“1) Kolluk güçleri, sanığın işlettiği ... isimli iş yerinde, açıkta, bandrolsüz şekilde poşetler içinde tütün mamulleri olduğunu tespit ederek iş yerinde muhafaza işlemi yaparak, Cumhuriyet savcısından arama kararı talep etmiştir.

2) Bursa Cumhuriyet Başsavcılığı, mahkemeden arama kararı talep etmiş, Bursa 1. Sulh Ceza Hâkimliği, 21.11.2022 tarih ve 2022/... D iş sayılı kararla, iş yerinde ve şüphelinin kullandığı dijital materyaller üzerinde arama yapılmasına karar vermiştir.

3) Kolluk güçleri, 21.11.2022 tarihinde, saat 18.00’da arama yaparak, bandrolsüz, dolayısıyla kaçak olduğu iddia olunan tütün ürünleriyle şüpheliye ait Iphone 3 mini telefona elkoymuştur. Tutanağa göre telefonların adli kopyaları olay yerinde alınmamış, doğudan telefonlara elkonularak sonradan adli kopyaları alınmıştır.

4) Telefon, çözümünün yapılması için Bursa Siber Suçlarla Mücadele Şube Müdürlüğüne gönderilmiştir.

5) Bursa Siber Suçlarla Mücadele Şube Müdürlüğü, hash değerinin alınıp alınmadığı belli olmayan imaj alma ve çıkarım raporu düzenlemiş, rapor dosyamıza gönderilmiştir.

6) Telefon ve adli kopya Bursa Cumhuriyet Başsavcılığının 2023/... sayılı emanet makbuzuyla emanete alınmıştır.

7) Bursa Cumhuriyet Başsavcılığı, 19.01.2023 tarih ve 2023/... numaralı iddianamesiyle, sanık hakkında 5607 sayılı Kanun’a göre cezalandırma talep etmiş, emanetin 2023/... sırasında kayıtlı telefonun ve sim kartının sanığa iadesini, USB belleğe alınan adli kopyanın ise dosyada delil olarak saklanmasını talep etmiştir.

CMK 134. MADDENİN ANAYASAYA AYKIRILIK NEDENLERİ

I) Terimler

8) “Bilgisayar“ terimi, 2001 tarihli Budapeşte Sanal Ortamda İşlenen Suçlar Sözleşmesi’nin 1/a bendindeki tanıma göre “bilgisayar sistemi, bir veya birden fazla program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder”. Bilgisayar kavramına ilişkin farklı tanımlar incelendiğinde hepsindeki ortak nokta; bilgisayarın veri alma, gönderme, işleme, depolama, verileri, önceden tanımlanmış programlar yardımı ile kendiliğinden işleme/değiştirme özelliği taşımasıdır. Bu açıdan “bilgisayar” terimi, sadece günlük dilde bilgisayar olarak adlandırılan cihazları değil, amaçsal yorumla işletim sistemi kullanan akıllı telefon olarak adlandırılan cihazları, tabletleri, giyilebilir akıllı aksesuarları (saat, gözlük gibi) ve benzer diğer aletleri de kapsar (İşletim sistemi kullanan cep telefonunun bilgisayar kavramına dâhil olduğuna dair bk 17. CD, 15.02.2017, 27517/1716; 16. CD 21.04.2016, 4672/2330).

9) Program, maddi varlığı olmayan ancak maddi varlıklar arasında iletişim kurarak bilgisayarın bir bütün halinde çalışmasını sağlayan, veri alan, depolayan, ileten, işleyen, gösteren, oynatan çeşitli dillerle oluşturulmuş komutlar dizinidir.

10) Bilgisayar kütükleri, olay kayıtları (log), verilerin saklandığı yer (veritabanı/database), veri saklanan donanımlar (harici harddisk, flash bellek, hafıza kartları)

gibi verilerin ve işlemlerin tutulduğu yer anlamına gelmektedir. Bu nedenle veri içeren donanım unsurları da (Adli önleme aramaları Yönetmeliği md 17/3) bilgisayar kavramına dâhildir. İnternet ortamında verileri tutmak için kullanılan, ücretli ve ücretsiz depolama alanları da (google drive, yandex disk gibi) bilgisayar kütüğü (uzak bilgisayar kütüğü) kavramı içindedir.

11) Bilgisayar kayıtları, bilgisayar içinde depolanan, tüm dijital veriler anlamına gelmektedir.

12) Bu tanımlara göre (tanımlar için Bk 16. CD, 24.04.2017, 3/3; 16. CD 21.04.2016, 4672/2330) tüm dijital veriler ve dijital veri depolayan, işleyen cihazlar CMK 134. madde kapsamındadır.

II) Anayasaya Aykırılık Sorunu

13) Anayasa'nın 2. maddesinde belirtilen hukuk devleti, eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, Anayasa ve hukukun üstün kurallarıyla kendini bağlı sayan, yargı denetimine açık olan devlettir. Hukuki güvenlik ile belirlilik ilkeleri, hukuk devletinin önkoşullarındandır. Kişilerin hukuki güvenliğini sağlamayı amaçlayan hukuki güvenlik ilkesi, hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar. Belirlilik ilkesi ise yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olmasını, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesini ifade etmektedir.

14) Anayasa Mahkemesi tarafından kişisel veri kavramının -belirli veya kimliği belirlenebilir olmak şartıyla- bir gerçek veya tüzel kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmiştir (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/180, K.2015/30, 19/3/2015; Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, § 49; Fatih Saraman, [GK], B. No: 2014/7256, 27/2/2019, § 57). işisel verilerin korunmasını isteme hakkını sınırlamaya yönelik bir kanuni düzenlemenin şeklen var olması yeterli olmayıp kuralların keyfîliğe izin vermeyecek şekilde belirli ve öngörülebilir nitelikte olması gerekir (AYM, E.2021/107, K.2022/109, 28/9/2022, § 17). Esasen temel hak ve özgürlükleri sınırlayan kanunun bu niteliklere sahip olması Anayasa'nın 2. maddesinde güvenceye alınan hukuk devleti ilkesinin de bir gereğidir. Hukuk devletinde kanuni düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesi gerekir. Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar (AYM, E.2015/41, K.2017/98, 4/5/2017, §§ 153, 154). Dolayısıyla Anayasa'nın 13. maddesinde sınırlama ölçütü olarak belirtilen kanunilik, Anayasa'nın 2. maddesinde güvenceye alınan hukuk devleti ilkesi ışığında yorumlanmalıdır.

15) Günümüzde bilgisayarlar, sıradan kişisel verilerden hassas kişisel verilere kadar tüm kişisel verileri ya doğrudan içermektedir ya da elkonulan bilgisayardaki izlerin takibi ile bu verilere ulaşmak mümkündür.

16) Elkonulan bilgisayarlar vasıtasıyla ele geçirilen kişisel verilerin bir listesini çıkartmak anlamsızdır. Banka kayıtları, haberleşme programlarındaki (whatsapp, Messenger gibi anlık, elektronik posta gibi kalıcı) iletişim içerikleri, sosyal medya uygulamalarına ilişkin kayıtlar, rehbere ekli kişiler dikkate alındığında sosyal ve dijital çevre, video, fotoğraf, belge, yazı gibi dokümanlar, erişilen, gezilen web sayfaları yoluyla internet geçmişi, aranan, aranılan kişiler, kısa mesaj yoluyla haberleşme gibi sayılarak tüketilemeyecek kadar çok veriye, bilgisayar üzerinden erişmek mümkündür.

17) Temel haklara müdahale eden kanunun, metni ve metninin olası uygulamalarıyla kötüye kullanmaya ve keyfiliğe karşı uygun ve yeterli güvenceleri içermesi gerekir (Iliya Stefanov/Bulgaristan, No. 65755/01, § 38, 22 Mayıs 2008). Bir norm, temel haklara ne kadar çok müdahale ediyorsa vatandaşlara sağlayacağı güvencelerin ve kötüye kullanımın önlenmesi açısından o kadar çok sıkı ve anlaşılır güvenceler sunmak zorundadır. Temel hak ve özgürlüklerin sınırlandırılmasında kanunilik ölçütünün ilk basamağı, şeklî bir kanunun varlığının gerekliliğidir (Tuğba Arslan, § 96; Fikriye Aytin ve diğerleri, § 34). CMK 134. madde, hem lafzı hem de metindeki "işlemin uzun sürecek olması" ibaresinin uygulamada kötüye kullanılması nedeniyle pek çok temel hakka yönelik yeterli güvenceyi içermemektedir.

Maddenin Lafzından Kaynaklanan Güvence Eksikliği

i) İletişime müdahalenin, Kanunda (CMK 135) ve AİHM kararlarında (Bk Zakharov-Rusya, Malone-Birleşik Krallık, Huvig-Fransa, Kruslin-Fransa, Klass ve diğerleri-Almanya, Silver ve diğerleri/Birleşik Krallık, Campbell/Birleşik Krallık, Leander-İsveç ve Lüdi-İsviçre, Karabeyoğlu-Türkiye) belirlenen temel şartları bulunmaktadır.

Haberleşmenin içeriğinin denetlenmesi, haberleşmenin gizliliğine ve dolayısıyla haberleşme özgürlüğüne yönelik ağır bir müdahale oluşturur (Yasemin Çongar ve diğerleri, § 52). Anayasa'nın 22. maddesi ve Sözleşme'nin ortak koruma alanı, haberleşme özgürlüğünün yanı sıra içeriği ve biçimi ne olursa olsun haberleşmenin içeriğinin gizliliğini de güvence altına almaktadır. Haberleşme bağlamında bireylerin karşılıklı ve toplu olarak sözlü, yazılı ve görsel iletişimlerine konu olan ifadelerinin gizliliğinin sağlanması gerekir (Yasemin Çongar ve diğerleri, § 49). Posta, elektronik posta, telefon, faks ve internet aracılığıyla yapılan haberleşme faaliyetleri. haberleşme özgürlüğü ve haberleşmenin gizliliği kapsamında değerlendirilmelidir (Yasemin Çongar ve diğerleri, § 50).

Bilgisayarlar, aynı zamanda iletişimi sağlayan, iletişim verilerini depolayan, iletişim verilerine geçmişe yönelik erişilmesine olanak veren, iletişimin içeriği yanında iletişime geçilen kişileri, iletişimin zamanını ve süresini de içeren veriler barındırmaktadır. Bu nedenle bilgisayara elkonulup incelenmesi, aynı zamanda (çoğu kez geçmişe yönelik bile olsa) iletişimin de tespiti anlamına gelmektedir. Hâlbuki iletişimin tespitinin, önemine ve ağırlığına göre bir suç listesinin olması, tanıklıktan çekinebilecek kişiler yönünden delil teşkil etmemesi, tesadüfi delile ilişkin özel kural içermesi, verilerin saklanması, kullanılması ve imhası için açık, anlaşılabilir ve erişilir kuralları içermesi gerekir.

Dijital iletişim, klasik iletişim araçlarına (telefonla konuşma, fax, mektup) göre daha işlevseldir, yaygın olarak kullanılır ve daha önemlisi hassas veriler içerir. CMK 134. madde,

elkonulup incelenen dijital iletişim içeriğinin elde edilmesi, saklanması, imhası, tanıklıktan çekinme hakkı olanlar yönünden hukuki değer ifade etmemesi, tesadüfi deliller yönünden hukuki değer açılarından, vatandaşlara yeterli koruma sağlamamaktadır.

ii) Gazeteciler (5187 sk, md 12; bkz. Roemen ve Schmit/Lüksemburg, B. No: 51772/99, 25/2/2003, § 46; Görmüş ve Diğerleri/Türkiye) avukatlar (Kruglov ve Diğerleri/Rusya § 125; Kırdök/Türkiye § 34, 50-51), mali müşavirler, hekimler (CMK md 45, 135/3, 136) gibi meslekleri gereği hassas bilgiler edinen ve bu nedenle tanıklıktan çekinme hakkına sahip kişilerin bilgisayarlarında inceleme yapılması halinde, çekinme haklarının hiçbir önemi kalmayacaktır. Bunun yanı sıra hâkimler/savcılar, avukatlar, noterler gibi özel soruşturmaya tabi kişilerle ilgili mekân araması (CMK md 116-119 ), gözaltı, yakalama gibi klasik koruma tedbirleri bazı şartlara bağlanmışken bilgisayarlarında arama hiçbir şarta bağlanmamıştır.

Nitekim Kırdök ve Diğerleri/Türkiye kararında AİHM, avukat bürosunda yapılan aramada el konulan bilgisayar ve flash bellekle ilgili Türk hukukunun bazı güvenceler vermediğine işaret etmiştir. Bunlardan ilki, avukat bürosunda yapılan aramada, arama kararının, aranan yerin özelliğini dikkate almadan hangi somut nesne ve belgelerin aranacağını belirtmeden tüm dijital verilere elkonulmasını emretmiştir. Dijital verilerin muhafazası için özel önlem alınmamıştır. Verilen hızlıca incelenmesi, geri iadesi, yok edilmesi ve gizliliğin korunması için yeterli yasal güvence bulunmamaktadır. Yasal düzenlemeler, avukat-müvekkil mahremiyetini koruma konusunda öngörülebilir değildir. Petri Sallinen/Finlandiya kararında AİHM, bilgisayara elkonulması ve bilgisayar üzerinde arama yapılmasına dair açık, erişilebilir, farklı yorumlara izin vermeyen kaliteli bir kanun olması gerektiğini ifade etmiştir.

CMK 134, genelde tüm vatandaşlar için özelde ise hassas meslekleri icra eden kişilerin verilerinin korunması için yeterli güvence içermemektedir.

iii) Klasik koruma tedbiri olan mekan aramasında, hakkında arama işlemi uygulanan kimsenin belge veya kâğıtlarını inceleme yetkisi, Cumhuriyet savcısı ve hâkime aittir (CMK md 122). Düzenlemenin amacı, belge ve kağıtlardaki suçla ilgisi olmayan kişisel verilerin korunmasıdır (bk Wieser ve Bicos Beteiligungen GmbH/Avusturya). CMK 122. maddedeki belge ibaresi, dijital belgeleri de kapsar. CMK 134. maddesi, ele geçen dijital belgeleri kimin inceleyeceğine dair açık düzenleme içermemektedir. Soruşturma konusu suçla ilgisi olup olmadığına dair bir ayırım yapılmadan, tüm dijital delillerin kolluk gibi herhangi bir soruşturma mercii tarafından incelenmesi, kişisel verilerin korunması açısından yeterli güvenceler içermemektedir.

iv) Bir veri veya veri depolama birimi, ilk sektörden son sektöre kadar kopyalandıktan sonra, adli kopyanın özet/hash değeri de hesaplanır. Hash değeri, veri üzerinde sonradan herhangi bir değişiklik yapılmasına engel olma amacıyla uygulanan bir tür dijital müdürdür. Klasik mekan aramasında CMK 119/4 madde, delillerin güvenilirliğini sağlamak için iki bağımsız gözlemcinin arama sırasında hazır olmasını zorunlu kılmaktadır (Bk Budak/Türkiye, Aydemir/Türkiye, Yaşar Yılmaz, B. No: 2013/6183, 19/11/2014). Hash değeri, adli kopyası alınan dijital verinin delil güvenliğini sağlayan en önemli unsurdur. CMK 134. madde, delil güvenliğini sağlama açısından hash değeri alma zorunluluğu içermediğinden veri ve delil güvenliğini sağlamaya elverişli güvenceler içermemektedir.

v) AİHM gizli tedbirlere ilişkin kanun hükümlerinin içermesi gereken asgari unsurları belirlemiştir. Bu kapsamda izleme kararı verilmesine yol açabilecek suçların niteliği; iletişimleri izlenecek kişi kategorisi, izleme sürelerinin sınırları, elde edilen verilerin inceleme,

değerlendirme ve saklanmalarına ilişkin esaslar, verilerin başkalarıyla paylaşılmasına ilişkin önlemler ve elde edilen verilerin ortadan kaldırılmasına ilişkin koşulların kanunda açık bir şekilde düzenlenmesi gereklidir (The Association hor European Iıntegrcıtion And Human Righls ve Ekimdzhiev/Bulgaristan, B. No: 62540/00. 28/6/2007, § 76, 77). Bilgisayarda arama, gizli icra edilen bir koruma tedbiri değildir. Ancak, bilgisayardan elde edilen kişisel verilerin önemi ve değeri, aynı ölçütlerin bilgisayarda aramada da uygulanmasını gerektirir. Adli kopya, tüm kurallara uygun alınmış olsa bile, saklanma şekli, saklanma süresi, inceleme süresi, verilerin ilgili kişiye iade edilmesi, adli mercilerde kalan kopyanın geri dönüşümü mümkün olmayacak şekilde imha edilmesi, suç olan unsurlarla olmayan unsurların ayrılması, suç teşkil eden verilerin geri döndürülemeyecek şekilde silinmesi kanunda düzenlenmemiştir. 135/3 ve 137 maddeler, kişiler verilerin kullanılması ve imhası yönünde insan haklarına uygun güvenceler içerirken, CMK 135. maddeye göre daha önemli veriler içeren bilgisayarlarda bu tür güvencelerin olmaması, başlı başına maddeyi yeterli güvencelerden mahrum bırakmaktadır.

vi) Bilgisayara elkonulduğunda, şüphelinin ya da ilgili kişilerin elkoyma ve bilgisayarda arama yapılmasına itiraz hakkının olmaması, incelenecek kişisel verilere daha en başından erişmeyi engelleme açısından önemli bir güvencedir. Kanun, açık bir itiraz yolu düzenlemediğinden yeterli yasal güvence içermemektedir.

AYM, 30.06.2022, 137/86 sayılı kararında, bilgisayarda arama kararına CMK 267 maddesi gereğince itiraz edilebileceğini ifade etmiş olsa bile (§ 379) Kanunda bu konu da açık bir düzenlemenin olması gerekir.

Hâkim kararları, genel olarak itiraz kanun yoluna tabidir. Maddede açık bir düzenleme olmamakla birlikte hâkim kararına itiraz edilebildiği varsayılsa dahi, madde, Cumhuriyet savcısının da bilgisayarda arama yapılmasına izin verebilmektedir. Cumhuriyet savcısı kararına itiraz yasa yolu düzenlenmemiştir. Bilgisayar gibi benzersiz kişisel verilere erişilmesine olanak sağlayan bir güvenlik tedbirine karşı ne hâkim kararına (Bk AYM, 30.06.2022, 137/86, § 379) ne de savcı emrine açıkça bir itiraz yolu düzenlenmemiş olması, bilgisayara el konulduğunda, henüz verilere erişilmeden, etkin bir itiraz yolunun kabul edilmemesi, maddenin yeterli güvenceleri sunmadığını göstermektedir.

vii) Bilgisayarda arama, bir koruma tedbiridir. Koruma tedbirinin hukuka uygun olmaması halinde hukukun üstünlüğünü koruyan demokratik bir devlet, tedbirin muhatabı olana kişiye tazminat ödemek zorundadır. AİHM, Kırdök/Türkiye kararında, bilgisayarda aramanın CMK 141/1-i maddesinde düzenlenen tazminat kapsamına girmediğini tespit etmiştir. Madde bu yönüyle de yeterli güvenceleri içermemektedir.

Uygulamadan Kaynaklanan Güvence Eksiklikleri

viii) Kanunun metni kadar metnin açık kaleme alınmamasından kaynaklanan uygulama sorunları da temel haklara müdahale kapsamında ele alınmalıdır.

CMK 134/2 maddede yer alan "işlemin uzun sürecek olması" ibaresi tam bir keyfiliğe neden olmakta, bu ibareden hareketle, soruşturma aşamasında adli kopya alınıp, hash değeri belirlenip adli kopyadan bir örnek ilgili tarafa verilmemektedir. Pek çok adli olaydan bilindiği üzere soruşturma makamları, bu konuda yeterli özeni ve hassasiyeti göstermemektedir. İşlemin uzun sürecek olması bahanesiyle dijital veri içeren bilgisayara, bilgisayar sayılan çıkarılabilir donanımlara (CD, flash bellek, harici harddisk gibi) elkonulmakta, daha sonradan elkonuluna eşya üzerinde rapor düzenlenmektedir. Davamıza konu olayda da böyle yapılmıştır.

AYM, 30.06.2022 tarih ve 137/86 sayılı kararında "işlemin uzun sürecek olması" ibaresini anayasaya aykırı bulmamıştı. AYM daha önceki kararlarında (Bk AYM 12.03.2009 tarih ve 106/54 sayılı karar; 12.03.2009 tarih ve 45/53 sayılı karar, 07.05.2009 tarih ve 22/55 sayılı karar, 20.05.2010 tarih ve 48/70 sayılı karar) CMK 231. maddeyi Anayasaya aykırı bulmamış, CMK 231/12 maddenin etkili bir iç hukuk yolu olduğunu değerlendirmişti (Bk (Asım Arı [GK] §§ 47-54). Ancak AYM, Anayasaya uygunluk konusunda bir normun sadece kendisini değil uygulamasını da dikkate alan son kararında (Bk AYM 20.07.2022, 121/88), normun yorum ve uygulamasının da yeterli anayasal güvenceler içermesi gerektiği sonucuna ulaşmıştır.

İşlemin uzun sürecek olması, soruşturma makamları açısından bir külfet gibi görünse de uzun sürse dahi adli kopya alma işleminin hukuka uygun olması, temel haklara yapılacak müdahalenin de hukuka uygunluğunu garanti eder.

CMK 134/2 maddedeki "İşlemin uzun sürecek olması" ibaresi, belirsiz ve kötüye kullanmaya uygun bir düzenlemedir. Uygulamada da kötüye kullanılmaktadır. İşlem ister uzun sürsün isterse sürmesin, soruşturma makamları, sanık açısından delil güvenliğini sağlamak zorundadır. İşlemin, gerçekten de katlanılamayacak kadar uzun sürmesi halinde, elkonulan bilgisayarın, ne kadar bir süre içinde, hangi şartlarda, kimin tanıklığında adli kopyasının ve hash değerinin alınıp inceleneceği de kanunda düzenlenmemiştir. Hem uygulamadaki kötüye kullanım hem de elkonulduktan sonraki işlemler açısından madde, yeterli güvenceleri sağlamamaktadır.

Yukarıda açıklanan nedenlerle;

CMK 134. maddesi, temel haklara ölçüsüz ve öngörülemez şekilde müdahale öngören, buna karşın kişisel verilere erişme, kişisel verilerin korunması, saklanması, imhası açısından yeterli güvenceler içermeyen bir madde olduğundan Anayasa'nın 2. ve 20. maddelerine,

Aykırı olduğundan iptali gerekir."