Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme

Serkan Gönen[1], Halil İbrahim Ulus[1], Ercan Nurcan Yılmaz[2]

[1] Gazi Üniversitesi Fen Bilimleri Enstitüsü
[2] Gazi Üniversitesi Teknoloji Fakültesi Elektrik Elektronik Mühendisliği
halilulus@gmail.com, serkangonen@gmail.com, enyilmaz@gazi.edu.tr
(Geliş/Received: 23.01.2016; Kabul/Accepted: 29.09.2016)
DOI: 10.17671/btd.90710

Özet- Bilişim sektöründeki gelişmeler bilgiye ulaşmayı kolaylaştırmış ve insanlara önemli faydalar sağlamıştır. Ancak bilişim alanında değişen ve gelişen teknolojik imkânlar yeni suç türlerini ortaya çıkartmış ve bilginin korunmasını güçleştirmiştir. Her alanda olduğu gibi bilişim sektörü alanında da suçlar konusunda var olan kanuni düzenlemeler, hızla yöntem değiştiren bilişim suçları ile mücadelede yetersiz kalmıştır. Özellikle kişisel verilerin korunması konusunda bilinç ve farkındalık eksikliği, yetersiz ve caydırıcı olmayan mevzuatla birleşince suçların engellenmesi zorlaşmaktadır. Buna rağmen ülkemizde bu tür suçlarla mücadele için aynı hızda ihtiyaç duyulan gerekli kanunlar oluşturulup yürürlüğe konulamamıştır. Bu çalışmada bilişim suçları ile mücadele ve kişisel verilerin korunması için mevcut kanunlar üzerinde eleştirel bakış açısıyla durulmuş; yeterlilikleri sorgulanarak hukuksal açıdan çözüm önerileri geliştirilmiştir.

Anahtar Kelimeler -- Bilişim Suçları, Kişisel Veri, Hukuksal Boyut

An Examination upon the Crimes Committed on Informatics

Abstract – The developments in the informatics sector has made reaching the information easier and provided important benefits for humans. However, changing and developing technological opportunities within informatics has led new crime types and made the protection of information harder. As in all fields, current legal regulations about the crimes in informatics are insufficient to struggle against cyber-crimes which change their methods quickly. The prevention of these crimes becomes harder especially when the lack of consciousness and awareness about the protection of personal data merge with the regulations which are not sufficient and deterrent. Despite this, necessary laws which are required to struggle with such kind of crimes at the same rapidness have not been legislated and put into action in our country. In this study, a critical perspective about the current regulations is discussed in terms of the struggle with crimes committed on informatics and the protection of personal data and solution recommendations in terms of legal perspective are developed through questioning their sufficiency.

Keywords-- Informatic Crime, Personal Data, The Legal Dimension

1. GİRİŞ (INTRODUCTION)

Dünyadaki sayısallaşma ve her şeyin İnternet tabanlı (everything over IP) hale gelmesine paralel olarak, ülkemizde de bu değişim hızlı bir şekilde yaşanmaktadır. Söz konusu sayısallaşma ve İnternet, sadece haberleşme yöntemlerimizi değiştirmekle kalmamış, yeni bir çalışma ve yaşam biçimi oluşturmuştur. Bilgi ve iletişim sistemlerinin yaygınlaşması; işlemlerin daha hızlı, kaliteli ve verimli işleyiş ile beraber vatandaşların yaşam standardını da artırmıştır. Ancak bilgi teknolojileri altyapısının bu kadar yaygınlaşması ve hatta bu yapıya bağımlı hale gelinmesi, söz konusu sistemlerin güvenliğinin sağlanamadığı hallerde kişi, kurum, kuruluş ve ülkeleri önemli risklerle karşı karşıya bırakabilmektedir. Çünkü yazılım alanındaki karmaşa ve saldırganların saldırı aracı olarak engin kaynaklara ulaşabilmesi de, sistem hatalarının ve açıklıklarının istismar edilmesini kolaylaştırmaktadır. Özellikle kanunlardaki boşluklar ve belirsizlikler, caydırıcı olmayan cezalar, bilişim suçlarının kolay ve ucuz işlenebilmesi ile suçluların tespit edilmesinin zorluğu suçluları bu alana doğru sevk etmektedir. Bu nedenle çalışmada, bilişim alanında işlenen suçlar ile kişisel bilgilerin korunmasına yönelik kanun ve düzenlemeler incelenecektir.

Çalışmanın müteakip bölümlerinde sırasıyla Türk Ceza Kanunu'nun 243 ve 244'üncü maddelerinde düzenlenen bilişim suçlarına ilişkin kanun maddeleri ele alınacak, üçüncü bölümde ise kişisel bilgilerin korunmasına yönelik kanun (taslak) maddesi ile diğer ilgili düzenlemelere yer verilecektir.

2. BİLİŞİM ALANINDA İŞLENEN SUÇLAR (CRIMES IN THE INFORMATION TECHNOLOGY AREA)

Bilişim terimi, "bilmek" eyleminden ad olarak türetilmiştir [1]. Diğer bir tanımda; bilişim insanların teknik, ekonomik, sosyal, kültürel, hukuksal veya benzeri alanlarda sahip oldukları verinin saklanması, saklanan bu verinin elektronik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve yüksek hızlı veri, ses veya görüntü taşıyan iletişim araçları ile aktarılması olarak ifade edilmiştir [2]. Bilişim suçu ise; bilgileri otomatik olarak işleme kabiliyetine sahip bir sisteme (bilgisayar, tablet, cep telefonu, vb.) kanun ve ahlak dışı yani izinsiz olarak girilmesidir [3,4]**.**

Bilişim alanında işlenen suçlar; bilişim sistemlerine karşı işlenen suçlar "Hedef Bilişim Sistemi" ve bilişim sistemleri ile işlenen suçlar "*Araç Bilişim Sistemi*" olarak iki gruba ayrılabilir. İlk durumda, bilişim sistemlerinde bulunan bilgilerin karakteristiği yani; gizliliği, bütünlüğü ya da erişilebilirliği hedef olmaktadır. Bilişim sistemi tarafından sağlanan hizmetler, depolanan, alınan ve gönderilen veriler ya da donanım olarak ifade edilen kurban bilgisayarlar zarar görmektedir. Servis Dışı bırakma (Denial of Service- DoS) saldırıları bu gruba örnek verilebilir. İkinci durumda yer alan suçlar ise; siber terörizm, çocuk pornografisi, nitelikli dolandırıcılık, fikri mülkiyet hakları ihlalleri ve yasadışı maddelerin çevrimiçi satışı gibi suçlardır. Bilişim suçlarının grupları değerlendirildiğinde; "Bilişim Alanında İşlenen Suçlar" kapsamına giren suçlar birinci gruptaki suçlardır.

Bilişim suçları; TCK 5273'ün 10. Maddesinde yer alan "Bilişim Alanında İşlenen Suçlar" başlığının 243, 244 ve 245'inci maddelerinde ele alınmaktadır.

2.1. Madde 243: Bilişim Sistemine Girme (Article 243: Accessing a Data Processing System)

Bilişim alanında suçlar kapsamında TCK'da ilk olarak, 243'üncü madde olan "bilişim sistemine girme" suçu düzenlenmiştir. Bu madde Avrupa Birliği'ne uyum süreci kapsamında değerlendirilebilir; çünkü Avrupa Konseyi Siber Suç Sözleşmesinin ikinci maddesindeki "yasadışı erişim" düzenlemesiyle paralellik taşımaktadır [5]. Kanun maddesi üç fıkradan oluşmaktadır.

TCK 243/1; "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir."

Maddenin ilk fıkrası değerlendirildiğinde; öncelikle sisteme "girme" yerine "erişim" ifadesinin kullanılması daha uygun olacaktır. Çünkü suçun konusu eylem sanal bir ortamda gerçekleştirilmektedir.

İkinci olarak, kanun maddesine göre hukuka aykırı olarak bir bilişim sistemine girilmiş olması, bu suçun oluşması için yeterli değildir. Sisteme girdikten sonra belirli bir süre sistemde kalması şart koşulmuştur. Aksi takdirde, bilişim sistemine hukuka aykırı olarak giren kişi, hedef sistemde belirli bir süre kalamazsa sadece teşebbüs söz konusu olacaktır. Bilişim sistemine girme suçuna ilişkin kanun tasarısı ilk kez 1997 yılında Bakanlar Kurulu tarafından TBMM'ye sunulduğunda, tasarı "bilişim sistemine hukuka aykırı olarak girilmesi veya orada kalınması" şeklindeyken; TBMM Adalet Alt Komisyonu'nda verilen önergede "bilişim sistemine hukuka aykırı olarak girilmesi ve orada kalınması" haline getirilmiştir. Diğer bir ifadeyle suç seçimlik hareketliyken, bağlı hareketli hale gelmiştir [6]. Ancak kanun maddesinde sadece izinsiz girişin suçun oluşumu için yeterli sayılması gerekmektedir. Bunun en büyük sebebi ise korunan hukuki değer olan kişilerin özel hayatına ihlal sadece sisteme giriş ile gerçekleşebilmektedir. Aksi durumda, bilişim suçluları, yüksek maliyet getiren değişiklik ve tahribata yol açan durumlara teşvik edilebilecektir. Çünkü izinsiz erişimler, gizli verilerin ve sırların elde edilmesine ve/veya sistemin ücretsiz kullanılmasına yol açabilmektedir.

Üçüncü olarak da, söz konusu kanun fıkrasında sistemde kalma süresi için bir açıklık getirilmemiştir. Bu nedenle sürenin yeterliliği konusunda son karar bağımsız mahkemelere, daha doğrusu savcı ve hâkimlerin bakış açısına bağlıdır. Diğer bir ifadeyle, bu noktadaki önemli husus hukuk alanında çalışanların bilişim alanındaki bilgileri ve yeterlilikleridir. Çünkü bu madde için, bilişim alanında uzman birisi için milisaniyeler yeterli olabilecekken, acemi veya bilgisi yetersiz diğer saldırgan için sistemde günlerce kalması istediği amaca ulaşması için yeterli olmayabilecektir. Bu nedenle, faillerin bu kapsamda bilgileri bakımından değerlendirilebilmesi son derece önem kazanmaktadır.

TCK Madde 243/2'de ise; "243/1'deki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir." hükmü yer almaktadır.

Bu fıkra; özel kişilere ait bir bilişim sistemine girmek ve orada kalmak halinde ihlal edilen hukuki yararın, bedeli karşılığında yararlanılan sistemlere girmek ve orada kalmak suretiyle ihlal edilen hukuki yarardan daha fazla korunmaya değer olduğu düşüncesine dayanmaktadır. İnternet üzerinden abonelik veya üyelik yöntemiyle ücreti karşılığı film, oyun, müzik, gazete ve yazılım gibi hizmetleri sunan sistemlere izinsiz şekilde girilmesi ve belirli bir süre kalınması bu fıkraya örnek olarak verilebilir. Ancak, burada göz ardı edilen husus ise, bu kapsamda yer alan ticari kurum ve kuruluşların hak ve özgürlüklerinin korunmasının da kanunen güvence altına alınmasıdır. Bu fıkra ile güvenceye aykırılık oluşmaktadır ve failleri söz konusu sistemlere karşı suç işlemeye teşvik etmektedir. Bu konuda, indirimin kaldırılmasının yanı sıra, TCK'nın 137'nci maddesinde olduğu gibi "Nitelikli Haller" düzenlenerek, kamu kurumları ve bankalar gibi

özellik arz eden sistemlere yetkisiz erişimin dikkate alınması gerekmektedir.

Son fıkra TCK Madde 243/3'e göre ise; " *Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.*" maddesi yer almaktadır.

Hükmün üçüncü fıkrasında daha ağır cezayı gerektiren nitelikli haller düzenlenmiştir. Bilişim sistemine yetkisiz erişim kastıyla girilmesi sonucunda sistemde bulunan verilerin değiştirilmesi, tahribi veya yok edilmesi halinde, cezanın ağırlaştırılmasını gerektirmektedir. Bu fıkrada dikkat edilmesi gereken temel nokta failin kastıdır. Çünkü fail doğrudan sistemde bulunan verileri değiştirmek, tahrip etmek veya yok etmek amacıyla sisteme erişim sağladıysa, failin kastı 243'üncü maddenin üçüncü fıkrasını değil doğrudan TCK'nın 244'üncü maddesinde yer alan "sistemi engelleme, bozma, verileri yok etme veya değiştirme" suçunu oluşturacaktır.

Kanun maddesinde değerlendirilmesi gereken bir diğer husus ise suçun manevi unsurudur. Bilişim Sistemine Girme suçunun manevi unsurunun oluşması için, failin bilerek ve isteyerek suç işleme kastı gereklidir. Bunun içinde, failin suç oluşturan eylemle ilgili yasal tanımlamaları bilmiş olması gereklidir [7]. Dolayısıyla bu konuda faili suçlayabilmek için, failin yaptığı eylemin suç olduğunu bildiğine dair kanıt gerekmektedir. Bu ise suçun mağdurları açısından oldukça adaletsiz bir tutumdur. Bu şart sadece korunan sistemler için aranmamaktadır. Örneğin kullanıcı adı ve parola girilmesi mecburi olan bir sisteme yetkisiz girilmesi durumunda suçun manevi unsuru kendiliğinden oluşmuş sayılmaktadır. Bu durum da; kanunlar tarafından korunmak için sistemlerin güvenlik önlemlerinin alınması gerektiğini göstermektedir. İstisna olarak da, sisteme giriş yetkisi olan bir kullanıcı faile giriş için yetki vermiş veya kendi kullanıcı adı ve parolasını söylediyse bu eylem artık hukuka aykırı olarak kabul edilmemektedir [8].

2.2. Madde 244: Bilişim Sistemini Bozma, Engelleme ve Verilerin Değiştirilmesi veya Yok Edilmesi
(Article 244: Preventing the Functioning of a System and Deletion, Alteration or Corrupting of Data)

TCK 244'üncü madde aşağıda belirtilen fıkralardan oluşmaktadır.
(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.
(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.
(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.
(4) İlk üç fıkrada tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

Madde 244 incelendiğinde; Madde 243'ün devamı niteliğinde olduğu görülmektedir. Bilişim sistemine giren ve kalmaya devam eden failin sistemi engellemeye ve bozmaya, bilişim sistemi içerisinde bulunan verileri yok etmeye veya başka verilerle değiştirmeye yönelik işlemler bu madde kapsamında değerlendirilmektedir.

Söz konusu kanundan önce doğrudan bilgisayar sistemlerinin işleyişi ile sistemde bulunan verilerin değiştirilmesine, tahribine veya yok edilmesine yönelik eylemler, suç olarak kabul görmediğinden cezalandırılmalarına imkân yoktu [9]. Bu nedenle 244'üncü maddenin bu alanda önemli bir adım olduğu görülmektedir.

Kanun maddesinin fıkraları ele alındığında; ilk fıkrada, sistemin işleyişini bozma veya engelleme ile sistem üzerinde işlenen verilere zarar verme veya değiştirme suçu ayrı ayrı değerlendirilmiş ve yukarıda belirtilen cezalar belirlenmiştir. Bu maddeler, siber suçlarla mücadele kapsamında oldukça önemlidir. Çünkü siber saldırılar sonucunda faillere uygulanacak yaptırımlar bu maddeler ile tespit edilmektedir.

Üçüncü fıkra ise, 243'üncü maddede de bulunması gereken önemli bir tespittir. 243'üncü maddenin ikinci fıkrasının değerlendirilmesi kısmında da belirtildiği üzere, kanun maddelerinde belirtilen yaptırımlar caydırıcılık taşımalıdır. Özellikle toplumun huzur ve güvenliği için ortak korunan değerlerde, söz konusu yaptırım oranının daha fazla olması gerekmektedir. Üçüncü fıkra, bu kapsamda gerçekleştirilmiş bir yaptırımdır. Ancak bu konuda ki temel problem, yarı oranda artırılacak cezanın da yeterince caydırıcılık özelliğini taşımamasıdır. Çünkü bir banka soygunu neticesinde çalınan "A" miktar para ile İnternet ortamında kullanıcıların hesaplarına erişerek ele geçirilen "A" miktar paranın cezai müeyyidesinin oldukça farklı olması adalet kavramı ile çelişmektedir. Bu fark da suçluları sanal ortama yöneltmektedir.

Son fıkra da ise, birinci ve ikinci fıkrada ifade edilen hususlar neticesinde, failin kendisi ya da başka birisine çıkar sağlaması müeyyideye bağlanmıştır. Bu fıkraya örnek olarak, bir öğrencinin bilgi sisteme erişerek notunu değiştirmesi ya da ticari bir firmanın rakibi olan firmanın işleyişini engellemesi verilebilir.

Bilişim alanında işlenen suçlar başlığının son maddesi olan 245'inci madde olan "banka ve kredi kartlarının kötüye kullanılması" ise 243 ve 244'üncü maddeden farklılık göstermektedir. Çünkü 243 ve 244'üncü maddeler doğrudan bilişim sistemine yönelik saldırıları içerirken, 245'inci madde kapsamında düzenlenen fiiller ise gerçek veya sahte kartlarla yarar sağlamayı cezalandırmaktadır. Bu nedenle çalışma da 245'inci madde incelenmemiştir.

3. KİŞİSEL VERİLERİN KORUNMASI (PROTECTION OF PERSONAL DATA)

Bilişim alanındaki hukuksal düzenlemelerin ilgilendiği temel sorun alanlarından bir diğeri; kişisel verilerin korunmasıdır. Teknolojinin ilerlemesi ve mahremiyet artırıcı teknolojilerin (akıllı telefonlar, bulut bilişim, sosyal paylaşım ağları, çevrimiçi davranışlara dayanan reklamcılık ve yer bilgisi vb.) ortaya çıkması ile kişisel mahrem ve gizli bilgilerin korunması zorlaşmıştır. Bunun örnekleri; yakın geçmişte yaşanan bir bankanın 2.7 milyon müşterisinin kredi kartı bilgilerinin çalınması (13.11.2014), "Ankara'da vatandaşlara ait tapu bilgilerinin çalınması (27.11.2014)", "Apple Icloud uygulamasını kullanan ünlülerin fotoğraflarının medyaya sızması (09.09.2014)" olayları ile görülmektedir. Siber ortamın özellikle ulusal sınırları aşarak uluslararası platformlarla birbirine bağlanması kişisel bilgilerin korunması ve takibi için kullanılan yöntemlerin uluslararası işbirliği olmadan etkinliğinin yetersiz kalmasına sebep olmaktadır. Uluslararası şirketlerin gücü ve kabiliyetleri bazen devletleri bu konuda önlem almada sınırlandırmaktadır. Bu yüzden uluslararası işbirliği ve entegrasyon bu konuda zaruridir.

Kişisel verilerin korunması yönünde uluslararası alanda ilk belge olark kabul edilen 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşmeyi Avrupa Konseyi 28.01.1981 tarihinde imzaya açmış, Türkiye bu belgeyi imzaya açıldığı gün imzalayan ilk ülkelerden birisi olmuştur. Fakat Türkiye imzalamasına rağmen onay sürecini işletmemiş; ayrıca günümüzde San Marino ise bu sözleşmeyi imzalamayan tek ülke konumundadır [10].

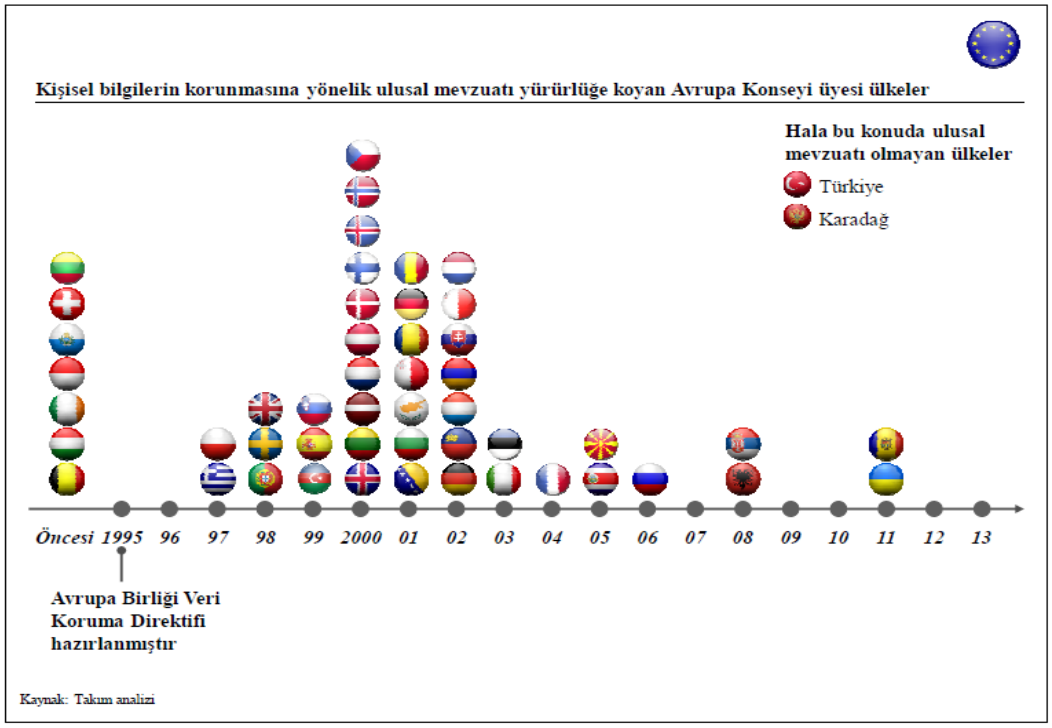
Tablo 1. AB Mevzuatında 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Avrupa Konseyi Sözleşmesi [11]
(No. 108 in EU Legislation Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hük.	İlgili Kanun	Veri Koruma Otoritesi
	İmza Tarihi	Onay tarihi			
Arnavutluk	2004	2004	Var	Var	Veri Koruma Komiseri
Avusturya	1981	1988	Var	Var	Veri Koruma Komisyonu
Belçika	1982	1993	Var	Var	Mah.Koruma Komisyonu
Bosna Hersek	2004		Var	Var	Veri Koruma Komisyonu
Bulgaristan	1998	2002	Var	Var	Kişisel Ver.Korm. Komisyonu
Hırvatistan	2003	2005	Var	Var	Kişisel Ver.Korm. Ajansı
G.Kıbrıs Rum Yönt.	1986	2002	Var	Var	Kişisel Ver.Korm. Komiseri
Almanya	1981	1985	Var	Var	Fed.Ver.Korm. Komiseri
İngiltere	1997	1997		Var	Evet
Yunanistan	1983	1995		Var	Kişisel Ver.Korm. Kurumu
İtalya	1983	1997		Var	Kişisel Ver.Korm. Kurumu
Rusya	2001		var		Kişisel Ver.Korm. Kurumu
Azerbeycan			Var	Var	
Ermenistan			Var		
Karadağ	2005	2005			
Türkiye	**1981**		**Var**		
ABD				Var	
Japonya				Var	Evet
Meksika			Var	Var	Evet
İsrail			Var	Var	

Ayrıca bazı kanun ve yönetmeliklerde parça parça hükümler bulunmasına rağmen daha ayrıntılı ve sadece kişisel verilerin korunmasını düzenleyen bir kanun bulunmamaktadır. Uluslararası alanda bu konuda kanunu bulunmayan çok az ülke bulunmaktadır. Bu yüzden kişisel hak, hürriyet ve özel hayatın korunduğu, ilgili kurum ve kuruluşların açık ve net bir şekilde görev ve sorumlulukların belirlendiği, bu alanla ilgili tüm hususları kapsayıcı ana bir kanunun çıkarılması elzemdir.

Kişisel veri; bilinen veya kimliği tespit edilebilir gerçek ve tüzel kişilere ilişkin tüm bilgilerdir [12]. Veri, her türlü bilgiyi kapsarken; kişisel veriler sadece bireylerin kimliklerine doğrudan veya dolaylı olarak ulaşılmasına olanak veren bilgilerdir [13]. Kişisel verilerin ihlali ise, kişinin özgür iradesiyle verdiği kabul beyanı dışında, yetkisi olmadığı halde ya da hukuka aykırı olarak kişisel verilerin zarara uğramasına, kaybolmasına, iletilmesine, değiştirilmesine, herhangi bir yere depolanmasına, kaydedilmesine, işlenmesine, açığa çıkarılmasına ve ilgili verilere erişilmesine neden olan durumlara güvenlik ihlali denir. Bu ihlallere karşı ülkemizde kişisel verilerin korunması ve suçluların cezalandırılması için pek çok kanunda çeşitli hükümler bulunmaktadır [14]. Özellikle Anayasanın 20. Maddesinde, "Herkes özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz."

hükmü ile kişilerin mahrem hayatları güvence altına alınmıştır. Fakat yine de kişisel verilerin korunması yönünde tüm kanunları kapsayan ayrı bir kanun yapılması gerektiği diğer Avrupa ülkeleriyle kıyaslandığında ortaya çıkmaktadır. Şekil 1'de görüldüğü üzere Avrupa Konseyi ülkeleri arasında Türkiye ulusal mevzuatı olmayan iki ülkeden biridir.



Şekil 1. Avrupa Konseyine Üye Ülkelerinin Ulusal Mevzuatlarını Yürürlüğe Koydukları Tarihler [15]
The National Legislature of The Country of Council of Europe Dates of Puts Into Effect

Ulusal mevzuat detaylı olarak incelendiğinde; kişisel verilerin korunması yönünde çeşitli hükümler bulunan kanunlar şunlardır:

- T.C. Anayasası- Md. 20-25
- Türk Ceza Kanunu (TCK)- Md. 132 -140
- Ceza Muhakemesi Kanunu (CMK)- Md. 75, 80, 134-138, 140
- Elektronik Haberleşme Kanunu Md. 51, 52
- Elektronik İmza Kanunu Md. 12
- Bankacılık Kanunu
- Banka Kartları Ve Kredi Kartları Kanunu Md.23
- Türk Medeni Kanunu Md. 23-25
- Bilgi Edinme Kanunu Md. 19-22
- Fikir ve Sanat Eserleri Kanunu 19, 83-86
- İş Kanunu Md. 75
- İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- Adli Sicil Kanunu Md. 11
- Türk Medeni Kanunu Md. 23, 24, 25
- Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği
- Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik.

Özellikle Türk Ceza Kanununda haberleşmenin ihlallerinde (TCK 132), kişiler arasında geçen konuşmaların dinlenmesi ve kayda alınmasındaki suçlarda (TCK 133), kişisel verilerin kanuna aykırı olarak kaydedilmesinde (TCK 135) kişilerin cezalandırılacağı belirtilmiştir. Ayrıca bu suçların nitelikli halleri (kamu görevlisi tarafından işlenmesi TCK 137) ve tüzel kişiler hakkında yaptırım uygulanması esasları (TCK 140) Türk Ceza Kanununda sıralanmıştır.

Bunun yanında suçların önlenmesi, soruşturulması veya kovuşturulmasında kanuna uygun olarak kişisel veriler tespit edilebilir, dinlenebilir, işlenebilir veya kayıt altına alınabilir. Bu durumların çerçevesi Ceza Muhakemesi Kanunu 134-140 arasında sıralanmıştır.

CMK'da yer alan suçların aydınlatılmasına yönelik uygulanan tedbirlerden "İletişimin tespiti, dinlenmesi ve kayda alınması" ve "teknik araçlarla izleme" olgularının tamamı Bıçak (2013) tarafından "Elektronik Takip" olarak nitelendirilmektedir. Ayrıca aynı kaynakta, yurtdışı görüşmeler dahil Türk Telekom tarafından yürütülen sabit telefon veya Turkcell, Vodafone, Avea gibi mobil hat şirketleri tarafından işletilen ve görüşmelere ait tüm detay bilgilerinin, kullanıcı ve kullanılan cihaz bilgilerinin, GPRS bağlantıları ile GPRS üzerinden İnternet bağlantılarının, SMS gönderim ve alım kayıtlarının,

İnternet üzerinden gönderilen ve alınan veri bilgilerinin (isim, hattın hangi bayiden alındığı ve zamanı) alınması ile anılan bilgilere ilişkin detay kayıtlarına ait verilerin canlı olarak alınması, elektronik takip kapsamında değerlendirilmiştir [16]. CMK'da belirtilen söz konusu maddeler kişisel veriler ve mahremiyetle doğrudan ilgili olduklarından bu bölümde maddelere kısaca değinmekte fayda bulunmaktadır.

- *İletişimin tespiti;* iletişimin içeriğine müdahale edilmesizin, kişinin kullandığı iletişim aracının diğer iletişim araçlarıyla kurduğu iletişimin türü, başlama ve bitiş zamanı, iletişim araçlarının kapsam alanında bulunduğu yer bilgisi ve iletişim araçları sahiplerinin kimlik bilgilerinin ortaya çıkarılması için yapılan işlemlerdir. Bu tedbir, şüpheli ve sanığa ait telefonlar hakkında uygulanır. Tüm suçların soruşturmasında ve kovuşturmasında başvurulabilir. Uygulanmasına hakim karar vermesine rağmen gecikmesinde sakınca bulunan hallerde savcı tarafından karar verilir. Ancak en kısa sürede hakim onayına sunulur ve hakim kararını en geç 24 saat içinde açıklar. Bu konuda ileriye dönük kimin kiminle, hangi baz istasyonundan, hangi tarihte ve ne kadar süre görüştüğüne karar alınabilecekken geçmişe dönük herhangi bir sınırlayıcı hüküm bulunmamaktadır. Buna yönelik düzenleme olmaması kişisel verilerin ihlaline yönelik önemli bir eksikliktir (CMK 135).

- *İletişimin dinlenmesi ve kayda alınması;* sabit veya mobil telefon ile ya da İnternet üzerinden yapılan görüşmelerin yetkili olarak belirlenen üçüncü kişiler tarafından canlı olarak dinlenilmesidir. İspat zorluğu nedeniyle kayda alınmayla birlikte ele alınmalıdır. Uygulanmasına hakim karar vermesine rağmen gecikmesinde sakınca bulunan hallerde savcı tarafından karar verilir. Ancak en kısa sürede hakim onayına sunulur ve hakim kararını en geç 24 saat içinde açıklar. Bu tedbire sadece kanunda belirtilen suçlarda başvurulabilir. Tedbirin uygulanmasında kişinin iletişim aracının kendi adına kayıtlı olması şart değildir. Bu konuda en sık yaşanan problemler; rastlantı sonucu bulunan başka suçlara yapılacak işlemler ve kayıtların imhasına yöneliktir. Rastlantı sonucu bulunan suçlarla ilgili kamu görevlisi durumu derhal savcıya bildirmelidir. Çünkü bu kayıtlar rastlantı sonucu bulunan suçla ilgili yasadışı delil niteliğindedir ve suçun soruşturma ve kovuşturma aşamasında kullanılamaz (CMK 138). Diğer bir konu; "dinleme ve kayıt işlemine son verilmesi halinde kayıtlar 10 gün içinde yok edilmeli ve Başsavcılık 15 gün içinde ilgilisine bilgi vermelidir" yükümlülüğü bulunmaktadır (CMK 137/3-4). Ayrıca suçla ilgisi olmayan kişilerin özel hayatına ilişkin bilgilerin soruşturma dosyasına konulmaması gereklidir. Ancak yukarıda belirtilen hususların uygulama ve denetimi ile ilgili ülkemizde ciddi eksiklikler bulunmaktadır.

- *Sinyal bilgilerinin değerlendirilmesi;* kişilerin yer tespitine ilişkin bilgilerdir [16]. Sadece kanunda belirtilen suçlarda uygulanabilir. Uygulanmasına hakim karar vermesine rağmen gecikmesinde sakınca bulunan hallerde savcı tarafından karar verilir. Ancak en kısa sürede hakim onayına sunulması gerekir ve hakim kararını en geç 24 saat içinde açıklar (CMK 135/3).

- *Teknik araçlarla izleme;* iletişim araçlarından faydalanmadan kişinin bulunduğu ortamdaki seslerin uzaktan dinlenmesi veya ortamın görüntülenmesi veya kişinin bulunduğu yerin algılayıcılarla tespiti gibi işlemlerden oluşur. Sadece Türk Ceza Kanununda yer alan belli suçlarda uygulanır. Tedbirin uygulanmasına ağır ceza mahkemesi tarafından oy birliğiyle karar verilir. Bu tedbire kişinin konutunda başvurulamaz (CMK 140).

- *Elektronik veri takibi;* bilgisayar veya bilgisayar sistemlerinde mevcut kayıt ve verilerin incelenmesi yoluyla yapılır [18]. Cumhuriyet savcısının isteği üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarının kopyalanmasına, bu kayıtların incelenerek metin hâline getirilmesine hâkim tarafından karar verilir. Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine, sistemlerde bulunan şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere erişilememesi halinde çözümün yapılabilmesi ve ihtiyaç duyulan kopyaların alınabilmesi için, bu cihazlara el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın derhal iade edilir. Bu tedbirin uygulanmasında hakim kararı zorunludur. Gecikmesinde sakınca bulunan hallerde dahi savcı ve kolluk karar veremez. Ayrıca sadece şüphelinin kullandığı cihazlarla sınırlı olmalıdır, aynı evde bulunsa bile diğer kişilerin cihazlarında uygulanmaması gerekir. Belirtilen tedbirlerin uygulanma süreleriyle ilgili Ceza Muhakemesi Kanununda 21.02.2014 tarihinde yapılan değişikle bazı düzenlemeler yapılmıştır.

Sonuç olarak; kişisel verilerin korunması konusuyla ilişkili tüm kanunların tek bir kanun altında toplanması gereklidir. Ayrıca uluslararası alanda siber ortam açısından güvenli ülke olunabilmesi için oluşturulan mevzuatla, gerekli olan uluslararası hukuk koordine edilerek gerekli düzeltmeler yapılmalıdır. Özellikle Avrupa Birliği 95/46/AT sayılı Veri Koruma Direktifinde belirtildiği üzere her yönden tam bağımsız denetleyici bir kuruluşun kurulması belirtilen ihlallerin denetlenmesi için zorunludur. Bu sayede, bilgi güvenliği hukuku alanında kişisel verilerin güvenliği kapsamında karşılan sorunlar bu kanun ile giderilebilecektir.

Tablo 2. Son Değişikliklerle Bilişim Alanında Başvurulacak Hukuksal Tedbirlerin Kıyas Tablosu [17]
(Comparative Table of the Recent Changes About Legal Precautions in Forensic)

Tedbir	**Kanun maddesi**	**Normal Suçlar**	**Örgütlü Suçlar (Uzatma)**	**Şüphe Türü**
İletişimin tespiti	CMK 135	2 + 1 ay	1+1+1= 3 ayı geçemez	Somut delillere dayalı Kuvvetli suç Şüphesi
İletişimin dinlenmesi ve kayda alınması	CMK 135	2 + 1 ay	+1+1+1= 3 ayı geçemez	Somut delillere dayalı kuvvetli suç Şüphesi
Sinyal bilgilerinin değerlendirilmesi	CMK 135	2 + 1 ay	+1+1+1= 3 ayı geçemez	Somut delillere dayalı Kuvvetli suç Şüphesi
Teknik araçlarla izleme	CMK 140	3 + 1 Hft	+1+1+1+1= 4 haftayı geçemez	Kuvvetli Şüphe
Elektronik veri takibi	CMK 134	-	-	Kuvvetli Şüphe

Fakat tüm yasal düzenlemelerden daha önemli diğer bir konu ise bireysel farkındalık ve eğitimin tesis edilmesidir. Bilgi güvenliğine yönelik farkındalık ve bilinçlendirme eğitimleri ilkokuldan başlayarak okul müfredatlarına eklenmeli, çeşitli seminerler düzenlenmeli ve bu sayede kullanıcılarda kişisel bilgilerin paylaşımı ve korunması yönünde bilinç oluşturulması gereklidir. Bu konuyla ilgili bir şirketin 18774 çalışan üzerinde yaptığı çalışmada katılımcıların verdiği cevaplar, ülkemizin kişisel verileri paylaşma konusunda yeterli bilinç düzeyine sahip olmadığını ortaya çıkarmıştır. Katılımcılarının çoğunun sosyal paylaşım sitelerinde kişisel verilerini paylaştığı Tablo 3'de görülmektedir [18].

Tablo 3. "Sosyal medyada profiliniz kariyerinizin hangi bilgilerini içermektedir?" Sorusuna Verilen Cevap [18]
"Your social media profiles career-related, contains what information?" Answer Questions Given

	1 (Hiç)	2	3 (nötr)	4	5 (çok)	Toplam
Kişisel Bilgiler (Ör.İlişki durumu, cinsiyet…)	6.0	2.6	4.7	15.5	71.2	100
Profilde Oluşan Kişilik	3.9	2.6	7.7	18.9	67.0	100
Fotoğraflar	5.6	3.4	14.6	24.0	52.4	100
İş Deneyimi	4.3	0.9	7.3	17.6	70.0	100
Kontak sayısı	6.4	6.0	18.9	18.9	49.8	100
Hobiler ve ilgi alanları	5.6	6.0	18.0	23.2	47.2	100
Profesyonel ödül ve dereceler	6.0	4.7	18.0	17.6	53.6	100
Başkalarının referans ve yorumları	6.0	5.2	13.7	21.9	53.2	100
Paylaşılan içerikler	7.3	3.9	19.3	23.2	46.4	100

Söz konusu araştırma göstermektedir ki; kullanıcılar bu durumun kişisel ve kurumsal açıdan bilgi güvenliği zafiyeti yaratabileceğinin, burada paylaştıkları bilgilerin istenmeyen amaçlarla kullanılabileceğinin farkında değillerdir. Ülkemizde sosyal medya aracılığıyla paylaşılan bilgilerin korunması, bu vasıtayla oluşan suçların aydınlatılması ve suçluların yakalanıp cezalandırılması için gerekli teknik ve hukuksal altyapı da yeterli değildir. Farkındalık eksikliği ile mevzuatın suçluları cezalandırmada yetersiz kalmasıyla birleştiğinde bilişim suçlarının engellenmesi oldukça zorlaşmaktadır.

4. SONUÇ VE ÖNERİLER (CONCLUSIONS AND RECOMMENDATIONS)

Günümüzün sürekli gelişen teknolojisi ile paralel olarak modernleşen iletişim kavramı sayesinde kişilere, şirketlere, bankalara, hastanelere ait önemli bilgiler bilgisayar ortamında tutulabilmektedir. Sayısal ortamdaki bu verilere sadece uygun yollardan erişmenin yanında aynı zamanda hukuka aykırı yoldan ulaşabilmek için de yine bilişim teknolojisi kullanılmaktadır. Bilişim sistemleri vasıtasıyla işlenen bu suçların diğer suçlara göre daha kolay ve ucuz işlenebilmesi faillerin ilgisini çekmektedir. Ayrıca siber saldırganların daha az bilgi ile daha kapsamlı alanlarda etki oluşturabilmeleri ve özellikle internet ortamı aracılığıyla saldırılar konusunda engin kaynaklara sahip olabilmeleri de saldırganları bu alana sevk etmektedir. Bunların daha da ötesinde, gerçek hayatta suç işlemekten çekinen insanlar, bilişim suçlarının kaynağının tespitinin zor hatta imkânsız olabilmesi, anonimlik, inkâr edebilirlik gibi özelliklerinden dolayı bilişim teknolojileri söz konusu olduğunda çok rahat suç işleyebilmektedirler. Bu nedenlerle, siber ortamda oluşabilecek tehlikelere karşı elektronik cihaz kullanan herkesin bilinçli olması sağlanmalıdır. Bu da kişilerin konuyla ilgili eğitim almasıyla; yani farkındalık oluşturulması ile mümkündür.

"Yasadışı erişim" terimi, bilişim sistemlerine ve bu sistemler üzerinde depolanan, işlenen veya transfer edilen verilerin güvenlik karakteristiklerine (gizlilik, bütünlük, erişebilirlik) yönelik tehdit ve saldırı biçimindeki temel suçları kapsamaktadır. Bilişim suçunun işlenmemesi için de caydırıcı önlemlerin başında ceza hukuku alanında gerekli yasal düzenlemelerin yapılması ve cezai yaptırımların etkin bir şekilde uygulanabilmesi gerekmektedir. Bu kapsamda, fiili olarak işlenen suçların cezaları ile kıyaslandığında oldukça düşük kalan bilişim suçlarının cezalarının incelenerek, bu suçların ilk basamağı olan bilişim sistemine yetkisiz girişten itibaren cezaların tekrar değerlendirilmesi ve etkili hale getirilmesi gerekmektedir. Çünkü siber suçlara ilişkin mevcut kanunlar değerlendirildiğinde; bilişim alanında işlenen suçların ilk basamağı olan, bilişim sistemine girme ve kalma suçu başta 244'üncü madde olmak üzere diğer suçlar için de bir ön koşuldur. Bu nedenle bu alanda yapılacak düzenlemeleri 243'üncü maddeden itibaren değerlendirilmesi gerekmektedir.

Kişisel verilerin korunması kapsamı önceki bölümlerde belirtildiği üzere birçok kanunda parça parça yer almaktadır. Ayrıca, uluslararası alanda işbirliğinin ve güvenliğin sağlanması için de, kişisel verilerin korunması ile ilgili kanunların uygulanmasının denetlenmesi, bu

bilgilerin istismar edilmesini önleyici teknolojik tedbirlerin koordineli bir şekilde tüm kurumlar tarafından uygulanması gerekmektedir. Bunun nedenle, kurumları koordine edecek ve denetleyecek bağımsız tek bir sorumlu kurumun oluşturulması; kişilerin, kurum ve kuruluşların görev ve sorumluluklarını belirleyen, insan hak ve özgürlüklerini ön planda tutarak, güvenlik-demokrasi, gizlilik-kullanılabilirlik dengesini sağlayan bir kanunun en kısa zamanda hazırlanması gerekmektedir. Özellikle yetkilendirilecek denetleyici kurumun bu kanunu özgürce uygulayabilmesi için hem ekonomik hem de idari yönden bağımsız olması oldukça önemlidir.

Ticari boyutun büyük bir bölümün siber ortama en yaygın biçimiyle de internet ortamına taşındığı çağımızda, Uluslararası boyuttaki kurum ve kuruluşlar yatırım yapacakları ülkeleri değerlendirirken inceledikleri en önemli kriterlerden birisi de siber güvenlik ve verilerin korunması ile ilgili mevzuatın bulunup bulunmadığıdır. Bu nedenle, ulusal refah ve itibar için öncelikle ulusal anlamda bilişim suçlarıyla mücadele ve bu kapsamda yasal mevzuatın gerçekleştirilmesinin, sonrasında da siber saldırıların kaynağının sınırının bulunmaması nedeniyle mücadele de uluslararası işbirliği ve mevzuatın oluşturulmasının önemi de ortaya çıkmaktadır.

Bilişim alanında işlenen suçların en hızlı değişim gösteren suç türü olduğu dikkate alınarak, bilişim suçlarıyla etkin ve süratli bir şekilde mücadele edebilmek için bilişim alanındaki gelişmeleri sürekli inceleyen ve ortaya çıkan değişiklikleri tespit eden, "Bilişim Alanında Uzman Hukukçulara" büyük ihtiyaç vardır. Bu kapsamda, bilişim suçları ile ilgili düzenlemelerin süratli bir şekilde uygulanması ve hukuksal açıdan denetlenmesi için tam yetkili ve bağımsız Bilişim İhtisas Mahkemeleri oluşturularak, bilişim hakimleri ve savcılarının görevlendirilmesi söz konusu ihtiyacı büyük ölçüde karşılayabilecektir. Çünkü bu sayede, sürekli değişen ve gelişen teknolojik imkanların ortaya çıkardığı yeni suçlarla mücadele için, belirli aralıklarla eğitimleri güncellenerek uzmanlaşmaları sağlanabilen hakim ve savcılara sahip olunabilecektir. Söz konusu eğitim ihtiyacı; hukuk fakültelerinde seçmeli bilişim derslerinin açılmasıyla, mesleğe atandıktan sonra bu alanda uzmanlaşması uygun görülen personele üniversitelerle yapılacak protokol kapsamında yüksek lisans ve doktora eğitimlerinin verilmesiyle ya da meslek içi kurslar ile karşılanabilecektir. Bunun yanında bilişim hukukuna ilişkin nitelikli avukatların yetiştirilmesi maksadıyla barolar ve üniversiteler tarafından bilişim hukukuna ilişkin programların sayısı ve etkinliğinin artırılması güçlü bir muhakemenin yapılmasına katkı sağlayacaktır. Mevcut durumda, bilişim savcıları görevlendirilmekle beraber, bilişim alanında gerekli eğitime sahip olmadıkları ve dolayısıyla bu alanda uzmanlıklarının yetersiz olduğu, bu nedenle de çoğunlukla bilirkişi raporlarına dayanarak sübjektif kararlar verildiği görülebilmektedir. Özellikle son zamanlarda bilgi ve teknoloji tabanlı yapılan saldırıların nitelik ile miktarındaki önemli artışlarda dikkate alınarak ve bilişim suçlarına ait davalarda süratli bir şekilde karar verilmesi zorunluluğu nedenleriyle Bilişim İhtisas Mahkemelerinin kurulmasının; kurulurken ise Çocuk Ceza Mahkemeleri veya Fikri ve Sınai Haklar (Ceza) Mahkemelerinin örnek alınmasının uygun olacağı değerlendirilmektedir.

KAYNAKLAR (REFERENCES)

[1] A. Köksal, "Adı Bilgisayar Olsun", *Cumhuriyet Kitapları, Bilişim Yazıları*, Ankara, 2010, (44).

[2] M. E. Artuk, A. Gökçen, A. C. Yenidünya, **Türk Ceza Kanunu Şerhi, 5. Cilt**, Turhan Kitapevi, Ankara, 2009, s. 4643.

[3] K. Doğan, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", *Hukuk ve Adalet*, (294), 2005.

[4] Y. Yazıcıoğlu, **Bilgisayar Suçları**, Alfa Yayınları, İstanbul, 1997.

[5] Y. Yazıcıoğlu, " Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi", *Hukuk ve Adalet: Eleştirel Hukuk Dergisi*, İstanbul, 2004, s.177.

[6] ESEN Sinan, **Malvarlığına Karşı Suçlar Belgelerde Sahtecilik ve Bilişim Alanında Suçlar**, Adalet Yayınevi, Ankara 2007, (s. 628).

[7] H. Karakehya, "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", *TBMM Dergisi*, 2009, sayı 81, s.1-24.

[8] Y. Erdoğan, " Bilişim Sistemine Girme ve Kalma Suçu ", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 2012, Cilt: 12, s. 363-1433.

[9] Y. Yazıcıoğlu, **Bilgisayar Suçları**, Alfa Yayınları, İstanbul 1997, s.20.

[10] H. Özdemir, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin Yayıncılık, Ankara, 2009.

[11] D.Y. Civelek, **Kişisel Verilerin Korunması Ve Bir Kurumsal Yapılanma Önerisi**, Devlet Planlama Teşkilatı Uzmanlık Tezi, **www.bilgitoplumu.gov.tr**, 2011.

[12] Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik, **http://www.mevzuat.basbakanlik.gov.tr**, 2013, Erişim Tarihi: 20.06.2015.

[13] Ç.Z. Ünsal, "Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu Ve Avrupa Birliği'nin 95/46/Ec Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi", *Araştırma, Hacettepe Hukuk Fakültesi Dergisi*, 2013, 3(1).

[14] A. Özdemir, E. Akçaoğlu, "Ceza Hukuku Alanında Kişisel Verilerin Korunması", *Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü*, 2014.

[15] Kalkınma Bakanlığı Bilgi Toplumu Dairesi, "Bilgi Güvenliği, Kişisel Bilgilerin Korunması ve Güvenli Internet Ekseni Mevcut Durum Raporu", **Bilgi Toplumu Stratejisinin Yenilenmesi Projesi**, 2013.

[16] V. Bıçak, "Suç Muhakemesi Hukuku", 3.Baskı, *Polis Akademisi Yayınları*, Ankara, 2013.

[17] 5271 sayılı Ceza Muhakemesi Kanunu, **http://www.mevzuat.gov.tr**, Erişim tarihi: 10.08.2015.

[18] Adecco Group, **İş Pazarı Bünyesinde Arz ve Talebin Eşleşmesinde Sosyal Medya Kullanımı İş Arayanların Türkiye'deki Algısı Raporu**, Türkiye, 2014.