

KİŞİSEL VERİLERİN KORUNMASI VE DİNLEMELER

İbrahim GÜL¹

GİRİŞ

Bu konu, Türk iç mevzuatının herkes için anlaşılması güçbir kısmıdır. Türkiye, AB Müktesebatını takip etmek için mevzuatını değiştirmek ve revize etme mücadelesi verse de; ulusal çatışma sebebiyle bazı alanlarda ve özellikle veri korumada bilinçli geciktirme olduğu düşünülmektedir. Türkiye’de veri korumayla ilgili bir taslak kanun mevcuttur.² Bu taslak kanunda, verinin kaydedilmesiyle bireylerin temel hakları arasında denge sağlanması amaçlanır.

Avrupa Komisyonunun Bilgi Koruma Günü (2014)/(Data Protection Day 2014) dolayısı ile Avrupa için yeni bir bilgi koruma sistemi çağrısının komisyon gündeminde hala tartışılıyor olmasından konunun güncelliğini yitirmeyeceği anlaşılmaktadır.³

Avrupa İnsan Hakları Mahkemesinin konuya ilişkin tutumunu yansıması açısından; AIHM konuya ilişkin ilk önemli kararını, Klass ve diğerlerinin Almanya’ya karşı yaptığı başvuru üzerine vermiştir. Bunun yanında Mahkemenin “özel yaşam” kapsamında gördüğü ve kişisel verilerin korunması açısından oldukça önemli olan bir kaç durum şöyle sıralanabilir: bireylere ilişkin kişisel bilgilerin resmi makamlarca toplanarak arşivlenmesi (Amann İsviçre’ye karşı, b.n. 27798/95; k.t. 16 Şubat 2000; Rotaru Romanya’ya karşı, b.n. 28341/95, k.t. 4 Mayıs 2001); telefon görüşmelerine ilişkin kayıtları izleme (Malone, Birleşik Krallığa karşı, b.n. 8691/79, k.t. 2 Ağustos 1984; P.G. ve J.H., Birleşik Krallığa karşı, b.n. 44787/98, k.t.25 Eylül 2001); toplanan verilerin toplanma amacı dışında kullanılması (Leander, İsviçre’ye karşı, b.n. 9248/81, k.t. 26 Mart 1987); sağlık verilerinin gizliliği (Z., Finlandiya’ya karşı, b.n. 22009/93, k.t. 25 Şubat 1997; M.S., İsveç’e karşı, b.n. 20837/92, k.t. 27 Ağustos 1997); emniyet güçleri tarafından parmak izi ve fotoğrafların alınması (Murray, Birleşik Krallık’a karşı, b.n. 14310/88, k.t. 28 Ekim 1994); kişisel verilere erişim hakkı (Gaskin, Birleşik Krallık’a karşı, b.n. 10454/83, k.t. 7 Temmuz 1989); kişisel verilerin gerektiğinden uzun süre tutulması (S. ve Marper, Birleşik Krallığa karşı, b.n. 30562/04, 30566/04, k.t. 4 Aralık 2008). Bu (karar içeriği) dolayısıyla, kişisel gelişim hakkını kapsamaktadır.”⁴

Mahremiyetin ve kişisel verinin sınır aşan akışının korunmasını düzenleyen OECD ilkeleri, 1981 Kişisel Verinin Otomatik İşlenmesi Konusunda Bireylerin Korunması için Avrupa Konseyi Sözleşmesi ve AB Direktifleri çerçevesinde, taslak kanun verinin kaydedilmesiyle ilgili bazı ilkeleri belirler ve “Kişisel Veriyi Koruma Kurulu” kurulmasını öngörür. Söz

¹Gümrük Ticaret Bakanlığı, Hukuk Müşaviri.Sınır Aşan Suçlarla Mücadele Bölgesel Teşkilatı (SECI Center) ve İstikrar Pactı Organize Suçlarla Mücadele Sekreteryası (SPOC) Önceki İçişleri ve Hukuk Başkanı.

² Bkz. Başbakanlık Kanun ve Kararlar Genel Müdürlüğü, “Kişisel Verilerin Korunması Kanunu Gerekçesi”ne, <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf>, (Erişim 21Mart2013).

³Avrupa Komisyonu, justice, http://ec.europa.eu/justice/newsroom/data-protection/news/140128_en.htm, (Erişim 29/01/2014).

⁴Elif Küzeci, “Anayasal bir hak: Kişisel verilerin korunması”,2010 Bilişim Kurultayı’, s.148

konusu taslağa göre 'Kurul', görevini yerine getirirken özgür olacak, hiçbir kurum veya otorite Kurulun kararlarını veya karar verme emrini deęiřtirme hakkına sahip olmayacaktır.

Bu Taslak Kanun'daki temel düzenlemeler řöyledir:

- Öncelik olarak, kaydetmenin temel ilkeleri büyük bir açıklıkla belirlenmiştir,
- Verinin kayıt edilmesi bireyin iznine bırakılmıştır,
- Özel kişisel bilginin işlenmesine yasak getirilmiştir,
- Kanuni düzenleme olması şartı ile kamu kurumlarının veriyi kaydedebileceęi öngörülmüřtür,
- Bireyler kaydedilmiş veriyi öğrenme ve bunu düzeltme hakkına sahip kılınmıştır,
- Yurtdışına veri akışına kısıtlamalar getirilmiştir,
- Veri Kayıt Sistemi kurulmuřtur.

Teřkilatlanmaya iliřkin olarak;

- Veri korumanın bağımsız denetim kurumları kurulabilir,
- Ulusal güvenlik ve suçluların kovuřturulması için bu kanunun uygulanmasıyla ilgili bazı istisnalar mevcuttur.
- Bu kanunun kapsamı dışında kalan veri iptal edilecektir.
- Bağımsız bir Kurul kurulmuřtur,
- Yasadıřılık durumlarında, idari ve adli yaptırımlar uygulanacaktır.

Ülkemizde kabul tarihi 7/5/2010 ve Kanun No. 5982 olan Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Deęişiklik Yapılması Hakkında Kanunun 2 inci maddesi ile Türkiye Cumhuriyeti Anayasasının 20. maddesine;"Herkes, kendisiyle 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 kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına iliřkin esas ve usuller kanunla düzenlenir." hükmü Anayasaya derç edilmiştir.

I. CEZA HUKUKUNDA KİŐİSEL VERİLERİN KORUNMASI

5327 sayılı Türk Ceza Kanunu'nda (TCK) kişisel verilerin korunması ile doğrudan iliřkili bir kısimsuçlara yer verilmiştir. Bu suçlar, "Özel Hayat ve Hayatın Gizli Alanına Karşı Suçlar" (md.132-140) başlıklı dokuzuncu bölümde yer almaktadır. Bu bölümde kişisel verilerle ilgili suçlar; haberleşmenin gizliliğini ihlal (md.132), kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (md.133), özel hayatın gizliliğini ihlal (md.134), kişisel verilerin kaydedilmesi (md.135), verileri hukuka aykırı olarak verme veya ele geçirme (md.136), verileri yok etmeme (md.138) suçları olarak karşımıza çıkmaktadır. Söz konusu suçlar ile bu yolla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri deęerlendirilebilir ve kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmi dört saat içinde yetkili ve görevli hakim onayına sunulur.

Ülkemizde bir veri koruma kanununun bulunmaması, SBS'yedahl olmaya engel teşkil etmektedir. Ayrıca, Türkiye, Sirene Ofisleri olarak adlandırılan ve suç ve suçlulukla mücadelede kullanılan, SBS ile en az Interpol ve Europol kadar önemli bir işbirliği kanalı olan Ofislerden de SBS'yedahl olmadığı için faydalanamamaktadır.

Veri koruma ve kişisel veri ile ilgili düzenleme taahhütleri, ülkemizin Katılım Ortaklığı Belgelerine cevaben hazırladığı 2001 ve 2003 Yılları Ulusal Programlarında da yer alan

yükümlülüklerdendir. 2008 Yılı Ulusal Programında ise bu konuya AB'nin Katılım Ortaklığı Belgesinde doğrudan atıf yapmaması sebebiyle değinilmemiştir. Bu durumun, AB gözünden, Türkiye'deki çalışmalarının 2008 yılından önce bitirilmiş olması gereken bir konunun aynı nitelikteki bir belgede tekrar yer verilmesine gerek görmemesi olarak bakılması mümkün olup, konunun bir zafiyet olarak değerlendirilmesi gerekmektedir.

II. KİŞİSEL VERİLERE İLİŞKİN YÜKSEKMAHKEME KARARLARI⁵

17.2.2010 günlü, 5952 sayılı Kamu Düzeni ve Güvenliği Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun'un;.....maddesinin iptali üzerine verilen Anayasa Mahkemesi Kararı aşağıdaki gibidir;

“İptali istenen kuralda Kamu Düzeni ve Güvenliği Müsteşarlığının ana hizmet birimlerinden olan Araştırma-Geliştirme Daire Başkanlığının terörle mücadele alanında, veri, bilgi ve belgeleri toplayabileceği, tasnif edebileceği, analiz ve değerlendirmeler yapabileceği hükmüne bağlanmaktadır.

“...İptali istenen kuralda geçen “veri”, “bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done” anlamına gelmekte olup, bilimsel, istatistiki, ekonomik, kişisel bilgileri de içine alan bir kavramdır. Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Ancak söz konusu hak sınırsız değildir. Kişisel verilerin korunması hakkı, veri sahibinin mutlak ve sınırsız bir veri hakimiyetini mümkün kılmamaktadır. Nitekim Türkiye'nin imzaladığı ancak uygulama kanununun yürürlüğe konamaması nedeniyle taraf olmadığı 1981 tarihli ve 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür. Bu nedenle, kişisel verilerin korunması temel hakkına kamu yararı nedenlerine dayalı olarak müdahale edilebilmesine olanak tanınmaktadır.

Terörle mücadele alanında strateji ve politikalar geliştirmekle görevli olan Kamu Düzeni ve Güvenliği Müsteşarlığının kendisine verilen görevleri yerine getirebilmesi için kişisel veriler de dahil olmak üzere bir takım bilgi ve belgelere ihtiyacının bulunması kaçınılmazdır. Ayrıca, söz konusu düzenlemenin kişisel verilerin korunmasını isteme hakkını aşırı derecede zorlaştıran ya da ortadan kaldıran, dolayısıyla hakkın özüne dokunan bir sınırlama olmadığı da açıktır. Açıklanan nedenlerle, iptali istenen kural, Anayasa'nın 13. ve 20. maddelerine aykırı değildir. İptal isteminin reddi gerekir.”Anayasa Mahkemesi yukarıdaki karar ile tanımı çok belirgin olmayan “terör” hususunda kişisel verilerin sınırsız bir biçimde kullanım ve depolanmasına izin vermiş bulunmaktadır.

Yargıtay 10. Ceza Dairesi'ne ait olan 31.01.2013 günlü, ve E. 2012/22375, K.2013/1077 sayılı kararında, “Sanıklar hakkında ‘uyuşturucu madde ticareti yapma’ suçu nedeniyle iletişimin dinlenmesi ve kayda alınması kararları alınmıştır.

⁵Anayasa Mahkemesi web sitesi,

http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar&id=10000357&content=ki%FEisel%20veriler, (Erişim 22 Haziran 2013).

Bu kararlara dayanılarak dinlenen telefon görüşmeleri, ancak 'uyuşturucu madde ticareti yapma' suçu yönünden delil olarak kullanılabilir. 'Suç işlemek amacıyla örgüt kurma veya suç işlemek amacıyla kurulmuş olan örgüte üye olma' suçları yönünden dinleme kararı bulunmadığından, sözü edilen telefon konuşmaları bu suçlarda delil olarak kullanılmaz.

"Somut olayda, örgüt oluşturmak için sanıkların sayısı yeterli ise de; suç işleme iradelerinde devamlılık ve aralarında hiyerarşik ilişki bulunduğuna ilişkin delil olmadığından, TCK'nın 220. maddesinde düzenlenen 'suç işlemek için örgüt kurma' ve dolayısıyla 'suç işlemek için kurulan örgüte üye olma' suçlarının unsurlarının oluşmadığı, hukuka aykırı delil niteliğindeki telefon konuşmalarının bu suçlar yönünden hükme esas alınamayacağı gözetilmeden, sanıkların bu suçlardan beraatları yerine mahkumiyetlerine karar verilmesi, ... bozmayı gerektirmiştir." şeklinde karar verilmiştir.

Usule uygun yapılan bir dinleme sırasında CMK m.138/2 kapsamına giren bir başka suçun işlendiği şüphesine ulaşıldığında yapılmaması gereken, o suç yönünden dinlemeye devam edilmesi ve elde edilen bilgilerin yargılamada kullanılmasıdır. Yapılması gereken ise, yeni suç yönünden yeni bir soruşturmanın başlatılmasıdır. Yeni soruşturmaya konu edilen suç, CMK m.135/6'da sayılan katalog suçlar kapsamında ve CMK m.135/1'in şartlarını taşımakta ise, ancak yeni bir iletişimin denetlenmesi kararı alınmak suretiyle telefon dinleme, konuşulanları kayda alma ve sinyal bilgilerinin değerlendirilmesi yöntemlerine başvurulabilecektir. Önceki dinleme kararından hareketle, dinleme kararına konu edilmeyen suç yönünden dinleme yapılamaz ve bu dinlemeden elde edilen delilleryargılamadakullanılamaz.

Keza; Yargıtay 5. Ceza Dairesi'ne ait 11.07.2012 günlü ve E.2009/9137, K.2012/8215 sayılı kararda, sanığın yakalanmasının sağlanması gerekçesiyle alınan iletişimin dinlenmesi kararının, CMK m.135/4 uyarınca ancak şüpheli veya sanığın yakalanabilmesi için mobil telefonun yerinin tespitinde kullanılabileceği, bu yöntemle bir başkasının iletişiminin dinlenemeyeceği, dava açıldıktan sonra yakalama için yapılacak iletişimin denetlenmesi dışında, bir başkasının telefonunun dinlenmesinin ve bu yolla bir başka suça ilişkin elde edilen delilin hukuka uygun sayılamayacağı ve mahkumiyete dayanak olarak kullanılamayacağı hususları gözetilerek, hukuka aykırı delil niteliği taşıyan dinleme kayıtlarının dikkate alınamayacağı, dosya kapsamında yer alan dinleme kayıtları dışında da, sanıkların mahkumiyetine yeter nitelikte, somut ve kesin delil bulunmadığından, atılı suçlardan sanıkların beraatlarına karar verilmesi yerine, yazılı gerekçelerle CMK m.206/2-a ve 230/1-b'ye aykırı davranılmak suretiyle mahkumiyet kararı verilmesinin bozmayı gerektirdiği ifade edilmiştir.⁶

III. TİCARİ SIR VE AVUKATLIK KANUNU

1136 sayılı Avukatlık Kanununun 4667 sayılı Yasa ile değişik üçüncü fıkrasında; "Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekaletname ibrazına bağlıdır. Derdest davalarda müzekkereler duruşma günü beklenmeksizin mahkemeden alınabilir." hükmü düzenlenmiş bulunmaktadır. 640 KHK ile İç ticaret görevleri Gümrük ve Ticaret Bakanlığı olarak yeniden

⁶AG Hukuk Bürosu, Telegon Dinlemede En Yeni Yargıtay Kararının İrdelenmesi, <http://www.aghukukburosusu.com/makale-266-telefon-dinleme-en-yeni-yargitay-kararinin-irdelenmesi.html>, (Erişim, 31/01/2014).

yapılanan mülga Gümrük Müsteşarlığına verildiğinden ticari sır kavramına bu bakanlıkla ilgili olarak değinilmelidir.

Avukatın talebi değerlendirilirken öncelikle talep konusunun avukatın temsil ettiği müvekkilin korunmaya değer hakları ile ilgisinin bulunup bulunmadığının belirlenmesi gerekmektedir.

Özel bir Kanun maddesi ile sınırlama getirilip getirilmediği hususunda ise, 4458 sayılı Gümrük Kanunu'nun 12 nci maddesinin 1 inci fıkrasında;

“Gümrük İdareleri gizli nitelikteki veya gizlilik esasına göre elde edilen bütün bilgileri saklamak zorundadır. Bu bilgileri veren kişinin veya makamın açık izni olmaksızın söz konusu bilgiler açıklanamaz. Şu kadar ki, gümrük idareleri verilerin korunmasına ilişkin yasal hükümler veya yargı kararlarının gereği olarak söz konusu bilgileri ilgili mercilere verirler.” hükmü düzenlenmiş bulunmaktadır.

Ticaret şirketlerinin gümrük işlemleri dolayısıyla gümrük idaresinin bilgisi dahiline giren bilgilerinden hangisinin gizli bilgi/ticari sır kapsamına girdiği hususu, "ticari sır" kavramının tanımına bağlıdır.

Bu arada belirtmek gerekir ki; 5397 sayılı Kanunun Ek 5. maddesine göre, “Ayrıca, kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların ihtiyaç duyulan bilgi ve belgelerinden yararlanabilmek için gerekçesini de göstermek suretiyle yazılı talepte bulunulabilir. Bu kurum ve kuruluşların kanuni sebeplerle veya ticari sır gerekçesiyle bu bilgi ve belgeleri vermemeleri halinde ancak hâkim kararı ile bu bilgi ve belgelerden yararlanılabilir.”

A. Ticari Sır

Türk pozitif hukuku incelendiğinde,18/10/2010 tarihli ve 27556 sayılı Resmi Gazetede yayımlanan "Dosyaya Giriş Hakkının Düzenlenmesine ve Ticari Sırların Korunmasına İlişkin Tebliğ"in bir ve ikinci fıkralarında ticari sır kavramının; “teşebbüslerin faaliyet alanları ile ilgili olan ve gizli tutma iradesine sahip oldukları, yalnızca belirli ve kısıtlı bir kesim tarafından bilinen ve elde edilebilen, başta rakipleri olmak üzere üçüncü kişilere ve kamuya açıklanması halinde ilgili teşebbüsün ciddi zarar görme ihtimali bulunan her türlü bilgi ve belgedir.” şeklinde tanımlandığı görülmektedir.

Yargı Kararları incelendiğinde de, ticari sır kavramının tanımının yapılmadığı, uyuşmazlığa konu olaya göre söz konusu bilgi ve belgelerin ticari sır veya ticari sır olmadığına karar verildiği, bazı kararlarda ticari sırrın unsurlarına yer verildiği görülmektedir(Danıştay 13. Dairenin 25/11/2008 tarihli ve E:2006/4829, K:2008/7417 sayılı; Yargıtay 11. Hukuk Dairesinin 28/10/2005 tarihli ve E:2005/11731, K:2005/10513 sayılı; Danıştay 1. Dairenin 10/4/2002 tarihli ve E:2002/26, K:2002/52 sayılı, Danıştay 10. Dairenin 6/3/2007 tarihli ve E:2004/10375, K:2007/891 sayılı kararı).

IV. TÜRKİYE’NİN ÇIKMAZI

Anayasa'nın⁷ 38/3 maddesindeki, “Kanuna aykırı elde edilmiş bulgular delil olarak kabul edilemez.” düzenlemesine paralel olarak Amerikan Ceza Hukuku sisteminde "zehirli ağacın meyvesi tabiri (Fruit of thepoisonoustree)" vardır. Buna göre hukuka aykırı elde edilen

⁷TBMM, Türkiye Cumhuriyeti Anayasası, <http://www.tbmm.gov.tr/anayasa.htm>, (Erişim, 01/02/2014).

deliller mahkemelerde dikkate alınmazlar. İlk olarak SilverthorneLumberCo. v. United States, davasından 1920 yılında kullanılmıştır. Bu ilkeye rağmen hukuka aykırı elde edilmiş delillerle Ülkemizde adaletin inşa edilmeye çalışıldığına şahit olunmaktadır. Anayasa'nın 22. Maddesi⁸ ile“Haberleşmenin gizliliği esastır. Haberleşme engellenemez ve gizliliğine dokunulamaz” hükmü ile anayasal koruma altına alınmış haberleşme gene aynı madde ile “Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâk” vs. soyut ve hukuksal olarak ölçülür olmayan ve genel sebeplerle kısıtlanabileceği düzenlenmiştir.

Dış ilişkilerde de benzer biçimde, Sınır aşan suçlarla mücadele kapsamında uluslar arası anlaşmalara ve girişimlere taraf olan Türkiye'nin kişisel verilere ilişkin uluslar arası standartları icra eder hale gelmemiş olması kaygı vericidir. Uluslararası nitelikte suçlarla mücadelede Türkiye, Europol ile 2004 yılında kişisel verilerin paylaşılmasına imkan tanımayan Teknik ve Stratejik Düzey İşbirliği Anlaşması imzalamıştır.

Türkiye'de yasal düzenleme bulunmamasının sonuçlarının uygulamaya yansıdığı alanlardan biri, adli yardımlaşma anlaşmalarının uygulanmasıdır. Bu konuda, başta Almanya olmak üzere, Konseye üye diğer devletler, Türk mahkemelerince yapılan kişiler hakkındaki adres tespiti, istinabe gibi istemleri, Türkiye'nin konuya ilişkin eşdeğer koruma mevzuatı bulunmadığı için geri çevirmektedirler. Türkiye'deki adli makamların, yabancı ülkelere ait vatandaşların nüfus ve sabıka kayıtlarını temin edebilmesi için düzenlenerek Interpol, Europol, aktarılabilmektedir. Durum bu olmasına rağmen SECI/SELEC⁹ Merkezi ile yapılan operasyonel işbirliği sürecinde kişisel bilgilere ilişkin bir sorun yaşanmamaktadır. EUROPOL ile operasyonelkoordinasyon işbirliği anlaşmasının yakın tarihte yürürlüğe girmesininbeklendiğibilinmektedir.

Hukuki konularda aşağıda yer verilen hususlar 1954 tarihli Hukuk Usulüne Dair Sözleşmesi ile 1970 tarihli Hukuki veya Ticari Konularda Yabancı Ülkelerde Delil Sağlanması Hakkında Sözleşme¹⁰ hükümlerine uygun olarak yapılmaktadır. Uluslararası istinabenin kaynakları ikili anlaşma veya çok taraflı sözleşmeler ile uluslararası adli yardımlaşma kurallarıdır. Uluslararası istinabe (adli yardımlaşma), bir devletin yetkili bir adli makamının diğer bir devletin adli makamı adına yerine getirdiği işlemler bütünüdür. İstinabe işlemleri, ilgili devletlerle aramızda yürürlükte bulunan ikili antlaşma ya da çok taraflı sözleşmeler, bunların bulunmaması halinde de, uluslararası teamül hukuku kuralları ve karşılıklılık ilkesi çerçevesinde yürütülmektedir.

Uluslararası ceza istinabe yoluyla yerine getirilebilecek işlemler:

- a)Şüpheli veya sanıkların ifadelerinin alınması veya sorgularının yapılması,
- b)Mağdur, müşteki, katılan, tanık veya bilirkişilerin dinlenmesi,
- c)Bilgi ve delil temini, banka kayıtları, muhasebe belgeleri, şirket dosyaları ve ticari belgeler de dahil olmak üzere, ilgili belge ve kayıtların asıllarının veya tasdikli suretlerinin sağlanması,
- d) Delil toplamak amacıyla; kazanç, malvarlığı, araç-gereç ya da diğer hususların tespiti veya izlenmesi,**

⁸A.e.,**MADDE 22-** (Değişik: 3/10/2001-4709/7 md.)

Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış mercii yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz

⁹ Güneşoğlu Avrupa Kolluk Kuvveti Merkezi (SELEC), Bükreş'te yerleşiktir.

¹⁰ TBMM, <http://www.tbmm.gov.tr/kanunlar/k5128.html>, (Erişim:02.05.2014).

- e) Delil amaçlı arama ve el koyma, eşya ve yer incelemesi,
- f) Yabancı mahkemelerce verilen el koyma veya benzeri tedbirlerin infazı,
- g) Yabancı mahkemelerce verilen nihai hükümlerde yer alan, hapis cezası, para cezası, müsadere, hak yoksunluğu veya diğer cezai yaptırımların infazı.¹¹

Yukarıda sıralanan genel esaslar uluslararası veri değişiminde rehber ilkeler niteliğindedir. Dolayısı ile bilinmesinde fayda mülhaza edilmiştir.

Avrupa Birliğinin kendine özgü kuralcı yaklaşımının ABD için söylenemeyeceği açıktır. ABD’de kuralcı bir yaklaşım yerine pragmatik bir yaklaşımın bilgi değişiminde hakim olduğu anlaşılmaktadır. Avrupa Birliği dışındaki ülkelerin veri değişimine ilişkine evrensel uluslararası anlaşmalardan çok ikili anlaşmalara göre hareket ettikleri görülmektedir. Bütün bunların yanı sıra ulusal devletlerin uhdelerinde bulunan verilerin paylaşımında kıskanç oldukları eğer karşılıklı menfaat söz konusu değilse söz konusu bilgi taleplerini ifade büyük olumsuzluklar yaşandığı bilinmektedir. Kontrollü teslimat gibi özel uygulamalar gibi anlık bilgi değişiminin hayati olduğu durumlarda dahi ulusal devletlerin gereken özeni göstermedikleri gözlemlenmektedir. Bu da esasen devletlerde uluslararası veri değişimi bilincinin halen oluşmadığını gösterir. AB’de bile üye ülkelerin bilgi değişimi EUROPOL üzerinden son derece düşüktür.

A. Kanuni Düzenlemeler

- a) Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Korunması Hakkında Yönetmelik (6 Şubat 2004)
- b) Bazı özel Kanunlar (4857 sayılı İş Kanunu, 5490 sayılı Nüfus Hizmetleri Kanunu)
- c) Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik
- d) Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında yönetmelik
- e) Bilgi Edinme Kanunu.

B. 5271 sayılı Ceza Muhakemesi Kanununu Düzenlemesi

1- "İletişimin tespiti, dinlenmesi ve kayda alınması" kenar başlıklı 135.¹² maddesinde, bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe

¹¹Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü,

http://www.uhdigm.adalet.gov.tr/adli_yardimlasma/adli_isbirligi_ceza/cz_istinabe.html, (Erişim:02.05.2014).

¹² CMUK 135. Madde metni şöyledir; **İletişimin tespiti, dinlenmesi ve kayda alınması**

MADDE 135. - (1) Bir suç dolayısıyla yapılan soruşturmalarda, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir ve kayda alınabilir. Cumhuriyet savcısı kararını derhâl hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir Cumhuriyet savcısı tarafından derhâl kaldırılır.

(5) Bu madde hükümlerine göre alınan karar ve yapılan işlemler, tedbir süresince gizli tutulur.

(6) Bu madde hükümleri ancak aşağıda sayılan suçlarla ilgili olarak uygulanabilir:

- a) Türk Ceza Kanununda yer alan;
 1. Göçmen kaçakçılığı ve insan ticareti (madde 79, 80),
 2. Kasten öldürme (madde 81, 82, 83),
 3. İşkence (madde 94, 95),
 4. Cinsel saldırı (birinci fıkra hariç, madde 102),
 5. Çocukların cinsel istismarı (madde 103),

sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişiminin tespit edilebileceği, dinlenebileceği, kayda alınabileceği ve sinyal bilgilerinin değerlendirilebileceği, Cumhuriyet savcısı tarafından verilen kararların derhâl hâkimin onayına sunulacağı; 135.maddenin altıncı fıkrasında ise; Bu madde kapsamında dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümlerin ancak fıkra da sayılan (katalog) suçlarla ilgili olarak uygulanabileceği;

2- "Kararların yerine getirilmesi, iletişim içeriklerinin yok edilmesi" kenar başlıklı 137. maddesinde, 135. maddeye göre verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hâkim onayının alınmaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhâl son verileceği; bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtların Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durumun bir tutanakla tespit edileceği; tespit ve dinlemeye ilişkin kayıtların yok edilmesi halinde soruşturma evresinin bitiminden itibaren, en geç onbeş gün içinde, Cumhuriyet başsavcılığının, tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgisine yazılı olarak bilgi verileceği;

3- "Teknik araçlarla izleme" kenar başlıklı 140. maddesinde, maddede sayılan suçların işlendiği hususunda kuvvetli şüphe sebeplerinin bulunması ve başka suretle delil elde edilememesi halinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetlerinin ve işyerinin teknik araçlarla izlenebileceği, ses veya görüntü kaydının alınabileceği, teknik araçlarla izlemeye hâkim, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından karar verileceği, Cumhuriyet savcısı tarafından verilen kararların yirmidört saat içinde hâkim onayına sunulacağı; hükme bağlanmıştır.

5237 sayılı Türk Ceza Kanunu'nun 132 ila 140.maddelerinde "Özel Hayata Ve Hayatın Gizli Alanına Karşı Suçlar" yaptırıma bağlanmış;2/7/2012 tarihli ve 6352 sayılı Kanun ile sözkonusu maddelerdeki cezalar da arttırılmıştır.

6. Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188),

7. Parada sahtecilik (madde 197),

8. Suç işlemek amacıyla örgüt kurma (iki, yedi ve sekizinci fıkralar hariç, madde 220),

9. İhaleye fesat karıştırma (madde 235),

10. Rüşvet (madde 252),

11. Suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282),

12. Silahlı örgüt (madde 314) veya bu örgütlere silah sağlama (madde 315),

13. Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337) suçları.

b) Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (madde 12) suçları.

c) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar.

d) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74 üncü maddelerinde tanımlanan suçlar.

(7) Bu maddede belirlenen esas ve usuller dışında hiç kimse, bir başkasının telekomünikasyon yoluyla iletişimini dinleyemez ve kayda alamaz.

YENİ MİT YASASI

Yeni MİT yasası ile¹³1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunun'da yapılan değişiklikler ile esaslı olarak MİT'e bilgi, güvenlik konularında sarıh (açık) yetkiler verilmiş, teşkilat görevlilerinin görevleri ve hizmet gereklerine uygun olarak güvenceli bir kamu ajanı statüsü kazandırmıştır. Benzer görev yapan teşkilatlar Türk Silahlı Kuvvetleri, Emniyet Genel Müdürlüğü vs. üzerinde koordinatif ve dominant bir pozisyon kazandırılmıştır. Özellikle, MİT görevlerinin ifası ve bu icrai faaliyetlerle bağlantılı etkili iş ve eylemleri yargı denetiminin dışına taşıyan bir özerk ve dokunulmaz alan yaratılmıştır.

Yapılan değişiklikler ile MİT görevlileri, adli kovuşturma ve soruşturmalardan görevleri ile ilgili olmak kaydı ile istisna tutulmuştur. Tanıklığa ilişkin ayrıcalıklar tanınmıştır. Tüm devlet teşkilatına MİT görevi ile ilgili birincil yükümlükler yüklenilmiştir. Her türlü iletişimin dinlenmesi ve takibine ve bu yöntem veya diğer yöntemlerle elde edilmiş her türlü veriye erişim imkanı tanınmıştır. Ayrıca, TBMM nezdinde bir komisyon kurularak teşkilatın işlem ve faaliyetlerini değerlendirme ve analiz etme imkanı tanınarak bir nevi denetime tabi kılınmıştır. Kişisel verilerin güvenliğini ve bireyin hak ve özgürlüklerini koruyucu öneriler geliştirmek amaçlı görevlerin bu komisyona verilmiştir. Genel olarak bu kanun modern istihbarat hizmetleri ve konseptine uygun standart düzenlemeleri içermektedir. Kanunda örtülü operasyonlara ilişkin düzenleme olmaması bir eksikliklerdir. Ancak MİT Yasasında derinlik ve genişlik oluşturan bu tadil/düzenleme iç/dış güvenlik, savunma, terörle mücadele, sınıraşan organize suçlarla doğrudan ilgili olan istihbarat örgütüne modern ve etkili yapısal dönüşüm olanağı tanınmıştır. Kişisel verilerin güvenliğini ve bireyin hak ve özgürlüklerini koruyucu öneriler geliştirilmesi ödevi ise kayda değer bir demokratik uygulamanın önünü açacaktır. TBMM nezdindeki komisyon istihbarat faaliyetlerinin gerçekçi ve etkili denetimi sağlayarak olağanüstü yetkilerle donatılmış teşkilatın kamu yararı doğrultusunda faaliyet göstermesi temin kılınacaktır.

V. YASA DIŞI DİNLEME TBMM REAKSİYONU VE YASAL ÇERÇEVE¹⁴

Telekomünikasyon yoluyla iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine ilişkin kararların, hangi kurumlar tarafından hangi şartlarda alınabileceği, kararların hangi mahkemeler tarafından verilebileceği, kararların taşınması gereken zorunlu unsurların neler olduğu, bu kararların hangi kolluk birimlerince yerine getirileceği ve kayıtların kimlerin sorumluluğunda olduğu gibi hususlar ve bu hakların ihlali halinde uygulanacak cezai yaptırımlar mevzuatta ayrıntılı olarak belirlenmiştir.

Anayasa ve yasalarca güvence altına alınan bu temel haklara ve etkin cezai yaptırımlara rağmen kamuoyunda böcek, gizli kamera veya uzaktan dinleme sistemi gibi dünyadaki teknik gelişmelerin bu konuda sağladığı yasal olmayan tüm yöntemleri kullanarak kişiler arasındaki konuşmaların dinlendiği, kayda alındığı ve bu kayıtların kimi zaman basın yayın yoluyla hukuka aykırı bir şekilde kullanıldığı yönünde kamuoyunda bir algı oluştuğu gözlemlenmektedir.

¹³6532 Sayılı Devlet İstihbarat Hizmetleri Ve Millî İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun, Resmi Gazete, 1.4.2014, 28983

¹⁴ TBMM web sitesi, "Yasa Dışı Dinlemeleri Araştırma Komisyonu Kuruldu", http://www.tbmm.gov.tr/eyayin/GAZETELER/WEB/MECLIS%20BULTENI/2469_2013_0000_0185_0000/0005.pdf, (Erişim 04Nisan2013).

Anayasa Mahkemesi'ne göre; "Anayasa'nın 22. maddesinde öngörülen haberleşme özgürlüğü, kişinin kesintiye uğramadan ve sansür edilmeden başkalarıyla iletişim kurma hakkıdır. Bu özgürlük, çok daha geniş bir alanı kaplayan "özel hayatın" bir yönünü oluşturur. Dolayısıyla "haberleşmenin gizliliği" kavramı, özel hayatın gizliliği kavramı içinde yer alır...Özel hayatın gizliliği ile haberleşmenin gizliliği, her türlü yasa dışı müdahaleye karşı Anayasa ve diğer yasalarla güvence altına alınmıştır." (AYMK.E.2008/115,K. 2011/86,T. 2.6.2011;AYMK.E. 1996/68,K. 1999/1,T. 6.1.1999). Anayasa'nın 22. maddesinde öngörülen bu güvence, hiç şüphesiz, üçüncü şahısların haberleşme özgürlüğüne yasa dışı müdahalelerini de kapsamaktadır.¹⁵

Tarafı olduğumuz ve onaylamakla iç hukuk mevzuatına dahil ettiğimiz "Avrupa İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi'nin 8. maddesinde de herkesin haberleşmesine saygı gösterilmesi hakkına sahip olduğu kurala bağlanmış, bu hakka bir kamu otoritesinin müdahalesinin ancak, ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda gerekli olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabileceği belirtilmiştir.

Kişiler arasındaki haberleşme içeriklerinin suç öncesi veya belli bir suça ilişkin soruşturma kapsamında Anayasa ve kanunların belirlediği koşullar çerçevesinde öğrenilmesinin veya kayda alınmasının hukuka uygun olduğu muhakkaktır.

Ülkemizde iletişimin denetlenmesi ve telefonların dinlenmesi, 1 Haziran 2005 tarihine kadar 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu, bu tarihten itibaren ise 5271 sayılı Ceza Muhakemesi Kanunu ile düzenlenmiştir.

Düzenlemeler suçların soruşturulması sırasında ve sanık takibi amacıyla kolluk kuvvetlerince iletişime yapılan müdahaleye ilişkin olup, sadece suç işlendikten sonra" yapılan, adli amaçlı dinlemeleri kapsamaktadır.

C. İstihbarat Hizmetleri kapsamında

Suç ve suçluluk ile mücadelede istihbarat vazgeçilmez bir araçtır. İstihbarat çalışmaları ise, bilgi toplamak ve depolamak şeklinde olduğundan, özel hayat ve aile hayatı ile yakından ilgilidir. Elektronik yoldan yapılan iletişimin suç öncesi alanda dinlenmesi ise, haberleşme hürriyeti ile ilgilidir. Anayasal düzenlemeler karşısında, Türkiye'de istihbarat hizmetleri ancak bir kanuna dayalı olarak yapılabilecektir. İstihbarat teşkilatları tarafından yürütülen faaliyetler; suç ile ilişkili olmayıp kuruluş yasalarında yer alan görevleri kapsamında ulusal güvenliğin sağlanması amacıyla, demokratik hukuk devletine yönelik tehdit unsurlarına ilişkin olarak düzenli ve sistemli bilgi toplama ve değerlendirmeyi gerekli kıldığından;3.7.2005 tarih ve 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ¹⁶ile ABkriterleri, Anayasanın 22 nci maddesinde yer alan temel ilkeler ve 5271 sayılı

¹⁵Bknz. "Böcek raporu Çiçekte", Sabah Gazetesi, 20 Haziran 2013, Bu kamsamda Sayın Çiçek, "Çiçek Komisyon Başkanı Yusuf Başer'e "Sizin çalışmanız tedirginlikleri ortadan kaldırmak, vatandaşın huzur içinde olmalarını sağlamak, 'dinleniyor muyum, özel hayatıma müdahale ediliyor mu?' tarzındaki bir seri sorunun cevabını bulabilmesi açısından önemli" şeklinde beyanatlarda bulunmuştu. <http://www.sabah.com.tr/Gundem/2013/06/20/bocek-raporu-cicekte>,(Erişim 26/06/2013).

¹⁶Tbmm, Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, <http://www.tbmm.gov.tr/kanunlar/k5397.html>, (Erişim,30/01/2014). Bu kanun ile;EK MADDE 5.- Jandarma, bu Kanunun 7 nci maddesinin (a) bendine ilişkin görevleri yerine getirirken önleyici ve koruyucu tedbirleri almak üzere, sadece kendi sorumluluk alanında 4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç, 250 nci maddesinin

Ceza Muhakemesi Kanununda belirtilen esaslara bağı kalınarak, iletişime müdahalenin "hangi hallerde" yapılacağı, "karar mercii" ve "süresi" şeklindeki temel unsurlara yer verilmek suretiyle "önleyici amaçlı istihbarat dinlemesi" ne dair düzenlemeler yapılmıştır. Bu çerçevede 2559 sayılı Polis Vazife ve Salahiyet Kanununun ek 7. maddesinde, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun ek 5. maddesinde, 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununun "Yetkiler" kenar başlıklı 6. maddesinde, önleyici, koruyucu veya istihbari tedbirler kapsamında telekomünikasyon yoluyla yapılan iletişimin hâkim kararıyla tespit edilebileceği, dinlenebileceği, sinyal bilgilerinin değerlendirilebileceği ve kayda alınabileceği düzenlenmiştir. 5397 sayılı kanunun Ek 5. Maddesine göre, "Yetkili ve görevli hâkim, talepte bulunan kolluk biriminin bulunduğu yer itibarıyla yetkili olan ve 5271 sayılı Kanunun 250 nci maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemesinin üyesidir."

Öte yandan 3.7.2005 tarihli ve 5397 sayılı Kanunun 1.maddesi ile 2559 sayılı Polis Vazife ve Salahiyet Kanununun ek 7. maddesine eklenen fıkra hükümlerine göre; "Bu maddede belirtilen işlemler ile 5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak dinlemeler, Telekomünikasyon Kurumu bünyesinde, Kurum başkanına doğrudan bağlı "Telekomünikasyon İletişim Başkanlığı" adıyla kurulan tek bir merkezden yürütülür.Bu maddede belirlenen usûl ve esaslara aykırı dinlemeler hukuken geçerli sayılmaz ve bu şekilde dinleme yapanlar hakkında 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu hükümlerine göre işlem yapılır."

Yukarıda açıklanan hükümler çerçevesinde, telekomünikasyon yoluyla iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine ilişkin kararların, hangi kurumlar tarafından hangi şartlarda alınabileceği, kararların hangi mahkemeler tarafından verilebileceği, kararların taşınması gereken zorunlu unsurlar, bu kararların hangi kolluk birimlerince yerine getirileceği ve kayıtların kimlerin sorumluluğunda olduğu hususları mevzuatta ayrıntılı olarak belirlenmiştir. Telekomünikasyon İletişim Başkanlığı tarafından resen dinleme yapılmamakta, dinlemeler talep üzerine mahkemelerce verilen kararlar çerçevesinde yerine getirilmektedir. Buna göre, hâkim kararı bulunmadıkça, gecikmesinde sakınca bulunan durumlarda ise yirmidört saat içinde hâkim onayı alınmadıkça dinleme

birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Jandarma Genel Komutanı veya istihbarat başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişimi tespit edebilir, dinleyebilir, sinyal bilgilerini değerlendirebilir, kayda alabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmidört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç yirmidört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir. Bu işlemler, 4.7.1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyet Kanununun ek 7 nci maddesinin onuncu fıkrası hükmüne göre kurulan merkez tarafından yürütülür. 5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak dinlemeler de bu merkez üzerinden yapılır. Uygulanan tedbirin sona ermesi halinde, dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.

Bu maddede belirtilen suçların önlenmesi amacıyla ve hâkim kararı alınmak koşuluyla, teknik araçlarla izleme yapılabilir. Ayrıca, kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların ihtiyaç duyulan bilgi ve belgelerinden yararlanabilmek için gerekçesini de göstermek suretiyle yazılı talepte bulunulabilir. Bu kurum ve kuruluşların kanuni sebeplerle veya ticari sır gerekçesiyle bu bilgi ve belgeleri vermemeleri halinde ancak hâkim kararı ile bu bilgi ve belgelerden yararlanılabilir

yapılabilmesi hukuken mümkün değildir. Kamu güvenliğini ve demokratik toplumu korumayı amaç edinen devlet otoritesinin, özellikle organize suçları ve terör eylemlerini önlemek amacıyla, bir takım gizli polisiye metotlarına müracaat etmeleri zorunludur. Ancak suç önleyici tedbirlerin gizli olması, bu tedbirlerin kötüye kullanılması sorununu da beraberinde getirdiği için, iletişim özgürlüğünün korunması bakımından mevzuatın etkili güvenceler öngörmesi gerekmektedir.

5397 sayılı Kanun ile ilk kez kanuni bir altyapıya kavuşturulmuş olan istihbarat amaçlı iletişimin denetlenmesi tedbiri bakımından, A.İ.H.M tarafından ortaya konulmuş olan bazı ilkelere Kanunda yer verilmemiştir. Özellikle istihbarat amaçlı iletişimin denetlenmesi tedbirine *ancak kuvvetli suç işleme tehlikesinin bulunduğu ve klasik bilgi toplama ve takip metodları ile sonuç alınamayacak durumlarda (son çare prensibi) başvurulabileceği* hususunun Kanunda açık bir biçimde yer alması gerekmektedir. İstihbarat amaçlı iletişimin denetlenmesine ilişkin kanun hükümleri bakımından önemli eksikliklerden birisi de, Kanun kapsamında gizli tedbirlerin denetimi için etkin bir denetim mekanizmasının oluşturulmamış olmasıdır. Özellikle gecikmesinde sakınca bulunan hallerde verilen yazılı emrin süresi içerisinde hâkim onayına sunulup sunulmadığının denetimi bu yetkinin kötüye kullanılması bakımından önemlidir. Ayrıca bu tedbirin uygulanmasından sonra, uygulamaya ilişkin olarak 5271 sayılı C.M.K'da olduğu gibi bir bilgilendirme düzenlemesine ihtiyaç bulunmaktadır. Bireylerin, iletişimlerinin denetlenip denetlenmediği konusunda bir bilgiye sahip olmadan herhangi bir hak arama vasıtasına müracaat edebilmesi mümkün değildir. Mevzuat içerisinde değişiklik kanunlarla getirilmiş olan bilgi edinme araçlarının etkin bir hak arama özgürlüğü sağladığını söylemek mümkün değildir.

5397 sayılı Kanun kapsamında istihbarat amaçlı iletişimin denetlenmesi tedbiri, “*suç önleyici tedbir*” niteliğinde düzenlenmiştir ve *suçun önlenmesi amacıyla ve sadece kanunda yer verilen sınırlı sayıda suç* bakımından müracaat edilebilecek bir tedbirdir. Ayrıca, *iletişimin denetlenmesine karar veren ve gecikmesinde sakınca bulunan hallerde idari görevliler tarafından verilen yazılı emri denetleyen hâkimin, özellikle kuvvetli şüphe sebepleri ve klasik tedbirlerin yetersiz kalacağına ilişkin (son çare prensibi) somut hususların varlığını araştırması ve onay ya da red kararını bu hususlar bağlamında gerekçelendirmesi gerekmektedir.*

5397 sayılı Kanun, iletişimin denetlenmesi tedbirinin denetimi bakımından, özellikle tedbiri bizzat icra eden, polis, jandarma ve M.İ.T. hakkında, *sadece genel teftiş ve denetim hükmüne yer vermiştir.* Sürekli “*dinlenme*” paranoyasının olduğu ve görevi sadece “*koordinasyon*” ile sınırlı olan T.İ.B.’in dahi “*kanunsuz dinleme*” gerçekleştirdiğinden bahisle ve hakim kararı ile müteaddit defalar arandığı ortamda, belki de ihtiyaç duyulan en önemli unsur, bu türden iddia ve şüpheleri ortadan kaldıracak bir etkili bir denetim mekanizmasıdır.¹⁷

Yukarıda açıklanan mevzuat çerçevesinde; kişiler arasındaki haberleşme içeriklerinin hukuka aykırı biçimde tespiti, dinlenmesi ve kayda alınması suç olduğu gibi; kişilerin gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının görüntülü veya sesli olarak saptanması ve kaydedilmesi de suçtur. Dolayısı ile

¹⁷Fatih Birtek, “İstihbarat Amacıyla İletişim Özgürlüğüne Müdahale Edilmesi Ve Müdahaleden Elde Edilen Materyallerin Delil Olarak Kabul Edilebilirliği”, Türk Hukuk Sitesi, http://www.turkhukuksitesi.com/makale_1284.htm, (Erişim, 29/01/2014). Not: Makalenin tüm hakları yazarı Öğr. Gör. Fatih Birtek'e aittir ve makale, yazarı tarafından Türk Hukuk Sitesi (<http://www.turkhukuksitesi.com>) kütüphanesinde yayınlanmıştır.

istihbaratın yegane ve asli işlev hammaddesi olan bilginin hukuk güvenliği ve hukuk devletinin esasları çerçevesinde faaliyet göstermesi gerekecektir.¹⁸

Yazılı emir¹⁹ kavramı TİB'e ait aşağıda detayı verilen yönetmelikle de düzenlenmiş olup uygulamada sıkça kullanılan bir hükümdür. Anılan yönetmeliğin 8. maddesinde, "Gecikmesinde sakınca bulunan hâllerde; Millî İstihbarat Teşkilatı Müsteşarı veya yardımcısı, Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanı ve Jandarma Genel Komutanı veya İstihbarat Başkanı tarafından telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması için verilen yazılı emir, yirmidört saat içinde 26 ncı maddenin birinci fıkrasında belirtilen yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç yirmidört saat içinde verir." Bu kararda yer alması gerekli unsurlar ise 9. maddede belirtilmiş olup madde metni dipnotta verilmiştir.²⁰ 4/5/2007 kabul tarihli 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun²¹ özgürlükleri kısıtlayıcı niteliktedir.

¹⁸Bkn. Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik, (RG, 10.11.2005/25989).

¹⁹Bkn. 10/11/2005 tarihli, Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi Ve Kayda Alınmasına Dair Usul Ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev Ve Yetkileri Hakkında Yönetmelik tarihli, TİB, <http://www.tib.gov.tr/tr/tr-menu-78-25989-sayili-resmi-gazetede-yayimlanan-yonetmelik.html>, (Erişim, 31/01/2014).

²⁰A.e, **Karar ve yazılı emirlerde belirtilmesi gerekli hususlar:**

MADDE 9- İletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına dair hakim kararında ve yetkili merciler tarafından verilen yazılı emirlerde;

a) Hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespiti imkân veren kodundan belirlenebilenler,

b) Tedbirin türü, kapsamı ve süresi,

c) Tedbire başvurulmasını gerektiren nedenler,

d) (Ek: RG-04/07/2007-26572)(1) Yazılı emrin verildiği tarih ve saat,

belirtilir. (Ek cümle: RG-04/07/2007-26572)(1) 6 ncı madde kapsamında 2803 sayılı Kanunun ek 5 inci maddesi uyarınca iletilen talepler ile verilen kararlar ve yazılı emirlerde sorumluluk alanına ilişkin bilgi ve/veya belgelere de yer verilir.

Kararlar en fazla üç ay için verilebilir. Bu süre aynı usulle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilir. Ancak, terör örgütlerinin faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim tarafından üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verilebilir.

²¹ TİB, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu, <http://www.tib.gov.tr/tr/tr-menu-42-kanunlar.html>, (Erişim, 30/01/2014).

Bu kanunun, Erişimin engellenmesi kararı ve yerine getirilmesini düzenleyen aşağıdaki maddesi ile internette iletişim ve yayını kısıtlanabilmektedir.

MADDE 8 – (1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

7) Kumar oynanması için yer ve imkân sağlama (madde 228),

suçları.

VI. HUKUK DIŐILİĐİN SIRADANLAŐMASI VE YAYGINLAŐMASI

Tüm bu yasal düzenlemelere ve etkin cezai yaptırımlara rağmen kamuoyunda böcek, gizli kamera veya uzaktan dinleme sistemi gibi dünyadaki teknik gelişmelerin bu konudaki sağladığı tüm imkân ve yöntemleri yasa dışı biçimde kullanarak kişiler arasındaki konuşmaların dinlendiği, kayda alındığı ve bu kayıtların kimi zaman basın yayın yoluyla hukuka aykırı bir şekilde kullanıldığı yönünde kamuoyunda bir algı olduğu gözlemlenmektedir.

Bu çerçevede;

- a) Ses ve görüntü kaydedici cihazları kişilerin konut veya işyerlerine hukuka aykırı biçimde yerleştirmek suretiyle ses ve görüntü kaydı yapılması;
- b) Üstün teknolojik araçlarla belli bir mesafeden kişinin bulunduğu ortamda yapılan konuşmaların hukuka aykırı olarak dinlenmesi ve kayda alınması;
- c) Bilgisayar üzerinden kişisel verilerin yasadışı yollarla ele geçirilmesi veya kişiye ait ses ve görüntülerin rızası dışında elde edilmesi,
- d) Kişilerin cep telefonlarının mesajlaşma trafiğini veya kayıtlı bilgilerinin yasadışı yollarla izlenmesi ve kaydedilmesi;

gibikamuoyunda ciddi rahatsızlık meydana getiren sorunların vatandaşlarımızdan gelen yoğun şikayet ve talepler dikkate alınarak, sorunun çözüm yolları ve alınması gereken yasal, idari, istihbari ve gerekli diğer tüm tedbirlerin tespiti amacıyla Türkiye Büyük Millet Meclisi tarafından bir araştırma yapılması kamuoyunun yasama organından bir beklentisi haline gelmiştir. Bu bağlamda TBMM bünyesinde araştırma komisyonu kurulmuştur.

Komisyonun konuyu salt dinleme bağlamından değil sorunun esasını teşkil eden kişisel verilerin korunması bağlamında ele alması daha kuşatıcı ve kalıcı çözüm üretilmesine sebep olacaktır. Dinlemeleri düzenleyen, CMUK 135. maddesinin, “Bu maddede belirlenen esas ve usuller dışında hiç kimse, bir başkasının telekomünikasyon yoluyla iletişimini dinleyemez ve kayda alamaz.” düzenlemesinin açık hükmünün etkili kılınması zarureti ortaya çıkmıştır. 5396²² sayılı Kanunda yer alan “Bu maddede yer alan faaliyetlerin denetimi, sıralı kurum amirleri, Emniyet Genel Müdürlüğü ve ilgili bakanlığın teftiş elemanları tarafından yapılır.” hükmünün uygulamada değeri olmayacağı açıktır. İşlemi ifa ve icra eden kurumun soruşturma, tahkikat olmadan hattızatında gizli yürütülen işleri denetlemesi mümkün olmamaktadır.

SONUÇ

Sonuç olarak yasa dışı dinlemelerin hangi araçlar kullanılarak yapıldığının, bu araçların nasıl temin edildiğinin, bu araçların imal ithal ve bulundurulması konusunda mevzuatta herhangi bir eksiklik olup olmadığı ve yaşanan bu sorunun çözümü amacıyla alınması gereken yasal, idari ve istihbari ve diğer önlemlerin tespiti için ciddi adımlar gereklidir.

OECD Konseyi, 11 Temmuz 2013 tarihinde C(2013)79] "Gizlilik Rehber İlke/eri ve Kişisel Bilgilerin Sınırlarını Değiştirilmesine İlişkin" bir Tavsiye Karara kabul etmiştir. Böylelikle, OECD'nin "1980 Gizlilik Rehber İlkeleri güncelleştirilmiştir. Bilindiği üzere, Tavsiye Kararları hukuken bağlayıcı olmamakla birlikte, üye ülkelerde uygulanması beklenmektedir. Söz konusu çalışma, Bilgi, Bilgisayar ve İletişim Politikaları Komitesi (ICCP) "Bilgi Güvenliği ve Gizlilik Çalışma Grubu" (WorkingParty on Information Security and Privacy-WPISP) tarafından yürütülmüştür.

²²Bkn. 5397 sayılı Kanunun “ (Ek fıkra: 3/7/2005 – 5397/1 md.) Bu maddede yer alan faaliyetlerin denetimi, sıralı kurum amirleri, Emniyet Genel Müdürlüğü ve ilgili bakanlığın teftiş elemanları (...) (1) tarafından yapılır.” hükmü. <http://www.tbmm.gov.tr/kanunlar/k5397.html>, (Erşim, 01/02/2014).

Yeni Rehber İlkelerde;

-kişisel bilgilerin korunması ve bilgilerin serbest dolaşımı amacıyla devletlerin gerekli iradeyi göstermeleri,

-üye ülkelerin kişisel bilgilerin korunması için "Ulusal Gizlilik Strateji"leri oluşturmaları ve alan ve bunları uygulamaya geçirmeleri,

-üye ülkelerin "gizliliği uygulama otoriteleri" oluşturmaları,

-veri toplamalarının hesap verilebilirliğinin sağlanması açısından "gizlilik yönetim programları" belirlemeleri,

-üye Ülke/erin "gizliliği uygulama otoriteleri" arası işbirliği ve eşgüdümün ilerletmeleri gerektiği ifade edilmekte olup,

-ICCI'nin Tavsiye Kararı'nın üye ülkelerce hayata geçirilip geçirilmediğini izleyeceği,

- kişisel bilgilerin sınırlar arası değişiminin hangi şartlar altında kısıtlanacağı,²³ hususları düzenlenmiştir.²⁴

Dolayısı ile uluslararası taahhütlerimize istinaden Ülkemizde kişisel bilgilerin uygulanabilir yasal düzenlemelerle kanunlaştırılması gerekmektedir. Yine de, Geçen yirmi yıl içinde kişisel bilgilerin korunmasına ilişkin bir eğilim oluşmuştur. Gelişmiş ülkelerin anayasal koruma ile hüküm altına alınmış bulunan kişisel bilgilerin korunması temel bir insan hakkı olarak kabul edilmektedir.

Önleyici ve adli dinlemelerin denetim mekanizmaları yetersizdir. Dinlemelerin, denetimsizliği kişi güvenliğini ve bunun dolayısıyla kamu güvenliğini tehdit etmektedir. Güvenlik bürokrasına terk edilmeyecek kadar hayati olan bu konunun gecikmeksizin özgürlükçü ve ileri batı devletleri ile paralel düzenlemelere kavuşturulması yararlı olacaktır. Gizli ve hassas bilgilerin kullanımı konusunda komisyon kurularak Anayasa ile koruma altına alınmış temel hak ve hürriyetler ile Uluslararası beklentilere, demokratik hukuk devletinin ilkelerini uygun bir biçimde dinlemelerin her türlü idari eylem ve işlem gibi kamu yararı ve hizmet gereklerine uygun ve idari ve adli açıdan denetlenebilir hale getirilmesi gerektir. 5397 sayılı Kanununun 1. maddesinde yer alan, "Bu maddede yer alan faaliyetlerin denetimi, sıralı kurum amirleri, Emniyet Genel Müdürlüğü ve ilgili bakanlığın teftiş elemanları ve Başbakanın özel olarak yetkilendireceği kişi veya komisyon tarafından yapılır." hükmünün fiiliyatta bir hüküm ifade edemediği son derece açıktır. Denetimsizliğin ve hassas veri elde etme yol ve yöntemlerinin sağlıklı olduğu ortamda, üretilen bilgilerin adli ve idari mercilerce kullanılmakta olması hukuk güvenliği ilkesini yok etmektedir.

KAYNAKLAR

AB Müktesebatının Üstlenilmesine İlişkin Türkiye Ulusal Programı, Cilt 1, 2001, (çevrimiçi) <http://www.abgs.gov.tr/index.php?p=195&l=1>.

AKSOY, Hüseyin Can, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara, 2010.

Australian Government, Office of the Privacy Commissioner, The Operation of the Privacy Act Annual Report, 1 July 2007-30 June 2008, Sydney, 2008.

²³ OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, (2013), <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>, (erişim, 28/01/2014).

BAĞCI, Hasan, “Yolsuzluklarla Mücadelede Veri Madenciliği”, Nisan 2009, http://www.alomaliye.com/2009/hasan_bagci_yolsuzlukla.htm.

BAŞALP, Nilgün, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara, 2004.

Birleşmiş Milletler, İnsan Hakları Evrensel Beyanamesi, 10/12/1948, Office of the High Commissioner for Human Rights, http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/trk.pdf.

Benyon, J., (1996), ‘Policing the Union: European Supranational Law Enforcement Co-operation’, Policing Public Order: Theoretical and Practical Issues, Avebury, England: Avebury/Ashgate Publishing Ltd.

CNIL, (Commission nationale de l’informatique et des libertés), 2007 Annual Activity Report, (çevrimiçi) <http://www.cnil.fr/fileadmin/documents/en/CNIL-AnnualReport-2008.pdf>.

Commission of the European Communities, COM (2001) 298 final, Network and Information Security: Proposal for a European Policy Approach, Brussels, 06/06/2001, http://www.justice.gov/criminal/cybercrime/intl/netsec_comm.pdf.

Convention of The Southeast European Law Enforcement Center. www.selec.org

Counter Terrorism Experiences of SECI MEMBERS COUNTRIES, SECI Anti Terrorism Task Force, June 2011, Ankara

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (ETS 108), Strasbourg, 28 January 1981, <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

Council of Europe, Human Rights and Legal Affairs, National Laws, http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/national%20laws/1NATIONALLAWS_en.asp#TopOfPage

Council of Europe, Resolution 1165 (1998) of the Parliamentary Assembly on Right to Privacy, 26 June 1998, http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta98/eres1165.htm#_ftn1.

DİNÇ, Engin, “Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye’nin Durumu”, (Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi), Diyarbakır, 2006.

European Commission, Flash Eurobarometer, Data Protection in the European Union-Citizens’ Perceptions, February 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

European Commission, “Justice and Home Affairs, Data Protection” http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.

European Commission, “Analysis and impact study on the implementation of Directive EC 95/46 in Member States”, http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

European Court of Human Rights, Case of Klass and others v. Germany, Strasbourg, 6 September 1978, <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=klass&sessionId=41003495&skin=hudoc-en>.

Europe Direct, Data protection in the European Union, Dialogue with citizens and business, EN/IRL, 2000, http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-ireland%20%20_en.pdf.

European Parliament and of the Council, Directive 95/46/EC on the Protection of individuals with regard to the processing of personal data and on the free movement of such data, 24.10.1995, http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

FAHSI, Par Magda, A divided Europe wants to protect its personal data wanted by the US, Rue 89, 04.03.2008, (çevrimiçi) <http://www.rue89.com/2008/03/04/a-divided-europe-wants-to-protect-its-personal-data-wanted-by-the-us>.

FRIEDMAN, Thomas L., Dünya Düzdür, çev. Levent Cinemre, I. Basım, Boyner Yayınları, İstanbul, Şubat 2006.

Günaydın, R. (2004) SECI Merkezi Görev Dönüş Raporu, Bükreş.

Gül, İbrahim; Alagöz, İsmail; Hildebrand Moritz, “Personal data and Information Exchange in the International Platform, Buchares, 2010

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris, 2002, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html,

OECD, Implementing the OECD Privacy Guidelines in the Electronic Environment, Focus on the Internet, 1997.

OECD, Ministerial Declaration on the Protection of Privacy of Global Networks, 1998, <http://www.oecd.org/dataoecd/39/13/1840065.pdf>,

OECD, Policy Guidance on Online Identity Theft, June 2008. OECD, Privacy Online,

OECD, Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, <http://www.oecd.org/dataoecd/43/28/38770483.pdf>,

Şahin, Cumhur, “Telekomünikasyon Yoluyla İletişimin Denetlenmesi – Yargıtay Kararları Çerçevesinde Bir Değerlendirme”, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C.XI, Sa.1-2, 2007.

Şen, Ersan, Telefon Dinleme - Gizli Soruşturmacı - X Muhbir, Ankara, 2010

United Nations, Guidelines for the Regulation of Computerized Personal Data Files Resolution no: A/RES/45/95, <http://www.un.org/documents/ga/res/45/a45r095.htm>,

US Department of Commerce, Safe Harbor Workbook, http://www.export.gov/safeharbor/sh_workbook.html.

Conseil de l'Europe , l'Europe des ministres de la Justice, 30e Conférence du Conseil de l'Europe des ministres de la Justice (Istanbul, 24-26 novembre 2010) – Rapport du Secrétaire Général, [https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Del/Dec\(2011\)1107/10.1&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383](https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Del/Dec(2011)1107/10.1&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383)

L'audit d'intelligence économique, mettre en place et optimiser un dispositif coordonné d'intelligence collective, Bernard Besson et Jean-Claude Possin, (ISBN 2-10-006699-4), Dunod, 2002,

Modèle d'intelligence économique, AFDIE, Economica, Bernard Besson, Dominique Fonvielle, 2004.

Jean Herveg, (dir.) La protection des données médicales: les défis du XXIe siècle, Anthemis, 2008

Bogdan Manolea, Protectia Datelor cu Caracter Personal, http://www.soros.md/files/publications/documents/Studiu_Protectie%20date%20prsonale.pdf

INTERNET SİTELERİ

www.avrupakonseyi.org.tr

www.conventions.coe.int

<http://ec.europa.eu/>

www.eur-lex.europa.eu

<http://ico.org.uk/>

www.legislation.gov.uk

www.oecdprivacy.org.

www.tbmm.gov.tr