
ERCİYES ÜNİVERSİTESİ
1978
ERCİYES ÜNİVERSİTESİ İLETİŞİM FAKÜLTESİ
2001

akademia

ISSN:1308-3198
Erciyes İletişim Dergisi "akademia" 2014
Cilt (Volume): 3, Sayı (Number): 4, (102-120)

Serpil Karlıdağ (Yrd. Doç. Dr.)
Başkent Üniversitesi Sosyal Bilimler MYO
skarli@baskent.edu.tr

YENİ İLETİŞİM TEKNOLOJİLERİ VE MAHREMİYET: E-BELEDİYELER KİŞİSEL BİLGİLERİ KORUYOR MU?

Özet

Kişilere ait özel bilgilerin kolaylıkla toplanıp üçüncü taraflara aktarılmasını sağlayan yeni iletişim teknolojileri mahremiyetin korunmasında yeni bir mücadele alanı oluşturmuştur. Sosyal medyada ya da internette yapılan işlemler yoluyla elde edilen ve işlenen bilgiler hem ticari kuruluşlar hem de kamu kuruluşları tarafından talep edilmektedir. Özde, kişilerden başka bir deyişle kullanıcılardan toplanan bilgilerin onların bilgisi dışında farklı amaçlarla kullanılması mahremiyet ihlali olarak görülmekte ve yoğun tartışmalara neden olmaktadır. Ancak günümüzde kişilere ait bilgiler belediyeler tarafından da toplamaktadır. Bilgi edinme hakkı dışında, vergi ödemek ve tahsilatlar gibi pek çok hizmeti sağlayan e-belediye sayfaları, isim, soyadı ve iletişim bilgilerinin dışında eğitim durumu, meslek gibi bilgileri de istemekte ancak bu bilgileri koruduğuna dair bir beyanda bulunmamaktadır. Dolayısıyla bu çalışmanın amacı, belediyelerin web sayfalarında elde edilen kişisel bilgilerin korunup korunmadığını araştırmaktır. Bu bağlamda, 16 büyük şehir belediyesi ile onlara bağlı belediyelerin web siteleri incelenmiş ve yapılan içerik analizinde belediyelerin büyük çoğunluğunun bu konuda bir sorumluluk üstlenmediği görülmüştür.

Anahtar sözcükler: mahremiyet, belediyeler, web ortamında içerik analizi

New Communication Technologies and Privacy: Do E-Municipalities Protect Personal Information?

Abstract

The new communication technologies which provide third parties with transmission of private information have created a new challange. Information obtained through social media or transactions made on the internet and subsequently processed is required both by commercial organizations and governmental agencies. In essence, the use of information collected from users without their knowledge and for ulterior motives is seen as a violation of privacy and subject to intense debate. However, today municipalities collect information about individuals. In addition to the service for the right to information, e-municipalities provide people with many services including tax collection and payments. Thence, they ask people certain information such as their education level and occupation besides their name, surname and contact information. However, they do not include privacy statements on their web sites. Therefore, this study aims to investigate whether the information obtained from municipalities' web pages is protected. In this context, the web sites of 16 largest city municipalities and municipal towns connected to them are examined and it was found that the vast majority of the municipalities in the content analysis do not bother to assume any responsibility regarding the issue of individual privacy.

Keywords: privacy, municipalities, content analysis on the web.

Giriş

Gün geçtikçe yaşam pratikleri içinde daha yoğun kullanılan yeni iletişim teknolojileri, vergi ödemekten karşılıklı haberleşmeye, e-ticaretten bilgi edinmeye kadar pek çok işlevi yerine getirirken çeşitli kaygılara da neden olmaktadır. Bu kaygılar, çoğunlukla çevrimiçi işlemlerde para kaybetmek ve sunulan hizmet karşılığında, kullanıcılardan istenen özel yaşama ait kişisel bilgilerin kötü amaçlarla kullanılabileceği konusundadır. Daha önceleri hastanelerin, bankaların, okulların, mağazaların ve diğer kurumların kendi dosyalarında kayıtlı bulunan kişisel bilgilere ulaşmak yorucu, zaman alıcı ve maliyetliydi. Ayrıca, bu bilgilere neden ulaşılmak istendiği konusunda geçerli bir gerekçe belirtmek gerekiyordu. Oysa, günümüzde sayısallaşma ve akıllı ağlar yoluyla kişisel bilgiler kolaylıkla toplanmakta, saklanmakta ve işlenmektedir. İşlenip veri tabanı haline getirilen bu bilgilerin yurt içinde ve yurt dışındaki üçüncü taraflara aktarılması ya da paylaşılması insanları huzursuz etmekte, bazılarını internet üzerinde işlem yapmaktan, sosyal paylaşım sitelerine girmekten alıkoymaktadır. Nitekim medyada sıklıkla kişisel verilerin hem ticari kuruluşlar hem de kamu kuruluşları tarafından talep edildiği ve işlenildiği haberi yer almaktadır. ABD hükümetinin PRISM programıyla 9 teknoloji şirketinin servis sağlayıcılarındaki kişisel bilgilere ulaştığı haberi (Hürriyet, 2013) ile Türkiye'de Milli Eğitim Bakanlığı, PTT, THY ve Tapu Kadastro'daki veri arşivine MİT'in istediği zaman erişebildiği haberi (www.bitdunyasi.com.tr) bu konuda en çok dikkat çekenleri olmuştur.

Çoğu kimse kendi bilgisi dışında kişisel bilgilerinin toplanıp, yayıldığının farkında olmakla birlikte, bu bilgiler üzerinde kontrolünün olmadığının da bilincindedir. Daha açık bir ifadeyle, kendisi hakkında hangi bilgilerin toplandığı ve nerelerde yayıldığı hakkında bir fikri bulunmamakta, bulunsa bile, günde milyonlarca kişisel bilginin işlem gördüğü bir ortamda bu bilgilere erişememektedir (Hough, 2009, 411-412). Kişisel verilerin korunmasıyla ilgili yapılan bir çalışma, halkın kamu sektörüne özel sektörden daha fazla güveniyor olduğunu gösterse de, çalışma daha ayrıntılı ele alındığında ve gözetim açısından bakıldığında, bu güvenin yerini belirsizliğe hatta güvensizliğe bıraktığı görülmektedir (Hallinan, Friedewald ve McCarthy, 2012, 263). Bununla birlikte, kullanıcılar bazı hizmetleri alabilmek için kişisel bilgilerin verilmesini adeta modern yaşamın bir gerekliliği olarak görmektedir. Böylece, bir taraftan mahremiyete büyük önem verilirken diğer taraftan toplumsal dışlanma yaşamamak veya sunulan hizmetlerden yoksun kalmamak için kişisel bilgilerin toplanması kabul edilmektedir. Bir anlamda araştırmacıların da ifade ettiği gibi "bilişsel uyumsuzluk" durumu olmaktadır (Hallinan, Friedewald ve McCarthy, 2012, 264). Sweeney'de doğum tarihi ve yeri verildiğinde kolaylıkla sosyal güvenlik numarasına erişilebildiğini ve bunun da kişiyi kimlik hırsızlığı için aday konumuna getirdiğini belirtmektedir (Hough, 2009, 412). Kullanıcılar kendilerini korumak için bazen kendileriyle ilgili yanlış bilgiler vermekte bazen de birden fazla e-posta adresi kullanmaktadırlar (Pollach, 2007).

Kullanıcıların kaygılarını gidermek için çoğu web sitesi "güvenlik" başlığı altında, kredi kartı ve şifre konularında kişisel bilgilerin nasıl güvenli bir biçimde kullanılacağı konusunda bilgi vermekte, kendi aldıkları önlemleri belirtmektedir. Bazı sitelerde "gizlilik" başlığı altında kişilerin bilgilerinin saklanacağı, kişinin kendi izni olmadan bu bilgilerin işlenmeyeceği ve üçüncü taraflara aktarılmayacağı belirtilmektedir. Bu tür mahremiyet beyanları üzerinde çalışmalar yapan Pollach (2007, 104), bu beyanların müşterilerin kişisel verilerinin sorumlu bir şekilde kullanılacağı konusunda ikna etmeye yaradığı gibi, ileride olabilecek davaları önlemek amacıyla da kullanıldığını ortaya koymuştur.

Kişisel veriler geçmişte de önemli olmuştur ancak post- Fordist üretim tarzı ile bu üretim tarzı içerisinde örgütlenen yeni iletişim teknolojileri, kişisel verilerin değişim değerini artırarak büyük bir piyasa haline gelmesine yol açmıştır (Acquisti,2010:8). Bireyler için kullanım değerine sahip olan kişisel veriler, işletmeler açısından ekonomik gözetim yoluyla sahip oldukları varlıklardır ve sermaye birikimine katkıda bulunmaktadır. Toplanan verilerin amaçları dışında kullanılabilmesi ve bireylerin, tüketicilerin günlük yaşamlarının onların bilgisi dışında izlenebilmesi mahremiyetleriyle ilgili kaygıları artırırken, bu verilerin korunmasını da önemli

kılmaktadır. Dolayısıyla, bu çalışmanın amacı, kişisel bilgilerin gittikçe değer kazanması kadar, korunmasının da aynı ölçüde önemli olduğu düşüncesine dayanarak Türkiye'deki belediyelerin kişisel verileri koruyor mu sorusunu araştırarak akademik bilgi birikimine katkıda bulunmaktır. Kamu ve özel kuruluşların kişisel verileri nasıl koruduğu hakkında pek çok çalışma yapılmış olmakla birlikte belediyeler konusunda yapılan çalışmaların azlığı bu çalışmanın önemini ortaya koymaktadır.

Bu çalışmada, 16 büyükşehir belediyesi ile onlara bağlı ilçe belediyelerinin web sayfalarına bakılmış ve kullanıcılara kişisel bilgilerinin korunduğuna dair herhangi bir güvencenin verilip verilmediği araştırılmıştır. Bir anlamda, vatandaşlara en yakın yerlerde en uygun hizmetleri sunmakla yükümlü olan belediyeler sundukları çeşitli hizmetler karşılığında elde ettikleri kişisel bilgileri koruduklarına dair bir beyanda bulunuyorlar mı, eğer bulunuyorlarsa bunu açıkça belirtiyorlar mı sorusuna yanıt aranmıştır.

MAHREMİYET, KİŞİSEL VERİLER VE KORUMA GEREKLİLİĞİ

Tek bir tanımı olmayan mahremiyet için çeşitli açıklamalar yapılmaktadır. Warren ve Brandies'e göre (1890), mahremiyet, "yalnız bırakılma hakkı" olurken, Westin'e göre, kişisel enformasyonu üçüncü taraflara açıklamama konusundaki biricik haktır (Paine, Reips, Stieger ve Buchanan, 2007, 526). İnsan mahremiyetin ne olduğunu en iyi onu kaybettiğinde ya da ihlal edildiğinde anlamaktadır (Adrian, 2013, 48). Avrupa hukuku mahremiyeti; insanın kendisine ait evi, özel yaşamı, aile hayatı, bedensel ve ruhsal bütünlüğü, onuru, şöhreti ve şahsına ait özel bilgileri kapsayan ve devlet müdahalesinin olmadığı bir alan olarak tanımlamaktadır. ABD'de ise, hükümetin herhangi bir gerekçesi olmadan el koyamayacağı ya da araştırma yapamayacağı bir kişisel alan olarak tanımlanırken, anayasal hak olarak belirlenmiştir (Kuner, 2009, 309). Bir anlamda mahremiyet, kişiyi çevreleyen fiziksel alanın dokunulmazlığına herhangi bir dış müdahalenin olmamasını, özerk karar vermeyi ve kişisel bilgiler üzerinde denetim sahibi olmayı ifade etmektedir (Bennett, 1992, 13). Hobbes ve Locke gibi ampirist ve liberal felsefi düşünürler açısından bakıldığında, mahremiyet, öncelikle birey ve toplum arasındaki ilişkinin doğasından kaynaklanan toplumsal ya da insani bir haktır. Nitekim İnsan Hakları Evrensel Bildirgesi'nin 12. maddesi uyarınca bir insan hakkı olarak kabul edilmektedir (Adrian, 2013,50). Medeni ve Siyasi Haklar Uluslararası Sözleşmesi'nin 17.maddesi de mahremiyeti insan hakkı olarak görmektedir. Her iki uluslararası metinde de benzer ifade ve kelimeler kullanılarak, kimsenin mahremiyetine, ailesine, evine ya da haberleşmesine keyfi bir müdahalede bulunulamayacağı gibi, onuruna ve şöhretine de bir saldırı yapılamayacağı açıkça belirtilmiştir (Adrian, 2013:50).

Bütün bunlara karşın, mahremiyet mutlak bir hak olmayıp, içinde bulunduğu yere ve zamana göre farklılık göstermektedir. Kamu yararı, toplumun gereksinimleri ya da diğer kişisel haklar mahremiyet hakkından önce gelebilmektedir. Mahremiyetin korunması karmaşık bir konu olurken, yasal olduğu kadar ekonomik ve toplumsal boyutlar da içermektedir. Kâr yapmak isteyen şirketler müşterilerinin bilgilerini toplayıp, işlerken ve üçüncü taraflara aktarırken onların haklarını ihlal ettiklerini düşünmemektedirler. Mahremiyet teknoloji ile de dinamik bir ilişki içerisinde bulunmaktadır. Yeni iletişim teknolojilerinin ortaya çıkıp gelişmesi mahremiyet için yeni mücadele alanları oluşturmuştur. Kişisel verilerin korunması bu alanların başında gelmektedir. Modern toplumlarda önemli işlevi olan kişisel verilerin, kişisel mahremiyet hakkı ile korunması talebiyle, yönetimlerin ve karar vericilerin enformasyon gereksinimi arasındaki gerilim günümüzdeki temel sorunlardan birisini oluşturmaktadır (Bennett, 1992,18). Aslında kişilerle ilgili bilgilerin kayda geçirilmesi medeniyetlerin kendisi kadar eskidir. Öyle ki, Akdeniz, Ortadoğu, Uzakdoğu ve Güney Amerika'daki antik medeniyetlere bakıldığında kişisel kayıt siteminin olduğu görülmektedir. Batı'da da modern devletin gelişmesi, yönetimin merkezileşmesi ve vergilerin konulması vatandaş devlet ilişkisine kayıt sistemini getirmiştir. Üç yüzyılı aşkın süredir devlet aygıtının genişleyip, güçlenmesi ve kurumsallaşmasıyla daha resmi, ayrımcı ve karmaşık bir kayıt tutma sistemi geliştirilmiştir (Bennett, 1992,18).

Günümüzde yapılan araştırmalar, kişilerin özellikle çevrimiçi eylemleri sırasında kaygılarının daha çok arttığını ortaya koymaktadır. Jupiter (2002) Amerikan tüketicilerinin %70'inin çevrimiçi kaygılara sahip olduğunu belirtirken, Harris (2004), anketine yanıt verenlerin %65'inin çevrimiçi kaygılar nedeniyle e-ticaret sitesine üye olmadıklarını belirtmiştir (C.Paine ve ark.,2007:527). Yine PC world'ün 2003 yılındaki araştırması, 1500 internet kullanıcısının %88'inin web siteleriyle e-posta adreslerini paylaşmaktan çekindiklerini ve %91'inin de web sayfalarını kullanırken izlendikleri endişesi taşıdıklarını ortaya koymuştur (C.Paine ve ark.,2007, 527). Hükümetlerin kullandıkları gözetim teknolojilerine ve uygulamalarına karşı bireylerin duyduğu güven de kritik düzeylerdedir. Ponemen Enstitüsü'nün yaptığı son araştırmalarda, 2005 yılında ABD hükümetine olan %52 güvenin, 2010 yılında %38'e düştüğü görülmektedir. İngiltere'de de 2008 yılında Joseph Rowntree Vakfı adına yapılan bir araştırma da, kişilerin %65'inin kendileriyle ilgili bilgilerin hükümet tarafından tutulmasından kaygılandıklarını ve 2006 yılında %53 oranında olan bu kaygının arttığını ortaya koymuştur (Hallinan, Friedewald, McCarthy, 2012:267). London School of Economics tarafından nüfus cüzdanlarına ilişkin yapılan bir araştırma da vatandaşların, hükümetlerin kendileriyle ilgili verileri tutmaları ve kullanmaları konusunda güvenlerinin düşük olduğu sonucuna varmıştır (Hallinan, Friedewald, McCarthy, 2012, 267).

Kişisel verilerin korunmasıyla ilgili düzenlemeler, kişilerin, kendilerini belirleyen özelliklerle ilgili verilerin korunmasını ve bu verilerin işlenmesiyle ilgili hak sahibi olmalarını amaçlamaktadır. Bazı devletler mahremiyet hakkını çok uzun süredir tanımakla birlikte, veri koruma yasasına sahip değildirler. Belirlenmiş veya kimliği saptanmış kişilerle ilgili enformasyon olarak tanımlanan kişisel veriler, Avrupa hukuku tarafından kendiliğinden önemli bulunmakta ve mülkiyetçi bir tonda insan hakları olarak kabul edilmektedir (Birnhack, 2008, 510). Kişisel verilerle ilgili kurallar yeni bir veri koruma kategorisi oluştururken, kaynağını mahremiyet ve insan onuru fikrinden almaktadır. Temelde, evlenmek, çocuk sahibi olmak, eğitim gibi çeşitli kararları içeren mahremiyet, veri korumasına göre daha geniş ve bağımsız bir kavram olmakla birlikte, bu iki kavram birbiriyle örtüşmektedir. Bir anlamda, "mahremiyet ve kişisel veriler aynı olmamakla birlikte ikiz kavramlardır" (Kuner, 2009, 309-308). Veri koruması da mahremiyet yasasından farklı ama ona bağımlı yeni bir yasal alan olarak çıkmış ve yeni iletişim teknolojileri ile küreselleşme sürecindeki gelişmeleri takip etmiştir (Birnhack, 2008, 511). Dolayısıyla, kişi toplum içerisinde bazı etkinliklerde bulunurken ve görevlerini yerine getirirken sağlamış olduğu bilgilerin gereksiz ya da onurunu zedeleyecek biçimde kullanılmaması beklentisi içindedir (Adrian, 2013, 49).

Kişisel Verilerin Korunması Konusundaki Düzenlemeler

Kişisel verilerin korunması için ilk kez, 1970'lerde benzer ilkeleri içeren çeşitli yasa ve önerilerin bir araya gelmesiyle, Adil Enformasyon Uygulamaları (Fair Information Practices) oluşturulmuş ve somut kurallar getirilmiştir. Adil Enformasyon Uygulamaları'na göre, kişisel veriler amacına uygun olarak toplanmalı, güncel ve doğru olmalı, amacına uygun süre içinde amacına uygun olarak kullanılmalı, yasal olmayan erişime karşı güvenliği sağlanmalı ve yasal olmayan yollarla toplanan verilerin silinmesi için veri sahibine gerekli hak verilmelidir. Bu temel ilkelerden sonra, hem veri öznelerinin çıkarını koruyan hem de uluslararası veri aktarımını sağlayan rehber ilkeler 1980 yılında OECD tarafından benimsenirken, 1981 yılında Avrupa Konseyi tarafından bir Sözleşme ile konuya dikkat çekilmiştir. Daha sonra Birleşmiş Milletler de bu konuda bir düzenleme oluşturmuştur. AB'nin alana girmesiyle 1995 yılında veri koruması düzenlenmiş ve kurumsallaşmıştır. Gelişen teknolojiyle birlikte kolaylıkla işlenen veriler karşısında, Avrupa vatandaşlarının mahremiyetini koruyabilmek için oluşturulan 95/46/EC sayılı Direktif'ten sonra internet kullanıcıları için daha fazla koruma içeren 2002/58/EC sayılı Direktif de uygulamaya konulmuştur (Beldad, De Jong ve Steehouder, 2009, 559). AB Veri Koruma Direktifi, kendisinden önce OECD, Avrupa Konseyi ve Birleşmiş Milletler tarafından oluşturulan ve bağlayıcı olmayan düzenlemelere göre daha etkin olmuştur (Birnhack, 2008, 511). Direktif, verilerin ırksal köken, siyasal inanç, sağlık veya cinsiyetle ilişkili biçimde sınıflandırılarak

işlenmesini yasaklamaktadır (Madde 8). Yine Direktif'e göre, verileri toplayanların ilgili kişileri (data subject)[1] bu konuda bilgilendirmesi gerekirken (Madde 10), ilgili kişilerin kendi verilerine erişme (Madde 12) ve işlenmesine karşı çıkma (Madde 14) hakları da bulunmaktadır.

E-mahremiyet Direktifi olarak da anılan Direktif 2002/58/EC, 2009 yılında gözden geçirilmiş ve bazı düzeltmeler yapılmış ve özellikle çerezler konusundaki tehlikeye dikkat çekilmiştir. Çerezler çoğu web sayfası tarafından kullanılmakta ve kullanıcının ağdaki gezintilerini gizlice kaydetmektedir. Öyle ki, kullanıcı hangi siteleri ziyaret etmiş, her bir web sayfasında ne kadar süre harcamış ve sitenin diğer kısımlarda ne kadar gezinmiş olduğu bilgisini toplamakta ve kullanıcıyla ilgili bir profil oluşturmaktadır (Adrian, 2013, 52-53). Çerezler başka bir araçla kullanılmadığı takdirde, kullanıcının kimliğine herhangi bir atıfta bulunmadan bilgileri toplamaktadır. Ancak çerezler başka bir programla bağlantılı çalıştığında ya da çerezlerin olduğu siteye kullanıcı adı ve diğer özel bilgiler verildiğinde, kimlikler belirlenmektedir (Adrian, 2013, 53). Dolayısıyla, 2009 yılındaki düzeltmeler ile getirilen kurallar, kullanıcının bilgisayarına gönderilen dosyalar yoluyla yerleştirilen çerezler için kullanıcının onayını zorunlu kılmıştır. Ancak bu kurallar tüm çerezlere uygulanmamıştır. Çünkü alışveriş işlemlerinde kullanılan "sepete ekle" gibi kısımlardaki çerezlerin, işlemin tamamlanması açısından bulunması gerekmektedir (McStay, 2012, 9).

Kişisel verilerin korunması hakkında kapsamlı kurallar getiren AB Veri Koruma Direktifi sadece AB'ye üye ülkeleri değil diğer ülkeleri de etkilemiştir. Türkiye'de de, Veri Koruma Kanunu Taslağı oluşturulurken AB Direktifi temel alınmış ve pek çok maddesi ona göre oluşturulmuştur. Ancak çok fazla istisnaya yer verilmiştir. Hala yasalaşamayan Veri Koruma Kanunu Taslağı ile ilgili eleştiriler bu istisnalar yönünde olurken, veri koruma hakkında yetkili ve idari yaptırım gücüne sahip olacak **"Veri Koruma Kurulu"nun** özerk mi yoksa yürütmeye mi bağlı olması konusunda da anlaşmaya varılamaması nedeniyle yasanın çıkmadığı düşünülmektedir (İlkiz, Umut Vakfı). Bu yasanın çıkmaması nedeniyle kişisel verilerin korunması halen Anayasa ve Medeni Hukukta belirtilen maddeler doğrultusunda yapılmaktadır. Telekomünikasyon alanındaki verilerin korunması için ayrıca Telekomünikasyon Alanında Elektronik Haberleşme Kanunu kabul edilmiştir. Türkiye Avrupa Siber Suçlar Sözleşmesi'ni de imzalamıştır. Ancak bunların hiç birisi münferit bir Veri Koruma Yasası'nın gerekliliğini ve iç hukukun da ona uyarlanması zorunluluğunu ortadan kaldırmamaktadır (Yaman Akdeniz, 2010)

ABD'de ise, kişisel veri koruması ve mahremiyetle ilgili sorunlara karşı kapsamlı bir yasa bulunmamakta, var olan yasalar da parçalı ve yetersiz bulunmaktadır (Stradford-Stradford, 1998, 17). Nitekim, Amerikan Sivil Özgürlükler Derneği danışmanı Chris Calabrese, "elektronik mahremiyetteki değişikliklerin parçalı olamayacağından" söz ederken ve Video Mahremiyet Yasasındaki düzeltmelere karşı "gerçek reform" talebinde bulunurken (Barclay, C.A.,2013, 359) temelde bu soruna değinmektedir. 2010 yılında Wall Street Journal'ın "Ne biliyorlar" başlığı ile başlatmış olduğu araştırma makaleleri, mahremiyetle ilgili verilerin korunmasına ilişkin kapsamlı bir yasanın çıkarılmasının önemini ortaya koymuştur. Çünkü, bu makalelerde, en bilinen 50 web sitesinin kullanıcıların bilgisayarına 60'dan fazla izleme çerezi yerleştirdiği ve bazılarının ortalama çerezlerden daha akıllı olarak, kullanıcının yerini, yaşını, gelirini ve sağlık koşullarını bile kaydettiğini belirtmiştir (Barclay, C.A., 2013:359-360). Başkan Obama yönetiminin daha kapsamlı bir mahremiyet koruma yasası için verdiği destek sonucunda bireylerin kendi bilgilerine erişerek kimliklerini yönetmeleri ve doğru olmayan enformasyonla mücadele edebilmeleri konusunda yeni tasarılar oluşturulmuştur. Ancak bu tasarılar yasalaşmamış ve Kongre yine daha parçalı mahremiyet yasası yaklaşımına dönmüştür (Barclay, C.A.,2013, 366).

Mahremiyet Beyanları

Daha önce de belirtildiği üzere, mahremiyetle ilgili kaygılar yeni olmamakla birlikte internet etkinliklerinin çeşitlenmesi ve kullanımının yaygınlaşması bu kaygıları daha çok artırmıştır.

[1] Kişisel verilerin Korunması Kanunu Tasarısı'nın 3. maddesinde veri öznesi (data subject) ilgili kişi olarak belirtilmiştir. Veri kütüğü sahibi ise, verilerin saklanması ve kullanılmasını (işlenmesini) kontrol eden ve bundan sorumlu olan gerçek ve tüzel kişilerdir (www.tbmm.gov.tr)

Kaybolan dizüstü bilgisayarlardaki bilgiler ya da hassas enformasyon sızıntıları medyada sıklıkla yer alırken, veri ihlallerine karşı yeni düzenlemeler yapılmaktadır. Güvenlik dondurma yasaları da, tüketicilerin kredi dosyalarını askıya alarak ve çalınan enformasyonlar yoluyla yeni hesapların açılmasını önlemektedir. Ancak tüm bu önlemler tüketicilerin kaygılarını azaltmamıştır. Nitekim 2008 yılında yapılan bir araştırma, daha önce de belirtildiği gibi, kişilerin özellikle web siteleri yoluyla toplanan kişisel bilgileri karşısında endişe duyduğunu ve bilgilerinin ne zaman izlendiğini bilmek ve kontrol etmek istediğini ortaya koymuştur (Anton, Earp ve Young, 2009).

Mahremiyetle ilgili kaygılar, yasal düzenlemelerin yanı sıra teknoloji, 3. tarafların teminatı ve mahremiyet beyanları gibi mekanizmaların kullanılmasını teşvik etmiştir (Arcand vd., 2007). Yapılan çalışmalar, kullanıcıların işlem yaptıkları web sitesine güven duymalarında çevrimiçi mahremiyet beyanlarının önemli bir ölçüt olduğunu göstermiştir (Earp vd, 2005; Arcand vd.,2007). İnternetin mahremiyet politikası örgütün veri toplama, kullanma ve bu verileri paylaşma ya da üçüncü taraflara aktarma uygulamalarını tanımlamaktadır. Eğer bu mahremiyet politikaları açıkça belirtilirse kullanıcı bu siteye daha çok güven duymaktadır (Han ve Maclaunin, 2002).

Mahremiyetle ilgili beyanlar çeşitli biçimlerde olabilmektedir. Bir kısmı kullanıcının bilgisini kullanmak için onun iznini talep ederken (opt-in), diğer bir kısmı da kullanıcıya, onun kişisel bilgileriyle ne gibi uygulamalar yapıldığı konusunda bilgi vermektedir (opt-out). Bir anlamda, ilkinde kullanıcıya daha çok kontrol gücü sağlanıp, bilgisinin nasıl kullanılacağı ve paylaşılacağı hakkında yetki verilirken, ikincisinde kullanıcı sadece haberdar edilmektedir (Arcand vd., 2007). Kullanıcının iznini talep eden opt-in biçimindeki mahremiyet beyanları, kontrol ve güven açısından kullanıcının pozitif algısını artırmaktadır. Ancak bu beyanların yeri de önemli olup, kullanıcının açıkça görebileceği bir yerde olmalıdır.

Earp (2005, 235) ve arkadaşları tarafından yapılan çalışma, mahremiyet politikaları ile kullanıcının beklentileri arasında farklılık olduğunu ortaya koymuştur. Kullanıcılar daha çok toplanan bilgilerin nasıl kullanıldığı, nereye aktarıldığı ve nasıl saklandığı konusuna odaklanırken, mahremiyet beyanları toplanan verilerin güvenliği ve korumasına vurgu yapmaktadır. Web sitesi sahibi kuruluşların, kullanıcıların kaygılarını göz önünde bulunduracak biçimde mahremiyet beyanlarını düzenlemeleri her iki taraf açısından da yararlı olacaktır. Kullanıcıların verilerinin nasıl paylaşılacağı veya ödünç verileceği, özellikle de hassas olarak nitelenen verilerin nasıl kullanılacağı, verilerin nasıl muhafaza edileceğinin belirtilmesi gerekmektedir. Bir anlamda, kuruluşların da bu verilerin saklanmasında ve aktarılmasında benzer kaygılara sahip olduklarını mahremiyet beyanlarında ifade etmeleri yararlı görülmektedir (Earp, 2005, 235). Pollach (2007), ABD'deki çevrimiçi politikaların kullanıcının kaygılarını azaltma yönünde tasarlanmadığını, onun yerine kuruluşları sağlık, finans ve çocukların özel yaşamlarını korumak için çıkartılmış bazı düzenlemelere karşı dava açılmaktan korumak için yapıldığını belirtmiştir. Pollach (2007) ayrıca, web sitelerinin ellerinde bulundurdukları verilerle ne gibi uygulamalar yaptıkları konusunda kullanıcılara bilgi vermelerinin güven oluşturacağını ve bu güvenle kullanıcının siteden alışveriş yapacağını, siteyi tekrar ziyaret edeceğini ve başkalarına tavsiye edeceğini de vurgulamıştır. Bu bağlamda web sitelerinde ya da çevrimiçi işlemlerdeki mahremiyet beyanları kullanıcıyı kişisel bilgilerini açıklama konusunda teşvik etmektedir.

Ancak kullanıcının bu beyanları görüp, okuması ve olumlu izlenimde bulunması gerekmektedir. Kullanıcının algısı ne kadar olumlu olursa, güveni de o kadar olmaktadır. Bir başka ifadeyle, bu beyanlar mahremiyet sorunlarıyla ilgili önemli işlevde bulunmaktadır (Milne ve Culnan, 2004). Onun için de bu beyanlardaki içerik ve dil önemli olmaktadır. Kullanıcı, kullanılan dili hukuki ya da karmaşık bulduğunda da okumamaktadır. Verilen bilginin niteliği de tatmin edici olmalıdır. Toplanan verilerin saklanması ve paylaşılması konusunda yeterli bilgilerin verilmemesi kullanıcıyı çelişkide bırakmaktadır. Bilgiler gerçekte kullanılmamakta mıdır yoksa kasıtlı olarak belirtilmemekte midir (Pollach, 2007) gibi kullanıcıyı tedirgin edecek sorular yerine onları rahatlatacak düzeyde bilgilerin görünür yerde olması uygun bir uygulama olacaktır.

Yöntem

Web ortamının çok büyük kolaylıklar sunması onun pek çok alanda kullanılmasına yol açmıştır. Nitekim diğer kamu ve özel kuruluşları gibi belediyeler de web yoluyla sağlanan olanaklardan yararlanmaktadırlar. Yöreyi ve sağlanan hizmetleri tanıtmanın yanı sıra yöre sakinleriyle karşılıklı etkileşim içerisinde bulunmaktadırlar.

Web sitelerinin yoğun kullanılması bu sitelerle ilgili araştırma yapılmasını da artırmaktadır. Kullanılan araştırma yöntemlerinden biri de içerik analizidir. İçerik analizi, yeni iletişim teknolojilerinden önce, gazete, radyo, televizyon, sinema gibi geleneksel medyadaki her türlü metinsel, görsel, işitsel malzemeye uygulanırken günümüzde web ortamındaki içerikler için de yaygın şekilde kullanılmaktadır. İçerik analizinin özellikle büyük miktardaki veriyle başa çıkabilmesi, ona web analizi konusunda açık bir üstünlük sağlamıştır (Krippendorff, 1980).

Ancak bazı zorluklara neden olmaktadır. Öncelikle statik bir araştırma tekniği olan içerik analizinin dinamik nitelikteki bir iletişim ortamı olan web ortamında kullanılması bu zorlukların başında gelmektedir (Mc Millan, 2000, 80). Nitekim sitelere bazen erişilemezken bazen de içerik değişiklikleriyle karşılaşılabilmektedir. Haluk Geray (2004, 139)'a göre, bir içerik analizinde öncelikle analiz biriminin saptanması ve amaca uygun olarak kavramların tanımlanması gerekmektedir. Kavramların çok geniş ya da dar biçimde tanımlanması sorunlara yol açabileceği için birbirini dışlayan kategorilerin oluşturulması gerekmektedir. Genellikle araştırma tüm araştırma evreni üzerinde olmayacağı için örneklem seçilmesi zorunlu olmaktadır.

Çalışmanın araştırma sorusu, belediyelerin kullanıcılara onların kişisel bilgilerini koruduklarına dair herhangi bir mahremiyet bildiriminde bulunup bulunmadıklarıdır. Eğer bulunuyorlarsa bu bildirim sitenin görünür bir yerinde ve açıkça yer almakta mıdır? Çalışmanın ana kitlesi web sayfası kullanan belediyeler olurken örneklem olarak 16 büyükşehir belediyesi ile onlara bağlı 336 ilçe belediyesinin web siteleri ele alınmıştır. Öncelikle Türkiye nüfusunun anlamlı bölümünü oluşturan ve en fazla kullanıcı kitlesine hizmet veren 3 büyük şehrin Büyükşehir belediyeleri ile onlara bağlı belediyelerin incelenmesiyle, analizde ele alınacak ölçütler geliştirilmiştir. Bu ölçütlerin geliştirilmesinde, AB Direktifi'nden uyarlanan Veri Koruma Kanunu Tasarısı ile daha önce Hollanda'da Ardion D. Beldad, Menno De Jong ve Michael F. Steehouder (2009) tarafından belediyelerle ilgili yapılan bir çalışmadan yararlanılmıştır. Araştırmada kullanılan ölçüm birimi mahremiyetle ilgili bir ifade, uyarı ya da bildirimin olup olmamasıdır. Mahremiyetle ilgili bu bildirim güvenlikle ilgili ifadelerden ayrı tutulmakla birlikte, güvenlik uyarılarının içindeki mahremiyetle ilgili uyarılar da incelemeye tabi tutulmuştur. Dolayısıyla, belediyelerin web siteleri, mahremiyetle ilgili beyanlar, güvenlikle ilgili duyurular ve bunlardan hiçbirisine sahip olmayanlar biçiminde kategorilere ayrılmıştır.

Çalışmada, amacı daha kapsamlı tanımlayan mahremiyet kavramı kullanılmış olmakla birlikte, belediyelerin ve konuya ilişkin olarak diğer tüm kurumların, yasaların ve düzenlemelerin mahremiyet yerine gizlilik kavramını kullanmış olmaları nedeniyle, yapılan alıntılarda ve tablolarda söz konusu kavram mahremiyet/gizlilik olarak kullanılmıştır.

Bulgular ve Analiz

16 büyük şehir belediyesi ve onlara bağlı ilçe belediyeleri ile toplam 336 belediyenin web sitelerine bakıldığında, 26 tanesinin açılmadığı, ya da kendilerine ait resmi web sitelerinin olmadığı ve yerelnet üzerinden bilgi verildiği görülmektedir. Bu nedenle 310 belediyenin web sitesi 8 kategoride ve mahremiyet açısından aşağıda belirtilen ölçütler bağlamında analiz edilmiştir (EK'te kategorilere göre belediyelerin listesi görülmektedir. 26 tane açılmayan, ya da kendilerine ait web sitesi olmayan belediyeler bu listede 9. kategori olarak yer almıştır):

5.1.Mahremiyetle ilgili herhangi bir bildiri ya da beyanda bulunmakta mıdır?

Belediyeler çok çeşitli başlıklar altında kişisel verileri toplamaktadırlar. Genelde, web sitesi yoluyla ödeme ve interaktif işlemler yapmak isteyen kişi, kendi güvenliği için şifre almak

ve pek çok soruya yanıt vermek zorunda kalmaktadır. Ancak mavi masa, beyaz masa, bilgi edinme, şikayet ve öneriler, sağlık formu, mezarlık bilgi sistemi ve ruhsatsız kazı ihbarı için de çok ayrıntılı kişisel bilgiler istenmektedir. Öyle ki ad, soyad, TC kimlik numarasının dışında pasaport, uyruk, cinsiyet, öğrenim durumu, meslek hatta kan grubu dahi sorulmaktadır.

Bu toplanan bilgilerin mahremiyetinin korunduğuna dair herhangi bir beyan ya da bildiri bulunmakta mıdır sorusu ile 310 belediyenin web sayfaları incelendiğinde yapılan tespitler şöyledir:

Tablo 1. Belediyelerin web sayfalarında mahremiyete dair beyanlar/bildiriler açıklaması yapılmıştır.

Mahremiyetle/Gizlilikle ilgili bildiriler/uyarılar	- Web sayfasında etkin gizlilik politikası/gizlilik ilkesi bulunan belediyeler	7	**29**
	- Gizlilik/mahremiyet ilkesi bulunmakla birlikte web sayfası açılmayan ya da boş çıkan belediyeler	6	
	- Mahremiyetle ilgili bilgi veren ancak taahhütte bulunmayan belediyeler	13	
	- Başvurunun gizli tutulup tutulmayacağını soran belediyeler	2	
	- İstek-şikâyet formunda; şikâyetin gizliliğini soran belediyeler	1	
Güvenlikle ilgili sayfalarında mahremiyet bildirimine yer veren belediyeler			**15**
Sadece güvenlikle ilgili bildirimde/uyarıda bulunan belediyeler			**95**
Ne mahremiyet/gizlilik ne de güvenlik uyarısında bulunan belediyeler			**171**
TOPLAM			**310**

Görüldüğü gibi sadece 7 belediyede (2'si büyükşehir belediyesi) kişisel verilerin mahremiyetinin korunacağına dair etkin gizlilik politikası beyanına yer verilmiştir. Bu belediyeler ; İstanbul Büyükşehir, Kartal, Üsküdar, Tarsus, Muratpaşa, Bursa Büyükşehir ve Aliağa belediyeleridir. Bunlardan, İstanbul Büyükşehir belediyesi'nin web sayfasının en altındaki "Site Kullanım Koşulları" tıklandığında, 11 maddelik web sitesi gizlilik politikası karşımıza çıkmaktadır. 10.maddesinde, "Büyükşehir Belediyesi internet sitesi üzerinden verilen kişisel bilgilerin hiçbir şekilde 3.şahıslarla paylaşılmayacağı ve ticari amaçlarla kullanılmayacağı" belirtilirken, 11.maddesinde bu siteye girmekle veya kullanmakla gizlilik politikası şartlarının kullanıcı tarafından kabul edildiği vurgulanmıştır. Üsküdar Belediyesi'nin web sitesinin altına koymuş olduğu "Gizlilik Sözleşmesi" de aynı İstanbul Büyükşehir Belediyesi'ndeki metin gibidir. Bursa Büyükşehir Belediyesinin altındaki "site kullanım şartları" tıklandığında, "Web Sayfası Gizlilik Politikası" başlığı ile İstanbul Büyükşehir Belediyesi ve Üsküdar Belediyesindeki maddelerin aynısı ortaya çıkmaktadır. Antalya'nın Muratpaşa Belediyesi de web sayfasının altına koymuş olduğu "Gizlilik Politikası" ile aynı metne ve aynı beyanlara sahiptir ancak çerezlerle ilgili 8.maddeyi kaldırmıştır. Kartal Belediyesi, web sayfasının altına iletişim/kullanım şartları/ gizlilik başlıklarını koymuş ve gizlilik başlığı tıklandığında, "ziyaretçilerin formlar aracılığı ile sundukları kişisel verilerinin üçüncü kişilere satılamayacağı, kiralanamayacağı ve hiçbir şekilde kullandırılmayacağı" belirtilmektedir. Ayrıca, kullanıcının sitedeki bağlantılar yoluyla gideceği diğer sitelerde aynı koşulların garanti edilememesi nedeniyle dikkatli olunması konusunda uyarıda bulunulmuş ve gizlilik politikasıyla ilgili görüş ve önerilere açık oldukları bildirilmiştir.

Tarsus Belediyesinin web sayfasının altında iletişim/kullanım şartları/gizlilik ibaresi yer almakta ve gizlilik kısmı tıklandığında aynı İstanbul Kartal Belediyesi'nde olduğu gibi, ziyaretçilerin formlar aracılığı ile sundukları kişisel bilgilerin üçüncü taraflara hiçbir şekilde aktarılmayacağı ve kullandırılmayacağı, sitedeki bağlantılar aracılığı ile gidilecek diğer siteler konusunda uyarılar ve gizlilik politikasıyla ilgili görüş ve öneriler için kendilerine başvurulabileceği belirtilmektedir.

Aliağa Belediyesi'nin sayfanın altına koymuş olduğu "Gizlilik İlkeleri/Kullanım Şartları" tıklandığında, gizlilik ilkelerinin aynen Kartal ve Tarsus belediyelerindeki gibi olduğu görülmektedir. Ancak o sitelerde bitiş cümlesi olarak yer alan ve kullanıcıların "Gizlilik Politikası'yla ilgili görüş ve önerileri için" bu belediyelere başvuru önerisi Aliağa Belediyesinde bulunmamaktadır. Ayrıca kullanım şartlarında, " internet üzerinden gönderilen yorum, öneri, fikir, grafik, vb dahil her türlü bilginin, herhangi bir ödeme yapılmaksızın belediyenin mülkiyetine geçeceği" ve belediyenin bu bilgileri sınırsız olarak kullanabileceği gibi bu bilgileri korumakla yükümlü olmadığı da açıkça belirtilmiştir. 18 yaşından küçük olanların sundukları bilgilerden de yine belediyenin sorumlu olmadığı bildirilmiştir.

Adana ve Ceyhan Belediyeleri'nde bulunan e-belediye sayfalarının da altında gizlilik ilkesi yer almakta, ancak tıklandığında açılmamaktadır. Benzer biçimde, Keleş (Bursa) Belediyesi'nin, sayfanın altına koymuş olduğu "Yasal haklar ve kullanım sözleşmesi" de açılmamaktadır. Ancak üyelik kaydı için 14 maddelik kuralları içeren listenin okunup kabul edilmesinden sonra üyelik formu kişisel bilgileri toplamakta ve kayıtlı kullanıcının yararlanabileceği başlıkları sıraladıktan sonra "kişisel bilgilerin gizli tutulacağını" belirtmektedir. Mudanya belediyesinin yeni kullanıcı kaydı kısmında da "kişisel bilgileriniz kesinlikle başkalarına verilmez veya satılmaz" denmiştir. Ayrıca, "Gizlilik Politikası" da sitede yer almış ancak tıklandığında "etkisiz" olarak çıkmıştır. Aynı şekilde Silifke ve Tekkeköy (Samsun) belediyeleri'nde bulunan "Gizlilik ilkesi" de boş olarak çıkmıştır.

Web siteleri Belsis tarafından yapılan Beypazarı, Altındağ, Polatlı, Mamak, Orhangazi, Yenişehir (Bursa), Yakutiye (Erzurum), Odunpazarı (Eskişehir), Tepebaşı (Eskişehir), Gaziantep Anaşehir Belediyesi, Şahinbey (Gaziantep), Mersin Akdeniz Belediyesi ve Kandıra (Kocaeli) belediyelerinin, e-belediye ve çerezler hakkında bilgi verdiği görülmüştür. E-belediye kısmında bilgi verilirken, "e-belediye olgusunun hayata geçirilebilmesi için bazı varsayımların olduğu" ve bu varsayımlar açıklanırken de, "hukuki olarak; kişisel özlük bilgilerinin mahremiyetinin sağlanacağı" belirtilmiştir. E-belediye kısmında hazırlanan ayrıntılı bilginin çeşitli kuruluşların yayınları[2], raporları ve makaleleri ile hazırlandığı görülmektedir. Bir anlamda burada yazılanlar belediyelerin kişisel verilerin korunması konusunda kendi taahhütleri yerine olması gerekenleri içermektedir.

Başiskele Belediyesi, kullanıcı tarafından yapılan başvurunun gizli tutulması isteniyorsa, gizli kutusunun işaretlenmesini belirtmekte, Anamur Belediyesi de istek-şikâyet formu ile bilgi toplarken şikâyetin gizli olup olmadığını sormaktadır.

Ankara'da Çankaya belediyesi ile benzer sisteme sahip olan 15 belediye, "güvenliğiniz için" başlıklı web sayfasında, "gizliliğinizi korumak adına, eriştiğiniz bilgisayarda özel hiç bir bilgi tutulmamaktadır" ile "işlemlerinizde kullandığınız banka kartları ile ilgili hiç bir bilgi tarafımızdan saklanmamaktadır" ifadelerine yer vermektedir. 95 belediyenin web sitesinde sadece güvenlikle ilgili bildirim ve uyarılara yer verildiği, 171 belediyenin web sitesinde ise ne mahremiyet ne de güvenlik bildirimlerine, uyarılarına yer verilmediği gözlenmiştir.

5.2. Mahremiyet beyanları neleri içermektedir?

Yukarıda da belirtildiği gibi, sadece İstanbul Büyükşehir, Kartal, Üsküdar, Bursa Büyükşehir, Tarsus, Muratpaşa ve Aliağa belediyeleri olmak üzere 7 belediyede mahremiyetle

[2] Türkiye belediyeler birliği yayınları, TÜSİAD, e-Devlet ve e-Belediye raporu, Yrd.Doç.Dr. Murat Erdal E-belediye kavramı ve İstanbul Büyükşehir belediyesi uygulaması, makalesi,Türkiye Bilişim Derneği, e-Devlet yolunda Türkiye, TBD Yayınları, Ankara,2002, başbakanlık, e-Türkiye 1.ara raporu, başbakanlık yayınları, Ankara,2002'den yararlanılmış.

ilgili etkin bir beyan bulunmaktadır. Kartal, Tarsus ve Aliağa belediyeleri, ziyaretçiler tarafından doldurulan formlar yoluyla elde ettiği kişisel verileri üçüncü kişilere satmayacağı, kiralamayacağı ya da hiçbir şekilde kullandırtmayacağını belirtmektedir. Kişisel bilgilere sadece yetkili belediye yöneticilerinin ve bilgileri gizli tutmayı kabul etmiş olan temsilcilerin erişebileceği belirtilmiştir. Yine her üç belediye de, kullanıcının, bu belediyelerin sitelerindeki bağlantılar aracılığıyla gidecekleri diğer sitelerin, bu belediyelerin mahremiyet ilkelerine uyacağını garanti edemedikleri için bu sitelere herhangi bir bilgi vermeden önce onların mahremiyet yaklaşımlarını değerlendirmelerini önermektedir. İstanbul Büyükşehir Belediyesi, Üsküdar Belediyesi ve aynı mahremiyet ilkelerini koymuş olan Muratpaşa ve Bursa Büyükşehir Belediyeleri de, internet sitesi üzerinden verilmiş olan kişisel bilgilerin hiçbir şekilde üçüncü şahıslarla paylaşılmayacağı ya da ticari amaçla kullanılmayacağını belirtmekte ancak "resmi makamlardan kullanıcıya yönelik bir suç duyurusu ya da soruşturma talebi gelmesi veya kullanıcının bu belediyelerin sistemlerinin çalışmasına engel olacak bir elektronik sabotaj ya da saldırıda bulunduğunun anlaşılması üzerine kullanıcının kimlik bilgilerinin yasal mercilere bildirileceği" ni de ifade etmektedirler. Bu belediyelerin kullanıcıya sunmuş olduğu mahremiyetle ilgili maddelerin standart olduğu ve özde kullanıcıdan çok belediyelerin kendilerini koruma altına almak için konulduğu düşünülmektedir.

Bursa Keleş Belediyesi ise, kullanıcı kayıt formu ile topladığı bilgilerin altına kullanıcıların üye olmakla sahip olacakları üstünlükleri sıraladıktan sonra "kişisel bilgilerin gizli tutulacağı" ibaresini koymuştur. Ancak kullanıcının üye olabilmek için okuyup onaylamak zorunda olduğu maddelere bakıldığında, kullanıcının girdiği her türlü verinin veri tabanında tutulacağını kabul edeceği ve her ne kadar bu bilgiler 3.taraflara aktarılmayacak olsa da "herhangi bir 'hack' olayı sonucunda bu bilgiler 3. şahıslara dağılırsa bundan webmaster, moderatör ya da yöneticilerin sorumlu tutulamayacağı" açıkça belirtilmektedir. 13 belediyede ise, e-belediye konusunda bilgi verilirken hukukla ilgili e-belediye varsayımlarından söz edilmekte ve "kişisel özlük bilgilerinin mahremiyetinin sağlanacağı" belirtilmektedir. Ancak bu belediyeler olması gerekenden söz etmekte ve gerçekte böyle bir taahhütte bulunmamaktadırlar.

Tablo 2. Belediyelerin mahremiyet beyanlarının içeriği

Kişisel verilerin ticarileştirilmeyeceği ve üçüncü taraflara aktarılmayacağı	7
Resmi makamlardan kullanıcıya yönelik bir suç duyurusu ya da soruşturma geldiğinde kullanıcının bilgilerinin verileceği	4
Erişilen bilgisayarda (kişiye) özel ve banka kartlarına ilişkin hiç bir bilginin saklanmayacağı	15
E-belediye varsayımları çerçevesinde "kişisel özlük bilgilerinin mahremiyeti sağlanacağı" belirtilmekle birlikte gerçekte bu taahhütün verilmediği belediyeler	13

5.3. Sadece güvenlikle ilgili beyanda bulunan belediyelerin güvenlik bildirimleri

Belediyelerin 35'i, "belediye aracılığıyla gerçekleştirilen ödemeler ve kişisel bilgilerin güvenliğinin belediye için önemli olduğu, bu nedenle gerekli güvenlik önlemlerini en yüksek seviyede tutabilmek için en yeni ve en iyi güvenlik önlemlerini sürekli araştırdıkları ve etkin güvenlik çözümlerini uygulamaya çalışmakta olduklarını" belirtmişlerdir. Kullanıcılara da güvenlikleri konusunda almaları gereken önlemler ile dikkat etmeleri gereken hususlar önemle vurgulanmıştır. Bunlar doğum günü, telefon numarası gibi başkaları tarafından kolayca tahmin edilebilecek olan şifrelerin oluşturulmaması, oluşturulan şifrelerin ortak olarak kullanılan ortamlara kayıt edilmemesi ve güvenli biçimde saklanması, halka açık alanlarda yapılan işlemlerde çok dikkatli olunması ve işlem bittikten sonra güvenli çıkış butonunun kullanılmasıdır. Yine herhangi bir işlem yapılırken anti-virüs programı kullanıldığından emin olunması da istenmektedir. 28 belediyede yapılan interaktif işlemlerde güvenliğin korunduğu sembollerle ya da kredi kartlarının kendi koruma sistemleriyle olduğu belirtilmektedir. Semboller çoğunlukla yerel yönetim yazılımlarında kullanılan Saysis ile bankalar arası kart merkezi tarafından sunulan

ve Visa, Mastercard tarafından geliştirilen3D sisteminin güvencesini göstermektedir. Çekmeköy Belediyesi ise güvenlikle ilgili sadece bilgi vermiş, güvenlik konusunda herhangi bir taahhütte bulunmamıştır. Bazı belediyeler güvenlik harfleri ya da doğrulama kodları kullanırken Tire Belediyesi yapılan ödemelerde, üçüncü taraflara bilgi aktarılmayacağı konusunda güvenlik sertifikası sunmaktadır.

10 belediyede ise güvenlik uyarısı bulunmakla birlikte, yapılan her türlü işlemler ile çalınmış veya kaybedilmiş bulunan kişisel şifre ve kişisel bilgiler konusunda sorumluluk kabul etmediğini açıkça belirtmektedir. Gizlilik politikası bulunan İstanbul Büyükşehir, Üsküdar, Bursa Büyükşehir, Muratpaşa belediyeleri de, "hiçbir teknolojik sistemin tamamen güvenli, "kurcalama" ya da "hacker-korumalı" olmadığını ve kullanıcı bilgilerine ilişkin "yetkisiz erişim", "hatalı kullanım" ya da "yanlış değişim" risklerini önlemek ve asgariye indirmek için gerekli tedbirlerin yazılım ve donanım olarak alındığını belirterek, buna rağmen doğacak zarardan kendilerinin sorumlu olmadığını vurgulamışlardır.

Tablo 3. Sadece güvenlikle ilgili beyanda bulunan belediyeler

Etkin güvenlik önlemleri almakla birlikte, kullanıcıların da dikkatli olmasını isteyen belediyeler	35
Güvenlik için kredi kartının kendi sistemini ve sembollerini kullanan belediyeler	28
Güvenlik uyarısında bulunan ancak sorumluluk almayan belediyeler	10
Diğer (güvenlikle ilgili harf, sertifika ve doğrulama kodu kullanan belediyeler)	22
Toplam	**95**

5.4. Bilgilerin hangi amaçla toplandığı belirtilmekte midir?

Kişisel Veri Koruma Kanunu Yasa Taslağı'nın 5.maddesi, (a) ve (b) bentlerine göre "kişisel verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi, verilerin belirli, açık ve meşru amaçlar için toplanması ve bu amaçlara aykırı biçimde yeniden işlenmemesi" gerekmektedir. Sitenin altında "gizlilik" başlığı ile kişisel bilgileri üçüncü taraflara aktarmayacağını ve kullandırtmayacağını açıkça belirten Kartal, Tarsus ve Aliağa belediyeleri, bu bilgileri yayınlar/ yazışmalar, e-posta ile basın bültenleri veya bildirimleri göndermek amacıyla kullandıklarını ifade etmişlerdir. Bu belediyeler ayrıca, "kullanıcı kimlikleri açıklanmadan istatistiksel bilgilerin (tarayıcı tipi, coğrafi konum, yaş, cinsiyet v.b.) internet sitesini iyileştirmek ve genel olarak kullanıcıları hakkında daha çok bilgi sahibi olmak amacıyla kullanıldığını" da belirtmişlerdir. Gizlilik sözleşmesine sahip İstanbul Büyükşehir Üsküdar, Bursa Büyükşehir ve Muratpaşa belediyeleri ise, kişisel bilgilerin "ticari amaçlarla kullanılmayacağını" beyan ederken, bu bilgilerin hangi amaçla kullanılacağından söz etmemişlerdir. Keçiören (Ankara), Kayseri Büyükşehir, Aksu (Adana), Başiskele (Kocaeli), Derince (Kocaeli), Körfez (Kocaeli), Havza (Samsun) ve İlkadım (Samsun) belediyeleri ise, herhangi bir mahremiyet/ gizlilik sözleşmesine sahip olmamalarına karşın "bu bilgilerin daha iyi hizmet vermek amacıyla istatistik oluşturmak için sorulduğu" nu bildirmişlerdir. Diğer belediyelerin web sayfalarına bakıldığında da, e-belediye uygulamalarının dışında, kişisel bilgi edinme formu ya da istek/öneriler/şikâyet formları aracılığı ile kişisel bilgilerin toplandığı, ancak hangi amaçla bu bilgilerin toplandığının belirtilmediği görülmektedir.

Tablo 4. Kişisel verileri hangi amaçlarla topladığını belirten belediyeler

Gizlilik/mahremiyet başlığına sahip ve her türlü bildirimi gönderebilmek, internet sitesini iyileştirmek ve tüketiciyi daha iyi tanıyabilmek amacıyla bilgi toplayan belediyeler	3
Gizlilik/mahremiyet sözleşmesine sahip olduğu halde kişisel bilgileri hangi amaçla topladığını belirtmeyen belediyeler	4
Gizlilik/mahremiyet ile ilgili hiçbir beyanda bulunmayan ancak daha iyi hizmet verebilmek amacıyla istatistik oluşturmak için bilgi toplayan belediyeler	8

5.5. Kişisel verilerin hangi düzenlemeye göre toplandığı belirtilmekte midir?

Kartal, Tarsus ve Aliağa belediyelerinde bu konuda hiçbir ifade bulunmazken, İstanbul Büyükşehir, Üsküdar ve Bursa Büyükşehir belediyelerine ait gizlilik sözleşmesinin 9.maddesinde ve Muratpaşa Belediyesinin 8.maddesinde, "bu politika T.C. yasalarına uygun olarak, hiçbir yasal tezada yer verilmeden yürütülecektir. Eğer bu politikanın herhangi bir maddesi, yasadışı geçersiz ya da herhangi bir nedenden ötürü yasal açıdan uygulanamaz durumdaysa, o halde söz konusu madde bu politikadan çıkarılabilir sayılacak ve geriye kalan maddelerin geçerliliğini ve yasal açıdan uygulanabilirliğini etkilemeyecektir" ifadesi yer almaktadır. Ancak söz konusu TC yasaları ile içerdikleri hak ve yükümlülükler açıkça belirtilmemektedir. Oysa kaynağını özel yaşamın mahremiyetinden alan kişisel verilerin korunması ile ilgili olarak 1982 Anayasasında ayrı bir hüküm bulunurken, Yeni Ceza Yasasının 134.maddesi, özel yaşama ilişkin konularda gizlice kaydedilmiş görüntü ve seslerin yayınlanmasını hatta kaydedilmesini suç saymaktadır. Kişisel Veri Koruma Kanunu Tasarısı'nın 5.maddesine bakıldığında ise; kişisel verilerin hukuka ve dürüstlük kurallarına uygun olarak belirli, açık ve meşru amaçlar için toplanması, toplanan verilerin amaçla bağlantılı, yeterli, orantılı olması gerekmektedir. Veriler gerektiğinde güncellenmeli ve gerektiği kadar muhafaza edilmelidir. Kişisel verilerin istatistiki veya bilimsel amaçlarla yeniden işlenebilmesi için yeterli koruma tedbirleri getiren düzenlemenin yanı sıra kişisel verileri kontrol edenin de gerekli tedbirleri alması zorunlu bulunmaktadır.

5.6.Mahremiyetle ilgili beyanlar açıkça görülmekte midir?

Mahremiyetle ilgili başlıklar, genelde sayfanın altında, iletişim, erişebilirlik ve site kullanım koşulları ile birlikte ya da bu koşulların içerisinde belirtilmektedir. İstanbul Büyükşehir Belediyesi, "Site Kullanım Şartları", Üsküdar Belediyesi "İletişim/Talep ve Öneri/ Gizlilik Sözleşmesi", Kartal Belediyesi "Anasayfa/İletişim/Kullanım Şartları/Gizlilik", Bursa Büyükşehir Belediyesi "Site Kullanım Şartları", Tarsus Belediyesi "İletişim/Kullanım Şartları/ Gizlilik", Aliağa Belediyesi "Anasayfa/İletişim/Gizlilik İlkeleri /Kullanım Şartları", Muratpaşa Belediyesi "Gizlilik Sözleşmesi ve Erişebilirlik" kısmında mahremiyetin korunacağından söz etmektedir. Bu başlıklar çok fazla dikkat çekmediği gibi, mahremiyetin korunacağına dair ifadeler "site kullanım şartları" içinde de yer alabilmektedir. Dolayısıyla siteler mahremiyetle ilgili bilinçli bir çabada bulunmazken, konuyla ilgili farkındalık geliştirmeyen kullanıcılar da bu sitelerin neleri güvence altına almak istediklerini ayırt etmemektedirler.

Tablo 5. Mahremiyet taahhüdünde bulunan belediyelerin beyanlarının görünürlük durumu

Mahremiyetle ilgili başlıkları, sayfanın altında, iletişim, erişebilirlik ve site kullanım koşulları ile birlikte ya da bu koşulların içerisinde gösteren belediyeler	7
Mahremiyet bildirimine sadece güvenlik kısmında interaktif işlemlerde yer veren belediyeler	15

5.7.Belediyelerde çerez kullanılmakta mıdır?

AB Direktifi 2002/58/EC kişisel verilerin korunmasıyla ilgili olarak, çerezlere değinmiş ve özellikle 5(3) maddesi ile çerez yerleştirilmesini dışarıdan müdahale olarak kabul etmiştir. Bu maddeye göre, çerez ile bilgi toplamak için mutlaka kullanıcının bilgilendirilmiş olması ve onayı gerekmektedir. 2008 yılında TBMM'ye sunulan "Kişisel Verilerin Korunması Kanunu Tasarısı"'nın 6.maddesi de, "kişisel veriler ancak ilgili kişinin açık rızasıyla işlenebilir" demektedir. Bununla beraber, kullanıcılara yerleştirilen çerezler hakkında bilgi çoğunlukla verilmemekte veya sıradan kullanıcının kolaylıkla anlayamayacağı teknik bir dil içinde gözden kaçırılmaktadır. Belediyelerin web sayfalarına bakıldığında da, açıkça çerez kullanıldığı ifade edilmemektedir. 25 belediye "üye giriş" kısmına, bir çerez olan "beni hatırla" butonu koymuştur. 14 belediye ise, çerezler konusunda kullanıcıya bilgi verirken kendilerinin kullanıp kullanmadığı konusunda bir bilgi vermemiştir. Bunlardan İstanbul Büyükşehir, Üsküdar, Bursa Büyükşehir Belediyeleri şu ifadeyi eklemişlerdir.

> "zaman zaman kullanıcıları tanımlayabilmek için onların bilgisayarlarına "cookie" olarak bilinen bilgi yerleştirildiği ve bilginin ziyaretçilerin bu siteyi ne zaman ve nasıl kullandığını göstermesinin sitelerinin gelişmesine yardımcı olacağını belirtmişlerdir. Kullanıcılar "cookie" almak ya da bu "cookie"lerin ne zaman yerleştirildiğini bilmek istediklerinde bu özelliğe sahip web tarayıcısı kullanarak bunu yapabileceklerdir"

Çerezler hakkında bilgi veren diğer belediyeler de bazı web sitelerinin buraları ziyaret eden kullanıcıların bilgilerini topladığını ve bir metin dosyasında tuttuklarını açıklamışlardır. Çerezlerin virüs yaymadıkları, ancak bu tür bilgileri tutmak istemeyen kullanıcıların ziyaret ettikleri web sitelerinde var olan "tanımlama bilgisi" kullanımını, güvenlik ayarları yoluyla denetleyebilecekleri ve güvenlik ayarlarını araçlar altındaki internet seçenekleri penceresinden gizlilik adımını seçerek gerçekleştirebileceklerini de belirtmişlerdir. Mudanya Belediyesi'nde de, kullanıcı girişi için gerekli butonlar tıklandığında, kırmızı yazı ile " bu noktadan sonra çerezlere izin verilmelidir" cümlesi ile karşılaşılmaktadır. Bir anlamda kullanıcı adını ve şifresini girerken, çerezle ilgili bir uyarı ile karşılaşmaktadır. Burada "beni anımsa" kutusu da yer almaktadır.

Tablo 6. Çerez kullanan belediyeler

Çerezler hakkında bilgi vermekle birlikte kendisinin kullanıp kullanmadığını açıklamayan belediyeler	14
Çerez kullandığını belirtmeyen anacak "beni hatırla" butonu ile bilgileri kaydettiği anlaşılan belediyeler	25
Çerez kullandığını açıkça belirten belediyeler	1

Sonuç ve Değerlendirme

İnternet bir taraftan günlük yaşamı kolaylaştırıp zenginleştirirken diğer taraftan kişisel bilgilerle ilgili kaygılara yol açmaktadır. Özellikle kullanıcının kişisel bilgilerinin satılması ya da izinsiz olarak üçüncü taraflara aktarıldığı bilgisinin sıklıkla medyada yer alması kullanıcıların kendi bilgileri üzerinde hiçbir denetimlerinin olmadığı algısına neden olmakta ve onları tedirgin etmektedir. Kaygılar karşısında pek çok ülkede çözümler üretilmeye çalışılmaktadır. Bu çözümlerin bir kısmı yasa ve düzenlemeye dayanırken bir kısmı da teknoloji ve mahremiyet beyanları gibi kullanıcıyı rahatlatabilecek farklı çözümler içermektedir. İş çevreleri, kendilerinin ve kullanıcıların yararına olabilecek faaliyetlerin yanı sıra sınır ötesi veri akışını da sınırlayacağı için daha sıkı yasa ve düzenlemeler yerine çeşitli yazılım programlarını ve web sayfasına konulan mahremiyet ve güvenlikle ilgili teminatları tercih etmektedir. Kullanıcıların ihtiyaç ve isteklerine daha kolaylıkla çözüm getirebilecek olan belediyelerin ise bu konuda çok duyarlı hareket etmedikleri görülmektedir.

Belediyeler kişisel bilgileri medeni durumundan, eğitim durumuna kadar ayrıntılı biçimde toplarken amaçlarını belirtmemektedirler. Kişisel bilgiler, sadece e-belediye kısmında kredi kartıyla ödeme yaparken değil, mavi masa, beyaz masa, bilgi edinme formu, şikâyet ve istek ile iletişim kısmında da toplanmaktadır. Bu bilgilerin nerede, nasıl kullanılacağı ve ne kadar süre ile saklanacağı bilgisi hiç verilmemektedir. Sadece 7 belediye mahremiyet politikası ya da mahremiyetle ilgili bildirimde bulunmaktadır. Bunların da belediyelerin kendi samimi taahhütleri olmaktan çok bu sistemleri oluşturan kuruluşların koyduğu tedbirler olduğu düşünülmektedir. Nitekim Kartal, Tarsus ve Aliağa belediyeleri aynı metni kullanırken, İstanbul Büyükşehir, Bursa Büyükşehir, Üsküdar, Muratpaşa belediyeleri de başka bir benzer metni kullanmaktadırlar. Yine Ankara ve İzmir Büyükşehir Belediyeleri bu tür bir mahremiyet politikası ya da bildirimine sahip değilken, Tarsus ya da Muratpaşa Belediyeleri gibi daha küçük belediyelerin mahremiyet beyanlarında bulunması bu düşünceyi desteklemektedir.

Aynı şekilde güvenlikle ilgili uyarılarda bulunan belediyelerin kendileri sorumluluk almak istememektedirler. Çerezler konusunda da açık davranmayan belediyelerin çoğu bu konuda bilgi vermekte ve kullanıcı istemediğinde, bilgisayar programı da uygun olduğunda

çerezlerden nasıl kurtulabileceğini açıklamakta, ancak kendilerinin çerez kullandığından söz etmemektedirler. Sadece bir belediye açıkça "bu aşamadan sonra çerez kullanılması gerektiği"ni belirtmektedir.

Kartal, Tarsus ve Aliağa belediyeleri mahremiyetle ilgili beyanlarını kısa ve anlaşılabilir biçimde sunarken diğerleri 10-11 madde halinde belirtmiştir. Buralarda belediyeler kullanıcıları rahatlatmak ve onlara mahremiyetleriyle ilgili güvence vermek yerine herhangi bir olumsuzluk durumunda kendilerini koruma çabasında oldukları görülmektedir. Mahremiyetle ilgili 7 belediyenin mahremiyet politikaları ve ilkeleri sayfaların altında yer almakta ancak bu konuya önem verip, araştırma yapmayan kişilerin kolayca farkına varacağı biçimde bulunmamaktadır. Güvenlikle ilgili önlemler ve uyarılar ise, interaktif işlemler yapılmak istendiğinde ortaya çıkmaktadır. Bu önlemler ve uyarılar da daha önce belirtildiği gibi bu sistemi yapan kuruluşlar tarafından standart metinler ya da semboller yoluyla sağlanmaktadır. Sistemlerde güvenlik teminatının ve uyarılarının yanı sıra belediyelerin bir kısmında kişisel verilerin üçüncü taraflara aktarılmayacağı bilgisi de verilmektedir. Bir anlamda güvenlik ve mahremiyet birbiriyle ilişkili olarak görülmektedir.

Sonuç olarak, belediyelerin web sayfalarıyla ilgili bu inceleme, belediyelerin kişisel verilerin korunması konusunda duyarsız olduklarını ortaya koymaktadır. Ülkede kişisel verilerin korunmasına dair bir yasanın olmaması, belediyelerin bu konulardaki hassasiyetleri görüp ona göre davranmaları için bir zorunluluk oluşturmamaktadır. Bu bağlamda, yasanın çıkarılması önemli olurken, kullanıcıların bu konudaki talepleri ve kendilerini koruma yönündeki aktif ve bilinçli çabaları da aynı biçimde önem arz etmektedir.

Kaynakça

Acquisti, A.(2010), The Economics of Personal Data and the Economis of Privacy", *OECD Privacy Guidelines*

Adrian, A. (2013), "How Much Privacy Do Clouds Provide? An Australian

Perspective?", *Computer Law& Security Review* 29, s.48-57

Akdeniz, Y. (2010) "Avrupa Siber Suçlar Sözleşmesini İmzalamak Yetmez!",

http://www.bianet.org/bianet/ifade-ozgurlugu/121206-avrupa-siber-suc-sozlesmesini-imzalamak-yetmez (13/08/2013'te erişildi).

Arcand M., Nantel J., Arles-Dufour M. ve Vincent A., (2007), "The Impact of Reading a Website's Privact Statement on Perceived Control over Privacy and Perceived trust", ACR Pre-Conference, Memphis,TN'de sunulan bildiri.

Anton, I.A., Earp, B.J. ve Young, D.J, (2009), "How Internet Users' Privacy Concerns have Evolved Since 2002", North Carolina State University Computer Science Technical Report #TR-2009-16.

Beldad, A. D., De Jong M. ve Steehouder M. F.,(2009), "When the Bureaucrat Promises to safeguard Your Online Privacy: Dissecting the Contents of Privacy Statements on Dutch Municipal Websites", *Government Information Quartetly 26,* s.559-566.

Bennett, C,J.,(1992), Regulating Privacy,:Data Protection and Public Policy in Europe and the United States Cornell University Press

Bilgi ve İletişim Teknolojileri Dünyası, www.bitdunyasi.com/tr/?Sayfa=Detay&Id=12517

Birnhack, M. D, (2008), "the EU Data Protection Directive: An Engine of A Global Regime", *Computer Law & security Report 24*, s.508-520.

Earp, B.J., (2005), "Examining Internet Privacy Policies Within the Context of User Privacy Values", *IEEE Transactions on Engineering Managemen,* vol.52.No.2.s. 227-237.

Geray, H., (2004), *Toplumsal Araştırmalarda Nicel ve Nitel Yöntelere Giriş*, Ankara:Siyasal Kitabevi.

Hallinan D., Friedewald M.l, McCarthy P. (2012), "Citizens' perceptions of Data protection and Privacy in Europe", *Computer Law & Security Review28,* s.263-272.

Han P. ve Maclaunin A., (2002), "Do Consumers Really Care About Online Privacy?", *Marketing Manage,* vol.11.no.1.s.35-38.

Hough, G.M., (2009), " Keeping It To Ourselves:Technology, Privacy, and the Loss of Reserve", *Technology in Society* 31, s.406-413.

İlkiz, F., "Büyük Umutlar ve Kişisel Veriler",http://www.umut.org.tr/public/forum.aspx?id=28973 (05/09/2013'te erişildi).

Krippendorff, K. (1980), *Content Analysis: An Introduction to Its Methodology.* Beverly Hills, CA.

Kuner, C. (2009), "An International Legal Framework for Data Protection:Issues and Prospects", *Computer Law& Security Review 25*, s.307-317.

Milne,G..R., ve Culnan, M..J.,(2004), "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices". *J.Interactive Marketing,*18,3,s.15-29.

Mc Millan, S..J., (2000), "The Microscope and the Moving Target. The Challenge of Applying Content Analysis to the World Wide Web", *Journalism& Mass Communication Quarterly,* Volume 77. No.1 s.80-98.

McStay, A.,(2012), "I consent: An analysis of the Cookie Directive and its implications for UK behaviroal advertising", *New Media &Society,* s.1-16

Paine C. ve ark.,(2007), "Internet Users' Perceptions of Privacy Concerns and privacy Actions", *Int.J.Human –Computer Studies 65*, s.526-536.

Pollach, I. (2007),"What's Wrong With Online Privacy Policies", *Communications of the ACM,*Vol.50.No.9,s.103-108.

Şahin Fırıncıbaşı, Ç, (2008), "Bir Pazarlama iletişim Medyası Olarak Web Ortamında İçerik Analizi Yapmanın Güçlükleri ve Olası Çözüm Önerileri", *Yönetim* Sayı 61, s. 52-71.

Stratford J.S ve Stratford J, (1998), "Data Protection and Privacyin the United States and Europe", *Iassist Quartetl.,* Fall, Vol.223, s.17-20

"Twitter, ABD hükümetinin kullanıcı verisi taleplerine direndi", Hürriyet (9 Haziran, 2013) www2.tbmm.gov.tr/d23/1/1-0576.pdf

EK- KATEGORİLERE GÖRE BELEDİYELER

Kategoriler	Kategori No
Web sayfasında etkin gizlilik politikası/gizlilik ilkesi bulunan belediyeler	**1**
Gizlilik ilkesi bulunan ama web sayfası açılmayan ya da boş çıkan belediyeler	**2**
Mahremiyetle ilgili bilgi veren ancak taahhütte bulunmayan belediyeler	**3**
Başvurunun gizli tutulup tutulmayacağını soran belediyeler	**4**
İstek-şikâyet formunda; şikâyetin gizliliğini soran belediyeler	**5**
Güvenlikle ilgili sayfalarında mahremiyet bildirimine yer veren belediyeler	**6**
Sadece güvenlikle ilgili bildirimde/uyarıda bulunan belediyeler	**7**
Ne mahremiyet/gizlilik ne de güvenlik uyarısında bulunan belediyeler	**8**
Web sayfası açılmayan, ya da resmi web sayfası olmayan belediyeler	**9**

KATEGORİLERE GÖRE BELEDİYELER								
SIRA NO	**BELEDİYELER**	**KATEG NO**	**SIRA NO**	**BELEDİYELER**	**KATEG NO**	**SIRA NO**	**BELEDİYELER**	**KATEG NO**
ANKARA								
1	Ankara Büyükşehir Bld.	7	10	Elmadağ Belediyesi	8	19	Kızılcahamam Belediyesi	8
2	Akyurt Belediyesi	2	11	Etimesgut Belediyesi	7	20	Mamak Belediyesi	3
3	Altındağ Belediyesi	3	12	Evren Belediyesi	8	21	Nallıhan Belediyesi	8
4	Ayaş Belediyesi	8	13	Gölbaşı Belediyesi	7	22	Polatlı Belediyesi	3
5	Bala Belediyesi	9	14	Güdül Belediyesi	9	23	Pursaklar Belediyesi	6
6	Beypazarı Belediyesi	3	15	Haymana Belediyesi	8	24	Sincan Belediyesi	8
7	Çamlıdere Belediyesi	8	16	Kalecik Belediyesi	8	25	Şereflikoçhisar Belediyesi	8
8	Çankaya Belediyesi	6	17	Kazan Belediyesi	8	26	Yenimahalle Belediyesi	7
9	Çubuk Belediyesi	7	18	Keçiören Belediyesi	7	-	-	-
ADANA								
27	Adana Büyükşehir Bld.	2	33	Karaisalı Belediyesi	7	39	Seyhan Belediyesi	8
28	Aladağ Belediyesi	8	34	Karataş Belediyesi	8	40	Tufanbeyli Belediyesi	8
29	Ceyhan Belediyesi	2	35	Kozan Belediyesi	7	41	Yumurtalık Belediyesi	8
30	Çukurova Belediyesi	7	36	Pozantı Belediyesi	8	42	Yüreğir Belediyesi	7
31	Feke Belediyesi	9	37	Saimbeyli Belediyesi	8	-	-	-
32	İmamoğlu Belediyesi	8	38	Sarıçam Belediyesi	8	-	-	-
ANTALYA								
43	Antalya Büyükşehir Bld.	7	50	Gazipaşa Belediyesi	8	57	Konyaaltı Belediyesi	7
44	Akseki Belediyesi	8	51	Gündoğmuş Belediyesi	8	58	Korkuteli Belediyesi	8
45	Aksu Belediyesi	7	52	İbradi Belediyesi	9	59	Kumluca Belediyesi	8
46	Alanya Belediyesi	7	53	Kale Belediyesi	8	60	Manavgat Belediyesi	7
47	Döşemealtı Belediyesi	8	54	Kaş Belediyesi	9	61	Muratpaşa Belediyesi	1
48	Elmalı Belediyesi	8	55	Kemer Belediyesi	7	62	Serik Belediyesi	7
49	Finike Belediyesi	8	56	Kepez Belediyesi	7	-	-	-

KATEGORİLERE GÖRE BELEDİYELER								
SIRA NO	BELEDİYELER	KATEG NO	SIRA NO	BELEDİYELER	KATEG NO	SIRA NO	BELEDİYELER	KATEG NO
BURSA								
63	Bursa Büyükşehir Bld.	1	69	İznik Belediyesi	8	75	Nilüfer Belediyesi	7
64	Büyükorhon Belediyesi	8	70	Karacabey Belediyesi	8	76	Orhaneli Belediyesi	8
65	Gemlik Belediyesi	8	71	Keleş Belediyesi	6	77	Orhangazi Belediyesi	3
66	Gürsu Belediyesi	8	72	Kestel Belediyesi	7	78	Osmangazi Belediyesi	7
67	Harmancık Belediyesi	8	73	Mudanya Belediyesi	2	79	Yenişehir Belediyesi	3
68	İnegöl Belediyesi	7	74	Mustafakemalpaşa Belediyesi	8	80	Yıldırım Belediyesi	7
DİYARBAKIR								
81	Diyarbakır Büykşhr Bld.	7	87	Dicle Belediyesi	8	93	Kocaköy Belediyesi	7
82	Bağlar Belediyesi	7	88	Eğil Belediyesi	8	94	Kulp Belediyesi	8
83	Bismil Belediyesi	8	89	Ergani Belediyesi	8	95	Lice Belediyesi	9
84	Çermik Belediyesi	8	90	Hani Belediyesi	8	96	Silvan Belediyesi	8
85	Çınar Belediyesi	7	91	Hazro Belediyesi	8	97	Sur Belediyesi	7
86	Çüngüş Belediyesi	7	92	Kayapınar Belediyesi	7	98	Yenişehir Belediyesi	7
ERZURUM								
99	Erzurum Büyükşehir Bld.	8	107	Karaçoban Belediyesi	8	115	Pasinler Belediyesi	8
100	AşkaleBelediyesi	8	108	Karayazı Belediyesi	8	116	Pazaryolu Belediyesi	7
101	Çat Belediyesi	8	109	Kazımkarabekir Belediyesi	8	117	Şenkaya Belediyesi	8
102	Dadaşkent Belediyesi	8	110	Köprüköy Belediyesi	9	118	Tekman Belediyesi	8
103	Hınıs Belediyesi	8	111	Narman Belediyesi	8	119	Tortum Belediyesi	8
104	Horasan Belediyesi	8	112	Oltu Belediyesi	8	120	Uzundere Belediyesi	8
105	Ilıca Belediyesi	7	113	Olur Belediyesi	7	121	Yakutiye Belediyesi	3
106	İspir Belediyesi	8	114	Palandöken belediyesi	7	-	-	-
ESKİŞEHİR								
122	Eskişehir Büyükşehir Bld	7	127	Han Belediyesi	9	132	Odunpazarı Belediyesi	3
123	Alpu Belediyesi	8	128	İnönü Belediyesi	8	133	Sarıcakaya Belediyesi	8
124	Beylikova Belediyesi	8	129	Mahmudiye Belediyesi	8	134	Seyitgazi Belediyesi	8
125	Çifteler Belediyesi	8	130	Mihalgazi Belediyesi	8	135	Sivrihisar Belediyesi	9
126	Günyüzü Belediyesi	8	131	Mihalıççık Belediyesi	8	136	Tepebaşı Belediyesi	3
GAZİANTEP								
137	Gaziantep Büyükşehir Bld	3	141	Nizip Belediyesi	8	145	Şehitkamil Belediyesi	7
138	Araban Belediyesi	8	142	Nurdağı Belediyesi	8	146	Yavuzeli Belediyesi	9
139	İshaliye Belediyesi	8	143	Oğuzeli Belediyesi	8	-	-	-
140	Kargamış Belediyesi	8	144	Şahinbey Belediyesi	3	-	-	-
MERSİN								
147	Mersin Büyükşehir Bld	2	152	Çamlıyayla Belediyesi	8	157	Tarsus Belediyesi	1
148	Akneniz Belediyesi	3	153	Erdemli Belediyesi	8	158	Toroslar Belediyesi	7
149	Anamur Belediyesi	5	154	Gülnar Belediyesi	8	159	Yenişehir Belediyesi	7
150	Aydıncık Belediyesi	8	155	Mut Belediyesi	8	-	-	-
151	Bozyazı Belediyesi	8	156	Silifke Belediyesi	8	-	-	-

KATEGORİLERE GÖRE BELEDİYELER								
SIRA NO	BELEDİYELER	KATEG NO	SIRA NO	BELEDİYELER	KATEG NO	SIRA NO	BELEDİYELER	KATEG NO
İSTANBUL								
160	İstanbul Büyükşehir Bld.	1	174	Büyükçekmece Belediyesi	6	188	Paendik Belediyesi	7
161	Adalar Belediyesi	8	175	Çatalca Belediyesi	8	189	Sancaktepe Belediyesi	6
162	Arnavutköy Belediyesi	6	176	Çekmeköy Belediyesi	7	190	Sarıyer Belediyesi	7
163	Ataşehir Belediyesi	6	177	Esenler Belediyesi	8	191	Silivri Belediyesi	8
164	Avcılar Belediyesi	7	178	Esenyurt Belediyesi	7	192	Sultanbeyli Belediyesi	8
165	Bağcılar Belediyesi	8	179	Eyüp Belediyesi	8	193	Sultangazi Belediyesi	7
166	Bahçelievler Belediyesi	7	180	Fatih Belediyesi	7	194	Şile Belediyesi	6
167	Bakırköy Belediyesi	7	181	Gaziosmanpaşa Belediyesi	7	195	Şişli Belediyesi	7
168	Başakşehir Belediyesi	7	182	Güngören Belediyesi	7	196	Tuzla Belediyesi	7
169	Bayrampaşa Belediyesi	6	183	Kadıköy Belediyesi	6	197	Ümraniye Belediyesi	6
170	Beşiktaş Belediyesi	6	184	Kağıthane Belediyesi	6	198	Üsküdar Belediyesi	1
171	Beykoz Belediyesi	7	185	Kartal Belediyesi	1	199	Zeytinburnu Belediyesi	7
172	Beykikdüzü Belediyesi	7	186	Küçükçekmece Belediyesi	7	-	--	-
173	Beyoğlu Belediyesi	7	187	Maltepe Belediyesi	8	-	-	-
İZMİR								
200	İzmir Büyükşehir Bld.	7	211	Dikili Belediyesi	8	222	Menderes Belediyesi	8
201	Aliağa Belediyesi	1	212	Foça Belediyesi	7	223	Menemen Belediyesi	7
202	Balçova Belediyesi	7	213	Gaziemir Belediyesi	7	224	Narlıdere Belediyesi	8
203	Bayındır Belediyesi	8	214	Güzelbahçe Belediyesi	8	225	Ödemiş Belediyesi	8
204	Bayraklı Belediyesi	8	215	Karabağlar Belediyesi	7	226	Seferihisar Belediyesi	7
205	Bergama Belediyesi	8	216	Karaburun Belediyesi	8	227	Selçuk Belediyesi	7
206	Beydağ Belediyesi	8	217	Karşıyaka Belediyesi	8	228	Tire Belediyesi	7
207	Bornova Belediyesi	7	218	Kemalpaşa Belediyesi	8	229	Torbalı Belediyesi	7
208	Buca Belediyesi	6	219	Kınık Belediyesi	8	230	Urla Belediyesi	7
209	Çeşme Belediyesi	7	220	Kiraz Belediyesi	8	-	-	-
210	Çiğli Belediyesi	8	221	Konak Belediyesi	7		-	-
KAYSERİ								
231	Kayseri Büyükşehir Bld.	7	237	İncesu Belediyesi	8	243	Sarız Belediyesi	9
232	Akkışla Belediyesi	9	238	Kocasinan Belediyesi	6	244	Talas Belediyesi	7
233	Bünyan Belediyesi	8	239	Melikgazi Belediyesi	7	245	Tomarza Belediyesi	8
234	Develi Belediyesi	8	240	Özvatan Belediyesi	9	246	Yahyalı Belediyesi	8
235	Felahiye Belediyesi	8	241	Pınarbaşı Belediyesi	7	247	Yeşilhisar Belediyesi	8
236	Hacılar Belediyesi	7	242	Sarıoğlan Belediyesi	7	-	--	-
KOCAELİ								
248	Kocaeli Büyükşehir Bld.	7	253	Derince Belediyesi	7	258	Kandıra Belediyesi	3
249	Başiskele Belediyesi	4	254	Dilovası Belediyesi	8	259	Karamürsel Belediyesi	8
250	Bekirpaşa Belediyesi	4	255	Gebze Belediyesi	8	260	Kardelen Belediyesi	9
251	Çayırhanı Belediyesi	8	256	Gölcük Belediyesi	7	261	Körfez Belediyesi	7
252	Darıca Belediyesi	8	257	İzmit Belediyesi	7	262	Saraybahçe Belediyesi	9

KATEGORİLERE GÖRE BELEDİYELER								
SIRA NO	**BELEDİYELER**	**KATEG NO**	**SIRA NO**	**BELEDİYELER**	**KATEG NO**	**SIRA NO**	**BELEDİYELER**	**KATEG NO**
KONYA								
263	Konya Büyükşehir Bld.	8	274	Derebucak Belediyesi	8	285	Karatay Belediyesi	8
264	Ahırlı Belediyesi	9	275	Doğanhisar Belediyesi	8	286	Kulu Belediyesi	8
265	Akören Belediyesi	8	276	Emirgazi Belediyesi	8	287	Meram	7
266	Akşehir Belediyesi	8	277	Ereğli Belediyesi	7	288	Sarayönü Belediyesi	8
267	Altınekin Belediyesi	8	278	Güneysınır Belediyesi	8	289	Selçuklu Belediyesi	7
268	Beyşehir Belediyesi	7	279	Hadim Belediyesi	8	290	Seydişehir Belediyesi	8
269	Bozkır Belediyesi	8	280	Halkapınar Belediyesi	8	291	Taşkent Belediyesi	8
270	Cihanbeyli Belediyesi	8	281	Hüyük Belediyesi	8	292	Tuzlukçu Belediyesi	8
271	Çeltik Belediyesi	8	282	Ilgın Belediyesi	8	293	Yalıhüyük Belediyesi	9
272	Çumra Belediyesi	8	283	Kadınhanı Belediyesi	7	294	Yunak Belediyesi	8
273	Derbent Belediyesi	8	284	Karapınar Belediyesi	8	-	-	-
SAKARYA								
295	Sakarya Büyükşehir Bld.	7	303	Güneşler Belediyesi	8	311	Nehirkent Belediyesi	9
296	Adapazarı Belediyesi	7	304	Hanlı Belediyesi	9	312	Pamukova Belediyesi	8
297	Akyazı Belediyesi	9	305	Hendek Belediyesi	7	313	Sapanca Belediyesi	7
298	Arifiye Belediyesi	8	306	Karapürçek Belediyesi	9	314	Serdivan Belediyesi	7
299	Bekirpaşa Belediyesi	8	307	Karasu Belediyesi	7	315	Söğütlü Belediyesi	8
300	Erenler Belediyesi	8	308	Kaynarca Belediyesi	8	316	Taraklı Belediyesi	8
301	Ferizli Belediyesi	8	309	Kazımpaşa Belediyesi	9	317	Yazlık Belediyesi	9
302	Geyve Belediyesi	8	310	Kocaeli Belediyesi	8	-	-	-
SAMSUN								
318	Samsun Büyükşehir Bld.	8	325	Çarşamba Belediyesi	8	332	Salıpazarı Belediyesi	8
319	Alaçam Belediyesi	8	326	Gazi Belediyesi	9	333	Tekkeköy Belediyesi	2
320	Asarcık Belediyesi	9	327	Havza Belediyesi	8	334	Terme Belediyesi	8
321	Atakum Belediyesi	8	328	İlkadım Belediyesi	7	335	Vezirköprü Belediyesi	8
322	Ayvacık Belediyesi	8	329	Kavak Belediyesi	8	336	Yakakent Belediyesi	8
323	Bafra Belediyesi	8	330	Ladik Belediyesi	8	-	-	-
324	Canik Belediyesi	8	331	Ondokuzmayıs Belediyesi	8	-	-	-