ELEKTRONİK DELİLLERİN DEĞERLENDİRİLMESİ VE KABUL EDİLEBİLİRLİĞİ - İYİ UYGULAMA ÖRNEKLERİ VE KARŞILAŞILAN ZORLUKLAR

ELEKTRONİK DELİLLERİN DEĞERLENDİRİLMESİ, YARGITAY UYGULAMALARI

A-İNTERNET VE VERİLER

Günümüz dünyasında bilgisayar, internet ve bilişim sistemlerinde meydana gelen gelişmelerle birlikte ekonomi/bankacılık, ticaret, iletişim, saldırı/savunma, sosyal ilişkiler/örgütlenme gibi alanlarda küresel boyutta önemli ilerlemeler sağlanmıştır.

Devletler, kurum ve kuruluşlar, şirketler ve bankalar için internet ve bilişim sistemleri hayati önem taşımaktadır. Artık internet çoğu kişi için bir yaşam şeklini almıştır.

İnternet ve bilişim sistemlerinin yaygınlaşması, bu alanda işlenen suçlarda da önemli artış meydana getirmiştir. Ceza yasalarında düzenlenen birçok suçun artık internet üzerinden de işlenebildiğini görmekteyiz.

Uygulayıcılar olarak şehirler ve ülkelerle sınırlı olmaksızın işlenebilen bu tür suçlarda her geçen gün yeni bir suç işleme şekli, yeni bir yöntemle karşılaşmaktayız. (Doğrudan&Dolaylı Bilişim Suçları, GÜL Ahmet, Seçkin, 2.Bası, s.9 vd.)

İnternet ortamında suç işlemelerin yaygınlaşması, adeta meslek edinilmesi, konunun uluslararası bir sorun halini alması sonucunda; uygulayıcıların bilinçlenmesi ve uluslararası işbirliği kaçınılmaz hale gelmiştir. Artık dijital bir ortamda suç işlenebilmesi için Rusya'dan ABD'ye, Çin'den Türkiye'ye, Afrika'dan Avrupa'ya gitmeye gerek duyulmamaktadır.

Bilgisayar başında oturan bir hacker (siber korsan) kilometrelerce uzaktan bir başkasının bilgisayarına, akıllı telefonunun içeriklerine ulaşabilmekte, virüs göndermekte, yazılım programları geliştirebilmektedir. Rahatlıkla düşman ülke savunma sistemine, gizli bilgilerine saldırı yapabilmekte, verileri ele geçirebilmektedir.

Artık sadece bir bilgisayardan ya da benzer veri saklama aygıtlarından elde edilen veriler delil olarak yeterli olmayacaktır. Dijital delillerin içeriği, ne maksatla oluşturulduğu, ne tür yarar sağlandığı, zarar gören kişilerle ilişkisi değerlendirilmeli, ortaya konulmalıdır. Örneğin bir mağdura yönelik şantaj içerikli görüntülere -dolandırıcılık maksatlı iletişim bilgilerine ulaşmak yanında, içerik sahibi ile mağdur arasında bağlantı kurulup kurulmadığı, yarar sağlanıp sağlanmadığı da araştırılmalıdır.

Teknolojik gelişmeler, internet ortamının son derece yaygınlaşması, uluslararası ile- tişimin kolaylaşması, kısaca dünyanın küçülmesi sonucunda sanal ortamda işlenen suç sayısı ve niteliği gün geçtikçe artmaktadır. Artık normal yaşantımızda gördüğümüz birçok suç tipinin dijital ortamda da işlendiğini görüyoruz.

Örneğin tehdit, hakaret, şantaj, hırsızlık, dolandırıcılık, sahtecilik, kredi kartı sahteciliği-dolandırıcılığı, haberleşmenin gizliliğini ihlal, kişisel verilerin kaydedilmesi, yayılması, müstehcenlik, devlet sırlarının yayılması, suç örgütü propagandası gibi çok sayıda suçun internet ortamında, bilişim sistemleri kullanılarak işlenmesi mümkün olmaktadır.

Suç işlemeyi meslek edinmiş birçok kişi, siber korsanlar, dolandırıcılık-şantaj şebekeleri yakalanmayı ve delillere ulaşmayı engellemek amacıyla sanal ortamı tercih etmektedir. Terör örgütleri de propaganda ya da örgüt faaliyetleri maksatlı bu alanı kullanmaktadır.

Bahsedilen ortamda veriler (bilgiler) hızla arttığından depolama ihtiyacı doğmaktadır. Bu depolama alanları ise, işlenen suçlar açısından bir delil toplama platformudur.

Verilere yönelik suçlar; verilerin çalınması, ulaşılmaz kılınması, değiştirilmesi, bozulması, yok edilmesi şekillerinde olabilir. Mağdurun verileri elde edilip kötüye kullanılarak haksız yarar sağlama yoluyla da suç işlenebilir. Bu şekilde kötüniyetli kullanımlar için internet ortamında veri toplama işine "veri korsanlığı" denilmektedir.

Türkiye'nin de taraf olduğu Avrupa Konseyi Siber Sözleşmesi'nin 2.maddesine göre, devletler verilerin güvenliğini korumaya yönelik tedbirler almak zorundadır.

Türk hukuk sisteminde internet ortamında işlenen suçlar yönünden, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi hakkında Kanun bulunmaktadır.

Bu yasanın 4.maddesi uyarınca internet ortamındaki verilerden bu veriyi üreten, değiştiren ve sağlayan kişi sorumludur. Yer sağlayıcılar ise gerekli bilgileri Bilgi Teknolojileri ve İletişim Kurumu'na vermek, gerekli tedbirleri almak zorundadırlar.

Bu yasa uyarınca Bilgi Teknolojileri ve İletişim Kurumu'nun intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu ve uyarıcı madde kullanımını kolaylaştırma, müstehcenlik, fuhuş gibi suçlarda önlem alma yetkisi de bulunmaktadır. Ayrıca özel hayata, kişisel verilere müdahale söz konusu olduğunda hakim kararı ile sınırlamalar söz konusu olabilmektedir.

B-DİJİTAL DELİL NEDİR?

Yukarıda açıklanan gelişmelerle birlikte dijital veriler büyümeye ve verileri saklayacak depolama yöntemleri farklılaşmaya başladı. Elektronik delil olarak da nitelenen bu kavram farklı şekillerde tanımlanabilmektedir.

"Bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen, soruşturma ve yargılama açısından hukuki değeri olan bilgi ve veriler" şeklinde tanımlanmakta, ayrıca "adli bilişimle ilgili bir çalışma sırasında bilişim sistemleri ve bu kapsamdaki depolama aletleri üzerinden elde edilen adli deliller" olarak da ifade edilmektedir.

Dijital delilin soruşturma aşamasında aydınlatıcı/yol gösterici yönü olabilmekle birlikte, mahkemelerde delil olarak kabul edilecek özellikte olması gerekir. Bir başka deyişle, bilişim alanında ortaya atılan iddiaların, işlenen suçların ispatı elde edilen dijital delillerin ikna ediciliğine, ispat gücüne ve hukuka uygunluğuna bağlıdır.

Bizler suçlar açısından delil değeri taşıyan ve yargılama sürecinde delil olarak kullanılabilecek her türlü manyetik ya da elektronik ortamda verileri saklayabilen aygıt ya da ortama dijital delil diyoruz.

Klasik delillerde gözle görülme, el koyma, muhafaza altına alma mümkün iken, dijital delillerde bu mümkün değildir. Dijital delillerin muhafazası için mutlaka donanım aygıtına ihtiyaç vardır.

Bu delillerin saklandığı alanlar olarak taşınabilen/taşınamayan bilgisayar/computer, harddisk, flash disk, CD/DVD, hafıza kartı, akıllı telefon, kart okuyucular, dijital fotoğraf ve video kaydediciler, ses kayıt cihazları, yazıcı, faks ve fotokopi makineleri, sim kartlar sayılabilir.

Bu çerçevede elde edilebilecek yazılı ve görüntülü dosyalar, fotoğraflar, video kayıtları, bilgisayar proğramları, SMS, MSN gibi yazışma kayıtları, gizli dosyalar/klasörler, kullanılan internet siteleri, internetten indirilmiş dosyalar, silinmiş dosyalar/klasörler, chat kayıtları dijital delil olarak kullanılabilecektir. (Bilişim Suçları ve İnternet İletişim Hukuku, Dr.M.Volkan Dülger, s.664 vd.)

Şikayetçi kurum, kuruluş ya da kişilere yönelik sistemlere karşı suç işlenmesi durumunda; bu kişi ya da kurumlara ait sistem ya da dijital veriler üzerinde yapılacak incelemeler de aynı derecede önem taşımaktadır.

C-TÜRK HUKUK SİSTEMİNDE DİJİTAL DELİL

Türk ceza yargılaması hukukunda maddi gerçeğin ortaya çıkması bakımından delil serbestisi ilkesi benimsendiğinden, dijital deliller de aynı çerçevede ele alınmaktadır. Ceza Muhakemesi Kanununun 217.maddesinde "Yüklenen suç, hukuka uygun bir şekilde elde edilmiş

her türlü delille ispat edilebilir" hükmü bulunmaktadır. Dolayısıyla ispat aracı olarak herhangi bir delil sınırlaması yoktur.

Dijital delillerin birden çok olması yanında diğer delillerle birlikte maddi gerçeğin ortaya çıkmasına katkı sağlayabileceği de kabul edilmektedir. Ancak herşeyden önce delil olarak kabul edilebilmesi açısından, Türk Ceza Muhakemesi Kanununun 134 ve devamı maddeleri ile ilgili yönetmelik hükümlerine uygun şekilde elde edilmesi; yani dijital delillere ilişkin koruma tedbirlerine uygun hareket edilmesi gerekmektedir.

Türk hukuk öğretisinde dijital delil," Bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir.Parmak izi veya DNA gibi genellikle görünmeyen bir yapıya sahiptir.

Sınırları kolayca ve hızlı bir şekilde geçebilir. Hassastır ve kolayca değiştirilebilir, bozulabilir veya yok edilebilir. Bazen zamana karşı hassastır. Elektronik deliller sözkonusu olduğunda; adli tıp ve diğer delil toplama usullerinin bu alanda da uygulanması gerekecektir." (Dülger,age, s.664 vd.) şeklinde açıklanmaktadır.

Yine bir başka deyişle, dijital veya elektronik delil, iddia edilen bir fiilin ispatında kullanılmak istenen veya saklanan veri, kayıt ve belgeler olarak da ifade edilmektedir.

Yani dijital deliller ses ve/veya görüntü tespit eden belge, ortam tespit eden belge, veri tespit eden belge veya ispat edilecek olayın kanıtlanmasına dolaylı olarak yardımcı olan olay ve iz şeklinde de ifade edilmektedir.(Dijital Delil ve İletişimin Denetlenmesi, Prof.Dr.Çetin Arslan, Hacettepe Ün.Hukuk Fak. Haziran-2014 9.Türkiye Ceza Hukuku Günleri Sempozyum Sunumu)

Dijital delillerin değişebilirliği, saldırıya açık olması nedeniyle bilimsel verilere, akla, mantığa, hayatın olağan akışına, maddi olaylara ve varsa diğer delillere uygun olmasını aramaktayız. Birden çok dijital delil bulunduğunda, deliller arasında tutarsızlık olmamalı, veriler karşılaştırılmalıdır. Delillere ulaşılma şekli, tarihi, kimden elde edildiği kesin olarak belirlenmelidir.

Türk hukuk sisteminde dijital deliller Ceza Muhakemesi Kanununun 134 ve devamı maddelerinde düzenlenmektedir.

134.maddede düzenlenen "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" işlemleri somut delillere dayanan kuvvetli suç şüphesi bulunması ve başka surette delil elde etme imkanının bulunmaması halinde hakim kararı ile mümkün görülmüştür. Gecikmesinde sakınca bulunan hallerde cumhuriyet savcısı kararı ile de bu işlemin yapılması ve sonrasında hakim onayına sunulması mümkün kılınmıştır.

135.maddede düzenlenen "İletişimin tespiti, dinlenmesi ve kayda alınması"

işlemleri de aynı gerekçelerle ve hakim kararı ile mümkün olacaktır. Ancak bu yönteme başvurulabilmesi açısından yasada sayılan "Göçmen kaçakçılığı ve insan ticareti, kasten öldürme, işkence, cinsel saldırı, çocukların cinsel istismarı, nitelikli hırsızlık ve yağma, uyuşturucu madde imal ve ticareti, suç işlemek amacıyla örgüt kurma, devletin birliğini ve ülke bütünlüğünü bozma, anayasal düzene ve bu düzenin işleyişine karşı suçlar..... gibi) yasada sayılan önemli suçlar sözkonusu olmalıdır.

140.maddede ise, aynı gerekçelerle şüpheli veya sanığın "kamuya açık yerlerdeki faaliyetlerinin ve işyerinin teknik araçlarla izlenebilmesi, ses veya görüntü kaydı alınabilmesi" imkanı getirilmiştir. Bu yönteme de yasada sayılan aynı suçların soruşturulması sırasında ve hakim kararıyla ibaşvurulabilecektir.

Açıklanan dijital delil elde etme yöntemlerine -sonradan hakim onayına sunulmak kaydıyla- acil hallerde cumhuriyet savcısı kararı ile de başvurulabilecektir. Delillerin güvenilirliğine, kararlara esas alınabilirliğine zarar gelmemesi açısından, yasada ayrıntılı düzenleme yapılmıştır. Yapılan düzenlemelerde yetkili makam, süre, amaç, gerekçe ve yöntem tüm ayrıntılarıyla açıklanmıştır.

Dijital delillerin elde edilmesi sonrası gerekli inceleme ve rapor düzenleme işlemleri, alanlarında uzman adli bilişim uzmanları tarafından yapılmaktadır. Soruşturma ve yargılama sırasında tereddüt doğuran hususlar ortaya çıktığında ise, teknik konularda uzman, tarafsız bilirkişilerden ayrıntılı raporlar alınabilmekte, tanık olarak bilgilerine başvurulabilmektedir.

D-YARGITAY UYGULAMASINDA DİJİTAL DELİLLER

Anayasa Mahkemesi, Yargıtay, Danıştay gibi yüksek mahkemeler anayasa, yasa ve yönetmeliklere aykırı olarak, yani yöntemine uyulmadan elde edilen dijital verilerin delil değerini kabul etmemektedir. Ayrıca kararlarında bu delillerin elde edilme yöntemlerine de vurgu yapmakta, hukuka uygun elde edilip edilmediğini, içeriğini, güvenilirliğini ve düzenlenen bilirkişi raporunu denetlemektedir.

Dijital delillerin 'manipülasyona açık olması, değiştirilebilme kolaylığı ve sanal olmasının' hükme esas alınmasını engellemeyeceği yüksek mahkeme kararlarında vurgulanmaktadır. Keza bu durum CMK'nın 217.maddesinde düzenlenen delil serbestisi ilkesine aykırı olacaktır.

Yargıtay Ceza Genel Kurulu'nun 20.12.2018 (2018/16-419 E-2018/661 K) ve 26.09.2017 günlü kararlarında ayrıntılı olarak açıklanan dijital veriler, ceza yargılamasında delil olarak kabul edilmiştir.

Ceza Genel Kurulunun 26.09.2017 gün, 2017/16-956 E-2017/370 K sayılı kararında, "sanıkların ByLock sistemini kullandıklarına ilişkin tespit, iddianamede unsurları gösterilen silahlı terör örgütüne üye olma suçunun bir delili niteliğinde olduğundan, hükme esas alınmasında bir isabetsizlik bulunmamaktadır." denilmekle, örgüt mensupları tarafından gizlilik maksatlı olarak bylock uygulama programının kullanılması hususunda usulünce yapılan tespitler, dijital delil olarak kabul edilmiştir.

Ayrıca Yargıtay 16.Ceza Dairesinin 19.07.2017 gün, 2017/1800 E- 2017/4837 K sayılı, yine 05.12.2018 gün, 2018/2915 E-2018/4868 K sayılı kararında, anılan programı indirmenin mesajlaşma için yeterli olmadığı, mesajlaşmanın gerçekleşmesi için sistem tarafından kayıt olan kullanıcılara otomatik olarak atanan ve kullanıcıya özel olan ID (kimlik) numarasının bilinmesi ve karşı taraftan onaylanması gerektiği, aksi halde kişiler listesine eklenemeyeceği ve mesajlaşma içeriğinin gerçekleşmeyeceği belirtilmiş, dijital delilin özelliği birçok kararda ayrıntılı olarak açıklanmıştır.

Yüksek mahkeme kararında bahsedilen dijital delilin elbette yukarıda açıklanan yöntemine uygun olarak elde edilmesi gerekmektedir.

16.Ceza Dairesinin 21/09/2017 tarihli kararında (2015/2056 E-2017/5023 K), "sanığın evinde ve işyerinde yapılan aramalarda elde edildiği iddia olunan tüm dijital medyaların -arama mahallinde imaj alınmadan, ilgilisine de bir kopyası verilmeden ve kanuna uygun gerekçesi de tutanağa yazılmadan el konulması nedeniyle CMK'nın 134.maddesi hükmü ve hukuka uygun yöntemlerle elde edildiklerinin kabul edilemeyeceği" belirtilmiş,delillerin hukuka uygun elde edilmesi gerektiği vurgulanmıştır.

Aynı dairenin 22.05.2019 gün, 2019/1613 E-3706 K sayılı kararında, "hükme esas alınan veri inceleme raporunun, veri inceleme raporuna dayanak delilin elde edilişine dair gizli tanık Garsonun daha önce hakim huzurunda alınmış ifade tutanağı ve CMK'nın 134.maddesine göre alınan mahkeme kararı ve varsa ayrıntılı analiz raporunun soruşturmayı yürüten Ankara Cumhuriyet Başsavcılığından getirtilmesi", şeklinde hükme dayanak dijital delilin dosya arasında bulunması gerektiğine işaret edilmiştir. Yine bir çok kararda (yukarıda anılan karar, 13.06.2019 gün, 2019/2874 E-4197 K, 16.09/2019 gün, 2019/2597 E-5281 K sayılılar) dijital delillerin CMK'nın 217.maddesi uyarınca sanık ve müdafiine okunması ve diyeceklerinin sorulması gerektiği belirtilmiştir.

8.Ceza Dairesinin 29/11/2017 günlü (2016/10741 E-2017/13486 K sayılı) kararında, "sanığın bilgisayarına el konulduktan 4 gün sonra Ceza Muhakemesi Kanununun 134.maddesine göre bilgisayar kütüklerinde arama kararı verilmesi nedeniyle, bilgisayardan deliller hukuka aykırı elde edildiğinden hükme ve incelemeye esas alınamayacağına" karar verilmiştir.

3.Ceza Dairesi'nin 13/02/2013 tarihli kararında (2011/36421 E- 2013/5261 K), "işkence iddialarıyla ilgili olarak karakol gözetim odası kamera görüntülerinin getirtilerek incelenmesi gerektiğine" karar verilmiştir. 8.Ceza Dairesinin 15.01.2020 gün ve 2019/20198 E-2020/776 K sayılı kararında da benzer hususa vurgu yapılmıştır.

8.Ceza Dairesinin 08.01.2020 gün, 2019/15788 E- 2020/226 K sayılı kararında " sanığın internet hattına tespit edilen tarihte başkalarının giriş yapıp yapmadığının ve kendisinin başkalarına ait hesaplara girişinin olup olmadığının belirlenmesi açısından ilgili internet sağlayıcısından bilgi istenmesi, katılana ait diğer hesaplardan suça konu hesaba para transferleri sırasında internet erişiminin sağlandığı IP numarasının tespiti" hususları eksiklik olarak belirtilmiştir.

16.CD.'nin 13.02.2018 gün, 2017/2966 E- 2018/380 K sayılı kararında, "Olay tutanağı ile görüntü ve DVD inceleme tutanaklarına göre sanığın elinde bulunan taş ile kolluk görevlilerine karşı üzerine atılı eylemi gerçekleştirdiği anlaşılmakla",denilerek eylemin sabit olduğuna karar verilmiştir.

Dijital delillerin diğer delillerle birlikte değerlendirilmesi, çelişki oluşturmaması gerekmektedir.

16.Ceza Dairesinin 27/02/2018 günlü (2017/3067 E- 2018/504 K) kararında ve benzer birçok kararında, "elde edilen birden çok dijital delillerin incelemelerinin tamamlanması ve bir bütün halinde ele alınması, diğer delillerle birlikte ele alınması gerektiğine, suçun işlenip işlenmediğinin buna göre değerlendirilmesi gerektiğine" vurgu yapılmaktadır.

Dijital deliller üzerinde suça ilişkin bulgu ve emarelerin bulunup bulunmadığının tereddüte yer vermeyecek şekilde tespiti yönünden bilirkişi incelemesi yaptırılması da ayrıca önem taşımaktadır.

Yargıtay 8.Ceza Dairesinin 13.01.2020 gün, 2018/5042 E- 2020/560 K sayılı kararı ve birçok kararında, " sanığın kullandığı bilgisayar kütüğünde bilirkişi incelemesi yaptırılarak suç konusu eylem ile ilgili bulgu ve emarelerin bulunup bulunmadığı kesin olarak tespit edildikten sonra hukuki durumunun tayin ve takdiri..." denilmek suretiyle, gerektiğinde bilirkişi incelemesi yaptırmanın önemi vurgulanmıştır.

Aynı dairenin 03/02/2015 günlü (2014/19342 E-2015/2322 K sayılı) kararında ve benzer birçok kararında ise, "şikayetçi ve sanığın bilgisayarlarına el konularak hard diskleri incelenip bilgisayarlar arasında bağlantı ve veri akışı olup olmadığının tespiti .....gerektiğinde bilirkişiden de görüş alınması" lüzumu vurgulanmıştır.

13.Ceza Dairesinin 14.01.2013 tarihli kararında (2011/28624 E-2013/1172 K),

"işyerinde bulunan güvenlik kamerasından elde edilen görüntülerin sanıktan temin edilecek görüntülerle karşılaştırılması gerektiğine" karar vermiştir.

Aynı dairenin 03/06/2014 tarihli kararında ise (2013/17864 E-2014-19714 K), "SMS mesaj delili diğer delillerle birlikte değerlendirildiğinde hukuka uygun delil" olarak kabul edilmiştir.

1.Ceza Dairesinin 17/10/2012 tarihli bir kararında (2012/2350 E-7688 K) bir cinayet yargılama dosyasına ilişkin olarak, "olay anına ilişkin görüntüleri içerir MOBESE kamerası görüntülerinin görüntü kalitesinin iyileştirilmesi ve görüntüdeki şahıslar ile ellerindeki suç eşyasının tespiti yönünden bilirkişi raporu alınması gerektiğine" karar verilmiştir.

Anılan kararda hukuka uygun delil vurgusu yapılmıştır (CMK 216-217). Aynı dairenin 16/01/2012 tarihli bir kararında ise (2008/10249 E- 2012/48 K), "soruşturma aşamasında temin edilen olay anı ve öncesine ilişkin görüntüleri içeren güvenlik kamerası görüntülerinin bilirkişiye çözümlettirilmesi ile çözüm tutanaklarının duruşma sırasında taraflara okunması ve diyeceklerinin sorulması gerektiğine" işaret edilmiştir.

16.Ceza Dairesinin 12.03.2018 gün, 2017/3892 E-2018/645 K sayılı kararında ise, "suça sürüklenen çocuğun olay esnasındaki fotoğraf ve video görüntülerinin, suça sürüklenen çocuktan temin edilecek..... mukayeseye elverişli fotoğraflarla birlikte Adli Tıp, Tübitak veya TRT gibi uzman kuruluşlara gönderilip görüntü ve fotoğraf analizleri yaptırılması" gerektiği vurgulanmıştır.

İletişimin tespitine ilişkin ses kayıtlarına itiraz edildiğinde "kayıtların analizinin yaptırılması" gerekmektedir. Yargıtay ceza daireleri analiz yaptırılmamasını eksiklik olarak görmektedir.(10.CD.07/02/2012 gün, 2011/3839 E - 2012/741 K)

Dijital delillere ilişkin incelemenin tarafsız bilirkişiye yaptırılması gerekmektedir.

9.Ceza Dairesinin 03/02/2011 günlü kararında (2009/3774 E-2011/767)," sanıkların evinde yapılan aramada ele geçirilen CD'lerin çözümünün tarafsız bilirkişiye yaptırılması gerektiği" ifade edilmiştir.

Dosya kapsamı itibariyle yeterli delil mevcut olduğunda, dijital delil inceleme sonucunun beklenmesi gerekmeyebilecektir.

Nitekim Yargıtay 16.Ceza Dairesi dosyada mevcut diğer delillerle mahkumiyeti yeterli gördüğünde, bylock tespit tutanağı ya da diğer dijital delillerin inceleme sonucunun beklenilmesini gerekli görmemektedir. Daire 23.05.2019 gün, 2019/2019/2863 E-2019/3765 K sayılı kararında (Benzer birçok dosyada) " Tüm dosya kapsamı gözetilerek diğer delillerin atılı suçun sübutu için yeterli olduğu görülmekle....." diyerek dijital delillerin tamamlanmamasını

eksiklik olarak görmemiştir)

Sonuç olarak Yargıtay ceza ve hukuk daireleri, dijital verilerin delil değerini kabul etmekte, içeriğini kararlarında tartışmaktadır.

D-TÜRK HUKUK SİSTEMİNDE BİLİŞİM SUÇLARI

Dijital deliller bağlamında son yıllarda giderek artan bilişim suçları kavramından bahsetmek gerekmektedir.

Tüm dünya gibi Türkiye'de de bilişim alanında işlenen suçların sayısı hızla artmaktadır. Ankara Emniyet Müdürlüğü'nün yaptığı bir araştırmaya göre son yıllarda özellikle kredi kartı dolandırıcılığı, bilgi hırsızlığı, çocuk pornografisi, sistemlere izinsiz erişim, özel hayatın gizliliğini ihlal, kişisel verilerin ele geçirilmesi ve telif haklarının ihlali suçlarına sıklıkla rastlanmaktadır.(Bilişim Suçları Kapsamında Dijital Deliller/Makale, Yusuf Uzunay-Mustafa Koçak, Ankara Emniyet müdürlüğü, Bilgi İşlem Şube Müdürlüğü)

Dijital ortamlarda işlenebilen suçlar yönünden Cumhuriyet Başsavcılıklarında ve emniyet birimlerinde özel birimler oluşturulmuştur. Bu birimlerin geliştirilmesi yanında, yargılama sürecinde de uzman mahkemelerin bulunması, bu çerçevede işbölümü düzenlemesi kaçınılmaz hale gelmiştir. Ayrıca hukuk öğretisinde dijital delil ve bilişim suçları kavramının yeterince yer almadığını görmekteyiz.

Türk hukuk sisteminde; bilişim sistemine girme, veri yerleştirme, verileri yok etme, gizleme, sistemlerin işleyişini engelleme ve bozma, bu yöntemlerle haksız yarar sağlama eylemleri doğrudan bilişim suçları kapsamında cezalandırılmayı gerektirecek şekilde düzenlenmiştir. Ayrıca bankalarca bilişim sistemleri ile bağlantılı olarak hazırlanıp kullanıma sunulan banka veya kredi kartlarına yönelik haksız yarar sağlama, sahte üretme, bu şekilde üretilmiş sahte kartları kullanarak yarar sağlama gibi eylemler de bilişim suçları kapsamında düzenlenmiştir.

Düzenlenen bilişim suçları yanında, yukarıda anlatıldığı üzere internet ortamında işlenebilen tüm suçlar yönünden de dijital veriler delil niteliği taşıyabilmektedir.

1 Haziran 2005 tarihli yargı reformuyla ceza hukukumuza ayrıntılı olarak giren bilişim suçları kavramı yönünden, uygulamaya yönelik bazı tereddütlerin/farklı yorumların halen sürdüğünü vurgulamakta yarar bulunmaktadır.

Uygulamada birçok eylemin yanlış değerlendirildiğine, davaların yanlış ya da eksik açıldığına, cumhuriyet savcılıkları ve mahkemelerce farklı değerlendirilmelerle yetkisizlik/görevsizlik kararları verildiğine, soruşturmaların/yargılamaların gereksiz uzadığına, delillerin kaybolduğuna sıklıkla rastlanmaktadır. (Gül, age. s.9)

Ayrıca bilişim suçları genellikle, Türk Ceza Kanununda düzenlenen özel hayatın gizliliğini ihlal (md 134), kişisel verilerin kaydedilmesi(md.135) verileri hukuka aykırı olarak ele geçirme (md.136), hırsızlık (md.141 vd.) dolandırıcılık (md. 157-158), güveni kötüye kullanma (md.155) gibi suçlarla sıklıkla karıştırılmakta ya da bilişim suçları yanında gerçek içtima kuralları gereği anılan suçların da oluşabileceği gözönünde tutulmamaktadır.

Aradan geçen süreye rağmen, uygulamaya yön verecek yüksek mahkeme kararlarında da farkılıklar gözlenmektedir.

Bu anlamda Yargıtay uygulamaları yönünden bazı örnekleri saymakta yarar bulunmaktadır.

-"Bir kimsenin banka hesabından bir şekilde temin edilen şifre kullanılarak internet yolu ile kendisi ya da başkası hesabına para aktarılması" eylemi, Yargıtay Ceza Genel Kurulunun 17.11.2009 gün, 2009/11-193 E-268 K sayılı kararı (ayrıca 25.11.2014 gün, 2013/13-448 E-2014/524 K) ile, TCK'nın 142/2-e madde ve bendinde yazılı "Bilişim Sistemlerinin Kullanılması Suretiyle Hırsızlık" suçu kapsamında değerlendirilmiştir. Ceza daireleri uygulamaları bu şekilde yerleşmiş olup, tali norm mahiyetindeki TCK'nın 244/4.madde ve fıkrasının uygulanması sözkonusu olmayacaktır.

İnternet ortamında oynanan oyun karakterlerinin çalınması eylemi, Yargıtay 13.Ceza Dairesinin 10.10.2017 gün, 2016/2155 E-2017/10403 K sayılı kararı ile, ekonomik değeri olsa bile TCK'nın 244/4.madde ve fıkrasında yazılı suçu oluşturacağı kabul edilmiştir.

Sonrasında ise Yargıtay 8.Ceza Dairesinin 13.12.2017 gün, 2017/1283 E-14186 K sayılı kararında da aynı doğrultuda karar verilmiş, uygulama bu doğrultuda devam etmektedir.

Ceza Genel Kurulunun 30.03.2010 gün, 2010/11-17 E-2010/65 K sayılı ve 04.03.2014 gün, 1439/104 K sayılı kararlarında belirtildiği üzere, banka veya kredi kartının fiziki varlığının ekonomik değeri olduğu kabul edildiğinden, kartın kullanılması eylemi yanında unsurları oluştuğu takdirde, hırsızlık, güveni kötüye kullanma ya da kaybolmuş veya hata sonucu ele geçmiş eşya üzerinde tasarruf suçlarının da oluşması mümkün olacaktır. Yargıtay 8.Ceza Dairesi kararlarında bu hususa işaret etmektedir.

TCK'nın 245/2 ve 3.maddelerinde düzenlenen suçlar yönünden Yargıtay uygulaması tereddütlere yol açmaktadır.TCK'nın 245/2.madde ve fıkrasında düzenlenen "başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi eğer 3.fıkrada yazılı "sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamış" ise hangi madde uyarınca cezalandırılacaktır?

Yargıtay Ceza Genel Kurulunun 09.05.2017 gün, 2017/11-211 E-2017/259 K sayılı ve 10.10.2019 gün,2016/11-492 E-2019/594 K sayılı kararlarına göre bu durumda geçitli suç sözkonusu olduğundan yalnızca 245/3.madde ve fıkrasından ceza verilmesi gerekmektedir.

Ancak Ceza Genel Kurulunun 2019 yılı aralık ayında verdiği ve henüz gerekçesi yazılmayan kararına göre, bu durumda iki ayrı suç da işlenmiş sayılacaktır.

Anılan Genel Kurul kararlarına dayanılarak bazı dairelerin eylemi tek suç kabul ettiği görülmektedir. (15.CD.14.10.2019 gün, 2017/30401 E-2019/9855 K sayılı)

Ancak bilişim suçları yönünden temyiz mercii olan Yargıtay 8.Ceza Dairesi bahsedilen durumda geçitli suçun söz konusu olmadığını, iki ayrı suçun oluştuğunu kabul etmekte, kararlarında işaret etmekte, uygulamasını bu yönde sürdürmektedir.

Son zamanlarda rastlanan "araçlara tanımlı taşıt tanıma sistemi kartını bir şekilde ele geçirerek kendi aracına yakıt alma" eylemini Yargıtay 15.Ceza Dairesi 17/09/2019 gün, 2017/17461 E-2019/8459 K sayılı kararında "Güveni Kötüye Kullanma" suçu olarak kabul ederken, 8.Ceza Dairesi 08.07.2019 gün, 2019/10316 E-9693 K sayılı kararında bilişim suçu oluştuğu gerekçesiyle eylemin TCK'nın 245/1.maddesinde yazılı suçu oluşturduğuna karar vermiştir.

Dijital deliller ve bilişim suçları yönünden Yargıtay uygulamalarında tereddütlerin önemli ölçüde giderildiği kanaatinde olmakla birlikte, Bölge Adliye Mahkemelerinin kurulması ve sayısının artması sonucu ilgili dairelerin uygulamalarında yeknesaklığın sağlanması da önem arz etmektedir. Keza anılan suçlardan açılan davaların birçoğu -halen CMK'nın 286.maddesi uyarınca temyiz yasa yolu kapalı olduğundan- Bölge Adliye Mahkemelerinde kesinleşmektedir.,

D-ADLİ BİLİŞİM

Dijital verilerin delil değerini koruyabilmesi açısından adli bilişim gittikçe önemini arttırmaktadır. Dijital deliller elde edilirken mutlaka adli bilişim kuralları uygulanmalı, soruşturma adımlarının usulünce ilerlediği belgelendirilmeli, doğruluğu tekrar edilebilir olmalıdır.

Açıklandığı üzere dijital deliller son derece hassas olup, kolaylıkla değiştirilmeye veya bozulmaya elverişlidir. Olağan bir olay yeri inceleme hassasiyetinden daha özenli, deneyim gerektirir bir çalışma yapılmalıdır.

Verilerin usulünce elde edilmemesi, hukuki zemin dışına çıkılması durumunda kötüye kullanma iddiaları gündeme gelebilmekte, sonradan oluşturulduğu şüphesi nedeniyle delil değeri zarar görmektedir. Bu nedenle dijital delillerin gizliliği, bütünlüğü, denetlenebilirliği korunmalıdır.

Özellikle facebook, twitter, instagram, whatsapp gibi yaygın olarak kullanılan sosyal paylaşım siteleri kullanılarak işlenen suçlarda yer sağlayıcı şirketlerin ABD menşeli olması nedeniyle (çocuk pornografisi, uyuşturucu temini, terör suçları gibi suçlar haricinde) bilgi temininde güçlük çekilmektedir. Ayrıca temin edilecek bilgilerin delil değeri de tartışma konusu olacaktır.

Bu nedenle özellikle soruşturma aşamasında şüphelilerin kullandığı dijital aygıtlar üzerinde yapılacak incelemeler son derece önem taşımaktadır. Bir bilgisayar/elektronik mühendisi-programcısı çoğu zaman yeterli gelmemektedir.

Dijital alanda işlenen suçlar yönünden bilgi sahibi, inceleme konusu sistem/program/yazılım konusunda yeterli bilgiye sahip, teknolojik gelişmeleri, siber teröristlerin suç işleme yöntemlerini yakından takip eden uzmanlara ihtiyaç bulunmaktadır. Ancak özel bilgi ve tecrübe gerektiren bu alanda uzman sayısı son derece yetersizdir.

Zamanında uzman incelemesine tabi tutulmayan dijital delillere zamanla ulaşılamamakta, delil değeri kalmamakta, bu nedenle yargılamalar delil yetersizliğinden beraatle sonuçlanmaktadır.

Ahmet GÜL

Yargıtay

Cumhuriyet Savcısı

YARARLANILAN KAYNAKÇA

1-Bilişim Suçları ve İnternet İletişim Hukuku, Dr.M.Volkan Dülger, İstanbul Bilgi Ün.Hukuk Fak. Seçkin Yayınevi, 2012-2.Baskı

2-Doğrudan-Dolaylı Bilişim suçları, Ahmet GÜL, Yargıtay Cumhuriyet Savcısı, Seçkin Yayınevi, 2017-2.Baskı

3-Dijital Delil ve İletişimin Denetlenmesi, Prof.Dr.Çetin Arslan, Hacettepe Ün.Hukuk Fak. Haziran-2014 9.Türkiye Ceza Hukuku Günleri Sempozyum Sunumu.

4-Bilişim Suçları Kapsamında Dijital Deliller/Makale, Yusuf Uzunay-Mustafa Koçak, Ankara Emniyet müdürlüğü, Bilgi İşlem Şube Müdürlüğü.

5-Türk Ceza Hukuku Özel Hükümler, Prof. Mahmut Koca-Prof.İlhan Üzülmez, Adalet Yayınevi,2.baskı, Ankara 2015