HUKUK DEVLETİNDE BİREYSEL GÜVENLİK EKSENİNDE BİLİŞİM TEKNOLOJİLERİ

Onur ÖZBEK[*]

Özet:

Bu çalışmanın temel hedefi, ilk aşamada, tarihsel süreç içerisinde zenginleşen hukuk devleti kavramının ve hukukun üstünlüğü ilkesinin, demokratik toplumlarda algılanış biçimlerini de göz önünde bulundurarak, doğuştan edindiği vazgeçilemez ana haklarla birlikte hayatını sürdüren bireyin karşısındaki yerini saptamak, daha sonra ise, devlet ile bizzat kişiyi ceza adaleti sisteminin yelpazesinde çarpıştırmaktır. Metodolojik olarak, konuya, bilişim suçları ve ortaya çıkarabileceği ceza muhakemesi hukukuna yönelik etkinlikler açısından yaklaşılmıştır. Buna ek olarak, ceza yargılaması sisteminde arama ve el koyma işlemleri olarak karşımıza çıkan koruma tedbiri biçimlerinin, bilişim sistemlerine hangi ilkelerle ve ne şekilde uygulanacağı incelenmiş, bu aşamada karşılaşılabilecek gerek teorik gerekse uygulama kaynaklı problemler için çözüm formülleri aranmıştır. Adli bilişim kavramı ve çalışma prensipleri yanında, incelenen temel konu olan koruma tedbiri, mukayeseli hukuk ve insan hakları açısından da değerlendirilmiştir. Orijinal, aktüel ve son derece tartışmalı bir önlem türü olan erişimin engellenmesi konusu da ihmal edilmemiştir.

Anahtar Sözcükler:

Hukuk devleti, insan hakları, bilişim teknolojileri, bilişim suçları (*cyber crimes*), adli bilişim (*computer forensics*), bilgisayarda arama ve el koyma, elektronik delil, yönetim hukuku, kolluk yetkileri, ceza muhakemesi, ceza adaleti (*criminal justice*)

[*] Polis Akademisi Güvenlik Bilimleri Enstitüsü Suç Araştırmaları Ana Bilim Dalı

HUKUK DEVLETİNDE BİREYSEL GÜVENLİK EKSENİNDE BİLİŞİM TEKNOLOJİLERİ

Giriş

Son yıllarda bilişim platformundaki teknolojik gelişmelere paralel biçimde, elektronik sistemler, gerek sosyal gerekse ticari yaşamda bireyler için vazgeçilmez unsurlar haline gelmiştir. Bilişim teknolojilerinin bu gelişiminin ve yaygınlığının bireylerin hayatını kolaylaştırması ve sosyalleşmelerini sağlaması gibi olumlu etkileri yanında, yeni suç tipleri yarattığı ve geleneksel suçların bilişim sistemleri yoluyla işlenmesinin önünü açtığı bir gerçektir. Günümüzde bilişim sahasında işlenen ve işlenebilecek olan suçların sayısı, bilişim teknolojilerinin hızlı gelişimi ile doğru orantılı olarak, küresel boyutta yadsınamayacak oranda fazlalaşma göstermektedir. Bu durağanlıktan son derece uzak gelişim devam ettikçe, mevcut suçların bilişim vasıtalarıyla işlenmesinin önünün açılmasının yanında, yeni suç tiplerinin ortaya çıkması dahi olasıdır. Anılan suç işleme tarzı, maddi veya manevi yarar sağlamak amacıyla ortaya çıkabilir; ayrıca, yasal düzlemdeki altyapı noksanlığı ve suçun niteliğinin gizlenmeye elverişliliği faili motive etmektedir.

Bilişim teknolojilerinin gelişmesine, adli bilişim metotları da kayıtsız kalmamaktadır; ne de olsa, ünlü Locard prensibine göre "her temas bir iz bırakır". “Delilden sanığa gitme” mottosunun modern ceza adaleti sistemlerinin temelini oluşturması, delil elde etmenin yargılama sürecindeki önemini vurgular; bu doğrultuda, adli bilişim yöntemlerinin ve ceza muhakemesi ilkelerinin denkleme uygun biçimde yerleştirilmesi zorunluluğu açığa çıkmaktadır. İşte tam da bu aşamada, devreye bilişim suçlarına (siber suçlar - *cyber crimes*) hasredilmiş maddi ceza hukuku normları ile ceza muhakemesi ilkeleri girmelidir.

Genel ve klasik ceza yargılaması prensiplerinin, bir anda ortaya çıkmış ve sosyal yaşamla bütünleşmiş bu yeni suç modeli ile ilgilenirken onunla baş etmekte yetersiz kalacağından hareketle, anılan suç modeline özgü bir takım özel ceza adaleti (*criminal justice*) normları belirleme ve bunları etkin bir biçimde uygulama zorunluluğu doğmuştur. Bu amaçla, adli bilişim (*computer forensic*) kavramının üzerinde durmak ve onun denklemdeki uygun yerini bulup yerleştirmek gerekmektedir. Adli bilişim, bu noktada devreye girerek, olası delil kabul edilen doneye herhangi bir zarar getirmeksizin, onu ceza yargılaması mekanizmalarına sunma fonksiyonunu üstlenir. Öyle ki, somut bir olayda maddi sorunu çözebilecek tek delil, belki de incelenen dijital delildir. Ona bir nedenle ulaşılamadığı veya uzmanlaşmamış personelce adli bilişim prensiplerine uygun hareket edilmediği durumlarda şüpheden sanık yararlanabilir; söz konusu sanık, bilgisayar teknolojilerine merak salmış yaramaz bir çocuk olabileceği gibi, çocuk istismarcısı bir sapkın da olabilir.

I. Ceza Muhakemesi Açısından Birey – Devlet Çatışması

Ceza adaleti sisteminin gözle görülen ana hedefi, her ne kadar suç soruşturması da azade olmamak üzere yargılama yaparak maddi gerçeği açığa çıkarıp buna

uygun cezayı saptamak ve uygulamak biçiminde karşımıza çıkıyor olsa da, bu amaca ulaşmakta insan hakları nosyonunun çizdiği sınırın dışına çıkılmaması başat şarttır. Hukukun ve üzerinde yükseldiği prensiplerin ne pahasına olursa olsun askıya alınmaması gerekir. Maddi gerçeğin ortaya çıkarılması mutlak ve istinasız bir amaç değildir; bu yolda temel hak ve özgürlüklere dokunmamak asıldır. Toplum - hukuk dengesini sağlamakta rol oynayan üç organdan bahsedilmiştir: uzmanlaşmış yazılı kural koyucu, gerektiğinde kural koymakla görevli yargı, hukuk kuralları ile mahkeme kararlarını uygulamakla görevli icra – infaz organları ve polis örgütlenmesi (Gürkan, 1994: 75-76). Üç organ da birbirlerinden kalın duvarlarla ayrılmış olmalı, ihtiyaç duyulduğunda açılacak pencerelerle fikir ve uygulama alışverişinde bulunabilmeleri sağlanmalıdır. Ufacık bir yetki gaspının veya bir oluşumun diğerinin haklarına sahip olduğu mülahazasıyla hareket etmesinin doğuracağı sonuçlar telafisi güç kayıplara gebedir.

Toplumsal barış ve güven ortamı olarak ifade edilen kamu düzeni nosyonu, güvenlik, dirlik ve esenlik, sağlık unsurları ile temellendirilmiştir (Gözübüyük, 2002: 270; Günday, 1998: 193-194). Yönetimin birincil görevi olan kamu düzenini (*public order*) korumak, bu şekilde kişilerin güvenli ve huzurlu bir ortamda hayatlarını sürdürmelerini sağlamak, amacıyla gerçekleştirdiği faaliyetler "kolluk faaliyetleri" olarak adlandırılır (Günday, 1998: 191). Yönetimin adı geçen yetkisi, temel hak ve özgürlüklerin bazı koşullarda[1] sınırlanabilmesi yanında, kişilere talimat verilebilmesi ve yasak uygulanması biçiminde genişlemektedir ki, bu noktada kolluk faaliyeti gören "idare" ile bireyler ve topluluklardan oluşan "kişiler", insan hakları bağlamında karşı karşıya gelip yarışmaktadır (Günday, 1998: 191). Burada birbirleriyle çarpışan ve sağlıklı bir ceza adaleti sistemi için dengelenmesi gereken fikirler "*crime control*" (suçu önlemeliyiz!) değerleri ile "*due process*" (kişi hak ve özgürlüklerini ön planda tutmalıyız!) modelidir: crime control nosyonu, kişi hak ve özgürlüklerinden ödün vermek pahasına olsa dahi suçun önlenmesini birincil amaç olarak kabul etmiş iken, due process tip, bireyi temel değer kabul ederek kolluktan ziyade hâkim ve savcıya güvenmekte ve bir kişinin özgürlüğünün dahi bütünüyle kamunun menfaati için feda edilemeyeceği düşüncesini benimsemektedir (Eryılmaz, 2006: 208-209). İki sistem arasında denge kurulamayıp birinci anlayışın esas alındığını düşünürsek suçla mücadele edebilmek pahasına kişi hak ve özgürlükleri savunmasız kalabilecek, ikinci anlayışa eğilim ise suçla mücadele açısından kolluğun başarısız olması ve suç oranlarının artması tehlikesini doğurabilecektir. İlk durumda bireyler kolluktan, diğerinde ise suçlulardan korkar olacak, her iki uçta da kişiler kendilerini güvende hissetmeyecek, sonuç olarak kişinin en iyimser bakış açısıyla "korku duymama hakkı" (Eryılmaz, 2003: 40) zedelenmiş olacaktır. Gerçekten de, polis baskısının sokaklarda hissedilmesi suç oranlarını aşağıya çekebileceği gibi, vatandaşların bu durumdan huzursuzluk duymalarına da yol açabilir (İçli, 2007: 432).

Olası kişisel hak kayıplarının gerçekleşmesini önlerken, aynı zamanda doğal bir sosyal olgu olarak kabul edilen suç ile başa çıkmak için *due process – crime*

[1] Temel hak ve özgürlükler, anayasada öngörülen nedenlerle, mutlaka yasama erkince yapılan bir kanunla, özlerine dokunulmaksızın ve ölçülülük ilkesi ışığı altında kısıtlanabilir; sınırlama, anayasanın lafzına ve ruhu ile demokratik ve laik toplum düzenine aykırı biçimde yapılamaz (Anayasa m.13).

control çatışması konusunda, toplumsal değişkenler de göz ardı edilmeksizin, denge sağlanması ve buna yönelik düzenlemelerin yasal düzleme oturtulması gerekmektedir. Kolluğun henüz ilk aşamada suçun işlenmesini önleme, daha sonra ise işlenmiş suçları araştırarak ceza adaleti sistemini aydınlatma biçiminde iki ayaklı bir görev ve buna bağlı yetki yapılanması vardır. 1 Haziran 2005 tarihinde yürürlük kazanan 5271 sayılı Ceza Muhakemesi Kanunu ile adli kolluk sistemine geçilmiş ve kolluğun adli yetkilerini ayrı bir teşkilatlanma ile yürütmesi fikri yasal düzleme oturtulmuştur. Adli kolluk (suç kolluğu), işlendiği varsayılan bir suçun gerçekten işlenip işlenmediğini araştıran, bir suç şüphesi ile faaliyetine başlayan, delil toplama ve değerlendirme konusunda uzmanlaşmış, iz bilimi (kriminalistik) prensipleri ile çalışan, sorgu taktikleri kullanan, suçla mücadele ile ceza muhakemesi ve insan haklarını özümsemiş teknik bir kolluk ünitesidir (Öztürk ve Erdem, 2006: 322-323; Öztürk vd,2004: 103-104). Kolluğun aslında özü itibariyle teknik bir konu olan suç soruşturmasını kural olarak bizzat yürüttüğü ve savcının adeta bir "danışman" konumunda olduğu Anglo-Amerikan ceza adaleti sistemi yanında, Kıta Avrupası'nda, terör suçları ve organize suçlar gibi belirli ağırlığı olan soruşturmalar dışında, suçu aydınlatma işi kolluk güçlerine hasredilmiştir (Eryılmaz, 2006: 217). Yasanın önünü açtığı adli kolluk teşkilatlanmasının sağlıklı biçimde yaygınlaşmasının sağlanabilmesi için eğitimli ve uzmanlaşmış personel yanında, teknolojik gelişmelere paralel biçimde teknik malzeme gereksinimlerinin karşılanması zorunluluğundan söz edilmektedir (Öztürk ve Erdem, 2006: 324; Öztürk vd,2004: 104).

Kolluk güçlerinin insan haklarını ihlal ettiği durumlarda iki temel mesleki amacı olduğu görülmektedir (Bıçak, 1999: 15-27): suçlu varsaydığı kişileri cezalandırmak ve delil elde etmek. Modern ceza adaleti sistemlerinden hiçbirinin kolluk güçlerine suçluları cezalandırma konusunda herhangi bir yetki tanımamış olmasının yanında, kolluğun görevi ve aynı zamanda soruşturma aşamasının ana hedefi olan delil elde etme sürecinde de insan haklarına saygılı biçimde hareket edilmelidir (Bıçak, 1999: 15-27). Kolluğa anayasa ve yasalarca tanınmış her bir yetki, temel hak ve özgürlüklerle yakın temas halindedir. İnsan hakları düşüncesinin doğurduğu kişi özgürlüklerinin, kolluğun yetkileri karşısında son derece kırılgan bir morfolojisi olduğu açıktır. Diğer bir açıdan bakıldığında ise, suç ve suçlu ile etkin bir savaşım veremeyen ceza adaleti sistemlerinin, sosyal yaşamda kaotik bir ortamın ortaya çıkmasına sebep olması kaçınılmazdır.

Hukuk devleti, hukukun her durumda hesaba katılabilirliği, hukukun güvenilirliği ve tüm devlet gücünün hukuka dayanması temellerinden yükselmektedir (Doehring, 2002:214). Devlet gereği tarafını tutan fikir çevreleri, devletin başat amacının güvenliği sağlamak olduğu, bu amaca ulaşılamazsa direnme yasağının tek istisnasının gerçekleşmiş olacağı ve böylece hükümdara başkaldırabilme hakkının ortaya çıkacağı tezinin sahibi olan toplum sözleşmecilerinden Thomas Hobbes'a atıf yapmışlardır. Hukukun ve insan haklarının üstünlüğünü savunan görüş ise, diğer bir toplum sözleşmecisi John Locke'un devletin görevinin özgürlükleri pekiştirmek ve insan onuruna aykırı hareket etmemek olduğu gerekçesiyle, insan haklarının mutlak ve sınırsız niteliğini

düstur kabul etmişlerdir. Birçok açıdan, oy hakkının hukuk devleti[2] yönünde kullanılması tutarlı bir seçim olacaktır ki, devlet gereği kavramı hukuk devletine oranla daha az gözle görülür ve elle tutulurdur. Hukukun üstünlüğünün hüküm sürdüğü hukuk devletinde (insan haklarına dayalı devlet[3]), insan hakları düşüncesi, yasa önünde eşitlik, yasasız suç ve ceza olmaması (*nullum crimen nulla poena sine lege*), çifte cezalandırma yasağı gibi birçok ilke somutlaşmış durumda bulunmaktayken, devlet gereği anlayışı (hikmeti hükümet – *reason of state* – *raison d'etat*) ise ideolojik morfolojisi itibariyle hem kişiden kişiye otoriteden otoriteye değişebilir hem de zamana karşı duyarlıdır.

Temel hak ve özgürlükleri kamu düzeninin sağlanması amacıyla sınırlayan, parlamentonun çıkardığı genel ve objektif nitelikli yasalara "kolluk kanunları" denir; idare, yönetsel kararlar eliyle bu yasaları kişilere uygulayıp kolluk faaliyetinde bulunarak kamu düzenini korumakta ve kamu düzeni ile bireysel özgürlükler arasında denge kurmaya çabalamaktadır (Günday, 1998: 192). İdarenin, anayasal esaslar ışığında kolluk kanunlarını uygulayarak temel hak ve özgürlüklere müdahale etme yetkisi vardır ki, bu yetki "kolluk yetkisi" olarak adlandırılır; idarenin kendisine tanınmış bir yetki bulunmaksızın temel hak ve özgürlüklere müdahalesi "fonksiyon gaspı"na yol açacaktır (Günday, 1998: 206). "Yönetimin yasalara uygun düşmesi prensibi"ne göre, bir hukuk devletinde idarenin hareketleri, ancak yasalar ve elbette anayasanın açıkça çizdiği yetki sınırlarından taşmıyorsa meşru sayılır (Doehring, 2002: 435-436).

Kamu düzeninin korunması için başvurulan kolluk faaliyetlerinin asıl amacının kamu yararını sağlamak olduğundan hareketle, demokratik bir rejimde bireysel ve özel yararlar ile bunların ifade edilmesi kolluğun faaliyet alanı dışında kalmalıdır; esas olarak, bireyin konutunda ve işyerindeki yaşantısı ile içsel ahlaki anlayışı ve yaşam tarzının kamusal çıkarlarla ilgisi olmaması nedeniyle, idari kolluğun bu sahaya müdahale etmemesi gerekir (Gözübüyük, 2002: 270; Günday, 1998: 192). Bireyin kamudan ayrık tuttuğu özel düzeninin, kamu düzenine aykırılık teşkil etmediği sürece, dokunulmaz olması asıldır. Bu aykırılığın unsurlarının net çizgilerle saptanamaması, tıpkı totaliter yönetimlerde görüldüğü gibi keyfiliğe ve böylece insan hakları ihlallerine yol açacaktır. "Siyasal tarafsızlık ilkesi", devletin, ilişkili olduğu azınlık veya çoğunluk üyesi her bireyin dünya görüşlerine, inançlarına, ideolojilerine eşit mesafede durması, kısaca hiçbir "iyi" anlayışını "kötü"lememesini ifade eder; bu prensip tanınmaz ise, "tek doğru" dayatması ile tehlikeli bir biz – onlar kutuplaşması açığa çıkabilir. (Arslan, 2005: 234).

Yüce bir değer olan insan onuru, kişiye bilinçli bir şekilde kendi kaderini ve yaşamayı dilediği çevreyi özgürce belirleme yeteneği vererek kişiliksizliği ortadan kaldıran manevi güç, kısaca hür irade olarak ifade edilmektedir (Öztürk vd, 2004: 34). Eğer iradeyi tamamen çevresel şartların yönlendirdiği savunulursa, insan sadece sebep – sonuç ilişkisi içerisindeki bir varlık olarak kalır; oysa insan, sağlıklı

[2] ABD Yüksek Mahkemesi'nin (1801-1835 dönemi Marshall Mahkemesi) 1803 tarihli meşhur Marbury v. Madison kararında hukuk devletine, "bireylerin değil hukukun hükümeti" (*government of law and not men*) tanısı koyulmuştu.

[3] 1982 Anayasası'nın lafzı (m.2) "insan haklarına saygılı devlet" biçimindeyken, 1961 Anayasası (m.2) bu ilkeyi "insan haklarına dayanan devlet" olarak tanımaktaydı.

ise, akıl sahibidir ve özgür iradesi ile içinde bulunduğu şartlara etki etme, bunları değiştirebilme gücüne sahiptir (Soyaslan, 2003: 39). En üstün ahlaki talepler olan insan haklarının korumaya çalıştığı başat değer de işte bu özgür irade temelinden yükselen insan onurudur. Her ne kadar idari kolluğun görevi toplumun maddi dışsal uyumunu korumak olsa da, yasalar, bireyin özel yaşam tarzının dışavurum biçimini kolluk faaliyetlerinin uygulama alanına sokabilir; ancak herhangi bir müdahale için, gerçekleştirilen davranışın kamu düzenini olumsuz etkilemeye yönelik açık ve yakın bir tehlike niteliği taşıması gerekmektedir[4]. Bireyin eylemi, kamusal uyumda gözle görülür biçimde ve yakın bir zamanda karışıklık meydana getirmeyecek ise, kolluğun olası bir müdahalesi "yetki aşımı" yaratır (Günday, 1998: 193). Bireyin kendi habitatında benimsediği özel içsel görüşleri, ancak bunların dışavurumunun kamuyu rahatsız edeceği noktada kolluğu ilgilendirir; kolluğun yetkisi o noktada başlar. Bu denklem, polisin önleyici nitelikli görevlerini işaret eder; amaç ise, bir suçun işlenmemesini ya da bir tehlikenin önüne geçilmesini sağlamak adına önlem almaktan ibarettir (Centel ve Zafer, 2005: 114).

Adli yetki kullanımı sırasında kolluğun işlediği bir suç söz konusu ise, Cumhuriyet Savcısı tarafından genel yargılama normlarına göre hareket edilerek doğrudan soruşturma yapılacaktır (CMK m.161/5). Karşılık olarak, suça karışan kolluk mensubuna idari görev gördüğü izafe edilebiliyor ise, Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun[5] uyarınca, soruşturmaya başlanabilmesi için idari izin verilmesini bir dava şartı olarak kabul edilen mekanizma, kısaca izin sistemi, uygulanacaktır (CMK 161/5). En üst dereceli kolluk amirleri açısından, hâkimlerin görevlerinden dolayı tabi oldukları muhakeme usulü işletilecektir (CMK m.161/5). Ayrık tutulan ağır cezayı gerektiren suçüstü durumunda ise, yargılama prensibini belirlemek için genel normlara gidilir. Özellikle, devletin egemenliğine tabi tüm kişilerin tek ve bağımsız bir yargılama gücüne bağlı olduklarını öngören "yargılama birliği" ilkesine aykırılık teşkil etmesi ve "iddianamenin iadesi" kurumunun da ceza muhakemesi sürecine entegre edilmiş olması gerekçeleriyle anılan yasa eleştiriye uğramıştır (Kunter ve Yenisey, 2005: 30-31).

II. Bilişim Sistemlerine Yönelik Koruma Tedbiri Uygulamaları

A. Ceza Muhakemesi Kanunundaki Kapsam

Uygulama alanı bilişim sistemleriyle sınırlı olan bu *sui generis* koruma tedbiri, ilk kez 5271 sayılı Ceza Muhakemesi Kanunu (CMK m.134) ile pozitif hukukumuza angaje olmuştur. Anılan aktivitenin, arama ve el koyma koruma tedbirlerinin özel bir hali olması nedeniyle, yasa sistematiği içinde bu önlemlere ilişkin kısımda düzenlenmesi yerinde görülmüştür (Centel ve Zafer, 2005: 309). Ancak yine de, bilgisayara yönelik arama ve el koymanın ayrı bir koruma tedbiri biçimi olarak mülahaza edilmesi gerekir (Özbek ve Bacaksız, 2006: 146).

---

[4] Bir örnek (PVSK m.8/C): "…mevzuata aykırı faaliyet gösteren genelevler, birleşme yerleri ve fuhuş yapılan evler ve yerler…faaliyetten men edilir."

[5] Anılan yasanın ilga ettiği Memurin Muhakematı Hakkında Kanunu Muvakkat ise, kural olarak, soruşturmanın bütününün idarece yapılacağını öngörmekte idi.

Türk Ceza Kanunu'nda yer alan bilişim suçları[6] yanında, bilişim sistemleri aracılığıyla işlenebilecek diğer suç tipleri, haberleşmenin engellenmesi (TCK m.124), hakaret (TCK m.125), hırsızlık (TCK m.142/2/e – nitelikli hal), dolandırıcılık (TCK m.158/1/f – nitelikli hal), müstehcenlik (TCK m.226), vs. şeklinde sayılabilir. Bunların dışında, Fikir ve Sanat Eserleri Kanunu'nda ve Elektronik İmza Kanunu'nda da bilişim suçu tiplerine rastlamaktayız.

Bilgisayarlarda arama ve el koymaya ilişkin koruma tedbiri, sadece adı geçen bilişim suçlarına yönelik soruşturmalarda değil, pozitif hukukun öngördüğü her türlü suç için yapılan soruşturmada başvurulabilecek bir önlem tarzıdır. Zaten yasa bu özgürlük alanının çerçevesini, bizzat seçtiği "bir suç dolayısıyla yapılan soruşturma" lafzıyla çizmiştir. Sonuç olarak, tedbirin başat amacı olan elektronik olsun ya da olmasın bir delile ulaşmak, hem bilişimle ilişkili suçlar hem de klasik suçlarla mücadele esnasında gerçekleşebilecektir.

Bilişim teknolojisindeki gelişmelerin sosyolojik ve kriminolojik izdüşümleri, yeni suç tipleri ortaya çıkmaktadır; bu suçların da ortak özelliği, sübutlarının ancak elektronik delil (dijital delil) sayesinde sağlanabiliyor olmasıdır. Bilgisayarların araç olarak kullanıldığı yeni nesil internet suçlarının başında çocuk pornografisi gelmektedir (Kunter ve Yenisey, 2005: 423). Böylece, belirtildiği gibi sırf elektronik delil ile aydınlatılabilen postmodern bir suç tipi gün yüzüne çıkmakta, bu açıdan ceza adaleti sistemi bu çeşit suçların takibinde izlenecek yöntemleri ve onlarla mücadele açısından kurulması gereken mekanizmaları düzenleyecek, adli bilişim tekniklerinden azade olmayan, en önemlisi de insan haklarına dayanan, bir öğretiye gereksinim duymaktadır.

Bilgisayarlara, dolayısıyla içerdiği her türlü program ve veri tabanına, uygulanacak arama ve el koyma işlemleri yasaca sıkı koşullara bağlanmıştır; arama işlemi için gözetilecek koşullar şu şekilde sıralanabilir:

- Bir suç nedeniyle yapılan soruşturmanın başlanmış ve sürdürülüyor olması,
- Başka şekilde delil elde etme olanağının bulunmaması,
- Cumhuriyet savcısının istemi üzerine hâkimin buna yönelik değerlendirmesinde olumlu karar vermesi,
- Aranacak bilgisayarı şüphelinin kullanmış olması,
- Suç şüphesinin bulunması

Yukarıdaki koşullar sağlandığı takdirde, arama yapılmasının yanında, bilgisayar kayıtlarından kopya çıkarılmasına ve bu kayıtların çözümünün yapılarak metin haline getirilmesine de zemin hazırlanmış olur. Ancak buraya kadar sayılan şartların gerçekleşmesi, el koyma aktivitesi için yeterli değildir. El koyma işlemi için, usulsüz uygulanması sonucunda doğabilecek olası hak ihlalleri nedeniyle, arama tedbirine kıyasla daha katı şartlar gözetilmiştir. Gerçekten de, el koyma

[6] Bilişim sistemine girme ve sistemde kalma (TCK m. 243), bilişim sisteminin işleyişini engelleme veya bozma (TCK m. 244/1), bilişim sistemindeki verileri yok etme veya değiştirme (TCK m. 244/2), bilişim sistemi aracılığıyla haksız çıkar sağlama (TCK m. 244/4), banka veya kredi kartlarını kötüye kullanma (TCK m. 245), kişisel verileri kaydetme (TCK m.135), kişisel verileri hukuka aykırı olarak ele geçirme veya yayma (TCK m.136), kişisel verileri yok etmeme (TCK m.138), haberleşmenin gizliliğini ihlal (TCK m.132)

önlemine başvurabilmek için, aramanın gerçekleşmiş koşullarının varlığı yanında şu durumlardan birinin de somut olayda bulunması gerekir:

- Şifrenin çözülememesi nedeniyle bilgisayara girilememesi ya da
- Gizlenmiş bilgilere ulaşılamaması.

Bu iki alternatif şart dışında el koyma tedbirine başvurulamayacağı gibi, çözüm ve kopyalama işlemleri sona erdiğinde tedbire maruz kalan eşya zaman kaybetmeden ilgilisine geri verilecektir (Öztürk ve Erdem, 2006: 567). Veri aranacak bilgisayar, şüpheli dışında, üçüncü kişilere veya resmi bir kuruluşa da ait olabilir; yasada bu konuda herhangi bir sınırlama göze çarpmamaktadır (Centel ve Zafer, 2005: 309). Bilgisayarın kime ait olduğunu, başka bir anlatımla elektronik taşınır malın malikini araştırmanın önemi yoktur. Odaklanılacak nokta, bilgisayarda bırakılan soruşturmayı aydınlatacak izlerdir.

Yasanın düzenlemesindeki şifre (*crypto*) tanımının sağlıklı bir biçimde saptanamaması eleştirilmelidir. Kastedilen şifre, işletim sisteminin (söz gelimi Windows'un) giriş parolası ise, incelemeye başlayabilmek için bu şifre adli bilişim yöntemleri açısından herhangi bir engel teşkil etmemektedir (Şen, 2006: 382). Bunun sebebi, adli bilişimde incelemenin işletim sistemi üzerinden yapılmaması, dolayısıyla işletim sistemine girmeden de istenilen verilere kolayca ulaşılmasıdır. Ancak yukarıdaki açıklamalar, Windows işletim sistemi ve sürümlerine ilişkin olup, Linux tabanlı yazılımlar veya özel olarak veriye ulaşmayı engellemek amacıyla yazılmış şifreleyici bilgisayar programları açısından geçerli değildir; bu durumda şifre çözümü daha uzun zaman alabilmektedir. Son derece yaygın bir biçimde kişisel ve kurumsal bilgisayarlarda kullanılan Windows yazılımları, algoritmik yapıları itibariyle veriye ulaşma yollarını engelleme konusunda korumacı değildir; fakat yine de, gizlenmiş bilgilere ulaşmak, adli bilişim metotları uygulanmaz ise, çok da kolay olmayacaktır. Karşılık olarak, kişiye esnek bir işletim sistemi sunarak geniş bir dijital çalışma alanı sunan profesyonel yazılımlar veya sırf veri saklamaya özgülenmiş programlar adli bilişimcileri veriye ulaşabilme açısından zorlayabilir. Olay yerinde profesyonel davranış biçimleri ve teknikler kullanılması, bu sakıncayı giderecektir.

Arama ve el koyma koruma tedbirinin en önemli şartı suç soruşturması esnasında somut olayda başka surette delil elde etme olanağının olmamasıdır. Tedbire başvurulabilmesi için suçun işlendiğine dair herhangi bir şüphe derecesi yasada öngörülmediğinden, en düşük şüphe derecesi olan basit şüphe dahi yasaca yeterli kabul edilmiş olmaktadır (Centel ve Zafer, 2005: 310). Bu bağlamda, yasanın lafzında bulunmayan, fakat ruhundan (*ratio legis*) çıkarılan, suç şüphesinin var olması koşulu, her ne kadar şüphenin derecesi konusu tartışmalı olsa da, doğal bir şart olarak karşımıza çıkmaktadır. Şüphe kavramı, yoğunluk dereceleri bakımından aşağıdan yukarıya doğru basit, makul, kuvvetli ve yeterli şüphe biçiminde sınıflandırılmıştır; yeterli şüphe, kamu davasının açılmasını mümkün kılacak yoğunlukta bir kuşkuyu işaret eder (Eryılmaz, 2000, 71-75). Yasanın, telekomünikasyon yoluyla gerçekleştirilen iletişimin denetlenmesi (CMK m.135) için kuvvetli şüphe arayıp, bilgisayarda aramaya yönelen bir şüphe yoğunluğu öngörmemesi son derece sakıncalıdır ki, iki durum arasında özel hayatın gizliliği açısından denklik olduğu açıktır. Aynı şekilde, bir cep telefonu somut olaya göre

bilgisayar işlevi görmüş olarak değerlendirilebiliyorsa, yasanın bilgisayarda arama ve el koymaya ilişkin hükümleri uygulama alanı bulmalıdır.

Görüldüğü gibi, bu nevi şahsına münhasır koruma tedbirine kovuşturma evresinde başvurulması mümkün değildir; yasa burada, arama ve el koymanın çerçevesini sadece soruşturma aşamasına ilişkin olarak çizmiştir. Gerçekten de, aleni bir duruşmada mahkemenin arama ya da el koymaya karar vermesi durumunda, tedbirden haberdar olacak kişilerin kayıtları yok etmeleri ihtimali doğabileceği sebebiyle, kovuşturma aşamasında tedbirden öngörülen fayda sağlanamayabilir (Centel ve Zafer, 2005: 310). Her ne kadar maddi ceza hukuku, gerçeğin ortaya çıkmasını engellemek amacıyla, bir suçun delillerini yok eden, gizleyen, değiştiren veya bozan kişinin altı aydan beş yıla kadar hapis cezası ile cezalandırılacağını öngörmüşse de (TCK m.281/1), yukarıdaki savın ışığı altında tedbirin soruşturma evresine hasredilmesi yerindedir. Bir adım daha ileri gidersek, maddi gerçeğe ışık tutmak gayesiyle, tedbire karar verilecek duruşmanın kapalı yapılmasına mahkemece karar verilmesi suretiyle (CMK m.182/2), tedbirin kovuşturma aşamasında da uygulanmasının önünün açılması ve böylece muhakemenin daha sağlıklı bir biçimde işlemesine olanak tanınması çözümünden bahsedilebilir. Ancak mevzuatta, duruşmanın aleni olduğunu öngören düzenlemenin (CMK m.182/1) istisnaları, genel ahlak veya kamu güvenliğinin kesin olarak gerekli kıldığı durumlar biçiminde sınırlandırılmıştır.

Bilgisayarlara yönelik aramanın ve özellikle el koymanın ortaya çıkarabileceği sonuçlar temel hak ve özgürlükler başta olmak üzere şahısların ticari, kişisel, mülki statüleriyle yakın temas halindedir. Öyle ki, bu düzlemde hak ve özgürlükler, anılan tedbirle çok kolay bir biçimde ihlale maruz kalabilecek, telafisi güç veya olanaksız olumsuzluklar yaratabilecektir. Sadece bilgisayarla iş yapan, söz gelimi bir bankanın veya şirketin bilgisayarlarına el koyma tedbirinin uygulanması demek, o müesseseyi iş yapamaz hale sokacak, hatta işlemin uzaması halinde müessesenin batması dahi söz konusu olabilecektir (Öztürk ve Erdem, 2006: 566). Bu durum, tedbirin, özellikle el koymanın, katı koşullara bağlanmasını haklı kılmaktadır. Her halde, yasaya aykırı arama ve el koyma nedeniyle maddi veya manevi zarar gören kişiler devletten tazminat isteyebilecektir (CMK m.141). Hakkındaki arama kararı ölçüsüz bir biçimde gerçekleştirilen kişi yanında, bilgisayarına koşulları oluşmadığı halde el konulan, bilgisayarının muhafazası için gerekli önlemler alınmayan, bilgisayarı amaç dışı kullanılan veya zamanında iade edilmeyen kişi de yasada öngörülen şartlara riayet ederek tazminat isteminde bulunabilir (CMK m.141/1/i, CMK m.141/1/j). Usule aykırı el koyma ile görevi kötüye kullanma (TCK m.257) veya muhafaza görevini kötüye kullanma (TCK m.289) suçları da oluşabilir.

Bilgisayarın, bireylerin hayat tarzlarının önemli bir parçası haline gelmesinin yanında, ticari yaşamda da son derece etkin bir biçimde kullanılmaya başlamasından hareketle, el konulacak şeyin aslında kişinin özel ve ticari yaşamı olarak algılandığı gerçeğini hatırlamak gerekir. Etkin biçimde bilgisayarla çalışan, onsuz adeta bir hiç olan müesseselerin tedbir sonucu ortaya çıkacak görece kayıplarının, işyerinin çalışamaz hale gelmesine veya kapanmasına yol açabileceği

ihtimali göz önünde bulundurulmalıdır. İnternet toplu kullanım sağlayıcıları (internet kahveleri) bu çeşit işyerlerine güncel bir örnek teşkil etmektedirler[7]. El konulan eşyanın gecikme olmaksızın iade edilmesi kuralı, işletmenin ticari yaşamına devam edebilmesini sağlamaktadır. Ancak bu aşamada, kişiye ait bilgisayarda suç eşyası kapsamında değerlendirilebilecek veriler varsa, tıpkı uyuşturucu madde, bomba, ruhsatsız silah, vs. bulunmasında olduğu gibi, bu veriler kişiye iade edilmeyecektir; örneğin, başkasına ait kredi kartı bilgileri ya da çocuk pornografisi unsurları elbette geri verilmeyecektir (Şen, 2006: 378-379).

Her ne kadar arama ve el koyma koruma tedbirlerinin bilgisayarlara uygulanmasıyla, tahmin edileceği gibi birçok kişisel bilgiye ulaşılması mümkün olsa da, kişinin gerek pozitif hukukça gerekse doğal hukukça korunan dokunulamayacak kalkanları vardır. İşte bu durum eşyanın tabiatına uygun şekilde, tedbirin uygulanabilme şartlarını katılaştırmıştır. Fail olduğu tahmin edilen kişideki varsayımsal suçluluk özelliklerinin şüphelide bulunup bulunmadığının tespiti amacıyla, şüphelinin kendisinin veya üçüncü kişilerin bilgisayar verilerine el konulabilmesi için bazı suçların işlendiği konusunda esaslı dayanak noktalarının varlığının gerektiği savunulmuştur (Centel ve Zafer, 2005: 311). Başka bir anlatımla, bu tedbire keyfi bir biçimde başvurulmamalı, belirtilmiş şartlara sıkı sıkıya uyulmalı, hatta belirli ağırlıktaki tahdidi suçlarda (katalog suç – çerçeve suç – sayılı suç) ve belirli yoğunluktaki şüphenin varlığı ile uygulanması sağlanmalıdır. Daha önce de belirtildiği gibi, mevcut yasa düzenlenmesi, tahdidi sayımın aksine, her türlü suça ilişkin olarak bu tedbirin uygulanabileceğini öngörmüştür; yeter ki, o suçun soruşturması başlamış ve sona ermemiş olsun. Bunun yanında, yine yasa hükmünde şüphe derecesinden, hatta şüpheden dahi, bahsedilmediği için uygulamada tedbirin keyfi biçimde kötüye kullanılmasının yaratacağı sakıncaların da üzerinde durmak gerekmektedir. Çünkü böyle bir keyfilik, genel bakımdan, suçla mücadele açısından toplumun çok küçük bir bölümünü oluşturan suçlulara temas etmeye çalışırken, aslında suçtan doğrudan veya dolaylı olarak zarar gören suçsuz çoğunluğun gereksiz ve haksız yere rahatsız edilmesine neden olabilecektir (Eryılmaz, 2003: 40).

Arama ve el koymanın uygulanmasının esas itibariyle hâkim kararına bağlı tutulmasının bu tedbirlere yargıç güvencesi kazandırdığı teorisinden hareketle, tatbikatta bu kararın hâkimlerce matbu form biçiminde kullanılması, kararda somut gerekçe gösterilmemesi ve tedbirin gerçekten zorunlu olup olmadığının belirtilmemesi eleştirilmektedir (Sevimli, 2007: 995). Oysa genel anlamda arama kararında, el konulmak üzere aranan eşyanın açıkça tanımlanması, ilgili suçun belirtilmesi ve aramanın geçerli olduğu sürenin yazılması gerekmektedir (Özbek ve Bacaksız, 2006: 178). Amerika Birleşik Devletleri Yüksek Mahkemesi (Supreme Court), Andresen & Maryland[8] davasında uygulanması beklenen tedbirin kesinlikle arama kararında çizilmiş sınırlar dışına taşamayacağına, Arizona &

[7] Bu konuda bkz. söz konusu işletmelerin sorumluluk, yükümlülük ile denetimlerinin usul ve esaslarını düzenleyen ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun uyarınca hazırlanan 1 Kasım 2007 yayım tarihli İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik.

[8] 427 U.S. 463 (1976) 74-1646

Hicks (1987) ve Horton & California[9] davalarında ise kolluk kuvvetlerinin arama kararında belirtilen amaç ve sınırla bağlı olduklarına hükmetmiştir (Sevimli, 2007: 999).

Yasa uyarınca, bilgisayara el koyma işlemi esnasında, sistemdeki tüm verilerin yedeklemesi yapılır; ayrıca, istemi halinde bu yedekten bir kopya çıkarılarak şüpheliye veya müdafiine verilir ve bu husus tutanağa bağlanarak imza altına alınır. Bilgisayara el koymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir; kopyası alınan bu veriler kâğıda yazdırılarak bu husus tutanağa kaydedilir ve ilgililerce imzalanır. Görüldüğü üzere, yukarıda olası menfi neticelerinden söz edilen el koyma tedbirine gidilmeksizin de sistem verilerinin düplikasyonu yapılabilecektir; ayrıca bu halde, bütün bilgilerin kopyasının alınması zorunluluğu da yoktur. Kopyası alınan verilerin kâğıda yazdırılması işlemi, kâğıt israfına sebep olabileceği dolayısıyla eleştirilebilir. Bunun yanında, bilgisayarda bulunan her bilginin aslına uygun biçimde yazıya dökülemeyeceği (söz gelimi video dosyası, müzik dosyası, resim dosyası, vs.), yazdırılsa dahi hem veri tabanı açısından fazla yer kaplayacağı hem de bu işlemin zaman alacağı gerçeği üzerinde durulmalıdır. Ulusal Yargı Ağı Projesi (UYAP) kapsamında, bu dosyaların hâkim ve savcıların kişisel bilgisayarlarınca incelenmesi sağlanarak bu problemin çözülebileceği, bilgilerin kâğıda yazdırılması kuralının zorunluluk olmaktan çıkarılıp hâkim veya savcının istemine bağlanabileceği savunulmaktadır (Şen, 2006: 382).

Sulh ceza hâkimince verilecek kararlara karşı olağan kanun yollarından biri olan itiraz başvurusunun yapılabileceğini öngören genel kural (CMK m.267), araştırma konusu olan bilgisayarda arama ve el koymaya ilişkin hâkim kararlarına karşı da uygulanır. Ancak bu noktada belirtilmelidir ki, koruma tedbirlerine ilişkin kararlar, hazır bulunmayan ilgiliye tebliğ edilmez (CMK m.35/2). İlgili, tedbiri kendisine uygulandığı anda öğreneceği için, 7 günlük itiraz süresi de o tarihten itibaren başlayacaktır (Centel ve Zafer, 2005: 311). Bilindiği gibi itiraz, kararın yerine getirilmesinin geri bırakılmasını kendiliğinden sağlamamaktadır. Ancak, kararı veren ve dolayısıyla itiraz için başvurulan merci olan sulh ceza hâkimi veya itiraz yerinde görülmediği için yasanın bahşettiği yetkiyle onu inceleme yetkisi edinen o yargı çevresi içindeki asliye ceza mahkemesi hâkimi tedbirin geri bırakılmasına karar verebilir (CMK m.268, CMK m.269).

Tedbire başvurulabilmesi için, bilgisayarında veri aranacak kişinin, soruşturulan suçu işlediğine veya aranan bilgileri kendi bilgisayarında sakladığına dair somut delil bulunması şartının yasada öngörülmemesi eleştirilmektedir (Centel ve Zafer, 2005: 312). Ancak, adı geçen tedbire zaten başka bir biçimde delil elde etme olanağı bulunmadığı için başvurulduğundan hareketle, yukarıda eleştirilen noktaya yönelik somut delilin elde edilebilmesinin düşünülmesi var olan sistemde mümkün olamaz. Böyle bir şartın öngörülmesi, ceza yargılaması sisteminin tıkanmasına yol açabilecektir; tartışılan sorun, yasanın hükümleri arasında koordinasyon sağlanmasına yönelik çalışmalarla ve bu doğrultuda yapılacak düzenlemeyle çözülebilir. Bunun yanında, yapılacak düzenlemeyle, tedbirin yöneldiği suça ilişkin soruşturmanın sonucunda takipsizlik kararının

[9] 496 U.S. 128 (1990) 88-7164

(kovuşturmaya yer olmadığına dair karar – CMK m.172) veya soruşturmanın kovuşturmaya bürünmesinden sonra kovuşturma bitiminde edinilen kanaati gösteren beraat kararının (CMK m.223/2) verilip kesinleşmesi ile elde edilen verilerin ceza dava dosyası ve münderecatından çıkarılarak yok edilmesinin önünün açılması sağlanmalıdır (Centel ve Zafer, 2005: 312). Suçsuzluğu kanıtlanana ait kişisel verilerin imha edilmesi gibi önemli bir güvencenin yasada öngörülmemesi, temel hak ve hürriyetlerin korunması ilkesi ile bağdaşmamaktadır.

Herhangi bir arama prosedürü esnasında tesadüfen elde edilen deliller olarak adlandırılan bulgulara bilgisayarda da rastlanabilir. Yasa uyarınca, bilgisayarda arama veya el koymanın tatbiki esnasında, yapılmakta olan soruşturmayla ilgisi olmayıp diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edildiği takdirde, bu delil muhafaza altına alınır ve keyfiyet derhal Cumhuriyet Savcılığı'na bildirilir (CMK m.138/1). Bu noktada, bilgisayara yönelik arama ve el koymanın ancak belirli ağırlıktaki suçlarda uygulanması gerektiği tezini tekrar savunarak, tıpkı sırf belirli suçlarda uygulanan telekomünikasyon yoluyla yapılan iletişimin denetlenmesi (CMK m.135, CMK m.138/2) bahsinde olduğu gibi, burada da tesadüfen delil elde etmenin kolaylığına ve bulunan şeyin yasak delil niteliğine bürünebilme özelliğine dikkat çekmek gerekir.

Günümüzde haberleşme eğiliminin telefondan daha ziyade, e–postaya (*e-mail*), sohbet (*chat*[10]) programlarına, internet sitelerine ve forumlarına yöneldiği yadsınamaz bir gerçektir. Sayılan araçların tümü, özleri itibariyle işteş yapılıdır ve yazılı iletişimi ön planda tutar; böylece, rastlantısal biçimde delil elde edilmesine de son derece müsait platformlardır. Bunun dışında, hafıza konusundaki ortak özellikleri nedeniyle yazılan her şeyin bir şekilde bulunabilmesi ve bir yerden bir şekilde mutlaka ortaya çıkması avantajı da adli bilişime son derece yardımcı olmaktadır; eski nesil bir telefon için ise, bu özelliklerin etkili bir biçimde kullanılması güçtür. Üzerinde durulması gereken önemli bir delil elde etme platformu da e–postadır. Bu oluşumun çalışma sistemi iki ayaklıdır: gönderici sunucuya metini ulaştır; sunucu metini alıcıya yollar. Böylece, ileti silinmiş olsa dahi, üç kaynakta da o metinin içeriğinden kırıntılar kalır. Bu özelliği dolayısıyla e–posta, belki de en kolay ulaşılabilen elektronik delil edinim yeridir. Türkiye İstatistik Kurumu'nun (TÜİK) 2007 yılında gerçekleştirdiği Hane Halkı Bilişim Teknolojileri Kullanımı Araştırması'nın sonuçlarına tam da bu noktada değinmek faydalı olacaktır. Çalışmaya göre, hanelerin %18.94'ünün internete erişim olanağı, bunların %79.39'unda ise internete bağlanabilen kişisel bilgisayar vardır; hane halkı bireylerinin %61.11'i internete her gün girmekteyken, genel olarak tüm kullanıcıların %45.96'sı evinden, %37.52'si işyerinden, %31.21'i internet kahvelerinden internete bağlanmaktadır ("İnternete Daha Çok Yolumuz Var", 2007).

Uluslarüstü hukuk açısından bakıldığında, Türkiye'nin henüz taraf olmadığı Avrupa Konseyi Siber Suçlar Sözleşmesi[11], bilişim suçları ile ilgili hükümler

[10] Bu konudaki toplumsal eğilime yönelik alan araştırması için bkz. Sanal Sohbet: Chat (http://www.e-sosder.com/dergidetay.php?id=39)

[11] Genel hükümler (m.14-15), depolanan bilgisayar verilerinin etkili şekilde korunması (*expedited preservation of stored computer data* – m.16), trafik verilerinin etkili şekilde korunması ve kısmen ifşa

yanında, bilgisayarda arama ve el koyma işlemlerine yönelik özel birtakım koruma tedbirleri öngörmüştür. Sözleşme, ifade özürlüğünü kısıtladığı, hümanist ceza normlarına aykırı olduğu, usule ilişkin düzenlemelerin amacını aşar tarzda bulunduğu yönünde eleştiriler almıştır (İnternet ve Hukuk Platformu, 2006: 5). Belirtilen tedbirlerle ilgili olarak en önemli özellik, bunlara genel bir izleme önlemi biçiminde, diğer bir deyişle önleyici kolluk görevi şeklinde başvurulmasının olanaksız olduğudur; başvuru için ön şart, somut bir ceza soruşturmasının varlığıdır (Dülger, 2004: 239). Üretim emri (*production order*) olarak adlandırılan kavram ise, yetkili merciin tedbir sürecini başlatan arama ve el koymaya yönelik kararını ifade etmektedir. Gerek milletlerarası işbirliği, gerekse ulusal güvenlik ve kamu barışı prensipleri doğrultusunda bir an önce sözleşmeye taraf olunması gerekliliği de savunulmakta, yasa koyucu bir yandan sözleşmeye imza atmaktan imtina ederken, diğer yandan benzer düzenlemeleri (örneğin, erişimin engellenmesi tedbiri) içeren kanunlar çıkarmaktadır.

B. Ceza Muhakemesi Kanunu Dışında Kalan İç Hukuka Özgü Düzenlemeler

1774 sayılı Kimlik Bildirme Kanunu'na 1996 yılında yapılan değişiklikle (KBK ek m.1), kolluk güçlerine ait karakollara il merkezlerinden ağ bağlantısı yoluyla sorgulanabilecek bilgisayar terminalleri yerleştirilmesi ve Bakanlar Kurulu'nca belirlenecek konaklama tesislerinin de tüm kayıtlarını bu terminallere bağlaması öngörülmüştür. Böylece belirli kurumların bilgisayarlarında arama yapılması mümkün kılınmıştır (Centel ve Zafer, 2005: 311). Bu örnekte, adli bilişimde delil elde etme kolaylığı açısından haklı bir öneme sahip olan ağ üzerinde (*on – site*) aramanın idare eliyle teşkilatlandırılmış özel bir biçimi görülmektedir.

1 Haziran 2005 yayım tarihli Adli ve Önleme Aramaları Yönetmeliği m. 17, Ceza Muhakemesi Kanunu m. 134'ün uygulama alanını genişletmiştir. Buna göre aranacak veya el konulacak kapsama bizatihi bilgisayarın yanında, bilgisayar programları ve verileri, uzaktaki bilgisayar, bilgisayar ağları, veri saklama birimleri de girmektedir. Bunun yanında, yedekleme işleminin bilgisayar ağları, uzaktaki bilgisayarlar ve çıkarılabilir donanımlara yönelik olarak da yapılabileceği öngörülmüştür. Yine 1 Haziran 2005 yayım tarihli Suç Eşyası Yönetmeliği m. 9/2, el konulan bilgisayarın korunması usulünü düzenlemiştir. Buna göre, bilgisayar ve sistemine ilişkin verilerin asılları ve kopyaları, ses – görüntü – yazı kayıtlarının bulunduğu depolama aygıtları ve diğer ilgili parçalar, bozulmalarını engelleyecek nem – ısı – manyetik alan – darbe gibi dış etkilerden korunmalarını sağlayacak uygun ortamda muhafaza edilir. Ceza muhakemesi içinde bir soruşturma işlemi olan veri takibi, bilgisayarlar, casus yazılımlar ve biçim tanıma sistemleri eliyle yapılmakta, böylece şahıs hakkında işitsel ve görsel takip yoluna gitmeden de bilgi toplama olanağı açığa çıkmaktadır (Şafak ve Bıçak, 2005: 254-255). Bu

---

edilmesi (*expedited preservation and partial disclosure of traffic data* – m.17), üretim emri (*production order* – m.18), depolanmış bilgisayar verilerinde arama ve elkoyma (*search and seizure of stored computer data* – m.19), trafik verilerinin gerçek zamanlı toplanması (*real time collection of traffic data* - m.20), içerik verilerinin akışının engellenmesi (*interception of content data* – m.21)

doğrultuda, Ceza Muhakemesi Kanunu (m.134) başta olmak üzere, iç hukuk düzeni elektronik delile ulaşma açısından eklemlendirilmiştir.

5651 sayılı yasaya göre, Hüküm uyarınca, tahdidi şekilde sayılmış katalog suçları[12] içerdiği konusunda yeterli şüphe bulunan internet sitelerine erişim engellenebilecektir. Bir internet sitesine erişilmesini engellemek amacıyla koruma tedbiri uygulanmasına dair karar, 24 saat içinde yerine getirilir; bu doğrultuda, karar derhal erişim sağlayıcısına (internete erişim hizmetini abonelerine sağlayan işletmeler) bildirilir ve gereğinin yapılması emredilir. Nihayet, takipsizlik veya beraat kararının kesinleşmesiyle de erişimin engellenmesi kaldırılır. Koruma tedbirinin uygulanmasına yönelik kararı, gerek soruşturma gerekse kovuşturma evresinde kural olarak hâkim verecektir. Soruşturma aşamasında gecikmesinde sakınca görülürse Cumhuriyet savcısı da bu kararı verebilir; 24 saatlik hâkimin yerindelik denetimi ve itiraz yolunun açıklığı genel kuralları yasada korunmuştur. Koruma tedbiri değil de, idari tedbir biçimindeki erişimin engellenmesinin uygulanması, diğer bir deyişle önleme amacıyla erişimin engellenmesi konusuna da değinmek gerekir. Buna göre, yer sağlayıcısı (site sahibi) veya içerik sağlayıcısı (sitenin içeriğini oluşturan kullanıcı) yurtdışında bulunuyorsa (5816 sayılı kanun hariç olmak üzere) anılan suçlar için veya söz konusu içerik çocuğun cinsel istismarına ya da müstehcenlik suçlarından birine ilişkinse, Telekomünikasyon İletişim Başkanlığı resen erişimin engellenmesi kararı verebilecektir. İdari tedbirin yaptırımı olarak öngörülmüş olan idari para cezasına karşı (ki bu hususta 10.000 TL ile 100.000 TL tutarında alt ve üst hudutlar çizilmiştir) İdari Yargılama Usulü Kanunu uyarınca kanun yolu açıktır.

Telekomünikasyon İletişim Başkanlığı'nın açıklamasına göre, çocuk istismarı ve müstehcen yayınlar konularında otomatik engelleme yapan programlar vasıtasıyla uluslararası filtreleme sistemi kullanılacakken, katalog suçlar konusunda ise kişisel veya kurumsal bilgisayar sistemlerinin dışında kalan kamuya açık yayınların takip edilmesi düşünülmektedir ("Nette Yasak Devri!", 2007). Türkiye Bilişim Derneği Yönetim Kurulu Üyesi Av. Mehmet Ali Köksal'a göre ise, devletin gerçek zamanlı biçimde internet trafiğini izlemesi gibi bir girişimi polis devleti olmaktır; öncelikle, başta çocuk pornografisi olmak üzere belirli yoğunluktaki suçlarla mücadele sağlanmalı, haberleşmenin ve özel hayatın gizliliği prensiplerine saygı gösterilmelidir ("İnternet Yönetmeliğine Sert Tepki", 2007). Erişimi engelleme yetkisini öngören yasanın yürürlüğe girmesi ile birlikte uygulanmaya başlayan "site kapatmaları" fenomeninin aktüel bir nesnesi olan Youtube internet sitesinde yaklaşık 50 milyon saatlik görüntü bulunmakta, dünya genelinde başat tüketicilerden biri de Türkiye olarak görülmektedir ("İnternet Gazeteciliği Güçlendiriyor", 2008). Süreç ilk defa, suç ihbarı alan Ankara Cumhuriyet Savcısı Kürşat Kayral'ın, 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'a aykırılık gerekçesiyle Nöbetçi Sulh Ceza Mahkemesi'ne başvurması ve mahkemenin talebi yerinde bulmasıyla başlamıştır ("Youtube'a

[12] İntihara yönlendirme (TCK m.84), çocukların cinsel istismarı (TCK m.103/1), uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (TCK m.190), sağlık için tehlikeli madde temini (TCK m.194), müstehcenlik (TCK m.226), fuhuş (TCK m.227), kumar oynanması için yer ve olanak sağlama (TCK m.228), 25 Temmuz 1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçlar

Erişim Engellendi", 2008). Erişim sağlayıcıya verilen talimat ile tedbirin gereği yapılmış, siteye "T.C. Ankara 12. Sulh Ceza Mahkemesi'nin 17.01.2008 tarih ve 2008/55 no.lu kararı gereği bu siteye erişim engellenmiştir (*Access to this web site has been suspended in accordance with decision no: 2008/55 of T.R. Ankara 12th Criminal Court of Peace*)" ibaresi eklenmiştir. İlk etapta engelleme, "www.youtube.com" alan adını kapsamına almış, internet kullanıcılarının ağ sistemindeki alan adı (*domain name service – DNS*) ayarlarını değiştirerek tartışmalı yasağı delmelerinin önüne geçememiştir. Gerçekten de, bir internet sitesine ulaşmanın birçok yolu vardır ki, bunlardan birisi de sitenin alan adı yerine, internet protokolü numarasını (*internet protocol number - IP*) kullanmaktır. Uygulamadaki bu yanılgının farkına varılmasıyla, Türkiye çıkışlı tüm IP numaralarına blokaj uygulanmış, siteye erişimin yolu kapanmıştır ("Youtube'a Erişmek Artık Mümkün Değil", 2008). Örnek vermek gerekirse, Youtube internet sitesine klasik anlamda "http://www.youtube.com" adresiyle erişilebildiği gibi, "http://208.65.153.253" pusulası ile de yönelmek mümkündür. Her alanı adının, matematiksel bir karşılığı, dijital platforma yansıyan bir izdüşümü vardır. Birkaç günlük gecikmeyle de olsa açık pencere kapatılmıştır; kullanıcılar ise, erişim için diğer yolları kullanmaya devam etmiştir. Bireysel haklar açısından bakıldığında, anılan yasak, özgürlükler hukukuyla, diğer bir deyişle haber alma hürriyetinin kısıtlanması ve ifade özgürlüğü konularıyla, yakından ilgilidir ve geniş katılımla tartışmaya açılmalıdır.

III. Adli Bilişim Metotları:

Bilgisayar ve her türlü çevre biriminden[13] elektronik delile ulaşma olasılığı bulunmaktadır. Ne de olsa, bilişim suçları, internet ve bilgisayarın eklentileri kullanılarak işlenen suçlar olarak tanımlanmıştır (Şen, 2001: 13). Bilgisayarın donanımına veya yazılımına el konulabilir; donanım veya yazılım illegal yöntemlerle elde edilmiş ya da suç işlemek için araç olarak kullanılmış olabileceği gibi bizzat delil de teşkil edebilir (Şen, 2006: 376). Elektronik delil, tıpkı parmak izi veya DNA gibi, ilk başta gözle görülemeyen gizli bir yapıya sahiptir ve rahatlıkla tahrif, tahrip ve yok edilebilir; ayrıca, zamana karşı son derece hassastır (A.B.D. Adalet Bakanlığı Ulusal Adalet Enstitüsü, 2001: 6). Elektronik olay yerinde sırasıyla, delil tespit edilecek ve tanımlanacak, olay yerinin dokümantasyonu yapılacak (fotoğraf, kroki, not, vs. aracılığıyla), delil toplanacak ve koruma altına alınacak, ambalajlanıp incelemek üzere nakliye edilecektir (A.B.D. Adalet Bakanlığı Ulusal Adalet Enstitüsü, 2001: 6). Gerekli teorik ve pratik bilgi ile ustalığa sahip olmayan kimsenin, bilgisayarda veri incelemesi yapmaması veya veri kurtarmaya çalışmaması, hatta klavye veya farenin hiçbir tuşuna dahi basmaması tavsiye edilmektedir (A.B.D. Adalet Bakanlığı Ulusal Adalet Enstitüsü, 2001: 6). Hatta böyle bir durumda, elektronik delile hukuka

[13] Ana bölüm (kasa), ekran, klavye, fare, bağlantı uçları ve kablolar, güç kaynağı ünitesi, harici sabit disk (*external hard disk*), taşınabilir sabit disk, modem, kablosuz modem (*wireless modem*), faks, dijital kamera, disket, yedekleme ünitesi, sürücü, *cd – dvd*, yazıcı ve çıktıları (hatta bazı yazıcıların kendi bellek kartları da bulunmaktadır), telefon, telesekreter, cep bilgisayarı (*databank*), dijital ajanda (*organizer*), çakar kart (*flashdisk*), çağrı cihazı, pos makinesi, tarayıcı (*scanner*), hoparlör, mikrofon, sunucu (*server*), vs.

aykırı biçimde erişimin Amerika Birleşik Devletleri Elektronik Haberleşmenin Gizliliği Yasası (*Electronic Communication Privacy Act*) başta olmak üzere, diğer federal yasaları da ihlal etme olasılığı vardır; hassas doğası nedeniyle, araştırma mutlaka profesyonel personel tarafından yapılmalıdır (A.B.D. Adalet Bakanlığı Ulusal Adalet Enstitüsü, 2001: 7).

Elektronik olay yerinde, "eğer açıksa bırak açık, kapalıysa bırak kapalı kalsın" kuralı işletilir (A.B.D. Adalet Bakanlığı Ulusal Adalet Enstitüsü, 2001: 25); bu sayede, olası bir veri kaybının önüne geçilecektir. Bunun yanında, dayanıksız parçalara ve aslında elektronik delil olmayan ancak olay yerinde bulunabilecek parmak izi, vücut salgısı, DNA gibi bulgulara öncelik verilmesi öğütlenmiştir. (A.B.D. Adalet Bakanlığı Ulusal Adalet Enstitüsü, 2001: 25-26). Bunun dışında, delil elde etmek için olay yerinde yer alan orijinal bilişim sistemini kullanmadan, kasanın arkasında bulunan güç bağlantısını kestikten sonra diğer tüm bağlı birimlere de daha sonra analiz merkezinde yapılacak birleştirme işlemine yardımcı olabilmesi için işaretler koyarak ve tüm parçaların manyetik alan gibi dış etkenlerden korunması sağlanarak taşıma gerçekleştirilir (A.B.D. İç Güvenlik Bakanlığı Gizli Servis: 4). Söz konusu cihaz dizüstü bilgisayarsa (*laptop*), güç bağlantısını kesmek işe yaramayacak, pili de çıkarmak gerekecektir (A.B.D. İç Güvenlik Bakanlığı Gizli Servis: 4); aynı şekilde herhangi bir ağ bağlantısı varsa ilk önce buna yönelik güç kaynağı etkisiz duruma getirilmelidir (A.B.D. İç Güvenlik Bakanlığı Gizli Servis: 5).

Delile ulaşma aşamasında nereye bakılacağı da önemli bir konudur. Örneğin, çocuk istismarı veya cinsel suçlar söz konusuysa bilgisayar oyunları, resimler, filmler, sohbet kayıtları (*chat logs*) gibi akla ilk gelen dokümanlar dışında kapsamlı bir inceleme yapılması şarttır. Gerçekten, veri saklamak isteyen her türlü yolla amacına ulaşılabilir; en basit ifadeyle, metin dosyalarının içine görüntü ekleyip muhafaza edebilir. Bu noktada, inceleme esnasında zaman açısından da çeşitli problemler görülmektedir. Alman hukukunda, inceleme öncesinde somut olay failine ilişkin olası nitelikler tespit edilerek anahtar kelime ve imgeler belirlenmektedir (Centel ve Zafer, 2005: 311). Verilerin yedeklenmesi (duplikasyon) genel anlamıyla, sistem çökmesi veya doğal bir etken sonucunda verileri kurtarmak amacıyla bilgilerin kopyasının alınması işlemidir ve yardımcı programlar eliyle uygulanır (Berber, 2004: 104). Zaten inceleme, orijinal veri kaynağı üzerinde değil, yedekleme sonucu elde edilen ikiz kardeşi üzerinde yapılır. Uygulamada bu amaçla, *MD5* ve *SHA - 1* algoritmalarını kullanan *FTK* (*forensic tool kit*) ile *MD5* ve *CRC* algoritmalarını kullanan *Encase* yazılımları kullanılmaktadır. Yedekleme, Windows jargonundaki gibi bir kopyala – yapıştır (*copy – paste*) işlemi değildir; sistemin birebir (*bit to bit – sector by sector*) kopyası alınmaktadır. Bu yolla, uçucu verilerin (bilgisayar kapandığında geri gelmeyen bilgiler) dahi kurtarıldığı görülmektedir. Elektronik delilin diğer delil çeşitlerine oranla son derece orijinal olan kaybolmayıp tekrar dirilebilme özelliğine adli bilişimde "vampir etkisi" denilmektedir. Silinmiş veriler (*deleted data*), efsanelerdeki vampirler gibi tekrar geri dönecektir (Berber, 2004: 110).

Sonuç

Genel anlamda arama ve el koymaya yönelik koruma tedbirlerinin ulaşılamayan delilleri elde etmek ve var olan delilleri garanti altına almak amaçlarından hareketle, dijital arenada koşulları farklı özel halleri ile ceza adaleti sistemi içinde düzenlenmesi yerinde olmuştur. Klasik bağlamda arama ve el koymanın suçla mücadele açısından elektronik delile ulaşmakta yetersiz kalacağı açıktır. Aynı doğrultuda, başta bilgisayar olmak üzere her türlü dijital aygıt vasıtasıyla işlenebilen suçları önlemek amacıyla, öğretiden ve uygulamadan gelen eleştiriler ışığında, başta koruma tedbiri hükümleri olmak üzere her bireye eşit uygulanacak ceza adaleti normları, teknolojik gelişmeye denk biçimde revize edilmeli ve öngörülen esaslarla etkin bir biçimde uygulanmalıdır. Bu bağlamda, bireyin temel hak ve özgürlükler alanına hukuka aykırı biçimde temas edilen bir oluşumun asla hukuk devleti olarak adlandırılamayacağı, böyle bir örnekte hukukun üstünlüğü prensibinden söz edilemeyeceği açıktır.

Dijital arenanın en *sui generis* özelliği veri ve iz kaybının son derece güç olmasıdır. Herhangi bir bilgisayar kullanıcısının silip ulaşılamaz duruma getirdiğini zannettiği bilgi, profesyonel bir adli bilişim uzmanı tarafından açığa çıkarılabilir. Sürdürülen bir suç soruşturmasında, dijital niteliği olsun veya olmasın, bilişim araçları üzerinden olayı aydınlatacak önemli deliller elde edilmektedir. Uygulamada verilerin hacmi ve kişilik haklarının ihlali olasılığı nedeniyle masraf çokluğu ve zaman darlığı konularında bazı sorunlara rastlanmaktadır. İncelemeye başlamadan önce ve inceleme sırasında kolayca hata yapılabilme ve bu hatanın telafisinin güçlüğü problemlerinden de bahsedilebilir. Bunun yanında, kablosuz bağlantı (*wireless*) teknolojisinin yaygınlaşmasıyla, suç aracı bilgisayarı tespit etme güçlüğü çekilmektedir; somut olay örgüsünde kapsama alanı geniş örnekler bulunuyorsa suçluya ulaşmak son derece zorlaşmaktadır. Böyle bir durumda, adli hataların ve en önemlisi de insan hakları ihlallerinin ortaya çıkma olasılığı da son derece fazladır.

Başta bilgisayar olmak üzere, her çeşit dijital aygıt vasıtasıyla işlenebilecek suçları kontrol altına almak amacıyla, doktrin ve uygulamadan gelen kritiklerin ışığı altında, alanında uzmanlaşıp adli bilişim teknikleriyle donatılmış personelin ülke genelinde eğitilmesi ve adli aktivitelerinin yaygınlaştırılması sağlanmalıdır. Aynı doğrultuda, ana prensip, ceza muhakemesi sürecinde devlet gücü kullananların, kişi temel hak ve özgürlüklerine keyfi uygulamalarla müdahale etmemesidir; aksi takdirde ihlal sonucu oluşan hak kayıplarına yönelik iddiaların birer birer uluslarüstü arenaya taşınması ile “versus Türkiye”nin olumsuz imajının törpülenmesi güçleşecektir.

KAYNAKÇA

Amerika Birleşik Devletleri Adalet Bakanlığı Ulusal Adalet Enstitüsü (U.S. Department of Justice National Institute of Justice) (2001), *Electronic Crime Scene Investigation: A Guide For First Responders*, http://www.ncjrs.gov/pdffiles1/nij/187736.pdf

Amerika Birleşik Devletleri İç Güvenlik Bakanlığı Gizli Servis (U.S. Department of Homeland Security Secret Service), *Best Practices For Seizing Electronic Evidence: A Pocket Guide For First Responders v.3*, www.forwardedge2.com/pdf/bestpractices.pdf

Arslan, Zühtü (2005) *Türkiye'de Liberal Düşüncenin Önündeki Engeller*, Modern Türkiye'de Siyasi Düşünce: Liberalizm, Cilt:7, 1.Bası, İstanbul

Bıçak, Vahit (1999) *İnsan Hakları İhlallerinde Yönelimler: Baskıdan Hileye (Trends on the Infringement of Human Rights: From Oppression to Deception)*, Liberal Düşünce Dergisi 15 (http://www.bilkent.edu.tr/~vahit/ar6.htm)

Centel, Nur / Zafer, Hamide (2005), *Ceza Muhakemesi Hukuku*, Beta Basım Yayım Dağıtım, 3. Bası, İstanbul

Doehring, Karl (2002) *Genel Devlet Kuramı (Genel Kamu Hukuku)*, 2000 Yılında Yayınlanmış 2. Basıdan Çeviren: Ahmet Mumcu, İnkılap Kitabevi Yayınları, İlk Bası, Ankara

Dülger, Murat Volkan (2004), *Bilişim Suçları*, Seçkin Yayıncılık, Ankara

Eryılmaz, M. Bedri (2006) *Suçla Mücadele Politikası Açısından Yeni Ceza Muhakemesi Kanunu*, Ceza Hukuku Dergisi Sayı:1, Seçkin Yayıncılık, Ankara

Eryılmaz, M. Bedri (2003), *Bir İnsan Hakkı Olarak Korku Duymama Hakkı ve AB Uyum Yasaları (As A Human Right Of Not To Feel Fear And EU Harmony Laws)*, Ankara Barosu Dergisi Sayı:4, Ankara Barosu Yayınları, Ankara

Eryılmaz, M. Bedri (2000), *Kolluğun Yetkileri Açısından Ceza Muhakemeleri Usulü Kanunu ile Yeni CMUK Tasarısının Karşılaştırılması ve Yeni Tasarının Düşündürdükleri…*, Ankara Barosu Dergisi Sayı:1, Ankara Barosu Yayınları, Ankara

Gözübüyük, Şeref (2002) *Yönetim Hukuku*, Turhan Kitabevi Yayınları, 16. Bası, Ankara

Günday, Metin (1998) *İdare Hukuku*, İmaj Yayıncılık, 3. Bası, Ankara

Gürkan, Ülker (1994) *Hukuk Sosyolojisine Giriş*, 2. Bası, Ankara

İçli, Tülin Günşen (2007) *Kriminoloji*, Seçkin Yayıncılık, 7. Bası, Ankara

İnternet ve Hukuk Platformu (2006), *Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı*, Çeviri, Ankara Barosu Bilgi İşlem Merkezi Yayınları, Ankara

Keser Berber, Leyla (2004), *Adli Bilişim (Computer Forensic)*, Yetkin Yayınları, İstanbul

Kunter, Nurullah / Yenisey, Feridun (2005), *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku*, Arıkan Basım Yayım Dağıtım, İstanbul

Milliyet Gazetesi, http://www.milliyet.com.tr

Özbek, Veli Özer / Bacaksız, Pınar (2006), *Ceza Muhakemesi Hukukunda Arama*, Ceza Hukuku Dergisi Sayı:1, Seçkin Yayıncılık

Öztürk, Bahri / Erdem, Mustafa Ruhan (2006), *Uygulamalı Ceza Muhakemesi Hukuku*, Seçkin Yayıncılık, 9. Bası, Ankara

Öztürk, Bahri / Erdem, Mustafa Ruhan / Özbek, Veli Özer (2004) *Ceza Muhakemesi Hukuku*, Turhan Kitabevi Yayınları, 2. Bası, Ankara

Resmi Gazete, http://rega.basbakanlik.gov.tr

Sevimli, A. Güçlü (2007), *Bilgisayar ve Bilgisayar Kütüklerine El Konulması ve Uygulamadaki Sorunlar*, İstanbul Barosu Dergisi Sayı:3, İstanbul Barosu Yayınları, İstanbul

Soyaslan, Doğan (2003) *Kriminoloji: Suç ve Ceza Bilimleri*, Yetkin Yayınları, 3. Bası, Ankara

Şafak, Ali / Bıçak, Vahit (2005), *Ceza Muhakemesi Hukuku ve Polis*, Roma Yayınları, Ankara

Şen, Bilal (2001) *Bilgisayar Suçlarının Getirdikleri ve Üzeyir Garih Cinayeti*, Polis Bilimleri Dergisi, Sayı: 29

Şen, Osman Nihat (2006), *Ceza Hukukunda Bilgisayar Araştırmaları*, Ceza Hukuku Dergisi Sayı:1, Seçkin Yayıncılık