DİJİTAL VERİLERİN İMHA SÜREÇLERİNİN TANIMLANMASI VE UYGULAMA YÖNÜNDEN DEĞERLENDİRİLMESİ

***

IDENTIFICATION OF THE DATA DESTRUCTION PROCESS OF DIGITAL DATA AND CONSIDERING IN TERMS OF APPLICATION

DOI: 10.33461/uybisbbd.598590

İlker KARA*

Öz

Gelişen teknolojiyle toplumun her sektörünün dijitalleşme ve iş modellerinin değişmesiyle birlikte düzenli veya düzensiz büyük miktarda veri çıktıları oluşmaktadır. Elde edilen bu verilerin analitik yöntemlerle işlenmesi sonucunda depolanabilmekte, uygun şifreleme yöntemleriyle saklanabilmekte ya da ihtiyaç doğrultusunda kullanılabilmektedir. Dijital verilerin sağladığı bu kolaylıkların yanı sıra büyük miktardaki verilerin yetkisiz kişilerin eline geçmemesi için imha edilmesi son zamanlarda büyük bir sorun haline gelmiştir. Literatürde yapılan çalışmalar genellikle verilerin korunmasına yönelik yapılmış olup, verilerin güvenli imha süreçlerine çok fazla değinilmemiştir. Bu çalışmada dijital verilerin imha süreçleri uygulama yönünden detaylı olarak incelenmiştir.

***Anahtar Kelimeler**: dijital veriler, kişisel veriler, imha.*

Abstract

With the digitalization of every sector, the society and the change of business models, a large amount of data outputs are formed regularly or irregularly. Obtained materials becomes storable as a result of analytical processing and it can be stored with appropriate encryption method or it can be used according to requirements. In adition to the ease of digital data,the destruction of large amounts of data to prevent unauthorized access has become a growing problem lately. Stuides in literature were generally done to protect data but the safe destruction of data has not been addressed much. In this study, the destruction of the processes of digital data was examined in detail.

***Keywords:** digital data, personal data, destruction.*

* Dr. Öğretim Üyesi Çankırı Karatekin Üniversitesi Sağlık Meslek Yüksek Okulu, karaikab@gmail.com
ORCID: 0000-0003-3700-4825

Geliş Tarihi / Received: 30.07.2019
Kabul Tarihi / Accepted: 17.10.2019

1. GİRİŞ

Veri (ing: data); incelenen konu hakkında yapılan araştırma, incelenme, analiz, veya öneriler sonucunda meydana gelen işlenmemiş, farklı kullanıcılar tarafından üzerinde yorum yapmaya imkan sağlayan işlenmemiş ham bilgilere denilmektedir (Yıldız, 2006:157). Dijital veri ise bilişim sistemleri ya da internet ortamında vasıtasıyla oluşturulmuş bilgi paketleri olarak bilinmektedir (Şengül, 2014:17). Dijital veriler, üretici tarafından uzak erişime açılabilir, farklı kullanıcılar tarafından değişiklik yapılarak farklı formatlar ile kaydedilebilmektedir (Jensen, 1986:266). Dijital veriler sahip oldukları bu avantajları nedeniyle kişisel kullanıcılar ya da resmi kuruluşlar tarafından yaygın olarak kullanılmakta birçok uygulama ve hizmetler dijital platformlara taşınmaktadır (Schroeder, 2016:15). Bu durum getirdiği kolaylıkların yanı sıra bazı problemlere de yol açmaktadır.

Bilişim ve iletişimin teknolojinin büyük bir hızla ilerlediği günümüzde birçok veri işleme ve depolama cihazları sayesinde düzenli veya düzensiz büyük miktarda veri elde edilmektedir. Her geçen gün çok hızlı bir şekilde üretilen veriler; iletişim, bankacılık, pazarlama veya kamusal alanda kullanılabilmektedir (Doğan, 2016:56). Bu verilerin türü, kapasitesine ve kullanım alanına göre farklı teknolojiler ile kullanılmakla birlikte güvenlik, erişilebilirlik veya istenmediği durumlarda güvenli olarak imha edilmesi için yeni yöntemler geliştirmeye ihtiyaç duyulmaktadır (Gantz, 2012:5). Bu gelişmelere gerekli önlemleri alamayan kurumlar veya bireysel kullanıcılar için büyük bir sorun haline gelmiştir. Bu amaçla geliştirilen yöntemler etkili olmakla beraber özellikle verilerin güvenli imhası alanında yapılan çalışmalar yetersiz kalmıştır.

2. VERİ KAVRAMI

Veri, bilginin yapılandırılarak depolanabilen hale getirilmesidir (Çetin, 2014:86, Canber, 2006:165). Anlamlı hale getirilen veriler istenilen amaç doğrultusunda bütünleştirilerek kolay analiz edilebilir hale getirilebilir. Veri, "Gizlilik, Bütünlük, Erişilebilirlik, Doğrulama, Yetkilendirme ve İnkâr Edememe" gibi temeller doğrultusunda oluşturulmalıdır (Baykara vd., 2013:231). Elde edilen verilerin belirli bir formatta işlenebilmesi ve gerektiğinde ulaşılabilmesi için veri tabanları oluşturulmuştur. Veri tabanları kullanıcılara verileri kullanarak işlem yapmalarına olanak tanımaktadırlar. Veri tabanı oluşturulması ve etkin şekilde kullanılabilmesi için özel yazılımlara ihtiyaç duyulmaktadır. (Sağıroğlu, 2008:23). Bu amaçla birçok veri tabanı sistemi oluşturulmuştur (Günümüzde en popülerleri; MySQL, Oracle, SQLite, PostgreSQL, Firebird vb.).

Dijital veriler uygun ortamlarda depolanabilme özeliklerine sahiptirler. Herman Hollerith'in geliştirildiği delikli kartlardan günümüz bulut teknolojisine (Online depolama) kadar depolama alanında birçok yöntem geliştirilmiştir (Biles, 1989:604). Depolan verilerin güvenli şekilde silinebilmesi veya yetkisiz kişilerin eline geçmemesi için doğru imhası süreçleri yürütülmesi hem kurumların hem de kullanıcılar için büyük bir sorun haline gelmiştir. Depolanan dijital veriler için literatürde herkes tarafından kabul gören bir imha yöntemi bulunmamakla beraber karşılaşılan problemlere geçici çözüm yolları bulunmuştur (Hughes, 2009:32). Bu sonuç depolanan verilerin kapasitesi büyüklüğü ve depolama cihaz alanlarının sayılarının artması çözülmesi zor bir hale neden olmaktadır (Şişkin, 2018:343). Bu çalışmanın amacı dijital verilerin imha süreçleri içeren pratik imha yöntemleri sunmaktır. Çalışma sonucunda dijital verilerin imhalarının uygulama yönünden karşılaşılabilecek sorunlara karşı çözüm önerileri sunulmuştur.

3. DİJİTAL VERİLERİN İMHA EDİLMESİNİN HUKUKİ BOYUTU

Hukuki kurallara göre uygun olarak oluşturulmuş dijital veriler çeşitli nedenlerle silinmesi gerektiğinde (İşlenmesi gereken sebepler ortadan kalktığında, kanuni zorunluluk veya kişinin rızası

gibi durumlarda) resen veya ilgili kurumun talebi doğrultusunda uygun yöntemlerle silinebilmektedir (Henkoğlu, 2017:243).

3.1. Avrupa İnsan Hakları Sözleşmesi

4 Kasım 1950'de Roma'da imzalanarak 3 Eylül 1953'te yürürlüğe giren "Avrupa İnsan Hakları Sözleşmesi" nin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesinin 1. fıkrasına göre, "Herkes, özel ve aile hayatına, konutuna ve yazışmalarına saygı gösterilmesi hakkına sahiptir" hükümde değinilen "özel hayata saygı hakkı", kişisel verileri de içermektedir (Gölcüklü, 1994:49). İlgili 8. maddenin 2. fıkrasında; "Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasa ile öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin iktisadi refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve hürriyetlerinin korunması için alınması gereken tedbirler bakımından mümkün olabilir." hükmünü öngörülmektedir. Bu bağlamda kişisel verilere kişinin rızasının olmadığı durumlarda yapılan müdahaleler suç kapsamında değerlendirilmektedir.

3.2. Türkiye Cumhuriyeti Anayasası

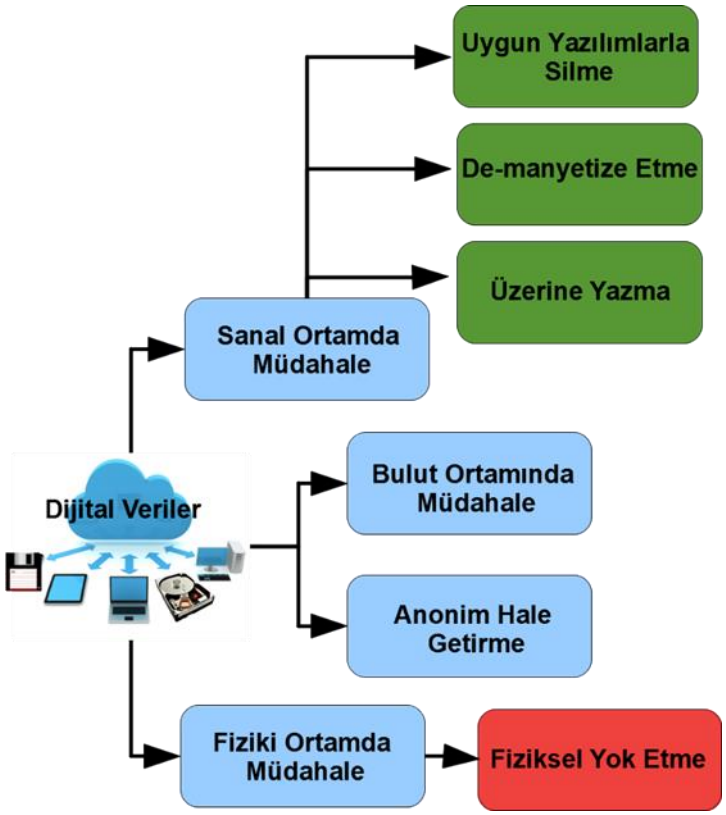
7 Kasım 1982'de yürüklüğe giren 2709 numaralı Türkiye Cumhuriyeti Anayasasının 20. Maddesinin 3 fıkrasında "Herkes, kendisi ile ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığı öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızası ile düzenlenir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü ile düzenlenmiştir (Göztepe, 2011:15). İlgili hükümde kişisel verilerin mutlak korunmasını gerekliliği vurgulanmıştır. Bu bağlamda kişisel verilerin yalnızca kişinin açık rızasıyla işlenebileceği ve kişisel verilerin nasıl korunacağına dair esas ve usullerin ilgili kanunla düzenleneceği öngörülmüştür.

3.3. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

7 Nisan 2016 tarihinde yürürlüğe giren "6698 Sayılı Kişisel Verilerin Korunması Kanunu", kişisel verilerin işlenmesi, özel hayatın gizliliğinin korunması ve temel hak ve özgürlükleri korumak için verilerin işlenmesi ya da silinmesi kurallarını düzenleme amaçlamaktadır (Henkoğlu, 2015:16). Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi ilgili kanun gereğince uygun şartlar altında yapılabilmektedir. Dijital verilerin kişinin rızasını içermeyecek durumlar ve üçüncü şahıslara aktarılmaması için yasal zemini oluşturulmaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanununa aykırı şekilde verilerin işlenmesi durumunda 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde uyarınca bir yıldan üç yıla kadar hapis cezası verilebilmektedir.

4. DİJİTAL VERİLERİ İMHA SÜREÇLERİ

Dijital verilerin silinmesi kullanıcıların hiçbir suretle tekrar erişilemez ve kullanılamaz hale getirilmesi işlemini tanımlamaktadır (Winter, 2013:12). Bu işlemi yapan sorumlu verinin tekrar erişilemez ve kullanılamaz hale getirilmesi için gerekli tüm teknik ve yasal tedbirleri almakla mükelleftir. Dijital verilerin güvenli imhası için pratikte uygulanan ve herkes tarafından kabul gören standart bir yöntem bulunmamaktadır (Chen, 2012:648). Verilerin çeşitliliği, kapasitesi ve depolama alanlarının teknolojik altyapılarının farklılıkları imha yöntemini doğrudan etkilemektedir. Pratik ve güvenli bir imha yöntemin bilinerek doğru şekilde uygulanması dijital verilerin güvenli imhası için gereklidir. Bu amaçla uygulanabilir bir dijital veri imha yöntemi Şekil 1'de verilmiştir.



Şekil 1: Dijital Verileri İmha Yöntemleri.

Dijital verilerin kayıt ortamlarında depolanabildiklerinden kayıt ortamlarına uygun yöntemlerle imha edilmesi gerekir. Bu nedenle imha süreçleri verilerin bulunduğu ortamlara göre müdahale edilmelidir. Dijital verilerin imhası dört başlık altında toplanabilir. Bunlar;

4.1. Sanal Ortamda Müdahale

Sanal ortam, veriler ile elektronik olarak iletişim kurulabilen bir ortamı açıklamaktadır. Veriler uygun depolama cihazlarında tutulduğundan imha edilebilmesi için; Uygun yazılımlarla silme, De-manyetize etme, Üzerine yazma, Bulut (cloud) ortamında müdahale, Anonim hale getirme, Fiziki ortamda müdahale, Fiziksel yok etme adımları uygulanabilir.

4.1.1. Uygun yazılımlarla silme: Hard disk, hafıza kartları, Taşınabilir bellekler, disketler ve CD-DVD'lerde depolana verilerin kalıcı ve güvenli olarak program vasıtasıyla silinme işlemidir. Bu işlemlerde verilerin tam olarak ve güvenli bir şekilde silindiği kullanılan program vasıtasıyla doğrulanabilir. En çok kullanılan yazılımsal silme programları; Moo0 Anti-Recovery, Disk Redactor, Eraser, SDelete, FileShredder, Turbo Shredder vb.

4.1.2. De-manyetize etme: Hemen hemen tüm depolama cihazları manyetik alana duyarlı malzemelerden üretilmiştir. Bu nedenle istenmeden yüksek bir manyetik alana maruz kalması cihazın tekrar kullanılamaz hale getirebilmektedir. Bu durumdan yola çıkarak verilerin imha edilmesi istenilen cihazların çok yüksek bir manyetik değere sahip özel cihazlara uzun süreli (ortalama 1 saat) maruz kalması üzerindeki verilerin tekrar okunamayacak biçimde bozulmasına neden olmaktadır.

4.1.3. Üzerine yazma: Dijital veriler bulunduğu depolama cihazlarında 0 ve 1'lerden oluşan düzenli yapılardan oluşmaktadır. Bu yapılar üzerine rasgele 0 ve 1'lerden oluşan rasgele yazılırsa verinin kurtarılması engel olunur. Bu işlem en az yedi kez tekrarlanması gereklidir. Bu işlemler için kullanılan en yaygın programlar; Disk-Wipe, R-Wipe & Clean, HDD Data Wiping vb.

4.2. Bulut (cloud) ortamında müdahale: Bilgisayar ve benzeri internet tabanlı cihazların kullanıcılar için verilerini depolayabilen istenildiği zaman ulaşılabilenini sağlayan hizmette bulut ortamı denilmektedir. Bulut sistemindeki verilerin imhası özel programlar vasıtasıyla yapılabilmektedir. Bu programlardan en yaygın kullanılanları Office 365, Dropbox'lar, Salesforce vb. Bu tedbirlere ek olarak eğer bir bulut sisteminden hizmet alınıyorsa kullanıcılar için ayrı ayrı şifreleme anahtarı oluşturularak istenilen kullanıcının kaynak erişimi hizmet sağlayıcılara erişim anahtarı iptal edilmesi gereklidir.

4.3. Anonim hale getirme: Anonim hale getirme işlemi, verilerin tüm ya da bir kısmını silerek ya da tanınmayacak şekilde değiştirilerek verinin tanımlayıcı ve kişiselleştirici özelliklerini yok etme işlemine denilmektedir. Bu işlem sonucunda hedef veriler tamamen bağımsız hale gelerek ilgili kişiyle bağını ortadan kaldırılır. Üçüncü bir kişinin bu verilere ulaşması mevcut hali ile kişiler ile bağlantı kuramayacağında sakıncasız hale gelmektedir. Verilerin anonim hale getirmek için hedef veriler bir kısmı veya tamamı uygun yazılımlarla silme, maskeleme, gürültü ekleme gibi yöntemler uygulanmaktadır.

4.4. Fiziki ortamda müdahale: Fiziki ortamda müdahaleler, verilerin depolandığı cihazların fiziki olarak kullanılmaz hale getirilmesi için yapılan tüm işlemleri (kırma, parçalama, eritme vb.) kapsamaktadır.

4.4.1. Fiziksek yok etme: Fiziksek yok etme, depolama cihazların kimyasallar ile eritilmesi, yakılması veya öğütücülerle parçalanmasını içermektedir. Bu işlemler sonucunda veriler tam anlamıyla imha edilmiş olmaktadır. Fiziki olarak yok etme işlemi diğer süreçlere göre daha maliyetli ve zaman alıcıdır. Bu nedenle diğer süreçler ile imhası olmadığı zaman son seçenek olarak kullanılması uygun olacaktır.

Literatüre de en yaygın olarak kullanılan dijital verileri imha süreci kurumlar tarafından dijital ortamlarda tutulan kişisel verilerin silinerek bulunduğu bilişim sistemde geri getiremeyecek şekilde formatlanması üzerinedir (Oğuz,. 2018:124). Bu yöntemin kamu kurumlarda kullanılan kurum bilgisayarlarında uygulanması bazı durumlarda sakıncalar içermektedir. Olası disiplin, idari veya adli soruşturmalarda tek delillin dijital materyallerin olması halinde delilerin incelenememesi ve soruşturmanın selameti doğrudan etkilemektedir.

5. SONUÇ

Dijital verilerin oluşturulması, gizliliği, korunması veya güvenli olarak erişilebilir olması kadar önemli bir diğer husus da güvenli bir şekilde imha edilebilmesidir. Dijital verilerin imha süreçlerinde dikkat edilmesi gereken birçok önemli hususlar bulunmaktadır. Bu hususlar veri depolama şekline göre doğru imha sürecinin seçiminden verilerin geri getirilemez olarak imha edildiğinden emin olunmasına kadar çok çeşitli süreçleri içermektedir.

Veri imhası süreçleri verilerin diğer özellikleri (güvenlik, gizlilik vb.) yanında genellikle ikinci planda kalan ve önemsiz olarak görülmektedir. Bu algı geri dönülmesi zor ve çok önemli güvenlik zafiyetleri oluşturmaktadır. Bu nedenle veri imha süreçlerinin her aşamasında çok dikkatli yapılarak maksimum özen göstermek gereklidir. İmha edilecek verilerin çeşitliliği ve miktarda büyük bir sorundur. İmha edilecek verilerin türlerine ve uygun yöntemlerinin önceden belirlenmesi güvenli veri imhası ve zaman kazandırması açısından önemlidir. Bu amaçla çalışmada uygulanabilir bir dijital verileri imha yöntemi detaylı olarak incelenmiştir.

Dijital verilerin imha süreçlerinde alınabilecek önlemler iki gruba ayrılabilir;

Bunlar;

i) Fiziki tedbirler,

ii) İmha personelinin farkındalıkları,

i) Fiziki tedbirler; güvenli olarak veri imha edilecek materyallerin nerede, hangi koşullarda, nasıl, kim tarafından imha edileceğini kapsamaktadır.

ii) İmha personelinin farkındalıkları; dijital verileri imha edecek personellin teknik ve hukuki boyutuna hâkim olması için gerekli eğitimleri kapsamaktadır.

Türkiye'de dijital verilerin imha süreçleri kurumlara göre farklılıklar göstermekle birlikte birçok sorunlarla karşılaşılmaktadır. Bu alanda yapılan çalışmalarda kişisel verilerin imhasında yoğunlaşmış olup diğer veri türleri için uygulamada detaylı bir çalışma bulunmamaktadır. Bu çalışmada verilen veri imha yöntemleriyle karşılaşabilecek veri tür ve çeşitlerine göre imha süreçleri detaylı olarak tanımlanmıştır. Çalışma bu boyutuyla literatüre sağlayacağı katkının yanı sıra uygulama imha süreçlerinde kullanılmasında yol gösterici olacaktır.

KAYNAKÇA

Baykara, M., Daş, R., & Karadoğan, İ. (2013). Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. In 1st International Symposium on Digital Forensics and Security (ISDFS'13) (pp. 231-239).

Biles, G. E., Bolton, A. A., & DiRe, B. M. (1989). Herman Hollerith: Inventor, manager, entrepreneur-a centennial remembrance. Journal of Management, 15(4), 603-615.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. Politeknik Dergisi, 9(3), 165-174.

Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In 2012 International Conference on Computer Science and Electronics Engineering (Vol. 1, pp. 647-651). IEEE.

Çetin, H. (2014). Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. Akdeniz Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 14(29), 86-105.

Doğan, K., & Arslantekin, S (2016). Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum. Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi, 56(1).

Gantz, J., & Reinsel, D. (2012). The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east. IDC iView: IDC Analyze the future, 2007(2012), 1-16.

Gölcüklü, F. (1994). Avrupa İnsan Hakları Sözleşmesi'nde" Adil Yargılama". Ankara Üniversitesi SBF Dergisi, 49(01).

Göztepe, E. (2011). Türkiye'de Anayasa Mahkemesi'ne bireysel başvuru hakkının (Anayasa Şikâyeti) 6216 sayılı kanun kapsamında değerlendirilmesi. Türkiye Barolar Birliği Dergisi, (95), 13-40.

Henkoğlu, T. (2017). Veri Koruma Kanununun Getirdikleri. Journal of Current Researches on Social Sciences, 7(2), 241-250.

Henkoğlu, T., & Uçak, N. Ö. (2015). Üniversite Kütüphanelerinde Kişisel Verilerin Korunması. Bilgi Dünyası, 16(1).

Hughes, G. F., Coughlin, T., & Commins, D. M. (2009). Disposal of disk and tape data by secure sanitization. IEEE Security & Privacy, 7(4), 29-34.

Jensen, J. R., & Christensen, E. J. (1986). Solid and hazardous waste disposal site selection using digital geographic information system techniques. Science of the total environment, 56, 265-276.

Oğuz, S. (2018). Kişisel verilerin korunması hukukunun genel ilkeleri. Bilgi Ekonomisi ve Yönetimi Dergisi, 13(2), 121-138.

Schroeder, G. N., Steinmetz, C., Pereira, C. E., & Espindola, D. B. (2016). Digital twin data modeling with automationml and a communication methodology for data exchange. IFAC-PapersOnLine, 49(30), 12-17.

Şengül, G., Atsan, F. K., & Bostan, A. (2014). Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri. 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 17-18.

Şişkin, D. Ş. (2018). Bilgi güvenliği ve kişisel verilerin korunması. Türk Kütüphaneciliği, 32(4), 342-345.

Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 23(2).

Winter, R. (2013). SSD vs HDD-data recovery and destruction. Network Security, 2013(3), 12-14.

Yıldız, A. K. (2006). Dijital Belge Yönetimi: Dijital Belgelerin Üretimi, Yönetimi ve Korunması için Rehber. Bilgi Dünyası, 7(1), 157-158.