde metinlerinin birbiriyle çeliştiği görülecektir. Şöyle ki CMK 134/2'ye göre dijital materyallere olay mahallinde el koyabilmenin şartı dijital verinin kopyasının alınmasına veriye ulaşımı sağlayacak programların şifreli olması ve imaj alma işleminin uzun sürecek olmasıdır. Kanun koyucu böyle bir şartın gerçekleşmesi durumunda el koyma koruma tedbirinin uygulanabileceğini açıkça hükme bağlamıştır. Bunun dışında, bu şartın gerçekleşmemesi durumunda dijital verinin kopyası olay mahallinde alınabileceğinden el koyma kararının alınmasına gerek kalmayacaktır. CMK 134/5'e göre de dijital verinin kopyası alınabilecek ise yani dijital veriye ulaşım şifresiz ya da imaj alma işlemi uzun sürmeyecekse el koyma kararının alınmasına gerek kalmayıp olay mahallinde dijital verinin kopyası alınacak ve dijital materyal sahibine iade edilecektir. Bu hususlar beraber değerlendirildiğinde el koyma sırasında dijital verinin kopyasını almak mümkün olmadığından CMK 134/3, CMK 134/2 ve CMK 134/5 ile çelişmekte ve düzeltilmesi gereken bir yasa metni olarak karşımıza çıkmaktadır. CMK 134/3'ün başlangıcı el koyma işlemi sırasında değil de el koyma işleminden sonra şeklinde düzenlenseydi bu çelişki ortadan kaldırılabilirdi.

Cmk 134/4'ün Uygulanmasında Yaşanan Aksaklıklar

CMK 134/2'de yer alan gerekçelerle (şifrenin çözülememesi, gizlenmiş bilgiye ulaşılamaması ya da inceleme işleminin uzun sürecek olması) veri depolama özelliği bulunan elektronik cihazlara el koyularak CMK 134/3 kapsamında el koyulan bu cihazların yedekleri alınmaktadır. CMK 134/4 gereğince de el koyulan yedeğin kopyası alınarak şüpheliye verilmekte ve bu safha taraflarca bir tutanakla imzalanarak kayıt altına alınmaktadır.

CMK 134/4'ün uygulanması sonucu bilgisayar ve kütüklerinde bulunan yasadışı içerikli bir verinin şüpheliye verilmesi gündeme gelmektedir. Yedekten kopyası alınmış verilerin nerde, nasıl korunacağı ile korunma süresinin ne kadar olduğu, şüpheliye teslim edilme usulü, verinin hangi dijital cihaz ile şüpheliye verileceği, bu dijital cihazı kimin temin edeceği gibi hususlar CMK 134/4'te bulunmamaktadır. Ayrıca veri depolama cihazlarının kapasitelerinin her geçen gün arttığı dikkate alındığında bu kadar verinin ilgili kurumlarda saklanması için yeterli teknolojik donanımlarının olup olmadığı, her dijital verinin saklanmasının gerekip gerekmediği ya da ne kadar süreyle saklanacağı gibi hususların yasal

bir zeminde düzenlenmesi ve bu hususların çözümü için yasanın bir an önce uygulamaya yönelik icra edilmesi gerekmektedir (Hekim ve Başıbüyük, 2013, s.152).

CMK 134/4 dijital verinin yedeklemesi yapıldıktan sonra yedeğin bir kopyasının verilmesi, çoğu durumda isabetli bir düzenleme olarak algılanabilir. Ancak özellikle de kopyası verilen yedeğin yasadışı veriler (pornografik çocuk görüntüleri, şantaj amaçlı tutulan video ve görüntülerin, bir suç örgütünün öldürmeyi düşündüğü kişilerin listesi, binlerce hatta on binlerce kişinin TC kimlik bilgileri ile banka hesap şifreleri ile bu kişilere ait daha nice özel bilgilerin bulunduğu bir listeyi vb. gibi) içerdiği durumlarda bu verilerin şüpheliye veya vekiline verilmesi suçluya suç işleme yolunda devam etmesine imkân sağlayacak bir ortam hazırlayacağı düşünüldüğünde mevcut yasal düzenlemenin bir an önce değiştirilmesi gerekmektedir (Doğanay, 2019, s. 21-22). El koymayla ya da arama sonucu ele geçirilen yukarıda bahsi geçen çocuk pornografisi gibi suç oluşturan içeriklerin ulaşılmaz kılınması ya da bu tip verilerin yedekleri alındıktan sonra silinmesi önem arz etmektedir. Avrupa Konseyi Siber Suç Sözleşmesi'nin 19/3 maddesinde erişilen bilgisayardaki verilerin kaldırılmasına ve erişilmez hale getirilmesine izin vermesine rağmen CMK'de bu çeşit verilerin erişilmez hale getirilmesine ya da silinmesine dair yasal bir düzenlemenin bulunmaması önemli bir sorundur (Tanrıkulu, 2014b, s. 459-460).

İlgili fıkrada yedeklenen veride kişilerin ticari ve özel yaşamlarına devam etmelerini sağlayacak verilerin bulunabilmesi, ayrıca ticari faaliyette bulunan kurum veya şirketlerin faaliyetlerini sürdürmeleri açısından yedeklenen kopyanın şüpheliye verilmesi faydalı bir işlem olarak görünmektedir. Ancak yukarıda bahsedilen sakıncalardan dolayı kopyanın, iadesi işlemi yapılmadan önce incelenmesi önem arz etmektedir. Zira incelemesi yapılacak dijital verilerin, sınıflandırma yapılarak içerisinde iadesi yapılmaması gereken verilerin ayıklanması ve şüpheliye ayıklanmış haliyle teslim edilmesi gerekmektedir. Bununla birlikte suç delili olacak elektronik verilerin hızlı bir şekilde tespit edilmesi, soruşturmanın kısa sürede sonuçlanmasına fayda sağlayacaktır. Devasa kapasitelerde veri yığınının içinden kısa sürede delil nitelikli ya da şüpheliye verilmemesi gereken veriye etkin bir şekilde ulaşılmasını mümkün kılmak için önceliklendirme yöntemi diye adlandırılan "TRİAGE" adlı adli bilişim yöntemi uygulanabilir (Değirmenci, 2020, s. 47). Örneğin "Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları, temsili çocuk görüntülerini veya çocuk gibi görünen kişileri kullanma (Türk Ceza Kanunu 226/3-ikinci cümle)" suçunu işleyen kişinin suç ispatı için şüphelinin kullandığı bilgisayar gibi elektronik veri depolayan cihazlarında resim ve video gibi görsel materyallerin bulundurması ya da bu materyalleri kullandığı veri deposundan gönderdiğinin ispat edilmesi gerekmektedir. İspat etme noktasında işi kısa sürede yaparak kolaylaştırma adına veri deposundaki devasa verileri tek tek incelemektense önceliklendirme yöntemi kullanılarak suçla ilgili görsellerin bulunduğu dosyaların ayıklanarak incelenmesi adli makamların zaman ve para açısından lehine bir yöntem olacağı değerlendirilmelidir (Doğanay, 2019, s. 20). Triage yöntemiyle suçla ilişkili şüpheliye verilmemesi gereken dosyalar saptanıp geri kalan dosyaların şüpheliye tesliminin sağlanması hukuken daha uygun bir yöntem olacaktır. Ancak böyle bir uygulamanın mümkün olması

için CMK 134'te yukarıda bahsi geçen yöntemi mümkün kılacak bir mevzuat düzenlemesine ihtiyaç olduğu düşünülmektedir. Çünkü bu tip durumlarda yedeğin bir kopyasının çıkarılıp şüpheliye verilmesi, şüpheliye verilmemesinden daha vahim sonuçlara sebebiyet verecektir.

Cmk 134/5'in Uygulanmasında Yaşanan Aksaklıklar

CMK 134/2'de el koymanın, şifrenin çözülememesinden dolayı verilere ulaşılamaması ya da işlemin uzun süreceğinin anlaşıldığı durumlarda yapılmaktadır. Verilere ulaşıldığı ya da işlemin uzun sürmediği hallerde el koyma tedbirine başvurulmadan da bilgisayar ve bilgisayar kütükleri gibi sistemdeki verilerin tamamının veya bir kısmının kopyası CMK 134/5 fıkrası uyarınca alınabilecektir. Ayrıca ilgili fıkrada kopyası alınan verilerin kâğıda yazdırılmak suretiyle tutanak altına alınacağı ve tutanağın ilgililerce imzalanacağı düzenlenmektedir.

Uygulamada sistemdeki verilerin kopyası, olay yerinde yani arama kararının verildiği adreste yapılmaktadır. İlgili fıkranın uygulanması sonucu binlerce hatta on binlerce sayfa çıktı ile uğraşılması zaman ve para israfına neden olacaktır. Bu nedenle madde metnindeki "kopyası alınan verilerin kâğıda yazdırılarak" hükmü yerine "adli kopya alma işlemi tutanağa yazılır" şeklinde değiştirilerek düzenlenmesi gerekmektedir. Madde metninin yukarıda anlattığımız şekilde düzenlenmesi neticesi "imaj alma tutanağı" ile binlerce sayfa çıktı almaktan vazgeçilebilecektir (Doğanay, 2019, s. 22,23). Başka bir çözüm yolu olarak CMK m. 134/5'te yer alan "Kopyası alınan veriler kâğıda yazdırılarak bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır" hükmü yerine, Adli ve Önleme Arama Yönetmeliği'nin 17/5'te yer alan "Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir." hükmü biçiminde düzenlenebilir. Bu şekilde yapılacak yasal düzenlemenin, kopyası alınan verilerin kâğıda yazdırılması sorununu ortadan kaldıracağı düşünülmektedir.

Cmk 134 Kapsamındaki Olaylara Cmk 116 ve Devamındaki Hükümlerin Uygulanması

Bilgisayar ve kütüklerinde koruma tedbiri olarak arama ve el koyma yapılabilmesini mümkün kılan özel hüküm niteliğinde CMK 134 varken bu cihazların incelenmesinde ve el koyma koruma tedbirinin uygulanmasında CMK 116 ve CMK 123'te düzenlenen adli arama ve el koymaya ilişkin genel hükümlerin uygulanmasının kanunilik ilkesine zarar vereceği düşünülmektedir. Özellikle de aşağıda bahsedeceğimiz hususlarda genel hükümlerin uygulanmasının, elde edilecek elektronik verilerin hukuki delil olma vasfını tehlikeye atacağı düşüncesini akla getirmektedir. Bunun yanında konuyla ilgili mevcut yasal düzenleme Sanal Ortamda İşlenen Suçlar Sözleşmesi hükümlerine uyarlanana kadar bilgisayar dışındaki cep telefonu, sabit ve taşınabilir hafıza depolayabilen cihazlar gibi dijital veri depolayabilen elektronik cihazlarda CMK 134'teki arama ve el koymaya ilişkin hükümlerin uygulanması gerekmektedir (Başlar, 2013, s. 86,87). Genel hükümlerdeki arama ve el koyma için makul şüphe yeterli iken bilgisayar ve kütüklerinin aranması ve kütüklere el koyulmasında CMK 134 gereğince daha yoğun bir şüphe olan kuvvetli şüphenin gerekli olduğu madde metninden

anlaşılmaktadır. Suç işlediği yönünde makul şüphe bulunan şüphelinin bilgisayarında arama yapılması durumunda yapılan arama faaliyetinin hukuk düzeni dışında kalacağı ve elde edilen delilin de hukuka aykırı olabileceği gözden kaçırılmamalıdır.

"CMK 120: Aramada hazır bulunabilecekler", "CMK 121/2-3'ün uygulanma prosedürü", "CMK 124: İstenen eşyayı vermeyenler hakkında yapılacak işlem" gibi yasal düzenlemeler CMK 134'te bulunmamaktadır. Ancak CMK 116 ve devam eden aramanın ve el koymanın genel hükümlerinde düzenlenen bu gibi hususların, CMK 134'ün uygulandığı olaylarda vuku bulması durumunda kanunda belirtilmese de genel hükümleri diye adlandırdığımız kanun maddelerinin uygulanıp uygulanmayacağı sorunu ortaya çıkmaktadır. Bilgisayar ve kütüklerinin aranması ve el koyulması gerektiği olaylarda CMK 134'te bulunmayan bir uygulamanın CMK 116 ve devamı maddelerine atıfla uygulanması (ki uygulanabileceğini düzenleyen bir kanun metni yoktur.) bazen bu sorunun çözümünde faydalı (CMK 116 ve devamında düzenlenen arama emrinde açıkça gösterilmesi gerekenler ile yapılan işlemlerin tutanağa dökülmesi, koruma tedbirini icra eden kolluk personelinin isimlerinin imzalı olarak tutanakta yer alması, faaliyetin sonucunda verilecek belge gibi) olabilirken bazen de çelişkili durumlara sebebiyet verebilir. Bu durumu açıklamak adına iki örnek verilebilir. Birinci örnek; CMK 134 kapsamında yapılan arama da CMK 120'de yazılı hazır bulunacaklar maddesinin işletilip işletilmeyeceği sorununa ilişkindir. CMK 134 kapsamında bir evde bulunan bilgisayarda arama yapılacağı zaman bu aramada CMK 134'te hüküm olmadığı için hazır bulunması gereken kişilere gerek olmadan arama yapabilecek miyiz? Yoksa CMK 120 işletilerek madde metninde sayılan kişilerin hazır bulunmasını, aramanın hukuki niteliğini sağlayacak bir şart olarak mı uygulayacağız? Bu noktada CMK 120'nin uygulanmasının herhangi bir hukuka aykırılığının bulunmadığı düşünülse de bunun niçin hukuka aykırı olmadığı cevabı askıda kalacaktır. CMK 120'nin hukuka uygun olduğuna karar verilse bile bu uygulamanın arama ve inceleme faaliyetlerini yavaşlatan ve çoğu zaman gereksiz olduğunu düşünen görüşlerin doğru olduğu kabulünde CMK 134'ün CMK 120'den farklı olarak kendine has bir düzenlemeye gidilmesini zorunlu kılmaktadır (Doğanay, 2019, s. 17). İkinci örneğimize geçmeden önce uygulamada çoğu durumda şüphelinin kullandığı e-maillerin bulunduğu bilgisayarın içerisindeki sabit diskte arama yapmadan önce CMK 134/2 gereğince sabit diske el koyulmakta daha sonra inceleme yapıldığının bilinmesi gerekmektedir (Başlar, 2013, s. 91,92). Bu açıklamadan sonra örneğimize geçecek olursak; bir bilgisayarda şüphelinin CMK 45'te bahsi geçenlerden olan nişanlısı ile yazıştığı e-mail içeriklerinin incelenip incelenmeyeceği sorusunun cevabı CMK 134'te düzenlenmediğinden CMK 126'nın bu olayda uygulanıp uygulanamayacağı sorunu ortaya çıkacaktır. CMK 126'nın uygulanabileceği varsayımından hareketle; Böylesi bir durumda el koyma kararı verilmiş bir harddiskte el koyma kararı verilmemesi gereken bir e mail olduğu düşünüldüğünde; e mail açısından CMK 134 gereği yapılan el koyma ile CMK 126 gereği el koymanın yapılmaması gerektiğinden iki kanun maddesi birbiri içerisinde çelişkili konuma düştüğü görülecektir. CMK 116 ve devamındaki maddelerde kural olarak önce arama faaliyeti yapılır suç unsuruna rastlanırsa el koyma tedbiri uygulanırken CMK 134/2 şartlarının oluştuğu durumlarda

şüphelinin kullandığı bilgisayara önce el koyma tedbiri uygulanmakta sonra arama ve inceleme tedbirine geçilmektedir. Bu açıdan bakıldığında CMK 116 ve CMK 123'teki arama ve el koyma ile CMK 134'teki arama ve el koyma farklı uygulamaları zorunlu kılabilmektedir. Bu ve benzeri örnekler çoğaltılabilir. Dolayısıyla bu tip sorunların çözülmesi için CMK 134 kapsamındaki arama ve el koyma ile ilgili ayrıntılı ve özel bir düzenleme yapılmalıdır.

Cmk 134'te Olmayıp Düzenlenmesi Gereken Konular

Dijital materyaller yapıları gereği uygun olmayan muhafaza koşullarında kolaylıkla bozulabilir, zarar görebilir ya da çalışmaz hale gelebilir. Dijital materyallerin zarar görmemesi için uygun ortam koşullarında korunması için yasal düzenlemelere ve uygulamalara ihtiyaç vardır. Suç eşyası yönetmeliğinin "Kıymetli eşya ve evrak ile bozulacak, değerini kaybedecek veya muhafazası zor olan suç eşyası hakkında yapılacak işlemler" başlıklı 9/2. fıkrasındaki "Bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilir" düzenleme, adli makamların, dijital materyalleri hassas yapılarından dolayı zarar görmemeleri için uygun ortamlarda muhafaza edilmesini görevlerinin bir parçası olarak görmektedir. 2014 yılından beri iç hukukumuzda uygulanan Sanal Ortamda İşlenen Suçlar Sözleşmesinin "Depolanan bilgisayar verisinin süratli şekilde korunması" başlıklı 16/2. fıkrasında sözleşmeyi iç hukukunda uygulayan devletlere bilgisayar verilerini korumaya ve bütünlüğünü sürdürmeye yönelik yasal düzenlemeleri yapmasını zorunlu kılmaktadır. Ancak CMK 134'te böyle bir düzenleme olmadığı gibi adli ve önleme arama yönetmeliğinde de bu konuya ilişkin bir yasal düzenleme yoktur (Başlar, 2013, s. 100,101). Çözüm olarak, hukuki dayanak noktası CMK 134 olan bir yönetmelik çıkarılarak dijital materyallerin nasıl, hangi yöntemle korunması gerektiği ayrıntıya inilmek suretiyle yasal bir düzenleme ile yapılmalıdır.

Bilgisayar, bilgisayar programları ve bilgisayarlarda arama gerek şüphenin yoğunluğu gerekse de son çare koruma tedbiri olarak uygulanması açısından CMK 116 ve devamı maddesindeki adli aramadan daha özel ve daha zor şartlara bağlanmış tabiri caizse şahsına münhasır bir arama faaliyetidir. CMK 134 incelendiğinde bu kapsamda şüphelinin kullandığı bilgisayarın hangi suç tipinde aranacağı özel olarak düzenlenmemiştir. Şüpheli hakkında Türk Ceza Kanunu'nda (TCK) herhangi bir suç işlediği yönünde kuvvetli şüphenin varlığı, başkaca delil elde etme imkânının olmaması şartları sağlandığında şüphelinin kullandığı bilgisayarı aranabilecektir. TBMM'ye sunulan Ceza Muhakemesi Kanunu Tasarısının 110. maddesi CMK 134'e ait hükümleri düzenlemekteydi. Bu Tasarının 110. maddesinin gerekçesi "İki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren cürümler hakkında yapılan soruşturmalarda bilgisayarda, bilgisayar programlarında ve bilgisayar kütüklerinde arama, kopyalama ve aygıta geçici olarak el koyma yapılabilir." şeklinde düzenlenmiştir (Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma, 2021; Değirmenci, 2018, s. 146-147). Gerekçe, iki yıl ve üzerinde hapis cezasıyla cezalandırmayı mümkün kılan bir suç hakkında şüphelinin kullandığı bilgisayarın aranabileceğinden bahsetmektedir. Ancak gerekçe bu haliyle gerekçesi olduğu kanun hükmünde olmayan bir düzenlemeyi

yapmaktadır. Buradaki sorun, CMK 134'ün kanun metninde yazılı olduğu haliyle herhangi bir suçta uygulanabileceği mi? Yoksa kanunun gerekçesinde belirtilen iki yıl ve daha fazla cezayı gerektiren suçlarda mı uygulanabileceğinin cevabının verilmesidir. Kanun hükmünde kullanılan ifadelerin açık, net ve anlaşılır olduğu, kanun metninde yazılı kelimelerin manalarının şüpheye yer vermeyecek şekilde düzenlenmesi halinde gerekçenin hadiseye uygulanmasının mümkün olmayacağı kabul edilmektedir (Capitant, Çeviren Demirel, 1956, s. 59). CMK 134/1'de "herhangi bir suç" şeklinde belirtilen ifadenin şüpheye yer vermeyecek şekilde manasının açık olduğu dolayısıyla mevzuatın bu haliyle şüphelinin bilgisayarında arama yapılabilmesi için kanunun gerekçesinin referans alınarak iki yıl ve daha fazlayı gerektiren suçların dışında bu kanun hükmünün uygulanamayacağını söylemek kanunilik ilkesi gereğince doğru olmayacaktır. Ayrıca gerekçede kanun hükmünün uygulanacağı suç tiplerinin iki yıl ve daha fazla cezayı gerektiren bir suç olduğunu belirtse de bu suçun alt sınırı mı üst sınırımı olduğu belirtilmediğinden, gerekçenin hadiseye uygulanacak suç tiplerini belirlemede anlamının muğlak olduğu gözükmektedir. Gerekçenin hadiseye uygulanması gerektiğini düşünenlerin önce bu muğlaklığı çözmesi gerekmektedir.

Bilgisayar ve kütükleri gibi dijital materyallerde arama yapılması durumunda kişilerin özel hayatına, haberleşme özgürlüğüne, kişisel verilerine, mülkiyet haklarına, bilimsel ve ticari sırlarına, basın ve ifade özgürlüğü gibi anayasada düzenlenmiş temel hak ve özgürlüklerine müdahale edilmektedir (Şahin, 2019, s. 271,272). CMK 134 kapsamında yapılacak bir aramanın TCK'da düzenlenmiş herhangi bir suçta uygulanmasının, örneğin basit bir hakaret suçunun aydınlatılması için şüphelinin kullandığı bilgisayarda arama yapmanın mağdura sağlayacağı hukuki menfaat ile şüphelin temel hak ve özgürlüklerine müdahale niteliğinde olan aramanın, şüphelinin korunan hukuki değerinde meydana gelen zarardan çok daha önemsiz olduğu gözden kaçırılmamalıdır. Bu sebeple dijital materyallerde arama ve el koymanın hangi suçlar kapsamında yapılabileceği açıkça düzenlenmesi gerekmektedir.

Bir suç işlediği yönünde kuvvetli şüphe bulunan kişinin CMK 100'e göre tutuklanabilmesi için suç tipinin CMK 100'de belirtilen katalog suçlardan olması veya üst sınırının 2 yıl ve daha fazla olmasını şart koşmuştur. Koruma tedbirlerinden tutuklamanın uygulanmasına ilişkin şartları düzenleyen CMK 100'deki gibi katalog suç tiplerinde ya da katalog suçların dışında üst sınırı 3 yıl ve üzeri hapis cezasını gerektiren suçlarda CMK 134'teki koruma tedbirinin uygulanabilmesine imkan sağlayacak şekilde yasal bir düzenlemeye gidilebilir. Ancak mevzuat bu haliyle kaldığı sürece TCK'da herhangi bir suç dolayısıyla CMK 134'ün uygulanmasının önünde herhangi bir engel yoktur.

Uygulayıcıların Yeterince Eğitilmemesi Nedeniyle Yapılan Hatalar

CMK 134 kapsamında arama kararında bahsedilen adreste yapılacak arama faaliyetine başlanabilmesi için aramanın konusu olan bilgisayar gibi elektronik verinin depolandığı cihazların sistemlerinin açık ve şifresiz girişe elverişli olması gerekmektedir. Zira canlı inceleme dediğimiz yöntem sistemin açık olması durumunda gerçekleştirilebilen bir

faaliyettir. Canlı incelemeyi yapacak personelin alanında eğitim almamış, uzmanlaşmamış kişilerce yazma koruma kullanmadan sisteme müdahale etmesi, sistem içindeki dosyalara veya dijital materyallere hatalı bir şekilde ulaşmaya çalışması gibi sebeplerden dijital materyaller çalışamaz hale gelebilmektedir. Bu durum sistem içindeki dosyaların tarih saat değişimleri, uçucu verinin kaybı gibi adli soruşturmayı sıkıntıya sokacak önemli sorunlara yol açmaktadır. Suçun ispatına yarayacak delillerin güvenilirliği ve zarar görmeden elde edilmesi için bu işlemi yapacak personellerin bilişim alanında uzmanlaşmış, tecrübeli kişiler olması suç soruşturmasında suçun aydınlatılması noktasında hayati bir öneme sahiptir (Doğanay, 2019, s. 19).

Teknolojik gelişmelerin baş döndürücü hızı, bilişim sistemlerinin her geçen gün yenisinin ve farklı çeşitlerinin ortaya çıkması, bilişim suçlarıyla mücadeleyi zorlaştırmakta özellikle de bu suçlarla mücadele eden adli görevlileri suçun aydınlatılmasını sağlayacak farklı yöntemleri kullanmaya mecbur bırakmaktadır. Zira bundan yirmi yıl önce bilişim suçlarıyla mücadele yöntemleri şu anki yaşadığımız zaman dilimindeki yöntemden tamamen farklıdır.

Bilişim suçlarıyla mücadele için polis teşkilatında bilişim suçlarıyla mücadelede şube müdürlüklerinin oluşturulmasına ve Adalet Saraylarında bilişim suçları büroları var olmasına rağmen bu birimlerde çalışan personelin adli bilişim suçları ile ilgili nitelikli eğitim almadıkları görülmektedir. Bilişim suçlarıyla ilgili hemen hemen tüm soruşturmalar kolluk tarafından yürütülmekte, matbu evraklarla bu alandaki suçlar, Kovuşturmaya Yer Olmadığı Kararları (KYOK-Takipsizlik) ile sonuçlandırılmaktadır. Bilişim suçları ile alakalı bütün işlemler kolluğun siber suçlarla mücadele birimi vasıtasıyla yerine getirildiğinden kolluğun bilişim suçlarını zamanında inceleyip, araştırmanın sonucunu savcılığa süratli bir şekilde sunması mümkün değildir. Açık kaynaktan araştırma yapmak gibi basit bir inceleme faaliyeti gerektiren konular kolluğun siber suçlarla mücadele eden birimleri tarafından yerine getirilmekte ve bu birimin ağır iş yükü göz ardı edilmektedir. Adli bilişimle görevli adli personellerin adli bilişim alanında tam donanımlı olmadıkları gibi Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve Telekomünikasyon İletişim Başkanlığı (TİB) personelleri de yeterli derecede bilgi ve eğitim düzeyine sahip değildir (Çakmakkaya ve Akpınar, 2018, s. 126).

Dijital Verilerin Yok Edilmesine Dair Prosedür Sorunu

Ceza Muhakemesi Kanunun (CMK) 134/1'de gecikmesinde sakınca bulunan halde cumhuriyet savcısı kararına istinaden elde edilen elektronik veri kopyaların ve çözümü yapılan metinlerin, cumhuriyet savcısı tarafından verilen bu karara hakim tarafından 24 saat içerisinde aksine karar verilmesi ya da hakimin bu 24 saatlik süre içerisinde bir karar vermemesi durumunda derhal gecikmeksizin imha edilmesi gerekmektedir. Bu açıdan bakıldığında böyle bir durumda imha edilme prosedürün uygulanmasında mevzuat açısından bir sorun yoktur. Ancak şüpheli hakkında soruşturma süresi içinde cumhuriyet savcısınca kovuşturmaya yer olmadığına dair karar verilmesi ya da şüpheli hakkında kovuşturma sonucunda beraat kararı verilmesi durumunda elde edilen kopyalar ve çözümü

yapılan metinlerin yok edilip edilmeyeceği, yok edilecekse ne kadar süre içerisinde yok edileceği gibi soruların cevabı CMK 134'te bulunmamaktadır. Bu konuyla ilgili yasal düzenlemeye ihtiyaç olduğu anlaşılmaktadır. Bu sorunun çözümüne yönelik öğretide CMK 137/3'ün kıyasen uygulanabileceği görüşü olsa da kanunilik ilkesi gereğince CMK 134 için ayrıca bir düzenlemenin yapılmasında fayda vardır. Çünkü CMK 137/3 İletişimin tespiti, dinlenmesi ve kayda alınması ilişkin kayıtların yok edilme prosedürünü düzenlerken farklı bir koruma tedbiri olan CMK 134 için de elde edilen verilerin kopyalarının imha prosedürü yasal zeminde açık ve anlaşılır şekilde düzenlenmelidir. Ancak şu an böyle bir düzenleme olmadığı için CMK 137/3 ün kıyasen CMK 134'e uygulanması durumunda; şüpheli hakkında takipsizlik kararı verilmesi ya da kovuşturmada şüphelinin beraat etmesi durumunda CMK 134 kapsamında elde edilen kopyaların ve çözümü yapılan metinlerin cumhuriyet savcısı denetiminde on günü aşmayacak süre içinde imha edilmesi ve bu uygulamanın tutanağa bağlanması gerekir (Ünal, 2011, s. 127).

Ceza Muhakemesi Kanunun 134. Maddesinin Uygulanmasında Görülen Diğer Sorunlar

Şüphelinin kullandığı bilişim cihazlarında arama yapmak için CMK 134 gereğince hâkim kararının olması gerekmektedir. Şüphelinin kullandığı bilgisayarda arama yapılmasına izin vermediği durumda hâkim kararının alınması gerektiği konusunda tereddüt yoktur. Ancak şüphelinin kullandığı dijital materyallerin aranması yönünde rızasının olduğu durumda da hâkim kararının alınmasına gerek olduğu aksi takdirde şüphelinin aramaya rıza gösterdiği durumlarda hâkim kararı olmadan yapılan aramalar neticesinde elde edilen deliller hukuka aykırı olacaktır. Bu madde kapsamında şüphelinin rızası ile elde edilen delillerin hukuka aykırı olduğu Yargıtay kararlarında mevcuttur. Örneğin Yargıtay bir kararında; şüphelinin işyerinde bilgisayar ve bilgisayar kütüklerinde hâkim kararı olmaksızın şüphelinin rızası ile arama yapılması akabinde tespit edilen kanıtların kanuna aykırı usullerle elde edildiğine hükmetmiştir. Yargıtay, şüphelinin suçu işlediğini ortaya çıkaracak delili bile yasak yöntemlerle elde edildiği gerekçesiyle hükme esas delil olarak kabul etmemiştir (YCGK 2017/961 Esas, 2019/622 Karar, 2019).

Bir suç şüphesiyle incelenmek istenen bilgisayar ya da başka bir bilişim sistemi cihazının içindeki veriye ulaşılmasını sağlayacak şifrelerin şüpheliden ya da üçüncü şahıslardan istenip istenmeyeceği hususunda mevzuatta açık bir hüküm yoktur. Şüpheliden bu şifrelerin istendiği durumda Anayasa 38/5'in-"Hiç kimse kendisini ve kanunda gösterilen yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlanamaz."- ihlal edilmesi sorunuyla karşılaşılabilir. Şüphelinin istemediği halde bu şifreleri vermeye mecbur edilmesi durumunda şüphelinin kendisini suçlayıcı delil vermeye zorlandığı gerekçesiyle anayasal bir suç işlendiğine şüphe yoktur. Fakat şüpheli zorlanmadan kendi isteği ile bu şifreleri vermesi durumunda bilgisayar içerisindeki suçla ilgisi bulunan verilerin hukuka aykırı bir yöntemle elde edildiği gerekçesiyle elde edilen elektronik verilerin hukuka aykırı olup olmayacağı tartışmalıdır. Kanaatimizce böyle bir durumda eğer elektronik

verilerin bulunduğu cihazın aranmasında ve incelenmesinde CMK 134'te sayılan hakim kararı ya da gecikmesinde sakınca bulunan halde cumhuriyet savcısının kararının olduğu durumlarda şifrenin şüphelinin rızasıyla verilmesinde herhangi bir hukuka aykırılığın olmayacağı düşünülebilir. Ancak şüpheli soruşturmanın ilk evresinde kolluğa rızası olduğunu söylediği, soruşturmanın ya da kovuşturmanın sonraki safhalarında rızasının olmadığını söylediğinde o güne kadar şüphelinin rızası dahilinde elde edilmiş delillerin akıbeti ne olacaktır? Böyle bir sonunun çözülmesi için mutlaka CMK 134'te bir düzenlemeye gidilmesi şarttır. Şu anki haliyle mevzuatımızda bu soruna bir yanıt verecek düzenleme bulunmamaktadır.

Elektronik verilerin şifrelendiği bir cihazda arama yapılmadan önce şifre çözme anahtarlarının üçüncü kişilerden istenip istenmeyeceği hususu mevzuatta düzenlenmemiştir. Eğer CMK 134 kapsamında bir prosedür mevcutsa elektronik verilere ulaşmak amacıyla şifre çözme anahtarı kendisinde mevcut olan üçüncü şahıslardan da rızalarını almak şartıyla istenmesinin ve şifre çözme anahtarının kullanılmasının hukuka uygun olduğu kanaati düşünülebilir. Ancak üçüncü kişilerin rızaları yoksa bu kişiler şifre çözme anahtarlarını vermeye zorlanamayacaktır (Başlar, 2020, s. 71).

Sonuç

Bilgisayar, bilgisayar kütüklerinde arama, kişilerin temel hak ve özgürlüklerine özellikle de Anayasanın 20. maddesinde yazılı özel hayatın gizliliğine müdahale olduğundan kanun koyucu bu hususu ayrıca düzenleme ihtiyacı görmüştür. Bu sebeple CMK 134'te, bilgisayar ve kütüklerinde yapılacak arama ve el koyma koruma tedbirleri ile ilgili bir düzenleme yapılmıştır. Ancak yapılan düzenleme uygulamada birtakım sıkıntılara sebep olmaktadır. Bu çalışmada bu sıkıntıların çözümüne yönelik CMK 134'te bazı değişikliklerin yapılması yönünde önerilerde bulunulmuştur. Bu öneriler doğrultusunda CMK 134'te yapılacak değişiklikler aşağıda sıralanmıştır:

CMK 134/1 Üst sınırı 3 yıldan fazla cezayı gerektiren bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları, bilgisayar kütükleri, cep telefonu, hafıza kartları gibi dijital veri depolama özelliği bulunan elektronik cihazlarda arama yapılmasına, elektronik cihaz kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek tespit edilen bulgu verinin raporlanmasına karar verilir. Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi, kovuşturmaya yer olmadığına dair karar verilmesi, ya da kovuşturma evresinde sanığın beraat etmesi hâlinde çıkarılan kopyalar ve veri raporları derhâl imha edilir.

CMK 134/2 Veri depolama özelliği bulunan dijital materyallerde canlı inceleme yapılarak da arama yapılabilir. Canlı inceleme esnasında şifrenin çözülememesinden dolayı

girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için mümkünse dijital materyalin bulunduğu yerde imajının alınması, bunun da mümkün olmaması halinde bu materyallere el koyulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el koyulan cihazlar gecikme olmaksızın iade edilir. El koyma kararının alınmasında uygulanacak prosedür birinci fıkrada bahsedilen prosedüre uygun olmalıdır.

CMK 134/3 Elektronik veri depolayan dijital materyallere el koyma işleminden sonra, sistemdeki mümkünse sadece suçla ilgili verilerin yedeklemesi yapılır. Sadece suçla ilgili verilerin yedeklenmesinde önceliklendirme yöntemleri gibi bilişim yöntemlerinden faydalanılarak bu işlem gerçekleştirilebilir. Bu yöntemlerin uygulanması ile suçla ilgili verilere ulaşılamıyorsa sistemdeki bütün verilerin yedeklemesi yapılır.

CMK 134/4 Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır. Ancak yedeğin içerisinde ya da yedeği alınmış dijital materyallerin içerisinde şüphelinin suç yolunda suç işleme yolunda devam etmesine imkân sağlayacak ya da pornografik çocuk görüntüleri gibi tespit edilen delilin şüpheliye verilmesinin verilmemesinden daha vahim sonuçlara sebebiyet vereceği durumda şüpheli ya da vekiline bu tür deliller verilmez. Bu delillerin tespitini hızlı ve etkin bir şekilde sağlayacak bilişim programlarından faydalanılabilir. Şüpheli ve vekiline verilmeyecek delillerin tespiti, kovuşturma evresinde hakim kararı, soruşturma evresinde Cumhuriyet Savcısı kararı ile tesis edilir.

CMK 134/5 Veri depolama özelliği bulunan dijital materyallere el koymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir.

Kaynakça

Aliusta, C. ve Benzer, R. (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 4(2), 35-42.

Aydoğan, H. (2009). *Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri*. Polis Akademisi Güvenlik Bilimleri Enstitüsü. Yüksek Lisans Tezi, Ankara.

Başlar, Y. (2013). Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri. *Uyuşmazlık Mahkemesi Dergisi*. (3), 82-105.

Başlar, Y. (2020). Adli Bilişim Sürecinde Karşılaşılan Sorunlar ve Çözüm Önerileri. *Türkiye Barolar Birliği Dergisi*. 33(148), 47-76.

Capitant, H. Çeviren Demirel, H. (1956). Kanunun Manasının Tayininde İzhari Çalışmaların Değeri. *Ankara Hukuk Fakültesi Dergisi*. XIII (1), 53-68.

Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma. (2021). https://barandogan.av.tr/blog/mevzuat/cmk-madde-134-bilgisayarlarda-bilgisayar-programlarinda-ve-kutuklerinde-arama-kopyalama-ve-elkoyma.html, Erişim Tarihi: 16.01.2021.

Çakmakkaya, B. Y. ve Akpınar, T. (2018). Bilişim Suçları ile Mücadelede Karşılaşılan Sorunlar. *Balkan ve Yakın Doğu Sosyal Bilimler Dergisi*. 4(3), 123-129.

Değirmenci, O. (2014). *Ceza Muhakemesinde Sayısal (Dijital) Delil*. Ankara: Seçkin Yayıncılık.

Değirmenci, O. (2018). Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve ElKoyma Koruma Tedbirinde (CMK m. 134), 7145 Sayılı Kanun'la Yapılan Değişikliklerin Değerlendirilmesi. *Terazi Hukuk Dergisi*. 13(146), 146-155.

Değirmenci, O. (2020). Adli Bilişimde Önceliklendirme (Triyaj) Yönteminin Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi. *Bilişim Hukuku Dergisi*. 2(1), 47-79.

Doğanay, H. A. (2019). *Mobil Adli Bilişiminin Önemi Bağlamında Hukuki Süreç ve Delil Zinciri Kavramı ile Yeni Nesil Mobil Cihazların İncelenmesinde Karşılaşılan Güncel Zorlukların Değerlendirilmesi*. Yüksek Lisans Tezi. Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara.

Doğanay, H. A. (2020). *Mobil Cihaz Adli Bilişiminde Karşılaşılan Güncel Zorluklar ve Delil Zinciri*. Ankara: Legem Yayıncılık.

Göktürk, N. Ve Şahin, C. (2019). *Ceza Muhakemesi Hukuku I* (10. Bası). Ankara: Seçkin Yayıncılık.

Hekim, H. Ve Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*. 4(2), 135-158.

Kunter, N., Nuhoğlu A. ve Yenisey F. (2010). *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku İkinci Kitap Hüküm Verme Görevi ve Ceza Muhakemesinin Yapısı* (17. Bası). İstanbul: Beta Yayınevi.

Özen, M. ve Özocak, G. (2015). Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi. *Ankara Barosu Dergisi*, 41-77.

Parlak, O. E. (2019). *Türk Ceza Muhakemesinde Bilişim Sistemlerinde Arama, Kopyalama ve El koyma*. Yüksek Lisans Tezi. Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Sanal Ortamda İşlenen Suçlar Sözleşmesi. (2014/09/08). 29083 Sayılı Resmi Gazete. Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5-1.pdf. Erişim Tarihi: 07.01.2021.

Şahin, C. (2019). Ceza Muhakemesinde Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma (Cmk M. 134). *Yaşar Hukuk Dergisi*, 1(2), 271-286.

Tanrıkulu, C. (2014a). *Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve El koyma.* Doktora Tezi. Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Tanrıkulu, C. (2014b). *Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve El koyma* (Birinci Baskı). Ankara: Adalet Yayınevi.

TDK (Türk Dil Kurumu), https://sozluk.gov.tr/. Erişim Tarihi: 11.01.2021.

Ünal, O. G. (2011). *Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve El Koyma*. Yüksek Lisans Tezi. Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Veri Yedekleme Nedir ve Gerekli midir?, https://www.ankarabilisim.org/tum-haberler/veri-yedekleme-nedir-ve-gereklimidir-haberi-71, Erişim Tarihi: 12.01.2021.

Yargıtay 17. Ceza Dairesi'nin 15.02.2017 tarihli ve 2015/27517 E., 2017/1716 K. sayılı kararı. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/. Erişim Tarihi: 12.12.2020.

YCGK 2017/961 Esas, 2019/622 Karar, 22 Ekim 2019 tarihli kararı. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/. Erişim Tarihi: 12.12.2020.