Akıllı Belediyecilik Zirvesi

2018 Bildirileri

AKILLI BELEDİYECİLİK ZİRVESİ 2018 BİLDİRİLERİ / 122
Editörler:
Yunus Demiryürek
Kerem Ulusoy

ISBN: 978-605-80820-8-3

Yayıncı Sertifika No: 15668

Kapak Tasarımı ve Grafik
Hasan Dede
Merve Zenginel
Batuhan Tanrıverdi

Birinci Basım: Ağustos 2019 (1000 adet)

Matbaa Adı: Matsis Matbaa Hizmetleri
Matbaa Sertifika No: 40421

Sarıdemir Mah. Ragıp Gümüşpala Cad. No: 10
Eminönü 34134 Fatih - İstanbul
Telefon: +90 (212) 402 19 00
Faks: +90 (212) 402 19 55
info@mbb.gov.tr
www.marmara.gov.tr
İnternet satış adresi: e-kitap.marmara.gov.tr

İÇİNDEKİLER

ÖNSÖZ

Günümüz insanları artık dijitalleşen, hızlanan, kolaylaşan ama bir o kadar da güvensizleşen bir dünyanın vatandaşları durumunda. İnsanlar, toplumlar, kültürler değişiyor. Belki de ilk defa böylesi köklü değişimleri canlı canlı gözlemleyebildiğimiz bir devirdeyiz. Neden? Çünkü her şey artık çok daha verimli, çok daha hızlı. Böylesi bir devinimde şehirlerin de değişmesi gerekliliği apaçık bir gerçek.

Artık şehir yönetiminin ihtiyaçları, 1000 yıl öncesinin ihtiyaçlarına göre temelde çok farklı olmasa da, yönetim araçları, bu araçların getirdiği sorumluluklar, ihtiyaçlar, talepler çok farklı. Vatandaşlar artık daha az bürokrasi, her an ulaşılabilir bir yönetim, daha fazla ilgi, daha hızlı hizmet ve yaşadığı şehrin yönetiminde söz sahibi olabilmeyi istiyor. Her an çevrimiçi dünyada var olabilmeyi, adeta yan yana olmayı bekliyor. Ve bunun için her türlü bilgiyi vermeye de hazır. Ya da farkında olmadan veriyor bile…

İşte bu noktada karşılıklı güven konusu ön plana çıkıyor. Yönetim, vatandaşın bilgisini topladıktan sonra, bunları en verimli şekilde işleyerek hayatı kolaylaştıran hizmetlere dönüştürmeli. Tüm bu işlemler sırasında bilgileri güvenli bir şekilde saklamalı, verileri sakladığı sistemleri koruyarak, inovasyon için belirli verileri, belirli kurallar çerçevesinde paylaşarak, veri yığınlarını anlamlandırmalı ve verimliliği artırmalıdır. Günümüzün yeni yeni gelişen en ideal yönetim şeması bu şekilde işlemelidir.

Bu anlamda, akıllı şehir kavramında "insan odaklılık" olgusu büyük önem arz ediyor. İlk geliştiği yıllarda "teknoloji odaklılık" olarak algılanan "akıllı şehir" kavramı, artık daha insan odaklı, daha duygusal bir düzlemde tartışılıyor. Teknoloji elbette ki bu kavramın en önemli bileşeni fakat bununla beraber çevreye duyarlılık, verimlilik, mobilite, sürdürülebilirlik, yaşam kalitesi, ekonomi, ulaşım, yönetim gibi kavramlar da önemli hale geliyor. Bu kavramların her biri, yaşadığımız dünyayı çocuklarımıza daha iyi bir yer olarak bırakabilme telaşı ile var.

Şehirlerimiz değişiyor çünkü insanoğlu değişiyor. Bugün "akıllı şehir" olarak kavramlaştırdığımız bu değişimi, belki de çok kısa bir süre sonra terk edeceğiz. İnşa ettiğimiz bu temeller standartlaşmaya başladıkça bu süre kısalacak.

Bu zirveyi yapmamızdaki amaç ise; Türkiye'nin akıllı şehir vizyonunun gelişimine yardımcı olabilmek, siber güvenliğin, kişisel verilerin korunmasının ve millileşmenin önemine vurgu yapabilmek. Bu yüzden, Akıllı Belediyecilik Zirvesi'ndeki konuşmacılarımızın her bir cümlesinin her bir kelimesini dikkatle dinledik ve önemli bilgiler derledik. Bu sürecin devam etmesi için oturum konuşmalarını kitaplaştırıp sizlerle paylaşıyoruz. Dilerseniz konuşmaların videolarına resmi YouTube kanalımızdan da ulaşabilirsiniz.

Marmara Belediyeler Birliğinin öncülük ettiği bu zirvenin asıl sahibinin sizler olduğunu hatırlatır, daha nice zirvelerde tekrar buluşabilmeyi temenni ederim.

M. Cemil Arslan
MBB Genel Sekreteri

I. OTURUM:

Dijital Dönüşüm Çağında Akıllı Şehir Kurmak

Faruk Eczacıbaşı

Eczacıbaşı Holding Yönetim Kurulu Başkan Yardımcısı ve Türkiye Bilişim Vakfı Başkanı

1954 yılında İstanbul'da doğan R. Faruk Eczacıbaşı, 1973 yılında İstanbul Alman Lisesi'nden mezun olduktan sonra, Berlin Teknik Üniversitesi İşletme Fakültesi'nde lisans ve yüksek lisans eğitimlerini tamamladı. 1980'de Eczacıbaşı Holding'in planlama departmanında çalışma hayatına atıldı. Eczacıbaşı Topluluğu'nun "kompüterizasyon" misyonunu üstlenen Faruk Eczacıbaşı, "Eczacıbaşı Bilgi İletim" şirketinin baş yöneticiliğini üstlendi ve Topluluğun "e-dönüşüm" sürecini yönetti. Halen başkanlığını yürütmekte olduğu, Türkiye'nin bilgi toplumuna dönüşmesi vizyonuyla 1995 yılında kurulan Türkiye Bilişim Vakfı (TBV) aracılığıyla Faruk Eczacıbaşı, çeşitli araştırma raporlarının hazırlanması ve bu konudaki politikaların şekillendirilmesi için çalışmaktadır. 1996 yılında Eczacıbaşı Holding Yönetim Kurulu Başkan Yardımcılığı'nı üstlenen Faruk Eczacıbaşı, halen bu görevi sürdürmektedir. Faruk Eczacıbaşı ayrıca 1999 yılından bu yana Eczacıbaşı Spor Kulübü Başkanlığı görevini yürütmektedir. Eczacıbaşı Kadın Voleybol Takımı bu dönemde; iki kez üst üste Dünya Şampiyonu (2015 ve 2016) olarak Türkiye'yi "Kadınlar Dünya Kulüpler Voleybol Şampiyonası'nın en başarılı ülkesi" mertebesine taşımış, 3 kez Avrupa, 9 kez Türkiye ligi ve 8 kez de Kupa Voley (eski adı ile Türkiye Kupası/Süper Kupa) şampiyonluğu elde etmiştir. Faruk Eczacıbaşı başkanlığındaki Eczacıbaşı Spor Kulübü, kadın ve spor alanında dünyanın en prestijli ödülü olan Uluslararası Olimpiyat Komitesi'nin (IOC) "Dünya Ödülü"ne layık görülmüş, IOC tarafından 18 yıldır verilen ödülü, ilk kez Türkiye'den bir aday kazanırken, kurumsal olarak dünyada bu ödülün ilk sahibi de Eczacıbaşı Spor Kulübü olmuştur. Son olarak, 'Daha Yeni Başlıyor' isimli kitabını 2018 yılında okuyucu ile buluşturan Eczacıbaşı, kendi kişisel deneyimlerinden, Eczacıbaşı Holding'in "kompüter" serüvenine; Türkiye'nin geçirdiği dönüşümlerden, dünyadaki son gelişmelere kadar birçok parametreyi değerlendirerek, her gün daha büyük bir ivmeyle hayatımıza giren teknolojik gelişmelerin getirdiklerini ve götürdüklerini incelemekte, gelecekte dünyayı iyisi ve kötüsüyle nelerin beklediğini tartışmaktadır.

DAHA YENİ BAŞLIYOR

Kendi amacımı hep insanlara farklı bir gözlük takmak olarak değerlendirdim. Yeni bir bakış açısının getirdiği farklılığın günümüzde çok değerli olduğunu düşünüyorum.

Ben planlamacı olarak çalışma hayatına başladım. Bundan 40 sene önce çalışmaya başladığım kurumda 5 yıllık planlar yapmak çok doğaldı.

- Dünya nereye gidecek?
- Dünya düzeni içerisinde, ülkemiz nereye gidecek?
- Türkiye'de, alanımızdaki rekabetin seyri nasıl değişecek?
- Bu rekabet sürecinde, kurumum nerede olacak?

vb. sorular, bizim önümüzdeki yolu nispeten daha iyi değerlendireceğimiz anlamını taşıyor.

40 sene önce dünyanın koşulları bambaşkaydı. Dünya nüfusu 4.3 milyar, Türkiye'nin nüfusu ise 42 milyondu. Daha da ötesi, Türkiye bir kaç tane devletin yönettiği televizyon kanalı ve radyo istasyonu ile sınırlıydı. Ayrıca birkaç tane gazetenin zayıf içeriği ile tüm dünyada olan biteni takip etmek ve yetinmek zorundaydık.

Aradan geçen süre bizi 21. yüzyıla taşıdı. Devran döndü… Dünya nüfusu 8 milyara ulaşırken, Türkiye nüfusu 80 milyonu buldu. Soğuk savaşlar bitti. Sovyetler Birliği yıkıldı. Küresel mal ticaret hacmi aynı dönemde 1,8 trilyon dolardan, 18 trilyon dolara ulaşarak, 10 kat arttı. Dünya ticaretinde o zamanlar %1 dolaylarında olan Çin ticari hacminde dünyanın en üstüne oturdu. 1978 yılında yıllık 1.5 milyar dolar dış ticaret açığı veren Çin, 2008 yılında yıllık 300 milyar dolar, 2017 sonunda ise yarım trilyon dolar fazla verir hale geldi. Herhalde, kantarın diğer kefesindeki ABD için, bileşik kaplar esasınca, durumun tersine işlediğini tahmin edersiniz…

Ve asıl önemlisi, 90'lı yılların başında internet diye bir kavram tüm dünyada üssel gelişmeyi tetikledi ve bilgisayarlar yeni bir iletişim aracı olarak hizmete başladı; ilk olarak haberleşmeyi, sonra girişimciliği, sonra akademik dünyayı, ekonomiyi ve nihayetinde siyasal ve sosyal yaşamı etkiledi.

Bugün, çalışma hayatıma atılmamdan 40 yıl sonra, artık internetsiz, sosyal medyasız bir yaşam düşünemiyorum bile… Küçücük bir köye dönüşmüş dünyamız var artık. İnternetin hayata geçişinin üzerinden yaklaşık 30 yıl geçti ve artık bundan başka bir hayat tarzını bilmeyen yeni nesil yetişti. Türkiye nüfusunun yarısı 30 yaşın altında. 40 yıl önce kullandığımız birkaç tane sinema, bir-iki tane radyo istasyonu ve gazete bir köşede sıkıştı kaldı. Haberlerimizi sayısı binlere varan kaynaklardan, radyolardan, televizyonlardan ve internet sitelerinden alıyoruz. Sosyal medyanın olumlu ve olumsuz etkilerini saymıyorum bile. Her gün yeni bir yenilik, yeni bir farklılık, alışkanlıklarımızı temelinden değiştiren bir değişimden bahsediyoruz.

Alışkanlıklarımızı değiştiren bozguncu yenilikler (İngilizce tabiri ile "Disruptive innovation") denildiğinde, 40 yıl önceki planlama dönemlerine geri dönmek istiyorum. Bu geçen 40 yıl içerisinde;

- Dünya haber alma alışkanlıklarını değiştirdi,
- Bilgiye ulaşmanın yolları değişti. Eskiden gittiğimiz kütüphaneler,, okuduğumuz kitaplar artık parmaklarımızın ucunda,
- Her daim yanı başımızda olan telefon, esas fonksiyonunu yitirerek 5. sıraya düştü,
- Masamızın üzerindeki her şey, artık telefonumuzun içerisinde,
- Paylaşım ekonomisi, sürücüsüz arabalar, robotlaşma, yapay zeka, blockchain, dijitalleşme vb. gibi yeniliklerin hepsine daha yeni başladık.

Alışkanlıklarımızı bozan değişimler süpriz olmasa yenilik olur muydu? Bozguncu yenilikler hesap edilebilse yenilik olur muydu?

40 yıl önce bu işe başladığımda, beş yıllık planlar yapardım. Bundan 5 yıl öncesini düşünün bakalım… Bugün dünyanın geldiği yeri tahmin edebilir miydik? Fütüristlerin 30 sene önce tahayyül ettiklerinin çok daha ötesine geçti dünyamız.

Bir de değişmeyenlare bakalım isterseniz…

Eğitim sistemleri 200 yıldır yerinden pek oynamış sayılmaz;

İnsanların bir arada yaşamasını sağlayan ekonomik yapılar, kent kültürü, hukuk ve sağlık sistemleri, sosyal yaşamlarımızı belirleyen normlar da pek değişmedi.

Peki nelerin değişmesini istemiyoruz?

Neredeyse 5.000 yıllık bir uygarlığın merkezinde yaşamanın gururunu hissediyoruz. Burası öyle bir coğrafyaki, 5 bin yıl boyunca her an taş üstüne taş koymaya devam etmiş.

Akdenizin tarihi bir şehri olan Venedik'te yaşadığım tecrübeyi sizlerle paylaşmak isterim. Venedik bugün dünyanın en fazla turist alan şenirlerinden bir tanesi. O kadar ki, artık şehrin sakinleriturizmin yoğunluğundan bıkmış durumda; şehre giren köprüler kapatılıyor. Sıklıkla tekrarlanan, turist çekmek için neredeyse gün aşırı düzenlenen festivalleri baltalıyor.

Turizmcilerin rüyalarından birisidir Venedik. Gel gelelim, şehrin bilinmeyen yanlarından bir tanesi Venedik'in altyapısının 18.yy'ın sonunda kapasitesini doldurduğudur. Bugün aynı şehir yılda 20 milyon ziyaretçiyi kaldırmaya çalışıyor. Ama bir yandan da yavaş yavaş yana yatıyor. Her yıl en az iki defa, bu adalar üstüne kurulmuş olan şehir, an azından dizlere kadar yükselen suyla mücadele etmek durumunda. İşin kötü yanı: her sene bu miktar artıyor ve şehir yavaş yavaş sulara gömülüyor. Dünyamızın durumu da pek farklı değil.

Cebimize giren yazı masamız hayatımızı ne kadar değiştiriyorsa, bu derece hızlanan dünyanın eğitim, hukuk, sağlık, siyaset ve şehircilik altyapısı da aynı hızla değişmek zorunda. Ve sizler bu yörelerin üstünde yaşayan insanları hem yaşatmak, hem ileriye götürmek, hem de bu gururun sürdürülmesi görevini üstlendiniz. Ne mutlu size…

Ancak, geçmişin zenginliğini önlenemez yeniliklerle birleştirmenin yükü de oldukça ağır. Yeni "akıllı şehir" modelleri her gün masalarımıza akıyor. Barcelonalar, Torontolar, City Lab örnekleri benim inceleme fırsatı bulduklarımdan yalnız bazıları.

Ancak herkes, daha yolun başında… Teknolojik değişime uyum sağlamak konusunda dünyanın her tarafı koşuya yeni başlıyor. Üssel değişimle başa çıkmaya çalışmak, yenilenmeyi devamlı tutmayı başarabilmek gerek.

Yapay zeka, veri akışı ve güvenliği "akıllı şehir" kavramına neler katacak? Veya benim şehrimi akıllı yapacak olan nedir? Kentler sakinlerinin aslında beklentileri nedir? Trafik günümüzün beklenti altında nasıl düzeltilebilir? Trafik kazaları nasıl azaltılabilir. Enerji ihtiyacı en verimli şekilde nazıl düzenlenebilir? Ve en önemlisi, ben kendi zenginliklerimi nasıl artırabilirim.

Her kentin kendine göre artıları ve eksileri var ama bildiğim bir şey daha var: Büyük bir şansa sahibiz. Dünyanın tarihi kültür merkezlerinin en önemlilerinden birisi olan Marmara'nın kentlerinin bu konuda pek zorlanacağını sanmıyorum.

Kendi zenginliklerimizi günümüzün koşullarıyla birleştirerek ileriye götürmek sizler için büyük fırsatlar barındırıyor. Bu noktadan sonra konumuz artık teknoloji değil. Teknolojinin kendisi her ne kadar akıllı gibi duruyorsa, aslında dönüp dolaşıp yönetenlerin zekasına dayanıyor. Her tekonoloji kendi yöneticisi kadar akıllıdır.

"Dünyanın her tarafı koşuya yeni başlıyor," diye altını çizdim. Daha 10 sene önce yabancısı olduğumuz kavramlardan konuşuyoruz. Ama o kavramlar etrafında doğan örneklerden veriler oluşuyor. "Veri yeni petroldür"deniliyor. O kullanılan petrolü bilgiye dönüştürmek sizin işiniz.

Eğer iyi örnekleri kullanmak istiyorsanız, siz de bilgilerinizi açın. Ancak verdiğiniz bilgileri açarsanız, Verdiğiniz kadar bilgi alabilirsiniz… Çok yakında, bir vatandaş olarak, hepinizin yaratacağı iyi örnekleri izleyebilmeyi dört gözle bekliyorum.

Okan Erhan Oflaz

Fatih Belediyesi Başkan Yardımcısı

1970 Erzincan doğumlu, ilk, ortaokul ve liseyi Erzincan'da okudu. 1991 yılında Yıldız Teknik Üniversitesi Harita Mühendisliği Bölümü'nden mezun oldu. Orta Doğu Amme Enstitüsü'nden Belediyecilik ve İmar Hizmetleri Programı, İstanbul Üniversitesi'nde Gayrimenkul Değerleme Uzmanlığı Sertifika Programı, eğitimlerine katıldı. 1991 yılında Erzincan Belediye Başkanlığı İmar Müdür Yardımcılığıyla başladığı iş hayatında sırasıyla; Tarım Bakanlığı Coğrafi Bilgi Sistemleri ve Uzaktan Algılama Merkezi Yöneticiliği ve Çekmeköy Belediyesi Fen İşleri Müdürlüğü görevlerinde çalıştı. 2005 -2012 yılları arasında Fatih Belediyesi Başkan Yardımcısı olarak görevini sürdürdü. 2012 yılında Çevre ve Şehircilik Bakanlığı Coğrafi Bilgi Sistemler Genel Müdürlüğü görevine atanarak, 2 yıl bu görevi yürüttükten sonra 18.04.2014 tarihinde tekrar Fatih Belediyesi Başkan Yardımcılığına atanan Okan Erhan Oflaz evli ve iki çocuk babasıdır.

DİJİTAL DÖNÜŞÜM ÇAĞINDA AKILLI ŞEHİR KURMAK

Endüstri 3.0 ile hayatımıza giren dijital dönüşüm, günümüzde Endüstri 4.0'a geçişte çok önemli bir rol oynamış ve sanayinin yanında yerel yönetimlerin hizmet alanları olan şehirlerin de akıllanmasına çok büyük katkı sağlamıştır. Günümüzde herhangi bir kamu kurumunda coğrafi bilgi sistemleri, elektronik belge yönetim sistemleri, yönetim bilgi sistemleri gibi bilgi teknolojileri artık bir standart haline gelmiş, eskinin bürokrasisi yerini sosyal belediyeciliğe bırakmıştır.

Her ne kadar akıllı şehir denince akla internet bağlantısı olan çeşitli sensör ve cihazların (Iot) entegre olduğu bilgi ve iletişim teknolojileri (ICT) ile donatılmış şehir mekanizmaları gelse de asıl önem arz eden konu bu teknolojileri şehre uygulayabilecek "akıllı insandır". Tekerleğin icadı ile başlayan ve günümüze kadar süren bilgi birikimi, teknolojide inanılmaz ivmelenmeye neden olmuştur. Herhangi bir insan aklından ziyade, sürekli deneyen, sorun çözen, denedikçe bilgi birikimi elde eden akıllı insan faktörü devreye girmiştir.

Teknolojiye bakış açısının sadece elektronik cihazlar olarak algılandığı günümüz koşullarında belirtmek gerekir ki, 16. yüzyılda inşa edilen Beyazıt Yangın Kulesi, dünyanın belki de ilk akıllı şehir uygulamalarından birisidir ve bu örnekten yola çıkarak bir teknoloji geliştirilmeden önce bir sorunun hâsıl olması gerektiği anlaşılmaktadır. Nasıl ki insanlar göç ederken eşyalarını taşıma sorunu için tekerleği icat ettiyse, iletişim sorunu için telefonu, aydınlatma için gaz lambasını, yangınları görebilmek ve hava tahmini için de yangın kulesini icat etmiştir. Bu da yine bilgi birikimi ve akıl ile olmuştur. Bu bağlamda, yerel yönetimlerin şehirdeki sorunların tespiti ve çözümü için gerekli akılı oluşturmasının önemi ortaya çıkmaktadır.

Ülkemizde, dünyanın dört bir köşesinde üretilen son teknoloji ürünleri kolaylıkla temin edilmekte ve kullanılmaktadır. Ancak ne yazık ki, bu teknolojileri kendimizin üreteceği kapasiteye henüz ulaşabilmiş durumda değiliz. Dönüp baktığımızda sanayimizde mevcut teknolojiye ait parçaları kolaylıkla üretilebilecek durumda olduğumuz görülmektedir ancak yeni bir teknolojik ürün bulmak ya da mevcut bir ürünü çok daha iyi hale getirecek geliştirmeleri yapmak için biraz daha zamana ihtiyacımız bulunmaktadır. Devletin vatandaşa en yakın noktası olan yerel yönetimler olarak, üniversiteler ve sivil toplum kuruluşları ile bir araya gelerek artık işçi toplumdan deneyen, düşünen, sorun çözmek için elini taşın altına sokmaktan çekinmeyen girişimci ve üreten topluma evirilmek için gereken eğitim, iş birliği ve desteği sağlamamız gerekmektedir. Bu bağlamda kuluçka merkezleri ve teknokent büyük önem arz etmektedir.

Fatih Belediyesi bünyesinde kurduğumuz Fatih YEPGEM ile bu amaca yönelik çalışmalar yapılmakta olup ülke genelindeki birçok girişimcimize çözüm ortaklarımız ile birlikte eğitim, psikolojik danışmanlık, laboratuvar ve atölye ortamı sağlanmış; hayalin ürüne dönüştürülmesi noktasında gerek melek yatırımcı buluşmaları, gerekse çeşitli kurum ve kuruluşlardan hibe desteği alınması konusunda başarılı projelere katkı sağlanmış, böylelikle yerli ve milli teknolojilerin geliştirilmesinde önayak olunmuştur. Bu alanda kazandığımız tecrübelerle görülmüştür ki; ülkemizde ciddi bir potansiyel bulunmakta ve bu potansiyelin ortaya çıkarılmasında şehir yönetimlerinin etkisi oldukça fazladır.

Sonuç olarak Akıllı Şehirleri kurmanın yanında bu şehirleri yönetmek için gerekli teknolojik gelişmeyi sağlamak için yerel yönetimlerin insan kaynaklarına daha fazla yatırım yapması gerekmektedir. Kurulacak kuluçka merkezleri, atölyeler ve teknokent ile girişimciler ve potansiyeli olan herkes desteklenmeli, kabuklarından çıkarılmalı ve yerli ve milli teknolojilerin üretilerek, akıllı yani konusunda uzmanlaşmış ve belli bir bilgi birikimine ulaşmış insanların ülkeye kazandırılması gerekmektedir. Ancak bu şekilde sürdürülebilir bir akıllı şehir kurulabilir.

Berrin Benli

Novusens İnovasyon ve Girişimcilik Enstitüsü Kurucusu

1963 Ankara doğumlu olan Benli, 1986 yılında ODTÜ Bilgisayar Mühendisliği Bölümü'nden mezun oldu. 2003 yılında Arizona University of Phoenix'in Executive MBA kapsamındaki "Global Management Programı"na devam etti. Bilişim Endüstrisinde 30 yılı aşkın deneyime sahip olan Benli, gerek gelişmekte olan, gerekse olgunlaşmış ulusal ve uluslararası pazarlardaki "Kurumsal Endüstri"deki deneyimini, "İş Yönetimi", "Teknoloji Adaptasyonu ", "İnovasyon" ve "Eğitim" le birleştirmektedir. Bilişim Endüstrisinde, uluslararası şirketlerde (Oracle Corporation, Intel Corporation gibi), yerel büyük sistem entegratörleri ve yazılım geliştirme şirketlerinde, bulunduğu pozisyonlarda hem "İş Yönetimi" hem de "Teknik Yönetim" rollerini yürütmüştür. 12 yıllık Oracle Corporation deneyiminde, gerek Türkiye'de, gerekse bölgesel (35'ten fazla ülkeyi kapsayan Avrupa, Ortadoğu ve Afrika Bölgesi) ve küresel (Amerika, Avrupa ve Ortadoğu Afrika, Asya Pasifik) çeşitli üst düzey yönetim rollerinde çalışmıştır. Avrupa ve Orta Doğu Afrika Bölgesi Destek Hizmetleri Bölümü'nde 35 ülke arasında "En İyi Ülke Destek Hizmetleri Direktörü" ödülünü alan Benli, "Müşteri Memnuniyeti", "Çalışan Memnuniyeti", "Finansal Performans" kategorilerinde, Türkiye adına "En Başarılı Ülke" ödüllerini pek çok yıl üst üste kazanmıştır. 2000 yılında, Türkiye Bilişim Medyası tarafından "e-Arena'da ilk Türk" başlığı ile, uluslararası platformda ilk 'Türk Kadın' unvanına layık görülmüştür. Intel Türkiye'de çalıştığı İnovasyon Merkezi'nde pek çok proje yürütmüş olan Benli, İnovasyon ve Girişimcilik alanındaki çalışmalarını, 2009'da kurmuş olduğu, Bilim, Teknoloji ve İnovasyon alanında Türkiye'nin ilk bağımsız ve özel "Düşünce Kuruluşu" (Think Tank) organizasyonu olan "NOVUSENS – İnovasyon ve Girişimcilik Enstitüsü"nde profesyonel olarak devam ettirmektedir. Benli, BİT'te en hızla büyüyen "Veri İnovasyonu" alanında 2013 Eylül ayında "Büyük Veri Enstitüsü"nü kurmuştur. 2014 Şubat ayında da "Akıllı Şehirler Enstitüsü"nü kuran Benli, gerek Türkiye'de, gerekse yurtdışında bu alandaki uzman kurum ve kuruluşlarla stratejik işbirlikleri geliştirerek, yenilikçi uygulamaların geliştirilmesi için çalışmaktadır.

AKILLI ŞEHİRLERE DÖNÜŞÜM

Akıllı Şehir Tanımı Nedir?

Akıllı şehir kavramının dünyada birden fazla tanımı var. Ortak paydalarına baktığımız zaman, felsefelerinin ortak olduğunu görebiliriz.

İngiliz Standartları Enstitüsü'ne (BSI) göre akıllı şehirler, vatandaşlarına sürdürülebilir, refah seviyesi yüksek ve katılımcı bir gelecek sunmak için, etkin olarak bütünleşmiş sayısal ve beşeri sistemlerden oluşur (2014).

Akıllı Şehirler Konseyi'ne (Smart City Council) göre, bilgi ve iletişim teknolojilerini, şehrin yaşanabilirliğini, çalışılabilirliğini ve sürdürülebilirliğini sağlamak için kullanan şehirlerdir.

Avrupa Birliği ise akıllı şehirleri, geleneksel hizmetlerin ve ağların sayısal teknolojileri ve telekomünikasyon teknolojilerini kullanarak, yaşayanların ve işyerlerinin fayda sağlayacağı şekilde daha verimli hale getirildiği yerler olarak tanımlıyor (2012).

Biz de, akıllı şehirler kavramını, çok kapsayıcı olduğuna inandığımız, Faruk Eczacıbaşı'nın tanımladığı şekliyle, "sınırlı kaynaklarını daha etkin, daha verimli kullanmak için bilgi ve iletişim teknolojilerine yatırım yapan, bu yatırımlar sonucunda tasarruf eden, bu tasarrufla sağladığı hizmet ve yaşam kalitesini yükselten, doğada bıraktığı karbon ayak izini azaltan, çevreye ve doğal kaynaklara saygılı, tüm bunları yenilikçi ve sürdürülebilir yöntemlerle yapan şehirler" olarak tanımlıyoruz ve ayrıca, kültür ve sanatıyla vatandaşlarını ve ziyaretçilerini birleştiren ve şehrin süreçlerine dâhil eden bir kavram olduğuna da vurgu yapıyoruz.

Mapping Smart Cities in the EU'nun raporuna göre (2014), dünyada, akıllı şehir kavramıyla benzeşen ve örtüşen, ilgili pek çok değişik kavram mevcut. Örneğin,

- Bilgi şehirleri (knowledge cities),
- Dijital şehirler (digital cities),
- Düşünebilen şehirler (ıntelligent cities),
- Ağ şehirler (wired cities),
- Çevreci şehirler (eco-cities),
- Yetenekli şehirler (talented cities),
- Sürdürülebilir şehirler (sustainable cities).

Şehir politikaları seviyesinde, gerek küresel, gerekse Avrupa seviyesinde, tüm bu kavramlar arasında, akıllı şehir kavramı baskın çıkmıştır. Bu nedenle dünyada çoğunlukla akıllı şehirler kavramı kullanılıyor.

Teknoloji, Bu Süreçte Nasıl Bir Rol Üstlenecek?

Novusens kurucuları olarak, 30 yıldır BİT sektöründe çalışıyor olmaktan edindiğimiz deneyimle, akıllı şehirlere dönüşüm yolculuğunda, teknolojinin rolünün kolaylaştırıcı olduğunu ve kesinlikle amaç değil araç olduğunu unutmamak gerektiğini düşünüyoruz.

Akıllı şehirler kavramı, Universidad del Desarrollo Üniversitesi'nde, girişimcilik, sürdürülebilirlik ve akıllı şehirler konusunda yardımcı profesör olarak çalışan Boyd Cohen'in akıllı şehir modeline göre, 3 evrim geçirmiştir (http://quq.la/Rtthj).

Akıllı Şehir 1.0 modeli, teknoloji merkezli olup, büyük/çok uluslu teknoloji sağlayan şirketlerin liderliğinin baskın olduğu şehir modelleri olarak oluşturuldu. İlk geliştirilen akıllı şehirler bu modelde olduğu için, akıllı şehir kavramı hep teknoloji kavramıyla eşleştirildi. Oysaki teknoloji, yaşadığımız şehirlerdeki yaşam kalitemizi artırmak için sadece bir araç. Türkiye'de akıllı şehir alanında ilk çalışan ve önderlik eden kurumlardan biri olarak, başından beri bu yanlış algıyı düzeltmeye gayret ediyoruz. Teknolojinin amaç olmadığını, sadece güçlü bir araç olduğu bilincini yaygınlaştırmaya devam ediyoruz.

İlerleyen yıllarda evirilen akıllı şehir modeli, Cohen'e göre Akıllı Şehir 2.0 modeli, teknoloji destekli ve teknoloji sağlayan şirketlerin liderliğinde değil, şehirlerin yerel yönetimlerinin sahipliğinde yürütülüyor. Çoğunlukla belediyelerin, vizyoner belediye başkanları ve şehir yöneticileri ile birlikte, şehirlerinin geleceğinin ne olması gerektiğine, akıllı teknolojilerin ve inovasyonun nasıl bir rol oynayacağına karar verdikleri bir süreci içeriyor. Bu modelde şehir yöneticileri, şehrin yaşam kalitesini artırmak için teknoloji desteğine odaklanıyorlar. Barselona, Singapur ve Rio dünyada bu modeli uygulayan örnek şehirlerdendir. Cohen'e göre, akıllı şehir modeli daha çok gelişim sağlayarak (Akıllı Şehir 3.0 modeli), vatandaş katılımlı bir karakteristiğe sahip oldu. Amsterdam, Seul gibi başarılı akıllı şehirler, gelecek kuşak akıllı şehirleri yönetebilmek için, yine teknoloji destekli ve vatandaş katılımlı akıllı şehir modelini uygulamaya başladılar. Cohen, Akıllı Şehir 2.0 + Akıllı Şehir 3.0'ın birleşmiş halinin, gelecek için en iyi model olmasını öngörüyor.

Nesnelerin interneti, büyük veri, açık veri, bulut bilişim, sanal gerçeklik, artırılmış gerçeklik, robot teknolojileri, blokzincir, mobil teknolojiler, 5G geniş bant ve fiber erişim altyapısı, SCADA (merkezi denetleme, kontrol ve veri toplama) sistemleri gibi hızla gelişen yüksek teknolojiler, akıllı şehirler uygulamalarında sıklıkla kullanılmaktadır.

Akıllı Şehirlerde Vizyoner Liderlik

Akıllı şehirlerde vizyoner liderlik, akıllı şehirlerin başarı faktörlerinin başında gelmektedir.

> "Şehri oluşturan vatandaşların aklı ve fikri de işe katılmadan, hiçbir şehir akıllı şehir olamaz." (Faruk Eczacıbaşı, TBV Başkanı)

> "Dünyada artık ülkeler değil, şehirler rekabet ediyor." (Zeynep Bodur Okyay, Kale Grup CEO)

> "Bir araya gelmek başlangıç, bir arada olmak gelişim, birlikte çalışmak ise başarıdır." (Henry Ford)

Faruk Eczacıbaşı'nın dediği gibi; bir şehrin akıllı şehir olabilmesi için, vizyoner liderlikle katılımcılık felsefesinin benimsenmiş olması çok önemli.

Zeynep Bodur Okyay'ın altını çizdiği gibi; artık dünyada ülkeler değil, şehirler birbiriyle yarışıyor. Hatta bugünlerde artık destinasyonlar arasında büyük bir rekabet var.

Bu yarış, küresel bir yarış. Bu yarışta başarı sağlayabilmemiz için işbirliği yapmamız şart. Henry Ford'un sözleri, akıllı şehirlere dönüşüm yolculuğu için de adeta olmazsa olmaz bir unsura, işbirliğinin önemine vurgu yapıyor. Özel sektör, kamu, STK'lar ve akademinin yapacağı işbirliğinin sağlanması, akıllı şehirlerin bel kemiğini oluşturması açısından, vizyoner liderliğin en önemli karakteristiklerinden biri olarak karşımıza çıkıyor. Kurumları arasında işbirliği sağlayamayan şehirlerin, akıllı şehir uygulamalarının başarılı olması pek mümkün görünmüyor.

Dünyadaki başarı örneklerinde olduğu gibi, ülkemizde de, akıllı şehirler uygulamalarının başarılı olabilmesi için, kurumlar arası işbirliğini artıracak ve güçlendirecek planlamaların yapılıp hayata geçirilmesi kritik önem taşımaktadır. Söz konusu planlamalar yapılmadan önce, kurumlar arası işbirliğinin önündeki engellerin iyi analiz edilmesi ve bu yönde ilgili hareket adımlarının atılması gerekmektedir.

Ülkemizde akıllı şehir konseptinin gelişimine ve dolayısıyla, şehirlerimizin sosyal ve ekonomik kalkınmalarına katkıda bulunabilmek amacıyla, Türkiye Bilişim Vakfı (TBV), İstanbul Teknik Üniversitesi Bilgisayar Mühendisliği işbirliğinde, Novusens'in Akıllı Şehirler Enstitüsü yürütücülüğünde, Mastercard ve Intel Türkiye sponsorluğunda, Türkiye Akıllı Şehirler Mevcut Durum Analizi ve Stratejisi İnisiyatifi'ni başlattık. Ulaşım, enerji ve su alanlarını kapsayan, Türkiye'nin büyükşehir belediyelerinde, bu belediyelere bağlı idareler ile ilçe belediyelerinde, sular idarelerinde ve enerji dağıtım şirketlerinde, Türkiye'nin akıllı şehirler konusundaki mevcut resmini ortaya koyabilmeyi ve bu doğrultuda ülke çapında geliştirilecek akıllı şehirler yol haritasının ve stratejisinin oluşturulmasında yol gösterici olabilmeyi amaçladık. Çalışmamızda, kurumlar arası işbirliği konusunda önemli tespitler elde ettik.

--- Türkiye Akıllı Şehirler Değerlendirme Raporu, 1 Mart 2016 (http://quq.la/OgFdv)

--- Akıllı Şehirlere Dönüşüm Yolunda Türkiye (http://quq.la/SbUtm)

Türkiye Akıllı Şehirler Stratejisi İnisiyatifi'mizin 2. aşamasında ise orta ölçekli şehirlerimize odaklanarak, şehirlerimizin, sistematik olarak, dijital dönüşüm modeliyle, akıllı şehirlere dönüşmesi için çalışmaya başladık. İlkini, Kale Grubu'nun hamiliğinde ve TBV'nin işbirliği ile Novusens Akıllı Şehirler Enstitüsü olarak, Çanakkale şehrimizde başlattık. Çanakkale'nin yaşanabilirliğine ve sürdürülebilirliğine, teknoloji aracılığı ile katkıda bulunmak ve rekabet gücünü küresel ölçekte yükseltebilmek amacını taşıyan "Aklım Fikrim Çanakkale" akıllı şehre dönüşüm projesinin birinci fazını 31 Mayıs 2017 tarihinde tamamladık. Aynı gün, Çanakkale'de yaptığımız bir basın lansman etkinliği ile projemizin sonuçlarını paylaştık. 5 Aralık 2017 tarihinde ise İstanbul'da, Hello Tomorrow Konferansı bünyesinde, projemizin çıktılarını, raporumuz ile birlikte paylaştık (http://quq.la/ocL5r)

Proje ekibi olarak, bu uzun dönüşüm yolculuğunda, ilk kıvılcımı çakmanın heyecanını taşıyoruz. Akıllı şehir uygulamalarında başarının en büyük anahtarı "işbirliği" yapabilmekte gizli olduğu için, Çanakkale'de, gerek kurumlar arası gerekse vatandaşlar arasında bu işbirliğini ve uyumu yaşamanın mutluluğu içindeyiz. Tüm paydaşlarla el ele vererek, bu dönüşüm yolculuğunda pek çok ilke imza atarak, Çanakkale'nin kendi ölçeğinde sadece ülkemizde değil, küresel olarak da model olmasını arzu ediyoruz.

Sistematik olarak akıllı şehre dönüşme yolculuğunda, uyguladığımız dönüşüm yol haritasında ilerlemeye devam ettik. Projemizin birinci fazını "Anlama", ikinci fazını ise "Öğrenme" şeklinde nitelendirilebilir. Projemizin ikinci fazını, 26 Şubat - 31 Aralık 2018 tarihleri arasında gerçekleştirdik. Çıktılarının, 2019 yılı başında duyurulması ve 2019 yılında başlayacak üçüncü fazın ise "Uygulama" fazı olması planlanmaktadır.

Bir yaşam felsefesi olarak gördüğümüz ve sürekli gelişerek devam edecek Çanakkale akıllı şehir dönüşüm yolculuğunun, fayda yaratması ve örnek olması için desteklerini esirgemeyen tüm kurum ve kuruluşlara, sahipliklerinden ve vizyoner bakış açılarından dolayı proje ekibi adına teşekkür ederiz.

Yankı Yalçın

Samsung İş Geliştirme ve İş Ortaklıkları Avrupa Sorumlusu

Türkiye'nin bilim ve bilim insanları geliştirme projeleri çerçevesinde kurduğu İzmir Fen Lisesinin, arkasından Boğaziçi Üniversitesi Elektrik Elektronik Mühendisliği Bölümünü bitirdi. Bitirme Projesinde Endüstri'de IOT uygulamaları üzerine çalıştı. Yüksek lisansını, US Auburn Üniversitesi ve Boğaziçi Üniversitesi ortak projesi, AI hardware uygulamaları üzerine yaptı. Doktorasını Boğaziçi Üniversitesi'nde, Nano Elektrik-Mekanik Sistemler bilim dalında, Kanser tedavisi ve Vücut içi suni döllenme amaçlı insan içi Nano Robot geliştirme çalışmaları üzerine yaptı. Doktorasını sonuçlandırmadan özel sektöre geçme kararı aldı.

2003-2005 yıllar arasında Boğaziçi Üniversitesinde Öğretim ve Araştırma Asistanlığı yaptıktan sonra 2005 yılı itibariyle özel sektörde çalışmaya başladı. VESTEL' de proje yöneticiliği, ürün yöneticiliği ve son olarak global iş geliştirme bölümü yöneticiliği yaptığı. Bu sırada IOT projeleri üzerine birçok projeyi hayata geçirdi. Arkasından BSH ve SAMSUNG'da bölgesel ve global IOT ve dijital dönüşüm görevlerinde yer aldı. Bu süreçte, uluslararası platformda "SmartTV and IOT Alliance" kurucu üyeliği (LG, Panasonic, Toshiba, Phillips and etc.) ve Türkiye'de "IPTV Derneği" kurucu üyeliği ve başkan vekilliği sorumluluklarını yerine getirdi. Dünyada yeni gelişmekte olan IOT ve SmartTV projeleri çerçevesinde Google, Amazon, Netflix gibi global ve bölgesel birçok firma ile türünün ilk örneği projelere imza atma imkanı buldu. Kişisel hakların ve verilerin korunumu konusunda, daha sonra diğer marka ve IOT girişimlerine emsal gösterilen, BTS ve Almanya hükümeti ile Avrupa birliğinin ilk onaylanan SmartTV GDPR projesine imza attı. Şu anda SAMSUNG HQ'da Bölgesel İş Geliştirme Projelerini yürütmektedir.

GÖBEKLİTEPE'DEN AKILLI ŞEHİRLERE (Nesnelerin İnterneti ve Bulut Teknolojileri)

Gelecekle ilgili hepimizin farklı bir beklentisi var. Bu beklentiler kişiden kişiye değiştiği gibi içinde yaşadığımız zamana ve şartlara göre de değişiklik gösteriyor. Akıllı şehirler için de durum farklı değil. 80'lerde çocuk olan ve zamanın popüler çizgi dizisi "Jetgiller" ile büyüyen birisi için akıllı şehirler; çantaya dönüşebilen, uçan arabalar ve yardımcı ev robotlarıdır. Bugün baktığımızda hala bu hayalden biraz uzağız. Günümüzde akıllı şehirden beklentilerimiz 80'lere göre biraz farklı. Yeni dünya düzeninde akıllı şehirlerden beklentimiz, kaynaklarımızın daha verimli kullanıldığı, kendimize daha çok vakit ayırabileceğimiz temiz ve doğal bir ortamdır. Bunu uçan arabalarla mı sağlayabiliriz, yapay zekâ ile mi yoksa veri madenciliği ile mi şu an tam netleşmiş değil ama insanlık olarak temel ihtiyaçlarımız konusunda en azından hemfikir olmuş durumdayız.

Akıllı şehircilik alanında bütün bu gelişmeler olurken, Türkiye bu gelişmelerin tarihsel sürecinde nerede bulunuyor? Ülkemiz ve bulunduğumuz coğrafya yüzyıllar, hatta yapılan son arkeolojik çalışmalar ışığında binlerce yıl boyunca uygarlığın eşiği ve ilk şehirleşmenin merkezi olmuştur. Hala tamamlanmamış olmakla birlikte, Göbeklitepe'de yapılan çalışmalarda şu an elde ettiğimiz verilere göre, insanların toplayıcılık döneminde, bir araya gelerek, ilk tapınaklarını, yani o zamanın şehir merkezini, bu coğrafyada kurmuştur. Bu tabi ki bir rastlantı değil. Ticaret ve gelişim yolları üzerinde bulunan verimli topraklarımız; uygarlıkların birleştikleri, tecrübelerini paylaştıkları ve bu tecrübeleri dünyaya yaydıkları bir merkez görevini görmüştür. Bu sebeple akıllı şehircilik uygulamalarının geliştirilmesi ve dünyaya yayılması için bir ilgi merkezi olarak coğrafyamız tarihsel mirastan süregelen önemli bir sorumluluk ve görev üstlenmektedir.

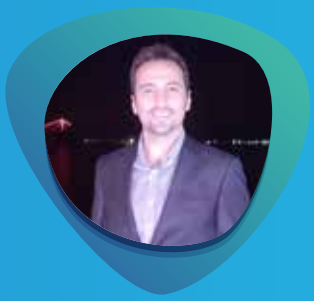
Yapılan arkeolojik çalışmaların da doğruladığı gibi, bulunan yazıtlar, zaman içerisinde insanoğlunun ihtiyaçlarının değişmediğini ama bunları karşılama yöntemlerinin değiştiğini göstermektedir. Yine bizim coğrafyamız üzerinde, Hattuşaş'da yapılan çalışmalarda bulunan tarihi yazıtlarda, ekmek tarifinin verilmesi ama ekmek yapımı için farklı yöntemlerin kullanılması buna güzel bir örnektir. Günümüzde insanların gelecek beklentileri, zamanın ihtiyaçlarını karşılama yöntemleri göz önüne alındığında, geçmişe göre farklılıklar göstermektedir. Bugün akıllı şehirlerden beklentimiz; insansız hava araçları (drone'ler) ile insan ve paket taşınması, daha hızlı iletişim, kesintisiz bağlantı, ucuz ve doğa dostu enerji ve hepsinden önemlisi zamanımızı verimli bir şekilde kullanabilmemizi sağlayacak yapay zekâ çözümleri-

dir. Buna güzel bir örnek, elektrikli, kendi kendine gidebilen (otonom, self-driving) araçlardır. Bu araçlar hem doğa dostu enerji ile dünyadaki mevcut kaynaklarımızı daha verimli kullanmamızı sağlarken hem de bize büyük şehirlerde ortalama olarak trafikte kaybettiğimiz 2 saatlik bir zamanı daha verimli kullanmamız için fırsat yaratmaktadır.

Dünyanın çeşitli ülkelerinde, örneğin; Amerika ve Kore'de bazı pilot şehirlerde denemeleri başlayan 5G teknolojisi, bize hızlı iletişim altyapısı sağlayarak akıllı şehirlerin temel yapı taşını oluşturacaktır. Bu çalışmaların dünyanın birçok ülkesinden önce Türkiye'de yapılmaya başlıyor olması ülkemizin ne kadar önemli bir konumda olduğunun ve şehircilik tarihi ve geleceği için ne kadar önemli bir sorumluluk taşıdığının göstergesidir.

Yeni teknolojilerin ve dolayısı ile akıllı şehirlerin önündeki engellerden birisi de adaptasyondur. Geliştirilen birçok proje, bu hizmetlerin insanların hayatlarının bir parçası haline gelmemesinden dolayı yok olmaktadır. Yeni bir teknolojinin hayatımıza uyum sağlayabilmesinin öncelikli şartı, bizlere mevcut ihtiyaçlarımızı karşılayabilmek için çok daha kolay ve faydalı bir yöntem sunmasıdır. Bunu sağlayan ürünler, kullanımının ve öğrenilmesinin kolay olması durumunda hayatımızın bir parçası olabilmektedir. Ancak bununla bitmemektedir. Hayatımıza giren her yeni teknoloji bizden belirli bir zamanı ve ilgiyi talep eder. Örneğin, telefonumuz çaldığında, ortamdaki diğer bütün cihazları susturmamızı talep eder, akıllı saatimiz onu unutmadan sürekli şarj etmemizi ister vs... Bütün bu ürünler bizden ilgi bekleyen çocuklarımız gibidir. Hayatımızda yer alan ve bize hizmet veren cihazların artması, teknolojik sürtünme denen bir etki yaratır. Yapılan çalışmalar 15 akıllı cihazdan fazlasını, teknolojik sürtünmeden dolayı, eş zamanlı olarak yönetemediğimizi göstermektedir. Bu sebeple, hayatımıza ciddi faydalar sağlasa da yönetilemez oldukları için birçok sistem ve akıllı ürün hayatlarımıza girememektedir. Yeni teknolojilerin ve akıllı şehir uygulamalarının bizim bir parçamız olabilmesi için, bize ihtiyaç duymadan birbirleri ile konuşabilir ve bizi anlayarak, doğru tercihler yapabilir bir seviye gelmeleri gerekmektedir. Gelecekte teknolojik sürtünmeyi kaldırabilecek en güçlü aday ise yapay zekâ olarak görünmekte. Samsung, Google, IBM, Amazon başta olmak üzere birçok firmanın ar-ge çalışmalarını bu konuya yönlendirmesinin altında yatan sebeplerden birisi de bu yeni sistemlerin hayatımıza entegre olabilmesinin önündeki engellerin kaldırılabilmesidir.

Dünyanın en kalabalık ve tarihsel mirası en güçlü bölgelerinden biri olarak, tarih boyunca ve günümüzde, şehircilikte dünyaya örnek olacak uygulamaların merkezi olan Marmara Bölgesi ve özellikle İstanbul, bu teknolojilerin hayata geçirilmesi ve yayılması için gerekli olan yoğunluk ve kompleksiteye fazlasıyla sahiptir. Türkiye'yi ve bir domino etkisiyle yaratarak önce yakın coğrafyamızı, akabinde dünyayı daha iyi bir yer haline getirecek olan, belediyelerimizin özel şirketler ve girişimciler ile yaptığı çalışmaların olumlu izdüşümlerini yakın dönemde göreceğimizi umuyoruz. Dostoyevski'nin dediği gibi "Dünya'yı kurtaracak olan güzelliktir" ve bu güzellik coğrafyamızda fazlasıyla mevcuttur. Mevcut ekip ve alt yapımız ile bunu en hızlı şekilde insanlık bahçesinin bir çiçeği haline geçireceğimize dair inancımız yüksektir.



Ahmet Onur Durahim

Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Öğretim Üyesi

Ahmet Onur Durahim, 2004 senesinde Boğaziçi Üniversitesi Endüstri ve İnşaat Mühendisliği Bölümlerinden mezun olduktan sonra 2012 senesinde Sabancı Üniversitesi Bilgisayar Bilimleri ve Mühendisliği Bölümünden doktorasını almıştır. 2013 yılından günümüze Boğaziçi Üniversitesi Yönetim Sistemleri Bölümünde Dr. Öğretim Üyesi olarak akademik hayatına devam etmektedir. Boğaziçi Üniversitesi'nde tam-zamanlı, Sabancı Üniversitesi'nde ise yarı-zamanlı olarak "Veri Bilimi ve Veri Analitiği, Sosyal Ağ Analizi ve Büyük Veri Analitiği" konularında dersler vermektedir. Araştırma konuları arasında "Yapay Zeka Uygulamaları, Sosyal Ağ Analizi, Büyük Veri Analitiği ve Bilgisayar ve Ağ Güvenliği" konuları bulunmaktadır.

YAPAY ZEKA TEKNOLOJİLERİ

Yapay zeka, görme, duyma, öğrenme ve muhakeme etme gibi insansı yeteneklerin makinelere kazandırılması amacıyla biyolojik sistemlerden esinlenerek geliştirilen sistemlerdir. Yapay zeka, içinde makine öğrenmesi ve bunun alt başlığı olan derin öğrenme, bilgisayarla görme ve doğal dil işleme gibi birçok disiplinin, makinelere zeka katma amacıyla bir araya getirilmesiyle oluşmuş kapsayıcı bir terimdir. Günümüzde yapay zeka sistemlerinin ortam değişikliklerine adapte olmalarının sağlanmasına da çalışılmakta ve böylece insan zekasının en önemli özelliği olan değişen duruma ve şartlara uyum gösterme yeteneğinin de makinelere kazandırılması amaçlanmaktadır. Yapay zeka teknolojileri günümüzde, hayatımızın her alanında etkili olmaya ve yaşantımızı değiştirmeye devam ediyor. Günümüzde, gündelik hayatında interneti kullanıp da herhangi bir yapay zeka teknolojisinden faydalanmayan insan sayısı oldukça azdır. Örneğin, herhangi bir e-posta servisi kullanıldığında, spam e-postaları filtreleyen yapay zeka algoritmalarından yararlanılmış olunmaktadır. Aynı zamanda e-postaların konularına göre sınıflandırılması da yine bir yapay zeka teknolojisi sayesinde gerçekleştirilmektedir. Bunların yanında, otoyollarda kullanılan plaka tanıma sistemlerinde, Facebook sayfalarında kullanıcılara sunulan içeriklerin belirlenmesinde, Youtube videosu izlendiğinde önerilen videoların belirlenmesinde ve daha birçok alanda yapay zeka teknolojileri kullanılmaktadır.

Son yıllardaki bu hızlı ilerleme üç önemli gelişmeye dayandırılabilir;

1. Günümüzde bilgisayarların işlemci güçlerinin ve hafıza kapasitelerinin artması ve maliyetlerinin düşmesi ile daha güçlü bilgisayar sistemleri ortaya çıkmıştır. Bu güçlü bilgisayar sistemleri, karmaşık problemlerin çözümüne yönelik geliştirilen yapay zeka algoritmalarının kısa zaman dilimlerinde üretilebilmelerine, yani eğitilebilmelerine olanak sağlayarak ilerlemeyi mümkün kılan önemli etkenlerden biri olmuştur. Bunların yanında, paralel çalıştırılabilen yapay sinir ağlarına özel Tensör İşleme Üniteleri (TPU) gibi donanımlar geliştirilmiş ve işlemlerin çok daha hızlı gerçekleştirilebilmesi sağlanmıştır.

2. İşlemci gücünün yanında ve bundan daha önemli olan diğer bir unsur ise büyük verinin ortaya çıkmasıdır. Özellikle internetin yaygınlaşmasıyla ve akıllı cihaz-

ların kullanımının artmasıyla birlikte, insanlar ve cihazlar tarafından üretilen veri çok büyük boyutlara ulaşmıştır. Bilindiği üzere son iki yılda üretilen veri, daha önceki zamanlarda üretilen veriden çok daha fazladır. Nesnelerin interneti hayatımıza daha çok girdikçe bu hız daha da artacaktır. İşte üretilen bu veriyi kullanarak öğrenen yapay zeka algoritmaları daha akıllı hale gelmekte ve hayatımıza büyük etkileri olmaktadır. Bir problemin çözümünde yapay zeka algoritması ne kadar çok örnekle eğitilirse o kadar başarılı sonuçlar elde etmektedir. Büyük veri teknolojileri sayesinde çok büyük ve çeşitlilik barındıran veri toplanıp, saklanabilmekte ve yapay zeka algoritmaları tarafından işlenebilmektedir.

3. Yapay zeka algoritmaları tarafından verilerin işlenmesi için geliştirilen ve açık kaynak olarak geliştiricilere sunulan platformlar ve bu platformlar çevresinde ve internet aracılığıyla oluşan toplulukların işbirlikleri, üçüncü büyük unsur olarak karşımıza çıkmaktadır. Özellikle, scikit-learn, Tensorflow, Keras, ve Torch gibi açık kaynak makine öğrenmesi ve özelinde derin öğrenme kütüphaneleri ve bunların yanında, kendi yapay zeka uygulamalarını kolayca geliştirebilmeleri için büyük firmaların kullanıcılara sundukları platformlar sayesinde, yapay zeka teknolojilerinin geliştirilmesi hızlanmıştır. Bu sayede, veri-bazlı olarak çözülmesi mümkün problemleri olan kişi ve kuruluşlar, bu platformlar ve topluluklar sayesinde çok daha az bilgi birikimine sahip olarak, bu problemlere yapay zeka teknolojileri ile artık çok daha kısa sürelerde çözüm üretebiliyorlar.

Yukarıda değindiğimiz üç ana unsura ek olarak, yapay zeka teknolojilerine yapılan yatırımların artmış olması da gelişmeyi hızlandırıcı bir etki oluşturmuştur. Yatırımlardaki bu artış, yapay zeka teknolojilerinin geliştirilmesine ve yaygınlaşmasına yönelik olarak, akademideki ve sanayideki iş gücünün de artmasına ve böylece ilerlemelerin çok daha hızlanmasına sebebiyet vermektedir. Narrative Science tarafından 2018 raporuna göre, yapılan anket çalışması sonuçlarına göre şirketlerdeki yapay zeka kullanımı 2016 yılı sonunda %38 iken yüzde 60'a yakın bir artışla 2018 senesine varıldığında bu oran %62 olmuştur.[1] Forrester araştırma şirketinin bir araştırmasına göre ise yapay zeka konusundaki yatırım, 2017 senesinde bir önceki yıla oranla %300 artış göstermiştir.[2] IDC araştırma şirketi ise yapay zeka harcamalarının 2021 yılında 52 milyar dolardan fazla olacağını tahmin etmektedir.[3] Bu göstergeler yapay zeka teknolojilerinin günümüzdeki önemini ortaya koymaktadır.

1 https://www.forbes.com/sites/gilpress/2016/07/20/artificial-intelligence-rapidly-adopted-by-enterprises-survey-says
2 https://www.forbes.com/sites/gilpress/2016/11/01/forrester-predicts-investment-in-artificial-intelligence-will-grow-300-in-2017
3 https://www.idc.com/getdoc.jsp?containerId=prUS43662418

Günümüzde geliştirilen ve kullanılan yapay zeka teknolojilerini ana başlıklar halinde aşağıdaki gibi inceleyebiliriz;

1. **Doğal Dil İşleme ve Metin Analitiği:** İnsanların konuşma dillerinin bilgisayarlar tarafından anlamlandırılması için çalışan bilgisayar bilimi ve aynı zamanda yapay zekanın bir alt dalıdır. Doğal dil işleme sistemleri, öncelikle analiz ettikleri metinlerdeki her bir cümlenin yapısını anlayıp, içerdikleri kelimelerin geçtikleri bağlamdaki anlamlarını belirlerler. Sonrasında bu cümlelerin adreslenen probleme yönelik olarak anlamlandırılmalarını sağlayan ve cümlelerin taşıdıkları duyguları ve barındırdıkları amacın ne olduğunu belirleyen yapay zeka teknolojileridir. Bilgisayarlar tarafından bu teknolojiler ile yapılan metin anlamlandırmaları, güvenlik sistemleri, dolandırıcılık tespiti, makine çevirisi ve kelime oyunlarındaki gibi, sorulan sorulara uygun cevaplar üretme gibi konulara yönelik kullanılmaktadır.

2. **Doğal Dil Üretme:** Doğru kelimeleri, doğru sırayla ve düzgün bir dilgisine sahip olarak bir araya getirip, dinleyici ya da okuyucu tarafından kolay anlaşılır cümleler oluşturulmasına çalışılan teknolojilere verilen addır. Kısacası, veriden anlamlı metinler oluşturulmasıdır. Doğal dil üretme, özellikle müşteri hizmetlerinde, raporlamada ve iş zekası durum özetlenmesinde kullanım alanı bulmaktadır.

3. **Uyumluluk:** Bir kurumun, kanunlara, mevzuatlara, kurallara, yönetmeliklere ve belirlenmiş standartların gerektirdiği şartlara olan uyumluluklarının belirlenmesi gerekmektedir. Para aklama ve dolandırıcılık işlemlerinin saptanmasında ve önlenmesinde, özellikle de doğal dil işleme teknikleri kullanılarak kanunlardaki, bir kurum için önemli olan değişikliklerin otomatik olarak saptanmasında yapay zeka teknolojileri kullanılmaktadır. Ayrıca bu işlemleri ve kontrolleri yerine getirmek için ayrılan insan iş gücü de böylece azaltılmaktadır.

4. **Konuşma Tanıma:** İnsan konuşmalarının saptanıp, toplanan ses verilerinin bilgisayarlar tarafından metin biçiminde doğal dile dönüştürülmesine yönelik geliştirilen teknolojilerdir. Konuşma, tanıma Siri ve Bixby gibi dijital asistanlarda, sesli mesajları metin mesajlarına dönüştüren uygulamalar gibi mobil uygulamalarda ve etkileşimli sesli yanıt sistemlerinde kullanılmaktadır.

5. **Sanal Asistanlar:** İnsanlarla sürekli iletişim halinde olan sanal (kişisel, dijital) asistanlar gün geçtikçe hayatımızın bir parçası haline gelmekteler. Özellikle akıllı cihazlar üzerinde sıkça kullanılan Bixby ve Siri gibi akıllı asistanlar ve bankacılık gibi diğer birçok sektörde çokça kullanılmakta olan sohbet robotu

(chat-bot) uygulamaları insan hayatını kolaylaştıran ve gündelik hayatımızın vazgeçilmez bir parçası haline gelmekte olan teknolojilerdir.

6. **Görüntü ve Yüz Tanıma:** Dijital görüntüdeki veya videodaki bir nesneyi ya da özelliği tanımlayıp tespit edilme işlemine görüntü tanıma denmektedir. Bu sistemlerin başaralı bir şekilde çalışabilmeleri için etiketlenmiş büyük veri gerekmektedir. Örneğin, bir görüntüde kedi olup olmadığını belirleyen bir teknoloji geliştirmek için, örnek bir görüntünün yanında o görüntüde kedi olup olmadığı bilgisinin de algoritmaya girdi olarak verilmesi yani etiketlenmesi gerekmektedir. Bu sistemlerin başarılı sonuçlar elde edebilmeleri için ise çok fazla etiketlenmiş veri ile eğitilmeleri gerekmektedir. Başarılı görüntü ve yüz tanıma sistemleri geliştirebilmek için gerekli olan bu etiketlemeleri büyük çapta yaptırmak için sosyal medyada insanlara görüntüler gösterilip, bu kişi kimdir, bu resimde ne görüyorsunuz, resimdeki arabaların olduğu kareler hangileridir gibi sorular sorulup, yüz ve görüntü etiketleme yaptırılmaktadır. Görüntü tanıma teknolojileri, plaka tanıma, röntgen filmleri, manyetik rezonans görüntüleri gibi tıbbi görüntüleri inceleyerek hastalık tanılama, ve son zamanlarda akıllı telefonlar aracılığıyla yüz tanıma teknolojileri ile kimlik doğrulama gibi alanlarda sıkça kullanılmaktadır.

7. **Güvenlik Uygulamaları:** Yüz tanıma sistemlerinin güvenli şehirler için kullanımına dair bir örneği, Uber şirketinin Microsoft ile geliştirdiği driver-selfie[4] sisteminde görmekteyiz. Bu sistemde sürücü, akıllı telefonu aracılığıyla yüzünün fotoğrafını anlık olarak uygulama üzerinden çekip, kimlik doğrulamasını anlık olarak uygulamaya yaptırıyor ve böylece hizmet veren sürücünün gerçekten o hesaba kayıtlı kişi olup olmadığı anlık olarak uygulama tarafından kontrol ediliyor. Bu yapay zeka teknolojisi ülkemizde de, sürücülerin gerçekten taksi, dolmuş veya otobüs sürmeye ehil ve o aracı kullanacak kişiler olarak kayıtlı olup olmadıklarının kontrolünde kullanılabilir. Böylece vatandaşlara daha güvenli hizmet sunulmuş olur.

8. **Duygu Tanıma:** Görüntü ve ses işleme yöntemleriyle bir kişinin duygusal durumunu belirleyen teknolojilerdir. Kişilerin mikro seviyedeki yüz ifadeleri, vücut dilinin verdiği ipuçları ve insanların konuşmalarındaki tonlamalar ve titreşimler, bu kişilerin duygularının anlaşılmasına yönelik yapay zeka teknolojileri tarafından kullanılmaktadır. Emniyet güçleri, sorgulama ya da takip sırasında bu

4 https://www.youtube.com/watch?v=aEBi4OpXU4Q

teknolojileri kullanarak potansiyel suçlular hakkında daha fazla bilgi elde edebilmektedirler. Bunun dışında duygu tanıma, firmaların bir ürünleri hakkında, müşterilerinin ne hissettiklerinin belirlenmesi ya da yeni tasarlanacak bir ürünün hangi özelliklerinin, müşteride ne tip duygular uyandırdığının anlaşılması için de kullanılmaktadır.

9. **İçerik Üretme:** İnsanların internet ortamında ürettikleri videolar, blog yazıları ve diğer bütün görsel ve yazılı içeriğin benzer şekilde otomatik olarak makineler tarafından üretilmesi için geliştirilen teknolojilerdir. Günümüzde bazı gazeteler ve televizyon kanalları yapay zeka teknolojilerini kullanarak içerik üretmektedirler. Ayrıca verilen bir metinden, o metindeki içeriğe göre video üreten teknolojiler de geliştirilmektedir.

10. **Makine Öğrenmesi Platformları:** Makine öğrenmesi yapay zekanın ve bilgisayar biliminin bir alt disiplini olup, amacı makinelerin öğrenmelerini sağlamaktır. Günümüzde Amazon, Google gibi birçok şirket ve Apache yazılım vakfı[5] gibi kuruluşlar, uygulama geliştirme arayüzlerini (API), algoritmaları, yapay zeka uygulaması geliştirmek için kullanılacak araçları ve büyük veri işleme altyapılarını ve makine öğrenmesi platformlarını açık kaynak olarak kullanıcılara sunmaktadırlar. Ayrıca bunların kullanımını kolaylaştırmak için ürettikleri eğitim dokümanlarını da paylaşarak, bu şirket ve kuruluşlar, yapay zeka uygulaması geliştirmeyi kolaylaştırıp, bu uygulamaların yaygınlaşmasında büyük rol oynamaktadırlar.

11. **Yapay Zeka Teknolojilerine Yönelik Özel Donanımlar:** Google, Cray, Alluviate, ve Nvidia gibi şirketlerin geliştirdikleri ve yapay zeka algoritmalarının hızlı ve paralel olarak çalıştırılabilmelerine olanak sağlayan ve bu algoritmaların çalışma prensiplerine yönelik özel olarak geliştirilen Grafik İşlemci ve Tensör İşlemcileri gibi donanımlardır. Bu donanımlar günümüzde özellikle derin öğrenme algoritmalarının hızlı eğitilmesinde büyük verimlilik sağlamaktadır.

12. **Derin Pekiştirmeli Öğrenme ve Oyunlar:** Elde edilmesi zor ve masraflı olan etiketlenmiş veri üzerinden öğrenen sistemlerin aksine pekiştirmeli öğrenmede sistem, çevreyle etkileşime girerek ve deneme yanılma yöntemleriyle öğrenmeyi gerçekleşmektedir. Derin pekiştirmeli öğrenmede ise derin öğrenme,

5 https://spark.apache.org/mllib/

pekiştirmeli öğrenme teknikleriyle birleştirilmektedir. Günümüzde sürücüsüz araçlardan, Atari oyunlarını ve satranç oynayan yapay zeka uygulamalarına kadar bir çok yapay zeka sisteminde derin pekiştirmeli öğrenme kullanılmaktadır. Son yıllarda dünya şampiyonları Lee Sedol ve Ke Jie'yi yenen yapay zeka sistemi AlphaGo[6] bu metodu kullanmaktadır.

13. **Siber Güvenlik Uygulamaları:** Bilgi ve organizasyon altyapılarına yapılan saldırı ve tehditleri anlık algılayıp, önleyen ve bunlara anlık karşılık veren bilgisayar ve ağ koruma sistemleridir. Son zamanlarda özellikle saldırı tespit ve önleme sistemlerinde yapay zeka algoritmaları çokça kullanılmaya başlanmıştır.

14. **Pazarlama Otomasyonu ve Öneri Sistemleri:** Yapay zeka uygulamaları pazarlamada özellikle müşteriyi tanıma için kullanılmaktadır. Müşteri bölümlendirmesinin ve sınıflandırmasının otomatize edilmesinde ve müşteri verilerinin entegrasyonunda yapay zeka teknolojileri kullanılmaktadır. Ayrıca, yapay zeka algoritmaları kullanılarak geliştirilen öneri sistemleri üzerinden, benzer müşterilerden ya da ürünlerden yola çıkarak ve müşterilerin geçmiş alışveriş alışkanlıkları da göz önünde bulundurularak, kişiselleştirilmiş ürün önerileri sunulmaktadır. Günümüzde izlediğimizde zevk alacağımız filmleri veya okumak isteyeceğimiz kitapları artık yapay zeka sistemleri bizler için bulup bizlere önerebilmekteler. Öneri sistemleri, Netflix gibi içerik sunan platformlarda ve Amazon.com gibi online alışveriş sitelerinde başarıyla kullanılmaktadır.

15. **Sürücüsüz Araçlar:** Günümüzde ulaşım ile ilgili olarak yaşadığımız birçok problemi çözmeye aday teknoloji sürücüsüz araç teknolojisidir. Sürücüsüz araçlar sayesinde trafikte geçirilecek zaman bir kayıp olmaktan çıkacak ve insanlar gerektiğinde toplantılarını ya da yapmaları gereken diğer önemli işlerini arabalarında yolculuk halindeyken güvenle yapabilecekler. Ayrıca, yine çok büyük bir problem olan trafik kazalarının da en aza indirilmesi sağlanarak hem maddi kayıpların, hem de can kayıplarının önüne geçilebilecektir. Sürücüsüz araçların geliştirilmesi yapay zeka teknolojileri göz önüne alındığında çözülmesi en zor problemlerden bir tanesidir. Hem çevrenin görsel olarak algılanması, hem ileriye dönük oluşacak sahnenin öngörülmesi, hem de ortaya çıkacak sorunlar karşısında kritik kararlar verebilecek bir sistemin geliştirilmesi kısa vadede başarılması zor gözüken bir problemdir.

6 https://www.youtube.com/watch?v=8tq1C8spV_g

Yapay Zeka Teknolojileriyle Ortaya Çıkabilecek Problemler

Yapay Zeka teknolojileriyle birlikte, hayatımıza etik ve ahlaki problemler de beraberinde gelmektedir. Akıllı şehirler inşa edilirken, bu problemlerin ortaya çıkmalarının engellenebilmesi için gerekli önlemlerin alınması büyük önem arz etmektedir. Özellikle kamera sistemleriyle elde edilen ve vatandaşlara ait kişisel veriler, mahremiyet problemini ortaya çıkarmaktadır. Bunun yanında bazı hizmetlerin en iyi şekilde sağlanabilmesi için toplanması gereken konum bilgileri gibi diğer kişisel verilerin de mahremiyeti zedeleyebileceği bilinmektedir. Bu sebeplerle yapay zeka teknolojilerinin, ortaya çıkabilecek mahremiyet sorunları göz önünde bulundurularak uygulamaya alınması gerekmektedir.

Yapay zeka algoritmalarında ortaya çıkan önemli problemlerden bir tanesi de algoritmik önyargılar olmaktadır. Yapay zeka algoritmaları, insanlar tarafından üretilen örnek verilerle eğitildiklerinden, insanlarda olan herhangi bir ırkçı ya da cinsiyetçi önyargıyı da öğrenmekte ve bu yargılarla karar vermektedirler. Örneğin, belediye tarafından yapılacak yardımların nerelere ve kimlere yapılacağına karar vermesi için geliştirilecek bir yapay zeka algoritmasının, bu önyargılardan arındırılmış olması gerekmektedir. Bunlara ek olarak, özellikle vatandaşların direk etkilenmesi söz konusu olduğu için, kullanılacak olan yapay zeka teknolojisinin verdiği kararların açıklanabilir olması da belli uygulamalarda önemli gereksinimlerden biridir.

Akıllı Belediyecilikte Yapay Zeka Teknolojisi Uygulamaları

Bu gelişmeler doğrultusunda cevaplanması gereken, "yapay zeka teknolojilerinden yararlanarak, şehirler daha akıllı ve bu sayede daha yaşanılabilir hale nasıl getirilebilir?" sorusudur.

Öncelikle belediyelerin, insan odaklı yapay zeka teknolojilerini göz önünde bulundurmaları gerekmektedir. Yapay zeka teknolojilerini kullanılabilir kılan ana unsurların başında veri gelmektedir. Belediyeler tarafından hizmet alan vatandaşlara, bu hizmetlerin başarılı bir şekilde ulaştırılabilmesi için, vatandaşların çoğunlukla kişisel olan verilerine gereksinim duyulacaktır. İlk olarak, vatandaşların bu verilerini belediyelerle güvenli ortamlar aracılığıyla paylaşabilmeleri sağlanmalıdır. Bunun için kablosuz ağ noktaları ile internete ulaşımın kolaylaşması ve veri iletiminin ve toplanan verilerin saklanmasının güvenli hale getirilmesi gerekmektedir. Bu amaçla, siber güvenlik stratejisi belirlenmeli ve bu çerçevede adımlar atılmalıdır. Sonrasında ise vatandaşın, şehirlerdeki yaşam kalitesini arttıracak ve şehirleri daha yaşanılır hale getirecek yapay zeka teknolojilerinin ve bu teknolojileri geliştirmek için

ihtiyaç duyulacak verilerin belirlenmesi gerekmektedir. Bu verilerin gönüllü olarak paylaşımının sağlanabilmesi için ise vatandaşlar bilinçlendirilmeli ve gerektiğinde vatandaşlara bu yönde kolay ulaşılabilir eğitimler sağlanmalıdır.

Akıllı şehirlerde, akıllı sinyalizasyon ve araç park yeri gösterme uygulamaları, kısa vadede hizmet olarak sunulabilecek yapay zeka uygulamalarıdır. Akıllı sinyalizasyon ile, kameralar ve algılayıcılar aracılığıyla elde edilen yoğunluk bilgisi kullanılarak, trafik ışık süreleri eniyileme algoritmalarıyla belirlenebilecektir. Bu sayede trafikte geçirilen süre azaltılarak, hem zaman hem de maliyet bakımından verimlilik sağlanacaktır. Bunun yanında araçların, park edebilecekleri boş otopark bulmak için trafikte geçirdikleri süre yine yapay zeka teknolojileri sayesinde azaltılabilecektir. Akıllı sinyalizasyon için kullanılacak olan kamera ve algılayıcılar, erken kaza saptama sistemi geliştirmek için kullanılabileceği gibi kazaya mahal verebilecek hareketlerde bulunan sürücülerin saptanmasında da kullanılabilecektir. Örneğin, plaka ve yüz tanıma sistemleriyle, trafik kurallarını çiğneyen sürücülerin, araç ve sürücü bilgileri gerekli birimlere aktarılabilecektir. Bu sistemler ayrıca gerekli durumlarda, oluşan bir kazanın fotoğraflarını ilgili birimlere göndererek, en kısa sürede kazaya müdahele edebilecek çekici ve ambulansı kaza mahalline yönlendirebilecektir.

Ulaşım ile ilgili başka bir uygulama da personel servislerinin, mümkün olduğunda farklı belediyeler tarafından paylaşımlarının sağlanması ve rotalarının eniyilenmesi olacaktır. Böylece aynı güzergah üzerinde ikamet eden personelleri taşıyan ve doluluk oranları az olan servisler birleştirilebilecek ve eniyileme algoritmalarıyla, belirlenecek hedefler gözönüne alınarak, en uygun rotalar belirlenebilecektir. Geliştirilecek olan bu rotalama eniyileme algoritmaları ayrıca çöp toplama gibi, araçlar ile sağlanan diğer hizmetlerde de kullanılabilecektir. Akıllı şehirlerde uzun vadedeki en önemli yapay zeka teknolojisi sürücüsüz araçlar olacaktır. Bu araçlar sayesinde trafik yoğunluğu azaltılarak, zamansal ve maliyetsel tasarruf sağlanacak ve karbon salınımının da azalmasıyla daha sağlıklı bir çevreye sahip olunacaktır. Bu sebeple, şehirleri sürücüsüz araçların kullanılabileceği şehirler haline getirebilmek için şimdiden gerekli stratejilerin belirlenmesi ve bu amaçla adımların atılması gerekmektedir.

Bunlara ek olarak, doğal dil işleme teknolojileri sayesinde, belediyelere internet siteleri aracılığıyla ya da e-posta yoluyla gelen istekler ve şikayetler otomatik olarak anlık incelenip, önceliklendirilip, ilgili birimlere yine anlık olarak iletilebilecektir. Böylece hem zamandan tasarruf yapılabilecek, hem de bu iş için ayrılmış olan personel daha başka görevlere atanarak verimlilik arttırılmış olacaktır.

Yapay zeka teknolojilerinin akıllı şehirlerdeki diğer önemli bir uygulama alanı ise güvenlik olarak karşımıza çıkmaktadır. Görüntü ve yüz tanıma sistemleri sayesinde hem suçun önlenmesi, hem de suçlunun kolay ve hızlı bir şekilde adalete teslim edilmesi sağlanabilecektir. Örnek teknolojilerde de bahsedildiği üzere, sürücülerin yüz tanıma sistemiyle doğrulanması sayesinde, sürücülerin gerçekten taksi, dolmuş veya otobüs sürmeye ehil ve o araca kayıtlı kişiler olup olmadıklarının kontrolü gerçekleştirilerek vatandaşlara daha güvenli hizmet sunulabilecektir.

İsmail Hakkı Polat

Dijital Dönüşüm Derneği Başkanı

1989'da Ortadoğu Teknik Üniversitesi Elektrik-Elektronik Mühendisliği Bölümü'nden mezun olan İsmail Hakkı Polat, 1989-2004 yılları arasında sırasıyla Siemens, Nortel-Netaş, Ericsson ve Turkcell gibi telekomünikasyon firmalarında mühendis ve yönetici olarak çalıştı. 2004 yılından bu yana Kadir Has Üniversitesi İletişim Fakültesi'nde Öğretim Görevlisi olarak "Yeni Medya" dersleri veren Polat, Türkiye'nin ilk Yeni Medya Bölümü'nün kuruluş çalışmalarında da rol almıştır. Ayrıca, Doğan Holding, Merkez Yayın Grubu ve Ciner Medya Grubu gibi medya kuruluşlarının mobil iletişim ile ilgili birimlerinin kuruluş ve interaktif servislerinin geliştirilmesi aşamalarında yönetici veya danışman olarak aktif görev yapmıştır. Polat, halihazırda Kadir Has Üniversitesi Yeni Medya Bölümü'nde Öğretim Görevlisi olarak dersler vermekte ve dönem dönem BBC Media Action'a Bakü Devlet ve Slav Üniversiteleri'nin Yeni Medya müfredatlarının hazırlanması konusunda danışmanlık yapmaktadır. New York'taki Open School of Journalism kuruluşu için Mobil Gazetecilik eğitimleri hazırlayan Polat, son dönemde kurum, kuruluş ve üst düzey yöneticilere Dijital Dönüşüm ve özellikle KriptoParalar konusunda kişiselleştirilmiş eğitimler vermekte ve stratejik dönüşüm danışmanlığı yapmaktadır. Polat'ın Yeni Medya konusundaki görüş ve düşünceleri, her hafta Bloomberg Business Week Türkiye dergisindeki köşesinde yayınlanmaktadır.

AKILLI BELEDİYECİLİK VE BLOKZİNCİR

Son dönemde yerel yönetimlerin gündeminde olan akıllı şehir uygulamalarının blokzincir tabanlı hale getirilmesi vatandaşa nasıl faydalar sağlayacak?

Şu sıralar belediye denildiğinde kamuoyunun gündemi 31 Mart'taki seçimlerle kuşatılmış durumda ama belediyecilik yani yerel yönetim hizmetleri uzun vadeli bakılması ve bu seçim gündemi kuşatmasının ötesinde değerlendirilmesi gereken bir olgu.

Blokzincir en temelde, insanların hâlihazırda yaptığı alışveriş, bilgi değişimi, bankacılık, ödeme, alım-satım gibi çeşitli günlük hayat işlemlerini internet üzerinden ama arada bir aracı kişi ya da kurum olmadan da güvenli hızlı ve şeffaf biçimde yapabilmesini sağlayan bir işleyiş. Blokzincirin yerel yönetimler için en önemli değeri ise, işlem kayıtlarının şeffaf olması ama kişisel bilgilerin mahrem kalabilmesini sağlayacak bir şifreleme yapısına sahip olması. Zaten bu işleyiş biçimi blokzinciri (kripto paralardaki gibi bir dijital değiş-tokuş ve ödeme protokolü olmasının ötesinde) bir dijital güven protokolü haline getirmektedir. Blokzincir tabanlı sistemler, güven amaçlı kullanılan ve iş süreçlerini merkezileştiren noter, banka gibi aracıları ortadan kaldıran değiştirilemez, taklit ve tahrif edilemez bir işleyişe sahiptirler ve hız ile şeffaflık gerektiren kayıtlar üretmek, yayınlamak ve saklamak (arşivlemek) için en elverişli çözümlerdir.

Bu bağlamda akıllı şehir ve blokzincir kavramlarını bir araya getirdiğimizde; kent kaynaklarını akıllı ve verimli kullanacak hız, şeffaflık ve vatandaşın katılımcılığı ile yüksek iş süreçleri tasarlamak ve bu bağlamda yerel yönetimdeki bürokrasiyi de azaltacak bir işleyiş yaratmak gibi bir hedef belirleyebiliriz.

Burada blokzincirin hâlihazırdaki akıllı şehir uygulamalarından en önemli farkı, mevcut uygulamaların bilgi analiz ve karar mekanizmalarının süper merkezi otomatize veya yapay zekaya dayalı ve giderek birer büyük biradere dönüşmesi olası sistemler üzerinden çalışırken; blokzincir sistemlerinin daha otonom ama konsensüs tabanlı sistemlere dayalı, dağıtık bir işleyiş yaratmasıdır.

Bu sayede vatandaşların sisteme katılımı ve sistemi denetlemesi de kolaylaşmakta. Konuyu bu şekilde ele aldığımızda ise, belediyelerde nasıl pratik kullanımlar olacağına ilişkin birkaç örnek de verilebilir. Mesela kentin bina, emlak ve arsa kayıtlarının şeffaf ve taklit edilemez biçimde dökümü çıkartılıp kayıt altına alınabilir ve bu kayıtlar da pafta ve ada bazında kent planlamalarında esas alınıp buradaki sicil

işlemleri, insan inisiyatifinden olabildiğince çıkarılarak merkezi olmayan bir halde de işler biçimde tutulabilir.

Bir başka örnek; kentteki akıllı tüm nesnelerin blokzincir üzerine taşınarak bu nesnelerden gelen trafik, afet, hava kirliliği gibi bilgilerin akıllı kontratlar üzerinden çeşitli aksiyonlara dönüşmesi (araçların rota değişikliği, afet bölgelerinde yapılacak altyapı sınırlamaları veya kesintileri gibi) olabilir. Bu işleyişin normal yapay zeka sistemlerinden en büyük farkı; sistemin süper merkezi olup da kırılması (hacklenmesi) halinde büyük felaketlere yol açacak sistemlerin, daha dağıtık ve şeffaf bir konsensüs mekanizması ile işlemesi ve söz konusu riskleri azaltmasıdır.

Blokzincir projelerinin çoğu bir token veya kripto paraya dönüştürüldüğünde, iş süreçleri çok daha işlevsel ve rasyonel hale gelmekte. Akıllı şehir kullanımı olarak çok önemli bir örneği de, İstanbul Kart'ın bir kripto paraya dönüştürülmesi üzerinden verebiliriz. Bu sayede İstanbulCoin'e dönüşmüş bir İstanbul Kart, sadece ulaşımda değil çok daha çeşitli bir hizmet portföyünün (su, doğalgaz faturaları, vergi, kültür-sanat aktiviteleri, otopark, vs...) ödemeleri için de kullanılabilir. Burada da mevcut sistemden en büyük farkı, tüm ödeme işlemlerinin anında ve açık biçimde muhasebeleştirilerek takip edilebilmesi olacaktır. Ayrıca, bu işleyişi vatandaşla ilişkilerde bir ödül sistemi olarak da kullanıp, vatandaşların kente yaptığı çeşitli katkılar (ağaç dikme kampanyalarına katılım, kaçak yapı ihbarı, kentle ilgili yaratıcı önerilerde bulunma) karşılığında ödüllendirilebilir. Belli sayıda etkinliğe katılanlara artı bir ödül, vergisini erken ödeyenler için indirim gibi bir ödül puan sistemi de kurulabilir.

Özetle; blokzincir tabanlı akıllı şehir uygulamalarının artması, belediyecilik hizmetlerinin sadece daha akıllı biçimde icra edilmesinin ötesinde daha şeffaf, daha katılımcı bir yönetim anlayışına geçilmesini de beraberinde getirecek ve belediyelerin de yerel yönetimden, yerel yönetişim anlayışına geçmesinde başrol oynayacaktır.

II. OTURUM:

Şehir Yönetiminde Siber Güvenlik ve Güncel Yaklaşımlar

Orkan Aytulun

TradeFive / Alibaba Cloud Yönetim Kurulu Üyesi & CEO

1973 yılında İstanbul'da doğan Orkan Aytulun, ortaokul ve liseyi İzmir'de okudu. Lise dönemi boyunca İzmir Karşıyaka Spor Kulübü'nde basketbol oynadı. İzmir 9 Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Kamu Yönetimi Bölümünden mezun oldu. Çalışma hayatı 1997 yılında bir tekstil firmasında başlayan Aytulun, 1998 yılında Rifle - Calvin Klein grubunda bölge müdürü ve Türki Cumhuriyetler'den sorumlu yönetici olarak görev yaptı. 1999 yılında Superonline Ege Bölge Müdürlüğü'nde Satış Temsilcisi olarak işe başladı. 2. altı ayın sonunda Türkiye'deki en başarılı satıcı seçildi. 2002 yılında Superonline'da Kanal Satış Şefi görevini üstlendi. Aynı yıl AVEA' da Ege Bölgesi Bireysel Müşterilerden Sorumlu Yönetici olarak işe başladı. Yöneticiliğini gerçekleştirdiği Ege Bölgesi, kurumsalda en başarılı satış ekibi seçildi. 2009 yılında AVEA operasyondan sorumlu Türkiye Satış Müdürü pozisyonuna getirildi. 2011 yılında Millenicom' da Kurumsal Kanallar Satış Direktörü olarak işe başlayan Aytulun, 2013 yılında Vodafone' a Kurumsal Satış Geliştirme Kıdemli Müdürü olarak geçiş yaptı. 2015 yılından itibaren Alibaba.com ve Alibaba Cloud'un iş ortağı TradeFive'ın Yönetim Kurulu Üyesi ve Genel Müdürü görevini yürütmektedir. Fenerbahçe Spor Kulübü üyesi olan Aytulun evli ve bir çocuk babasıdır.

DİJİTALLEŞEN ŞEHİRLER

Dünyanın lider B2B e-ticaret platformu Alibaba.com, işletmelerin uluslararası pazarlara girişlerini kolaylaştırırken, Alibaba Cloud ise bu dijital dönüşüme şirketlerin kolay entegrasyonunu sağlayacak ve destek olacak altyapı ve çözüm hizmetlerini sunmaktadır. 40'tan fazla sektör ve 6 binden fazla ürün grubunun bulunduğu Alibaba.com üretici, tedarikçi, aracı ve distribütörleri dünyanın her yerinde bir araya getiren lider bir köprü konumundadır. Alibaba.com ve Alibaba Cloud'un Türkiye'deki tek yetkili iş ortağı TradeFive, her boyuttaki işletmenin ihtiyacı olan bulut bilişim hizmetleri ve katma değerli hizmetleri geliştirmekte, doğru e-ticaret yapabilme eğitimleri vererek, işletmelerin teknolojik entegrasyonunu kolaylaştıracak ve onları uluslararası pazarlara taşıyacak her türlü hizmeti sunmaktadır.

Alibaba ekosisteminde bulut servis sağlayıcısı olarak hizmet vermekte olan Alibaba Cloud aynı zamanda dünyadaki en büyük bulut servis sağlayıcıları arasında yer almaktadır. Dünya üzerinde milyonlarca kullanıcısı bulunan Alibaba Cloud, dijitalleşen dünyaya hızlı bir şekilde giriş yapılması, maliyet avantajı ve kolay adaptasyon sağlanması konularında şirketlere destek olduğu gibi artık toplumun her kesiminde teknolojik gelişmeleri hayata katmaktadır. Günümüzde şehirlere yönelik göç sonucu popülasyon artışı geleneksel yöntemlerle etkin bir yönetimi mümkün kılmamakla birlikte akıllı projeleri artık ihtiyaç haline getirmektedir. Hızlı ve kontrolsüz şehirleşme yerini 'Akıllı Şehir'lere bırakmaya başlamaktadır.

Alibaba Cloud'un çalışmalarından olan "Akıllı Şehirler" projesi; nüfus yoğunluğunun beraberinde getirdiği araç kalabalığı, trafik problemleri, altyapı sorunları, güvenlik sorunları, toplu taşıma ve eğitim sorunları sonucu şehir yönetimi aksaklıkları ve problemlerine destek olmak amaçlı hayata geçirilmiştir. Örnek olarak seçilen nüfus yoğunluğu yüksek şehirlerde (Hangzhou, Kuala Lumpur, Macau, Chongqing) başarı ile günlük hayata entegre edilmiş olan bu proje, şehrin beyni şeklinde çalışan bir karar alma ve harekete geçme teknolojisidir. Örnek şehirlerden olan Hangzhou şehri, Alibaba Grubu'nun 1999 yılında doğduğu şehirdir ve "Akıllı Şehirler" projesi ilk kez burada hayata geçirilmiştir. Günlük hayatın her noktasında yapay zeka ile iç içe olan Hangzhou şehri, kendi kendisini yönetebilen, akıllı teknoloji ile donatılmış bir şehirdir. Toplu taşıma kullanımından ödeme sistemlerine, trafik akışından alışverişe kadar hayatın her alanında zamandan tasarruf ve verimlilik ön plandadır.

Yapay zekanın başarılı yönetilmesi sonucu şehirlerde verimliliğin ve hayat kalitesinin artmasının yanı sıra günlük hayatta zaman kullanımı optimizasyonu ile sürdürülebilirliği arttırmak mümkün olmaktadır. "Akıllı Şehirler" projesinin bir şehre

entegre olması ile birlikte zaman kaybı, teknoloji ile engellenmekte ve karar alma mekanizması olan "City Brain" sistem içerisinde kararları hızlıca hayata geçirmektedir.

"Akıllı Şehirler" projesinin beraberinde getirdiği şehir yönetimini kolaylaştıran "City Brain" sayesinde, günlük hayatta olabilecek tehlikelere karşı önlemler alınmış durumdadır. Örneğin bir ambulans hastaya en hızlı şekilde ulaşmakta veya bir itfaiye aracı yangın alanına en kısa yoldan trafik ışığı optimizasyonu sayesinde ulaşarak müdahale edebilmektedir. Sistem içerisindeki veriler sayesinde en doğru müdahaleler gerçekleştirilerek hayatlar kurtarılmaktadır. Bunların yanı sıra toplu taşıma ve araç optimizasyonları sayesinde daha etkin bir ulaşım rotası çıkarılmakta ve bu sayede trafik probleminin ortadan kaldırılması hedeflenmektedir.

"Akıllı Şehir" projesi sayesinde şehirler kendi kendilerini yönetebilmekte, arka planda çalışan binlerce belki milyonlarca cihazdan gelen tüm verileri toplayıp analiz etmekte ve anlık aksiyon alabilmektedir. Şehirlerin dinamiğine uygun belirlenen yol haritaları sayesinde eldeki kaynaklar optimize edilerek, akıllı teknoloji hayatın bir parçası ve çözüm mekanizması haline gelmektedir.

"Akıllı Şehirler" projesinin karar alma mekanizması olan "City Brain" dışında Alibaba Cloud'un "Industrial Brain", "Agricultural Brain" ve "Aviation Brain" gibi endüstride, tarımda, üretimde ve havacılık sektöründeki uygulamaları ve projeleri sayesinde, hayatın her alanında yapay zekâ ve toplanan verilerin tüm olanaklarından yararlanarak hayatı kolaylaştırmak hedeflenmektedir.

Fatih Zeyveli

Beyaz.net Genel Müdürü

Mehmet Fatih Zeyveli: 1973 yılında Malatya'da doğdu. İlk, orta ve lise öğrenimlerinin ardından ODTÜ Elektrik-Elektronik Mühendisliği bölümünü bitirdi. Marmara Üniversitesi'nde asistan olarak görev yaptı. Yüksek Lisansını İTÜ Elektronik ve Haberleşme Yüksek Mühendisliği bölümünde tamamladı. 1997 yılında kurucu ortakları arasında yer aldığı BeyazNet firmasında halen Genel Müdür olarak görev yapmakta. Bilişim ve İnovasyon Derneği'nin Kurucu Başkanı ve halen Yönetim Kurulu Başkanlığını sürdürmekte. Çeşitli sivil toplum örgütlerinde aktif görevler yürütmektedir. Akıcı olarak İngilizce konuşabilmektedir. Evli ve 2 çocuk babasıdır.

YENİ NESİL SİBER OPERASYON

Bilişim güvenliğinde tehditler gün geçtikçe artıyor ve karmaşıklaşıyor. Özellikle veri sızıntıları yıldan yıla artıyor. İnsanların kişisel verileri toplu bir şekilde ele geçiriliyor, internete sızdırılıyor ve kötü amaçlar için kullanılıyor.

Mail hesap şifreleri, müşteri hesapları, üyelik bilgileri birçok farklı yöntemle ele geçiriliyor. Türkiye'nin de 49 milyon seçmen veri tabanı, adres, kimlik vs. bilgilerle beraber kaptırıldı ve bu bilgiler kişiler için ciddi bir tehdit oluşturuyor. Ayrıca siber saldırılar, siber ordular, endüstri hırsızlıkları gibi çok farklı bir dünya ile karşı karşıyayız. Siber savaşlar için geleceğin savaşları deniliyor; birçok ülke siber ordular kuruyor: Siber savunma, siber saldırı timleri oluşturuluyor.

Bilişim farklı alanlarda yaygınlaştıkça, tahmin edilemeyecek farklı siber tehditler yaşanıyor. Kalp pillerinin durdurulması, arabaların elektronik sistemlerine sızılması, akıllı oyuncakların ele geçirilmesi vb. yaşananlara baktığımızda şunu söyleyebiliriz: Saldırı yüzeyi çok genişledi. Artık sadece web sayfaları, yazılımlar ve veri tabanları risk altında değil; giyilebilir teknoloji cihazları, kameralar, reklam ekranları, turnikeler, plc cihazları, scada cihazları, otomasyon sistemleri, sensörler tehdit altında.

Uygulamalar artıyor akıllı sistemler yaygınlaşıyor, dijital işlem sayısı katlanarak artıyor. Yani milyonlarca işlem için milyonlarca log kaydı tutuluyor, milyonlarca güvenlik kontrolü yapılmaya çalışılıyor. Kısacası tehditleri tespit etmek için yapılan kontroller de zorlaşıyor. Trafik arttıkça trafiği izlemek de zorlaşıyor. Tüm risklere ve sıkıntılara rağmen teknoloji hayatı kolaylaştırıyor ve teknoloji olmadan yapamayız. Ayrıca şunun da farkında olmalıyız: güvenlik mümkündür. Farkında olmalıyız, dikkatli olmalıyız ve önlemlerimizi almalıyız. Uçtan uca bir güvenlik bakış açımız olmalı. Genişleyen saldırı yüzeyi ve artan veri trafiği "Yeni Nesil Güvenlik" çözümlerini zorunlu kılıyor. Güvenlik de gelişiyor ve farklılaşıyor. Tek bir çözümün tüm tehditleri engellemesi mümkün değil. Farklı farklı çözümlere ihtiyaç var.

Yeni nesil güvenlik çözümü olarak da aşağıdaki başlıklar sayılabilir:

Çok Katmanlı Güvenlik

Güvenlikte hattı müdafaa yoktur, sathı müdafaa vardır. O satıh da bütün sistemdir. İnternet girişi, web sunucu, mail sunucu, son kullanıcı her noktada farklı teknolo-

jiler kullanılarak zararlı olanlar farklı noktalarda engellenir. Bir önlemin yakalayamadığı bir tehditi bir başka önlem yakalar, bu sayede maksimum güvenlik sağlanır.

Güvenlikte Yapay Zeka Kullanımı

Yoğunluğun fazla olduğu alanlarda trafiği takip etmek zor. Özellikle saldırı anında tesbit edebilmek için ve saldırı sonrası analizinin sağlıklı yapılabilmesi için daha akıllı sistemlere ihtiyaç var. Makine öğrenmesi ve yapay zeka teknolojileri izleme, denetim, tehdit algılama ve alarm sistemlerini kapsayan otomatize siber savunma teknikleri için kritik öneme sahip bir altyapı olarak tanımlanır. Kullanıcı davranışlarını analiz edip sınıflandırarak iyi ve kötü aktiviteleri birbirinden ayırabilme, birbirinden bağımsız gibi görünen saldırı göstergelerini yorumlayıp korelasyon kurallarına göre alarm üretme gibi çeşitli kritik işlevlere sahip olan güvenlik yapay zeka uygulamaları, siber savunma ekiplerinin işini kolaylaştırdığı için önümüzdeki yılda önemi artacak olan güvenlik trendlerinden biri olarak tanımlanıyor.

Kimlik Bazlı Güvenlik (Identity Based Security)

Ağa bağlanan kullanıcı veya cihazların tanımlanmasını ve erişebileceği kaynakları sahip olduğu haklara göre belirlemeyi esas alan identity-based security mobil iletişim, bulut bilişim ve BYOD gibi yeni teknolojiler için yeni bir erişim kontrol sistemi sunan bir teknoloji. Bu teknoloji geleneksel güvenlik çözümlerinin uyguladığı IP ve Port bilgilerine göre erişim kontrolü yapmak yerine kullanıcı veya grup bilgilerine göre erişim kontrolü yaparak daha verimli bir denetim mekanizması sunmaktadır. Özellikle bulut servislerinin güvenliğinde geleneksel uygulamaların yetersiz kalması identity-based security sisteminin yaygınlaşmasına neden olacağı öngörülüyor.

Uç Nokta Güvenliği

Merkezi güvenlik bakışından, uç nokta güvenliğine bir dönüş var.
HTTPS ve TLS1.3 ile Riskleri Uç noktada yakalamak daha önemli hale geldi
Uç noktada daha akıllı çözümlere ihtiyaç var. EDR, MDR, Exploit Engelleme, Beyaz Liste gibi uç nokta güvenliği çözümlerinin önümüzdeki yılların ilgi çeken konuları arasında olması öngörülüyor. Uç nokta güvenliğiyle ilgili başlıca metodolojiler Endpoint Protection Platform (EPP) ve Endpoint Detection and Response(EDR) çözümleridir.

Uç Nokta Koruması (EPP), uç nokta cihazlarına kurulan ve zararlı yazılım saldırılarını önlemek, kötücül aktiviteleri tespit etmek ve olaya müdahale için verileri sağlamak gibi görevleri olan güvenlik platformudur. Saldırı göstergeleri olarak tanımlanan IOC'leri ve davranışsal analiz yöntemlerini kullanır. EPP, ayrıca yapay zekânın

yanı sıra tehdit avcılığı gibi insana dayalı denetimler ve tuzak saldırı tespit sistemleri gibi özellikleriyle de öne çıkmaktadır. Uç Nokta Algılama ve Yanıt (EDR), endpoint cihazlara ait kullanıcılar, dosyalar, çalışan prosesler, kayıt defteri, bellek ve ağ olayları gibi kritik verileri kayıt altına alıp lokal olarak uç nokta cihazında veya merkezi bir veri tabanında saklayan güvenlik platformudur. Güvenliği kırma girişimlerinin erken saptanması ve gerekli müdahalelerin yapılabilmesi için bu veriler bilinen saldırı göstergeleri ve davranışsal analiz yöntemleri uygulanarak analiz edilir.

Uç nokta güvenliğinin önemli işlevleri:

- Kullanıcı davranışlarını sınıflandırma
- Siber saldırılara karşı koruma
- Ağdaki iç tehditlere karşı koruma
- Veri kaybı önleme
- Ağ erişim kontrolü
- Entegre güvenlik duvarı
- Ayrıcalıklı kullanıcı kontrolü
- Zararlı yazılım bulaşmasına karşı koruma
- Diskler ve e-posta trafiği için şifreleme
- Uç nokta tespiti ve gerekli prosedürleri uygulama
- Beyaz liste oluşturarak çalıştırılacak uygulamaların kontrolü
- Baseline oluşturarak normal kullanıcı davranışlarından sapmaları tespit etme
- Filtreleme ve güvenli internet kullanımı sağlayarak web trafiğini kontrol

Yazılım Geliştirirken Güvenliği Sağlama (Devsecops)

Yazılım geliştirmede güvenliği projenin başından itibaren devreye almak esasına dayanan DevSecOps; yazılımın yanı sıra bulut, altyapı ve paydaşlarla yapılan çalışmalarda da uygulanması gereken bir modeldir. Önümüzdeki yıl DevSecOps trendinin daha çok ilgi çekeceği 2019 siber güvenlik tahminleri arasında. DevSecOps önemli işlevleri:

- Agile metodlarını uygulayarak kodların küçük parçalar halinde sık aralıklarla teslimi, böylece zafiyetlerin hızlıca kontrolünün sağlanması ve kalite güvencesi süreçlerine kod analizinin de dahil edilmesi,

- Geliştirmenin tüm aşamalarında otomatize testleri uygulamak,

- Tehditlerin büyük sorunlara dönüşmeden elimine edilebilmesi için güvenlik uzmanlarının desteğinin alınması,

- Yeni bir kod yazıldığında veya mevcut yazılımda değişiklik yapıldığında uyumluluk kontrollerini sağlamak, böylece raporlama ve denetim için her an hazır olmak,

- Düzenli güvenlik taraması, kod analizi ve sızma testi gibi süreçleri iyi bir şekilde işleterek her an tehditlere karşı hazırlıklı olmak,

- Yazılım ekiplerinin güvenli yazılım geliştirme açısından eğitilmesine destek vermek.

Güvenlik Operasyon Merkezleri (Security Operation Center)

Güvenlik Operasyon Merkezleri, kurumların güvenliklerini yüksek seviyede tutmak için saldırı olaylarını algılama, analiz etme, önleme ve müdahale etme gibi adımları uygulayarak sürekli izleme ve iyileştirme işlemlerini en verimli şekilde uygulamaya çalışan deneyimli bir ekip ve bu ekip için sağlanan teknolojik altyapı olarak tanımlanabilir. SOC ayrıca siber istihbarat aksiyonları, derinlemesine zararlı yazılım analizi ve devamlı olarak koruma ve tespit metodlarını geliştirmek ve iyileştirmekten sorumlu tehdit avcılığı işlevine sahip Threat Defense Operations(TDO) birimini de bünyesinde barındırır.

SOC'un Görevleri

- İzlenmesi gereken kritik bilişim sistemlerine ait logların analiz araçlarına gönderilmesini sağlayacak sorunsuz çalışan bir altyapı kurmak ve bunun için güvenlik izleme cihazlarını ve araçlarını en iyi şekilde yapılandırmak,

- Korelasyon kurallarını gözden geçirmek ve düzenlemek, saldırı göstergelerini araştırmak, alarmları analiz etmek, alarmların kritiklik ve etki derecesini belirleyerek aciliyetine göre sıralamak, saldırı kaynaklarını belirlemek gibi zararlı aktiviteleri tespit için gereken önemli süreçleri güvenlik izleme cihazlarının yardımıyla en iyi şekilde yönetmek,

- Olay müdahale politikalarını ve adımlarını etkili bir şekilde planlamak ve uygulamak,

- Gerçekleşen saldırılar ve alınan aksiyonlarla ilgili çalışmalar yaparak iyileştirme ve kurtarma süreçlerini yönetmek, adli analiz süreçlerine destek sağlamak,

- Her bir olay sonrası çıkarılması gereken derslerle ilgili çalışmalar yaparak güvenlik seviyesinin arttırılması, izleme ve tespit sistemlerinin ve güvenlik politikalarının elde edilen sonuçlara göre güncellenmesi gibi kritik işlemleri gerçekleştirmek.

Siber Tehdit İstihbaratı

Merkezi Siber İstihbarat Veri Tabanları, Siber güvenlik tehditleri, tehdit aktörleri, istismar kodları, zararlı yazılımlar, zafiyetler, IOC'ler (Indicator of Compromise), tehditin kapasitesi, arkaplanı/altyapısı, motivasyonu, amacı, kaynağı gibi kritik unsurlara ait verilerin toplanıp değerlendirilmesi ve bunların bir saldırıya dönüşemeden savunma mekanizmalarının harekete geçirilmesi gibi süreçleri kapsar. Saldırı göstergelerinin aciliyet, doğruluk ve önceliklerinin tanımlanması ve doğru bir şekilde değerlendirilebilmesi için bağlamın belirlenmesi önem taşımaktadır. Bunun için cevap aranması gereken sorular:

- Bütün bir tehdit olgusu içinde bu göstergenin rolü nedir?

- Bu göstergenin varlığı bir saldırının başlangıcına mı işaret etmektedir (keşif-tarama safhası mı yoksa istismar kodu yerleştirme-saldırı safhası mı)? Ya da sistemin ele geçirilmesine mi yoksa veri sızıntısına mı işaret ediyor?

- Söz konusu tehdit aktörü bu davranış türleri için biliniyor mu?

- Hedef alınan sistemin üzerindeki varlıklar kritik değere sahip mi?

- Söz konusu saldırı göstergesi ne kadar karmaşık?

- Bu girişimin ardındaki tehdit aktörünün motivasyonu nedir?

- Bu göstergeden önce ve sonra aynı varlık üzerinde gerçekleşen diğer aktiviteler nelerdir?

- Diğer varlıkların şu anki veya geçmişteki durumları nedir?

Red Team

Penetrasyon testlerinden ayıran başlıca özelliği kuruma ait bilgi varlıklarının analizini başka bir deyişle saldırı gerçekleşmesi halinde ne tür hassas verilerin sızdırılabileceğini ortaya çıkarmayı amaçlamasıdır. Sızma testi ile benzer yanları ise saldırganların gerçek hayatta kullandığı teknikleri ve yöntemleri kullanmasıdır. Bu taktik ve yöntemler sızma testinde olduğu gibi zafiyetlerin tek tek belirlenmesinde değil de kritik bilgilere ulaştıracak olan açıkları bulmak için kullanılır. Red Team'in görevleri arasında sosyal mühendislik testleri ve fiziksel güvenlik de yer alır. Red Team metodolojisinin en önemli unsuru bir saldırının ne kadar süre tespit edilemeden kurumda etkili olabileceği ve saldırılara yanıt sistemlerinin ne kadar başarılı olduğu gibi ölçümlerin de yapılmasına yardımcı olarak gerçek saldırılara yakın derecede bir değerlendirme sağlamasıdır.

- Kritik öneme sahip iş süreçlerine ait bilgi varlıklarına karşı risklerin ve zafiyetlerin belirlenmesi,

- Risklerin yönetiminin ve kontrolünün sağlandığı süreç eşliğinde gerçek saldırılara ait teknik taktik ve prosedürlerin (Techniques, Tactics and Procedures (TTPs)) simüle edilerek güvenlik seviyesinin testi,

- Kurumun karmaşık ve hedefli tehditleri tespit etme, yanıt verme ve önleme yeteneklerini ölçmek,

- Kurumun kendi blue team ve olay müdahale ekip üyeleri ile kordineli çalışarak atak etkilerini azaltıcı destek vermek ve kapsamlı bilgilendirmeler yapmak.

Tuzak Saldırı Tespit Sistemleri

Siber saldırı tespit sistemlerinin farklı bir yöntemi olarak sunulan ve kurum ağına gerçekleştirilen sızma ve atak girişimlerine ait bilgileri toplamak ve analiz etmek için yapılandırılmış olan Honeypot gibi tuzak saldırı tespit sistemleri, yeni nesil aktif savunma teknolojierinin bir parçası olarak değerlendirilmektedir. Tuzak saldırı sistemi sahte dosyalar, sahte giriş bilgileri, sahte ağ paylaşımları, sahte cache girdileri ve sahte uç nokta birimleri gibi tekniklerin yadımıyla saldırının kimden geldiği, saldırı teknikleri ve verilebilecek yanıtın ne olabileceği gibi konularda bilgi sağlar. Honeypot sistemleri saldırı yöntemlerinin belirlenmesi, kötücül yazılım tespiti ve analizi, adli bilişim, sıfırıncı gün açıklıklarının saptanması, kurum içi saldırganların

tespit edilmesi, botnetlerin tespiti ve web uygulamalarının açıklıklarının saptanması gibi çalışmalar için kullanılabilmektedir.

Çok Faktörlü ve Biyometrik Kimlik Doğrulama

Son zamanlarda ortaya çıkan SIM swap atağında siber suçlular kurban hakkında toplayabildikleri kadar veri toplayarak kişisel bilgiler, doğum günü, telefon numaraları ve güvenlik sorularına yanıt gibi çeşitli kritik bilgileri ele geçirirler. Bu bilgileri kullanarak GSM sağlayıcısından aynı hesap üzerinden yeni bir SIM kart aktive edilmesini talep edip kullanıcıya ait her türlü mesajlaşma, telefon konuşmaları, email, sosyal medya ve banka hesapları gibi kritik verilere erişim sağlarlar. Bu saldırı genellikle cep telefonuna gönderilen kod ile doğrulamayı esas alan iki faktörlü kimlik doğrulama sisteminin gücünü de kötü yönde etkilemektedir. Yüz tanıma gibi biyometrik kimlik doğrulama sistemlerinin de alternatif bir kimlik doğrulama yöntemi olmasını sekteye uğratması nedeniyle güvenlik uzmanları yeni bir arayış olarak davranışsal biyometri sistemine işaret etmektedir.

Sadece parola ile korumaya dayanan güvenlik sistemlerinin yetersiz kalması çok faktörlü kimlik doğrulama yöntemlerini öne çıkarıyor. Ancak her kurumun farklı farklı çok faktörlü kimlik doğrulama yöntemleri kullanması kullanıcıların süreci yönetmelerini zorlaştırıyor. Bu nedenle çok faktörlü kimlik doğrulama sistemlerinin bir standarda kavuşturulması gerekiyor. Önümüzdeki yılın MFA(Multi-Factor Authentication) kullanımını kolaylaştıracak ve zorunlu kılacak yöntemlerle gelmesi bekleniyor.

Zühtü Kayalı

Yönetim Sistemleri Danışmanı

Üniversite yıllarından başlamak üzere çok farklı alanlarda çalıştı. Ana çalışma alanı bilişim teknolojileri - yazılım geliştirme - donanım destek hizmetleri oldu. İlk öğrendiği programlama dili üniversite yıllarında (1981) Fortran 4 olmuştur. 2000'li yıllardan sonra yönetim sistemlerine yönelmiştir. Kalite yönetim sistemleri çerçevesinde dokümantasyon, İPK, karar verme, problem çözme, iç tetkik, kriz yönetimi gibi konularda eğitimler verilmiştir. 2005'den itibaren stratejik yönetim planlama danışmanlıkları verilmiştir. Bilgi güvenliği konusunda hem uygulama hem yönetim sistemi konusunda danışmanlıklar verilmiştir. Başlıca çalışılan kurumlar: İçişleri Bakanlığı, Emniyet Genel Müdürlüğü İstihbarat Bilgi İşlem, Maliye Bakanlığı Muhasebat ve Bütçe ve Mali Kontrol Genel Müdürlükleri, İş Bankasının iştirakleri, bazı banka iştirakleri ile İETT, İBB, Etimesgut, Keçiören belediyeleri ile farklı konularda çalışmalar yapılmıştır. Üniversiteler ile çalışılmıştır. Ulusal / uluslararası akreditasyona sahip belgelendirme kuruluşlarına bağımsız tetkikçilik hizmetleri devam etmektedir.

BELEDİYECİLİKTE SİBER GÜVENLİK RİSK ANALİZİ

Özet

Bu makalede bilgi güvenliği ve özellikle belediyecilik alanında yaşanan veya yaşanması muhtemel siber saldırılar çerçevesinde yapılan risk analizlerinin yönetimsel boyutu ele alınacaktır.

Giriş

Kurumlar, faaliyetlerini daha etkin yönetmek, kontrol etmek, sonuçlara odaklanarak maliyetleri kabul edilebilir sınırlar içine çekmek ve benzer güdülerle yönetim sistemlerini, kendileri için bir kurtuluş reçetesi olarak gördüler. İkinci dünya savaşından sonra yönetim sistemleri sonuçlara odaklanarak istatistiksel proses kontrol teknikleri ve benzeri araçlarla ürün ve hizmetlerinin beklenen şartları sağlamasını temin edecek yapısal değişikliklere gittiler ve tüm süreçlerini yönetim sistemleri gereksinimleri ile uyumlu hale getirdiler. Artık daha az fire, daha etkin maliyet yönetimi, daha yüksek karlılık, üretim ve hizmetin her aşama da kontrolü, öngörülebilir olumsuzluklara önceden tepki verebilme kabiliyeti belirleyici olmaya başladı.

Bu konuda başarıya ulaşan kurumlar, ayrıntılı bir dokümantasyon, görev/rol tanımları, talimatlar, planlı bakım/gözden geçirme, izleme metriklerinin belirlenmesi, başarım (performans kriterleri) ölçeklerinin oluşturulması, sonuçlarının değerlendirmesi ve kurulu sistemlerini sürekli tetkik ederek (dahili – tedarik/müşteri – harici) iyileştirdiler. Bu çalışmaların sonucunda "Toplam Kalite" (Total Quality) kavramı daha sık konuşulur oldu.

Ölçek ekonomisi, küreselleşme, üretimin üretici ülkelerin sınırları dışına kayması, şirketlerin yeni rekabet şartlarına bağlı olarak ulusal özelliklerinden sıyrılarak uluslararasılaşması, Birleşmiş Milletler, Uluslararası Çalışma Örgütü, AB müktesebatı, bankacılık sektörü için Basel kriterleri, Dünya Ticaret Örgütü gibi organizasyonların çevre, insan hayatı, iş dünyası üzerindeki düzenlemeleri (regülasyon), buna bağlı olarak ülkelerin kendi mevzuatını uyumlaştırma çalışmaları ile başlangıçta yalnızca kurumların kendi iç işleyişine bağlı olarak gelişen yönetim / yönetişim yapısı, artık kendi dışındaki (ulusal / uluslararası / bölgesel) gereksinimlere / şartlara uyumluluk göstermek zorunluluğu ortaya çıkmıştır.

Yine kendi içine odaklanmış, kendi faaliyetlerine / süreçlerine yönelik yapılanmış kurumlar, dağınık yapıları nedeni ile bilimsel, teknolojik, coğrafi, kültürel, sosyolojik, iklimsel etkileri de değerlendirmek durumunda kalmışlardır. Farklı ülkelerde,

bölgelerde üretim / hizmet sunumu, o bölgenin / ülkelerinin, demografinin şartları ve gereksinimleri, şirketlerin stratejik gelecekleri bağlamında riskleri de değerlendirmelerini zorunlu hale getirmiştir.

Yönetim sistemleri bu eğilimlere bağlı olarak kurumlardan çevre, iş güvenliği, hizmet, bilgi güvenliği, süreç, operasyonel, sosyal sorumluluk, süreklilik risklerini değerlendirmelerini ve risk analizleri sonucu çıkabilecek gereksinimlerinin beklentileri, plan ve uygulamalarını yönetim / yönetişim sistemlerine dahil etmelerini istemektedir.

Risk Yaklaşımı

Yönetim sistemleri tüm organizasyonlar için aynı / benzer şekilde uygulanabilecek bir risk yaklaşımının verilmesini amaçlamaz. Yönetim sistemleri, konusu, konumu, olanakları, altyapısı gibi parametrelere bağlı olarak kurumların kendi risk yaklaşımlarını oluşturmasını veya mevcut / uygun herhangi bir risk yöntemini / yaklaşımını seçebileceğini baştan kabul eder. Bilgi güvenliği yönetim sistemi için de tanımlanmış, tartışılmış, yayınlanmış, üzerinde çalışılan herhangi bir risk yaklaşımı tavsiye edilmez.

Kurumlar, bu makale özelinde belediyelere verdikleri hizmetlerin özellikleri, gereksinimleri, teknolojik / BT altyapılarının beklentileri bağlamında risk yaklaşımlarını belirlemek veya seçmek durumundadırlar. Siber ataklara / saldırılara / tehditlere / zayıflıklara bağlı olarak operasyonel / işletimsel bazda riskler değerlendirilebilir ve önlemler alınarak etkileri en aza indirgenebilir. Ancak yönetimin / yöneticilerin teknik yeterliliklere sahip olarak risk vektörlerini bilmesi, anlaması, alınan önlemlerin etkinliğini değerlendirmesi beklenemez. Bu durum dikkate alınarak risk yaklaşımı yönetimin sorumlulukları bakış açısından ayrıca ele alınması veya mevcut risk çerçevelerine dahil edilmesi beklenebilir. Yönetimin sorumluluklarına bağlı olarak risk çerçevesi aşağıdaki prensipleri içerecek şekilde formüle edilebilmelidir:

a. **Risk yönetimi değer yaratır ve yaratılan değerleri korur.**

Risk yönetimi hedeflere sürekli ulaşmayı ve performans artışını destekler.

> *Hedeflerin üst yönetimin ortaya koyduğu genel çerçeve ile uyumluluğu özellikle belirgin hale getirilmeli, üst yönetim hedefleri ile risk yönetimi / kriterleri / ölçekleri arasında bağlantılar açıkça tanımlanabilir olmalıdır.*

b. **Risk yönetimi kurumun tüm süreçlerinin ayrılmaz bir parçasıdır.**

Risk yönetimi kurumun diğer faaliyetlerinden bağımsız olarak kendi başına ayakta kalan bir aktivite değildir. Stratejik planlama ve proje ve değişim yönetimi süreçleri de dahil olmak üzere kurumun tüm süreçlerine dahil olmalıdır.

Kurumsal süreçler ve süreçler arasındaki ilişkiler bağlamında, süreç girdileri, süreç çıktıları, süreç işlemlerinin riskleri, risklerin gerçekleşmesi halinde muhtemel sonuçlar, muhtemel sonuçları meydana getirebilecek olasılıklar gerçekçi şekilde risk yaklaşımı içinde adreslenmelidir.

c. **Risk yönetimi karar verme faaliyetinin bir parçasıdır.**

Risk yönetimi karar vericilerin doğru karar vermesi için bilgilendirici seçenekler sunar, faaliyetleri önceliklendirir ve alternatif faaliyetlerin sonuçları arasındaki farklılıkları ortaya koyar.

Risk yaklaşımında, riskleri azaltmak veya kabul edilebilir seviyeye indirmek veya kabul edilebilir seviyede tutabilmek için maliyetler, ihtiyaçlar, gelecek projeksiyonlarına bağlı olarak gereksinim duyulan yatırımların kararını verecek üst yönetimin bu kararlarını etkileyecek içeriğin açık olarak ifade edilmesi gerekliliktir.

d. **Risk yönetimi belirsizliği açıklıkla işaret eder.**

Risk yönetimi belirsizliği ve belirsizliğin doğasını ve nasıl ifade edilebileceğini açıklıkla ele alır.

Belirlenmiş risklerin tamamen anlaşılabilir olması mümkün değildir. Anlaşılabilir olması veya tamamen açık olması onun risk olmaktan çok bir faaliyet olarak yapılandırmasına neden olabilirdi. Risk ifadeleri kurumların mevcut durumlarının bir belirsizliğinin fonksiyonu olması nedeni ile üst yönetimlere apaçık şekilde anlatılmasını gerekli kılar. Alınan kararların, yapılan yatırımların hesap verilebilirliği veya toplamsal paydaşlara açıklanabilmesi, sonuçların kabul edilebilirliğinin garantisi olacaktır.

e. **Risk yönetimi sistematik, yapılandırılmış ve zamansaldır.**

Risk yönetimine sistematik, zamansal ve yapılandırılmış bir yaklaşımla etkin, karşılaştırılabilir sonuçlar elde edilir.

Risk değerlendirmeyi yapan / uygulamasından sorumlu birimlerin, bölümlerin hesap verilebilirliği, sonuçların karşılaştırılabilirliği açısından zamansal olmalı ve bu risk planlarında açıkça taahhüt edilmelidir.

f. **Risk yönetimi uygun olan en iyi bilgiyi temel alır.**

Risk yönetimi sürecinin işletilmesi için girdi olan veriler geçmiş veriler, deneyim, paydaş geri beslemeleri, gözlem, tahmin ve uzman görüşleri gibi bilgi kaynaklarına dayanır.

Bilgi kaynakları eğer uzmanlaşmış bir içeriğe sahip ise yöneticiler için bir özet ile açık hale getirilmelidir.

g. **Risk yönetimi şeffaftır ve her şeyi kapsar.**

Paydaşların ve her seviyedeki karar vericilerin uygun ve zamanında katılımıyla risk yönetim sistemi her zaman organizasyonla uyumlu ve güncel kalmalıdır.

Risk yaklaşımında özellikle belediyeler için paydaşların da uygun şekilde temsil edilmesi ve risk kriterleri belirlenirken bakış açılarının değerlendirilmesi ele alınmalıdır.

h. **Risk yönetimi dinamik, tekrarlı ve değişime duyarlıdır.**

Risk yönetimi sürekli olarak değişikliği algılar ve tepki verir.

Düzenli olarak riskler yöneticilerin de içinde olacağı toplantılarda değerlendirilmelidir. Alınan kararlara yöneticilerin katılımı sağlanmalı, sonuçların paylaşılmasında / dağıtılmasında ortak irade inşa edilmelidir.

SONUÇ

Yukarıda ifade edilen çerçeve içinde belediyelerin siber güvenlik kapsamında kurdukları risk yönetiminin belli başlı yönetimsel parametreleri aşağıya çıkarılmıştır:

1. Risk Çerçevesi (Framework)

Organizasyon ilgili tüm tarafları içine alacak, bilimsel, teknolojik, altyapısal, toplumsal vb. tarafları da içine kapsayan bir "Risk Değerlendirme Platformu" oluşturmalıdır. Risk yönetimini yalnızca eknik bir faaliyet olarak görmemeli, riske maruz kalabilecek veya etkilenebilecek belirlenebilmiş olan ilgili tüm tarafları içermelidir.

2. Risk Değerlendirme – İşleme Süreci

Risk değerlendirme / İşleme ile ilgili süreçler, prosedür veya politikalar yalnızca teknik bakış açısını içermemeli, yasal şartları, belediyelerin stratejik yönlerini, gelecek vizyonlarını, bütçe ve insan kaynağı gibi gereksinimlerini de içerecek şekilde genişletilmelidir.

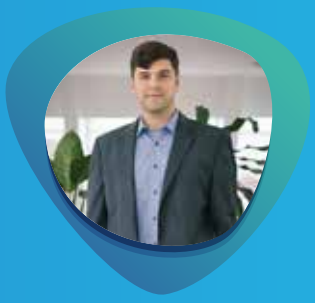
3. Tehdit Analizi

Bilgi güvenliğinde tehdidin kaynağı sektöre, kurumun faaliyetlerine ve sorumluluk alanlarına göre değişkenlik gösterir. Mevcut şartlarda, tetkiklerde karşılaştığımız durumlarda "tehdit kaynağı" çok fazla değerlendirilmemektedir. Ancak belediyecilik hizmetlerinin mahiyeti, sonuçların vahameti göz önüne alındığında belediyecilik hizmetlerine yönelik bilgi güvenliği risklerinde "tehdit kaynağı" özel olarak değerlendirilebilir. Aşağıdaki başlıklar tehdit analizi için kontrol edilmelidir:

- Sistemi ve belediyeleri ilgilendiren, kritik olarak bilinen veriler açıkça tanımlanmalıdır.
- Tehdit olabilecek, kritik varlıkları, verileri etkileyebilecek saldırı / atak kaynakları belirlenmeli ve önceliklere bağlı olarak seçilmelidir.
- Saldırı kaynaklarının etkilerini azaltmak için güvenlik kontrolleri tanımlanmalı ve gereksinimler belirlenerek tedarik şartları değerlendirilmelidir.
- Tehditlerin kategorize edilmesine bağlı olarak sonuçları analiz edilmelidir.

KAYNAKLAR:

- OGEC GRC TECHNOLOGY GUIDE – 2011
- TS ISO/IEC 27001:2013. Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği
- BSI ISO 31000:2018. Risk Management – Guidelines
- NIST. Veri Merkezli Sistem Tehdit Modelleme Rehberi (SP-800 154)



Bilgin Metin

Bağımsız ISO 27001 Tetkikçisi – Danışman – Yönetim Sistemleri Eğitmeni

Bilgin Metin ilk olarak İstanbul Teknik Üniversitesi, Elektronik Haberleşme Müh. Bölümünden Lisans derecesi aldı. Daha sonra Armada Bilgisayar A.Ş.'de CISCO ürünleri için bilgisayar ağları ve ağ güvenliği projeleri tasarımı-kurulumu konularında çalıştı. Sırasıyla Boğaziçi Üniversitesi, Elektrik-Elektronik Müh. Bölümünden yüksek lisans ve doktora derecelerini aldı. Bu dönemde özel sektörde veri haberleşmesi, LAN, WAN ve ağ güvenliği sistemlerinin tasarımı, desteği ve kurulumu konularında danışman olarak hizmet etti. 2007 yılında Boğaziçi Üniversitesi, Yönetim Bilişim Sistemleri Bölümünde Yardımcı Doçent olarak çalışmaya başladı. 2014 yılında doçent ünvanını aldı ve şu an aynı bölümde görevine devam etmektedir. Bilgi ve haberleşme sistemleri için elektronik devre tasarımı, siber güvenlik, bilgi güvenliği ve bilgi teknolojileri yönetişimi konularında çalışmaktadır. Uluslararası konferans ve dergilerde 80'den fazla yayını çıkmıştır. Ayrıca şu ana kadar birçok ulusal ve uluslararası konferansın düzenleme kurulunda yer almıştır. 2014 yılında YBS 2014 (Yönetim Bilişim Sistemleri Konferansı), 2012-2017 arası ELECO (Elektrik Elektronik Mühendisliği Konferansı) ve 2016 yılında ECIS 2016 (European Conference of Information Systems) örnek olarak verilebilir. ISACA (Information Systems Audit and Control Association) İstanbul Chapter ve Türkiye Bilişim Derneği İstanbul Şubesi yönetim kurulunda görev almaktadır.

Ayrıca şu anda BÜSİBER (Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi) Projesi yöneticiliği görevini de yürütmektedir.

KURUMSAL SİBER RİSK YÖNETİMİ

Günümüz dijitalleşme çağında çoğu kuruluş dijitalleşme stratejileri kapsamında daha fazla veri ve bilgiyi siber uzayda tutmaya başlamaktadır. Özellikle bilginin güç olduğu günümüz toplumunda, önemli ve hassas bilgiler üreten ve bu bilgiler ile çalışan kuruluşlar siber saldırganların hedefi haline gelmektedir.

Siber tehditler her büyüklükteki kuruluş için çeşitli zorluklar ortaya çıkaran bir risktir. Siber tehditler, kurumsal risk yöneticilerinin genelde karşılaştıkları risklerden daha farklıdır. Tipik kurumsal risklerden farklı olarak, siber tehditler, savunmalar uygulandıkça aynı hızda taktik geliştirip değiştirebilen akıllı failler tarafından oluşmaktadır (Marotta ve McShane, 2018). Bu sayede geçmiş verilerin gelecekteki saldırıları öngörümlemek için kullanılması engellenir. Ayrıca, siber riskler asimetrik bilgi, ilişkili kayıp ve bağlantılı güvenlik sorunları ile karşı karşıya kalmaktadır (Marotta vd., 2017; Shetty vd., 2018). Allianz'a göre (2015) siber suçlar global ekonomiye yılda 445 milyar dolara mal olmaktadır. Bu rakamın yaklaşık yarısını dünyanın en büyük ekonomileri kapsamaktadır ve gelecek yıllarda bu rakamın artması beklenmektedir.

Siber saldırganlar amaçlarına ulaşabilmek için tek bir sefer başarılı olmaları yeterken, kuruluşların saldırıları engelleyebilmek için her defasında başarılı olmaları gerekmektedir. Bu durumda kurumsal risk yöneticilerine büyük sorumluluk düşmektedir. Sigorta temelli risk engelleme stratejileri bize riskin tamamen yok edilemediğini çok öncesinden göstermiştir. Tamamen yok etmek yerine, finansal kanallar ile oluşabilecek zararın hafifletilmesine odaklanılmıştır, aynı zamanda riskin sigorta yolu ile başka bir tarafa transfer edilmesi sağlanmıştır. Yine de sigorta tek başına riski azaltmaya yetmemektedir. Günümüz bilgi ve iletişim teknolojilerinde kurumsal riski azaltmak için en uygun model; kavrama, azaltma ve transfer etme süreçlerine teknoloji, iş süreçleri ve sigortayı entegre eden risk yönetim yaklaşımıdır. İşte risk yönetimi, bir kuruluşun karşı karşıya olduğu risk faktörlerini tam anlamıyla kavramak ile başlamaktadır (Siegel, Sagalow ve Serritella, 2002).

Literatürde bulunan tanımlardan ve ISO 27001 gibi çeşitli risk yönetimi standartlarından yola çıkarak siber güvenliğin veya bilgi güvenliğinin sadece teknik bir ihtiyaç değil aynı zamanda sosyal ve örgütsel bir ihtiyaç olduğunu kavramaktayız

(Werlinger vd., 2009; Singh vd., 2013). Teknik faktörler; yeni teknolojilere yatırım, kaynak ayırma ve yazılım ve donanım bileşenleri satın alma gibi faktörleri içermektedir (Somroo vd., 2016). Sosyal faktör çalışanların farkındalığı, eğitimi ve davranışlarının incelenmesini içerirken, örgütsel faktör güvenlik politikaları geliştirmek

ve bu politikalarının uygulanıp uygulanmadığının kontrol edilmesi ve örgüt içi uygunluğun hayata geçirilip geçirilmediğinin kontrolünü içermektedir (Chang ve Lin, 2007). Kosub'un (2015) yaptığı çalışmada literatürdeki diğer çalışmalardan ve ISO 27005 bilgi güvenliği risk yönetimi standardından derlediği basit bir kurumsal siber risk yönetim sürecinin aşamalarını aşağıdaki gibi tanımlamıştır:

1. Risk Tanımlaması

Bu aşama, firmanın iş modelini, hedeflerini ve değerlerini belirlemek ve kavramak, iş için bilgi teknolojilerinin (BT) uygunluğunu belirlemek ve son olarak BT güvenliği seviyesinde karar kılmak ile başlayıp, alttan-üste veya üstten-alta yöntemlerinden birisini kullanarak tüm siber risklerini belirlemek ile sonuçlanmaktadır.

2. Risk Değerlendirme ve değerleme

Riskin değerlendirilmesi çoğunlukla risklerin sayısallaştırılması ile mümkün olmaktadır ister kalitatif ister kantitatif yollarla olsun. Riskin sayısallaştırılması ise en basit şekilde bir risk olayının gerçekleşme olasılığı ile gerçekleşmesi halinde yaratacağı etkinin belirlenmesi ile gerçekleşmektedir. Bunu yapmanın en basit yöntemi ise bir risk matrisi oluşturmaktır. Bu yöntemin yanı sıra, sürekli gelişen bilgi ve iletişim teknolojileri ve daha entegre örgüt yapılarıyla ortaya çıkan karmaşık yapının risklerini daha iyi değerlendirebilmek için çok sayıda farklı risk değerlendirme yöntemi bulunmaktadır.

3. Riske Yanıt

İlk iki aşamada tanımlanmış ve sayısallaştırılmış olan bu riskleri öncelik sırasına koyarak, risklere verilebilecek 4 farklı cevap bulunmaktadır:

a. Riskten kaçınma (Örneğin, kötü koşullarda inşaatın durdurulup bu sebepten oluşabilecek risklerden kaçınmak)

b. Riski azaltma (Firewall kurmak)

c. Riski transfer etmek (Siber güvenlik sigortası yaptırmak)

d. Riski kabul etmek (Düşük etkili ve olasılıklı riskler için tercih edilebilir)

4. Risk Kontrolü

Bu aşamada, tanımlanmış olan riskler ve bu risklere ilişkin geliştirilen yanıt mekanizmalarının uygunluğu belirli aralıklarla kontrol edilmelidir. Yeni riskler ortaya çıkabilir veya öncesinde uygulanmış olan yanıt mekanizmalarında değişiklikler yapılabilir. Bu aşama, aynı zamanda belirli zamanlarda sızma testleri ve siber çözümlerin açıklarının testleri gerçekleştirilerek gözden kaçmış olan açıkların tespiti sağlanmaktadır.

5. Risk Kültürü ve Yönetimi

En güvenli sistem bile en zayıf halkası kadar güçlüdür sözünden yola çıkarak, diğer aşamalarda kuruluşun güvenliğinin sağlanması için yapılanlar ancak çalışanların farkındalığı ve örgütsel bir güvenlik kültürünün gelişmiş olması ile başarılı olabilir. Bu sebeple bu aşamada, firmalar çalışanlarının farkındalığını arttırmak için eğitimler düzenleyip örgütsel güvenlik kültürü geliştirmeyi amaçlamaktadır. Son olarak da iş devamlılığı planının oluşturulması da bu aşamada yer almaktadır. Siber riskler, diğer kuruluş risklerinin yanında eksik değerlendirilmesi ve bilgi güvenliğinin artık yasal gerekliliklerinin olması iyi bir siber risk yönetimi ihtiyacını arttırmaktadır. Bu anlamda yapılacak çalışmalarının değeri ve önemi ortaya konulmaktadır.

KAYNAKLAR

Allianz, 2015, Allianz Risk Barometer 2016-Top Risks in Focus: Cyber Incidents. Retrieved from http://www.agcs.allianz.com/insights/expert-risk-articles/top-risks-in-focus-cyber-incidents/

Chang, S. E., & Lin, C. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438–458

Kosub, T. (2015). Components and challenges of integrated cyber risk management. Zeitschrift für die gesamte Versicherungswissenschaft, 104(5), 615-634.

Marotta, A., & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. Risk Management and Insurance Review, 21(3), 435-452.

Marotta, A., F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, 2017, Cyber-insurance Survey,Computer Science Review, 24: 35-61.

Shetty, S., M. McShane, L. Zhang, J. P. Kesan, C. A. Kamhoua, K. Kwiat, and L.L. Njilla,2018, Reducing Informational Disadvantages to Improve Cyber Risk Management,Geneva Papers on Risk and Insurance-Issues and Practice, 43(2): 224-238.

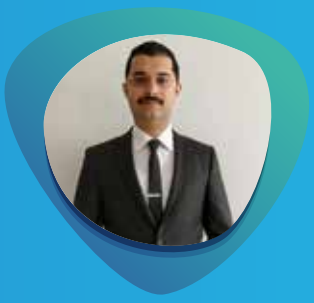
Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-risk management: technical and insurance controls for enterprise-level security. Information Systems Security, 11(4), 33-49.

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ISM) practices: lessons from select cases from india and germany. Global Journal of Flexible Systems Management, 14(4), 225–239

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security, 17(1), 4–19

* Bu yazı Meltem Mutlutürk'ün katkılarıyla hazırlanmıştır.



Onur Aktaş

Bilgi Teknolojileri ve İletişim Kurumu Siber Güvenlik Uzmanı

2010 senesinden beri siber güvenlik alanında çalışma yapmakta olan Onur AKTAŞ, güvenlik testleri, zafiyet tespiti, sömürü geliştirme konularında uzmanlaşmıştır. Onur AKTAŞ Gazi Üniversitesi Bilgi Güvenliği Mühendisliğinden yüksek lisansını tamamlanmış, Hacettepe Üniversitesinde Bilişim Hukuku yüksek lisansına ve Bilgisayar Mühendisliği doktorasına devam etmektedir.

AKILLI BELEDİYECİLİK VE SİBER SALDIRILAR

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması" başlıklı 4. eylem maddesi uyarınca kurulmuştur.

USOM, ülkemizde siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması adına kurulmuş olup, internet aktörleri, kolluk güçleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişim ve koordinasyon USOM vasıtasıyla gerçekleştirilmektedir. USOM siber güvenlik olaylarına yönelik alarm, uyarı, duyuru faaliyetleri yapmakta, kritik sektörlere yönelik siber saldırıların önlenmesinde ulusal ve uluslararası koordinasyonu sağlamakta ve ulusal siber güvenliği sağlama adına çeşitli faaliyetler yürütmektedir.

Siber saldırılar özellikle kritik özel sektör ve kamu kurumlarımıza yönelik önemli tehditlerden biridir. Bilişim alt yapılarında kullanılan siber güvenlik çözümleri, doğru yönetildiği takdirde başarılı önlemler alınabilmektedir. Öyle ki yapılan bazı araştırmalar içerisinde, yakın zamanda güvenlik duvarı gibi sistemleri atlatmanın tek yolunun %99 ihtimalle insan hatalarından kaynaklanacağı bilgisi yer almaktadır [1]. Bununla birlikte sistemlerin karmaşık olması, düzenli olarak değişmesi, bilişim altyapısında çok fazla sistemlerin bulunması, yönetim zorluğu ve insan hatası gibi çeşitli faktörler bilgi güvenliği ihlallerine sebebiyet verebilmektedir.

Yapılan çalışmalar göstermektedir ki, siber saldırıların gerçekleştirilmesi için gerekli teknik bilgi birikimi ihtiyacı gün geçtikçe azalmakta ve siber saldırılar basit hale gelmektedir. Bunun, açık kaynak kodlu araçların çok fazla otomatik işlem yapması, internet kullanımının artması ve bilgiye erişiminin hızlanması gibi farkı nedenleri vardır. Güvenlik bakış açısıyla kurulmayan ve tespit etmesi kolay zafiyetler içeren sistemler büyük oranlarda, herkese açık yayınlanan araçlar veya basit saldırılar ile bilgi güvenliği ihlaline uğramaktadır. İnternetin düzenli olarak kötü niyetli kullanıcılar tarafından zafiyetli sistemleri bulmaya yönelik tarandığı ve zafiyetleri sistemlerin otomatik olarak ele geçirildiği bilinen bir durumdur. Günümüzde, hedef odaklı olmadan, otomatik olarak zafiyetli sistemleri tarayan kötü niyetli sistemlerin artacağını öngörmek oldukça kolaydır. Kamu ve kritik özel sektöre ait bilişim sistemlerine yapılan en önemli siber saldırılardan birisi hedef odaklı siber saldırılardır. Bu tür saldırılarda kötü niyetli kişiler bir kurumu hedef almakta, uzun süreli ve çoğunlukla üst düzey gizlilikle siber saldırılarını gerçekleştirmektedir.

İster hedef odaklı saldırılara isterse otomatik olarak zafiyet taramayan sistemler akıllı belediyecilikte kullanılan bilişim altyapıları için önemli riskler taşımaktadır. Özellikle yeni kurulan sistemlerin siber güvenlik bakış açısıyla inşa edilmesi gerekmektedir. Bir sistemin risklerini anlayabilmek için ilgili sistemi yakından tanımak gerektiğinden, akıllı belediyecilik konusunda bilgi birikimine sahip siber güvenlik mimarlarına ilgili projelerde ihtiyaç bulunmaktadır. Milyonlarca vatandaşımıza hizmet verecek akıllı belediyecilik alt yapısı ancak doğru bilgi birikimine sahip siber güvenlik mimarları, kritik sistemlerde kullanılan milli çözümler, siber güvenlik süreçlerinin tam olarak yürütülmesi, izleme-alarm sistemlerinin yapılandırılması, güvenlik bakış açısına sahip teknik bir ekip ve farkındalık seviyesi yüksek çalışanlar ile siber saldırılardan korunması mümkün olabilir.

Bu kapsamda USOM, ulusal siber güvenliğin sağlanabilmesi için belirlenen kritik sektörlere ve diğer sektörlere ait tüm alanlarda çalışmalarına 7/24 olarak devam etmekte ve akıllı belediyecilik sistemleri de dâhil olmak üzere, vatandaşlarımızı etkileyebilecek siber güvenlik riskleri önceliklendirerek analiz, takip ve duyuru işlemlerini sürdürmektedir.

---

[1] https://www.gartner.com/doc/2254717/brand-firewall-best-practice-enterprises (Erişim Tarihi; 31.01.2019)

Çağdaş Mersinlioğlu

Küçükçekmece Belediyesi Bilgi İşlem Müdürü

Çağdaş Mersinlioğlu, Yıldız Teknik Üniversitesi İnşaat Fakültesi Harita Mühendisliği bölümünü bitirdi. Bahçeşehir Üniversitesinde Kentsel Sistemler ve Ulaştırma Yönetimi üzerine yüksek lisans yaptı. İş Güvenliği Uzmanlığı, Proje Yönetim Uzmanlığı, Kamulaştırma Bilirkişiliği ve Kalite Yönetim Sistemleri üzerine eğitimler ve uzmanlık sertifikaları aldı. 2008-2011 yılları arasında İBB iştirak şirketlerinde ve belediyelere projeler uygulayan çeşitli özel sektör temsilcilerinde görev yaptı. 2011 yılı itibarıyla Küçükçekmece Belediyesi Bilgi İşlem Müdürlüğü'nde sırası ile kontrol mühendisliği ve teknik bakım şefliği görevlerinde bulundu. Halen Küçükçekmece Belediyesinde Bilgi İşlem Müdürü olarak görev yapmaktadır.

KÜÇÜKÇEKMECE, SİBER KAHRAMANLARINI ARIYOR

Akıllı Şehirlerde' de siber güvenlik kavramı belediyecilik yaklaşımları ile çok özdeşleşmiş olacak ki teknolojiler kadar hızlı tüketilmedi ve güncelliğini koruyor. Özünde bilginin güvenliğini sağlamak temeli üzerine kurulmuş olan bir terminolojidir. Hepimizin bildiği üzere bilgi, işlenmiş, analiz edilmiş veriye deniliyor. Peki veriyi korumak neden bu kadar önemli çünkü veri modern dünya çağın petrolü olarak nitelendirilmektedir. Mali ve marka değeri en yüksek şirketlerden olan Facebook, Google ve Whatsapp gibi örneklerden yola çıkacak olursak temelinde; veriyi doğru toplayan, güncelleyen, işleyen, yöneten ve paylaşan bir yapı üzerine kuruldukları görülmektedir. Biz yerel yönetimler olarak bu kadar kıymetli olan veriyi nasıl koruyabiliriz. İlk basamakta donanım ve yazılım teminleri ile fakat her donanım ve yazılımın zafiyetleri bulunmakta ve kamu ihale kurumu sitesinde tüm kurumların hangi donanım ve yazılım ürünleri ile çalıştığı çarşaf liste gibi yayınlanmaktadır. İkinci basamakta ise insan kaynağı var fakat alanında yetişmiş insan kaynağı bulunmak ve bunları kamu standartları içerisinde istihdam etmek çok zor olmaktadır. Bu nedenle potansiyeli olan gençlerin keşfedilmesini sağlayarak bunların iyi bir eğitim almasında destek olmak sonrasında özel sektör dinamizmi içerisinde istihdam edilmelerini sağlayarak hizmet satın almak mevcut koşullar içerisinde kullanılabilecek en iyi yöntem olarak görülmektedir. Tüm bu bilgiler ışığında ilgili ve keşfedilmeyi bekleyen gençlerin bulunması adına 81 ilde 81 Milli Siber Kahraman projesinin bir proje ortağı olarak "Küçükçekmece Siber Kahramanlarını Arıyor" sloganı ile yola çıktık. Önceliği daha dezavantajlı olduklarını düşündüğümüz meslek liselerine vererek Küçükçekmece' de konumlu bulunan 19 meslek lisemizin 11 tanesinde bilgi-

sayar programlama ve elektrik elektronik bölümleri olduğunu tespit ettik her ay program neticesinde 1 meslek lisemizde siber güvenlik söyleşileri düzenledik. Her okulda 100 civarında öğrencimiz ile söyleşilerimizi gerçekleştirdik. 13 ay boyunca devam eden proje kapsamında 1300 öğrencimizle siber güvenliğin temel terminlerini konuştuk ve sonrasında tamamına online sınavlar gönderdik.

Bilgisayar Programlama ve Elektrik Elektronik Bölümleri olan fakat öğrencilerin temel eğitimlerini alabileceği laboratuvar ortamı bulunmayan okullarımıza bilgisayar laboratuvarları kurduk.

İlgi duyan ve sınavlarda başarı olan ilk 15 öğrencimize eğitim öğretim dönemi sonunda Sefaköy Kültür ve Sanat Merkezinde 600 kişilik bir katılımla ödül töreni düzenledik. Bu sayede alttan gelen gençlerin bu konulara özenmesini teşvik etmeye çalıştık.

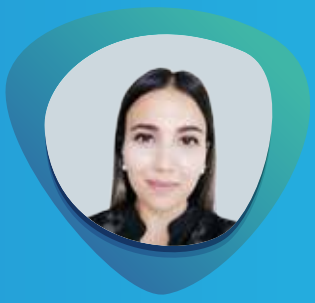
Belediye Başkanımız tarafından dereceye giren 15 adet lise 3. Sınıf öğrencimize 2 günlük bir siber güvenlik kampı hediye edildi. Küçükçekmece Uygulamalı Girişimcilik ve İnovasyon Merkezinde gerçekleştirilen 2 günlük kamp sürecinde gençlerimize üst düzey siber güvenlik eğitimleri verildi ve uygulamalı platformlar da yazılı, sözlü ve uygulamalı testler yapıldı. Bunların içerisinde başarılı olan 4 öğrencimiz Tüsidam tarafından bir üst basamak siber güvenlik eğitimlerine katılmaya hak kazandı.

Unutulmamalıdır ki dönüşüm yerelden başlar genele yayılır. Fakat dönüşümün tamamının kamu eli ile yapılması mümkün değildir. 1300 öğrenci ile başladığımız bir yolculukta 3. Basamağa yalnızca dört öğrencimiz geçebildi. Tüm süreçler tamamlandığın 1 ve/veya 2 Küçükçekmeceli öğrencimizin bu eğitimleri başarı ile tamamlayarak bu alanda bir kariyer planı çizmesini bekliyoruz. Yani 18 ay süren bir projede %0.001 binde bir oranla insan kaynağı yetiştirebiliyorsunuz. Bu

nedenle bu potansiyelli gençlerin bundan sonraki süreçlerde çok iyi bir üniversite eğitimi alması ve özel sektör tarafından cezbedici sosyal hakları ile istihdam edilmesi gerekmektedir. Özetle ülkemizin böyle bir dönüşüme ihtiyacı vardır ve bu kamu, sivil toplum kuruluşları, üniversiteler ve özel sektörün iş birliği ile ancak gerçekleştirilebilecektir.

III. OTURUM:

Kişisel Verilerin Yönetiminde Sorumluluklar ve Riskler



Cennet Alas Şekerbay

Kişisel Verileri Koruma Kurulu Uzmanı

Cennet Alas Şekerbay, 2009 yılında Selçuk Üniversitesi Hukuk Fakültesi'nde lisans eğitimini, 2013 yılında Gazi Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk A. B.D. Medeni Hukuk bilim dalında tezli yüksek lisans eğitimini tamamladı. 2011 yılından 2017 yılına kadar Kültür ve Turizm Bakanlığı Telif Hakları Genel Müdürlüğünde, 2017 yılından bu yana ise Kişisel Verileri Koruma Kurumunda uzman hukukçu olarak görev yapmaktadır.

5846 sayılı Fikir ve Sanat Eserleri Kanunu değişiklik çalışmaları ve ikincil mevzuat çalışmaları ile 6698 sayılı Kişisel Verilerin Korunması Kanunu ikincil mevzuat çalışmalarında yer almış olup eser sahibinin manevi hakları, koruma süreleri, kültür fonu kesintileri (copyright levy), reprography hakkı konularında yazılmış hakemli/hakemsiz makale ve tez çalışmaları bulunmaktadır. Ayrıca, Kişisel Verileri Koruma Kurumu'nun kuruluşundan itibaren ulusal mevzuatın uygulanması ve Kurumun tanıtılması konusunda eğitim, seminer ve paneller başta olmak üzere birçok çalışmada aktif olarak yer almaktadır.

BİR VERİ SORUMLUSU OLARAK, BELEDİYELERİN 6698 SAYILI KANUNDA TABİ OLDUĞU YÜKÜMLÜLÜKLER

I. GİRİŞ

Akıllı belediyecilik söz konusu olduğunda, akıllı şehirler, akıllı kentler gibi kavramlar sıkça karşımıza çıkmaktadır. Aslında sorun şu ki; ne şehirler, ne araçlar, ne kentler akıllıdır. Akıllı olma, insana özgü bir durumdur.

Ürün ve hizmetlerin geliştirilmesi, birçok işin araçlar/robotlar vasıtasıyla yapılmasını sağlayarak bireyin katlanacağı iş yükünün azaltılması ve böylece daha konforlu hayat standartlarının gerçekleştirilmesi, seri üretimin, verimliliğin artırılması, bunun yanı sıra ticari, ekonomik ve kamusal çıkarların gerçekleştirilmesi gibi amaçlarla günümüzde yoğun şekilde bireye ait veriler kullanılmaktadır. Özellikle otonom araçlar, yapay zekâlı robotlar ve nesnelerin interneti gibi teknolojilerin geliştirilmesi ve etkin şekilde kullanımı için bireye özgü durumlar, davranışlar, tercihler ve beğeniler gibi birçok bilginin işlenmesi ve analiz edilmesi gerekmektedir.

İşte tam bu noktada, karşımıza kişisel verilerin korunması kavramı çıkmaktadır. Anayasanın ikinci kısmında kişinin temel hak ve ödevleri düzenlenmektedir. Özel hayatın gizliliği de kişinin temel haklarından biridir. Bu hak, Anayasa'nın 20. maddesinde güvence altına alınmıştır. Teknolojik gelişmelerin temel hak ve hürriyetlere müdahale edebilmeyi kolay hale getirmiş olması ve bu durumun hukuki bir sorun olarak kendini göstermesi bu konuda yasal düzenlemeler yapmayı gerekli kılmıştır. 2010 yılında yapılan Anayasa değişikliği ile Anayasa'nın 20. maddesine bir fıkra eklenmiştir. Buna göre; "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 ilişkin esas ve usuller kanunla düzenlenir." Anılan hükme dayanarak, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu (Bundan sonra kısaca "6698 sayılı Kanun" olarak anılacaktır.) 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir.

Bu çalışmada, 6698 sayılı Kanun kapsamında kişisel veri, ilgili kişi, veri sorumlusu, veri işleyen gibi başlıca kavramlar açıklanarak kişisel verilerin korunması konusu ile ilgili olmak üzere belediyelerin gerçekleştirdiği faaliyetler kapsamında veri sorumlusu olarak belediyelerin yükümlülükleri konuları açıklanmaya çalışılacaktır.

Bu çalışma, Kişisel Verileri Koruma Kurumu tarafından hazırlanan ve kaynakçada belirtilen eserlerden derlenerek hazırlanmıştır.

II. BAŞLICA HUSUSLAR

6698 sayılı Kanunda, yalnızca gerçek kişilerin verilerinin korunması öngörülmektedir. Kanunda kişisel verisi işlenen gerçek kişiyi ifade etmek için "ilgili kişi" ifadesi kullanılmıştır. Korunması gereken kişi, düzenlemenin tanımlar kısmında açıkça belirtildiği üzere "gerçek kişi"dir.

Kişisel veri, belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgidir. Kişisel veriyi, kişisel olmayan verilerden ayırabilmek için temelde iki ölçütten yararlanıldığı söylenebilir. Buna göre, kişisel veriden söz edebilmek için, verinin bir gerçek kişiye ilişkin olması ve bu kişinin de belirli ya da belirlenebilir nitelikte olması gerekmektedir.

Kişisel verilerin işlenmesi ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder. Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder. Tüzel kişiler, kişisel verileri işleme konusunda gerçekleştirdiği faaliyetler kapsamında bizatihi kendileri "veri sorumlusu" olup ilgili düzenlemelerde belirtilen hukuki sorumluluk tüzel kişinin şahsında doğacaktır. Bu konuda kamu hukuku tüzel kişileri ve özel hukuk tüzel kişileri bakımından bir farklılık gözetilmemiştir. Mahalli idarelerden olan belediyelerin de kamu tüzel kişileri olduğu Anayasa'da düzenlenmektedir. Buna göre, belediyeler, 6698 sayılı Kanun kapsamında gerçekleştirdikleri veri işleme faaliyetleri bakımından veri sorumlusu olarak değerlendirilecektir. Ayrıca, veri işleyen kavramına değinmekte de fayda var. Veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişiler olarak tanımlanmaktadır. Bu kişiler, kişisel verileri kendisine verilen talimatlar çerçeve-

sinde işleyen, veri sorumlusunun kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği ayrı bir gerçek veya tüzel kişidir.

III. VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

Kanunun 3. maddesinde, veri sorumlusu "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlanmıştır. Veri sorumlusu, kişisel verileri bizzat işleyebileceği gibi veri işleme faaliyetini gerçekleştirmek üzere üçüncü bir kişiyi de yetkilendirebilir. Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen bu tür gerçek veya tüzel kişiler, Kanunun 3. maddesinin (1) numaralı fıkrasının (ğ) bendinde "veri işleyen" olarak adlandırılmıştır. Kanunda kişisel verilerin korunmasına ilişkin bazı yükümlülüklerin, veri sorumluları ile birlikte veri işleyenler için de getirildiği unutulmamalıdır. Veri sorumlusunun 6698 sayılı Kanun kapsamında düzenlenen başlıca yükümlülükleri aşağıdaki şekilde sayılabilir.

- Veri sorumluları siciline kayıt yükümlülüğü
- Veri işleme şartlarına uyum sağlama yükümlülüğü
- Aydınlatma yükümlülüğü
- Genel ilkelere uyum sağlama yükümlülüğü
- Aktarım usul ve esaslarına uyum sağlama yükümlülüğü
- Veri güvenliği yükümlülüğü
- Silme, yok etme, anonim hale getirme yükümlülüğü
- Başvurulara cevap verme ve Kurul kararlarına uyma yükümlülüğü

A. Veri Sorumluları Siciline Kayıt Yükümlülüğü

Kanunun 16. maddesine göre, Kişisel Verileri Koruma Kurulu (Bundan sonra kısaca "Kurul" olarak anılacaktır.) gözetiminde Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili (Bundan sonra kısaca "Sicil" olarak anılacaktır.) tutulacaktır. Yine bu maddeye göre kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce bu Sicile kaydolmak zorundadır. Ancak, Kanunun 16 ncı maddesinin (2) numaralı fıkrasında, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından Veri Sorumluları Siciline kayıt zorunluluğuna istisnalar getirilebileceği belirtilmiştir. Bu kapsamda, Kurul tarafından Sicile kayıt yükümlülüğünden istisna tutulan veri sorumluları şöyledir:

- Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler,

- 18/01/1972 tarihli ve 1512 sayılı Noterlik Kanunu uyarınca faaliyet gösteren noterler,

- 04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanuna göre kurumuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler,

- 22/04/1983 tarihli ve 2820 sayılı Siyasi Partiler Kanununa göre kurulmuş siyasi partiler,

- 19/3/1969 tarihli ve 1136 sayılı Avukatlık Kanunu uyarınca faaliyet gösteren avukatlar,

- 1/6/1989 tarihli ve 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu uyarınca faaliyet gösteren Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler,

- 4458 sayılı Gümrük Kanunu uyarınca faaliyet gösteren Gümrük Müşavirleri ve Yetkilendirilmiş Gümrük Müşavirleri,

- Arabulucular,

- Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar.

Sicile kayıt başvurusu, aşağıdaki bilgileri içeren bir bildirim ile yapılacaktır:

- Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri,
- Kişisel verilerin hangi amaçla işleneceği,
- Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar,
- Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları,
- Yabancı ülkelere aktarımı öngörülen kişisel veriler,

- Kişisel veri güvenliğine ilişkin alınan tedbirler,
- Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

Bu bilgilerde herhangi bir değişiklik olması halinde, söz konusu değişikliklerin derhal Kuruma bildirilmesi gerekmektedir. Böylelikle, Sicilin güncelliğinin sağlanması hedeflenmiştir.

Ayrıca, Sicile ilişkin diğer usul ve esasları belirlemek üzere hazırlanan Veri Sorumluları Sicili Hakkında Yönetmelik, 30.12.2017 tarihli ve 30286 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir. Bu Yönetmeliğin amacı, 6698 sayılı Kanun gereğince Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak tutulacak olan Veri Sorumluları Sicilinin oluşturulması, idaresi ile Veri Sorumluları Siciline yapılması öngörülen kayıtlara ilişkin usul ve esasları belirlemek ve uygulanmasını sağlamaktır.

18.08.2018 tarihli ve 30513 sayılı Resmi Gazetede yayımlanan "Sicile Kayıt Yükümlülüğünün Başlama Tarihleri" ile ilgili Kurulun 19.07.2018 tarihli ve 2018/88 sayılı kararı ile

- Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihinin 01.10.2018 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 30.09.2019 tarihine kadar süre verilmesinin kabulüne,

- Yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihinin 01.10.2018 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 30.09.2019 tarihine kadar süre verilmesinin kabulüne,

- Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olmakla birlikte ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihinin 01.01.2019 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 31.03.2020 tarihine kadar süre verilmesinin kabulüne,

- Kamu kurum ve kuruluşu veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihinin 01.04.2019 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 30.06.2020 tarihine kadar süre verilmesinin kabulüne karar verilmiştir.

Kişisel Verileri Koruma Kurulunca 6698 Sayılı Kanunun Geçici 1. maddesine (*) göre ilan edilen Veri Sorumluları Siciline kayıt tarihleri

Veri Sorumlulukları	Kayıt yükümlülüğü başlangıç tarihi	Kayıt için verilen süre	Kayıt için son tarih
Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları	01.10.2018	12 ay	30.09.2019
Yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları için	01.10.2018	12 ay	30.09.2019
Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumlulukları	01.01.2019	15 ay	31.03.2020
Kamu kurum ve kuruluşu veri sorumlulukları	01.04.2019	15 ay	30.06.2020

(*) GEÇİCİ MADDE 1- (2) Veri sorumluları, Kurul tarafından belirlenen ve ilan edilen süre içinde Veri Sorumluları Siciline kayıt yaptırmak zorundadır.

B. Veri İşleme Şartlarına Uyum Sağlama Yükümlülüğü

Kişisel verilerin işlenmesi, kanunun 3. maddesinde tanımlanmıştır. Buna göre; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem, kişisel verilerin işlenmesi olarak kabul edilmiştir. Kişisel verilerin işlen-

me şartları ise kanunun 5. maddesinde sayılmış olup buna göre aşağıdaki hallerden en az birinin bulunması durumunda kişisel verilerin işlenmesi mümkündür:

- İlgili kişinin açık rızasının varlığı,
- Kanunlarda açıkça öngörülmesi,
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- Verinin ilgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Kişisel verilerin işlenme şartları, yani hukuka uygunluk halleri, Kanunda sayma yoluyla belirlenmiş olup bu şartlar genişletilemez. Kişisel veri işleme, Kanunda bulunan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmamaktadır. Veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılması, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacaktır. Nitekim ilgili kişi tarafından verilen açık rızanın geri alınması halinde, veri sorumlusunun diğer kişisel veri işleme şartlarından birine dayalı olarak veri işleme faaliyetini sürdürmesi hukuka ve dürüstlük kurallarına aykırı işlem yapılması anlamına gelecektir. Bu kapsamda, veri sorumlusu tarafından kişisel veri işleme faaliyetinin amacının öncelikli olarak açık rıza dışındaki işleme şartlarından birine dayanıp dayanmadığı değerlendirilmeli, eğer bu amaç kanunda belirtilen açık rıza dışındaki şartlardan en az birini karşılamıyorsa, bu durumda veri işleme faaliyetinin devamı için kişinin açık rızasının alınması yoluna gidilmelidir. Kişisel verilerin işlenme şartları her bir kişisel veri işleme faaliyetinin amacının kanun bakımından hukuki dayanağını oluşturmaktadır. Kişisel veri işleme faaliyetinin amacında birden fazla sayıda kişisel veri işleme şartı bulunabilir. Örneğin, maaş bordrosu düzenlemek amacıyla çalışanların kişisel veri-

lerinin işlenmesinin hukuki dayanağı, kişisel veri işleme şartlarından sözleşmenin ifası ve veri sorumlusunun hukuki yükümlülüğünün yerine getirilmesidir.

C. Aydınlatma Yükümlülüğü

Kanun koyucu kişisel verileri işlenen ilgili kişilere bu verilerinin kim tarafından, hangi amaç ve hukuki sebeplerle işlenebileceği, kimlere hangi amaçlarla aktarılabileceği hususunda bilgi edinme hakkı tanımakta ve bu hususları, veri sorumlusunun aydınlatma yükümlülüğü kapsamında ele almaktadır. Buna göre veri sorumlusu, kanunun 10. maddesi çerçevesinde kişisel verilerin elde edilmesi sırasında bizzat veya yetkilendirdiği kişi aracılığıyla aşağıdaki bilgileri ilgili kişiye sağlamakla yükümlüdür:

- Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- Kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- 11. maddede sayılan diğer hakları.

10.03.2018 tarihli Resmi Gazetede yayımlanan "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ" ile aydınlatma yükümlülüğü kapsamında veri sorumlularınca uyulması gereken usul ve esaslar konusunda düzenleme yapılmış olup veri sorumlularınca aydınlatma yükümlülüğü yerine getirilirken bu hususlara da dikkat edilmesi gerekecektir.

Veri işleme faaliyetinin dayanağı ister ilgili kişinin açık rızası isterse 6698 sayılı Kanundaki diğer veri işleme şartları olsun her halde veri sorumlusunun ilgili kişiyi aydınlatma yükümlülüğü devam etmektedir. Diğer bir ifade ile ilgili kişi, kişisel verisinin işlendiği her durumda aydınlatılmalıdır. Bunun istisnası 6698 sayılı Kanunun 28. maddesinin (2) numaralı fıkrası ile düzenlenen durumlardır.

Veri Sorumluları Siciline kayıt yükümlülüğü bulunan veri sorumluları bakımından, aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilecek bilgiler, Sicile açıklanan bilgilerle uyumlu olmalıdır. Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine ya da onayına tabi değildir. Tek taraflı bir beyanla aydınlatma yükümlülüğü yerine getirilebilir. Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı ise veri sorumlusuna aittir.

Ç. Genel İlkelere Uyum Sağlama Yükümlülüğü

Kişisel verilerin hukuka uygun olarak işlenebilmesi için uyulması gereken genel ilkeler 6698 sayılı Kanunun 4. maddesinde düzenlenmiştir. Veri sorumluları tarafından kişisel veri işleme faaliyetlerinde her zaman gözetilmesi gereken bu ilkeler şöyledir;

- Hukuka ve dürüstlük kurallarına uygun olma,
- Doğru ve gerektiğinde güncel olma,
- Belirli, açık ve meşru amaçlar için işlenme,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

D. Aktarım Usul ve Esaslarına Uyum Sağlama Yükümlülüğü

Kişisel verilerin aktarılması, 6698 sayılı Kanunda iki başlık altında ele alınmıştır. Kanunun, 8. maddesinde kişisel verilerin yurtiçinde aktarılmasına ilişkin hükümlere, 9. maddesinde ise kişisel verilerin yurt dışına aktarılmasına ilişkin hükümlere yer verilmiştir. Veri sorumluları tarafından kişisel verilerin hukuka uygun bir şekilde aktarılabilmesi için belirtilen maddelerde yer alan usul ve esaslara uygun hareket edilmesi gerekmektedir. Aksi takdirde, aktarım Kanuna aykırı olacaktır.

1. Kişisel Verilerin Yurt İçinde Aktarılması

Kanunun 8. maddesi ile kişisel verilerin, üçüncü kişilere aktarılması düzenlenmektedir. Kanunun 3. maddesinin (1) numaralı fıkrasının (d) bendinde tanımlanan genel nitelikteki kişisel veriler ile 6. maddesinin (1) numaralı fıkrasında sayılan özel nitelikli (hassas) kişisel veriler bu madde kapsamında aktarılabilecek verilerdir. Kanunun 9. madde başlığı "kişisel verilerin yurtdışına aktarılması" olarak düzenlendiğinden 8. maddede belirtilen üçüncü kişiler yurtiçindeki kişiler olarak, yapılacak aktarım yurtiçinde gerçekleşecek veri aktarımı olarak anlaşılmalıdır.

Kişisel verilerin aktarılması veya devralınması eylemleri, veri işleme faaliyeti olarak tanımlandığından, burada da kişisel verilerin işlenmesi için ya Kanunun 5 inci maddesinin (1) numaralı fıkrası gereğince ilgili kişinin açık rızasının bulunması ya da Kanunun 5. maddesinin (2) numaralı fıkrası ve 6. maddesinin (3) numaralı fıkrasında düzenlenen veri işleme şartlarından en az birinin bulunması ve özel nitelikli veriler bakımından yeterli önlemlerin alınması gerekmektedir.

2. Kişisel Verilerin Yurt Dışına Aktarılması

Kanunun 9 uncu maddesi ile kişisel verilerin yurtdışına aktarılması düzenlenmektedir. Kişisel veriler, ilgili kişinin açık rızası ile yurt dışına aktarılabilir. Ayrıca, Kanunun 5 inci maddesinin (2) numaralı fıkrası ile 6 ncı maddesinin (3) numaralı fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;

- Yeterli korumanın bulunması,
- Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması,

kaydıyla ilgili kişinin açık rızası aranmaksızın da kişisel veriler yurt dışına aktarılabilir.

Yeterli korumanın bulunduğu ülkeler Kurul tarafından belirlenerek ilan edilir. Ancak henüz böyle bir belirleme yapılmamıştır. Bu nedenle, tüm ülkeler, yeterli korumanın bulunmadığı ülke statüsündedir ve açık rıza dışında bir veri işleme şartına dayanılarak yapılacak yurt dışına veri aktarımlarında, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması gerekmektedir.

Kurul, kişisel verilerin yurtdışına aktarılmasında yeterli önlemlerin bulunup bulunmadığı ile yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri durumunda;

- Türkiye'nin taraf olduğu uluslararası sözleşmeleri,
- Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,
- Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,
- Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,
- Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri değerlendirmek ve ihtiyaç duyması hâlinde ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.

Burada veri sorumlusu bakımından önem arz eden husus, her somut veri aktarım faaliyeti bakımından, aktarılan verinin niteliği, işlenme amaç ve süresi ile verinin aktarıldığı ülkede bulunan veri sorumlusu tarafından alınacak önlemler gibi hususlarda nitelikli bir tespitin yapılmasıdır.

Kurulun 02.04.2018 tarihli ve 2018/33 sayılı kararı ile yurtdışına veri aktarımında veri sorumlularınca hazırlanacak taahhütnamede yer alacak asgari unsurlar belirlenmiş olup 16.05.2018 tarihinde Kurumun internet sitesinde (kvkk.gov.tr) ilan edilmiştir.

E. Veri Güvenliği Yükümlülüğü

6698 sayılı Kanun kapsamında, veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerini dört temel başlıkta ele alabiliriz.

1. Teknik ve İdari Tedbirleri Alma

Kanunun 12. maddesinin (1) numaralı fıkrasına göre veri sorumlusu;

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- Kişisel verilerin muhafazasını sağlamak

ile yükümlüdür. Veri sorumlusu bu yükümlülüklerini yerine getirmek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Kişisel verilerin veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde ise söz konusu tedbirlerin alınması hususunda, veri sorumlusu bu kişilerle birlikte müştereken sorumludur. Dolayısıyla veri işleyenler de veri güvenliğinin sağlanması için tedbir alma yükümlülüğü altındadır. Buna göre, örneğin, veri sorumlusunun şirketine ilişkin kayıtlar bir muhasebe şirketi tarafından tutuluyorsa, verilerin işlenmesine ilişkin birinci fıkrada belirtilen tedbirlerin alınması hususunda veri sorumlusu muhasebe şirketiyle birlikte müştereken sorumlu olacaktır. Ayrıca, veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak Kurulun yetki ve görevleri arasında yer almaktadır. Bununla birlikte, Kurul tarafından belirlenecek asgari kriterler esas alınmak üzere sektör bazında işlenen kişisel verilerin niteliğine göre ilave tedbirlerin alınması da söz konusu olabilecektir.

Veri güvenliğine ilişkin alınacak önlemlerin her bir veri sorumlusunun yapısına, faaliyetlerine ve tabi olduğu risklere uygun olması gerekmektedir. Bu nedenle, veri güvenliğine ilişkin tek bir model öngörülememektedir. Uygun önlemlerin belirlenmesinde şirketin büyüklüğü veya cirosunun yanı sıra veri sorumlusunun yaptığı işin ve korunan kişisel verinin niteliği de önemlidir.

2. 6698 Sayılı Kanuna Uygunluk Denetimi

Veri sorumlusu, kendi kurum veya kuruluşunda, 6698 sayılı Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. Kanun hükmü ile denetimin veri sorumlusu tarafından yapılması gerektiğini öngörülmektedir. Veri sorumlusu bu denetimi kendisi gerçekleştirebileceği gibi, bir üçüncü kişi vasıtasıyla da gerçekleştirebilir.

3. Sır Saklama Yükümlüğü

Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri 6698 sayılı Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

4. Veri İhlal Bildirimi

İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

F. Silme, Yok Etme, Anonim Hale Getirme Yükümlülüğü

Kanunun 7. maddesi ile kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi düzenlenmektedir. Buna göre, hukuka uygun olarak işlenmiş olsa bile, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler, resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. Örneğin;

- Kişisel verileri işlemeye esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,
- Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olduğunun tespit edilmesi,

- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- İlgili kişinin, 6698 sayılı Kanun'un 11. maddesinin (1) numaralı fıkrasının (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verileri işleme faaliyetine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,
- Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi veya yok edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya 6698 sayılı Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikayette bulunulması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,
- Kanunun 5 ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması gibi hallerde kişisel verilerin silinmesi, yok edilmesi ya da anonim hâle getirilmesi gerekir.

İşlenmesini gerektiren sebeplerin ortadan kalktığı hallerde kişisel verileri silmek, yok etmek veya anonim hale getirmek veri sorumlusunun yükümlülüklerindendir. Bunun için ilgili kişinin başvurusu şart değildir. Bununla birlikte, ilgili kişinin kişisel verilerinin silinmesini veya yok edilmesini talep etme hakkı bulunmaktadır. Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin usul ve esasları belirlemek üzere hazırlanan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" 28.10.2017 tarih ve 30224 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir. Yönetmelik çerçevesinde kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

Yönetmeliğin 8. maddesinin (1) numaralı fıkrasına göre kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Yönetmeliğin 9. maddesinin (1) numaralı fıkrasına göre kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Son olarak Yönetmeliğin 10. maddesinin (1) numaralı fıkrasına göre kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir su-

rette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

G. İlgili Kişilerin Başvurularını Cevaplama ve Kurul Kararlarına Uyma Yükümlülüğü

6698 sayılı Kanunun 13. maddesinde veri sorumlusuna başvuru düzenlenmektedir. Buna göre, ilgili kişiler, 6698 sayılı Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir. Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusunca gereği yerine getirilir.

10.03.2018 tarihli ve 30356 sayılı Resmi Gazetede yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe göre veri sorumluları, ilgili kişiler tarafından yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla yapılan başvuruları niteliklerine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırmalıdır. Ancak, işlemin ayrıca bir maliyet gerektirmesi hâlinde, veri sorumlusu, Kurulca belirlenen tarifedeki ücretleri başvuruda bulunan ilgili kişiden isteyebilir. Veri sorumlusu, talebi kabul eder ise veya gerekçesini açıklayarak reddeder ise bu cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusu tarafından bu talebin gereği yerine getirilir. Başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde ise alınan ücret ilgiliye iade edilir. Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir.

Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda yapacağı inceleme sonucunda bir ihlalin varlığını tespit ederse, hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek, kararı ilgililere tebliğ eder. Veri sorumlusu, bu kararı, tebliğ tarihinden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirmek zorundadır.

KAYNAKLAR

Kişisel Verileri Koruma Kurumu: Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, KVKK Yayınları, Mart 2018, Ankara

Kişisel Verileri Koruma Kurumu: 100 Soruda Kişisel Verilerin Korunması Kanunu, KVKK Yayınları, Nisan 2018, Ankara

Kişisel Verileri Koruma Kurumu:Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), KVKK Yayınları, Ocak 2018, Ankara

Kişisel Verileri Koruma Kurumu: Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, KVKK Yayınları, Ocak 2018, Ankara

Kişisel Verileri Koruma Kurumu: Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, KVKK Yayınları, Mart 2018, Ankara

Mustafa Afyonluoğlu

Siber Güvenlik, E-Yönetişim ve E-Devlet Kıdemli Uzmanı

Mustafa Afyonluoğlu lisans ve yüksek lisansını Hacettepe Üniversitesi Elektrik-Elektronik Mühendisliği'nde tamamlamış olup ayrıca Bilişim Hukuku (Bilgi Üniversitesi) ve İyi Yönetişim (Boğaziçi Üniversitesi) alanlarında yüksek lisansları bulunmaktadır ve doktora tezi Ulusal e-Devlet Modelinde Kişisel Verilerin İmhası üzerinedir. Diğer akademik çalışmaları (Yale Üniversitesi'nde Sosyal Politikalar, Anadolu Üniversitesi'nde Hukuk) halen devam eden Afyonluoğlu, 27 yıl boyunca özel sektörde ve kamuda farklı seviyelerde yöneticilik görevleri yapmış, 5 tanesi Başbakanlık tarafından önceliklendirilen ve ödül alan 70'den fazla ulusal / uluslararası büyük ölçekli çalışmanın proje yöneticiliğini yürütmüştür. TÜBİTAK'da e-Dönüşüm Birim Yöneticisi ve e-Devlet Danışmanı, Ulusal e-Devlet Eylem Planı Koordinatörü, Başbakanlık e-Devlet Danışma Grubu Başkanı, Başbakanlık e-Devlet Uzmanı, AB Kapasite Geliştirme Kilit Uzmanı, göç ve e-Devlet alanında BM koordinatörü, Siber Güvenlik Kıdemli Uzmanı olarak gerçekleştirdiği görevlere ilaveten Türkiye Tek Temas Noktası ve Perakende Bilgi Sistemi'nin analiz ve tasarımında Bakanlık danışmanı olarak katkı sağlamıştır. Halen, kişisel veriler ve kamuda blok zincir uygulamaları üzerine çalışmaları devam etmekte olup ayrıca Arap Ekonomik Birliği Konseyi "Arap Dünyası Dijital Ekonomi Stratejisi"nin hazırlanmasındaki görevini sürdürmektedir.

E-DEVLET AÇISINDAN KVK UYGULAMALARI

ÖZET

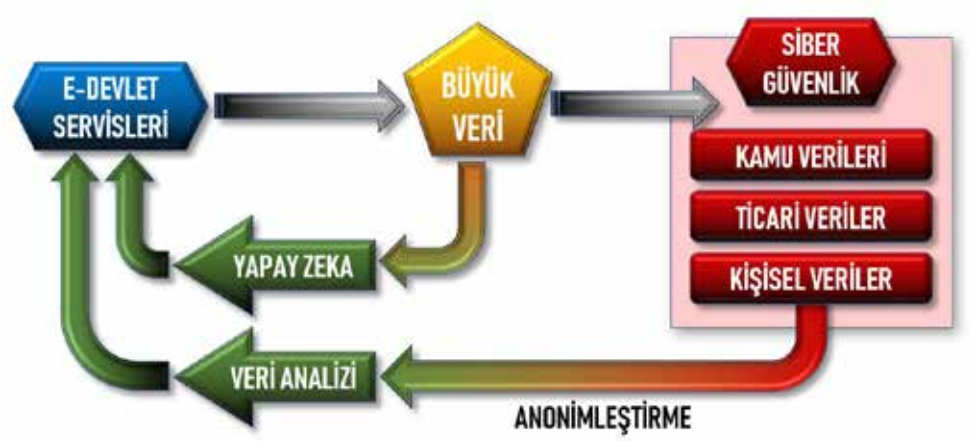
e-Devlet uygulamalarının yaygınlaşması ile birlikte, en büyük paydaş olan vatandaşa ait kişisel verilerin korunması da, özellikle elektronik dünyada önemli bir husus olarak karşımıza çıkmaktadır. Gerek bu konudaki mevzuat yükümlülüklerinin yerine getirilmesi, gerekse olası veri sızıntıları sebebiyle kurumsal itibarın zedelenmemesi için, mevzuatsal, idari ve teknik yükümlülüklerin net ve bütüncül olarak ele alınması ve bir politika çerçevesinde uygulamaya aktarılması gerekmektedir. Bu çalışmada, e-devlet hizmetlerinden doğan kişisel veriler esas alınarak, pratikte en çok karşılaşılan yanlış uygulamalar ve bunlara ilişkin çözüm önerileri ile süreci kolaylaştırıcı teknik yapılar ele alınmıştır.

Anahtar Kelimeler: e-Devlet, Kişisel Veriler, KVK, GDPR, Kişisel Verilerin Korunması, Veri Haritalama, Anonimleştirme, Yerel Yönetimler

1. GİRİŞ

Kamu kurumları tarafından vatandaşa (G2B), iş dünyasına (G2B) ya da diğer kamu kurumlarına (G2G) verilen elektronik hizmetler kapsamında gerek hizmeti sağlayabilmek için toplanan veriler, gerekse hizmet sonucu oluşan yeni veriler, yüksek hacimlerde veri oluşturmaktadır. Yeni alanlarda ekonomik katma değer sağlamak (açık veri), istatistiki çalışma yapmak veya hizmet kalitesini iyileştirmek için, oluşan bu veriden istifade edebilmek oldukça önemli hal almıştır. Özellikle bilgi işleme ve analiz kapasitelerinin gelişmesine ilaveten yapay zekâ gibi araçlara ait algoritmaların daha olgunlaşması, bu cazibeyi daha da arttırmıştır.

Oluşan bu büyük verinin yapay zekâ dünyasında, algoritmalara öğrenme girdisi olarak kullanılmasında ve bunun sonucunda daha nitelikli hizmetlerin ortaya çıkmasında veri gizliliği bakımından bir sakınca oluşmamaktadır. Çünkü mevcut veriler ifşa edilmemekte, paylaşılmamakta, sadece derin öğrenme sürecinde yapay zekânın olgunlaşması için gerekli olan sayısal değerlerin çözünürlüğünün (tutarlılığının) artmasında kullanılmaktadır. Bununla birlikte, ticari veriler, kamu verileri ve kişisel verilerden oluşan bu büyük veri havuzu ile birlikte verinin siber güvenliğinin sağlanması daha kritik bir husus olarak gündeme gelmektedir. Bir alt küme olan kişisel veriler bakımından bu havuzdaki verilerin korunması hem hassasiyet gerektirmekte hem de bu alandaki mevzuata uyum açısından (ticari verilerde ve kamu verilerinde olduğu gibi) birtakım yükümlülükler ve buna bağlı olarak cezai müeyyideler getirmektedir.



Bu havuzdaki verilerin anonimleştirilmesi sayesinde oluşan açık veri, yeni ekonomik faydalar sağlamak, istatistiki sonuçlar yayımlamak ve araştırma-geliştirme çalışmalarına altlık sağlamak bakımından oldukça değerli bir kaynaktır. Bu kapsamda yüksek fayda üretebilmek için anonimleştirme işleminin yapılması giderek daha büyük bir ihtiyaç olarak karşımıza çıkacak, üstelik bu işlemin hatasız yapılması (yani her koşulda ifşaya mahal vermemesi) ve hatta mümkün olduğunca veri fayda kaybının en az olmasına[1] yönelik baskılar artacaktır.

"e-Devlette Veri Döngüsü" (Şekil 1) olarak adlandırabileceğimiz bu süreçlerde hedeflenen faydaya ulaşabilmek için iki önemli başlıkta olgunlaşma ihtiyacı bulunmaktadır:

1. e-Devlet alanında yeterli olgunluğa ulaşmak ve bu vesileyle kaliteli (temiz, hatasız, eksiksiz ve güvenilir) büyük veri oluşturmaya başlamak,

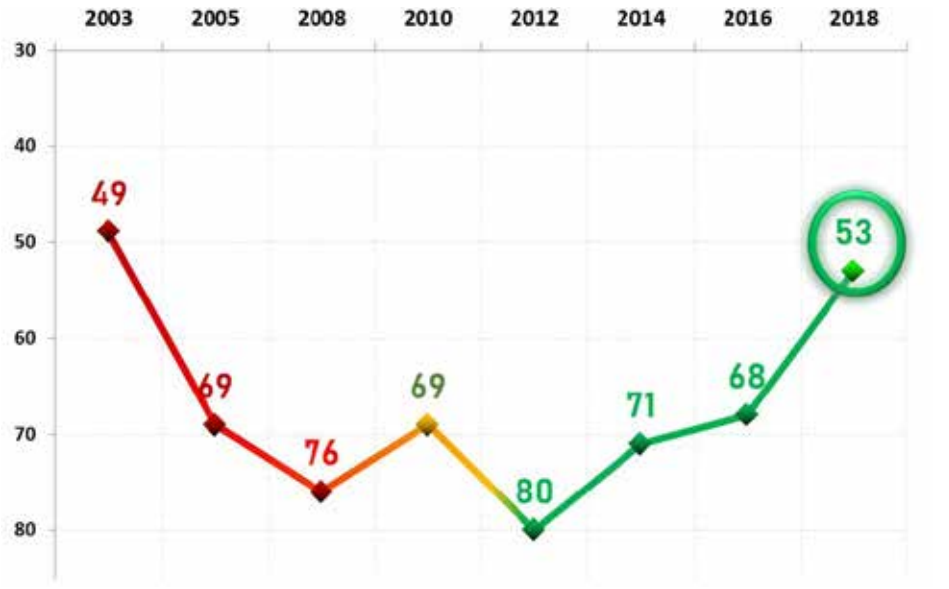
2. Bu verilerden istifade ederken özellikle kişisel veriler bakımından sağlıklı ve verimli anonimleştirme süreçlerini sağlayabilmek.

2. YEREL YÖNETİMLERDE KİŞİSEL VERİLER

Türkiye'de e-devlet açısından gelişmeler ele alındığında, özellikle Başbakanlık tarafından e-devletin en üst seviyeden koordinasyonunun ele alındığı (2008), uluslararası ölçümleme kuruluşları ile birebir çalışmaların ve yakın temasların başladığı (2012) dönemden itibaren, kamu kurumlarının sağladığı elektronik hizmetlerin çeşitlenmeye ve olgunlaşmaya başlaması ile birlikte Türkiye'nin e-devlet sıralamasında hızla yukarıya doğru tırmandığı görülmektedir.

1 Veri fayda kaybının minimum olması, ulusal mevzuat ile işaret edilen anonimleştirme seviyesini elde ederken anonimleştirmeden kaynaklı kaybın en düşük seviyede tutulmasıdır.

2003 yılından bu yana uluslararası alanda 16 kuruluş tarafından e-devlet ölçümleme çalışması[2] yapılmakla beraber bu çalışmalar arasında 193 ülke ile en geniş kesimi kapsayan, en uzun süredir[3] düzenli ve tutarlı olarak devam eden ve ölçümleme yöntemlerinin şeffaflığıyla en çok dikkate alınan çalışma Birleşmiş Milletler e-Devlet Olgunluk Ölçümlemesidir[4]. Şekil 2'de, bu ölçümlemelerde Türkiye'nin yıllar içerisindeki ilerlemesi görülmektedir.



Şekil 2 Birleşmiş Milletler e-Devlet Olgunluk Ölçümlemesi - 15 Yıllık Süreçte Türkiye'nin Sıralamadaki Yeri[5]

2 Uluslararası e-Devlet Ölçümleme Çalışmalarının Kıyaslaması ve Değerlendirilmesi, Afyonluoglu, M. Alkar, A. 2017, ECDG 17. Avrupa Dijital Devlet Konferansı, Çevrimiçi, http://afyonluoglu.org/PublicWebFiles/Papers/ECDG2017-Mustafa%20Afyonluoglu%20Ali%20Ziya%20Alkar.pdf, Erişim Tarihi: 18.01.2019

3 Birleşmiş Miletler e-Devlet Ölçümleme Çalışma Raporları, 2003'den bu yana her 2 yılda bir yayımlanmakta olup bugüne kadar toplam 8 rapor yayımlanmıştır.

4 Birleşmiş Milletler e-Devlet Gelişmişlik Endeksi Rapor Arşivi, Çevrimiçi, http://afyonluoglu.org/e-devlet/egovbench/bench_un/ , Erişim Tarihi: 18.01.2019

5 Birleşmiş Milletler UNDESA e-Devlet Kalkınma Endeksi, https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/176-Turkey/dataYear/2018

Bununla birlikte, e-Devlet Ölçümlemesi denilince büyük bir kesim tarafından çok bilinmeyen önemli bir diğer çalışma, BM LOSI[6] (Birleşmiş Milletler e-Devlet Yerel Yönetimler Çevrimiçi Hizmet Endeksi) ölçümlemesidir[7]. İlk kez 2018 yılında başlatılan bu çalışma ile, tüm dünyadan, geneli temsil edecek 40 ülke ve her ülkeden bir şehir seçilmiş, söz konusu ölçümlemede 60 kriter esas alınmıştır. Bu kriterlerin 12 tanesi teknoloji, 26 tanesi içerik sunumundaki kalite ve yeterlilik, 13 tanesi hizmetin sunulmasındaki yöntemler ve 9 tanesi de yerel yönetimin elektronik katılımcılıkta ortaya koyduğu imkanlar başlığındadır.

Türkiye, bu çalışmada Asya bölgesindeki 13 ülkeden birisi olarak seçilmiş ve Türkiye'den İstanbul Belediyesi ölçümlemeye dahil edilmiştir (Tablo 1). İstanbul, 14.1 milyon nüfusu ile, Asya bölgesinden seçilen diğer pilot şehirler arasında, nüfusu en büyük ikinci şehirdir. Değerlendirme sonucunda, Asya grubundan 3 ülkenin ilk 15'e girdiği görülmektedir. İstanbul bu listede 11. sırada (eşdeğer puanlamalar dikkate alındığında 7. sırada) yer almaktadır (Tablo 2). Bu büyüklükte nüfusa sahip bir şehir için çok ciddi bir başarı olan bu değer, yerel yönetimlerdeki olgunluğumuzda da diğer belediyelere örnek teşkil edecek niteliktedir.

ÜLKE	**NÜFUSU**
Çin-Şangay	14.35 Milyon
Türkiye-İstanbul	14.10 Milyon
Hindistan-Mumbai	11.98 Milyon
G. Kore-Seul	9.86 Milyon
Endonezya-Jakarta	9.61 Milyon

6 LOSI: Local Online Service Index (Yerel Çevrim içi İndex)
LOSI Kriterlerine Örnekler:
Teknoloji: Tarayıcı uyumluluğu, mobil cihazlardan erişilebilirlik, portalde kolay arama ve bilgiye erişim, yabancı dil desteği…
İçerik Sunumu: Belediye hakkında bilgiler, bütçesel bilgiler, ihale duyuruları, iletişim bilgileri, sağlanan servislerle iğli bilgiler, açık veri sunumu, çevrimiçi destek, ilgili diğer kamu kurumlarına bağlantılar…
Hizmet Sunumu: Kişisel verilere erişim, kimlik doğrulama imkanı, e-postalara cevap gecikme süresi, adres değişiklik bildirimleri, e-ödeme, çevrimiçi yapı izni…
Katılımcılık: Gerçek zamanlı iletişim, taleplere geri dönüş, sosyal ağ özellikleri, halka açık alanlardaki etkinlik bildirimleri, katılımcı bütçe, katılımcı ortak alan planlama, yaklaşan e-katılım etkinliklerinin duyurulması…
7 Bu çalışma ilk kez 2018 yılında başlatılmış olup, bu konudaki tüm detaylar ve sonuçlar "E-Devlet Olgunluk Ölçümleme 2018 Raporu"nun 7. bölümünde yer almaktadır.

ÜLKE	NÜFUSU
Pakistan – Karaçi	9.34 Milyon
Japonya – Tokyo	9.27 Milyon
Tayland – Bangkok	6.46 Milyon
S. Arabistan – Riyad	5.19 Milyon
BAE – Dubai	2.98 Milyon
Kazakistan – Almatya	1.51 Milyon
Malezya – Kuala Lumpur	1.59 Milyon
Sri Lanka – Kolombo	0.65 Milyon

Tablo 1 BM LOSI Aday Ülkeleri-Asya Bölgesi

Sıralama	Ülke	Karşılanan Kriter Sayısı
1	Moskova	55
2	Cape Town	53
2	Tallinn	53
4	Londra	51
4	Paris	51
6	Sidney	50
7	Amsterdam	49
7	Seul	49
9	Roma	48
9	Varşova	48
11	Helsinki	47
11	İstanbul	47
11	Şangay	47
14	Madrid	46
14	NYC	46

Tablo 2 BM LOSI Ölçümleme Sonuçları

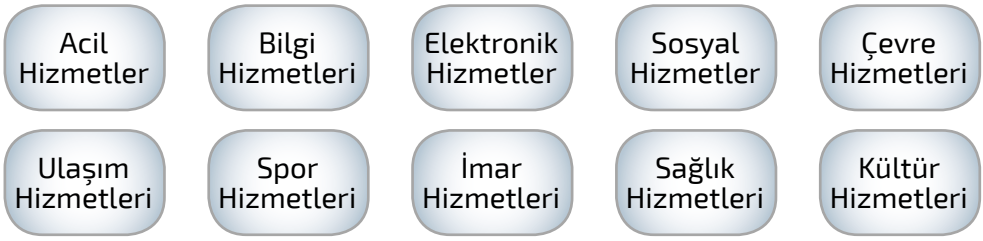
Belediyeler, vatandaşa en çok temas eden ve en yoğun hizmeti sağlayan birimler olarak bu anlamda en önemli yönetim birimleridir. Yerel yönetimlerde elektronik hizmet sunumunun olgunluğu, en başta vurgulanan hedeflere ulaşmak bakımında çok önemli avantajlar sağlamaktadır.

Bu açıdan belediyelerdeki veri çeşitliliğine bakıldığında, hizmet sunduğu vatandaşların yanısıra, personeli ile ilgili veriler, imtiyaz sözleşmeleri kapsamında özel sektör ile oluşturduğu iş ilişkileri de kişisel veriler içermektedir.

Belediyelerin verdiği hizmetler ele alındığında bunların 10 temel grupta toplandığı görülmektedir (Şekil 3). Bu hizmetler vesilesiyle ortaya çıkan veriler:

- Kişisel veriler
- Ticari veriler
- Kamu verileri

olarak gruplanmakta, ayrıca bu verilerin anonimleştirilmesinden oluşan bir veri grubu da doğmaktadır.



Şekil 3 Belediye Hizmet Kategorileri

Bu hizmet başlıkları arasında, veri olarak en büyük hacmi ve çeşitliliği oluşturan başlık elektronik devlet hizmetleridir. Dolayısıyla verimliliği yüksek tutmak için ilk aşamada e-devlet kapsamında elde edilen ve üretilen verilere odaklanmak en pratik yaklaşım olacaktır.

3. E-DEVLET UYGULAMALARINDA KİŞİSEL VERİLER

Kişisel verilerin kurumların gündeminde önem kazanmasındaki temel motivasyon, ilk aşamada, ortaya koyulan yasal yükümlülükler ve bu yükümlülüklerin yerine getirilmemesi durumunda oluşacak cezai müeyyideler olmuştur. Nitekim ülkemizde bir milyon liraya kadar uygulanabilen cezai müeyyide[8], Avrupa Veri Koruma

8 6698 Sayılı Kişisel Verilerin Korunması Kanunu Madde 18: "(1) Bu Kanunun;
a) 10. maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,
b) 12. maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,
c) 15.maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,
ç) 16. maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar, idari para cezası verilir.", Çevrimiçi, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf , Erişim Tarihi: 18.01.2019

Tüzüğü (GDPR) kapsamında Avrupa Birliği'nde 20 milyon Euro (veya küresel cironun %4'ü) gibi oldukça büyük rakamları karşımıza çıkarmaktadır[9].

Ancak Gartner'in Kasım 2019 tarihli raporunda[10] bu alanda önemli bir tespit dikkati çekmektedir. Artık kurumlar ve sektörün motivasyonu, mevzuata uyumdaki eksiklik ya da hatalardan kaynaklı cezai müeyyideler yerine, verilmesi hedeflenen hizmet için "bu veriyi almanın gerçekten şart olup olmadığına" doğru kaymıştır. Çünkü bu alanda yapılan hatalar, yasayla verilen maddi cezalardan daha da önemli olarak kurum ya da şirketin itibarını zedelemektedir. Dolayısıyla etik ilkeler ve kurumsal güvenin / imajın korunmasına yönelik hassasiyet daha çok öne çıkmaya başlamıştır.

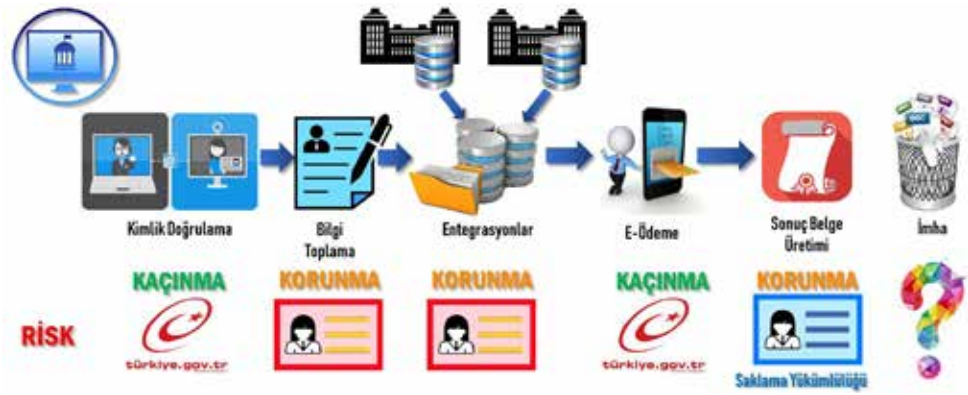
Bu açıdan bakıldığında, e-devlet hizmetleri sağlarken toplanabilecek verileri 2 kategoriye ayırmak mümkündür:

1. Hizmetin verilmesi için şart olan, bu veri olmadan hizmeti sağlamanın mümkün olmadığı "asli hizmet verileri": Veri sorumlusu, bu verinin teminine / talebine yönelik yetkiyi mevzuattan alırlar. Aynı şekilde ilgili mevzuatta bu verinin alınış ve işleme şartları ile saklama yükümlülükleri de tanımlanmıştır. Bu gruptaki verilerin temini için açık rıza alınması gerekmemektedir. Aksi takdirde bu verilerin işlenmesi, muhafazası, paylaşımı ve imhasında yine açık rızaya bağlanan yükümlülüklerin İlgili Kişi'ye karşı yerine getirilmesi gerekecektir.
2. Mevzuatta herhangi bir talep ve tanım bulunmamakla birlikte, pratik yaşamı kolaylaştırmak için alınan "yardımcı veriler": Örneğin bir kaza anında daha hızlı sağlık müdahalesi için taksicilerden kan grubu bilgisinin alınması veya belediyelerin, vergilerin unutularak geç yatırılması durumunda vatandaşın mağdur olmaması için onlara daha önceden SMS ile haber verebilmek amacıyla cep telefonu numaralarını alması.

Uygulamada genel olarak en yaygın hata, ikinci gruptaki ekstra bilgileri vatandaştan isterken, asıl hizmetin yapılmasına ilişkin şarta bu verinin teminini bağlamalarıdır. "Battaniye Rıza"[11] olarak da bilinen bu yaklaşım ile, vatandaş hizmeti alabilmesi için "bu veriyi vermek zorunda bırakılmakta", aslen mevzuatta belirlenen açık rıza prensipleri işletilmemiş olmaktadır. Çözüm olarak 6698 sayılı kanunun 5. maddesinde belirtilen çerçevede açık rıza alınmalı ve hizmet şartına bağlanmamalıdır.

9 Avrupa Veri Koruma Tüzüğü, Madde 83-5: "Aşağıdaki hükümlere ilişkin ihlaller, 2. paragraf uyarınca, 20.000.000 Euro'ya kadar veya, bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'üne kadar idari para cezalarına (hangi meblağ yüksek ise, o geçerlidir) tabidir:", Kişisel Veriler Mevzuatı, Mustafa Afyonluoğlu, 2018, Çevrimiçi, http://afyonluoglu.org/book-01 , Erişim Tarihi: 18.01.2019, Sayfa:1039-1040.
10 Gartner Top 10 Strategic Technology Trends for 2019, Gartner, Çevrimiçi, https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/ , Erişim Tarihi: 18.01.2019
11 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Belediyelerdeki yaygın bir elektronik hizmet örneğine bakıldığında, önce kimlik doğrulama, ardından sağlanacak hizmete ilişkin vatandaştan alınması gereken bilgilerin talep edilmesi, akabinde bu hizmet için diğer kurumlarda var olan bilgileri entegrasyonlarla (veya istisnai durumlarda geleneksel yöntemlerle) alma, sonrasında da bu hizmete ilişkin bir hizmet bedeli (veya harç, resim vb.) var ise elektronik ödeme işlemini gerçekleştirme ve son aşamada da hizmetin sonuç çıktısını (makbuz, ruhsat, izin yazısı vb.) oluşturma şeklinde genel bir süreç ele alınabilir (Şekil 4). İçerikleri incelendiğinde bu aşamaların hepsinde kişisel verilerin olduğu görülmektedir. Dolayısıyla bu süreçte riskleri minimuma indirmek için, (bilgi güvenliği süreçlerinde olduğu gibi) her adımın risk değerlendirmesini yapmak en sağlıklı yöntemdir.



Risk değerlendirmesinde en çok tercih edilen yöntem, "riskten kaçınma" yollarından birisi olarak, (hizmet kalitesi, güvenliği ve disiplininde bir kayba sebep olmamak ve daha yüksek fayda-maliyet sağlamak şartıyla) "imkan var ise bu riski, (tercihen asli görev alanı bu olan) başka bir aktöre devretmek"tir. Nitekim verdiğimiz örnek için, kimlik doğrulama ve elektronik ödeme hizmetlerinde e-devlet kapısı (nitekim kimlik doğrulama işleminin e-devlet kapısı üzerinden yapılması ilgili yönetmelik gereğidir[12]) bu hizmetleri sağlayabilir. Dolayısıyla bu iki aşamadaki kişisel veri alma, saklama ve imha yükümlülükleri kendiliğinden ortadan kalkacaktır. Sonuç aşamasında ise, resmi bir belge üretildiğinden, buna ilişkin saklama yükümlülükleri dikkate alınarak veri koruma modeli ve politikası geliştirilmelidir. Gözden kaçırılmaması gereken daha önemli bir husus, saklama yükümlülüğünün sona ermesine müteakip kurumun takdiri / kurumsal politikası veya ilgilinin "Unutulma Hakkı" talebi kapsamında gündeme gelecek olan kişisel verinin imhasıdır. Silme,

12 E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul Ve Esaslar Hakkında Yönetmelik Geçici Madde 1: "(1) Kamu kurum ve kuruluşları sundukları ve/veya sunacakları e-devlet hizmetlerinden kullanıcıların istifade edebilmesi amacıyla gerekli olan kimlik doğrulama işlemini, bu Yönetmeliğin yayımı tarihinden itibaren en geç 12 ay içerisinde sadece e-devlet Kapısı üzerinden yapar.", 3.09.2016 tarih ve 29820 sayılı Resmi Gazete, Çevrimiçi, http://www.resmigazete.gov.tr/eskiler/2016/09/20160903-2.htm, Erişim Tarihi: 18.01.2019

yok etme ya da anonimleştirme olarak gerçekleştirilecek olan bu süreçteki sorunlar ve çözüm önerileri, ayrı bir çalışma olarak ele alınmış olup bu makalede detaylara yer verilmemiştir.

6698 sayılı kanunun çok yakın dönemde hayata geçmiş olması sebebiyle çoğu zaman rol tanımlarında tereddütler olduğu görülmektedir. Veri sorumlusu, veri işleyen ve ilgili kişiyi tayin etmek için en basit yöntem Tablo 3'de gösterilmiştir. Belirtilen sorular sorulduğunda cevabın karşılığı, bu sorunun olduğu bölümdeki tanımdır. Örneğin, işlenecek veride teknik olarak nasıl yapılacağına hangi teknik yöntemlerin kullanılacağına karar veren taraf, "Veri İşleyen"dir.

İlgili Kişi (Veri Sahibi), kişisel verisi alınan gerçek kişidir. Bir üniversitede, öğrenciler, akademik personel, sözleşmeli personel, ziyaretçiler, üniversite hastanesinde tedavi gören hastalar, Wi-Fi Kullanıcıları, ilgili kişi konumundadır.
Veri Sorumlusu, ilgili kişiden veriyi isteyendir. Veri sorumlusu, işleme amacı ve araçlarını belirler, veri kayıt sistemini kurar ve yönetir. Veri sorumlusu neyin neden ve idari olarak nasıl yapılacağına karar veren, veriyi paylaşan ve saklama şartlarını belirleyen taraftır.
Veri İşleyen, veri sorumlusunun verdiği yetki ile veriyi kullanan ve veri üzerinde işlem yapan taraftır. Veri işleyen, verinin işlenmesinin nasıl yapılacağına teknik olarak karar veren taraftır.

Tablo 3 Kişisel Verilerde Temel Tanımlar

Bu kapsamda en çok yanlış değerlendirilen husus "Veri Sorumlusu" ile ilgilidir. Genelde bilgi sistemlerinden ve verilerin teknik anlamda muhafazasından sorumlu birim bilgi işlem birimleri olduğundan, kanunda bahsedilen Veri Sorumlusu'nun da bilgi işlem yöneticisi olduğu gibi yanlış bir algı oluşabilir. Oysa KVK Kurumu'nun rehberlerinde de açıkça belirtildiği gibi, Veri Sorumlusu tüzel kişiliğin bizatihi kendisidir, burada veri sorumlusu olarak bir şahıstan bahsedilmemektedir[13]. Kişisel verilere ilişkin kurumda kolay bir geçiş başlatmak ve sonrasında sağlıklı bir işletme süreci yaşayabilmek için, öncelikle "veri haritalaması" yapılması gerekir. Bunu için gereken temel aşamalar Şekil 5'de gösterilmektedir. Bu süreçte yanlış bilinen bir husus, TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi[14] kapsamında yapılan bilgi gizlilik kategorilendirmesinin, kişisel verilerde veri haritalaması sürecinde ih-

13 Veri Sorumlusu ve Veri İşleyen Kılavuzu, Kişisel Verileri Koruma Kurumu, Sayfa 2 – Tanımlar, Çevrimiçi, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf, Erişim Tarihi: 18.01.2019

14 TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, Çevrimiçi, https://www.tse.org.tr/IcerikDetay?ID=2311 , Erişim Tarihi: 18.01.2019

tiyaç duyulan kişisel veri kategorileri ile aynı olduğunun zannedilmesidir. Arada anlamsal ilişki olsa da, 27001'de "bilgi varlıkları" ele alınırken, KVK'da "veri"ler kişisel veri perspektifinde (özellikle veri paylaşımı ve anonimleştirme süreçlerinde kullanılmak amacıyla) kategorilendirilmektedir.

Şekil 5 Veri Haritalama Aşamaları

Aradaki bağı ve farkı daha iyi gözlemleyebilmek amacıyla, Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanan bilgi varlıkları gizlilik sınıflandırma seviyesi ile kişisel veri kategorileri Tablo 4'de gösterilmiştir.

Veri Gizlilik Kategorileri
Çok Gizli
Gizli
Özel
Hizmete Özel
Ticari Gizli
Ticari Özel
Kişiye Gizli
Kişiye Özel
Tasnif Dışı

Kişisel Veriler Kategorileri
1. Açık Tanımlayıcılar
1.1.Tekil Açık Tanımlayıcılar
2. Yarı Tanımlayıcılar
3. Özel Nitelikli Kişisel Veri
3.1. Hassas Kişisel Veri
4. Tanımlayıcı Olmayan Öz Nitelikler

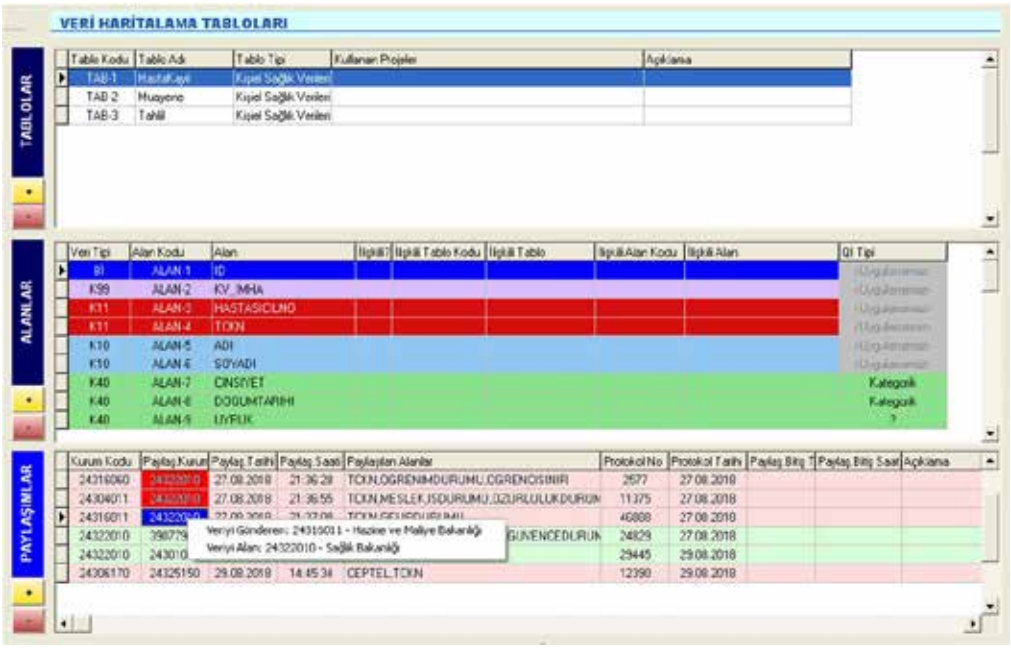
Tablo 4 Bilgi Varlıkları Gizlilik Sınıflandırılması[15] ve Kişisel Veri Sınıflandırmaları[16]

Veri haritalama işlemi, kamu kurumları için genelde yeni bir hususdur. Örnek olması bakımından, bir hastanedeki hasta, muayene ve tahlil tablolarına ilişkin bir veri haritasının neye benzediğini gösterir örnek görüntü Şekil 6'da yer almaktadır. Kurumun veri haritalaması yapacağı her bir tablo için, tablodaki her sütunun kişisel veri bakımından kategorilenmesi, diğer tablo alanları ile ilişkisi, hangi kurumlara ne kapsamda ne zaman verildiği ya da hangi kurumlardan alındığı gibi, aslında verinin takibini kolaylaştıracak bir zincir yönetim modelidir. Haritalamadan sonra, mevcut yazılımların uyumlandırılması gerekecektir, çünkü mevzuattaki özellikle veri imhası ile ilgili süreçlerin pratik olarak yönetilebilmesi için, eğer imkan var ise (kaynak

15 Bilgi Varlıklarının Gizlilik Derecelerinin Sınıflandırılması Kılavuzu, Ulaştırma ve Altyapı Bakanlığı, Çevrimiçi, http://www.udhb.gov.tr/doc/siberg/siberbilgi.pdf , Erişim Tarihi: 18.01.2019

16 Kişisel Verilerde Anonimleştirme, Doktora Tezi, Mustafa Afyonluoglu, Hacettepe Üniversitesi, 2018.

kodlardan ya da dokümantasyondan veri yapısına hakimiyet var ise) veri tablolarına bazı güncellemeler yapmak bu süreci kolaylaştıracak ya da otomatize edebilecektir. Son aşama işletme için sürdürülebilirlik kurgusudur. Burada kastedilen, yapının sağlıklı işlemesi için iç kullanıcılara verilecek eğitimler ve olası ifşa ya da ihlallerin izlenebilmesi için bir izleme sisteminin oluşturulmasıdır.



Şekil 6 Veri Haritası Örneği – Özet Gösterim

Veri haritalama, uygulama sürecinde hayatı çok kolaylaştıracağı için hem GDPR hem de ulusal mevzuat tarafından öngörülmektedir. Örneğin gerek saklama yükümlülüklerinin sona ermesi gerekse ilgilinin unutulma hakkını kullanmak istemesi halinde, mevzuatta bu verilerin uygun imha yöntemlerinden birisi ile imha edilmesi gerektiği hallerde, yönetmelikte bu verinin üçüncü kişilere aktarılması halinde buralar nezdinde de gerekli işlemlerin yapılması yükümlülüğü getirilmiştir. Yoğun veri ortamında veri yerleşim ve paylaşım zincirini kolayca takip edebilmek için veri haritalaması bu yükümlülüğün yerine getirilmesinde çok önemli bir araçtır.

Saklama yükümlülüğü ise, maalesef mevzuatımızda tek bir yerde toplanmamıştır. Bu konuda bir derlemenin yapılması, kurumların bunları tek tek takibini yapmaması ve gözden kaçırmaları engellemek için önemli bir adımdır. Bu alanda yapılan doktora çalışmasında[17], kısmi bir envanter çalışması gerçekleştirilmiş ve oldukça dağınık bir yapı olduğu ortaya çıkmıştır. Bu aşamada, KVK Kurumu'nun bu alan-

17 Kişisel Verilerde Anonimleştirme, Doktora Tezi, Mustafa Afyonluoglu, Hacettepe Üniversitesi, 2018.

da insiyatif alarak mevzuat derlemesi ve kategorilendirmesi şeklinde bir çalışmayı yaparak kamu kurumları, üniversiteler ve özel sektöre sunması hem yeknesaklığı sağlayacak hem de uygulama hatalarını minimuma indirecektir.

4. SONUÇ

e-Devlet ile birlikte özellikle elektronik ortamda yoğun olarak işlenmeye başlayan kişisel veriler, aynı zamanda veriden katma değer üretebilmek bakımından oldukça kıymetli bir kaynak olarak karşımıza çıkmaktadır. Özellikle vurgulamak gerekir ki, bu verilerin ifşası halinde Veri Sorumlusu, cezai müeyyidelerin yanısıra kurumsal itibarın zedelenmesi bakımından da önemli kayıplarla karşı karşıya kalmaktadır. Bu sebeple mevzuattaki yükümlülükler bakımından, kişisel verilerin kurumsal yönetiminde (toplama, işleme, paylaşma, saklama ve imha süreçlerinde) risk yönetimi esas alınmalıdır. Bunun için özellikle kimlik doğrulama ve elektronik ödeme gibi aşamalarda riskin devredilmesi söz konusudur. Söz konusu yükümlülüklerin özellikle imha aşaması için en kritik bileşen olan veri haritalama ve uygulamalarda harita uyumlandırılması, yüksek hacimde veriye sahip kurumlar için vazgeçilmez bir araçtır.

e-Devlet hizmetlerinde kişisel verilerin korunmasına ilişkin tüm süreçlerin bütüncül olarak ve başarılı şekilde yürütülebilmesi için, üst yönetimin konuya sahipliği ilk şart olarak görülmektedir.

Özgür Eralp

Avukat

Avukat Özgür Eralp 1993 yılında Ted Ankara Koleji'nden, 2000 yılında Ankara Üniversitesi Hukuk Fakültesi'nden mezun olmuştur. 2000 yılından beri Ankara'da serbest avukatlık yapmaktadır.

2004 yılından beri Ankara Adliyesinde 700'den fazla dosyaya bilirkişi raporu hazırlamıştır. 2007 yılından beri Başkent Üniversitesi Hukuk Fakültesi'nde ve Ufuk Üniversitesi Adalet Meslek Yüksekokulu'nda ve Ankara Üniversitesi Adalet Meslek Yüksekokulu'nda öğretim görevlisi olarak ders vermektedir.

2013 yılından beri Kurucusu olduğu Eralp Bilgi Teknolojileri İletişim Danışmanlık Organizasyon Yayıncılık Ltd.Şti aracılığıyla Bilgi ve İletişim Teknolojileri konularında danışmanlık ve eğitim hizmetleri vermektedir. 2015 yılından beri Turk Elektronik Para A.Ş'de Yönetim Kurulu Üyesi olarak görev yapmaktadır.

30'dan fazla ilde 100'e yakın konferansta sunum yapmış, yurt içinde ve yurt dışındaki bir çok seminere katkı vermiş olup Bilişim Hukuku ile ilgili 50'den fazla makalesi bulunmaktadır. 2007 yılında yayınlanmış "Hukukçular için Bilişim Terimleri Sözlüğü" isimli 2013 yılında yayınlanmış "İnternet Bankacılığı'nın Teknik, Hukuki ve Ceza Boyutu" isimli kitabı bulunmaktadır.

KİŞİSEL VERİLERE İLİŞKİN SUÇLAR VE KABAHATLER NETİCESİNDE VERİLECEK HAPİS, İDARİ PARA VE DİSİPLİN CEZALARI

Kişisel verilere ilişkin suçlara verilecek hapis cezaları 5237 Sayılı Türk Ceza Kanunu'nda, idari para cezaları 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda, disiplin cezaları ise 657 Sayılı Devlet Memurları Kanunu'nda düzenlenmiştir.

HAPİS CEZALARI

6698 Sayılı Kişisel Verilerin Korunması Kanun'un 17. maddesine göre Kişisel Verilere İlişkin Suçlar ve Cezai Yaptırımlar 5237 sayılı Türk Ceza Kanunu'nun ilgili hükümlerine (md. 135-140) atıf yapılmak suretiyle düzenlenmiştir. Ayrıca, kişisel verileri yok etmeyenlerin ise Türk Ceza Kanunu'nun 138. maddesine göre cezalandırılacağı hüküm altına alınmıştır.

Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140'ıncı madde hükümleri uygulanır. Kanun'un 7. maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.

NO	EYLEM	MADDE	CEZA
1	Kişisel verileri hukuka aykırı olarak kaydetmek	TCK madde 135/1	Bir yıldan üç yıla kadar hapis cezası
2	Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin kişisel verileri hukuka aykırı olarak kaydetmek	TCK madde 135/2	Bir yıldan üç yıla kadar hapis cezası yarı oranında artırılır.
3	Kişisel verileri, hukuka aykırı olarak bir başkasına vermek yaymak veya ele geçirmek	TCK Madde 136	İki yıldan dört yıla kadar hapis cezası
4	Bu suçlar; Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenirse	TCK Madde 137	Yukarıda verilecek cezalar yarı oranında artırılır.
5	Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmemesi	TCK Madde 138/1	Bir yıldan iki yıla kadar hapis cezası
	Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması	TCK Madde 138/2	Verilecek ceza bir kat artırılır.

Özel Nitelikteki Kişisel Verilere İlişkin Hapis Cezaları

Türk Ceza Kanunu'nun 135. maddesine göre kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin kişisel verileri hukuka aykırı olarak kaydetmek verilecek cezada arttırıcı sebep olarak öngörülmüştür. Kişisel Verilerin Korunması Kanunu'nun 6. maddesine göre kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güven-

lik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesiyle kişisel veri ve özel nitelikli kişisel veriler kavramları ile ilgili olarak yasal dayanaklar oluşmaya başlamıştır.

Yargıtay Ceza Genel Kurulu 2012/1514 E. , 2014/312 K.10.06.2014 karşı oy gerekçesi

Türk Ceza Kanunu'nun 135. maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesi ve 136. maddesinde ise verileri hukuka aykırı olarak verme, yayma ve ele geçirme suçları düzenlenmiştir. Bugüne kadar kişisel verilerin neler olduğuna dair kanunun çıkarılmaması nedeniyle TCK'daki 135 ve 136. maddelerindeki hukuka aykırılığın hangi hallerde oluştuğuna ilişkin başvurulabilecek kapsayıcı bir kaynak ya da norm olmaması nedeniyle bu iki madde eksik norm sayılırlar. Belki zamanın ihtiyaçlarına cevap verecek 'Kişisel Verilerin Korunması Kanunu' Meclisten geçtiğinde bu çerçeve düzenleme tamamlanmış olacaktır. Bununla beraber adı geçen ceza maddeleri yürürlükte olduğundan uygulanması sırasında çok dikkatli olunması gerekir. Doktrinde birçok tanım ve kapsam belirlemesi yapılmaktadır. Bu bilimsel görüşlerden hareketle kişisel verilerin hangileri olabileceğini belirlemek gerekir. Şu da bir gerçek ki, bu verilerin tamamının da ceza normları ile korunması gerektiği düşünülmemelidir. Bu tasnifin esasını genel yaşam mahremiyetinden hareketle özel hayatın gizli alanını korumayı amaçlayan ve sağlayan bilgiler olarak anlamak gerekir.

Bilimsel görüşlerden hareketle kişisel verilerin neler olabileceğini şu başlıkları altında sınıflandırabiliriz:

a. Yaşam şekline ilişkin kişisel veriler: Kişilerin üçüncü kişiler tarafından ayırımcılığa uğramaması ve haysiyetinin korunmasıyla ilişkili olarak dini inançları, cinsel tercihleri, etnik kökeni, suç geçmişi, politik eğilimleri ve kişisel özel aktivitelere ilişkin bilgiler.

b. Ekonomik ve finansal kişisel veriler: Suçlular tarafından suistimale ve kimlik hırsızlığına hedef olmamak için kişinin mali varlığı, sahip olduğu hisse ve hesaplar, borçları, yaptığı alış verişler, kredi kartlarına ilişkin veriler. Ayrıca sayılan bu bilgiler ile kişinin nerede ve kimlerle bulunduğuna, sağlık bilgilerine ilişkin bilgiler de ortaya çıkarabileceğinden ve varlık bilgisinin toplumsal açıdan da özel sayılmasından dolayı önemi artmaktadır.

c. Bilişim alanına ilişkin kişisel veriler: e-postaların bizzat adresleri veya şifreleri, internet ortamında paylaşılan kişisel veriler mahrem olarak değerlendirilebilir. Bunun önemi şu bakımdan artmaktadır, internette gezinti yapan kişi birçok kişisel bilgileri paylaşmakta, bu bilgiler kayıt altına alınmakta, yine internet erişimine ilişkin iz kayıtlarının hizmet sağlayıcı ve sunucu sahipleri tarafından tutulabiliyor olması nedenleriyle artmaktadır.

d. Sağlıkla ilgili kişisel veriler: Sağlık verileri kişilerin iş güvenliğini, toplum içindeki statüsünü ve sigorta kapsamını etkileyen hassas bilgilerdir. Ayrıca sağlık verileri kişilerin sosyal yaşantısı ve psikolojik durumları hakkında bilgi edinilmesine neden olabilir. Biyometrik veriler de (kişinin kendine özgü fiziksel veya biyolojik niteliklerine dayalı olarak insanların kimliğini tespit için dijital teknolojiden faydalanma bilimi) kişisel veriler arasındadır.

e. Politik kişisel veriler: Toplum içinde yaşayan kişilerin siyasi tercihleri toplum katmanları arasında bilinme halinde ayırımcılığa maruz kalma ihtimali bulunduğundan bu bilgiler de kişisel veridir.

Kişinin; Türkiye Cumhuriyeti kimlik numarası, adı, soyadı, doğum tarihi, doğum yeri, nüfusa kayıtlı olunan yer (İl, İlçe, mahalle veya köy), anne adı, baba adı, medeni hal (Evli, bekâr, boşanmış), cilt ve aile sıra no, kan grubu evlenme tarihi, boşanma tarihi ve mahkeme kararı özet bilgileri, ad-soyad veya diğer kayıt düzeltmeleri, vatandaşlıktan çıkarılma bilgileri, evlatlık ilişkisi, adres, din, bitirilen okullar (ilk-orta-yüksek), hastalıklar, hastalıklar ile ilgili tahlil sonuçları (DNA bilgileri), mali durum (servet, alınan ücretler), ahlaki eğilimler, zaaflar, çevre ile ilişkiler, hatıra, anı ve günlükle ilgili defterindeki bilgiler, siyası görüş (oy verdiği partiler, üye olduğu dernekler), alışkanlıkları, sevdiği kitaplar veya gazeteler, alışveriş eğilimleri, vergi numarası, e posta adresi, banka bilgileri, bilgisayarının IP numarası, emeklilik ve kurum sicil numarası, aldığı ödüller, parmak izi, avuç içi izleri, mektupları, yazılar, kitaplar. telefon numaraları, mesajları, fiziki kimliği (boy, kilo, engellilik durumu, ten rengi, göz rengi, saç rengi ve şekli, sesi, genel görünüm, ayak ve beden numarası) ve çok daha fazla bilgi kişisel veri kapsamında değerlendirilebilecektir.

Yargıtay 8.Ceza Dairesi 2017/22787 E. , 2017/13124 K. 22.11.2017

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli

sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir.

Yargıtay 8.Ceza Dairesi 2017/21010 E. , 2017/12831 K. 16.11.2017

Somut olayda da; iş yerindeki aramada bulunan ve ne şekilde sanık tarafından ele geçirildiği anlaşılmayan gerek yabancı gerek Türk vatandaşlarına ait fazla miktarda sahteliği saptanmayan nüfus cüzdanları ile pasaportların kişisel verileri ele geçirmek amacıyla bulundurulduğu anlaşılmakla, sanığın eyleminin Türk Ceza Kanunu'nun sayılı Yasanın 43/2. madde kapsamında zincirleme şekilde Türk Ceza Kanunu'nun 136. maddesi gereğince cezalandırılması, ele geçirilen belge sayısı gözönüne alınarak Türk Ceza Kanunu'nun 3 ve 61. maddeleri uyarınca alt sınırdan uzaklaşılarak temel cezanın tayini gerekirken suç vasfında yanılgıya düşülmek suretiyle hüküm kurulması,

Yargıtay 8.Ceza Dairesi 2017/19872 E. , 2017/11910 K. 26.10.2017

Sanık hakkında kaybolmuş veya hata sonucu ele geçmiş eşya üzerinde tasarruf ve kişisel verileri hukuka aykırı ele geçirmek, suçlarından kurulan hükümlere yönelik yapılan incelemeye gelince; aynı işyerinde çalıştıkları anlaşılan ...'a ait nüfus cüzdanını soyunma odasındaki dolabın altında bulup, fabrika güvenliğine teslim etmeyi unuttuğunu belirten sanığın, mağdura ulaşma imkanı bulunmasına rağmen söz konusu nüfus cüzdanını hukuka aykırı olarak elde bulundurup suçta kullanması eyleminin hırsızlık suçunu oluşturacağı gözetilmeden suç vasfında yanılgıya düşülerek yazılı şekilde hüküm kurulması,

Yargıtay 8.Ceza Dairesi 2017/15706 E. , 2018/866 K. 31.01.2018

Türk Ceza Kanunu'nun 136/1. maddesinde düzenlenen suçunun mağduru, bilgileri ve şifreleri elde edilmeye çalışılan kişi olup, suçtan doğrudan zarar görmeyen A. Bankası'nın davaya katılma hakkı bulunmadığı halde, katılan sıfatı ile davaya kabulüne karar verilerek, katılan Necdet ve katılan kurum lehine vekalet ücreti tayini ile vekalet ücretinin sanıklardan alınarak hazineye irad kaydına karar verilmesi; diğer sanıklarla kart kopyalamak üzere anlaşıp karşılığında menfaat elde ettiği anlaşılan sanığın eyleminin, çalıştığı restoranta gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmekten ibaret olduğu diğer sanıkların sahte

kart üretmek ve bu kartları kullanmak suçlarına iştirak ettiğine dair dosya kapsamında delil bulunmadığı anlaşılmakla, eyleminin Türk Ceza Kanunu'nun 136. maddesinde düzenlenen birden fazla kişiye ait kişisel verileri hukuka aykırı olarak ele geçirme suçunu oluşturduğu gözetilmeden suç vasfında yanılgıya düşülerek yazılı şekilde hükümler kurulması,

Yargıtay Ceza Genel Kurulu 2012/1510 E. , 2014/331 K. 17.06.2014

Bu açıklamalar ışığında uyuşmazlık konusu değerlendirildiğinde; Türk Ceza Kanunu'nun 135 ve 136. maddelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerde sadece sır niteliğinde kişisel verilerin korunacağına ilişkin bir hükmün bulunmaması ve aksine 135. maddenin gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesi, yayılması ve ele geçirilmesi fiillerinin kanunun 136. maddesindeki suçu oluşturduğu kabul edilmelidir. Bu kapsamda somut olayda, sanığın genel yayın yönetmenliğini yaptığı gazetede köşe yazarı olarak çalışan katılanın yazdığı köşesinde kullanılan fotoğrafın, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle sanık tarafından internetteki özel bir arkadaşlık sitesine kimlik, adres ve telefon bilgileri verilmeksizin ve erkek arkadaşı aradığı açıklamasıyla konulması eylemi, TCK'nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçunu oluşturmaktadır.

Yargıtay Ceza Genel Kurulu 2012/1510 E. , 2014/331 K. 17.06.2014 KARŞI OY

Bununla birlikte sanığın eylemi, aynı zamanda katılanın onur, şeref ve saygınlığını rencide edebilecek nitelikte olması nedeniyle Türk Ceza Kanunu'nun 125. maddesinin birinci ve dördüncü fıkrası uyarınca alenen hakaret suçunu da oluşturmaktadır. Bu nedenle hukuki anlamda tek fiil sayılması gereken eylem ile hem TCK'nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçu, hem de aynı kanunun 125/1-4 maddesinde düzenlenen alenen hakaret suçu oluştuğundan, sanık hakkında 5237 sayılı Türk Ceza Kanunu'nun 44. maddesindeki farklı nev'iden fikri içtima hükümlerinin uygulanması ve oluşan suçlardan en ağır cezayı gerektiren kişisel verileri hukuka aykırı olarak yayma suçundan sanığa ceza tayin edilmesi gerekmektedir.

Yargıtay 12.Ceza Dairesi Yargıtay 12. C.D. 2017/150 E. 2017/6231 K.

Özetle, herhangi bir özellik arz etmeyen, yanında kişiyi belirleyen başka bir bilginin bulunmadığı (T.C. kimlik numarası, telefon numarası, e-posta adresi) bir fotoğra-

fın, umuma sunulmuş olması nedeniyle başka bir sitede yayınlanmasının kişisel verileri yayma suçunun konusunu oluşturmayacağı, sadece katılanın bekâr, erkek arkadaş arayan bir bayan olarak gösterilip küçük düşürdüğünden eylem Türk Ceza Kanunu'nun 125/1-4. maddesi kapsamında hakaret suçunu oluşturur. Nasıl ki aynı bilgiler ve resim sokak duvarlarına ve ilan panolarına yapıştırılsa hakaret suçu oluşacak idiyse burada da aynı suç oluşur.

Sanığın, bir karede mağdurun kendisini yanağından öptüğü, diğerlerinde kendisine sarıldığı ve her ikisinin üzerlerinde günlük kıyafetleri bulunduğu halde yan yana poz vererek çektirdikleri fotoğraflarını, mağdurun bilgisi dahilinde facebook hesabında yayımladıktan sonra, söz konusu fotoğrafları, mağdurla ayrılmalarına ve mağdur tarafından kaldırılması istenilmesine rağmen yayımlamaya devam ettiği olayda; iddiaya konu sanıkla mağdur arasındaki ilişkinin varlığını ve boyutunu gösteren fotoğrafların, daha önce mağdurun rızasına uygun olarak facebook adlı sosyal paylaşım sitesinde yayımlanmış olması karşısında, bu fotoğraflar, mağdurun özel yaşam alanına ilişkin ve özel hayatının gizliliğini ihlal edecek nitelikte görüntüler olarak kabul edilemeyeceğinden, sanığın, mağdura ait kişisel veri niteliğindeki fotoğrafları, mağdurun rızasına aykırı şekilde yayımlamaya devam etmesi biçiminde sübut bulan eyleminden dolayı TCK'nın 136/1. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet kararı verilmesi gerektiği gözetilmeksizin, yasal ve yeterli olmayan yazılı gerekçelerle sanık hakkında CMK'nın 223/2-a maddesi gereğince beraat kararı verilmesi, 5237 sayılı Türk Ceza Kanunu'nda hukuka uygunluk sebepleri; kanunun hükmü ve amirin emri 5237 sayılı Türk Ceza Kanunu'nun 24. maddesine göre kanunun hükmünü yerine getiren kimseye ceza verilmez. Yetkili bir merciden verilip, yerine getirilmesi görev gereği zorunlu olan bir emri uygulayan sorumlu olmaz. Konusu suç teşkil eden emir hiçbir surette yerine getirilemez. Aksi takdirde yerine getiren ile emri veren sorumlu olur. Emrin, hukuka uygunluğunun denetlenmesinin kanun tarafından engellendiği hallerde, yerine getirilmesinden emri veren sorumlu olur.

Meşru Savunma ve Zorunluluk Hali

5237 sayılı Türk Ceza Kanunu'nun 25.maddesine göre gerek kendisine ve gerek başkasına ait bir hakka yönelmiş, gerçekleşen, gerçekleşmesi veya tekrarı muhakkak olan haksız bir saldırıyı o anda hal ve koşullara göre saldırı ile orantılı biçimde defetmek zorunluluğu ile işlenen fiillerden dolayı faile ceza verilmez. Gerek kendisine gerek başkasına ait bir hakka yönelik olup, bilerek neden olmadığı ve başka suretle korunmak olanağı bulunmayan ağır ve muhakkak bir tehlikeden kurtulmak veya başkasını kurtarmak zorunluluğu ile ve tehlikenin ağırlığı ile konu ve

kullanılan vasıta arasında orantı bulunmak koşulu ile işlenen fiillerden dolayı faile ceza verilmez.

Hakkın Kullanılması ve İlgilinin Rızası

5237 sayılı Türk Ceza Kanunu'nun 26. maddesine göre hakkını kullanan kimseye ceza verilmez.Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez.

İDARİ PARA CEZALARI

Kişisel verilere ilişkin idari para cezaları 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda düzenlenmiştir.

Kanun'da öngörülen yükümlülüklere aykırı davranılması halinde uygulanacak idari yaptırımlar 18. maddede düzenlenmiştir. İdari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır. Kabahat kapsamında sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi halinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir.

6698 Sayılı Kişisel Verilerin Korunması Kanun'un Kabahatler başlıklı 18. maddesine göre verilebilecek idari para cezaları aşağıdaki gibidir.

NO	EYLEM	YASAL DAYANAK	PARA CEZASI
1	Aydınlatma yükümlülüğünü yerine getirmeyenler	KVK madde 18/1-a	5.000 TL – 100.000 TL
2	Veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler	KVK madde 18/1-b	15.000 TL – 1.000.000 TL
3	Kurul tarafından verilen kararları yerine getirmeyenler	KVK madde 18/1-c	25.000 TL – 1.000.000 TL
4	Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler	KVK madde 18/1-ç	20.000 TL – 1.000.000 TL

Bu kapsamda; aydınlatma ve veri güvenliğini sağlama, Kurul kararlarını yerine getirme ile Sicile kayıt ve bildirim yükümlülüklerine aykırı davranılması kabahat olarak öngörülerek idari para cezası yaptırımına bağlanmıştır. İdari yaptırımlara Kurul tarafından karar verilecek olup, verilen yaptırım kararlarına karşı yargı yolu açıktır.

Kişisel Verileri Koruma Kurumu Kurul Kararları Özetleri

Bir Gerçek Kişinin Adının Geçtiği Köşe Yazısının Silinmesi Talebi

Bir gerçek kişinin adının geçtiği bir gazetedeki köşe yazısının, kişinin hala kamuyu ilgilendiren bir konumda olduğu hususu da dikkate alınarak, ifade özgürlüğünün bir yansıması olan basın özgürlüğünün kapsamında olduğu değerlendirildiğinden 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 28. maddesinin (1) numaralı fıkrasının (c) bendi uyarınca, ilgili kişinin söz konusu köşe yazısının silinmesine yönelik talebine ilişkin olarak Kurulca yapılacak herhangi bir işlem bulunmadığına karar verilmiştir.

Özel Nitelikli Kişisel Verilerin Kanuna Aykırı Şekilde İnternet ve Sosyal Medya Mecralarında Paylaşılması

İlgili kişiye ait özel nitelikli kişisel veri olan sağlık raporunun, bir hastahane nezdinde hastaların tedavi sürecinde yer alan hekimler tarafından, veri sorumlusuna ait mobil olarak kullanılan bir uygulamadan alınan ekran görüntüsünün başka bir cihaz tarafından çekilmesi suretiyle internet ve sosyal medya mecralarında paylaşılması ve bu itibarla özel nitelikli bir kişisel verinin sosyal medya aracılığıyla geniş bir kitleye ifşa edilmiş olduğu dikkate alınarak, Kurulca yapılan resen inceleme neticesinde; 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12. maddesinin (1) numaralı fıkrasının (c) bendi kapsamında kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin edemeyen veri sorumlusu hakkında Kanun'un 18. maddesi uyarınca idari para cezası uygulanmıştır.

İş Başvurusu Sürecinde İşlenen Kişisel Verilerin Hukuka Aykırı Şekilde Paylaşılması

a. İlgili kişi tarafından, online olarak insan kaynakları hizmeti sunan veri sorumlusuna ait bir platform üzerinden yapılan iş başvurusunun akabinde; veri sorulusunun, ilgili kişiye ait başvuru bilgisi, ad ve soyadı ile e-posta adresi bilgisini içeren kişisel verileri herhangi bir hukuki sebebe dayanmadan diğer işe başvuranlarla paylaştığı tespit edildiğinden; bu durumun; 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12. maddesinin (1) numaralı fıkrasına aykırılık teşkil

etmesi nedeniyle anılan şirket hakkında kanunun 18. maddesi uyarınca idari para cezası uygulanmıştır.

b. Bir şirketler topluluğu bünyesinde yer alan birden çok veri sorumlusu şirketler arasında veri aktarımı gerçekleştirilmesinin, üçüncü kişiye veri aktarımı olarak değerlendirildiği, bu itibarla aynı şirketler topluluğu bünyesinde yer alan veri sorumluları arasında gerçekleşecek veri aktarımında da 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 8. maddesi hükümlerinin esas alınması gerektiği dikkate alındığında, iş başvurusunda bulunan bir adayın açık rızası olmadan kişisel verilerinin bir şirketler topluluğu altında yer alan veri sorumluları arasında aynı veri tabanını kullanmak suretiyle paylaşılmasının kanunun 12. maddesinin (1) numaralı fıkrasına aykırılık teşkil etmesi nedeniyle, anılan Şirket hakkında kanunun 18. maddesi uyarınca idari para cezası uygulanmıştır.

Kişisel Veri Güvenliği İhlalinin Geç Bildirimi

İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesinin veri sorumlusu tarafından en kısa sürede ilgilisine ve Kurula bildirimde bulunulmamasının; veri sorumlusunun gerçekleşen veri ihlalini ilgili kişilere 17 ay, Kurula ise 10 aylık gecikmeyle bildirmesinin kanunda belirtilen "en kısa süre"yi aşan bir süre olduğu ve bu durumun kanunun 12. maddesinin (5) numaralı fıkrası kapsamında veri güvenliği ihlali olarak değerlendirilmesi nedeniyle Kurul tarafından kanunun 18. maddesi gereğince ilgili veri sorumlusu hakkında idari yaptırım uygulanmasına karar verilmiştir.

Açık Rızanın Hizmet Şartına Bağlanması

Veri sorumlusu tarafından kanunun 5. maddesinin (2) numaralı fıkrasının (c) bendi kapsamında sözleşmenin taraflarına ait kişisel veri işlenmesi durumunda ayrıca açık rıza alması ve de açık rızayı üyeliğin ve hizmetin dolayısıyla sözleşmenin bir koşulu olarak dayatmasının;

- Diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına geleceği,

- Ayrıca hizmetin açık rıza şartına bağlanmış olmasının açık rızayı sakatlayacağı, dikkate alındığında, bu durumun kanunun 4. maddesinde yer alan hukuka ve dürüstlük kurallarına uygun olma ve işlenme amacı ile bağlı, sınırlı ve ölçülü olma ilkelerine aykırılık teşkil etmesi nedeniyle, Kurul tarafından kanunun 12.

maddenin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında kanunun 18. maddesi uyarınca idari yaptırım uygulanmasına karar verilmiştir.

İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık)

Mahkemece veri sorumlusundan ilgili kişi hakkında bazı kişisel verilerin talep edilmesi ve veri sorumlusunun gereğinden fazla kişisel veri aktarımında bulunmasının;

- Kanunun 8. maddesinin (2) numaralı fıkrasında atıfta bulunulan kanunun 5. maddesinin (2) numaralı fıkrasının (ç) bendinde yer verilen hukuki yükümlülüğün yerine getirilmesi için zorunlu olması kapsamında değerlendirilemeyeceği,

- Kanunun 4. maddesinin (1) numaralı fıkrasının (ç) bendinde yer alan işlendikleri, amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık teşkil ettiği, dikkate alınarak, Kurul tarafından kanunun 12. maddesinin (1) numaralı fıkrası çerçevesinde ilgili kişiye ait kişisel verilerin güvenliğini sağlayamayan veri sorumlusu hakkında kanunun 18. maddesi uyarınca idari yaptırım uygulanmasına karar verilmiştir.

Veri Sorumlusu Tarafından Kanunda Belirlenen Süre İçerisinde İlgili Kişiye Cevap Verilmemesi

İlgili kişinin veri sorumlusuna kanunun 11. maddesinde sayılan hakları kapsamında başvuruda bulunmasına rağmen veri sorumlusunun süresinde ilgili kişiye cevap vermemesi üzerine;

- Kurul tarafından veri sorumlusunun ilgili kişiye kanunun 11. maddesi kapsamında talep ettiği hususlarla ilgili olarak, kanunun 15. maddesinin (5) numaralı fıkrası gereğince kararın tebliğinden itibaren 30 gün içerisinde cevap vermesi, aksi takdirde kanunun 18. maddesi uyarınca hakkında idari yaptırım uygulanacağı hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.

- İlgili Kişinin Kişisel Verilerinin Silinmesi Talebinin Yerine Getirilmemesi

- Veri sorumlusunun, halihazırda aktif olmayan müşterisinin (ilgili kişi) kişisel verilerinin silinmesi hususundan talebini yerine getirmemesi üzerine;

- Veri sorumlusunun tabi olduğu mevzuat uyarınca işlediği kişisel verileri 10 yıl boyunca muhafaza etmesi zorunluluğu bulunduğundan, Kurul tarafından aktif olmayan müşterilerin kişisel verilerinin, kanunun 4. maddesinde yer verilen genel ilkelere uygun olarak saklama amacı dışında işlenmemesi gerektiği yönünde veri sorumlusunun talimatlandırılmasına karar verilmiştir.

Kişisel Veri Güvenliğinin Sağlanması Amacıyla Uygun Güvenlik Düzeyini Temin Etmeye Yönelik Gerekli İdari ve Teknik Tedbirlerin Alınmaması

- Veri sorumlusu tarafından müşterisinin (ilgili kişi) kişisel verilerinin yer aldığı bir belgenin, aynı isme sahip başka bir kişiye gönderilmesinin; veri sorumlusu açısından sistemsel bir açığa işaret ettiği dikkate alınarak, kurul tarafından kanunun 12. maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğinin sağlanması hususunda gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kanunun 18. maddesi uyarınca idari yaptırım uygulanmasına karar verilmiştir.

- Veri sorumlusunun bir çalışanının, talebi olmamasına rağmen müşterisinin (ilgili kişi) kişisel verilerini, kendisine yetki tanımlaması yapılan sistemler aracılığıyla kişisel amaçları için sorgulaması nedeniyle, kurul tarafından kanunun 12. maddesinin (1) numaralı fıkrası gereğince veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kanunun 18. maddesi uyarınca idari işlem tesis edilmesine karar verilmiştir.

Kanunda Yer Alan Genel İlkelere Aykırı Şekilde Kişisel Veri İşlenmesi (Hukuka ve Dürüstlük Kurallarına Uygun Olma ile Belirli, Açık ve Meşru Amaçlar İçin İşleme İlkelerine Aykırı Kişisel Veri İşlenmesi)

Veri sorumlusu tarafından ilgili kişinin talebi üzerine gerçekleştirilen işlemde veri sorumlusu tarafından işlemin gerektirmediği kişisel veri içeren bir belgenin müşteriden istenilmesinin;

- İlgili mevzuatta yer almaması

- Ulaşılmak istenen amaç ile bağdaşmaması nedeniyle kanunun 4. maddesinin (2) numaralı fıkrasının (a) bendinde yer verilen hukuka ve dürüstlük kurallarına uygun olma ilkesi ile (c) bendinde yer verilen belirli, açık ve meşru amaçlar için işlenme ilkesine aykırılık teşkil ettiği dikkate alınarak, kurulca kanunun 12. maddesinin (1) numaralı fıkrası çerçevesinde kişisel veri güvenliğini sağlamaya

yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 inci maddesi uyarınca idari yaptırım uygulanmasına karar verilmiştir.

Kanuna Aykırı Şekilde Kişisel Verilerin Paylaşılması

- Veri sorumlusu tarafından, bir şirketin çalışanlarına e-posta yoluyla gönderilen sözleşme örneklerinde veri sorumlusu tarafından, işveren iletişim adresi kısmına şirketin adresinin yazılması gerekirken, kanunun 5. maddesinde sayılan kişisel veri işleme şartlarından herhangi birine dayanmaksızın şirket adına sürecin yönetiminden sorumlu kişinin (ilgili kişi) ev adresinin yazılması nedeniyle, Kurul tarafından kanunun 12. maddesi kapsamında veri güvenliğini sağlayamayan veri sorumlusu hakkında kanunun 18. maddesi uyarınca idari yaptırım uygulanmasına karar verilmiştir.

DİSİPLİN CEZALARI - 657 SAYILI DEVLET MEMURLARI KANUNU

Kişisel verilere ilişkin disiplin cezaları ise 657 Sayılı Devlet Memurları Kanunu'nda düzenlenmiştir. Anayasa'nın 129. maddesinin 2. fıkrasına göre, "memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşları ve bunların üst kuruluşları mensuplarına savunma hakkı tanınmadıkça disiplin cezası verilemez."

Kamu hizmetlerinin gereği gibi yürütülmesini sağlamak amacı ile kanunların, tüzüklerin ve yönetmeliklerin devlet memuru olarak emrettiği ödevleri yurt içinde veya dışında yerine getirmeyenlere, uyulmasını zorunlu kıldığı hususları yapmayanlara, yasakladığı işleri yapanlara durumun niteliğine ve ağırlık derecesine göre 657 sayılı Devlet Memurları Kanunu'nun 125. maddesinde sayılan disiplin cezalarından birisi verilir.

Devlet memurlarına verilecek disiplin cezaları ile her bir disiplin cezasını gerektiren fiil ve haller şunlardır:

a. **Uyarma:** Memura, görevinde ve davranışlarında daha dikkatli olması gerektiğinin yazı ile bildirilmesidir.

b. **Kınama:** Memura, görevinde ve davranışlarında kusurlu olduğunun yazı ile bildirilmesidir.

c. **Aylıktan kesme:** Memurun, brüt aylığından 1/30 - 1/8 arasında kesinti yapılmasıdır.

d. **Kademe ilerlemesinin durdurulması:** Fiilin ağırlık derecesine göre memurun, bulunduğu kademede ilerlemesinin 1 - 3 yıl durdurulmasıdır.

e. **Devlet memurluğundan çıkarma:** Bir daha devlet memurluğuna atanmamak üzere memurluktan çıkarmaktır.

Cüneyt Yılmaz

Bağcılar Belediyesi Bilgi İşlem Müdürü

2005 yılında Bağcılar Belediyesi Bilgi İşlem Müdürlüğünde mühendis olarak görev yapmaya başlayan YILMAZ, aynı yıl Kent Bilgi Sistemi Entegrasyonu projesinde görev aldı. 2005-2007 yılları arasında Bağcılar Belediyesi Yönetim Bilgi Sistemi ve Kent Bilgi Sistemi sorumlusu olarak görevine devam etti. Aynı görevdeyken, 2007-2011 yılları arasında İstanbul Valiliği Proje Koordinasyon Birimi (İPKB) tarafından yürütülen İSMEP (İstanbul Sismik Riskin Azaltılması ve Acil Durum Hazırlık Projesi) kapsamında pilot iki belediyeden biri olan Bağcılar Belediyesi'nde proje yöneticiliğini üstlendi. 2012 yılında elektronik imza (e-imza, mobil-imza), e-yazışma, Kayıtlı Elektronik Posta (KEP), dijital arşiv entegrasyonu ve e-süreç yönetimini kapsayan EBYS Projesinin gerçekleştirilmesinde rol aldı. Bağcılar Belediyesi, bu süreçte gerçekleştirdiği, ilk elektronik imzalı işyeri ruhsatı, ilk e-Yazışma, ilk KEP gönderisi gibi ilklerle birçok kez e-TR finalisti oldu ve 2016 yılında Marmara Belediyeler Birliği tarafından e-Başvuru Yönetimi, ve e-Arşiv projeleri ile Altın Karınca Ödüllerine layık görüldü.

2013 yılında Yönetim Bilgi Sisteminin web tabanlı ve süreç bazlı hale getirilmesi için başlatılan WebMIS Projesinde proje yöneticiliğini üstlenen YILMAZ, Ocak 2014'te Bilgi İşlem Müdürlüğü görevine getirildi.

BELEDİYECİLİK AÇISINDAN KİŞİSEL VERİ YÖNETİMİ UYGULAMALARI: BAĞCILAR BELEDİYESİ MODELİ

Belediyecilik, özellikle de büyük şehirlerdeki belediyeler için geniş bir kitleye, yasalarla belirlenmiş, sorumlu olduğunuz hizmetleri vermeyi, görevleri yerine getirmeyi ve bunları yaparken üretilen birçok veri ve bilgiyi yönetmeyi, kayıt altına almayı gerektirir. Bu verilerin, hizmetlerin veriliş hızına uygun, kesintisiz, sürdürülebilir, güvenli, hızlı ve bir "değer" olarak görülerek yönetilmesine, teknolojik gelişmelerle ortaya çıkan sistemler olmadan pek de olanak kalmamıştır. Burada değer olarak görmekle anlatılmak istenen, bir bilgi ve verinin anlamlı bir şekilde biçimlendirilmesi, ondan yeni bilgi, veri ve hizmetler türetilmesi, eş zamanlı olarak bilgi ve yazılım teknolojileriyle, belge ve arşivler yoluyla, gerektiğinde geleceğe sunulacak birer kanıt olarak, güvenli bir şekilde saklanması, korunmasıdır.

Kullanılan teknolojilerin sunduğu kolaylıklar kadar, oluşabilecek tehditlerin ortadan kaldırılması, bu düz olmayan, dikenlerle dolu e-Dönüşüm yolunda güvenliğin de sağlanması gerekmektedir. Sebep çok açıktır: Elde edilen veri ve bilginin saklanması ile ilgili faaliyetler, hukuki, maddi ve her şeyden önce insani bazlı haklar çerçevesinde gerçekleşir.

Belediyecilik, bir yandan hizmet kalitesini yükselterek akıllı şehirlere, ideal kentlere doğru evrilirken, bir yandan da söz konusu tehditleri, hata ve kayıpları engelleyebilmek adına gelişen teknolojiyi arkasına alan, etkili yöntemler arayışındadır. Belediyeler, gelişimin her gün yaşandığı bu teknolojik süreçte, ona ayak uydurmak, dönüşümlerini sağlıklı gerçekleştirmek ve sorumlu oldukları taraflara karşı, yerine getirmekle yükümlü oldukları hemen her şeyi güvenli bir şekilde korumalıdırlar. Belediyelerde Kişisel Verilerin Korunması, yukarıda anlatılan hizmet süreçlerinde yerine getirilmesi gereken salt teknolojik bir faaliyet veya olgu değildir. Birbiriyle ilişkisel birçok faaliyetin beraber yürütüldüğü, kararların alınıp organizasyonların yapıldığı, başlı başına önemli, dev bir süreçtir. Vatandaşın talep ettiği hizmetle ilgili ondan istenen bilgi ve belgelerle başlar, hizmetin üretilme adımlarında personelin veri ve bilgiye erişimi, kayıt mekanizmaları, dış kurum ve kuruluşlarla gerçekleşen veri alışverişleri ve entegrasyonlar, hizmeti alanın doğrudan iş süreçlerine, üretilen bilgi ve belgelere erişim faaliyetleriyle devam eder, iş kayıtlarının tutulması, sonuçlanması, üretilen dosya ve belgelerin yasal çerçevede belirlenen süre ve koşullarda saklanması ile son bulur. Bu adımların her birinde kişisel verilerin bütünlüğünün bozulmasına, ifşasına neden olabilecek tehditler bulunabilir. Özellikle veriye erişim, belge hazırlama ve saklama düzeylerinde yaşanabilecek olumsuzlukların ön-

lenebilmesi için yalnızca önleyici faaliyetler yeterli değildir. Daha öncesinde kişisel verilerin yönetiminde alınan sorumluluklar ve riskler hakkında topyekûn bilgi sahibi olunmalıdır. Kişisel verilerin korunması aynı zamanda kurumsal iş yapma kültürünün bir parçası olmalı, bunun için de sürecin personelin farkındalığını sağlayan ve yükselten eğitimlerle başlaması gerekmektedir. Önlem niteliğinde yapılan, eğitimler, kurulacak sistemler ve işletilecek süreçler kendi alanlarında ulusal ve uluslararası standartlara uygun olmalıdır.

Belediyecilik açısından kişisel verilerin korunmasına destek sağlayan uygulamaları şöyle sıralayabiliriz:

- Bilgisayar Okur-Yazarlığının Geliştirilmesi İçin Personel Eğitimleri
- İş Süreçleri ve İş Akışları Eğitimleri
- Elektronik Belge Yönetim Sistemi ve Dijital Arşiv Uygulamaları
- Elektronik İmza Uygulamaları
- Rol Bazlı Yetki Sistemleri
- Bilgi Güvenliği Yönetim Standardı
- Belge ve Arşiv Yönetim Standardı
- İş Sürekliliği Standardı
- Yazılımların Entegrasyon Altyapıları ve Servislerinin Güvenliği
- Güvenlik Operasyon Merkezi

Bu uygulamaların bazılarının oturtulması uzun soluklu süreçler gerektirebilir. Örneğin iş süreçleri eğitimleri ve süreç bazlı EBYS uygulamalarıyla, kurumsal süreçlerin kapalı süreçler olarak tanımlanması, hizmetin adımlarında verinin ve belgelerin kontrol dışı değiştirilmesinin, yetkisiz erişiminin önüne geçilmesini sağlar. Bu alandaki projelerin analiz fazları bir yılı bulabilir. Bu bir kayıp değildir, çünkü yukarıda bahsedilen kullanıcı yetkilendirme, bu yetkinin kullanımı, elektronik imza uygulamalarına geçiş, elektronik akış düşüncesinin yerleştirilmesi gibi değerler bu projeler süresince kuruma kazandırılabilir.

Resim 1- Süreç Yönetiminin Oluşturulmasının Adımları

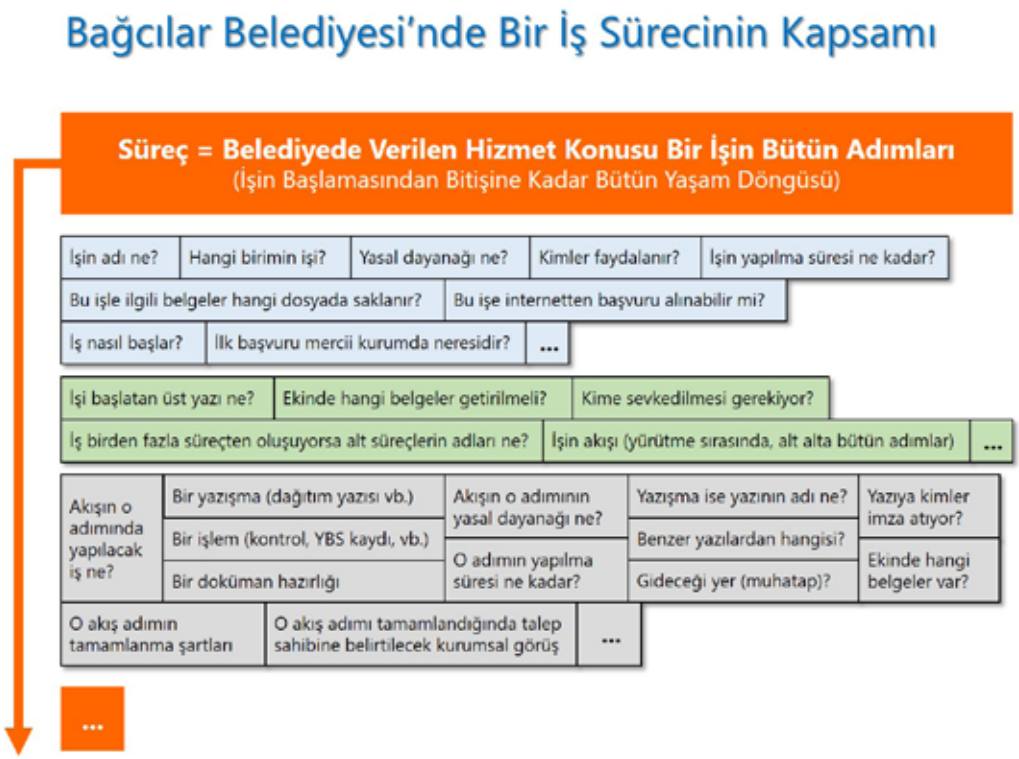
Belediyelerde kişisel verilerin en çok kullanıldığı alanlar, başvurudan başlayıp, bir dosya bütünlüğünde ilerleyen, belge hazırlanan ve saklanan iş süreçlerini kapsamaktadır. Bu süreçlerde vatandaşlardan birçok bilgi ve belge alınır. Alınan bilgilerin kullanımı sırasında süreci yürüten kişilerin her bilgiye erişmesi, görmesi, değiştirmesi, silmesi elbette ki istenmez. Bu nedenle kişilerin görev ve sorumlulukları, hiyerarşik yapı içerisindeki yerleri ve risk durumlarına göre yetkilerin organizasyonu gerekir. Kullanılan yazılımlardaki en küçük bilgi alanını görmekten, yazılımın bütününe müdahale etmeye kadar geniş bir yelpazede yetki organizasyonu yapılmasını sağlayan güvenlik uygulamaları gereklidir. Benzer şekilde, kurumun güvenli internet erişimine sahip olması, taleplerin yapıldığı erişim köprüsünün kontrolünün yapılması, tüm yapının web ortamına taşındığı düşünülürse çok ciddi bir güvenlik duvarı uygulamasını gerektirir.

Uzun soluklu bir e-Dönüşüm serüveni geçiren Bağcılar Belediyesi'nde "Kişisel Veri Yönetimi" uygulamalarına çok kısa sürede geçilmemiştir. Yukarıda anlatılan uygulamalar belli bir sırada ve düzen içerisinde, farklı projelerle hayata geçirilmiş ve birbirleriyle olan ilişkileri sağlanmıştır.

Bu anlamda Bağcılar Belediyesinin önünü açan ilk proje İSMEP olmuştur. Bağcılar Belediyesi, Dünya Bankası ve İstanbul Valiliği İstanbul Planlama ve Koordinasyon Birimi tarafından yürütülen Sismik Riskin Azaltılması ve Acil Durum Hazırlık Projesi kapsamında seçilen iki pilot belediyeden biridir. İmar süreçlerinin iyileştirilmesi ile başlayan süreç, donanım ve yazılım altyapısının iyileştirilmesi, EBYS ve web tabanlı süreç bazlı bir yönetim bilgi sistemi ile devam etmiştir. Bu kapsamda tüm personelin süreç farkındalık eğitimleri verilmiş, yazılım ve sistem kullanımı becerileri geliştirilmiş, bilgi güvenliği odaklı hizmet sunumuna geçilmiştir. Bu proje ve uyum sürecinde gerek kurum içinde üst yönetimden kullanıcıya, gerekse kurum dışında iletişim ve entegrasyon sağlanan diğer kamu kurum ve kuruluşlarına kadar birçok zorluklar yaşanmıştır. Bu zorlukların aşılmasında en büyük yardımcı politika belirlemek, hedef odaklı çalışmak ve zorluk yaşanan noktalarda uygulama ile ikna edebilmektir.

İSMEP'le başlayan, EBYS Projesi ile devam eden e-Dönüşüm sürecinin kurumumuza kazandırdığı deneyim ve iş yapma kültürü "Kişisel Veri Yönetimi"ne uyum sürecine büyük katkı sağlamıştır. Kurumsal altyapının oluşturulması sonrasında, süreçler ve dijital arşivin tanımlamaları yapılmış, belediyemize nitelikli başvuruların (özellikle imar süreçleri) web üzerinden yapılması sağlanmıştır. Sisteme katılan tüm yazılım bileşenleri Bilgi Güvenliği Standardına uygun hale getirilmiştir ve kurumumuza ISO 27001 Bilgi Güvenliği Yönetim Standardı kazandırılmıştır. Tüm hizmet süreçleriyle elektronik yönetime geçen Bağcılar Belediyesinde kullanılan süreç bazlı EBYS, yukarıda sayılan uygulamaların hemen hepsini kapsamaktadır. Güvenli elektronik imza, e-devlet entegrasyonu, web başvuru yönetimi, çağrı merkezi entegrasyonu ve buna benzer altyapılar güvenlik esaslı olarak oturtulmuştur. Kullanılan EBYS'nin TS 13298 T1 standardına ve bu standardın öngördüğü güvenlik isteklerine, veri, dosya ve belgeye erişim yetki ve hiyerarşisine sahip olması da katkı sağlamaktadır. Çünkü kurumumuzda tüm elektronik bilgi, belge ve arşiv yönetimi bu standardın gereklerine göre yapılmaktadır ve TS13298 Kurumsal Yeterlilik Sertifikasyonuna sahip ilk belediyedir. Web Tabanlı Yönetim Bilgi Sistemimiz gerekli güvenlik altyapılarına sahiptir ve "Nesnelerin İnterneti" alanındaki ödüllü projelerimize altlık teşkil etmektedir.

Resim 2 - Bağcılar Belediyesi'nde Bir İş Sürecinin Kapsamı



KVKK ile yeniden gözden geçirilen süreç ve alanlarda risk değerlendirmeleri yapılmış, Kişisel Veri Yönetimi sorumlusu belirlenmiş, kişisel verilerin tespiti için organizasyon oluşturulmuştur.

Bağcılar Belediyesinde her şey, Yönetim Bilgi Sistemi, Doküman Belge ve Arşiv Yönetim Sistemi, Coğrafi Bilgi Sistemi gibi tüm sistemler "veri temelli" bir yapı üzerine inşa edilmiştir. Bu verinin içerdiği kişisel verilerle birlikte korunması ve güvenle saklanmasını sağlayan bir Veri Tabanı Yönetim Sistemi oluşturulmuştur. Dünyanın en güçlü veri tabanı sistemlerinden biri tercih edilmiş olup, konfigürasyonu veri kaybının yaşanmasını önleyecek, yedekleme ve felaket kurtarma altyapılarını kapsayacak şekilde oluşturulmuştur. Belediye birimlerimizin süreç yönetimi kurgusu sayesinde kurumdaki tüm iş ve hizmetler sürekli olarak analiz edilmektedir ve veri takibi online olarak yapılabilmektedir. Bu analizler elbette ki veri güvenliği ve kişisel verilerin korunmasını da kapsamaktadır. Özellikle kullanılan süreç yönetimi sayesinde hizmetten yararlanan vatandaşların başvuruları sırasında ve başvuru sonrasında kurumda yürütülen tüm işlemler, elektronik ortamda ve veri temelli bir yapı üzerinde yürütüldüğünden, talep edilen tüm kişisel verilerin yasal dayanağı

ve kurum veri tabanında ve bilgi sistemlerinde hangi alanlara işlendiği, nerelerde saklandığı ve ne kadar sürede saklanacağı gibi, "Kişisel Veri Yönetimi"ni ilgilendiren ve ilgili KVKK'nın kurumlardan talep ettiği tüm kurallara uyum başarılı bir şekilde sağlanabilmektedir.

Uyum çalışmaları kapsamında kurumumuzda gerçekleştirilen ve belgelendirme süreçleri başarıyla tamamlanan; ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi, ISO 22301:2012 İş Sürekliliği Yönetim Sistemi ve BS 10012:2009 Veri Koruma Kişisel Bilgi Yönetim Sistemleri standartları tamamen sürdürülebilir, güvenlikli bir altyapıyı sağladığından "Kişisel Veri Yönetimi" açısından birbirleriyle ilişkilidir. Uyum çalışmaları kapsamında Bağcılar Belediyesinde yapılan çalışmaları aşağıdaki şekilde gruplayabiliriz.

- Kişisel Veri Sorumlusunun Maruz Kalabileceği Riskler
- Kişisel Veri Koruma Organizasyonu
- KVKK Teknik Tedbirleri x ISO 27001 BGYS İlişkisi
- KVKK İdari Tedbirleri x ISO 27001 BGYS İlişkisi

Kişisel Veri Sorumlusu belediyenin tüzel kişiliğini temsilen Belediye Başkanıdır ki, KVKK kapsamında veri sorulusunun maruz kalabileceği; Yetkisiz Erişim, Kişisel Verilerin İfşası, Kişisel Veri Sızıntılarından Veri İşleyenle Uygun Sözleşmeler Yapılmaması gibi bir takım riskler bulunmaktadır. Bu risklerin analizleri yapılıp, Kişisel Veri Koruma Organizasyonu oluşturulmuş, riskler göz önünde bulundurularak teknik ve idari tedbirler alınmıştır. Özellikle ISO 27001 standardı ve KVKK arasında alınması gereken teknik ve idari tedbirler açısından ilişkiler bulunmakta olup, kurumda bu standartların sağlanabilmesi adına gerçekleştirilen her türlü gayret ve çalışma söz konusu standartlarla ilgili bir kurum kültürü oluşturulmasında önemli katkı sağlamıştır.

Resim 3 - Kişisel Veri Sorumlusunun Maruz Kalabileceği Riskler

Resim 4- Kurumsal KVKK Organizasyonu

Belediyemiz bir adım daha ileri giderek, siber güvenlik önlemleri ile verilerin ve dolaylı olarak da kişisel verilerin korunmasına katkı sağlayan önemli bir altyapıya daha sahiptir. Güvenlik Operasyon Merkezi olarak adlandırdığımız, inovasyon ödüllü projeyle kuruma kazandırdığımız güvenlik altyapısı, dışarıdan gelen tüm ağ trafiğini log izleme sisteminde toplar, 3000'in üzerinde korelasyon kuralına göre analiz eder ve oluşan alarmlar, kurum dışındaki bir "Güvenlik Operasyon Merkezi"ne aktarılır. Alarmlar, bu noktada "Güvenlik Operasyon Denetimi" analistlerinin sürekli gözetiminde tutulur, oluşan olaylar sürekli takip edilir. Önlem alınması gereken güvenlik olayları online portal üzerinden kurumumuza ulaştırılır. Belediye Siber Güvenlik ekipleri, bu portala erişerek, buradaki güvenlik olaylarına müdahale ederler, yaptıkları işlemleri ve sonuçlarını aynı portala girerler, böylece olayın başından itibaren güvenlik olaylarının takip, tespit ve müdahale aşamaları kayıt altına alınır. Uçtan uca güvenlikli bir konfigürasyona sahip olan bu altyapıyla yetkisiz, zararlı veya siber güvenlik tehdidi oluşturan erişimlerin kişisel veriler de dâhil olmak üzere verileri risk altına alması önlenir.

Kişisel Verilerin Korunması Belediyemizin bir bütün olarak gördüğümüz çalışan, yazılım, süreç ve güvenlik altyapılarının bir ayrılmaz bir parçasıdır. Kurumsal e-Dönüşüm devam ettiği sürece de güncel tutulmaya, sürekli analiz edilerek tüm riskler minimize edilmeye çalışılacaktır. Bu anlamda bilgi teknolojilerindeki gelişmelerin de takipçisi olmak durumundayız.

IV. OTURUM:

Şehir İçin Yerli Ve Milli Çözümler

Serkan Aziz Oral

TURK Elektronik Para A.Ş. Genel Müdürü

1993 yılında Söke Hilmi Fırat Anadolu Lisesinden, 1998 yılında Ankara Üniversitesi Siyasal Bilgiler Fakültesi İktisat Bölümünden mezun olmuştur. 2010-2011 yılları arasında ABD'de University of Connecticut'ta Finansal Risk Yönetimi (MSFRM) alanında yüksek lisansını tamamlamıştır. Halen Ankara Üniversitesi Sosyal Bilimler Enstitüsünde İşletme alanında doktora çalışmasına devam etmektedir.

Çalışma hayatına 2000 yılında T.C. Ziraat Bankası A.Ş. Bankacılık Okulunda uzman yardımcısı olarak başlamıştır. 2001 yılında Bankacılık Düzenleme ve Denetleme Kurumunun açtığı yarışma sınavında başarılı olmasının ardından BDDK Ekonomik Değerlendirmeler Dairesinde Bankacılık Uzman Yardımcısı olarak görevlendirilmiştir. 2003 yılında Bankacılık Uzmanı, 2011 yılında Bankacılık Başuzmanı olan Serkan Oral 2003-2007 yılları arasında BDDK Kuruluşlar I Dairesinde 2007-2017 yılları arasında ise Uygulama I Daire Başkanlığında görev almıştır. BDDK'da izin ve yetki işlemleri, banka mali bünye analizleri, risk yönetimi ve sorunlu banka çözümlemeleri konusunda çalışmış, kurum içi ve kurumlar arası birçok komite ve çalışma grubunda yer almıştır. Turk Elektronik Para A.Ş.'de iç sistemler ve yasal uyumdan sorumlu Genel Müdür Yardımcısı olarak görev yapmış olup, 2018 yılı itibari ile Turk Elektronik Para A.Ş Genel Müdürü olarak başladığı görevine halen devam etmektedir.

YERLİ VE MİLLİ ÇÖZÜMLER

Dijital değişimin ya da şehirliler için yerel ve milli çözümlerin bulunması büyük önem arz etmektedir. Duruma öncelikli olarak küresel perspektiften, ekonomik boyutuyla bakılması gerekiyor. Son olarak yerel ve milli çözüm adına tarafımızdan sunulan güzel bir örnek aktarılacak.

Dünya ekonomisi teknoloji ile birlikte ciddi bir değişimin içerisine girdi. Teknolojik gelişmeler bu anlamda küresel ekonomiyi çok önemli etkiledi. Hepimizin bildiği bir örnekle başlarsak; dünya küresel ekonomiyi ya da ekonomi tarihini etkileyen 4 tane temel değişim var. Birincisi hepimizin hâkim olduğu 18. yüzyılda başlamış ağır sanayi üretimi ve bunun beraberinde getirdiği uluslararası ticaretle şekillenen dönem olan sanayi devrimi, ciddi ikinci dönem 1980'li yılların başlarında ortaya çıkan bilgisayar devrimi. Bu ciddi anlamda küresel ekonomide bir çığır açıyor. Üçüncü dönem 90'ların başında ortaya çıkan internet devrimi ile artık ekonomi anlayışı bambaşka bir boyuta erişiyor. Son dönem ise 2010'dan itibaren ortaya çıkan e-ticaret dediğimiz e-finans dönemidir. Bir sonraki dönemde tarihçiler, ekonomi tarihçileri blok zincirini de yeni bir dönem olarak ekleyebilecektir. Birinci dönem, sanayi devrimi dediğimiz olgu 18.yüzyılda başlıyor ve 20. yüzyılın ortalarına kadar devam ediyor. Yani yüzyıldan fazla bir süre bu etki var. Ama son 40 yıllık dönemde küresel ekonomiyi etkileyen 4 ana dönem var. Bu doğrultuda, tarih olgusu bile eskisinden daha hızlı değişiyor. Bunun temel sebebi teknolojide yaşanan gelişmeler, teknolojinin hızla değişmesi, önünü alamadan yaptığımız bir değişim.

Bu tarihsel süreci en güzel anlatan hususlardan bir tanesi her yıl yayınlanan Fortune 500 adı verilen dünyadaki en büyük 500 şirketin yer aldığı listedir. 1960'lı yıllarda bu listede yer alan firmalardan %65'i artık o listede yok. Çok büyük bir önem arz eden bu olguya yani dijital dönüşüme, ekonomik dönüşüme ayak uyduramadılar ya da daha da önemlisi artık yeni firmalar var. Çok daha büyük potansiyel ekonomi yaratan firmalar var. Bu dijital dönüşüm, temelde insan ihtiyaçlarından kaynaklanıyor. Dijital çözüm, bireyin toplumdan ziyade kendisine yönelik ihtiyaçların karşılanması çözümünü yaratıyor. Bu durum ulaşımdan kişisel iletişime kadar her alanda karşımıza çıkmaktadır. Teknolojinin faydaları, insanların ihtiyaçlarını karşılamaya yönelik olmasından dolayı kolay kabul görmektedir. Bu durumun bize getirdiklerini, iktisat teorisinden yol çıkarak bahsedecek olursak, her arz kendi talebini yaratıyor artık.

Şehircilik anlamındaki büyük dönüşümler beraberinde teknolojik gelişmeleri getirdi ve şehirciliği bambaşka bir boyuta taşıdı. Akıllı şehirler dediğimiz kavram meydana geldi, artık şehirlerin bu yönü çok büyük önem taşıyor. Akıllı şehrin temel unsurları o şehrin sakinleri ve o şehrin yöneticileridir. Şehir sakinlerinin ihtiyaçlarının karşılanması temel hedef ama karşınıza bir kıt kaynak sorunu çıkıyor. Bu kaynakların etkin kullanımı ve sürdürülebilir bir yapı içerisinde kullanılması akıllı şehirciliğin temelini oluşturuyor. İçerisindeki en önemli unsurlardan biri bu kaynakları bir arada tutabilmek ve etkin kullanımını sağlamak, bu da teknoloji ile oluyor. Birleşmiş Milletlerin yaptığı bir çalışmada hâlihazırda dünya nüfusunun %55'i civarında bir nüfusun şehirde yaşadığı, önümüzdeki 30 yılda ise bu oranın %68'e çıkacağı öngörülmüştür. Yine ekonomik boyutuna baktığınızda akılcı şehircilik kavramıyla yaratılan ekonominin boyutunun 33 trilyon Dolara ulaşacağı söyleniyor. Bu bir realitedir, dolayısıyla akıllı şehircilik şehrin ihtiyaçlarını, şehir sakinlerinin ihtiyaçlarını karşılamasının ötesinde bir ekonomi de yaratıyor.

Bizim faaliyet alanımız "Finansal Teknoloji" teknolojik gelişmelerin finansal boyutunda faaliyet gösteriyoruz. Dolayısıyla bu kavramlar bizim için çok önemli. Şehircilikte, akıllı şehircilik kavramı içerisinde finansal teknolojilerin de beraber çalışabileceği çok önemli noktalar var. Yerli ve milli çözüme geçtiğimizde ben kendi uygulamamızın buna güzel bir örnek olduğunu düşünüyorum. Sayın Başkanımla beraber yürüttüğümüz bir çalışmamız var. Bu örnek üzerinden yerli ve milli bir uygulamanın neler yaratabildiğini göstermeye çalışacağım. Esenyurt Belediyesi ile beraber güzel bir proje yürütüyoruz. Oradaki sosyal yardımların ön ödemeli kartlar aracılığıyla doğru kanallar aracılığı ile, doğru kişilere ulaştırılmasını sağlıyoruz. Bunun getirilerinden bahsedersek, bu sosyal yardımların gerçek anlamda etkin bir şekilde kullanılmasını sağlıyor. Belediyelerin temel amacı sosyal yardımlar için ayrılan bütçenin, gerçekten ihtiyaç sahiplerine iletilmesidir ve o ihtiyaç sahibinin ihtiyacını karşılayabilmesi gerekir. Klasik uygulamalarda nakit ödemeden tutun ya da ihtiyaca yönelik mal ve hizmetlerin onlara iletilmesine kadar çeşitli uygulamalar var. Ama akıllı teknolojiler sayesinde biz şunu sağlıyoruz; gerçekten o ürüne, o hizmete ya da ihtiyaç sahibi neye ihtiyaç duyuyorsa gerekli meblağ, bu kartlara yükleniyor. Bu kartlara yüklenen tutar yalnızca o ihtiyaca yönelik olan alanlarda o proje kapsamında harcanıyor. Bizim yaptığımız şey belirlenen tutarın belirlenen kitle/alana için harcanmasının sağlanması. İkinci boyutu ise sosyal boyut olarak ele almak isterim. Bu yardımdan yararlanan kişiler hiçbir şekilde rencide olmadan normal bir birey, ekonomik bir birey gibi sahip oldukları kartlarla bu kanallarda istedikleri harcamaları yapabiliyorlar. Dolayısıyla toplumsal olarak da böyle bir

güçlendirici yapısı var. Bir başka boyut ise, harcamalar yine belediye sınırları içerisinde istenen noktalara çevrilebiliyor. Belediye içerisinde yer alan belli ürünleri satan firmalar var. Bu harcamaların mağazalar üzerinde yapılmasını, bunun dışına çıkmasını engelleyebiliyoruz. Dolayısıyla, projenin kapsamı neticesinde ürünlerin gerçek ihtiyaç sahiplerine ulaşmasını mümkün kılınıyor. Burada yerli ve milli kavramını bir kez daha vurgulamak gerekir. Bu proje, Türkiye'nin ödeme noktasıdır. Türkiye'nin ödeme yöntemi adıyla piyasada yer alan ama istediğimiz kadar bilinmeyen, ülkemizin sahip olduğu bir Troy markasıyla yürütülmektedir. Tamamen yerli ve milli bir şirket aracılığıyla Türk halkına sunulan bir proje. Lokal bazda baktığınızda yerel bir kalkınma sağlıyor. Yalnızca o belediye sınırları içerisinde bir takım değerlerin daha da gelişmesini ayrıca tüm imkânlarla, o belediye sınırları içerisinde kalması sağlanabiliyor. Geniş kapsamlı düşünüldüğünde ise bu bütün il ve ülkeye yayılabilir. Sınırlarımız içerisinde kendi değerlerimizi, ekonomik gücümüzü ve kaynaklarımızı kullanabilmeyi sağlar. Türkiye'de bu potansiyel mevcut. Finansal teknoloji alanına baktığımda bizim teknoloji geliştirici firmalarımız ve orada çalışan ekibin yurtdışından geri kalan bir yanı olmadığını söylemek isterim. Bu anlamda yerli ve milli birçok değeri yaratabileceğimizden eminim. Şehircilik anlamında, finansal teknolojiler anlamında birlikte birçok projeye imza atabileceğimiz kanısındayım.

Doç. Dr. Aslı Deniz Helvacıoğlu

Boğaziçi Üniversitesi İnovasyon ve Rekabet Odaklı Kalkınma Çalışmaları Uygulama ve Araştırma Merkezi Müdürü

Marmara Üniversitesi İngilizce Uluslararası İlişkiler Bölümü mezunudur. Marmara Üniversitesi AB Enstitüsü'nde AB Yüksek Lisansı ve AB Hukuku Doktorası yapmıştır. İnovasyon hukuku ve politikaları çerçevesinde yenilikçi politikaların kurgulanması, inovasyon stratejilerinin oluşturulması ve inovasyon eko-sistemlerinin yapılandırılması alanlarında çalışmalar yürütmektedir. Güncel çalışmaları veri yoğun yenilikçi eko-sistemlerde kişisel verilerin korunması, yenilikçi teknolojilere yönelik yasal düzenlemeler, akıllı şehirlerde veri yönetimi, yenilikçi tarım sistemlerinde inovasyon yönetimi başlıkları altında yer almaktadır.

AKILLI ŞEHİRLERDE YERLİ VE MİLLİ ÇÖZÜMLER İÇİN İNOVASYON STRATEJİSİ

İnovasyona yönelik algı, inovasyon kavramına ait çıkarımlar ve tanımlamalar, inovasyon stratejisi için büyük önem taşımaktadır. Sadece teknolojik ve/veya sürece yönelik iyileştirme veya yenileştirme çabasından öte, inovasyon bir kültürdür. Yenilikçilik kültürünü benimsemiş ve içselleştirmiş olmak, yani inovasyon kültürünü hayata geçirebilmek ise açık inovasyon ekosistemlerini oluşturmak ve ilgili tüm paydaşların faydalanabileceği etkileşimli inovasyon alanlarını kurmakla mümkün olabilmektedir.

Bu bağlamda, milli ve yerli inovasyonun çıkış noktasına yönelik doğru bir yaklaşıma sahip olmak için yenilikçilik akımlarının tarihsel gelişimini incelemek yardımcı olabilir. 1970'lerle başlayan ulusal şampiyonlar, yerini 1990'larda küreselleşmeye ve 2000'li yıllara gelindiğinde yerel küreselleşmeye bırakırken, günümüzde yenilikçi teknolojiler ve süreçlerde yaşanan hızlı gelişmeler ile yerli ve milli yenilikçi ürün ve süreçler değer kazanmaya başlamıştır. Artık küresel pazarlarda belirleyici olan, yenilikçilikten kaynaklanan katma değer ile rekabet gücü elde eden girişimlerdir. Günümüzde dünyanın genel konjonktürü, inovasyon performansında ikili bir yapıya işaret etmektedir. Bu yapının ilk ayağını inovasyon kültürü ve yenilikçilikle ilerleyen, teknoloji odaklı ve veri ile gelişen yeni nesil sistemler oluşturmaktadır. Bu, yeni teknolojilerle desteklenen yenilikçi ürün ve süreçlerin büyük kapasiteleri ile değişen geleneksel pazarlar, katma değeri yüksek pazarlara dönüşmektedir. Diğer yanda ise inovasyon ivmesini yakalayamamış, daha ziyade yenilikçi ürünlerin pazarı haline gelmiş, yenilikçilik atılımında geri kalan ülkeler bulunmaktadır.

Bu görünüm inovasyonun stratejik bir tercih olduğunu da göstermektedir. Stratejik tercih, inovasyonun nerede hızlandırılabileceği yönünde olmalıdır. Türkiye bu noktada genç nüfusu ve girişimcilik içgüdüsüyle şanslı bir konumdadır. Bununla birlikte yenilikçiliği destekleyecek eko-sistemlerin çeşitlendirilerek sayılarının artırılması ve bu tip eko-sistemlerde paydaşlar arasındaki etkileşimde yeterli sürekliliğin sağlanması gelişmeye açık alanlar olarak karşımıza çıkmaktadır. Hollanda örneğine bakacak olursak, inovasyon ve özellikle kümelenme odaklı inovasyonda ileri bir performansa sahip olan Hollanda'da temel yaklaşım dörtlü sarmal olarak nitelendirdiğimiz bütün ilgili paydaşların bir arada çalıştıkları ve birbirlerine fayda sağladıkları yenilikçi, etkin ve sürdürülebilir işbirliğine ve etkileşime dayanan ortamlar kurgulamaktır.

Bu bağlamda dünyada insancıl, sosyal, kapsayıcı inovasyon kavramları; bireyleri özelleştiren, bireylerin insani gelişimlerini destekleyen inovasyonlar önem kazanmaktadır. Bu tip inovasyonları başarı ile hayata geçirebilmek yerel yönetimlerin önemli atılımlarından biri olarak kabul edilmektedir. Yerel yönetimlerin, üniversiteler, girişimciler, özel sektör, sivil toplum ve kamunun diğer paydaşları ile birarada çalışabilecekleri eko-sistemler yaratmaları gerekmektedir.

İnovasyon stratejisinin yerel yönetimler düzeyinde hayata geçirilmesinde gelişmekte olan ülkelerde yaşanan en yaygın sorun ise, finansa erişim ihtiyacı ve inovasyona yönelik finansal kaynakların sürdürülebilir olarak yenilikçi fikirlerle örtüşecek düzeyde çeşitli mekanizmalar ile uygulanabilmesidir. Bu ihtiyaç bir noktada teşvik mekanizmalarının da değişmesini öngörmektedir. Alışılmış teşvik sistemleri incelenecek olursa; AB ve Türkiye'de benzer ancak ABD'de daha farklı sistemler uygulanmaktadır. AB ve Türkiye'de beklenti; kamunun fonlaması, fonların hedef göstermesi, fonlarla araştırma ve geliştirme süreçlerinin hızlanması ve nihai pazarlara yönelik ürünlerin de belli bir zaman içerisinde çıkartılması yönündedir. Hibe fonları veya düşük geri ödemeli, uzun vadeli kredi sistemlerinin geliştirilebilir olması önem taşımakla birlikte, bu kadar yüksek düzeye ar-ge fonları ile ar-ge süreçlerinin fonlanması, nihai ürünün ortaya çıkma hızı üzerinde yavaşlatıcı bir etki de yaratabilmektedir. ABD'de ise yaklaşım; reel sektörün inovasyon talepleri ve eko-sistem talepleri üzerine yapılandırılmaktadır. Teşvikler rekabet gücünü desteklemek ve nihai ürünün payını artırmak ve küresel katma değerini yükseltmek üzere kullanılmaktadır.

Bu çerçevede; bilgi üreten ve yenilikçi atılımları bulunan paydaşlara destekleyici fonlar sunmak önemlidir. KOSGEB ve TÜBİTAK fonları ile birlikte, yerel yönetimler kendi eko-sistemleri içerisindeki gençlere, girişimcilere, özel sektöre, daha küçük, mozaik fon olarak adlandırılabilecek fonlar sunabilmelidir. Yerel yönetimler tarafından oluşturulacak bu tip fonlar; uzun süreli, ve sonunda nihai başarıya göre ödeme yapan büyük ölçekli fonların yerine; daha küçük, çıktıları kısa dönemde elde edilebilecek, süreç içerisinde birçok farklı paydaşı bir araya getirebilecek yapıları ile çok düzeyli ve etkileşimli inovasyon eko-sistemlerinin oluşturulmasında kullanılabilecektir.

İnovasyonu tetikleyen üç etken bulunmaktadır; girişimcilik, cesaret, hayal gücü. Aslında bunlar inovasyonun duygusal etkenleridir. İnovasyonu tetikleyen bir diğer etken de değişimin yaratacağı fırsatların da farkedilebilir olmasıdır. İnovasyon anlatısının dayandığı sistem kurgusu büyük önem taşımaktadır. Milli, yerel ve bize ait bir inovasyon anlatısı oluşturabilmek ve bu anlatının fayda üzerinden kurgu-

lanması çok önemlidir. Böylelikle paydaşlar arasında bir heyecan oluşturulabilir ve insanlar yenilikçi girişimleri ile fayda üretebilecekleri düşüncesiyle heyecan duyarak motivasyon kazanabilirler. İnovasyonun sürekliliği de bir diğer önemli hususstur. Bu süreklilik iki etkene dayanmaktadır. Birincisi bilginin ve katma değerin sürdürülebilir olması, yani bir başka deyişle inovasyonu besleyecek bilimsel bilginin erişilebilir olmasıdır. İkincisi ise bu bilginin paylaşılma düzeyidir. Tüm paydaşlar bu bilginin erişilebilir olduğunu görmeli ve ondan faydalanabilmelidir. Bu tip açık eko-sistemlerde yenilikçilik toleransının artığı görülmektedir. Bu tolerans işbirliğini desteklemektedir. Birbirleri ile rekabet içerisinde olan kurumlar dahi bu tip eko-sistemlerde işbirlikleri oluşturarak fayda sağlama yoluna gidebilmektedir. İyi, doğru hakkaniyetli, adil bir inovasyon eko-sisteminin oluşturulabilmesi bu yolla mümkün olabilecektir.

İnovasyon eko-sistemlerinin sorunları incelendiğinde; en temel sorunlardan birinin bu eko-sistemde üretilen verinin yönetimi olduğu görülmektedir. Yapay zekâ, büyük veri analizleri gibi yenilikçi teknolojilere dayanan yeni yöntemler, etkin veri yönetişimi ihtiyacını ortaya çıkarmaktadır. Özellikle akıllı şehirlerde veri yönetişimi, veri sınıflandırılması, verinin açık veriye anonimleştirilerek dönüştürülmesi ve yenilikçi iş modelleri ve girişimcilere sunulması değerli fırsatlar ortaya çıkarmaktadır. Bütün bu değişen ve gelişen sistem içerisinde, paylaşılan bilgi ve verinin, etkin bir veri yönetişimi ile, bir süreç inovasyonu olarak konumlandırılması yani marka değeri kazanması da mümkündür. İnovasyon yönetimi; sadece ar-ge sürecini yönetmek değil, sahip olunan yenilikçi çıktıların pazar düzeyinde de yönetimini ve değerini yönetmek anlamına gelmektedir. Bu değer iki şekilde yönetilebilir, birincisi maddi değerin, piyasada yönetilmesi iken, ikinci husus da insani fayda üzerinden bu oluşturulan inovasyonun nasıl çeşitlendirilebileceğinin yönetilmesidir. Bu katma değerin artırılması ve farklı paydaşlarla yenilikçi çıktıların zenginleştirilmesi anlamına gelmektedir. 2000'li yılların başında inovasyon patent, telif gibi fikri mülkiyet yönetimi ve piyasa değeri üzerinden yani kapital üzerinden tanımlanırken, günümüzde inovasyon fayda, sürdürülebilirlik, döngüsel ekonomi, insani ve sorumluluk sahibi olan toplumsal katkılar ile tanımlanmaktadır. Bu çerçevede yerel yönetimlerin, yerli ve milli inovasyon stratejisinde iki alanda değerli katkıları bulunmaktadır. Bunlardan ilki, yarattıkları inovasyon markası ile nihai tüketiciye ve halka ulaşma ve etkileşim içerisinde olma becerileridir, ikincisi ise kendi içlerinde verimli ve sürdürülebilir inovasyon eko-sistemleri kurabilecek dinamiklere sahip olmalarıdır.

Yerel Yönetimlerde Akıllı Şehirlerde Yerli ve Milli Çözümler için İnovasyon Stratejisi Öncelikleri

- Yerel inovasyon eko-sistemleri (yüksek etkileşimli, çok düzeyli, sürdürülebilir),
- Yerel yenilikçi teşvik ve fon mekanizmaları,
- Fayda odaklı yenilikçi çıktılar,
- İşbirliği ve inovasyon kültürü,
- Bilgi ve katma değerin sürekliliği ve
- Etkin Veri Yönetişim modelleridir.

Türker Gülüm

Profelis Bilişim - GIBUX Projesi Yöneticisi

TED Ankara Koleji mezunu olan Türker Gülüm lisans ve yüksek lisans eğitimini Orta Doğu Teknik Üniversitesi'nde tamamlamıştır. 1987 yılından bu yana bilişim sektöründe çalışmakta olan Türker Gülüm, Türkiye'de özgür yazılımın yaygınlaştırılması adına emek vermiştir. Orta Doğu Teknik Üniversitesi, Yakın Doğu Üniversitesi ve TÜBİTAK'ta çalışan Türker Gülüm, üyesi olduğu Türkiye Bilişim Derneği ve Linux Kullanıcıları Derneği'nin yönetim kurullarında görev almıştır.

Ayrıca PostgreSQL Geliştirici ve Kullanıcıları Derneği'nin de üyesi olan Türker Gülüm, daha önce bir süre TOBB Yazılım Meclisi'nde de STK temsilcisi olarak bulunmuştur. Türkiye'de bir kurumda 37000'den fazla son kullanıcıyla, halen en yaygın kullanılan yerli masaüstü Linux dağıtımı olan GİBUX dağıtımını geliştirerek yerli kaynakların yurtdışına aktarımının azalması adına faaliyet gösteren Profelis Bilişim ve Danışmanlık firmasının yönetici ortağı olarak çalışmaktadır.

ÖZGÜR VE AÇIK KAYNAK KODLU YAZILIMLARLA GÖÇ STRATEJİLERİ

Kamunun Özgür ve Açık Kaynak Kodlu Yazılımlara Bakışı

Yerli ve Milli yazılım endüstrisinin lokomotifi olacağı öngörülen açık kaynak kodlu ve özgür yazılımların yaygınlaşması çalışmalarının Kamu'da 2003 yılında başlatılan e-dönüşüm Türkiye Projesi'ndeki 7 numaralı eylem ile başladığı söylenebilmektedir. Projedeki 7 numaralı eylem "Kamu Kurum ve Kuruluşlarında Açık Kaynak Kodlu Yazılımların Uygulanabilirliği" olarak belirlenmiştir. Türkiye'nin teknolojik açıdan dünya ölçeğinde yarışabilecek yerli ürün ve destek koşullarının hazırlanmasını da amaçlayan e-Türkiye Girişimi Eylem Planı ve sonrasında 28.07.2006 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren Bilgi Toplumu Stratejisi (2006-2010) ve Eylem Planı içinde de açık kaynak kodlu yazılımların kamuda uygulama sahası artırılarak, bu yazılımların getirdiği avantajlardan en üst düzeyde yararlanılması stratejik hedeflerden biri olarak sayılmıştır.

Benzer şekilde 6 Mart 2015 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı'nda belirtilen stratejiler arasında da kamuda açık kaynak kodlu yazılımların kullanımının destekleneceği ve açık kaynak kodlu yazılım ekosisteminin gelişiminin sağlanacağı ifadesi bulunmaktadır.

Üniversiteler hariç tutulursa kamu kurumlarında özgür ve açık kaynak kodlu yazılım kullanımıyla ilgili 2000'li yıllara kadar bazı denemeler yapılmakla birlikte kurumsal göç olarak sayılabilecek nitelikte projeler yapılmamıştı. Bazı kurumların belirli alanlardaki özgür yazılım kullanma deneyimleri başarılı olsa da bu çalışmaların çoğunluğu diğer kurumlarla paylaşılmayan ve kısıtlı sayılabilecek bir kullanım alanını içermekteydi. TÜBİTAK'ın 2004'te başlattığı Linux tabanlı Ulusal Dağıtım geliştirme çalışmaları ilk sonuçlarını 2005'te vermiş ve Pardus'un ile kararlı sürümü dağıtılmaya başlanmıştır. 2000'li yıllardan günümüze kadar özgür ve açık kaynak kodlu yazılımlar artık pek çok kurumda deneme olarak değil artık iş kritik uygulamalarda da tercih edilir olmaya başlamıştır. İlk başlarda lisanslamadaki maliyet avantajı nedeniyle tercih edilen özgür ve açık kaynak kodlu yazılımlar artık güvenlik ve performans özellikleri nedeniyle de tercih edilmeye başlanmıştır. Belki de özgür yazılımların tercihindeki en önemli konulardan biri de kullanıcılarını marka bağımlığından kurtarıyor olmasıdır. Bu bağlamda yerli yazılım endüstrisinin de dikkatini çeken özgür ve açık kaynak kodlu yazılımlara yönelme son yıllarda artmıştır.

Özgür ve açık kaynak kodlu yazılım kullanmak isteyen kurumların önüne gelen en önemli konu ise yıllardır oturmuş yapıları olan ve sahipli yazılım kullanan bu kurumların kendi göç stratejilerini nasıl oluşturacaklarının belirgin olmamasıdır. Özgür ve açık kaynak kodlu yazılımlara nasıl göç edeceğine, önceliklendirmenin nasıl yapılacağı, hangi adımların atılması gerektiği ve belki de en kritik olanı göç sırasında hangi sorunlarla karşılaşılacağına ilişkin referanslar ancak bu konudaki başarılı projelerde elde edilen deneyimlerle oluşmaktadır. Bu bağlamda Gelir İdaresi Başkanlığının yürütmüş olduğu GİBUX projesi özellikle son kullanıcılardan başlayarak işletim sistemi göçü sürecinin başarılı ve en güzel örneklerinden biri olmuştur. Projenin pilot çalışmaları tamamlanarak 2014 yılı ikinci yarısından sonra yurt sathındaki tüm Vergi Dairelerine yaygınlaştırılmaya başlanmıştır. Böylece yerli ve milli işgücü ve kaynaklar kullanılarak Gelir İdaresi Başkanlığının kurumsal gereksinimleri doğrultusunda Gelir İdaresi Başkanlığı için özelleştirilmiş bir işletim sistemi olan GİBUX ortaya çıkmıştır. Bu projeyle elde edilen en önemli deneyim diğer kurumlar için de kurumsal göç stratejilerinin oluşturulmasına ışık tutmaktadır.

Yerlilik ve Millilik Açısından Özgür ve Açık Kaynak Kodlu Yazılımlar

Yerlilik ve millilik kavramları açısından özgür ve açık kaynak kodlu yazılımlar değerlendirilmeden önce kavramların tanımlarının netleştirilmesinde yarar vardır. Herhangi bir ürünün yerli ürün sayılabilmesi için Yerli Malı Belgesi'ne sahip olması gerekmektedir. Yani söylem üzerine üretilen ürünlerin yerli olması mümkün değildir. Yerli katkı oranın nasıl hesaplanacağı ise Bilim, Sanayi ve Teknoloji Bakanlığının 13.09.2014 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren SGM 2014/35 numaralı Yerli Malı Tebliği'nde belirlenmiştir. Buna göre Sanayi Sicil Belgesi'ne sahip sanayi işletmesi tarafından ürünün üretilmesi ve Sanayi Sicil Belgesi'ndeki "Üretim Konusu" içeriğinde yer alması, tamamen Türkiye'de üretilen veya elde edilen ürünler ile üretim sürecinin önemli aşamalarının ve ekonomik yönden gerekli görülen en son esaslı işçilik ve eylemin Türkiye'de yapılmış olması ve yerli katkı oranının en az %51 olması gerekmektedir. Tam bu noktada ise hem yazılım ürünlerinin sanayi ürünü olup olmadığı ve hem de özgür yazılımlar için yerli katkı oranının en az %51 olarak nasıl belirleneceği tartışması gündeme gelmektedir.

Milli ürün tüm fikrî ve sınai hak sahiplerinin yabancı uyruklu gerçek veya tüzel kişide bulunmadığı ürünler olarak ifade edilmektedir. Yani herhangi bir "milli ürün" için tasarım aşamasından başlayarak teknoloji geliştirme de dahil tüm üretim döngüsü içinde hak iddia edebileceklerin Türkiye'deki gerçek ve tüzel kişiler olması gerekmektedir.

Türkiye Bilişim Derneği'nin Kasım 2018 tarihli "Yerli ve Millî Yazılım Endüstrisi Raporu"[1] da benzer şekilde konuyu ele almıştır. Raporda "Fikrî ve sınai hakların lisanslarla korunduğu yazılım sektörü millîlik kavramı üzerinden değerlendirildiğinde başka hiçbir ürün veya sektörde olmayan ve karşılaşılmayan farklı durumların" oluşabileceği vurgulanmış ve "Genel kamu lisansı (GPL) veya benzeri özgür yazılım lisanslarına sahip mülkiyetsiz yazılımların millî olup olmadığına ilişkin tartışmalar yapılmaktadır. Özünde fikrî hakların tamamı tüm insanlığa devredilmiş ve kopyalama, değiştirme ve çalıştırma gibi temel özgürlüklerin lisans belgeleriyle herkese tanınmış olması bu yazılımların kodlarından yararlanarak geliştirilen yazılımların ulusal sayılabilmesini mümkün kılmaktadır. Tek koşul temelindeki lisans haklarının devamlılığın sağlanabilmesidir." denilmektedir.

Yerel Yönetimlerde Özgür ve Açık Kaynak Kod Dönüşüm Stratejileri

Sunduğu hizmetler açısından kesintiye tahammülü olmayan yerel yönetimler için hassas olan konu, toplanan vergilerin verimli şekilde ve doğru alanlarda kullanıldığının şeffaf biçimde vatandaşlara hesabının verilmesidir. Günümüzde yerel yönetimlerin birçok hizmetinin yanında e-belediyecilik hizmetlerinin de verimli ve kesintisiz çalışması beklenmektedir. Yerel yönetimler de gelişen bilişim teknolojisine ve yaygınlaşan internet kullanımına kayıtsız kalmamakta ve hizmetlerini bu alanda da geliştirmektedir. Ancak bilişim alanındaki yatırımların yüksek olması yerel yönetimleri özgür ve açık kaynak kodlu yazılımlar kullanmaya yönlendirmektedir. Yetişmiş eleman konusunda avantajları olan pek çok belediye kendi olanaklarıyla ve deneyimleriyle özgür ve açık kaynak kodlu yazılımlara göç projeleri başlatmıştır. Yerel yönetimlerin göç stratejilerini iki temel karar yönlendirmektedir. Bu da özgür yazılıma göç çalışmalarını sunucular ve verilen hizmetler üzerinden mi başlanacağı yoksa belediyedeki son kullanıcılardan mı başlanacağı kararıdır.

Ancak herhangi bir göç çalışmasında başlamadan önce mutlaka çok ayrıntılı bir yazılım ve donanım envanteri çıkartılması gerektiği unutulmamalıdır. Envanter çalışması sonrasında uyumsuz olabilecek donanımların belirlenmesi ve göç projesinin belirli aşamalarında bu donanım grubunun değiştirilmesine yönelik çalışmanın planlanması gerekmektedir. Göç sürecinde kullanıcıların hangi yazılımları ne sıklıkla ve ne amaçla kullandıklarının belirlenmesi orta vadede pilot uygulamaların da nasıl yapılacağını belirleyecektir. Yapılan çalışmalarla uyumluluk matrisi oluşturulmalı ve önceliklendirmeler buna göre kararlaştırılmalıdır.

1 Türkiye Bilişim Derneği, Kasım 2018, Yerli ve Millî Yazılım Endüstrisi Raporu

Birçok yerel yönetim yetişmiş elemanlarının daha deneyimli olduğu sunucular üzerinden göç çalışmasına başlamayı tercih etmektedir. Öncelikle taşınabilecek basit ama temel hizmetlerden sayılan DNS gibi hizmetleri sonrasında ise e-posta, etki alanı ve veritabanları gibi diğer katmandaki hizmetlerin taşınmasını planlamaktadır.

Halen bazı yerel yönetimlerde göç çalışmaları başlamış olup sunucularda Pardus veya Linux çekirdeğine sahip uygun dağıtımları seçilebileceği, özgür veritabanlarından performans ve uyumluluğu açısından PostgreSQL'in, ofis uygulaması için Türkçe dil desteğinin bulunduğu LibreOffice veya OpenOffice'in tercih edilebileceği, etki alanı için kurumun gereksinimlerine uygun olacak şekilde OpenLDAP, SambaBox veya LiderAhenk kullanılabileceği, son kullanıcıların Firefox veya benzeri web tarayıcıları kullanabileceği şekilde planlamalar yapılabilmektedir. Basit hizmetlerin taşınması sırasında elde edilen deneyim ve motivasyon ile etkisi daha yaygın olabilecek hizmetlerin göçü planlanabilmekte ve üst yönetim desteği daha güçlü olarak sağlanabilmektedir.

Son olarak vurgulanması gereken önemli konulardan birinin göç stratejilerinden en sık karşılaşılan engelin sosyal faktörler olduğu unutulmamalıdır. Her göçte olduğu gibi özgür ve açık kaynak kodlu yazılımlara yapılan göçte de bazı sorunlarla karşılaşılabileceği, sosyal tercihler ve alışkanlıkların kırılmasında da üst yönetimlerin dirençli ve kararlı durmasının teknik ekipleri da daha motive edeceği unutulmamalıdır.

Dr. Hakan Kalyoncu

Yörenet Teknoloji Genel Müdürü

Boğaziçi Üniversitesi, Elektrik ve Elektronik Mühendisliği mezunu olan Kalyoncu, yüksek lisans ve doktorasını da aynı okulda gerçekleştirdi. 1982 yılında UNIX işletim sistemi ve C Programlama dili ile tanıştı ve profesyonel yaşamı boyunca sayısız yazılım geliştirme projelerinde görev aldı; çeşitli açık kaynak yazılım projelerine doğrudan ya da dolaylı olarak katkı sundu. 1988-1993 yıllarında Boğaziçi Üniversitesi'nde Araştırma Görevlisi, 1993-1998 yıllarında TÜBİTAK Marmara Araştırma Merkezi, Bilişim Teknolojileri Araştırma Enstitüsü'nde (MAM BTAE) Uzman Araştırıcı olarak çalıştı. Bu dönemde AUTOCORD kısa adlı EUREKA Projesinin ve GARİLDİ kısa adlı ve TTGV destekli ar-ge projesinin Proje Yürütücülüğünü yaptı; Teknoloji Yönetimi Derneği'nin kurucu üyesi oldu ve üç yıl boyunca yönetim kurulu üyeliği görevini yürüttü. Boğaziçi ve Marmara Üniversitelerinde konuk öğretim görevlisi olarak yüksek lisans dersleri verdi. 1999-2000 yıllarında TÜBİTAM MAM BTAE Enstitü Müdürü olarak görev yaptı. O dönemde Enstitüsüne kazandırdığı sayısız ulusal ve uluslararası projelerin yanısıra BTAE'nin Kara Kuvvetleri Komutanlığı'nın ATAK Saldırı Helikopteri Geliştirilmesi Projesi kapsamında Özgün Görev Bilgisayarı'nın Türkiye'de ve milli olarak geliştirilmesi için "Teknik Yönetim Sorumlusu" ve "Ana Yüklenici" olarak görevlendirilmesini sağladı. Aynı dönemde TÜBİTAK MAM Türkiye Ukrayna Ortak Araştırma Laboratuvarı Yönetim Kurulu Üyesi olarak görev yaptı. Halen Yönetim Kurulu Başkanlığını yürüttüğü YÖRENET Teknoloji A.Ş.'nin kurucu ortağıdır.

AÇIK KAYNAK KODLU UYGULAMALAR VE MİLLÎLEŞME ÇÖZÜMLERİ

Makalemde "Milli Yazılım ve Göç Stratejileri" konusundaki görüş ve deneyimlerimi sizlerle paylaşacağım. Ancak öncesinde "Milli Yazılım" kavramını biraz irdelemek ve bu terimden ne anladığımız ya da anlamamız gerektiği konusuna değinmek istiyorum. Ardından İşletim Sistemleri özelinde çeşitli ülkelerin milli yazılım deneyimlerinden örnekler verdikten sonra Açık Kaynak yazılımların önemini vurgulayacak ve bu konuda devlet ve kamu/özel sektör kurumları için öneriler getireceğim. Son olarak bu yaklaşım doğrultusunda uygulanabilecek olası göç stratejilerine değineceğim.

Millî / Özgür

Milli yazılım kavramını anlamak için öncelikle Milli sözcüğünün anlamına bakmamız gerekir diyerek Türk Dil Kurumu'na başvurduğumuzda doğru sözcüğün "Milli" değil "Millî" olduğunu görüyoruz.

Milli: sıfat Mil içeren

Millî: sıfat Milletle ilgili, millete özgü, ulusal

"İstiklal Harbi'nde millî duyguları aksettiren ümit ile dolu yazılarını hâlâ unutmadık." O. S. Orhon

Millî Yazılım bize ne anlatıyor?:

- Milletle ilgili yazılım?
- Millete özgü yazılım?
- Ulusal yazılım?

Sanırım bunların hiçbiri "Milli ve Yerli Yazılım" teriminin bizlere çağrıştırdığını tam anlamıyla karşılamıyor.

O halde bir de "Açık Kaynak" ya da "Özgür" yazılım kavramlarına bakmakta fayda var.

Millî Açık Kaynak

İlk bakışta Millî ve Açık Kaynak kavramları birbirleri ile çelişiyor gibi gözüküyor. Ancak gerçekte birbirlerini tamamlayan kavramlar bunlar.

Sormamız gereken ilk soru "Bu kavramların gerçekleştirilmesi mümkün mü?"

- Milletle ilgili açık kaynak yazılım?
- Millete özgü açık kaynak yazılım?
- Ulusal açık kaynak yazılım?

Mümkün ise "Katma değeri" ve "Sürdürülebilirliği" açısından üzerinde düşünmemiz gerekiyor. Bu bağlamda uzun felsefi tartışmalar yerine ülkemizde ve dünyadaki deneyimlere kısaca bir bakmamız yeterli olacaktır. Bu amaçla sistemlerin ana yazılımı olarak tanımlayabileceğimiz işletim sistemini temel alarak Milli İşletim Sistemi hedefine yönelik olarak ülkemizde ve dünyada bu konudaki deneyimlerden birkaçını buraya taşımak istiyorum

Milli İşletim Sistemi

Hangisi Milli İşletim Sistemi

	• Fedora / RHEL • OpenSUSE / SUSE • Ubuntu • CentOS • ...	• Pardus • Kylin • Red Star • Canaima • ...

Yukarıdaki tablonun sol kısmında günümüzde yaygın olarak kullanılmakta olan Linux tabanlı birkaç dağıtımı sıralanıyor.

Diğer tarafta ise yine Linux tabanlı birkaç "millî" dağıtımı listelenmiş durumda.

Ticari dağıtımlar hemen herkes tarafından bilinmekte o nedenle bu dağıtımlara sadece değinmekle yetiniyor, ayrıntılara girmiyorum. Ancak hangisi milli işletim sistemi sorusunu yanıtlamadan önce daha az bildiğimiz sağ taraftaki deneyimleri biraz daha detaylı irdelememizde fayda var.

Türkiye: Pardus

Türkiye'nin millî işletim sistemi olarak tanımlayabileceğimiz Pardus işletim sisteminin tarihçesini kısaca aşağıdaki gibi özetleyebiliriz:

- 2005 – 2011 yılları arasındaki birinci dönemi
    - Linux çekirdeği üzerine özel dağıtım olarak tasarlandı
    - Dağıtıma özel alt projeler oluşturuldu
        - Çomar – yapılandırma yönetimi
        - PiSi – paket yönetim sistemi
        - Yalı – kurulum aracı
        - Kaptan – masaüstü yapılandırma sihirbazı
        - ...
- 2012 ve sonrasındaki ikinci dönemi
    - Özel (millî) dağıtımdan vazgeçilerek Debian tabanlı dağıtım modeline geçildi,
    - Kamu ihtiyacı olarak ortaya çıkan çeşitli "millî olarak adlandırabileceğimiz" alt projeler oluşturuldu,
        - Ahtapot – çok katmanlı savunma,
        - EnGerek – kimlik yönetimi,
        - Etap – etkileşimli tahta,
        - LiderAhenk – merkezi yönetim
        - ...

Yukarıdaki kısa özetten kolaylıkla görülebileceği gibi 2005 yılında Linux çekirdeği etrafında özel ve özgün dağıtım olarak hayatımıza giren Pardus projesi zaman

içerisinde bu özgünlüğünden vazgeçerek Debian tabanlı bir dağıtım olarak yoluna devam etti. Altında kendine özgü ve "Millî" projeleri ile birlikte...

Kuzey Kore: RedStar OS

Kısa tarihçesi:

- 1998: ilk geliştirme Fedora tabanlı
- 2017: Red Hat 4.0 kullanımda

Özellikleri

- Kapalı ve güvenli bir işletim sistemi
- The Korea Times (Güney Kore gazetesi):... the operating system "is mainly designed to monitor the Web behavior of its citizens and control information made available to them."
- Ülke içerisinde kullanıma yönelik yapılandırılmış durumda geliyor
- MacOS'i andıran (KDE tabanlı) arayüze sahip

Özetle, ilk olarak 1998 yılında Fedora tabanlı olarak geliştirilen bu sistem, bir Güney Kore gazetesinde çıkan makaleye göre daha çok kullanıcısına sunulan bilgiyi kontrol etmeye ve kendisini kullanıcısına karşı korumaya yönelik yapılandırılmış.

Venezuella: Canaima

Kısa tarihçesi:

- 4 Mart 2011 – kamuda kullanılmak üzere resmen duyurulan Debian Linux tabanlı bir işletim sistemi

Özellikler

- GNOME grafik arayüze sahip
- LibreOffice kurulu olarak dağıtılıyor
- Dağıtıma özel WebKit tabanlı Cunaguaro web tarayıcısı var.

- Distrowatch Şubat 2013: son 12 aylık kullanıma göre dünyanın en popüler 185. dağıtımı

Özetle; 2011 yılında Venezuella tarafından kamuda kullanılmak üzere Debian tabanlı olarak geliştirilen Canaima işletim sistemi masaüstü bilgisayar kullanıcılarını hedefliyor ve internet istatistiklerine göre dünyada önemli bir kullanıcı sayısına ulaşmış durumda.

Çin: Kylin

Kısa tarihçesi:

- 2001 – 2010 tarihleri arasında Kylin OS adıyla FreeBSD tabanlı olarak kullanıldı.
    - Bu dağıtımın başlıca hedefleri:
        - Sunucu platformları desteği
        - Uluslararası Unix standartlarına uyum
        - Yüksek performans, devamlılık ve güvenlik
- 2010 yılında NeoKylin adıyla ve Linux temelli olarak yenişendi ve 2013 yılına kadar kullanımda kaldı
    - Masaüstü desteği öncelikli
- 2013 yılında Çin hükümetinin Ubuntu Linux'un geliştiricisi olan Canonical firması ile yaptığı anlaşma sonucunda Ubuntu Kylin adıyla halen kullanımda olan sürümü hazırlandı.
        - Masaüstü ve dizüstü bilgisayarlar için
        - Sogou Input Method for Linux (*) kapalı kod

Küba: Nova

2009 yılından başlayarak Ubuntu tabanlı ayrı bir dağıtım olarak Küba'da yaygın bir şekilde kullanılan bu sistemden 2018 yılında vazgeçildi ve indirme sunucusu kapatıldı. Küba Hükümeti Nova dağıtımı yerine CentOS ile devam kararı aldı.

Münih, Almanya: LiMux

Milli İşletim Sistemi'ne göçün en ilginç örneklerinden biri de Almanya'nın Münih il konseyinin 2003 yılında aldığı karar ile projesi başlatılan Ubunlu tabanlı LiMux işletim sistemidir.

Kısa tarihçesi:

- 28 Mayıs 2003 tarihinde il konseyinin planlamaya onay vermesi ile Ubuntu tabanlı bir dağıtıma geçiş süreci başladı,
- 2005-2013 yıllarında toplam 18000 kişisel bilgisayar ınMicrosoft Windows'tan LiMux'a göçü gerçekleşti,
- Bu dönemde proje sayesinde 16 M USD tasarruf edildiği raporlandı,
- İl Konseyi'nin Kasım 2017'de aldığı kararıyla 2020 yılına kadar tamamlanmak üzere tersine göç (Microsoft Windows) başlatılması kararlaştırıldı,
- Ekim 2018'de tesrine göçün destekçileri CSU ve SPD herbiri seçimde %10'dan fazla oy kaybetti. Bu nedenle projenin akıbetinin ne olacağı belirsizliğini koruyor.

"Millî İşletim Sistemi"ne Yaklaşımlar

Örnek Mili İşletim Sistemi deneyimlerini değerlendirdiğimizde her ülke farklı yollardan geçmekle birlikte 3 ana yaklaşım ile karşılaşıyoruz.

1 - Açık Kaynak'tan Kapalı ve Millî İşletim Sistemi

İlk olarak "Açık Kaynaktan Kapalı ve Milli İşletim Sistemi" olarak adlandırabileceğimiz yaklaşıma baktığımızda, bu yaklaşımın en başarılı örneği olarak Kuzey Kore RedStar OS karşımıza çıkıyor. Bu yaklaşımda mevcut herhangi bir açık kaynak işletim sistemi dağıtımını alıp kendinize özel dağıtım oluşturuyorsunuz. Bu dağıtımı amacınıza uygun bir şekilde yeniden yapılandırdıktan ve gerek duyduğunuz ya da uygun olduğunu düşündüğünüz şekilde güncelledikten sonra kendi özel dağıtımınıza sahip oluyorsunuz. Tabii ki sahiplendiğiniz tüm yazılım / paket lisanslarının bu şekilde kullanıma izin vermesi koşuluyla. Aslında ticari şirketler tarafından oldukça yaygın olarak kullanılan bir yöntem olan bu yaklaşımın bilinen en başarılı örneği olarak, Apple'ın freeBSD temelli MacOS işletim sistemini gösterebiliriz. Ve

"Milli Yazılım" geliştirmeyi düşünen ulusal şirketlerimiz için de dikkate alınması gereken bir yaklaşım olduğu kanısındayım.

2 - Açık Kaynak Millî İşletim Sistemi

Diğer bir yaygın olarak kullanılan yaklaşım, herhangi bir açık kaynak dağıtımın belirli bir sürümünü alıp kendi dağıtımınız olarak yeniden paketlenmesi şeklinde uygulanıyor.

Bu yaklaşım Pardus'un her iki fazında kullanıldı. Başlangıçta Pardus kendi özgün paket yönetimi gereçlerini kullanırken ikinci fazda Debian paketlerini kullanma yolunu tercih etti.

3 - Açık Kaynak Milli İşletim Sistemi

Bu yaklaşımın en ayırt edici özelliği "Millî" den vazgeçerek mevcut yaygın açık kaynak dağıtımlara yönelmek olarak karşımıza çıkıyor.

Bu bağlamda, topluluk desteği yanında kurumsal desteği olan dağıtımların kullanılması öneriliyor ve destekleniyor.

Bu amaçla yaygın olarak kullanılan dağıtımlar şunlardır:

- Ubuntu
- RHEL / Fedora / CentOS
- SLES / OpenSUSE

Hemen tüm demokratik ülkelerde yaygın olarak kullanılan bu yaklaşıma incelediğimiz birçok daha kapalı yönetimlerde de dönülmüş ya da dönülmekte olduğunu görüyoruz. Örneğin, yıllarca kendi dağıtımı olan Kylin işletim sistemini kullanmakta olan Çin hükümeti, 2013 yılında Ubuntu kullanmaya karar verdi. Üstelik kendisine özgü gerekli olduğunu düşündüğü farklılıkları da Ubuntu'nun sahibi olan Canonical şirketine yaptırtarak. Benzer şekilde yılarca kendi Millî işletim sistemi olan Nova'yı kullanan Küba, 2018 yılında bundan vazgeçerek mevcut CentOS dağıtımını kullanma kararı aldı.

Hangi Açık Kaynak?

Yukarıda dünyadaki uygulamalarına baktığımız her ülkede sürekli artan şekilde ilgi odağı olan Açık Kaynak İşletim sistemi kullanımının özellikle kapalı toplumlarda

başlangıçta "Millî Açık Kaynak İşletim Sistemi" olarak heyecan uyandırdığını görüyoruz. Ancak bu örneklerin neredeyse tamamında sürdürülebilirlik konusunun ciddi bir sorun olduğu gerçeği ile karşılaşıldığını, bir kısmının belirli bir yaygın dağıtımın (genellikle Debian) paketlerini kullanan ara çözümlere yönelmekle birlikte son aşamada doğrudan yaygın bir dağıtımı kullanmaya karar kılındığını görüyoruz.

Bu bağlamda, Türkiye'de "Milli İşletim Sistemi" ısrarından vazgeçip "Açık Kaynak İşletim Sistemi" ve "Açık Kaynak Projelere dayanan Milli Yazılım Sistemleri"ne yönelmek en akılcı yol olarak karşımıza çıkıyor.

Peki Türkiye olarak bunu nasıl gerçekleştirebiliriz?

Öncelikle bu konunun bir kurumun tek başına altından kalkamayacağı boyutta bir proje olduğunun kabul edilmesi ve Millî bir strateji geliştirilmesi gerekir. Bu stratejik yaklaşımda aşağıdaki üç ana başlık altında çalışmalar yürütülmesi faydalı olacaktır:

1. Açık Kaynak Yazılımlar için proje ekipleri oluşturulması

- Ulusal bir kurum (TÜBİTAK) koordinasyonu ile stratejik ar-ge konuları belirlenmeli, bu konulara uygun açık kaynak projeler seçilerek bu projelere katılım özendirilmeli ve bu projelere yapılan millî katkı oranında katılımcılar desteklenmelidir.

- Millî amaçlar doğrultusunda gerek duyulan yeni açık kaynak projelerin oluşturulması özendirilmelidir.

- Hedeflenen projelere uzman yazılımcı/grafiker/çevirmen katılımı sağlanmalı, bu projelerin ulusal öncelikler doğrultusunda yönlendirilmesine çaba gösterilmelidir.

- Mevcut Pardus projelerinin dağıtım bağımsız hale getirilerek gerçek açık kaynak projelere dönüştürülmesi çalışmasına hızla başlanmalıdır. Bu projelerin kendi topluluklarının (yabancı geliştiricilerin katılımı ile) oluşturulması ve büyütülmesi için çalışılmalıdır. Bu başarılabilirse milli projelerimizin major dağıtımların birer parçası olması sağlanabilir.
    - Ahtapot – çok katmanlı savunma
    - EnGerek – kimlik yönetimi
    - Etap – etkileşimli tahta
    - LiderAhenk – merkezi yönetim
    - ...

2. Yetkin çalışan havuzunun desteklenmesi

Kamuda gerek sunucularda gerekse masaüstü ve dizüstü bilgisayarlarda kullanılmak üzere birden çok sayıda (tipik olarak 3 ya da 4 adet) alternatif dağıtım belirlenmeli ve bu dağıtımların kullanılması desteklenmelidir.

Gerek kamu çalışanlarının gerekse özel sektör şirketlerinin belirlenen bu dağıtımlar için uygun ve geçerli sertifikalara sahip olmaları özendirilmelidir.

- Örneğin, belirlenmiş olan bu dağıtımlar için üretici firma tarafından verilen sertifika sahibi çalışanlara daha yüksek aylık verilmesi,

- veya da destek hizmetinin sadece yeterli düzeyde üretici firma sertifikasına sahip firmalardan alınması,

3. Nitelikli eko-sistem oluşması

Yukarıdaki ilk iki madde doğrultusunda çalışmalar yürütüldükçe eko-sistem kendiliğinden oluşmaya oluşmaya başlayacak ve zaman içerisinde niteliği artacaktır. Ancak, bu bunlara ek olarak kamu gereksinimlerini karşılamak üzere destek ekiplerinin oluşturulması uygun olacaktır. Benzer şekilde hizmet verecek destek ekiplerine sahip şirketlerin desteklenmesi yararlı olacaktır.

Özgür Yazılıma Göç

Peki bu "Açık Kaynak İşletim Sistemi" ve "Milli Yazılım" hedefine yönelik olarak kamu kurumlarımız ve özel sektörümüz nasıl bir yol izlemeli?

"Özgür Yazılıma Göç" ara başlığı altında bu konuyu biraz irdelemek gerekirse;

Göç 1

- Kurum içerisinde farkındalık yaratılması ve üst yönetimin desteğinin sağlanması göç projesinin başarısının olmazsa olmazıdır.

- Bu aşamada kullanıcıların eğitimi de planlanmalı ve ilk eğitimlere bu aşamada başlanmalıdır.

- Göç projesi gerek zaman gerekse kaynak açısından planlanmalı, bu planlama ile birlikte proje ekibi yetki ve sorumlulukları ile birlikte oluşturulmalıdır.

- Planlama aşamasında mevcut lisansların durumu da değerlendirilmeli. Olabildiğince lisans süresi ile uyumlu bir zaman planı yapılmalıdır.
- İstemci ve sunucu sistemler için kuruma uygun dağıtım(lar) bu aşamada belirlenmelidir. Belirlemede dağıtımın yaygınlığı ve arkasındaki topluluk desteği yanısıra yerel destek konusu da özellikle değerlendirilmelidir.

Göç 2

Bir kez göç kararı alındıktan sonra göç ile uyumlu olmayan yeni projeler kesinlikle engellenmeli, yeni geliştirilecek/alınacak yazılımların kurum göç stratejisi ile %100 uyumlu olması sağlanmalıdır.

Örneğin; uygulama kaynak kodu açık olsa dahi, belirli ürün/üretici bağımlılığı olan (Internet Explorer bağımlı web arayüzü, Oracle Web Logic bağımlı Java uygulaması, vb.) yazılımlar kesinlikle elenmelidir.

Göç 3

Ancak ilk iki aşama sorunsuz geçildikten sonra sistemlerin göç çalışmasına başlanmalıdır. Kurumun öncelikleri doğrultusunda planlandığı şekilde göç işlemi uygulamaya konmalıdır.

İdari kararlılık ve kurum içi sosyal ön hazırlıklar sayesinde teknik anlamdaki göç süreci sıkıntısız ve çalışanlar için eğlenceli bir seyahat haline gelecektir.

Sonuç

Milli Yazılım ve Göç Stratejileri konusundaki görüş ve deneyimlerimi sizlerle paylaşmaya çalıştığım bu makalemde, "Millî Yazılım" kavramı irdelenerek "Açık Kaynak" yazılımların ulusal projelerimiz için önemi vurgulandıktan sonra, dünyadaki "Millî İşletim Sistemi" örnekleri incelenmiş, bu yaklaşımın kısıtlı katma değeri yanısıra özellikle sürdürülebilirlik sorunundan kaynaklanan nedenlerle kaynak israfından öteye bir anlam ifade etmediği gösterilmiştir.

Bu bağlamda, "Millî İşletim Sistemi" ya da "Millî Yazılım" ısrarı yerine "Açık Kaynak" yazılımların ulusal boyutta ve stratejik anlamda desteklenmesinin önemi vurgulanmış, bu konudaki öneriler sıralanmıştır.

Son olarak kurumların "Açık Kaynak" sistemlere göçü için bir yol-haritası verilmiştir.

Kaynakça

- Comparison of Linux Distributions, https://en.wikipedia.org/wiki/Comparison_of_Linux_distributions
- Pardus web sitesi, https://www.pardus.org.tr/
- Red Star OS, https://en.wikipedia.org/wiki/Red_Star_OS
- Canaima (operating system), https://en.wikipedia.org/wiki/Canaima_(operating_system)
- Kylin (operating system), https://en.wikipedia.org/wiki/Kylin_(operating_system)
- Ubuntu Kylin, https://en.wikipedia.org/wiki/Ubuntu_Kylin
- Nova (operating system), https://en.wikipedia.org/wiki/Nova_(operating_system)
- LiMux, https://en.wikipedia.org/wiki/LiMux

Üstün Murat Yıldız

Pendik Belediyesi Bilgi İşlem Müdürü

Lisans öğrenimini T.C. Haliç Üniversitesi, Bilgisayar Mühendisliği bölümünde tamamladı. 2007 - 2008 yılları arasında Garanti Teknoloji firmasında mühendis olarak görev yaptı. 2008 – 2011 yıllarında dil öğrenimi tamamlamak için Amerika'da bulundu ve Southern States University'de İşletme Yönetimi üzerine yüksek lisansını tamamladı. 2012 yılında Pendik Belediyesi Bilgi İşlem Müdürlüğü'nde göreve başladı. İş Geliştirme Birim Yöneticiliği ve Yazılım Bölüm Yöneticiliği görevlerinde bulundu. 2016 yılı itibariyle, Bilgi İşlem Müdürü olarak görevini yürütmektedir.

BELEDİYECİLİKTEKİ BAŞARILI GÖÇ STRATEJİLERİ, PENDİK BELEDİYESİ MODELİ

Öncelikle sizlere Pendik Belediyesi'nde yapılan dijital dönüşüm hakkında detaylara girmeden kısa bir bilgilendirme yapacağım ve belediyelerde başarılı bir göç stratejisinin nasıl olması gerektiğini aktaracağım.

Özellikle 2009'dan itibaren bilgi teknolojileri alanında gerçekleştirilen yatırımlarla birçok kamu hizmetini vatandaşın belediyeye gelmeden alabilmesi sağlandı. Bu süreçte gerek TÜBİTAK gerekse diğer teknoloji sağlayıcılarından da destek alarak özellikle yerli teknolojilerin kullanımına öncelik veren bir yönetişim anlayışı ortaya koyduk. Dijital dönüşüm kapsamında, 2010 yılında fiziksel arşivlerin dijitalleştirilmesi tamamlandı. Böylece 2012 yılında, elektronik belge ve inşaat süreçleri içerisindeki tüm projeler (mimari proje, statik proje, elektrik proje vb.) dijital imza kullanılarak üretilmeye başlandı. Şehirdeki profesyoneller bu sürece dahil edilerek, bir model oluşturuldu ve tüm süreçler dijital ortama taşındı. Vatandaş başvuruları e-devlet üzerinden alınmaya başlandı ve bu çalışmalar sayesinde Türkiye'de belediyeler ilk kez e-devlet kapısı üzerinden hizmetlerini sunmaya başladı.

Dönüşüm süreçlerinde öncelikle üst yönetimin desteği bilişimcilerin arkasında olmalı ve ekip projeye inanmalıdır. Pendik Belediyesi olarak üst yönetimin vizyonu çerçevesinde bütün projelerde önce firmalara daha sonra yurt dışına bağımlılığı azaltmak ve zamanla ortadan kaldırmak düşüncesiyle bir hedef belirledik.

Bütün yeni alım ve geçişlerimizde açık kaynak kod ürün kullanmayı amaçladık. Kullandığımız yazılımları kaynak kodlarıyla almak ve mümkün olanları kendi yazılım ekibimizle ihtiyaçlarımızı karşılamak amacıyla yürüttüğümüz bu projeye Açık Kaynak Kod (AKK) Dönüşüm Projesi adını verdik. İş akışımızda Kurum Bilgi Yönetim Sistemleri (MIS) yazılımı başta olmak üzere birçok konuda önemli ilerlemeler kaydedildi. Aynı zamanda açık kaynak kod kullanım farkındalığı yükselen ve her geçen gün bu konularda yetkinliği artan bir personel grubuna sahip olduk. Açık Kaynak Kod Dönüşüm Projesi Vizyonumuzda ana motivasyon kaynağımız asla maddi olmadı. İlk önce dışa bağımlılığı azaltmak, bilişim ve teknolojide yerli üretimi teşvik etmek, İkinci olarak bilgi güvenliğini sağlamak temel amacımız olmuştur. Bunların yanı sıra elbette lisans maliyetlerinden kurtularak iyi bir tasarruf imkanı da elde ediyorsunuz. Örneğin; yaptığımız araştırmalar neticesinde Türkiye'de 1.397 belediyede yaklaşık 500 bin bilgisayar kullanılıyor. Bilgisayarların işletim sistemi olarak kullanılan yazılımları ve belediyecilik hizmetleri için kullanılan

diğer yabancı kaynaklı yazılımlara ödenen yıllık lisans maliyeti yaklaşık 15 Milyar TL olduğunu tahmin ediliyor. Tüm bu çalışmaların ülkemiz geleceği ve kurumumuz için ne kadar faydalı olabileceğini anlamamıza, değerli TÜBİTAK ekibiyle tanışmamız vesile oldu. İlk olarak, TÜBİTAK'la Kamu Açık Kaynak Kod Konferansı'nda temas kurduk ve araştırmalarımıza başladık, başarılı ve başarısız örneklerini inceledik. Öncesinde ve 2016 yılı içerisinde TÜBİTAK ile yapmış olduğumuz çalışmalar neticesinde, 2017 Şubat ayında ev sahipliğini yaptığımız Pardus Kullanımı ve Desteği konulu protokol imza töreniyle (İstanbul'da 9 ilçe belediyesi) TÜBİTAK'la çalışmalarımız resmiyet kazandı. Bu süreçte başta PARDUS olmak üzere Açık Kaynak Kodlu yazılımlara geçişimizde ivme kazanarak yeni bir döneme girmiş olduk.

Eğitim

Göç öncesi, iyi planlanmış bir eğitim bu süreçte ilk adım olmalı hatta eğitim göçün temeli olmalı diyebiliriz. Personelimize yönelik Pardus projesinin temelini oluşturan Linux ve diğer açık kaynak kod yazılımları eğitimlerine hız verdik. TÜBİTAK tarafından düzenlenen KAK öncesi eğitimlere, AB (Akademi Bilişim) eğitimlerine, LKD gibi gönüllülerin vermiş olduğu eğitimlere katılarak kurum olarak eksik olduğumuz konularda öncelikle bilgi işlem personelimizi dahil ederek yetkinlik seviyemizi artırdık.

ANALİZ ve PLANLAMA

Bilgi İşlem içerisinde göç hakkında her türlü konuyu konuşup, tartışıp ve karara bağlayacağımız bir proje ekibi oluşturduk. Pardus test ortamı oluşturarak analiz çalışmasını başlattık. Tüm müdürlüklerde kullanılan uygulama ve donanımların testlerini yaparak sorun olan noktaları tespit ettik ve bu listeye göre Pardus göçünü 4 faz halinde devam ettirme kararı aldık.

Bu fazların ayrımını kullanıcının bilgisayar kullanımına, zorluk derecesine ve gerekli donanımlara göre aşağıdaki gibi ayırdık:

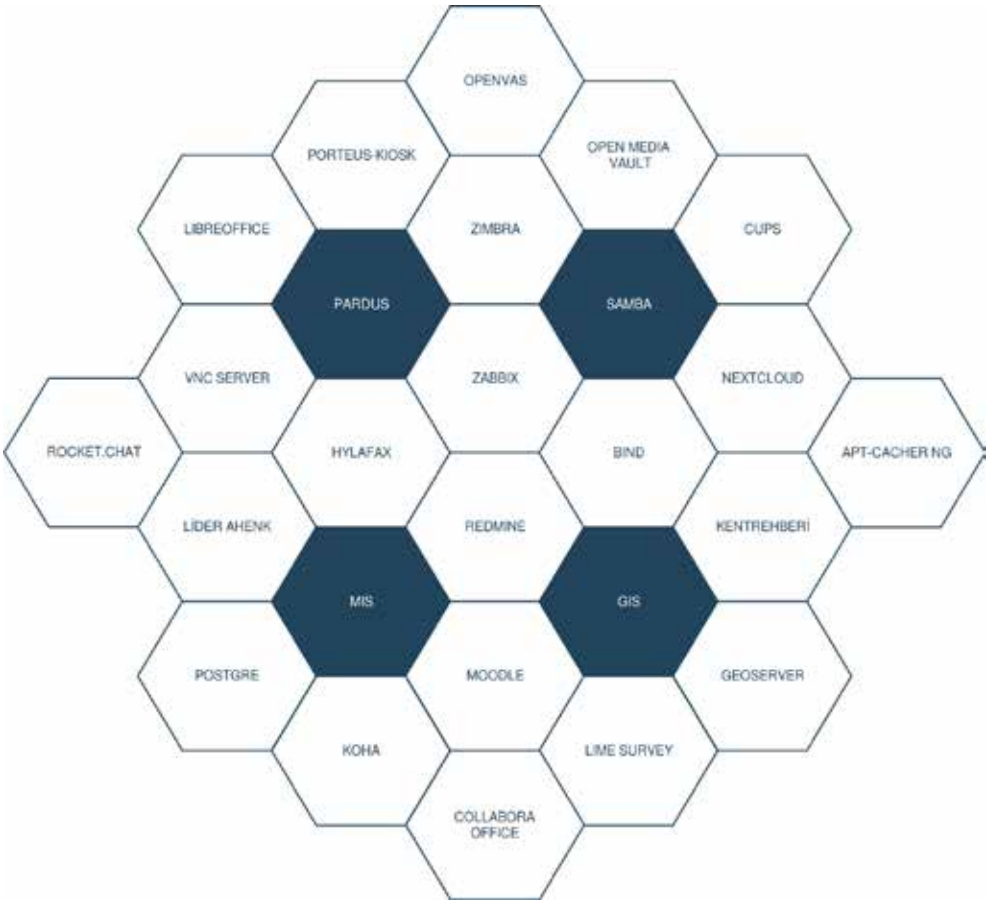
A. HEMEN GÖÇ (Hiçbir işlem yapmadan göç yapılabilecek kullanıcılar)

B. KOLAY GÖÇ (Göç için bizim çözüm üretmemiz gereken kullanıcılar)

C. ORTA GÖÇ (Göç için dış kurumların çözüm üretmesi gereken kullanıcılar)

D. ZOR GÖÇ (Göç için yüksek maliyetli çözüm veya köklü mimari değişikliği gerektiren kullanıcılar)

Planlama kapsamında hedeflerin belirlenmesi, görev dağılımlarının yapılması ve tüm işlemlerin kayıt altına alınarak karşılaşılan sorunların zaman kaybı yaşanmaksızın çözümleriyle oluşturulması için açık kaynak kodlu bir yazılımla yani Redmine'ı kullanarak projeyi yönetmeye başladık. Aynı zamanda karşılaşılan sorunların çözümlerini bir kütüphanede topladık. Projemizin bundan sonraki adımlarını ürün odaklı anlatmaya çalışacağım, proje kapsamında göç çalışmaları tamamlanmış ve önemli gördüğüm örneklerden bahsedeceğim. Diğer ürünler hakkındaki merak edilen detaylara Linkedin sayfamdan erişebilirsiniz.



1. Pardus (Son Kullanıcı İşletim Sistemi)

Açık Kaynak Kod Dönüşüm Projesi kapsamında birçok dönüşüm gerçekleştirdik. Bunların arasında en önemli yeri, Pardus dönüşümü oluşturmaktadır. Bilindiği üzere Pardus uzun zaman önce başlamasına rağmen çeşitli sebeplerle kesintilere uğramış, projeden istenen verim alınamamış ve kararlı bir halde kurumsal kullanıma uygun hale getirilememişti.

Özellikle son iki yılda bu konuda ciddi bir mesafe alınmış, sorunların çok büyük kısmı giderilmiştir. Pardus'un bu atılımı, yazılımı kullanmak için bizlere büyük cesaret vermiş ve dönüşüm sürecimizin hızlanmasına vesile olmuştur. Bugüne geldiğimizde 2018 yılında kullanıma sunulan Pardus 17.4 ile eski sorunların tamamına yakını çözüme kavuşturulmuş, özellikle son kullanıcı memnuniyetini sağlamada ilerleme kaydedilmiştir. Böylece Pardus projesiyle yabancı ve kapalı kaynak kodlu yazılımlara verilen yüksek lisans maliyetinden kurtulmak için tüm kamu kurum ve kuruluşlarına, özel sektöre önemli bir fırsat sunulmuştur. Kurumda kullanılan bilgisayarlar üzerinde kurulu tüm yazılım ve donanımların raporu çıkarılmış, bu yazılım ve donanımlarla ilgili yapılan arge çalışmaları ışığında göç yapılacak bilgisayarlar dört ana başlıkta toplanmıştır.

A) HEMEN GÖÇ (Hiç bir işlem yapmadan göç yapılabilecek kullanıcılar)

- Göç yapılmasında herhangi bir engel olmayan bilgisayarlardan oluşmaktadır. Bunlar kullanılan yazılım ve donanım özelliklerine göre Pardus'ta hiçbir sorun yaşamayacağı öngürülen bilgisayarlardan oluşmaktadır.

- Genellikle güvenlik, danışma, kütüphane vb. gibi sadece internet kullanan bilgisayarlar bu kapsama girmektedir.

- İlk olarak bu bilgisayarların göç işlemi tamamlanmıştır.

B) KOLAY GÖÇ (Göç için Pendik Belediyesinin çözüm üretmesi gereken kullanıcılar)

- Genellikle web tabanlı otomasyonlar, ofis, dosya sunucusu, yazıcı, tarayıcı vb. kullanan personellerin bilgisayarları bu gruba girmektedir.

- Müdürlüğümüzce kurulmuş Pardus Laboratuvarında bu bilgisayarlar üzerinde koşan yazılımlarla kullanılan donanımlar test edilmiş çalışmayan donanım ve yazılımlarla ilgili arge çalışmaları yapılmıştır.

- Arge sonuçlarına göre yazılım ve donanım birimlerimiz yapabilecekleri düzeltmeleri yapmış, sonucu müspet olan bilgisayarlarda göç işlemleri gerçekleştirilmiştir.

C) ORTA GÖÇ (Göç için dış kurumların çözüm üretmesi gereken kullanıcılar)

- Yapılan arge çalışmaları sonucunda çözüme kavuşturulamayan donanımsal ve yazılımsal sorunların yaşandığı bilgisayarlardan oluşmaktadır.

- Bu sorunlar TÜBİTAK'a bildirilmekte ve çözüme kavuşturuldukça sorunun yaşandığı bilgisayarlar göç ettirilmektedir.

D) ZOR GÖÇ (Göç için yüksek maliyetli çözüm veya köklü mimari değişikliği gerektiren kullanıcılar)

- Genellikle teknik müdürlüklerde bulunan bilgisayarlardan oluşmaktadır.

- Mevcut şartlarda Pardus'da çalışmayan, alternatifi bulunmayan ya da alternatifini yetersiz ve kullanışsız olan yazılım ve donanım mühteva eden bilgisayarlardır.

- Netcad, Autocad, Activex gibi programlar ya da eklentilerin yoğun kullanıldığı birimleri kapsar.

- Bu bilgisayarlar için ise uygulama sanallaştırma gibi projelerimiz mevcuttur.

2. LibreOffice (Ofis Uygulaması)

LibreOffice, daha fazlasını daha kolay ve hızlı yapmanızı sağlayan güçlü bir ofis takımıdır. LibreOffice, pazardaki en güçlü Özgür ve Açık Kaynaklı Ofis yazılımını oluşturmayı sağlayan birçok uygulama içermektedir: Writer kelime işlemci, Calc hesap tablosu uygulaması, Impress sunu, Draw çizim ve akış şeması uygulaması, Base veritabanı ve veritabanı ön ucu ve Math matematik yazılımı... LibreOffice, Word, Excel, PowerPoint ve Publisher gibi birçok belge biçimiyle uyumludur. LibreOffice, bunların ötesine giderek daha çağdaş bir açık standart olan Açık Belge Biçimi – ABB (OpenDocument Format – ODF) kullanımı sağlıyor.

Geçiş Aşamaları

- LibreOffice konusunda bilgi işlem personelinin ve müdürlük asistanlarının eğitimlerini tamamladık.

- Göç yapılmadan önce tüm işletim sisteminde LibreOffice sürümünü kurduk ve diğer Office uygulamaları ile eş zamanlı çalışmasını sağladık. Böylece geçiş öncesinde yaşanabilecek zorlukların önüne geçtik.

- Sonra tüm bilgisayarlardan diğer Office ürünlerini kaldırdık. Ofis uygulaması olarak sadece LibreOffice kurulumu yaparak tamamıyla ofis göç sürecini tamamlamış olduk.

- Diğer Office uygulamalarında oluşturulan doküman kullanılmak istendiğinde formül ve veriler düzgün çalışıyorken görsel biçimlendirmelerde sıkıntı yaşandığı görülmüştür. Bu dosyaların hibrit yapıda kullanılması yerine LibreOffice üzerinde yeniden oluşturulması sağlanarak büyük oranda problemin önüne geçilmiştir. Aynı sorun farklı kurum ve firmalardan gelen dosyalarda da mevcuttur. Dışarıda "Open Document" formatlarının kullanımı yaygınlaştıkça bu sorun ortadan kalkacaktır.

3. Zimbra (Mail)

Kurumumuzda geçmişte mail server olarak Microsoft Exchange Server kullanılmaktaydı. Microsoft Exchange Server üzerinde bulunan Takvim, Kişiler, Görevler, Mobil E-Posta Push Desteği özelliklerini karşılayabilen açık kaynak kodlu, e-Posta server olarak tespit ettiğimiz Zimbra Mail Server'a geçiş yapılmasına karar verildi.

Kullanıcı Geçişi

- Sunucu geçişi henüz başlamadan önce kullanıcı bilgisayarlarında Microsoft Exchange sunucusuna bağlı olarak çalışan e-posta uygulamasından kurtulmak amacıyla kullanıcılarda e-Posta istemcisi olarak Mozilla Thunderbird uygulamasına geçiş yapılmıştır.

- Exchange sunucunun terk edilerek Zimbra sunucuya geçiş yapılmasının ardından tüm kullanıcılarımızın masaüstlerine Zimbra web arayüzü kısayolu atılmıştır. Zimbrada bulunan web arayüzü desteğiyle çok kullanışlı basit arayüze personelimiz kısa sürede alışmıştır. e-Postaya ek olarak "Takvim, Görevler, Evrak Çantası" gibi özellikleri tam anlamıyla kullanılmaya başlanmıştır. Böylece Thunderbird'de yaşanan problemler çözüme kavuşmuş, e-Posta için masaüstü uygulama kullanımı terk edilmiştir.

Sunucu Geçişi

- Zimbra mail sunucusunun kurulmasının ardından Microsoft Exchange üzerinde bulunan 1.5 TB posta kutusu, Exchange sunucusu hala hizmet vermeye devam ederken Zimbra üzerine kopyalanmıştır. Bu kopyalama işlemi yaklaşık 20 gün sürmüştür.

- Tüm posta kutularının kopyalanmasının ardından Exchange sunucusunun hizmeti kapatılarak kullanıcı posta kutularında oluşan değişikliklerin kopyalan-

masına başlanmıştır. Bu süreç 3 günde tamamlanmıştır. Bu sürenin ardından Zimbra sunucumuz devreye alınarak kullanıma açılmıştır.

- Exchange sunucusunda bulunan Takvim Thunderbird üzerinden görüntülenememekte ve yönetilememektedir. (Yeni versiyonlarda denenmelidir.)
- Exchange sunucusu üzerinde bulunan adres defterinin ve e-Posta grupları çekilememektedir. (Yeni versiyonlarda denenmelidir.)
- Kullanıcı oturum bilgilerinin değişimi durumunda Thunderbird üzerinden hesap ayarlarının yeniden yapılandırılması gerekliliği sebebiyle arayüz karışıklığının da verdiği etkiyle bilgisayar bilgisi zayıf kullanıcılarda yaşanan E-Posta kullanım zorluğu mevcuttur.

4. Zabbix (Sistem ve Network İzleme Uygulaması)

Zabbix uygulama, sistem, ağ ve altyapıların izlenlenmesi (monitoring) ve uyarılar üretilmesi (alarm) için bir sunucu servisidir. Özgür bir yazılım olması, esnek kullanımı ve performansı sebebiyle tarafımızca kullanılmaya başlanmıştır. Bu uygulamayla uçtan uca bütün Sistem ve Network altyapısında ortalama 70.000 civarında sensörü izliyoruz.

GNU Genel Kamu Lisansı 2. sürüm kurallarına göre yayınlanmıştır.

5. Open Media Vault (Dosya Sunucusu)

Open Media Vault Debian tabanlı yeni jenerasyon bir dosya sunucusudur. İçerisinde SSH, FTP, SMB/CIFS, DAAP media server, Rsync gibi servisler bulunur. Modüler dizaynı sayesinde .eşitli eklentiler yazılıp uygulanabilir.

Kurumumuzda daha öncesinde Windows Fileserver kullanılıyordu. Özgür bir yazılım olması ve bütün paylaşım, kota ve izinlerinin yönetimini tek bir arayüzde toplayarak kolaylık sağladığı için Open Media Vault'a geçiş yaptık.

6. Lider – Ahenk Geçişi

Lider – Ahenk, kurumsal ağ üzerindeki sınırsız sayıda farklı sistemi ve kullanıcılarını tek merkezden yönetebilmeyi, izlemeyi ve denetlemeyi sağlayan, TÜBİTAK ULAKBİM tarafından geliştirilen açık kaynaklı bir yazılım sistemidir.

Kurumda Pardus göçü yapılan bilgisayarları ve kullanıcıları tek bir merkezden yönetebilmek, sürekli genişleyen ve değişen bilişim araçları üzerindeki kurumsal politikaların, güvenlik gereksinimlerinin etkin, esnek ve düşük maliyetlerle karşılanması gerekmektedir. Bu ihtiyaçları karşılamak üzere TÜBİTAK'ın da tavsiyesiyle kurumumuzda Lider-Ahenk kullanımına geçildi. Lider - Ahenk ve Lider Konsol olmak üzere üç ana bileşenden oluşmaktadır. Lider - Ahenk sisteminin merkezinde Lider bulunur ve Ahenkleri (clientleri) yönetmeye yarar. Ahenk; clientlara yüklenir, Lider'den gelen komutların clientta uygulanmasından sorumludur. Lider Konsol ise Lider'in kullanıcı arayüzüdür.

Lider Kurulumu

Lider – Ahenk installer ile Lider olarak hizmet verecek sunucu üzerinde aşağıdaki bileşenlerin kurulumu yapılır.

- Veritabanı
- Ldap Sunucu
- XMPP Sunucu
- Lider (Karaf) Sunucu

Bu aşamadan sonra Ldap ve Client yönetimi Lider Konsol arayüzü üzerinden yapılıyor.

Ahenk Kurulumu

- Lider – Ahenk installer ile clientlara kurulumu yapıldıktan sonra Lider'e benzersiz bir UID'yle register olur ve aşağıda bulunan görseldeki gibi Lider Konsol'da görünür.
- Lider Konsol üzerinde; clientlara politika uygulayabilme, ahenk bilgisi öğrenme, ekran görüntüsü alabilme ve betik çalıştırılabilme vb. işlemler yapılabilmektedir.

Avantajları

- Açık kaynak kodludur.
- Windows ve Aktif Dizin bağımlılığından kurtulabilmektedir.
- Tamamen yerli imkanlarla geliştirilmiştir.

- TÜBİTAK tarafından geliştirilmiştir.
- Çok fazla ve esnek eklentileri mevcuttur.
- Her ölçekte uygulanabilirdir.

Dezavantajları

- Ahenklerin UID'ye göre sıralanmasından kaynaklı hangi bilgisayarın hangi UID'ye ait olduğunun tespit edememekte ve tek tek ahenk bilgilerine bakılması zorunluluğu bulunmaktadır. (Yeni güncelleme ile çözüm getirilecektir. Bu sorunu aşmak için ayrı bir Calc belgesinde UID ve Hostnamelerin olduğu bir tablo tutulmaktadır.)
- Ahenk kurulumu sonrasında clientta yapılan değişikliklerin ahenk bilgisi kısmındaki bilgileri güncelleyememektedir.
- LDAP arama kısmında hostname, ip ya da her hangi bir veriye göre arama yapma özelliği stabil çalışmamaktadır.
- Geçiş yapılan dönemde kurulumla ilgili yeterli doküman bulunamamaktadır.

Not: Anlatımlar LiderAhenk sürüm 1.0 üzerinde yapılmıştır. Yakın zamanda yeni sürüm ile birçok sorun giderilmesi hedeflenmektedir.

7. HylaFax (Fax Sunucusu)

Kurumların faks alma-gönderme ve faksları saklama ihtiyaçlarını giderebilmek amacıyla hazırlanmış açık kaynak kodlu, geliştirilebilir, esnek, kullanıcı dostu, kullanımı basit, küçük, orta ve büyük ölçekteki kurumlara uygun ücretsiz bir faks programıdır.

8. Cups (Yazıcı Sunucusu)

Kurumumuzda 130 adet yazıcının üzerinde çalıştığı farklı bir yazıcı sunucusu kullanılmaktaydı. Yazıcı sunucusu üzerinde bulunan özellikleri karşılayabilen açık kaynak kodlu Cups Server'a geçiş yapılmasına karar verdik.

Cups Server kurularak kurumda bulunan tüm yazıcılar Cups Server'a taşındı. Tüm kullanıcılar Cups Server'a bağlanana kadar eski yazıcı sunucusu ve Cups Server aynı anda hizmet vermeye devam etti. Tüm kullanıcıların Cups Server'a taşınma-

sının ardından yazıcı sunucusunun kullanımı terk edilmiştir. Pardus kapsamında geçiş yapan tüm kullanıcılar yeni Cups Server'dan çıktı almak üzere kurulmuştur. Cups server driver paylaşıldığı için Pardus kullanıcılarına ayrıca driver kurmaya gerek kalmamıştır.

9. BIND DNS (Domain Name Server) Sunucusu

BIND (Berkeley Internet Name Daemon), Unix ve Linux işletim sistemleri üzerinde geçerli olarak gelen bir DNS servisidir. Dünyadaki isim sunucularının büyük çoğunluğu BIND üzerinde çalışır.

Kurumumuzda Bind'i aktif olarak kullanmaktayız. BIND yazılımı gerekli bütün sorgu ve dönüt işlemlerini içeren bir mimariye sahiptir. 3 temel bölümden oluşur:

- Domain Name Resolver
- Domain Name Authority Server
- Tools

Bu süreçler bir dizi toollar kullanılarak gerçekleştirilir, bunlara popüler bir örnek DIG Tool verilebilir. (DIG Tool BIND'a özel değildir, herhangi bir DNS sunucusunda da kullanılabilir.) BIND açık kaynaklı bir yazılımdır; eğer kurumunuz daha fonksiyonel bir yazılıma ihtiyaç duyuyorsa BIND'ı yeniden yapılandırabilirsiniz. Community tarafından sürekli geliştirilmektedir.

10. NextCloud (Bulut Uygulaması)

Gelişen teknolojiyle birlikte ihtiyaç duyulan tüm verilere her yerden ulaşılabilmesinin önemiyle ortaya çıkan ihtiyacımız üzerine bulut hizmetimizin de olmasına karar verdik. İhtiyaç üzerine yapılan araştırmalar sonucu Nextcloud ve Owncloud ürünleri öne çıkmıştır. Nextcloud'un tamamen ücretsiz ve kararlı olması sebebiyle Nextcloud'da karar kılarak bu ürün kullanıma alınmıştır.Ayrıca kurum içerisinde fileserver olarak kullanılan Linux Open Media Vault sunucularımıza entegrasyon sağlanarak mobil cihazlar üzerinden arazide bulunan personellerimizin bulut uygulaması aracılığıyla fileserverlara erişimi sağlandı.

Sunucu Geçişi

Linux sunucu üzerine Nextcloud uygulaması kurularak kurumsal ldap'ımızla entegre edildi. Kullanıcıların mevcut e-Posta hesaplarıyla bulut hesabına giriş yapabilmeleri sağlandı.

Kullanıcı Geçişi

Web üzerinden yayın yapan uygulamamıza tüm dünyadan mobil ve masaüstü uygulamalarıyla ayrıca web browser üzerinden erişilebilmektedir.

11. VNC (Anlık Ekran Paylaşma Uygulaması)

Kullanıcılara destek vermek amacıyla daha öncesinde bir mesajlaşma uygulamasının ekran paylaşma arayüzü kullanılmaktaydı. Bu mesajlaşma uygulamasının terk edilmesinin ardından kullanıcılara destek verme amacıyla VNC kullanımına geçilmiştir.

Özelleştirilebilme seçeneklerinin daha basit arayüzle yapılabilmesi sebebiyle öncelikle UltraVNC denenmiştir. Ancak UltraVNC'de Windows bilgisayarlar arasında yapılan bağlantılarda yaşanan kesintiler ve donmalar sebebiyle "TightVNC" uygulaması kullanılmıştır. TightVNC uygulaması Windows üzerinde service olarak çalışabilmekte aynı zamanda parola koruması ve bağlantı onayı seçeneklerini sağlayabilmektedir. Bu özellikler ile ihtiyacımızı karşılamıştır. Kullanıcının izinsiz bağlantıları önleyebilmesi için arkaplanda çalışan TightVNC servisinin yönetilmesini sağlayan bir program Bilgi İşlem Müdürlüğü tarafından hazırlanarak kullanıcı bilgisayarlarına yüklenmiştir.

12. Porteus-Kiosk (Kiosklar İçin Linux Dağıtımı)

Porteus Kiosk, sadece web tarayıcısı kullanmanıza izin veren, hafif bir Linux dağıtımıdır. Tarayıcının ayarları, kullanıcının yazılım indirme ve kurma işlemleri yapılmaması için ayarlanmıştır. Kiosk'u çalıştırdığınızda, seçiminize göre otomatik olarak Firefox veya Google Chrome açılır. Geçmiş kaydı tutulmaz, parolalar kaydedilmez ve güvenlik nedeniyle menüdeki çoğu ayar kapatılmıştır. Tarayıcı yeniden başlatıldığında, geçmiş kaydıyla ilgili herhangi bir iz kalmaması için bütün çerezler silinir ve yeni, temiz bir oturum açılır. Porteus Kiosk belediyemize bağlı ya da destek verdiğimiz; okullar, kütüphaneler, kafeler, ofis vb. yerlerde, bilgi, reklam, resim veya video görüntüleme amaçlı, web tabanlı otomasyon programları çalıştırma, kullanıcıların sadece internet kullanımına izin verilmesi istenen alanlarda kullanılmaktadır.

13. Koha (Kütüphane Uygulaması)

Küçük ölçekliden büyük ölçekliye her türlü kurumun/üniversitenin kolaylıkla kullanabileceği bir kütüphane otomasyon sistemidir. GPLv2 lisansıyla dağıtılır. Özgür yazılımın sunduğu olanaklar sayesinde özgürce ve ücretsiz olarak kullanılabilmektedir. Web arayüzünden kullanım ve yönetim sunan bir yapıya sahiptir ve Kültür Bakanlığına bağlı tüm kütüphanelerde kullanılmaktadır.

14. Moodle (Uzaktan Eğitim Uygulaması)

Moodle, özetle bir çevrimiçi kurs yönetim sistemidir. Kurum içinde verilen birçok eğitim, moodle portalı üzerinden hizmete sunulmaktadır.

15. Redmine (Proje Yönetim Uygulaması)

Kurumumuzca Pardus Göç Projesinin takibi için kullanılan açık kaynak kodlu bir web platformudur. Aşağıda giriş sayfası bulunmaktadır.

16. LimeSurvey (Anket Uygulaması)

Kurum içi ve kurum dışı anket uygulamalarında dışa bağımlılıktan kurtulmak ve açık kaynak kodlu bir uygulamaya geçiş yapmak amacıyla ubuntu sunucu üzerine LimeSurvey uygulaması kurularak hizmete alınmıştır. İç ve Dış Dns Kayıtları oluşturularak tüm dünyadan erişilebilir hale getirilmiştir bir anket ve forum uygulamasıdır.

Not: Kurulumu ve sistem gereksinimleri oldukça basit olan Limesurvey'in kurulumu hakkında detaylı bilgi için tıklayınız: https://manual.limesurvey.org

17. PostgreSQL (Veritabanı Uygulaması)

PostgreSQL; sql standartlarına uygun, açık kaynak kodlu ve ücretsiz, ilişkisel bir veritabanı yönetim sistemidir. Hemen hemen bütün Unix türevi işletim sistemlerinde ve NT çekirdekli Windows sistemlerde çalışır. PostgreSQL iyi performans veren, güvenlik ve özellik bakımından gelişmiş düzeydedir. PostgreSQL Postgres VTYS'nin geliştirilmesiyle oluşturulmuştur. Zengin veri tiplerini (Array, JSON, integer, boolean vs.) destekler. Açık kaynak dünyasında en güçlü veritabanı olarak bilinen PostgreSQL kurum içerisinde birçok projede aktif kullanılmış, sorunsuz çalıştığı gözlemlenen ürün tüm projelerde kullanması için karar alınmıştır.

18. GeoServer

Geometrik Dataları (veritabanları, wms,wfs,wmts yayınları ve SHP dosya kaynakları) web ortamında yayınlayabilmek için geliştirilmiş, geometrileri stil dosyasıyla gösterebilen tile server olarak tanımlanabilir. Haritacılar ve GIS yazılımcıları daha çok web tabanlı GIS uygulamalarında kullanılmaktadır. Platform bağımsız olarak kullanılabildiği ve web tabanlı yönetim GIS uygulamalarında neredeyse tüm formatları desteklediği için tercih edilmiştir. Platform bağımsız olarak kullanılabildiği ve web tabanlı yönetim GIS uygulamalarında neredeyse tüm formatları desteklediği için tercih edilmiştir.

19. Samba Domain (Aktif Dizin Sunucusu)

Samba projesi 1992'de Andrew Tridgell tarafından başlatılmıştır. Kendisi, Microsoft Windows kullanan bilgisayarlar ile dosya ve yazıcı paylaşımı yapmayı sağlayan araçlar topluluğudur. SMB ağ protokolünü kullanır ki bu Windows ağ uygulamasının kalbidir. Samba GNU Genel Kamu Lisansı altında yayınlanan tamamen özgür bir yazılımdır. Samba tam anlamıyla Windows AD'nin özelliklerine sahiptir. Ortamdaki Clientlar Domain sunucusunun Samba AD veya Windows AD olup olmadığını anlayamaz. Windows AD'nin Linux tarafında özgür ve muadil ürünü diyebiliriz.

Kurumumuzda Samba Domain testleri devam etmektedir. Şu anda kurumumuzda Samba4 kullanılarak yönetimi kolaylaştırmak amacıyla geliştirilen ürünler olan Profelis firmasının geliştirdiği Sambabox ve BeyazNet firmasının geliştirdiği Talia Domain ürünlerinin POC'leri yapılmıştır.

Avantajları

- Windows (veya Samba istemcileri) için bir sunucu vazifesi görme: dosya ve yazıcı paylaşımı. Buna PDF sahte-yazıcılar da dahildir. Böylece ağıdaki her yazıcı, PDF dosyalarını yazabilir.

- Bir Windows ağında alan denetleyicisi (Domain Controller) olarak iş görmek (kullanıcıları doğrulamak vb.) için kullanılabilir.

- Başka bazı karışık işleri yapmak için kullanılabilir. Örneğin Windows alan denetleyicisini (Domain Controller) kullanarak Linux/UNIX kullanıcılarının doğrulaması yapılabilir.

20. Collabora Office

Collabora Office uygulamasına Office 365 muadili olarak düşünebilirsiniz. NextCloud ürünü ile entegre ederek kullanabilirsiniz böylece kurum içinde kullandığınız ortak alanlarınızdaki dokümanlarıda düzenleyebilirsiniz.

21. Rocket.Chat

Diğer online chat uygulamalarında da olduğu gibi xmpp protokolünü kullanır ve muadilleri ile aynı ve birçok kullanışlı özelliğe sahiptir. Mobil, web ve platform bağımsız masaüstü uygulamalarına sahiptir, kullanışlı ve kararlı bir üründür.

22. Alfresco (Documentum Uygulaması) (Devam Ediyor.)

Alfresco açık kaynak kodlu kurumsal doküman içerik yönetim sistemidir. Genel olarak kullanılan standartlarla uyumludur ve tanınmış dosya tiplerinin büyük bir çoğunluğunu desteklemektedir. Kullanıcıların paylaşımlı disklerini bir bütün halinde kullanmamızı sağlar. İçerisinde web arama özelliğini Firefox ya da IE7 üzerinden sağlar. Bünyesinde yetkilendirme özelliği, sosyal medya entegrasyonu, kullanıcılara özellik atama, cloud üzerinden servis olarak kullanma özelliklerini bulundurur. Ürün açık kaynak kodludur ve geliştirilmek istendiğinde rahatlıkla geliştirilebilecek API'leri bünyesinde barındırmaktadır.

Alfresco, birçok ECM uygulamasını oluşturmak için kullanılabilir. Doküman, resim, dijital varlık ve web içeriği yönetimi gibi önemli uygulamaların yanı sıra işletmelere değer katan bir dizi özel uygulamalar vardır. Alfresco, data service, user interface, application oluşturma yetenekleri sağlar. Alfresco geliştirilirken Rest, Spring MVC, Spring Webflow ve Grails gibi frameworkler kullanılmıştır. Ürünün community versiyonu ücretsizdir. Kaynak kodu açık olduğu için özel ihtiyaçlar doğrultusunda ürünü geliştirmek de mümkündür.

23. ProcessMaker, Camunda, Activiti (BPM Uygulaması) (Devam Ediyor.)

Süreç Dizayn Aracı, İş Takip Ekranı Yönetim bölümlerinden oluşur. ProcessMaker ürünü BPMN 2.0 standartlarını destekliyor olup, bunun dışında Activiti BPM ve Camunda BPM ürünleride açık kaynak iş süreçleri yönetim platformu olarak, global çapta tercih edilen ürünler arasında yer almaktadır. Demo test çalışmalarımız tamamlandıktan sonra göç çalışmasını bu 3 üründen birine doğru yapmayı planlamaktayız.

Sonuç olarak, yukarıda kısaca sizlere aktarmaya çalıştığım ürünlerin göç çalışmaları tamamlanmış birçok uygulama kurum içerisinde aktif kullanılmakta ve çalışabilirliği ispat edilmiştir. Göç projesinin başarılı olabilmesi için öncelikle iyi bir ekibiniz olmalı ve bu ekip göç yapılabileceğine inanmalı veya tüm çalışmaları yapacak yetkin ve tecrübe sahibi bir firma ortağınız olmalı. Sonrası sadece bir noktadan başlanmak ve kararlılıkla vazgeçmeden sonuca gitmekte bitiyor. Belediyeler olarak; kütüphaneler, sosyal tesisler ve semt konakları gibi vatandaşa direk temas eden birimlerde Pardus ve yerli yazılımların kullanılması bu ürünlerin vatandaşa tanıtılması ve kullanım alışkanlığı kazandırılarak farkındalığın artırılmasına katkıda bulunabiliriz. Tesislerimizi kullanan gençlere dokunabilirsek, geleceğimiz için en büyük katma değer bu olacaktır.

Yazının daha detaylı versiyonu için: http://quq.la/rwAJ2


#ABZ2018
www.abz.com.tr
MARMARA
akıllı belediyecilik zirvesi
19 ARALIK 2018 İSTANBUL
Belirli Taşıtlara Özel Yeşil Dalga
Kuala Lumpur, Malaysia


2011


İSTANBUL

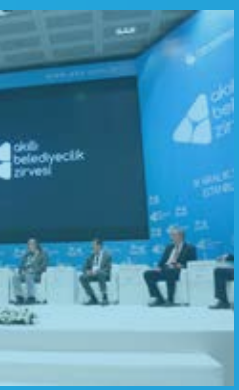

ŞEHRİN
MARI
isbak
sbak


akıllı
belediyecilik
zirvesi


param
MEGA


İSTANB


param
MEGA


akıllı
belediyecilik
zirvesi


BilgeAdam
TECRÜBE İS


MARMARA
akıllı
belediyecilik
zirvesi


kamusis
enerjis
muhas