Yüzüncü Yıl Üniversitesi
Fen Bilimleri Enstitüsü Dergisi

http://dergipark.gov.tr/yyufbed

Derleme makalesi/Review article

Dijital Kanıtlarının İncelemeleri ve Hukuki Boyutu

İlker KARA[*1]

[1]Çankırı Karatekin Üniversitesi, Eldivan Sağlık Hizmetleri Meslek Yüksek Okulu, Çankırı Türkiye
*karaikab@gmail.com

Makale Bilgileri

Geliş: 02.06.2019
Kabul: 19.09.2019
Online Yayınlanma Aralık.2019

Anahtar Kelimeler
Kişisel veriler, Bilişim Suçları, Türk Ceza Kanunu, Ceza Muhakemesi.

Öz: Gelişen teknoloji insanlara getirdiği yenilikler ve kolaylıklar kadar yeni sorunları ve tehditleri de ortaya çıkarmıştır. Özellikle bilişim alanında büyük bir hızla artan suç türü ve oranı tüm toplumları derinden etkilemektedir. Bilişim suçlarıyla mücadele kapsamında ulusal ve uluslararası boyutta cezai yaptırımlar, uygulama, usül ve yöntemleri kanunlarla düzenlenmiştir. Fakat her geçen gün yeni suç türü ve yöntemlerinin ortaya çıkması yasal düzenlemelerin bu suçlarla mücadele edilmesini güçleştirmektedir. Ülkemizde bilişim suçları ile mücadele 5237 sayılı Türk Ceza Kanunun (TCK) 134 ile 139 ve 5271 sayılı Ceza Muhakemesi Kanunun (CMK) 134 üncü maddesi ile düzenlenmiştir. Bu çalışma, bilişim suçlarıyla mücadele de halen kullanılan yasal düzenlemeleri uygulama boyutunu değerlendirerek yaşanan sorunlar için çözüm önerileri sunmaktadır.

Examining Digital Evidence and Legal Dimension

Article Info

Received: 02.06.2019
Accepted: 19.09.2019
Online Published December.2019

Keywords
Personel Data, Cyber-Crimes, Turkish Law, Criminal Procedure.

Abstract: Advances in technology has brought new challenges and threats to people as well as innovations and conveniences. The crime types and the rate that is increasing rapidly especially in the field of information and communication technologies (ICT) affect all societies profoundly. Within the scope of the fight against ICT crimes, criminal sanctions at national and international level, implementations, procedures and methods are regulated by law. However, the emergence of new crime types and methods makes it difficult for legal regulations to cope with these crimes. In Turkey, the fight against ICT crimes has been organized with Articles 5237 and 139 of the Turkish Penal Code (TPC) No.5237, Article 134 of the Criminal Procedure Code (CPC) No.5271. This study evaluates the implementation of the legal regulations currently used in the fight against ICT crimes and provides solutions for the problems experienced.

1. Giriş

Teknolojide yaşanan gelişilmelere birlikte bilişim sistemleri hayatımızın her alanına girmiş bulunmaktadır. Bu gelişmelere siber suçlular hızlıca ayak uydurarak yasa dışı faaliyetlerini genişletmeye devam etmektedir. Özelikle internet üzerinden çok rahatlıkla yapılabilen siber saldırı araçları, siber suçluların hedeflerine ulaşmada en büyük araçları konumundadır. Bilişim suçu kötü niyetli kişiler tarafından bilişim sistemlerini kullanarak işlenen suçlar olarak tanımlanmaktadır (Brown, 2015; Wall, 2017; Ngo, 2017).

Günümüzde yapılan siber saldırılar; verileri yasa dışı erişme, verilerin yetkisiz olarak değiştirme ya da tamamen silme üzerine yoğunlaşmaktadır (Yar, 2019; Dawson, 2015). Bu amaçla

özel olarak tasarlanan zararlı yazılımlar hedef sistemlere sızmakta ve sistemleri kullanılmaz hale getirmektedir (Küçükvardar, 2015). Bu tehditler her geçen gün güncellenen yeni nesil zararlı yazılımlarla büyümektedir. Tehdit ile mücadele devam etmekle birlikte tam anlamıyla üstesinden gelinememiştir.

Yüksek maddi getirisi ve düşük yakalanma nedeniyle riski nedeniyle bilişim yoluyla işlenen suçlar her geçen gün artmaktadır (Atasever, 2019). Artan bilişim suçlarının soruşturulması ve aydınlatılmasında bilişim incelemeleri en önemli bölümünü oluşturmaktadır. Ülkemizde adli bilişim incelemeleri 5237 sayılı Türk Ceza Kanunun 134-39 uncu maddeleri hükümlerince uygulanmaktadır (Özen, 2015). Gelişen teknolojiyle her geçen gün yeni suç ve suç türlerinin çıkması bu suçlarla aktif mücadele ve hukuki boyutunu sorunlu bir hale getirmektedir. Bu çalışmada dijital kanıtlara müdahale yöntemi, adli bilişim incelemelerinin uygulamasında yaşanan sıkıntılara değinerek hukuki boyutunun yeterliği konusuna eğilmektir.

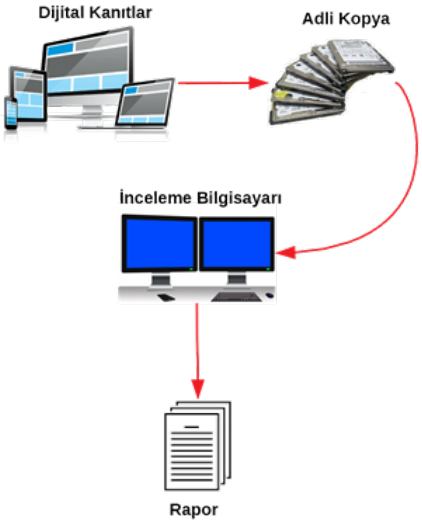
2. Adli Bilişim İncelemeleri

Adli bilişim incelemeleri kolluk kuvvetleri veya özel laboratuvarlarda bilişim uzmanları tarafından yapılmaktadır (Orta, 2015; Varol, 2017; Kara; 2018). Adli bilişim incelemeleri genel olarak iki bölümden oluşmaktadır. Bunlar; a) Dijital delillere müdahale ve b) İnceleme sürecidir.

2.1. Dijital verilere müdahale:

Adli bilişim incelemelerin ilk bölümü dijital verilere müdahaledir (Kaursar, 2017). Bu bölüm adli inceleme sürecinin sağlıklı bir şekilde tamamlanabilmesi için hayati öneme sahiptir. Bu aşamada yapılacak olası hatalar sürecin tamamını etkileyerek belki de inceleme sürecinin başlamadan bitirebilmektedir. Adli inceleme sürecinde şüpheli tarafın davalarda en çok itiraz konusu olan bölüm dijital verilere müdahale ve delilerin usulüne göre toplanması olmaktadır. Bu nedenle adli uzmanlar dijital verilere müdahale ederken çok dikkatli olması gerekmektedir. Dijital veriler bilgisayar kütüklerinde depolanabildiği gibi uçucu verilerde sistemde bulunabilmektedir. Bu nedenle canlı sistemlere müdahale ederken öncelikle uçucu verilerin adli kopyasını alınması gereklidir. Uçucu veriler sabit diskte depolanmamaktadır. Uçucu veriler rasgele erişimli bellek (RAM)'de depolanmaktadır ve suç konusu bilgisayarın güç akışı kesildiği anda veriler silinmektedir (Çakır, 2013).

Sabit veriler ise uluslararası standartlara uygun olarak toplanmalıdır. Bu amaçla oluşturulan ve herkes tarafından kabul gören sistem ve araçları kullanmalıdır. Dijital verilere müdahale şartlar elverdiği şekilde olay yerinde yapılmalıdır. Olay yerinde müdahale edilemeyen deliler laboratuvar ortamımda müdahale edilmelidir. Ayrıca olası şaibeleri ortadan kaldırmak için alınan adli kopyaların bir nüshası müştekiye verilmelidir. Dijital verilere müdahale yöntemi Şekil 1'de verilmiştir.



Şekil 1. Dijital verilere müdahale ve inceleme yöntemi.

2.2. İnceleme süreci

Soruşturma kapsamanın da toplanan veriler güvenli bir ortamda çalıştırılarak inceleme aşamasına geçilmektedir (Casey, 2011; Saferstein, 2002). Suç türü ve incelenen materyalin türüne (Bilgisayar, cep telefonu, tablet vb.) göre farklı analiz programları kullanılmaktadır. İnceleme süreci temel olarak dört bölümden oluşmaktadır. Bunlar; i) Verileri elde etme, ii) Verileri tanımlama, iii) Verilerin değerlendirilmesi ve iv) Raporlamadır.

i. Verileri elde etme: İnceleme sürecinin ilk adımı olarak bilinmektedir. Bu süreçte verilerin dijital materyalde bırakacakları olası izler tespit edilmeye çalışılır. Sonraki adımdaki verilerin tanımlanması muhtemel suç unsurlarının teknik incelenmesi adımını oluşturur.

ii. Verilerin tanımlanması: Veriler elde edildikten sonra bunların tanımlanması gereklidir. Tanımlanan veriler suç unsu olup olmadığını değerlendirme adımda kullanılmaktadır.

iii. Verilerin değerlendirmesi: Bu aşamasında kesin olarak suça konu olan veriler tespit aşaması ve güvenilir şekilde başka bir kişi tarafından da ulaşılabilir olması sağlanmaktadır.

iv. Raporlama: Son adımda elde edilen veriler uygun formatta dokümantasyonunun yapılarak adli merciler iletilmek üzere hazırlanmaktadır.

3. Dijital Kanıt İncelemelerinin Hukuki Boyutunun Değerlendirilmesi

Adli bilişim incelemeleri 5237 sayılı Türk Ceza Kanunun 134-139 uncu maddeleri kapsamında yapılmaktadır (Centel, 2002). Bahse konu kanun maddelerinde "Özel hayatın gizliliğini ihlal - Kişisel verilerin kaydedilmesi - Verileri hukuka aykırı olarak verme veya ele geçirme - verileri yok etmeme ve Şikâyet " başlıkları altında değerlendirilmektedir.

Kişisel veri; bireyin kimlik bilgilerinden telefon numarası, araç plakası, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP (İnternet Protokol) adresi, e-mail adresi, cihaz bilgileri, sosyal paylaşım site üyelikleri, ailevi bilgileri gibi kişiyi doğrudan veya dolaylı olarak ilgilendiren tüm verilere denilmektedir.

24 Mart 2016 tarihinde "Kişisel Verilerin Korunması Kanunu" yasalaşmıştır. Kabul edilen kanuna göre, kişisel verilerin ancak usul ve esaslara uygun olarak incelenebileceği belirtilmiştir. Kişisel verilerin incelenmesi için ilgili kişinin açık rızası gerekli görülmüştür. İlgili kişinin açık rızası aranmaksızın, aşağıdaki şartlardan en az birinin varlığı halinde verilerin incelenebileceği ön görülmüştür;

İlgili kişi istenildiği takdirde, kişisel verilerin incelenip incelenmediğini öğrenebilecek, incelenen bilgiler hakkında bilgi talep edebilecektir. Bu bilgiler eğer üçüncü kişilere aktarılmışsa bu durum ilgili kişiye bildirilecektir. Kişisel bilgilerin mahremiyeti korunacak, eksik veya yanlış incelenmesi halinde gerekli düzeltmelerin yapılmasını isteyebilecektir. İncelenen kişisel verilerin silinmesini veya yok edilmesini isteyebilecek, bu durumlardan zarara uğraması halinde ise zararın giderilmesini talep edebilecektir.

Özel hayatın gizliliği, herhangi bir kısıtlamaya ve zorlamaya bağlı olmaksızın kişisel özgürlük kapsamında değerlendirilmelidir. Özel hayatın gizliliğinin korunması gerekliliği açık iken kamusal faaliyetler için bir takım müdahaleler yapılması bazı durumlarda zorunlu hale gelebilmektedir. Kişisel verilerin incelenmesi olay yerinde ve adli bilişim laboratuvarlarında alınan adli kopyalar için uluslararası standartlar da geçerli teknikler kullanılarak analiz edilmektedir. Bu bağlamda adli incelemelerde veri bütünlüğünün sağlanması için alınan adli kopyalarda MD5, SHA1 değerlerinin yer alması gerekmektedir.. Bu değerler her dijital materyalin parmak izi gibi olup herhangi bir müdahalede (veri ekleme-silme) değişmektedir. Bu tedbir yapılan tüm işlemlerin tarafsızlığını sağlamaktadır. Adli bilişim uzmanlarınca suç konusu materyallerin incelemesinin usul ve yöntemi CMK 134. maddesinde düzenlenmiştir.

CMK 134. maddesi "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlıkları altında değerlendirilmektedir (Centel, 2002). Söz konusu maddede; bilgisayar, bilgisayar programları ile bilgisayar kütükleri terimlerinin kullanılması uygulamada anlam kargaşasına neden olmaktadır. Bu durum veri işleyebilen materyallerin (Cep telefonu, Hard disk, CD, DVD, video kayıt cihazları vb.) bu kapsamda değerlendirmenin yoruma açık hale getirilmektedir. Avrupa Konseyi Siber Suçlar Sözleşmesinde 19. maddesinde; "bilgisayar sistemi ya da bu sistemin parçası ve bunlarda saklanan veriler ile bilgisayar verilerinin saklandığı cihazlar" şeklinde

tanımlanarak bu kargaşa engellenmiştir (Özen, 2015). Ayrıca "başka surette delil elde etme imkânının bulunmaması halinde" ibaresinin değiştirilmesi gereklidir. Bu durum dijital kanıtlardan elde edilen verilerin sanki son çareymiş gibi algılanmasına sebep olmaktadır. Ayrıca sadece şüphelilerin kullandığı dijital materyaller kavramı tanımlanmıştır. İlgili kanunu düzenlemede mağdur, maktul, şikâyetçilerinde dijital materyallerin incelenmesini talep edebileceği durumlarda göz önünde bulundurulmalıdır.

Uygulama yönünden adli kopya (imaj) alma işlemlerinin olay yerinde tatbik edilmesi uygulamada büyük sorunlara neden olmaktadır. Adli bilişim uzmanlarının olay yerinde imaj alma cihazların [Tableau TD1, TD2 veya TD3 (Adli Kopyalama Cihazı)] sağlıklı bir şekilde kullanılabilmesi için uygun elektrik alt yapısı ve araç, gereçlerine ihtiyaç duyulmaktadır. Bu gereksinmelerinin tam olarak sağlanamaması nedeniyle suç şüphesi olan dijital materyallerin olay yerinde el koyularak adli imajlarının laboratuvar ortamında alınması daha sağlıklı olacaktır. Bu nedenle ilgili kanun maddesinde adli imaj alma işlemlerinin hangi şartlar altında yapılacağı tanımlanması gereklidir. Bu duruma istisnayı durumlarda olay yerinde zorunlu olarak adli imaj alınmasında eklenebilir (Örneğin; kurumsal bir şirketin işlerinin aksamaması için sunucularının adli imajı olay yerinde alınabilir). İmaj alma işlemlerinin hangi durumlarda ve nasıl uygulanması gerekliliği detaylı olarak kanun maddesinde açıklanarak kanun maddesinin düzenlenmesine ihtiyaç duyulmaktadır.

CMK'da, şifrenin çözülememesi, gizlenmiş verilere ulaşılamaması ya da adli imajının alınabilmesi için olay yerinde el koyma işleminin yapılacağı tanımlanmıştır. Ancak söz konusu sonuç uygulamalarda sorunlara neden olmaktadır. Çünkü şüpheli materyalin şifreli olduğunu tespit etmek için olay yerinde uygun programlar ile incelemeler yapılması zorunludur. Bu tespit işlemi zaman alıcı ve karmaşıktır. Olay yerinde bu süreci takip etmek ve sonuçlandırmak ön görülemeyen birçok sorunları içermektedir.

Adli imaj alınacak dijital materyalin kapasitesi ve sayısı öngörülemediğinden kopyala işlemi için kullanılacak boş disklerin sayısı ve kapasitesi tahmin edilememektedir. Ayrıca adli imajların alınacağı boş disklerin kimin tarafından karşılanacağı belli değildir (Cumhuriyet Savcılıkları ya da Kolluk güçlerinden mi?). Olay yerinin güvenliğinin alınmasında büyük bir sorun olarak görülmektedir. Adli imaj alma işlemlerinin saatler hatta günler sürdüğü durumlar yaşanabilmektedir. Özellikle terör faaliyetleri gibi sorunlar olay yerinde güvenlik tehlikelerinin oluşmasına neden olmaktadır.

Olay yerinde el konulan dijital materyalin adli imajının alınabilmesi halinde suç konusu materyalin zaman kaybedilmeden şüpheliye geri iade edilmesi gerekliliği vurgulanmıştır. Avrupa Konseyi Siber Suçlar Sözleşmesi "Saklanan bilgisayar verilerinin aranması ve bunlara el konulması" başlıklı 19. maddesinin 3. fıkrasının d bendinde kolluk kuvvetlerince suçun devamını engellemek amacıyla suç şüphesi olan veriler kullanılamaz hale getirilmesi gerekli olduğuna değinilmiştir (Centel, 2002). Özellikle çocuk pornosu gibi suçların verileri (resim veya videoları) tamamen kullanılmaz hale getirilmesi gerekliliği vurgulanmıştır. Bu durum ülkemizdeki ilgili maddelerde herhangi bir düzenleme bulunmamaktadır. Bu sonuç adli bilişim uzmanları tarafından farklı yorumlanmasına yol açmaktadır. Bazı durumlarda suç unsurunun teslim edilmediği bazı durumlarda herhangi bir işlem yapılmadan suç konusu şüpheliye teslim edilmektedir. Çocuk pornosu veya kişisel bilgiler (kredi kart bilgileri, banka kullanıcı bilgileri gibi) içeren suç unsuru materyallerin teslim edilmesi ne kadar doğru bir uygulamadır? Bu ve benzeri durumların suçun devam etmemesi ve yeni suçlara yol açmaması için nasıl bir yol izleyeceği belirlenmelidir.

4. Sonuç

Bilişim ve teknolojik alanda yaşanan hızlı gelişmeler yeni suç ve suç türlerini ortaya çıkmasına neden olmuştur. Bu sonuç suç ve suçlu kavramının tanımlarını değiştirerek ceza ve adalet sistemi için de farklı bir bakış açısı geliştirilmesini zorunlu hale getirmiştir. Ülkemizde içinde bulunduğu pek çok ülke bu konu ile ilgili tedbirler ve yasal düzenlemeler için çalışmalara devam etmektedir.

Kişisel verilerin korunması hakkı, temel insan hak ve özgürlükleri arasında yer almaktadır. Kişisel verilerin korumasındaki amaç, bireylerin kişiliklerinin özgürce gelişmesine olanak sağlayarak, devlet otoritesi veya başka kişiler tarafından rahatsız edilememesini sağlamaktır. Teknolojide yaşanan

gelişmeler geleneksel yöntemlerle yapılamayacak birçok kişisel veriye ulaşılabilir kılmıştır. Bu durum kötü niyetli kişiler için devletlerarası sınır tanımayan bir fırsata dönüşmüştür. Bu sonuç kişisel verilerin korunmasına ilişkin ulusal ve uluslararası düzenlemelere ihtiyaç duyulmuştur. Bu bağlamda uluslararası bilgi paylaşımı için ülkelerin iç mevzuatlarının da uyumlu olma ihtiyacı da önemli bir etken olmuş ve 24.03.2016 tarihinde "Kişisel Verilerin Korunması Kanunu" yasalaşarak yürürlüğe girmiştir.

Kişisel verilerin korunmasında birinci sorumlu kişinin kendisidir. Sorumlu kişi gerekli önlemleri almak zorundadır. Bu konuda kişi gerekli çabayı göstererek farkındalık düzeyini artırmalıdır. Tek başına teknolojik önlemler yeterli değildir. Kişilerin, özgürlüğün nerede başlayıp nerede bittiğini bilmesi gereklidir. Suç işlenmesi noktasında yasal otorite müdahalesi kaçınılmaz olmaktadır.

Teknolojide yaşanan hızlı gelişmeler sebebiyle ceza muhakemesi hükümleri, suçlar ile etkin biçimde soruşturulması açısından uyum göstermek zorundadır. CMK 134. maddesi bahsedilen "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde" kavramı yerine "Bilgi depolayabilen, işleyebilen ve değiştirebilen her türlü araç ve gereçler" olarak tanımlanması maddenin yanlış veya eksik yorumlanmamasına ve anlam çelişkisini ortadan kaldıracaktır.

CMK'nın tanımlar kısmında; şüpheli, sanık, müdafi, vekil, soruşturma, kovuşturma aşamasında söz konusun dijital materyaller terimleri detaylı olarak tanımlanması gereklidir. CMK 134. maddesinin 2. fıkrası kapsamında alınan adli imajlar sürecinde şüphelinin veya avukatının bulunabilmesi belirtilmemiştir. Bu durum farklı yorumlanabilmekte bazı durumlarda şüphelinin veya avukatının hazır bulunmasına izin verilmemektedir. Bu sonuç yapılan işlemler hakkında çekinceler ve itirazlara neden olmaktadır. Yapılan imaj alama işlemlerinin uygulayıcılar tarafından video ile kayıt altına alınması olası itirazlara karşı etkili bir çözüm olabilir. Bu nedenle CMK 134. Maddenin şu şekilde güncellenmesi uygun olacağı değerlendirilmektedir.

CMK 134. Maddesinin 4. Fıkrasında belirtilen "alınan imajın verilmesi" kavramı şüpheliye adli imajın verilmesini zorunlu hale getirmiştir. Bu durum bazı suçların (çocuk pornosu, kişisel bilgiler gibi) işlenmesine devam edilebileceğini ön görememiştir. Bu ve benzeri suçlardan dolayı yapılan adli imaj işlemlerinin kopyalarının verilmemesi gereklidir. Bu suçlar tanımlanarak yapılan incelmeler ve istinat edilen suçlar kapsamında olması durumunda kolluk tarafından kopyaların kullanılmaz hale getirilmesi bu durumun kanun maddesinde yer verilmesi uygun olacağı düşünülmektedir.

Kaynakça

Atasever, S., Özçelik, İ., & Sağıroğlu, Ş. (2019). Siber terör ve DDoS. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 23(1), 238-244.

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, 9(1), 55.

Casey, E. (2011). *Digital Evidence And Computer Crime: Forensic Science, Computers, And The İnternet*. Academic press.

Centel, N., Zafer, H., & Çakmut, Ö. (2002). *Türk Ceza Hukukuna Giriş*. Beta 815 s.

Çakır, H., & Kılıç, M. S. (2013). Bilişim suçlarına ilişkin delil elde etme yöntemlerine genel bir bakış. *Turkish Journal of Police Studies/Polis Bilimleri Dergisi*, 15(3), 23-44.

Dawson, M. (Ed.). (2015). *New Threats And Countermeasures İn Digital Crime And Cyber Terrorism.* IGI Global.

Kara, I., & Aydos, M. (2018, December). Static and Dynamic Analysis of Third Generation Cerber Ransomware. *In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)* (pp. 12-17). IEEE.

Kausar, F., & Alyahya, T. N. (2016). Akıllı Android Telefonlar İçin Fiziksel Adli Imaj Edinim Araçları. *IJCSNS*, 16(11).

Küçükvardar, M. (2015). *Bilişim Devrimi: Reel Gerçekliğin Sanal Gerçekliğe Dönüşümü*. Marmara Üniversitesi Sosyal Bilimler Enstitüsü Gazetecelik AnaBilim Dalı Bilişim Bilim Dalı, Yüksek Lisans Tezi, İstanbul, 1-165.

Ngo, F., & Jaishankar, K. (2017). Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. *International Journal of Cyber Criminology*, 11(1),1-9.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime And Society*. SAGE Publications Limited.

Özen, M., & Özocak, G. (2015). Adli bilişim, elektronik deliller ve bilgisayarlarda arama ve el koyma tedbirinin hukuki rejimi (cmk m. 134). *Ankara Barosu Dergileri*, 73(1), 43-77.

Orta, M. (2015). *Bilişim Suçlarında Adli Analiz* (Doctoral dissertation, Selçuk Üniversitesi Sosyal Bilimleri Enstitüsü).

Saferstein, R., & Hall, A. B. (Eds.). (2002). *Forensic Science Handbook* (Vol. 1). Upper Saddle River: Prentice Hall.

Varol, A., & Sönmez, Y. Ü. (2017). Review of evidence collection and protection phases in digital forensics process. *International Journal of Information Security Science*, 6(4), 39-46.

Wall, D. S. (2017, July). Towards a conceptualisation of cloud (Cyber) crime. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 529-538). Springer, Cham.