İletişim Kuram ve Araştırma Dergisi - Sayı 57 /Bahar 2022
Ankara Hacı Bayram Veli Üniversitesi
İletişim Fakültesi
Süreli Elektronik Dergi
E-ISSN: 2147-4524

Veri İhlallerinde Kurumsal İletişimin Rolü: Yemeksepeti Örneği

The Role of Corporate Communication In Data Violations: Example of Yemeksepeti

Müge Bekman, Öğr. Gör. Dr., İstanbul Üniversitesi-Cerrahpaşa Üniversitesi TBMYO, E-posta: mugebekman@yahoo.com

https://doi.org/10.47998/ikad.1035349

Anahtar Kelimeler:

Halkla İlişkiler,
Kurumsal İletişim,
Mahremiyet,
Veri Mahremiyeti,
Siber Saldırı.

Öz

Çağdaş dönemin ayırt edici özelliği; yaşamın dijitalleşmesidir. Dijitalleşme doğrultusunda yaşamın her alanı etki altında kaldığı için kurumlar da bundan bağımsız değildir. Kurumlar, gün geçtikçe dijital teknolojilere daha çok angaje olurken, tüm işleyiş süreçleri de dijital dönüşümlere tabi olmaktadır. Bireyler açısından ise yeni mahremiyet, yeni bir boyuta evrilmektedir. Mahremiyet, klasik anlamını yitirirken veriye dayalı bir boyut kazanmakta ve bu veriler konusunda hem hassasiyet oluşmakta, hem de saldırılar artmaktadır. Veri mahremiyetine dönük siber saldırıların artışı ile kurumların hem önleyici, hem de bilgilendirici rolü her geçen gün daha da artmaktadır. Dolayısıyla bireylerin verileri konusunda daha hassas olmaları ile kurumsal iletişimin açıklamaya ve kontrol altına almaya dönük tavırları önem kazanmaktadır. Kurumsal iletişim veri mahremiyeti sürecini hem kurum içi, hem de kurum dışı olarak iki yönlü yürüterek kurumların her anlamda ayakta kalmalarını sağlamaktadır. Bu makalede hem uluslararası veri mahremiyeti raporları, hem de Yemeksepeti'nin yerel ölçekte yaşadığı veri hırsızlığı sorunu, kurumsal iletişimin rolü açısından nitel bir çalışma yöntemi olan durum çalışması (case study) ile incelenmektedir.

Keywords:

Public Relations,
Corporate Communication,
Privacy,
Data Privacy,
Cyber Attack.

Abstract

The distinctive feature of the contemporary era is the digitization of life. Since all areas of life are under the influence of digitalization, institutions are not independent of it. As institutions become more and more engaged in digital technologies, all their operational processes are subject to digital transformations. In terms of individuals, the new privacy evolves into a new dimension. While privacy loses its classical meaning, it gains a data-based dimension, and both sensitivity and attacks increase regarding these data. With the increase in cyber attacks on data privacy, both the preventive and informative role of institutions is increasing day by day. Therefore, with the fact that individuals are more sensitive about their data, the attitudes of corporate communication towards disclosure and control are becoming important. Corporate communication ensures the survival of institutions in every sense by carrying out the data privacy process both internally and externally. In this article, both international data privacy reports and the problem of data theft experienced by Yemeksepeti on a local scale are examined with a case study, which is a qualitative study method in terms of the role of corporate communication.

Araştırmacı Orcid ID : 0000-0002-8400-0993
Geliş Tarihi : 10.12.2021
Kabul Tarihi : 17.03.2022

Giriş

Yenilenen dinamikleriyle birlikte teknoloji, hayatın her alanında çok büyük bir hızla yerini almaktadır. Teknolojinin tarihi çok yeni olmasına rağmen, özellikle son iki yüzyıldır çok büyük teknolojik değişimler yaşanmakta ve insan hayatı da bu değişimden açıkça etkilenmektedir. İnsanların hayatlarının yeni bir uzantısı olan internet tabanlı araçlar, beraberinde getirdikleri kolaylıklarla birlikte bireyleri her geçen gün kendilerine daha bağımlı bir hale getirmektedir. Teknoloji, belirli kolaylıklar sağladığı gibi zorluklara da neden olmaktadır. Teknolojinin sağladığı birçok avantajın yanında bilinçsiz kullanım sebebiyle çok büyük riskler de söz konusudur. Teknolojinin bu denli hızla gelişimi ve her an erişime imkân tanıyan yapısı sayesinde, istenilen her yer ve her zamanda bilgiye ulaşmak oldukça kolay bir hale gelmiştir. Bu bilgilere özellikle de kişisel bilgilere başkalarının ulaşımı kolaylaşmıştır. Teknoloji; içerisi ve dışarısı, kamusal ve özel gibi ayrımları neredeyse ortadan kaldırarak, tek ve ortak bir alan yaratmaktadır.

Teknoloji bilgiye erişim imkânlarını her şekilde artırırken, gizli kalması gereken özel bilgilerin de korunması için yeni yöntemler oluşturulmasını sağlamaktadır. Teknolojik araçlar her türlü sınırı çok kolay bir biçimde aşabildiği için kişiye ait bilgilerin korunmasında farklı ve yeni yolların yaratılmasına imkân tanımaktadır. Eskiden bilgiyi belirli mekânlarda ya da ortamlarda muhafaza etmek mümkünken, bugün artık böylesi bir yöntem geçerli değildir. Çünkü gündelik hayatın her anı dijital ortamlara taşındığı için bir şeyleri saklamak kolay değildir. Dijital ortamlar, sadece bireylerin değil, aynı zamanda kurumların da yerini aldığı ya da alması gereken devasa bir platformdur. Ayrıca kurumlar, dijital ortamlarda müşterilerinin bilgilerinin güvenliğinden de sorumludur. Bu teknolojiler bireyleri bir yandan da dijital medyada gözetim nesnesinin gönüllü katılımcıları haline getirmektedir. Ancak kurumlar, insanların mahremiyetlerini ve veri güvenliğini sağlamakla mükelleftir. Çalışmanın ilerleyen bölümlerinde veri mahremiyetinin nasıl hayati bir öneme sahip olduğu detaylıca ele alınacaktır.

İnsanların gönüllü ortaklığıyla beraber gözetim artık normalleşmekte ve herkes tarafından kabul gören bir norma dönüşmektedir. Dijital medyada var olabilmek adına tüm bilgiler paylaşılmakta ve kurumların bunu işlemesine izin verilmektedir. Burada önem arz eden hususlar söz konusudur. Birincisi; insanlar her ne kadar bu dijital platformlara dâhil olsalar da bilgilerinin açıkça paylaşılmasını ve bilinmesini istemiyorlar, hatta mahrem olanın gizli olarak kalması gerektiğini düşünüyorlar. Bilinmek ve tanınmak gibi arzusu olmayan birçok insan için temel dürtü bu yöndedir. Bunun dışında ikinci konuyu; dijital ortamlarda elde edilen verilerin çalınmasını ve farklı amaçlarla kullanılmasını kurumların engelleme yönünde attıkları adımlar oluşturmaktadır. Dijital ortam, sürekli değişim içerisindedir, kurumsal iletişimin gözetleme ve gözetlenme ilişkilerinde müşterilerinin kişisel bilgilerini daha korunaklı hale getirmesi artık bir zorunluluk haline gelmiştir.

Çalışmanın ilk bölümünde; mahremiyetin kavramsal açıdan içeriğine bakılacaktır. Buradan hareketle tüm bu değişimin bir parçası olan kurumların da hızla değişen yenidünya düzeninde, mahremiyet kavramı eşliğinde, hedef kitlesiyle olan ilişkilerinin önemine, sahip oldukları verinin korunmasının, kurum ve marka sürdürülebilirliği açısından değerine değinilecektir. Kısaca konunun anlaşılabilmesi adına mahremiyet

perspektifinden hareketle, kurumsal iletişimin temel stratejileri, siber saldırılar ve koruma çalışmaları ekseninde anlaşılmaya çalışılacaktır.

Mahremiyetin Dönüşen Yapısı

Lügatte gizlilik manasına gelen mahremiyet kavramı (Türk Dil Kurumu, 2011), bir bakıma bir şeyin gizli hâli ve gizli yönü (Yeğin, 1993) anlamlarına da gelmektedir. Öte yandan bu kavram, kadın ve erkek ilişkileri ekseninde irdelendiğinde bilhassa özel mahiyette dokunulmazlık olarak da algılanmaktadır (Diler, 2014). Bireyin yaşamı toplumsal yapının şartlarından, toplumsal yapının şartlarını da bireyin yaşamından bağımsız olarak düşünülmesi mümkün değildir (Giddens, 2014, s. 25). Buradan hareketle toplumsal şartlar dikkate alındığı zaman, mahremiyetinde modernleşme sürecinde öneminin arttığı da görülmektedir. Toplumlar aynı zamanda paylaşmanın ve onaylanmanın da diğer adıdır. Bunun yanında paylaşılmış ve onaylanmış olanı da daha önemli bir hale getiren güçler birliğidir (Bauman, 2011, s. 46). Bununla birlikte günümüzde ise, bilgi işlem çağının yaşandığı gerçeği göz önüne alındığında, mahremiyet kavramının dijitalle belli bir bütün oluşturması da ayrı bir önem kazanmıştır. Mahremiyetin tanımı ile ilgili verilen hususlar, dijital mahremiyet kavramını tam olarak karşılayamadığı gibi salt tek yönlü değil, teknolojiyi üreten, kullanan ve etkileşim hâlinde olanlarla birlikte çok yönlü bir bütünün parçaları olarak görünmektedir (Barkuş & Koc, 2019). Birey, mahremiyet hakkını ve kavramını yaşantısının her alanında kullanabilmektedir ve kullanmalıdır da. Bu hak, doğumdan itibaren başlamakla birlikte, insanın yaşantısının her safhasında geçerli olacak bir olguyu ifade etmektedir. Mahremiyet kavramını Baudrillard tüketim toplumuyla ilişkilendirerek açıklamaktadır. Tüketimi artık sadece ürünlerin ve hizmetlerin tüketimi olmasının ötesinde, düşüncelerin de tüketimi olarak nitelemektedir. Bu tüketimi de her evde bulunan televizyonun bireyin en mahrem alanına girerek, medyayı bir araç olarak kullanarak bireyi bir tüketim metasına dönüştürdüğünü ve mahremiyetini etkilediğini söylemektedir (Baudrillard, 2008, s. 28-30). Nitekim günümüzde yapılan akademik çalışmalar, doğumda bile mahremiyet konularına eğilmekte ve bireyin yaşamındaki her alanın mahremiyetin sınırları ve hakları ile korunması gerekliliğini ortaya koymaktadır (Sayın Ağa & Kömürcü, 2015). Yirmi birinci yüzyılda insanının yaşantısını devam ettirebilmesi için bir bakıma bağımlı olmak zorunda kaldığı dijital teknoloji ve araçlar, mahremiyet kavramı içinde ayrı bir yer ve önem teşkil etmektedir.

Her bireyin kullanmakta olduğu cep telefonu, bilgisayar ve tablet gibi nesneler, internetle bağlantılı olarak adlandırılabilecek bu cihazlar, mahremiyet kavramına ayrı bir boyut getirmiş ve kavramı çok yönlü kılmıştır. Dijital medyanın son yıllar içerisinde hayatın hemen her alanına dâhil olması, dijital mahremiyete ayrı bir önem atfedilmesine sebep olmuştur. Dijital medya, mekân ve zaman sınırlarını ortadan kaldırarak bireylerin benliklerini sunma yarışına girmesine ve görme, gösterme, gözetleme sistemine dayalı yeni bir iletişim şekline neden olmaktadır (Utma, 2018). Dijital medyada iletişim araçları aracılığıyla bireylerin özel hayatlarına dair fotoğraflar yayınlanabilmekte ve yine bireylerin şahsiyetlerine dair yorumlar yapılabilmektedir (Gündoğdu, 2014). Bu durum, mahremiyet kavramını internet dünyasında korunmaya muhtaç bir olgu olarak ortaya çıkarmıştır. Çünkü bireye ait olanlar, ortalığa saçılmış durumdadır.

Teknolojinin vazgeçilmez bir unsur olmasıyla birlikte, insan hayatının her safhasını etkileyen ve dönüştüren muhtelif yeni ağlar da gündeme gelmektedir. Mesela internet böyle bir ağdır. Bununla birlikte artık mahremiyet ilişkisini tek bir yapı içerisinde değerlendirmenin doğru olmadığı gibi, gözetim kavramını da bu iki olgu ile irdelemek gerekmektedir. Özellikle son 20 yıl içerisinde mahremiyet ve gözetim ilişkisi bambaşka bir hâl almıştır ve her geçen gün değişmeye de devam etmektedir. Dijital kavramının dönüşümü, mahremiyet algısını da farklı bir boyuta taşımaktadır.

Gelişen enformasyon teknolojileriyle birlikte bilhassa devletler, halkı denetlemek ve gözetim altında tutmak adına birtakım teknolojik araçlardan yararlanmaktadır. En bilinen örnekler olarak e-Devlet Kapısı, e-belediyeler, MERNİS, MOBESE kameraları, e-kimlik gibi uygulamalar, bir başka deyişle dijital gözetimin unsurları olarak ortaya çıkmaktadır (Bozoğlu, 2018). En basitinden MOBESE kameraları kamusal alanlarda güvenliği sağlamak amacıyla yıllardır birçok ülke tarafından kullanılan bir gözetleme sistemidir (Goold, 2002, s. 191-193). Adı anılan uygulamalar, teknolojinin evrilmesiyle birlikte bireylerin hayatlarını daha da konforlu hâle getirmek için üretilmişlerdir. Ancak bir başka boyut, bu uygulamaların dijital gözetim ile doğrudan ilişkili olduğunu da gözler önüne sermektedir. Bu uygulamalar üzerinde yürütülen tartışmaların en önemlileri; e-Devlet Kapısıyla birlikte dijital vatandaşlığın modernleştirildiği, MERNİS Projesi ile global üretim sistemine uygun emek gücünün sağlandığı ve gözetim ile denetim tekniklerinin kullanıldığı uzun süredir tartışma konusu olmaktadır (Efe, 2013).

Mahremiyet; esasen bireyin koruması gereken ve istendiği kadar gözetime müsaade edilen bir kavramıdır. Ancak dijital çağda bu kavram anlamlarını ve niteliklerini hem kaybetmekte, hem de değiştirmektedir. Birey, dijital medya başta olmak üzere çevrimiçi ortamda mahremiyetin sınırlarını gözetmeden paylaşım yapabilmekte ve bunun sorumluluğu kendisinin üzerindeyken sonuçlarını bilmeyerek hareket etmektedir.

Mesela Google, Facebook ve Twitter gibi teknoloji devleri, geliştirdikleri her uygulamada kullanıcıya fayda ya da eğlence sunuyor gibi görünse de, aslında arka planda derin mahremiyet endişelerini de beraberinde getirmektedir. Bu bağlamda yüz tanıma sistemleri ile kişisel mahremiyetin birinci dereceden ihlâl edildiği çok açık bir gerçektir. Günümüzde popüler hâle gelen cep telefonlarında parmak izi ile tanıma sistemleri, bireyleri milyonlarca insandan ayıran en önemli özellik olan parmak izini doğrudan bu teknoloji firmalarının sistemlerine sunmakta ve kullanıma hazır hale getirmektedir. Mahremiyet ihlâli de bu noktadan sonra başlamaktadır. Çünkü kurumun kişisel verileri kötü niyetli kullanmama taahhüdüne karşılık, kötü niyetli kullanıcılar ve siber korsanlar mezkûr verileri kolayca ele geçirebilmekte ve bu veriler mahremiyet ihlâli konumunda değerlendirilebilmektedir.

Bugüne kadar teknoloji bağlamında veri ihlalini, yeni yüzyılın devasa siber firmaları nezdinde değerlendiren birçok çalışma yayınlanmıştır. Muhtelif veri ihlâllerinden ötürü cezaya mahkûm edilen Facebook da bu noktada sıklıkla eleştiriye tabi tutulmuştur (Sunal & Karadoğan, 2012). Facebook dışında Twitter, Instagram, Microsoft ve Google gibi yenidünya düzeninin devleri, mahremiyet algısına yeteri kadar hassasiyet göstermemektedir. Zira mahremiyet, başkaları tarafından değil, bireyin bizzat kendisinin

koruması gereken bir olgu hâline getirilmiştir. Kişisel unsurların ve bilginin, veri olarak kıymetli bir hale gelmesi ile mahremiyet pratiklerinin veriye odaklı bir biçimde dönüştüğü görülmektedir.

Dijital Çağda Veri Mahremiyeti

Veri paylaşımı açısından dijital gözetimin her zaman "kötü" veya "faydasız" olması düşünülemez. Sanal âlemde paylaşılan kişisel veriler ve bu verilerden işlenerek ortaya çıkan başkaca veriler, kimi zaman kullanıcı konumundaki bireyin lehine olabilmektedir. Mesela son on yılda daha da gelişmiş olan dijital reklam algoritmaları, kullanıcının kişisel ilgi alanlarına yönelik ürün ve hizmetleri sunmayı başarabilmektedir. Daha önce satın alınarak okunmuş bir kitaba benzer başka bir kitabın reklam olarak gösterilmesi bu durumu açıkça ispat etmektedir (Özdemir, 2020). Dijital medyada yapılan tercihler, kullanılan platformlar, arama motorlarındaki kelimeler, beğenilerin oluşturduğu kişisel veriler, yine dijital medyadaki kurumlarca satın alınmakta ve ürünlerini onlara uygun hedef kitleye yönlendirmede daha da başarı sağlamaktadırlar. Böylece birçok farklı problem hiç doğmadan çözüme kavuşturulmaktadır. Ancak çok farklı ve büyük hukuki sorunlar da söz konusu olabilmektedir.

Mahremiyetin ve dijital gözetimin en önemli neticesi; hiç şüphesiz insan haklarına yapılan ihlâllerdir (Bölükbaş, 2014). Günümüzde kullanıcılar daha çok merak ve keyif için dijital mecralarda vakit geçirmektedirler. Bu aktiviteler, kimi zaman insan hakları ihlâline kadar giden veri hırsızlığını da beraberinde getirmektedir. Sıklıkla tartışılan konu, teknoloji firmalarının ürettiği yazılımlar aracılığıyla, siber korsanların yaptıkları işi kullanıcıların kendi izinleriyle gerçekleştirmeleri ve kişisel verileri ihlâl etmeleridir. Nihayetinde çoğu kullanıcı, herhangi bir yazılımı kullanırken, yazılım kullanım koşullarını incelememekte ve kullanımından doğacak olan veri işleme ve kullanma izninin neler olduğunu bilmemektedir. Bu durum siber zorbalık ile değil, kullanıcının tamamen kendi inisiyatifi ile verilen bir karar olduğu için, bilinçsiz de olsa mahremiyet ihlâli anlamına gelmektedir. Bu hususun en korkunç tarafı, esasen bireyin yaşantısının her alanında görülmesidir. Zira telefon görüşmelerinin kaydedilmesi, konum verisi ile bulunulan lokasyonun kayıt altına alınması, kredi kartı nakit akışları ve yaşam alışkanlıkları gibi her türlü mahrem bilgi, dijital gözetimin menfi tarafları arasına girmektedir (Canbolat, 2013). Bireyin sahip olduğu tüm bilgiler ve dijital hareketleri de aynı zamanda veri olarak işlenmekte, depolanmakta ve sonrasında gerekli görülen her koşulda kullanılmaktadır.

Bununla birlikte dijital dünyanın en önemli merkezleri hâline gelen dijital ağlar, dikkate değer bir yapıya sahiptirler. Kimi araştırmacılar, gözetleme ile söz konusu dijital paylaşım sitesinde yapılan paylaşımların aralarında bir ilişki olduğunu düşünmektedirler. Onlar için yeni bir kamusal alan konumundaki dijital platformlar, bireylere gerçek dünyadan daha özgür bir ortam sunmaktadır. Bu ortam dâhilinde gözetleme "merak" unsurunu, gözetlenme de "beğeni" kültürünü tetikleyerek daha başka insanlara ulaşma ve gözetleme durumunu meydana getirmektedir (Türk & Demirci, 2016).

Fakat burada yeni bir sorun ortaya çıkmaktadır. Bu sorun beğenilme ve gözetleme unsuru aracılığıyla bulunulan kamusal sahaların aslında "bedava" olmamasıdır. Çünkü esasen yeni kamusal alan olarak kabul edilen bu tür dijital paylaşım sitelerinde ürün,

kullanıcının kendisi olmaktadır (Goodman, 2016). Kullanıcının izni dâhilinde ortaya çıkan veri paylaşımları, bu kamusal mekân sahibi global "unicorn" şirketlerin, veri işleme hizmetini çok öte prosedürler ile gerçekleştirerek yukarıda da örneği verildiği üzere kişiselleştirmede çığır açmaktadırlar. Ancak bu işlemler gerçekleştirilirken, sağlanan kamusal alan hizmetinin bedava olduğu algısı insanlarda bulunmaktadır. Konunun ne denli önemli olduğunun anlaşılması açısından, 2018 yılında ortaya çıkan büyük bir veri ihlâlini hatırlamak yeterli olacaktır. İngiltere Bilgi Komisyonu, Londra Analytica isimli veri analiz firmasının, popüler dijital paylaşım sitesi Facebook'ta kayıtlı bulunan 50 milyon kullanıcının profil verilerini usulsüz olarak kullandığını duyurmuş ve konuyla ilgili olarak soruşturma başlatmıştır (BBC News, 2018). Dünyada gerçekleşen ve en büyük veri ve gizlilik ihlâline verilen cezaya istinaden Amerika Federal Ticaret Komisyonu, Facebook'un 5 milyar dolar ceza ödeyeceğini duyurmuştu (Sputnik, 2019). Kurumlar sahip oldukları kişisel verileri[1] depoladıklarında ayrıca bunların güvenliğinden de sorumlu oldukları gerçeğini kabul etmelidirler. Bu bilgilerin mahremiyetinin sağlanması hedef kitlenin tercihlerini de etkilemektedir. Dolayısıyla kurumlar veriler ile hedef kitlelerini gözetlemekte, yönlendirmekte ve gelecekteki adımlarını hem öngörmekte hem de yönlendirmektedir.

Mahremiyete Siber Saldırıda Kurumsal İletişimin Önleyici Rolü

Yirminci yüzyılın ikinci yarısından bu yana dijital çağ kapsamında siber korsanlık faaliyetleri artarak devam etmektedir. Dijitalleşmenin internetle birlikte hız kazandığı 1990'lar, çok önemli bir tarihsel kırılma anıdır. Çünkü internet ağı (world wide web) tüm dünyayı kuşatarak yeni bir sürecin başlatıcısı olmuştur. Bir yandan da kişisel bilgisayarların (personal computer) yayılması ile süreç eşzamanlı olarak ilerlemiştir. Artık herkes istediği anda istediği kurum ve kişi ile irtibata geçebildiği gibi dışarıdan gelebilecek saldırılara da açık hale gelmiştir. Bu süreçte özel alan yani mahremiyet ev içinde kalmayıp dışarıya taşındığı gibi dışarısının yani kamusal alanın da içeriye gelmesine imkân tanınmaktadır. Dolayısıyla yeni bir tehdit ve süreç insanların hayatına siber saldırı olarak dâhil olmaktadır.

ABD Ulusal Araştırma Konseyi 2009 tarihinde Siber Saldırıyı bilgisayar sistemleri üzerinden bilgiyi hedef alan, değiştiren, küçük düşüren ya da yok eden kasıtlı eylemler olarak tanımlamıştır (Singer & Friedman, 2015). Siber güvenlik kavramı Türkiye'de Ulusal Siber Güvenlik Stratejisi ve 2016-2019 yıllarını kapsayan Eylem Planında da şöyle tanımlanmıştır:

> "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini" (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016).

1 Türkiye özelinde kişisel verilerin korunması kanunu Resmî Gazetede 7/4/2016 tarihinde, 6698 sayılı kanun numarasıyla yayınlanmıştır. Bu kanunun birinci maddesinde kanunun amacı şu şekilde ifade edilmektedir: "Bu Kanunun amacı, 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 düzenlemektir" (Kişisel Verilerin Korunması Kanunu (KVKK), 2016, madde 1).

Her geçen güz hızla değişen ve gelişen teknolojiye bağlı olarak siber saldırılar da artmaktadır. Bu saldırılardan dolayı meydana gelen yıkıcı sonuçlar ve maddi zararlar neticesinde ülkeler ve kurumlar olası tehditler karşısında önlem almak ve savunma stratejileri geliştirmek zorunda kalmaktadırlar (Yayla, 2014, s. 185). Siber saldırılar hem bireylere, hem de kurumlara gerçekleştirilen birçok saldırıyı, dolandırıcılığı ve atağı ifade etmektedir. Bu faaliyetler kötü niyetli bilgisayar korsanları tarafından kimi zaman para, kimi zaman eğlence, kimi zaman da şöhret ya da sabotaj için gerçekleştirilmektedir.

Siber saldırıların tarihi çok eskilere gitmese de bilgi açığı üzerinden avantaj sağlamak daima var olagelmiştir. İnternet, bilgisayar ve akıllı telefonlar ile siber saldırıların doğası iyice değişmiştir. Veri üzerinden yapılan saldırılar çok kalabalık kitlelerin tüm mahrem bilgilerini çalmak ve sonrasında manipüle etmek için kullanılmaktadır. Veriye dayalı saldırılar eskinin değerli tüm maddi çıkarlarını ifade etmekte, hatta bugünkü karşılığı olmaktadır. 2000'li yıllardan itibaren artık siber korsanlar faaliyet alanlarını tamamen kişisel verilere odaklamış durumdadır. Kişisel verilere erişilen alanda, muhtelif algoritmalarla başka bilgilere erişmek de mümkündür. O yüzden kişisel veriler üzerinden başka bilgilere geçiş yapmak ve daha fazlasına erişmek imkân dâhilindedir.

İnternet kullanıcılarının birçoğu, izahlara rağmen kişisel verilerinin ele geçirilmesini, para kaybedilen bir siber korsanlık eylemiyle bir ve eş tutmamaktadır. Onlar için para çok daha mühim bir rol oynamaktadır ve kişisel bilgiler birçok açıdan önemsiz hale gelmektedir. Oysa gelişen hukuk sistemlerinde kişisel verilerin önemi yasal düzenlemeler ile güvece altına alınmaya ve kullanıcılar bilinçlendirilmeye başlanmıştır. Özel hayatın gizliliği de, önem derecesi had safhada olan bir konudur. Bu anlamda özel hayatın fiziksel olarak korunduğu konutlar, düşünsel anlamda genişletilerek siber alan kavramıyla özdeşleştirilmiştir ve konunun bağlamı sadece maddi unsurlar ile sınırlandırılamayacağı görülmüştür.

Nitekim İtalyan Ceza Kanunu'nda "siber alan" kavramı; özel hayatın gizliliğini nitelendiren en önemli unsur olan "konut" kavramıyla bir tutulmuştur (Talay, 2018). Siber korsanlık faaliyetlerine mevzu olabilecek kişisel verilerin toplanması, sadece kullanıcının rızasına bağlanmış olup daha sonra da bu verilerle ilgili gerekli düzeltmelerin kullanıcı tarafından yapılabilmesi ön görülmüştür. Kullanıcılar, kurumların sahip oldukları kişisel verilerin gene kurumlar tarafından korunmasını istemelidir. Kullanıcılar bu durumu kurumsal yapı içerisinde iletişim süreçlerinin bir görevi olarak görmektedir. Bireye göre kurum, sahip olduğu hedef kitlesinin bilgilerini depolayabilir ama başkalarının gözetiminden korumalıdır. Dolayısıyla bugünün en önemli tehdidi olabilecek mahremiyete saldırı olan siber saldırı, önemini çok kuvvetli bir biçimde korumaktadır ve gelecek dönemlerde önemi daha da artacaktır.

Literatüre bakıldığında benzer çalışmalar görülmektedir. Kurumsal veri ihlali, nedenlerini, zorluklarını, önleme ve gelecek talimatlarını içeren makalede; son yıllardaki kurumsal veri ihlallerinden, milyonlarca bireyin kişisel bilgilerinin sızdırılmasının sonuçlarından ve bu nedenle ortaya çıkan milyonlarca dolarlık mali zararlardan bahsedilmektedir (Cheng, Liu, & Yao, 2017, s. 3). Başka bir çalışmada veri ihlallerinin bağlamsal risklerine ampirik bir yaklaşım üzerinden bakılmış ve veri ihlallerini artışından

etkilenen kurumlar için ciddi mali ve yasal sonuçları olan olaylar incelenmiştir. Buradan hareketle bağlamsal veri ihlali riskini artırabilecek veya azaltabilecek faktörleri belirlemek için fırsat suç teorisi, kurumsal anomi teorisi ve kurumsal teorinin uygulanması üzerine araştırmalardan bahsedilmektedir (Sen & Borle, 2015, ss. 314-341). Kurumun hedef kitlesinin kişisel ve kart bilgilerinin veri ihlalinde neden korunması gerektiği araştırılmakta ve bu kayıplar sonucu kurumların ne kadar zarara uğradığı gösterilmektedir (Manworren & Letwat, 2016, ss. 257-266). Veri ihlallerinde olayların tamamen ifşa edilmesinin, kimlik hırsızlıklarının azaltılmasındaki rolüne bakılmış ve ampirik çalışmalar sonucunda bunun %6,1'lik bir oranda azaldığı tespit edilerek, farklı bir yaklaşım metodu ortaya konmuştur (Romanosky, Telang & Acquisti, 2011, ss. 256-286). Son olarak; büyük veri ihlalinde oldukça gündemde yer tutan Cambridge Analytica, 50 milyon Facebook kullanıcısının bilgilerini, seçmenlerin profillerini kullanılmıştır. Böylece, Cambridge Analytica olayı en büyük veri ihlallerinden biri olmuştur. Aynı zamanda bu verilerle birlikte güçlü bir yazılım oluşturulmuştur. Bu yazılımla elde edilen veriler, sandıktaki seçimlerin sonuçlarını tahmin edebilmek ve etkileyebilmek için kullanılmıştır. (Cadwalladr & Graham-Harrison, 2018, ss. 17, 22).

Amaç ve Yöntem

Bu makalede nitel araştırma yöntemlerinden durum çalışması (case studies) ya da bir diğer adıyla örnek olay analizi kullanılmaktadır. Ele alınan durum ise; veri ihlalleri ve bu ihlaller karşısında kurumların, kurumsal iletişim stratejisi olarak neleri benimseyip nasıl davranışlar sergilediğini incelemekten oluşmaktadır.

Durum çalışmasında bir olguyla ilişkili olarak bütüncül bir yorum ve analiz hedeflenmektedir. 1960 ve 1970'ler boyunca pozitivist araştırma yönteminin egemenliği doğrultusunda, nitel bir çalışma olarak durum çalışması pek kullanılmamıştır. Ancak 1980'lerden itibaren durum çalışmaları artmış ve alandaki uygulamaları hızlı bir yükseliş göstermiştir (Hartley, 1995). Durum çalışması bazen bir, bazen de birden fazla olayın, olgunun, programın ya da iç içe geçmiş yapıların incelenmesini sağlamaktadır. Durum çalışmalarında ele alınan konu, belirli bir zamana ve mekâna hapsedilerek tanımlanmakta ve incelenmektedir. Aynı zamanda durum çalışmasının kendi içerisinde altı adet alt türü vardır. Bunlar; kısaca tarihsel örgütleme (historical organization), gözlemsel (observational), hayat hikâyesi (life history), durum analizi (situation analysis), çoklu alan (multisite) ve çoklu durumdur (multicase) (McMillan, 2000). Bu makalede ise; durum çalışması içerisinden iki alt başlık olan gözlemsel ve durum analizi birlikte kullanılmaktadır. Çünkü ele alınan veriler ve kurum davranışları hem belirli gözlemlere, hem de durumlara dayanmaktadır. O durumlar içerisinde kurumların veri hırsızlığına dair verdikleri cevaplar ise gözlem kısmını oluşturmaktadır. Bu nedenden ötürü durum çalışmasının iki alt yöntemi birlikte kullanılmakta ve veri ihlallerine dair çok daha kuşatıcı cevaplar aranmaktadır.

Durum çalışmasının analizi en temelde üç amaç doğrultusunda kullanılmaktadır. Birincisi; herhangi bir olayı doğuran nedenleri ve ayrıntıları tanımlamaktır. İkinci amaç; o olayla ilgili olarak olası açıklamaları ve ihtimalleri gündeme getirmektir. Son olarak ise;

olayı bütüncül bir şekilde değerlendirebilmektir (Gal, Borg, & Gall, 1996). Aynı zamanda durum çalışması genellikle güncel bir olay etrafında gerçekleştirilmektedir. Olayın kesin sınırlarını çizmek zor olduğu ve birden çok kaynaktan veri geldiği için bütüncül ve yerinde bir analiz gerektirmektedir (Yin, 1984). Dolayısıyla birçok noktadan elde edilen veriyi düzgün ve bütüncül bir biçimde değerlendirmek önem arz etmektedir.

Örnek olaylar çalışma şekilleri bakımından ise genel itibariyle üçe ayrılmaktadır (Berg & Lune, 2015, s. 367-368):

> 1) Keşfedici örnek olay: Herhangi bir olgu yakından gözlemlenerek ortak bir teorileştirilmeye gidilmektedir. Çok daha büyük bir yapının küçük bir örneklemini teşkil etmektedir.
>
> 2) Açıklayıcı örnek olay: Nedensellik bağları araştırılırken kullanılmaktadır. Karmaşık olguları ve birden fazla değişkeni incelemektedir.
>
> 3) Tanımlayıcı örnek olay: Genel teorik bir yaklaşımdan hareketle ele alınan olguya yaklaşılmaktadır. Ele alınacak olan örnek olay net bir şekilde tanımlanmaktadır. Çünkü başlangıç aşamasındaki tanıma göre araştırma süreci belirlenmektedir.

Durum çalışmaları, kendi içerisinde ele alınan konunun büyüklüğüne değişik gösterebilmektedir. Bazen bir olgu, olay, kişi ya da gruplar çalışmanın konusunu oluşturabilmektedir. Dolayısıyla araştırma esnasında tek bir sorun ele alınabileceği gibi birkaç soruna da birlikte odaklanmak mümkündür. Bu çalışmada ise örnek olay çalışma şekillerinden farklı biçimlerde yararlanılmaktadır. Bunlarla birlikte elde edilen verilerin değerlendirme süreci de kendi içerisinde çok farklı bir konudur.

Durum çalışmasında elde edilen verilerin analizi de çok büyük bir öneme sahiptir. Bu konu için dört tane temel analiz yöntemi vardır (Creswell, 2013, s. 199):

> 1) Kategorik toplulaştırma; elde edilen verilerin konuyla ilişkili bir biçimde bir araya getirilmesi neticesinde örnek bir yapının oluşturulmasıdır.
>
> 2) Doğrudan yorumlama ise; ele alınan tek bir örnekten hareketle anlam çıkartmaktır.
>
> 3) Model kurma yönteminde; iki ya da daha fazla sayıdaki olay arasında belirli benzerlikler ve ilişkiler kurmak öne çıkmaktadır.
>
> 4) Durumlardan hareketle doğal genelleştirmeler oluşturmada ise; belirli durumların örnek alınarak onun genele teşmil edilebilecek bir yapı olmasını sağlamaktır.

Durum çalışmalarında hem geçerliliği, hem de güvenilirliği sağlamak adına bazı önlemler de alınmaktadır. Alınan önlemlerden birincisi; araştırmacının konu ile olan irtibatını yani etkileşim süresini uzatmasıdır. Böylece araştırmacı gözlemini derinleştirebilir ve çeşitlendirebilir. İkinci önlem yöntemi ise; araştırmacının farklı veri çeşitleme yöntemlerini kullanmasıdır. Veri çeşitlemesi ile verinin farklı yöntemlerle elde edilmesi kastedilmektedir. Kaynak bir tane olsa da o kaynaktan farklı çeşitlerde verileri almak, verilerin test edilmesini ve desteklenmesini kolaylaştırmaktadır. Üçüncü olarak; araştırmada elde edilen sonuçların araştırmaya dâhil olanlar ile sonradan paylaşılması ve onların da fikirlerinin alınmasıdır. Buradaki amaç ele alınan olayın doğru, yansız ve olabildiğince farklı insanların da görüşleri alınarak gerçekçi bir biçimde yansıtılmasıdır.

Son önlem ise; araştırmacının elde ettiklerini yani bulgularını diğer araştırmacılar ile paylaşması ve onların da fikirlerini almasıdır. Böylece o araştırmacının fark etmediği hatalar giderilmiş olur, hem de alternatif yaklaşımlar ve cevaplar geliştirilebilir (Merriam, 1990).

Durum çalışmasında insan, kurum, grup ya da ortam incelenebilmektedir. Durum çalışmalarını nicel ve nitel bir biçimde gerçekleştirmek mümkündür. Durum çalışmasında ana amaç; belirli bir olguyla ilişkili olarak sonuçları açıkça ortaya koymaktır. Sonuç sürecinde o olguyla ilişkili olarak birçok nedeni ilişkilendirmek de mümkündür. Durum çalışmasında veri toplamak için birçok yöntem söz konusudur ve bu yöntemler sayesinde birbirini farklı açılardan teyit eden veri çeşitliliği sağlanmış olmaktadır. Bu tanımlardan, yöntemlerden ve açıklamalardan hareketle gelecek bölümde veri sızıntıları hem küresel hem de Türkiye ölçeğinde birlikte ele alınacaktır.

Uluslararası Raporlar Doğrultusunda Siber Saldırı

Bu bölümde veri ihlalleri ve siber saldırıların küresel ölçekteki bilgilerinden hareketle, kurumsal iletişim bazlı yaklaşım için önerilen tablo üzerinden kurumların veri ihlal durumlarında ve öncesinde yapması gerekenler açıklanacaktır. Verilen raporlarda küresel açıdan maddi değerler ele alındığı ve ortak para birimi Amerikan doları cinsinden işlem hacmine sahip olduğu için tablolarda para birimi dolar olarak verilmektedir. Küresel açıdan veri ihlallerinin oynadığı role değinilerek Türkiye'de bu bağlamda neler yaşandığı nicel veriler üzerinden analiz edilecektir. Bölüm boyunca IBM Security'nin "Cost of a Data Breach Report 2020" raporunun verileri üzerinden analizler gerçekleştirilecektir.

Tablo 1: *Global Çalışma Raporu*

Ülke/Bölge	2020/Örneklem	Örnek Yüzdesi	Para Birimi	Çalışma Yılı
Amerika	63	%12	Dolar	15
Hindistan	47	%9	Hindistan rupisi	9
İngiltere	44	%8	Pound	13
Almanya	37	%7	Euro	12
Fransa	36	%7	Euro	7
Brezilya	35	%7	Brezilya reali	9
Japonya	33	%6	Yen	11
Orta Doğu[1]	29	%6	Riyal	7

1 Ortadoğu bölümü Suudi Arabistan ve Birleşik Arap Emirliklerinden oluşmaktadır.

Kanada	26	%5	Kanada doları	6
Güney Kore	24	%5	Güney Kore wonu	3
Güneydoğu Asya Milletleri Birliği[2]	23	%4	Singapur doları	2
Avustralya	23	%4	Avustralya doları	11
İskandinavya[3]	23	%4	İsveç kronu	2
İtalya	21	%4	Euro	9
Latin Amerika[4]	21	%4	Arjantin pesosu	1
Türkiye	20	%4	Türk lirası	3
Güney Afrika	19	%4	Güney Afrika randı	5
Total	524			

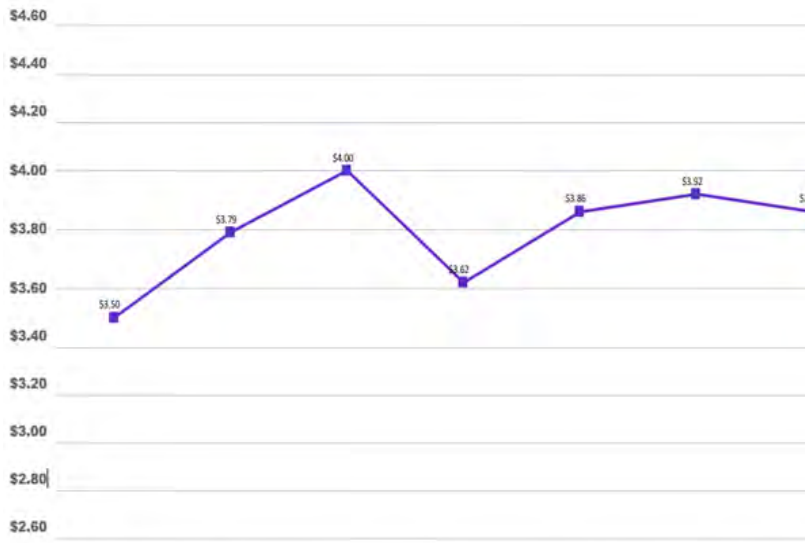
Kaynak: (IBM Security, 2020, s. 15)

Tablo 1'de 2020 senesi içerisinde yaşanmış veri ihlallerinin maliyet raporu gösterilmektedir. Bu rapor küresel açıdan 17 ülke/bölge içerisinde yer alan 17 sektörden, 524 kuruluşun incelenmesiyle elde edilen sonuçların birleştirildiği küresel bir sonuçtur. Ülkeler/bölgeler çalışma yıllarına göre değişiklik arz etse de, en çok vakanın Amerika'da yaşandığı ve %12 ile ilk sırada yer aldığı görülmektedir. Veri hırsızlığı konusunda da 15 yıldır üzerinde çalışılan tek ülke; Amerika'dır. Türkiye ise veri hırsızlığı çalışmalarına 3 yıldır dâhil olmuştur ve 20 tane ulusal ölçekli vaka yaşanmıştır. Raporda bazı durumlarda verilerin karşılaştırılması amacıyla sonuçları ülke/bölge veya sektöre göre ayrılmaktadır. Çünkü bazı ülkelerde/bölgelerde ve sektörlerde örneklem boyutları oldukça küçük olsa da, kuruluşlar çalışmada temsili olması amacıyla seçilmiş ve kullanılmıştır (IBM Security, 2020, s. 14).

2 Güneydoğu Asya bölümü Singapur, Endonezya, Filipinler, Malezya, Tayland ve Vietnam'dan oluşmaktadır.

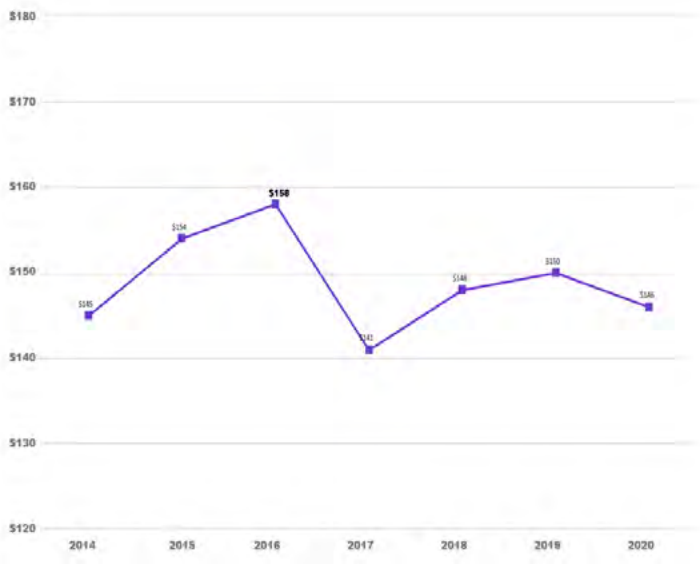
3 İskandinavya bölümü Danimarka, İsveç, Norveç ve Finlandiya'dan oluşmaktadır.

4 Latin Amerika bölümü Meksika, Arjantin, Şili ve Kolombiya'dan oluşmaktadır.



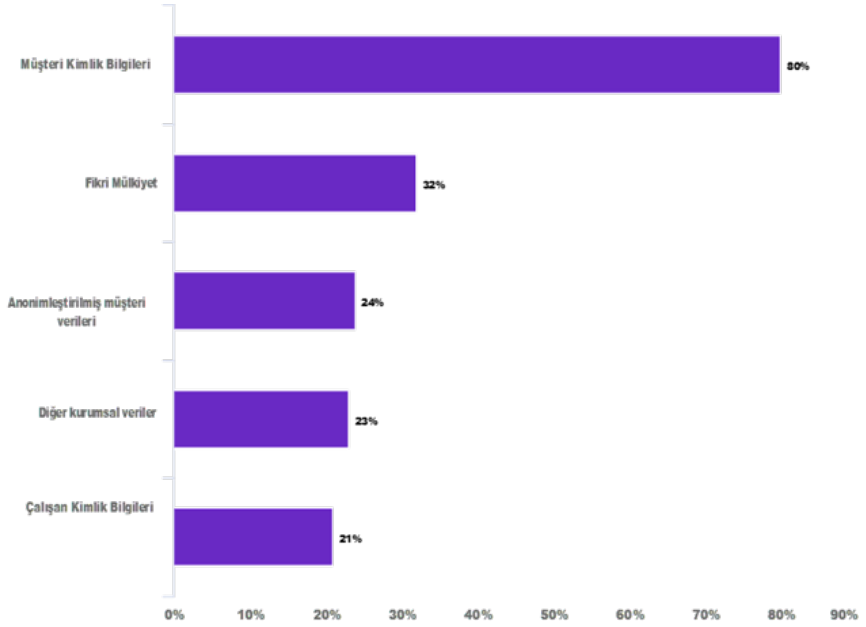
Şekil 1: Bir Veri İhlalinin Ortalama Toplam Maliyeti (Amerikan doları (milyon) cinsinden hesaplanmıştır) Kaynak: (IBM Security, 2020, s. 16).

Veri ihlalinin ortalama toplam maliyeti 2014 yılında bu yana %10 artmıştır. Şekil 1'de yedi yıl boyunca veri ihlalinin küresel ortalama toplam maliyeti gösterilmektedir. Yedi yılın ağırlıklı ortalama maliyeti ise; 3,79 milyon dolardır. Dolayısıyla veri ihlali, bu rakamların da gösterdiği gibi küçümsenecek bir halde değildir. Bu maliyetlere bakıldığında milyon dolarlara ulaşan kurumsal zararlar çok açık bir biçimde görülmektedir. 2020 senesinde veri ihlalinin maliyeti küresel ölçekte; 3,86 milyon dolardır. Veri ihlali maliyetlerinin hesaplanmaya başladığı 2014 senesinden bu yana ulaşılan en yüksek maliyet, 2016 senesindeki 4 milyon dolardır. Her ne kadar sonrasında doğrusal bir artış gözlenmese de, ilerleyen yıllarda veri ihlali maliyetlerinin artacağını tahmin etmek zor değildir.



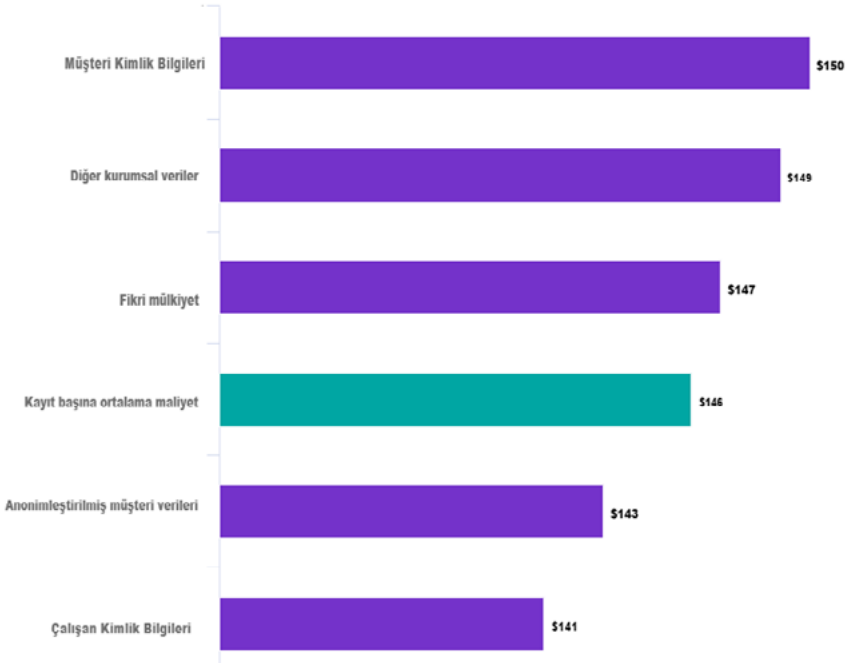
Şekil 2: Bir Veri İhlalinin Kayıt Başına Ortalama Maliyeti Kaynak: (IBM Security, 2020, s. 17).

Şekil 2'de son yedi yılda bir veri güvenliği ihlali başına ortalama maliyet gösterilmektedir. Bir veri ihlali başına maliyet 2019'dan 2020'ye geçildiğinde bir miktar azalarak, 146 dolara gerilemiştir. Yedi yıl boyunca bir veri ihlalinin ağırlıklı ortalaması; 149 dolardır. Dolayısıyla büyük ya da küçük fark etmeksizin tek bir verinin değeri; 140 ile 160 dolar arasında dalgalanmaktadır. Gelecekte de verinin değerinin artacağı ve bu maliyet kalemlerinin çok daha önemli hale geleceği açıktır.



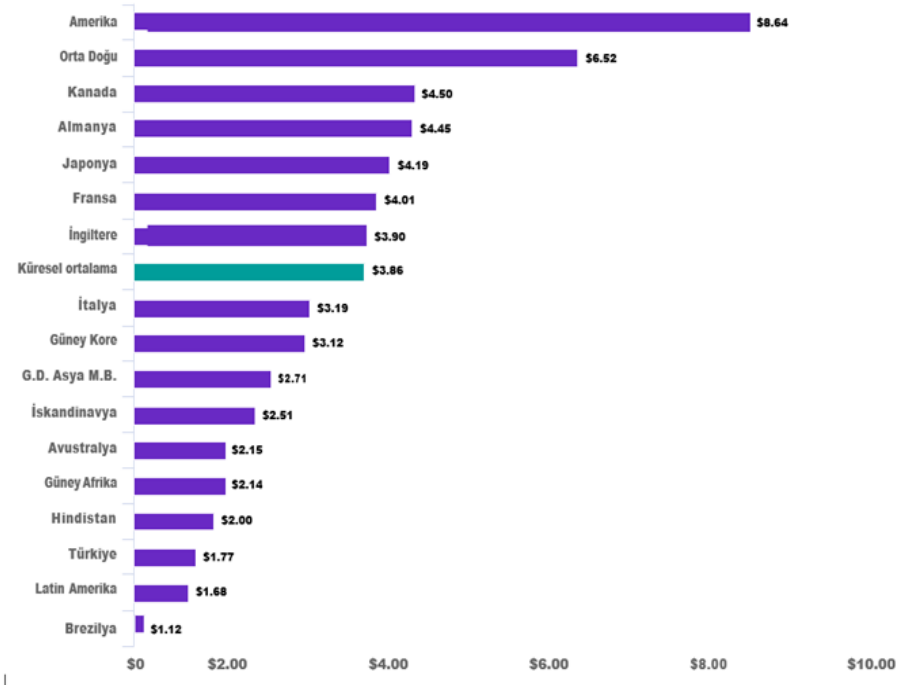
Şekil 3: Güvenliği İhlal Edilen Kayıt Türleri (Her Kategorideki Verileri İçeren İhlallerin Yüzdesi) Kaynak: (IBM Security, 2020, s. 18).

Şekil 3'te gösterildiği üzere müşteri kimlik bilgileri, genellikle ihlallerde en çok kaybedilen veya çalınan veri türüdür. Veri ihlallerinin %80'i müşteri kimlik bilgilerini içermektedir. İhlallerin %32'si fikri mülkiyetin güvenliğinde, %24'ü ise anonimleştirilmiş müşteri verilerinin güvenliğinde yaşanmaktadır. Bu tabloda müşteri kimlik bilgilerinin açık ara önde olması, çok büyük bir önem arz etmektedir. Çünkü diğer veriler çok spesifiktir ve belirlenmiş alanlarla kısıtlıdır. Hâlbuki müşteri kimlik bilgileri her alanda işe yarayabilecek birçok farklı bilgiyi içermektedir. Bunun içerisinde müşteriyi dolandırmaktan, müşteriye ait hesapların ele geçirilmesine kadar birçok unsur yer almaktadır. Çalışanların kimlik bilgileri %21 ile en az öneme sahiptir. Çünkü bir kurumun sahip olduğu çalışan sayısı daima kullanıcı sayısından az olduğu için, veri ihlallerinde ana grup çalışanlar hiçbir zaman olmamaktadır. Sayıca çok olan müşterilere yönelmek ve onların da sadece o kuruma ait bilgilerini çalmak yerine, o müşteriye tüm verinin çalınması çok daha önemlidir.



Şekil 4: Güvenliği İhlal Edilen Veri Türüne Göre Kayıt Başına Ortalama Maliyet Kaynak: (IBM Security, 2020, s. 19).

Şekil 4'te belirtildiği üzere müşteri kimlik bilgileri, güvenliği ihlal edilen en maliyetli veri türünü oluşturmaktadır. Müşteri kimlik bilgilerinde kaybolan veya çalınan kayıt başına ortalama maliyet; 150 dolardır. Fikri mülkiyetin maliyeti kayıt başına 147 dolarken, anonimleştirilmiş müşteri verileri kayıt başına 143 dolar ve çalışan kimlik bilgileriyse kayıt başına 141 dolar maliyet oluşturmaktadır. Bir önceki tabloda da ifade edildiği üzere, oransal olarak öneme sahip olan müşteri kimlik bilgileri, maliyet açısından da aynı değere sahiptir. Müşteri kimlikleri bilgileri büyük bir farkla olmasa da, diğer kurumsal verilerin önüne geçerek maliyet yükünü en çok oluşturan kalemdir. İhlal edilen her bir verinin değeri 141 dolar ile 150 dolar arasında değişmektedir. Önceki tablolarda da değinildiği üzere, dijitalleşmenin ve gözetleme pratiklerinin artışı ile ihlal edilen veri maliyetlerinin de artacağını öngörmek çok doğaldır.



Şekil 5: Ülkeye veya Bölgeye Göre Bir Veri İhlalinin Ortalama Toplam Maliyeti Kaynak: (IBM Security, 2020, s. 23).

Şekil 5'e göre bir veri ihlalinin ortalama toplam maliyeti, ülkeden ülkeye değişiklik göstermektedir ve ilgili tabloda Amerika'daki kurumların en yüksek ortalama toplam maliyete sahip olduğu görülmektedir. İlk sırada; 8,64 milyon dolarla Amerika yer alırken onu, 6,52 milyonla Ortadoğu izlemekte, Türkiye 1,77 milyon dolarla, Latin Amerika 1,68 milyon ve Brezilya ise 1,12 milyon dolar ile en düşük ortalama toplam maliyetlere sahip olan ülkeleri teşkil etmektedirler. Türkiye gibi bazı ülkelerde bu çalışmalar yeni yapılmaya başlandığı için, düşük ortalamaya sahip olunması tek başına bir değer ifade etmemektedir. Türkiye için üç senedir, Latin Amerika içinse bir senedir yapılıyor olmasının olası sonuçlarıdır bunlar. Dolayısıyla veri ihlaline önem veren ve dijitalleşmenin önde olduğu ülkelerde ya da bölgelerde, maliyetlerin yüksek çıkması olağan bir sonuçtur. Dijital unsurların artışı ile veri ihlallerinin artışı doğru orantılıdır. Türkiye ve Latin Amerika ülkelerinde bu maliyet kaleminin önümüzdeki yıllarda artış göstereceği açıktır.

Görüldüğü üzere IBM Security'nin hazırlamış olduğu "Cost of a Data Breach Report 2020" en küçük bir veri ihlalinin ne gibi maddi sonuçlar doğurduğunu ortaya koymaktadır. Maliyetler hem ülkeler, hem de kurumlar için oldukça yüksektir. IBM'in (2021) hazırladığı son yarıyıl raporu ise önceki 7 senenin ortalama veri ihlali maliyetleri açısından en yüksek değerlere sahiptir ve 2021 senesi diğer senelere veri ihlalleri açısından fark atmaktadır. Bu süreçte en büyük etkiyi pandemi yaratmıştır. IBM firmasının 2020 analizine bakıldığında yapılan veri ihlali maliyetlerinin 3,86 milyon dolar olan ortalaması 2021 senesi tamamlanmadığı halde 4,24 milyon dolara yükselmiştir. Dolayısıyla içinde bulunulan 2021 yılı, kendisinden önceki 7 senelik süreci ve her türlü veriyi aşarak ortalama en yüksek toplam maliyete sahip olmuştur. Covid-19 dönemi koşullarında uzaktan çalışma zorunluluğu gibi nedenler de bu maliyetleri arttırmıştır. Yine yapılan araştırmada uzaktan çalışma koşullarının faktör olarak alındığı veri ihlal durumlarındaki ortalama maliyet,

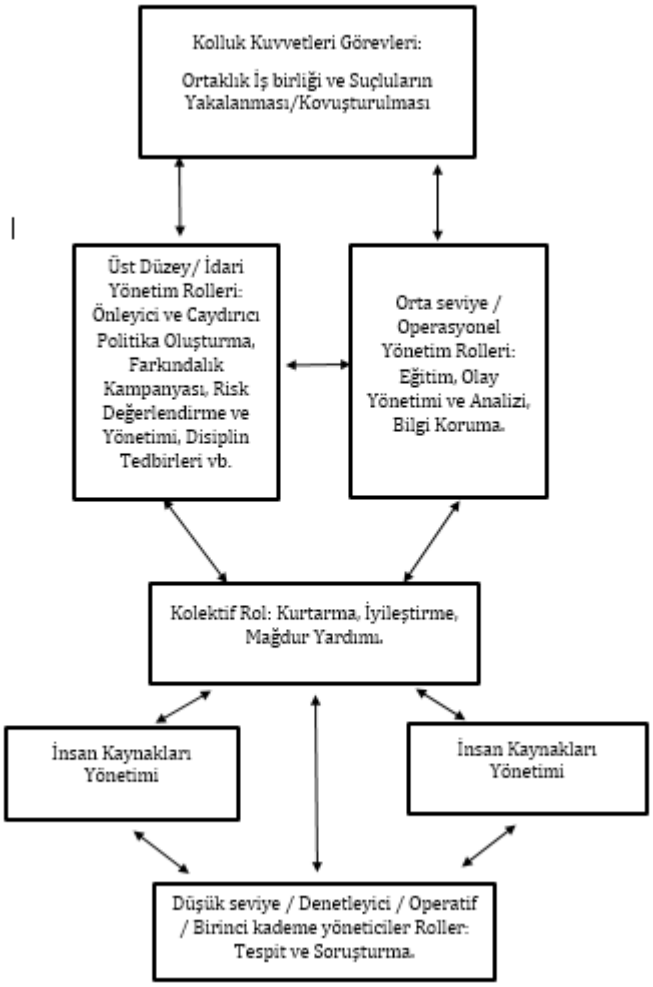
normal zamanlara göre 1,07 milyon dolar daha yüksek çıkmaktadır (IBM Security, 2021). Buradan da anlaşıldığı üzere Covid-19 koşullarıyla çevrimiçi hareketin fazlalaşması, beraberinde veri ihlallerinin de artmasına sebep olmaktadır. Diğer senelerde olduğu gibi veri ihlallerinde en öne çıkan konu; kimlik bilgilerinin ele geçirilmesidir ve bu veriler genelin %20'sini oluşturmaktadır. Tüm bunlarla birlikte siber saldırıya ve veri ihlaline uğrayan bir kurum, ayrıca hedef kitlesini oluşturan müşterilerini kaybetme riskini de beraberinde taşımaktadır. Çünkü müşterinin kurumla paylaştığı kimlik bilgileri ve kredi kartı bilgileri de bu veri ihlalin bir parçası olmaktadır. Kurumsal iletişim konusunda kurumların çok dikkatli, proaktif ve karşılıklı iletişim tabanlı bir süreci yönetmeleri gerekmektedir.

Buradan hareketle veri ihlallerinde en üst sırayı alan kimlik hırsızlıklarının hep dışarıdan saldırılarla gerçekleştiği düşünülürken, yapılan araştırmalarda tam tersine %70 kadarının ilgili kurumun içyapısını oluşturan çalışan veya çalışanların işbirlikçileri tarafından gerçekleştirildiği bilinmektedir (Collins, 2005). Son yıllarda kurum içinden meydana gelen müşteri kimliklerine dayalı veri ihlallerine ait suç vakaları artış göstermektedir.

Bu bağlamda veri güvenliğinin sağlanmasının iki aşamalı bir yapısı bulunmaktadır. Bunlardan ilki; sistem kullanıcısının kendini uygulamadaki diğer kullanıcıların karşısında güvende hissetmesidir. İkincisiyse; bu sefer sistemin kendisinin onu kullananlara ne şekilde güvenmesi gerektiğini oluşturan aşamalarıdır (Singer & Friedman, 2015). Bundan ötürü birçok kurum, gerçekleştirdikleri ticari organizasyonlarda kurumsal itibar açısından zararlarını korumayı düşünerek, var olan sorunun boyutlarını kabul etmelidir. Bu suçların kontrolü ve önlenmesi için kapsamlı bir çerçeve zorunludur. Özellikle de kurum içi süreçlere detaylıca bakmak hem bu çalışmanın zeminini teşkil etmektedir, hem de yapılması gerekenleri ortaya koymaktadır. Veri ihlali süreçlerinde kurum içi davranışlara bakmak önem arz etmektedir.

Bulgular ve Tartışma: Yemeksepeti Örneği

Kurum içi veri ihlallerinin yaşanmasını engellemek amacıyla, proaktif bir yaklaşım oluşturmak, kurum prosedür ve kurallarının sınırlarının oluşturulması için Shah ve Okeke tarafından (2011, s. 369) geliştirilen rol tabanlı çerçeve modeline göre hareket edilmesi kurumsal iletişim ve itibar için oldukça uygun olacaktır. Çünkü kurum içi çalışan sebebiyle yaşanacak bir veri ihlali, kurumun değerine oldukça zarar verecektir. Bu nedenden ötürü öncelikli olarak Shah ve Okeke'nin birlikte hazırlamış olduğu "Rol Tabanlı Çerçeve" Türkçeleştirilecektir. Bu çerçevenin ne gibi faydalar sağladığı, neyi amaçladığı, artı ve eksi yanları tartışmaya açılacaktır.



Şekil 6'da görüldüğü üzere kurum içi bir veri ihlali olayında, kurumun proaktif yaklaşımı sırasında bu şekilde hareket etmesi, kurumsal iletişim ve itibar yönetiminde daha faydalı olacaktır. Öncelikle daha önce de belirtildiği üzere kurum; çalışanlarını bir tehdit olarak dikkate almadığı için bunun yüksek maliyetli sonuçlarına katlanmak zorunda kaldığı verilerle birlikte görülmektedir. Hareket tarzı içerisinde rol tabanlı çerçevede en temel nokta; ülkenin yasaları ve yasaları uygulayan kolluk kuvvetleridir. Var olan yasa ve yaptırımlar öncelikle bu tarz ihlalleri engelleyici nitelik ve özelliklerde olmalıdır. Kolluk kuvvetlerinin, olayları raporlamasının ve analiz etmesinin ötesine geçmek için gerekli güç ve becerileri bulunmaktadır. Kurumun veri ihlalleriyle ilgilenmek için dışarıdan uzman ekiplerden de hizmet alması tavsiye edilmektedir. Bu doğrudan bir destek olabileceği gibi eğitim amaçlı da olabilmektedir. Zaten kurumların önleme tedbirleri konusunda eğitime tabi tutulmaları burada çok önemli bir rol oynamaktadır.

Sonraki aşamada yani kurum içi temel aşamada ise; üst düzey yöneticiler bulunmaktadır. Çalışan kaynaklı, müşteri kimlik veri ihlallerinde, olası durumların

öncesinde önlenmesinde üst düzey yönetimin rolü son derece önem arz etmektedir. Kurum içinde önleyici ve caydırıcı politikalar oluşturmalı, risk değerlendirmeleri yaparak olası durumlarda hareket tarzı, yönetim şekli ve disiplin kuralları hazırlanmalıdır. Bu model, herhangi bir kurumda etkili bir kimlik veri ihlali politikası oluşturulması anlamına gelmekte ve kimlik hırsızlığını önlemeye yönelik bütünleşmiş bir çerçevenin geliştirilmesine yönelik gerekli olan ilk adımı oluşturmaktadır. Olası prosedürler hazırlanırken, kurumdaki iç veri ihlali kaynaklı durumların ortaya çıkma olasılığını azaltabilecek kesin sınırlara sahip, tüm diğer bileşenleri de içeren bir kurallar dizisi oluşturulmalıdır. Bu aşamada kurumun üst düzey yöneticilerinin temkinli davranmaları beklenmekte ve hatta aralarından en az bir yöneticinin bireye ve kuruma ait bilgilerin korunması, olası sahtekârlıkların tespiti, soruşturmalar ve olay yönetiminin sağlanmasında da etkin rol oynaması beklenmektedir. Böylece önleme politikaları bir kurumun tüm seviyeleri tarafından kabul görmekte ve yöneticilerin bu süreçlerde yer alarak edindikleri deneyimleri daha etkili politikalar geliştirmelerine de ayrıca yardımcı olmaktadır (Shah & Okeke, 2011).

Kurumlardaki orta düzey yönetimden kasıt, bölüm başkanları, bölüm yöneticileri ve bölge müdürlükleri gibi pozisyonlardan oluşmaktadır. Bu pozisyondakiler, çalışanların eğitimlerinden, olayların yönetiminden, analizlerin gerçekleştirilmesinden ve sahip olunan kurumsal bilgilerin korunma süreçlerinden ve bunların düzgün bir biçimde işleyişinden, üst düzey yönetime karşı sorumludurlar. Orta düzey yöneticiler, ayrıca üst yönetimin oluşturduğu prosedürleri ve kurumsal amaç planlarını da uygulamaktan sorumludurlar. Orta düzeyli yöneticiler, üst-alt kademe arasında köprü görevi görerek, kimlik veri ihlaline karşı önleyici ve caydırıcı politikaları uygulatabilmelidirler. Kısaca bu orta düzey yönetimin sorumlulukları; çalışanların eğitimini, olayların analiz ve yönetimini, süreçlerin ve iletişimin koordinasyonunu sağlamaktır. Öncelikle kurum çalışanlarının kuruma ve müşterilere ait bilgileri koruma ve sahip olunan verilerin güvenliği konularında eğitimi öncelikli olmalıdır. Kurum çalışanlarının eğitim dâhilinde ilgilerini yasalar, prosedürler ve kurum politikaları oluşturmalıdır. Aynı zamanda sonuçları ve yaptırımları konusunda net bilgi sahibi olmalıdırlar. Bazı durumlarda olayların etkin yönetimi için çalışanların eğitimlerini desteklemek amacıyla seminerler oluşturabilirler. Üst ve orta düzey yöneticilerin karşılıklı iletişim içerisinde çalışması bir gerekliliktir.

İlk kademe yönetimi ise; genellikle mağaza müdürleri, bölüm amirleri, süpervizörler, vardiya amirleri, ustabaşılar ve ekip liderlerinden oluşmaktadır. Kurum içinde en temel görevleri; günlük iş süreçlerinin denetimi ile ilgilidir. Bu kademedeki ara yöneticiler, çalışanlarla günlük olarak etkileşim içerisinde olduklarından dolayı, üzerlerinde çok güçlü etkileri ve kontrol mekanizmaları bulunmaktadır. Veri ihlali durumlarının tespitinde ve soruşturulmasında çok önemli bir yerleri bulunmaktadır. Çalışanları gözlemleme ve analiz etme fırsatı da bulunmaktadır.

Diğer bir basamağı oluşturan ve iç kimlik veri ihlalleriyle ilgili olası suçların tehdidini azaltmanın en etkili yollarından biri insan kaynakları yöneticileridir. Bu yöneticiler tarafından, tüm çalışanlar arasında farkındalık düzeylerinin yükseltilmesi en önemli etkenlerden birini oluşturmaktadır. İç kimlik veri hırsızlığıyla ilgili herhangi bir suça karışmanın veya gizlice parçası olmanın sonuçları çalışanlara iyice bildirmelidir. Kurumlar, insan kaynakları aracılığıyla, personellerinin, kurum içinde oluşabilecek

şüpheli olayları, faaliyetleri ve durumları kime ve hangi birime bildirmeleri gerektiğini öğrenmelerini sağlamalıdır. Ayrıca, iletilen durumun gizlilik ve profesyonelce ele alınacağından emin olmalıdırlar. Kurumların insan kaynakları basamağı, henüz işe alım süreçlerinde iki basamaklı bir inceleme yaparak bu durumu azaltabilirler. Öncelikle başvuru yapanın sabıka kaydına bakarak ve ilgili kişi ile ilgili güvenlik araştırması yapması da, ayrıca bu tarz yaşanabilecek suçlara ve sahtekârlıklara karşı etkili önleyici tedbir olacaktır (Shah & Okeke, 2011).

Kurumların işe alımlarla ilgili olası durumlarının çoğu, belirli bir yönü kapsayan ve resmi olarak belirlenmiş politikalarla alakalıdır. Bu politikaların içerisinde mutlaka, veri ihlali yönetimi politikası, çalışan veri ihlali önleme politikası, davranış kuralları veya iş etiği belirlenmelidir. Aynı zamanda bu tür suçlar için açık disiplin prosedürleri, uygunsuz faaliyet-sahtekârlık raporlaması ve ihbar ödülleri politikasıyla, personel yardım politikasının da belirlenmiş olması gerekmektedir. Rol tabanlı çerçeve modeli, yeni geliştirilmiş ve kapsamlı olarak kurum içi hareket stratejisinin her kademesini kapsamaktadır. Ancak buna rağmen hangi aşamanın ya da hangi düzey yönetimin en etkili olduğunu veya farklı süreçlerin, kurum iç dinamiklerinin birbirleriyle nasıl daha iyi etkileşime girebileceğini bulmak için daha fazla kurum içi çalışmaya gereksinim duyulmaktadır. Her kurum kendi kültürünü ve yönetimsel dinamiklerini inşa etmelidir ve bir yandan da etmektedir. Her kurumun kendine özgü bir politikası ve iç kuralları mevcuttur. Kısaca Şekil 6, kurum içi çalışanlar sebebiyle müşteri veri ihlalleri yaşanmadan önce alınması gereken önlemlerden, işe alım süreçlerinden, prosedürlerden ve eğitimlerden bahsetmektedir.

Alınan önlemlere ve uygulanan kurallara rağmen, bir veri ihlali söz konusu olursa, olay sonrasında en önemli olan; kurumun bu sürece nasıl sahip çıkacağı ve nasıl yöneteceğidir. Tam bu noktada devreye, kurumsal iletişim girmektedir. Çünkü bir yönetim stratejisi olan kurumsal iletişim, kimlik veri ihlallerinin yaşandığı durumlarda zamanında, açıklayıcı, bilgi verici, doğru ve ilgili kişi tarafından gerekli açıklamaların ve bilgilendirilmelerin yapılmasını sağlamaktadır. Proaktif bir yaklaşım içererek, alınan önlemler ve sürecin olası sonuçları ve sonuçların yönetimi hakkında kamuoyuna ivedilikle haber verilmelidir. Tüm bu konuları daha iyi tartışıp analiz edebilmek için Yemeksepeti'nin yaşadığı siber saldırı ekseninde yapılan kurumsal açıklama incelenecektir.

Yemeksepeti 27 Mart 2021 tarihinde saat 14:01'de Twitter hesapları üzerinden birbirini takip eden iki tweet ve 5 sayfa açıklama metni ile kamuoyuna, sistemlerine yapılan siber saldırıyla ilgili açıklama yapmıştır. Bu açıklamada 25 Mart 2021 tarihinde, Yemeksepeti'ndeki kullanıcı veri tabanına, kimliği tespit edilemeyen korsan ya da korsanlar tarafından siber bir saldırının gerçekleştirildiği bilgisi paylaşılmıştır. Bu bilgide bir kısım veri ihlali yapıldığı ve kullanıcıların hesap bilgilerinin bir bölümünün çalındığı ifade edilmiştir. Bunun üzerine çalınan bilgilerin detayları paylaşılmıştır. Uygulamaya kayıtlı kullanıcılar için en önemli detaylardan biri olan; kredi kart bilgileri ya da finansal bilgilerinin ele geçirilemediği söylenmesine rağmen, insanların akıllarında belirli soru işaretleri ister istemez oluşmuştur.

Açıklamanın en başında veri ihlalleri karşısında birçok devletin, kurumun ve firmaların tehdit altında olduğundan bahsedilmekle birlikte, siber saldırılardan tamamen korunmanın bir yöntemi olmadığına değinilmiştir. Siber saldırıya rağmen, Yemeksepeti'nin kurum olarak elinden gelen tüm önlemleri aldığı açıklanmıştır. Ardından olayın detaylarına girilerek kredi kartı bilgilerinden, finansal bilgilere ve şifrelere, aynı zamanda Facebook ve Apple hesaplarına da bir saldırı gerçekleştirilemediği belirtilmiştir. İlk elden kullanıcıların açıklamalar vasıtasıyla en önemli verilerine bir şey olmadığı, hatta güvende oldukları açıklanmıştır. Zaten bu tarz önemli verilerin Yemeksepeti'nin sisteminde saklanmadığı ifade edilmiştir. Kullanıcı kredi kartı ve finansal bilgilerin, kurum veri tabanında değil, kurumun kullandığı Mastercard aracı kurumu veri tabanında saklandığı söylenmektedir ve bunun akabinde Mastercard firmasında veri ihlaline dair herhangi bir güvenlik sorunun oluşmadığı da görülmektedir. Dolayısıyla kullanıcılar açısından en azından ilk bilgiler böylece elde edilmiştir.

Ardından ise veri hırsızlığına tabi olan konular ve nesneler büyük bir şeffaflık örneği gösterilerek tek tek açıklanmıştır. Bunlar sırası ile şöyledir: Ad-Soyad, Doğum Tarihi, Telefon Numarası, E-posta Adresi, Adres Bilgisi ve son olarak Giriş Şifreleri.

Yemeksepeti'nin en azından veri hırsızlığı yoluyla ele geçirilen bilgileri açıklamış olması önem arz etmektedir. Çünkü kullanıcıların bu bilgiler vasıtasıyla başına gelenlerden haberdar olarak, kendi güvenliklerini tesis etmeleri sağlanmaktadır. Kullanıcı çalınan bilgileri değiştirme ve kişisel sistemine müdahale etme imkânına sahip olabilmiştir. Ancak buradaki tek ve belki de en büyük sorun veri hırsızlığının yaşandığı tarih ile açıklamanın yapıldığı tarih arasında iki günlük yani 48 saatlik bir farkın olmasıdır. Bu bağlamda kullanıcıların iki gün boyunca sistemlerinde maddi ve manevi sorunlar yaşanmış olabilir. O yüzden bu tarz siber saldırı durumlarında anında iletişim kurabilmek ve oluşabilecek her türlü zarardan kullanıcıları koruyabilmek adına kurumsal iletişim stratejilerinin önceden belirlenmiş olması ve bu durumlarda devreye sokulması gerekmektedir. Veri ihlalinin 25 Mart'ta yaşanmasına karşın, açıklamanın 27 martta yapılması akıllara bu veri ihlalinin kurum içi kaynaklı olabileceği fikrini de getirmektedir. Bunun gerekçesi olarak da kurumunun veri ihlalinin ilk yapıldığı saatlerde açıklama yapmaması ve olayın üzerinden iki gün geçtikten sonra kurumsal bir açıklamanın yapılmış olması gözükmektedir.

Süreç boyunca Yemeksepeti'nin belki de en büyük hatası; açıklamada durmadan kurumun her türlü hatadan azade olduğu ve yapılması gerekenleri titizlikle yaptığı yönünde oluşturmaya çalıştığı algıdır. Açıklamanın üçüncü sayfasında yapılmış olanlar açıklanmış ve tüm kamu kurum ve kuruluşlarıyla paylaşılması gerekenler paylaşılmıştır. Kurumsal düzeyde üzüntü duyulduğu ve bilgilendirmelerin zamanında yapıldığı ifade edilmiştir. Tüm bunlarla birlikte veri güvenliğinin en hassas konu olduğu ve Yemeksepeti kullanıcılarının verilerini korumak adına çalışmaların gerçekleştirildiği görülmektedir.

Genel olarak açıklamalar bittikten sonra son açıklama sayfasında iki tane soru eşliğinde cevaplar iletilmiştir. Bu iki sorudan bir tanesi; kredi kartlarının güvenliği ile alakalıdır. Bir diğer soru ise; Yemeksepeti hesaplarına başka kişiler tarafından erişim sağlanıp sağlanamayacağıdır. İlk soruya açıklamanın en başında da yer verilmiştir. Ancak

şimdi daha detaylı bir açıklama yapılmıştır. Bu durum ise kredi kartı bilgilerinin belki de en hassas konu olduğunu göstermektedir. Çünkü açıklama metninde iki defa aynı konu işlenmiştir. Kredi kartı bilgilerinin MasterCard altyapısı tarafından korunduğu ve korunma sürecinde her türlü altyapı hizmetinin MasterCard tarafından sağlandığı, bilgilerin de Yemeksepeti veri tabanlarında tutulmadığı görülmektedir. Dolayısıyla Yemeksepeti'ne dönük bir siber saldırının kartlara müdahale edemediği anlaşılmakta ve bu durum da kullanıcıların çok önemli bir konuda rahatlamalarını sağlamaktadır. Bir diğer konu ise; 3.kişilerin Yemeksepeti hesaplarına erişim sağlayıp sağlamayacağı hususudur. Bu konu da net bir açıklama ile bertaraf edilir. Kullanıcıların şifrelerinin kripto algoritmalar ile korunduğu ve maskelendiği ifade edilmiştir. Dolayısıyla herhangi bir korsanın şifreleri görmesi mümkün olmadığı gibi kurumun bile bu şifrelere erişmesinin imkânsız olduğu açıklanmıştır.

Kurumsal iletişim stratejisi açısından birçok doğru nokta olmakla birlikte ana hata zamanlama konusunda olmuştur. Dijital iletişim pratiklerinin ve veri hırsızlığının saniyeleri içerisinde gerçekleştiği bir dönemde iki günlük gecikmeyle açıklama yapmak kullanıcılar açısından hem güven hem de güvenlik sorunları teşkil etmektedir. Aynı zamanda kurum içi "Rol Tabanlı Çerçeve"nin de iyi oturtulamadığı görülmektedir. Kurum içi ve dışı stratejilerin önceden belirlenmediği ve duruma en azından kurumsal iletişim açısından çok sağlıklı yaklaşılamadığı belli olmaktadır. Dolayısıyla çerçevelerin önceden iyice çizilmesi ve rollerin tanımlanması ile çok daha iyi bir kurumsal iletişim süreci, veri hırsızlığı yaşandığı andan itibaren sürdürülebilir. Zaten bu çalışmanın amacı da rol tabanlı çerçeveyi belirleyerek kurumların en azından kurum içerisinde daha iyi adımlar atmasını sağlamaktır.

Sonuç

Türkiye'de günümüzde 55 milyonun üzerinde dijital medya kullanıcısı bulunmaktadır. Öte yandan nüfusun yüzde 75'i de aktif olarak internet kullanmaktadır. Bu durum Türkiye'nin, mahremiyet kavramının dijitalleşmesi açısından ciddi bir araştırma sahasına sahip olduğunu göstermektedir. Bu bağlamda veri ihlallerinin yaşanmaması adına ciddi önlemler alınmalıdır. Keza bilişim hususunda yeteri kadar eğitim ve bilinçlendirmenin yapılamadığı Türkiye'de, dijitalleşen mahremiyetin, kullanıcının izni olmadan gerçekleştirilmesi her geçen gün artmaktadır. Bunun yanı sıra hükümetler tarafından kişisel verilerin korunması hususunda ne kadar çaba gösterilse de egemen güç olarak kimi zaman dijital gözetimin öznesi de yine devlet ve özel kurumlar olabilmektedir. Dolayısıyla bireyin kendisini koruması ve içinde bulunduğu durumu fark etmesi beklenmektedir. Bireyin kendi çabaları veri mahremiyeti açısından çok büyük bir rol oynamaktadır.

Mahremiyet kavramı, birey için en önemli kişilik hakları arasına girmektedir. Bu durum, yasa koyucu tarafından da kanunlarla koruma altına alınmıştır ve her geçen gün daha da geliştirilmektedir. Ancak dijitalleşen çağla birlikte bu durum maalesef fazlasıyla ihlâl edilir bir duruma dönüşmüştür. Bireyler, teknoloji firmalarının ürettikleri yazılımlarla birlikte kendi iradeleri doğrultusunda kişisel verilerinin toplanmasına ve işlenmesine izni

vermekte, bu da doğrudan mahremiyet kavramını zedelemektedir. O yüzden bireyin ne yaptığını bilmesi ve bu hak ihlallerini fark etmesi gerekmektedir. Mahremiyet ihlâlinin, ayrıca siber zorbalık durumu da bulunmaktadır. Siber korsanlar, mahremiyet kavramını zor ve yasa dışı yollardan ihlâl etmektedir. Her iki durumda da bireyin mahremiyet kavramı zedelenmekte ve ortaya büyük veri ihlâlleri çıkmaktadır. Dijital düzlemde yaşanan ihlaller kişilerin birçok bilgisinin çalınmasına neden olduğu gibi tek bir noktayla ya da konuyla sınırlandırılamamakta ve çok daha büyük sorunlara yol açmaktadır.

IBM'in raporlarına göre 2021 senesi henüz tamamlanmamışken, veri ihlalleri açısından son 7 seneyi geçmiş ve birinciliği elde etmiş durumdadır. Burada Covid-19 nedeniyle uzaktan çalışma sürelerinin ve dijital ortamlarda bulunma sürelerinin artması ile veri ihlalleri normal zamanlara göre daha da artmış gözükmektedir. Veri ihlalleri raporlarına bakıldığında; ilk sırayı kimlik bilgilerinin oluşturduğu görülmektedir. Buradan hareketle günümüzde birçok kurum ve birey, mahremiyet ihlâli konusunda oldukça zor durumlarda kalmaktadırlar. Son yıllarda yasa koyucunun artan dirayeti nispeten daha belirgin olsa da, dünyanın geneli itibarıyla hâlâ mahremiyetin suiistimal edildiği de bir gerçektir. Yukarıda izah edilen sebeplerden ötürü kullanıcı, kendi kişisel güvenlik alanını belirlemeli ve bilişim dünyasında bilinçli olarak hareket etmelidir. Kurumlar ise müşterilerinin kişisel verilerini korumasının hem marka güvenirliliği, hem de marka tercihinde ne denli önemli olduğunu bilmeli ve kontrollü dijital gözetim sınırlarında faaliyet göstermelidirler. Böylece kurumsal iletişimin sürdürülebilirliğini sağlamak için sahip olduğu verileri oldukça özenli bir biçimde korumalıdır.

Yemeksepeti siber saldırı sonucunda, çok ciddi bir veri ihlaline maruz kalmıştır. Kurumsal iletişim stratejisi olarak bu süreçte geç açıklama yapan kurum, çalınan verilerin niteliğini ifade etmiştir. İhlal edilen veriler; ad-soyad, doğum tarihi, telefon numarası, e-posta adresi, adres bilgisi ve giriş şifreleridir. Ortada büyük bir sorun olmasına rağmen, kullanıcıları tatmin edecek düzeyde yeterli bir açıklama yapılmamıştır. Veri ihlali 25 Mart tarihinde yaşanmasına rağmen, kurum bir açıklama yapmamış, olayın üstünden iki gün geçtikten sonra 27 Martta Twitter üzerinden açıklama yapmıştır. Bu açıklamada ise; siber saldırıları her kurumun yaşadığına değinilerek, durumu normalleştirme çabası gütmüşlerdir. Buradan hareketle, kurum her türlü hatadan uzak olduğunu ve yapılması gerekenleri yaptığını iddia etmiştir. Bu yapılanların sonucu göstermektedir ki, veri ihlali konularında kurumların önceden pro aktif bir kurumsal iletişim stratejisi geliştirmeleri gerekmektedir. Veri ihlali sürecinin daha iyi yönetilmesi adına rol tabanlı çerçeve dağılımlarının, kurum içinde daha şeffaf bir şekilde kurgulanması önem arz etmektedir.

OECD (Organisation for Economic Co-operation and Development/ Ekonomik Kalkınma ve İşbirliği Örgütü) ise hazırladıkları ve tavsiyelerini içeren metnin, uygulanmasıyla birlikte siber uzay alanındaki hali hazırdaki risk oluşturan durumların değerlendirilmesi ve bu konuyla ilgili uygulanacak yönetimsel faaliyetlerin daha kapsamlı bir kamu politikası haline dönüştürülmesi için belirli teşvik olanaklarının da oluşturulması gerektiğini düşünmektedir. Bu bağlamda uluslararası ve bölgesel düzeyde hem devlet yönetimi açısından, hem de sivil toplum kuruluşlarıyla birlikte ortak ve yeni koordinasyonu sağlayacak mekanizma ve yapılar kurulmalıdır. Bunun yanında da kamu ve özel sektördeki kurumlarında ortak iş birliklerini güçlendirmeleri de gerekmektedir

(OECD, 2015).

Artık internet ve bilgisayar tabanlı sistemlerin kullanıldığı gözetleme pratikleri, hayatın her alanını hiç ara vermeksizin kuşatmaktadır. Dijital medya uygulamalarının ve kullanıcı sayısının artışı ile süreç güç kazanarak yoluna devam etmektedir. İnsanların politik ve ekonomik nedenlerle attıkları adımlar takip edilirken, ticari faaliyet içerisinde bulunan kurumlar, bu gözetlemeyi kurumsal iletişim stratejilerini geliştirmek ve hedef kitleyi anlamak noktasında kullanmaktadır. Tüm bu süreç, Covid-19 döneminde yoluna daha da artarak devam etmektedir. Bu gereksinim ve bireyin dijital ortamda var olma çabası ve Covid-19 gibi salgın dönemlerinin bu var olma çabasını zorunlu kıldığı günümüz şartlarında, kurumların sahip oldukları verilerin değerini, kurum ve marka sürdürülebilirliği açısından önemini, daha da fazla kavramaları gerekmektedir. Mahremiyet kavramı, teknolojinin getirdiği dijital çağla yeniden şekillenmiştir. Bu dijital çağın, yeni kullanıcıları olan kurumlar, hedef kitlelerinin bilgilerinin ve verilerinin güvenliğini sağlamakla yükümlüdürler. Çünkü insanların ve kurumların, bu teknolojik araçlara duydukları gereksinim gün geçtikçe artmaktadır. Veri ihlallerinin artışını azaltmak yönünde çok ciddi adımlar atılması gerekmektedir.

Kaynaklar

Barkuş, F., & Koc, M. (2019). Dijital Mahremiyet Kavramı ve İlgili. Bilim, Eğitim, Sanat ve Teknoloji Dergisi, 1(3), 35-44.

Baudrillard, J. (2008). Tüketim Toplumu. İstanbul: Ayrıntı.

Bauman, Z. (2011). Bireyselleşmiş Toplum. (Y. Alogan, Çev.) İstanbul: Ayrıntı.

BBC News. (2018, Mart 20). 5 soruda Facebook verilerini 'usulsüz kullanmakla' suçlanan Cambridge Analytica. BBC: https://www.bbc.com/turkce/haberler-dunya-43469094 adresinden alındı

Berg, B. L., & Lune, H. (2015). Sosyal bilimlerde nitel araştırma yöntemleri. Ankara: Eğitim Kitabevi.

Bozoğlu, T. (2018). Teknoloji, yönetim ve mekân: Gözetim, denetim, mahremiyet ve mekânsal yapılandırmayla pratiklerinin kurumsallaşması. Ekonomi, Politika & Finans Araştırmaları Dergisi, 3(3), 259-288.

Bölükbaş, Ö. Ö. (2014). İnsan hakları ve elektronik gözetim. Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The guardian, 17, 22.

Canbolat, M. (2013). Gözetim toplumu ve mahremiyet. Çağın Polisi Dergisi , (139), 28-30.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5), e1211.

Collins, J. (2005). National institute of justice crime report. USA: US Department of Justice, Office of Justice Programs, Michigan State University.

Creswell, J. W. (2013). Nitel araştırma yöntemleri. Ankara: Eğiten Kitabevi.

Diler, R. (2014). Mahremiyet eğitimi ve önemi. Gaziosmanpaşa Üniversitesi İlahiyat Fakültesi Dergisi, 2(1), 69-98.

Efe, F. (2013). Kent bilgi sistemlerinin oluşturulmasında verilerin disiplinlerarası araştırma ve analizlere uygun kurgulanması: e-kent modeli. Akademik İncelemeler Dergisi, 8(3), 127-161.

Gal, M. D., Borg, W. R., & Gall, J. P. (1996). Educational research an introduction. USA: Longman.

Giddens, A. (2014). Modernite ve Bireysel Kimlik-Geç Modern Çağda Benlik ve. İstanbul: Say.

Goodman, M. (2016). Geleceğin suçları- dijital dünyanın karanlık yüzü. İstanbul: Timaş.

Goold, B. J. (2002). Public area surveillance and police work: The impact of CCTV on police behaviour and autonomy. Surveillance & Society, 1(2), 191-203.

Gündoğdu, A. (2014). Dijital demokratik toplum kamuda sosyal politika. Ankara: Nonn Yazılım.

Hartley, J. F. (1995). Case studies in organizational research. C. Cassell, & G. Symon içinde, Qualitative methods in organizational research: A practical guide. London: Sage.

IBM Security. (2020). Cost of a data breach report. IBM: https://www.ibm.com/downloads/cas/RZAX14GX (Erişim Tarihi: 10.09.2021) adresinden alındı

IBM Security. (2021). Cost of a data breach report 2021. IBM: https://www.ibm.com/tr-tr/security/data-breach (Erişim Tarihi: 15.09.2021) adresinden alındı.

Kişisel Verilerin Korunması Kanunu. (2016). T. C. Resmi Gazete. (07.04.2016) (Sayı: 29677). https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf. (Erişim Tarihi: 10.03.2022) adresinden alındı.

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. Business Horizons, 59(3), 257-266.

McMillan, J. H. (2000). Educational research: Fundamentals for the consumer. New York: Longman.

Merriam, S. B. (1990). Case study research in education. San Francisco: Jossey-Bass.

OECD. (2015). Digital security risk management for economic and social prosperity: OECD recommendation and companion document. Paris: OECD Publishing.

Özdemir, Ş. (2020). Post-panoptikon çağı: Gözetimin dijitalleşmesi ve çevrimiçi kimliğin gizliliği. Anadolu Üniversitesi Sosyal Bilimler Dergisi, 20(3), 81-108.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft?. Journal of Policy Analysis and Management, 30(2), 256-286.

Sayın Ağa, S., & Kömürcü, N. (2015). Doğumda mahremiyet. Türkiye Klinikleri Doğum-Kadın Sağlığı ve Hastalıkları Hemşireliği- Özel Konular, 1(3), 9-15.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. Journal of Management Information Systems, 32(2), 314-341.

Sener, G. (2013). Sosyal medyada mahrem ilişkiler gözetleme ve dijital şiddet. XV. Akademik Bilişim Konferansı. Antalya: Akdeniz Üniversitesi.

Shah, M., & Okeke, R. (2011). A framework for internal identity theft prevention in retail industry. 2011 European Intelligence and Security Informatics Conference. doi:10.1109/eisic.2011.29.

Singer, P. W., & Friedman, A. (2015). Siber güvenlik ve siber savaş. (Çev. A. Atav). Buzdağı Yayınevi.

Sputnik. (2019, Temmuz 24). Facebook, Cambridge Analytica skandalı için 5 milyar dolar ceza ödeyecek. Sputnik: https://tr.sputniknews.com/abd/201907241039753703-facebook-cambridge-analytica-skandali-icin-5-milyar-dolar-ceza-odeyecek/ adresinden alındı

Sunal, G., & Karadoğan, İ. E. (2012). Gözetlenen ve gözetleyen bir toplumda, beden ve mahremiyet ilişkisi: Facebook örneği. Akdeniz İletişim Dergisi, 21-41.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). Ulusal siber güvenlik stratejisi ve 2016- 2019 eylem planı.

Talay, Ö. (2018). Mobil ortam reklamlarında dijital gözetim algısı: dijital göçmenler ve dijital yerlilerin karşılaştırmalı analizi. . Antalya: Akdeniz Üniversitesi, Sosyal Bilimler Enstitüsü.

Türk Dil Kurumu. (2011). Büyük Türkçe sözlük. Ankara: TDK.

Türk, G. D., & Demirci, E. (2016). Sanal dünyada dönüşen mahremiyet algısı; Instagram örneği. 1st International Academic Research Congress, (s. 518-525).

Utma, S. (2018). Mahremiyet olgusu ve sosyal medyada mahremiyetin serüveni. Uluslararası Sosyal Araştırmalar Dergisi, 11(59), 1193-1204.

Yayla, M. (2014). Siber savaş ve siber ortamdaki kötü niyetli hareketlerden farkı. Hacettepe Hukuk Fakültesi Dergisi, 4(2), 85.

Yeğin, A. (1993). Osmanlıca-Türkçe ansiklopedik büyük lûgat. İstanbul: Türdav Yayınları.

Yin, R. (1984). Case study research:Design and methods. Beverly Hills: Sage.

Destekleyen Kurum/Kuruluşlar: Herhangi bir kurum/kuruluştan destek alınmamıştır.

Çıkar Çatışması: Herhangi bir çıkar çatışması bulunmamaktadır.