Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi
Hacettepe University Journal of Faculty of Letters

Cilt/Volume: 35 Sayı/Number:2
Aralık/December 2018

doi: 10.32600/huefd.439007

Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi

The Concept of Privacy and Personal Data in Digital Life: Analysis of Perceptions of Students' at Hacettepe University Department of Information Management

Şahika EROĞLU*

Öz

Kişisel verilere yetkisiz erişim ve bu verilerin yetkisiz kişi ve kuruluşlarca kullanımları, günümüz dünyasında öne çıkan sorunlardan biri olarak algılanmaktadır. Bu bağlamda konunun mahremiyet (gizlilik) kavramı çerçevesinde değerlendirilmesi ve toplumun her kesiminde konuya yönelik farkındalığın oluşturulması önem taşımaktadır. Bu çalışma, günlük hayatlarında çoğunlukla dijital ortam ile etkileşim içinde olan kullanıcı gruplarından biri olan öğrencilerin konuya ilişkin algı ve farkındalık düzeylerini ortaya çıkarmayı amaçlamaktadır. Belirtilen amaç doğrultusunda, aldıkları lisans eğitiminin bir sonucu olarak kurumlarda kişisel verilerin yönetimi ile ilgili süreçlerde yer alma potansiyeli taşıyan Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğrencileri analiz edilmiştir. Bu kapsamda öğrencilerin dijital ortamlardaki mahremiyet ve kişisel veri algıları ile ilgili web tabanlı bir anket, literatür taramasından yararlanılarak geliştirilmiştir. 34 sorudan oluşan web tabanlı bu anket 280 öğrenciye gönderilmiştir. 151 öğrenci tarafından yanıtlanan anket ile öğrencilerin kişisel veri mahremiyeti farkındalıklarına yönelik bulgular elde edilmiştir. Çalışma sonuçlarında öğrencilerin neleri kişisel veri olarak algıladıkları, konuyla ilgili farkındalık eksiklikleri ve karşılaşabilecekleri olası durumlara yönelik ne tür önlemler aldıkları vurgulanmıştır.
Anahtar Sözcükler: Mahremiyet, gizlilik, kişisel veriler, kişisel veri güvenliği.

Abstract

Unauthorized access to personal data and use of such data by third parties are seen as one of the most prominent problems in today's world. In this regard it is important to evaluate data usage and sharing activities of individuals within the framework of the term privacy and to create awareness of the issue in the society. This study aims to reveal perceptions and awareness levels of students who are one of the user groups mostly interacting with the digital environment in their daily lives. In the light of the described aim, students at Hacettepe University Department of Information Management who have the potential to take part in the processes related to the management of personaldata in the institutions as a result of the undergraduate education, are examined. In this regard, a web based questionnaire about personal data privacy perceptions was developed according to literature review. The questionnaire consisting of 34 questions was delivered to 280 students. The survey, which was answered by 151 students, provided findings on students' privacy awareness of personal data. The results illustrate which data are perceived as personal by the students, their lack of awareness about the subject and also point out the kind of measures they took to protect it.
Keywords: Privacy, secrecy, personal data, personal data security.

* Araş. Gör. Dr., Hacettepe Üniversitesi Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bölümü, sahikaeroglu@hacettepe.edu.tr

Giriş

Elektroniklerin kullanımı ve bilgi teknolojilerinin gelişimiyle ortaya çıkan dijital devrimle birlikte mahremiyete (gizlilik) yönelik tanımlar ve düşünceler de değişim göstermiştir. Mahremiyetin yapısı ve uygulanışıyla ilgili mevcut düşüncelerimiz teknolojik gelişmelerle şekillenmektedir. Daha önceleri bedensel gizlilik ile ilişkilendirilen mahremiyet kavramı teknolojiyle birlikte internet gizliliği, kişisel verilerin gizliliği gibi farklı açılardan ele alınmaya başlamıştır. Genel olarak, kullanıcıların çevrimiçi ortam üzerinden gerçekleştirdiği bankacılık işlemleri, ticari işlemler, alışveriş, vatandaşlık hizmetleri ve sosyal ağ etkileşimi gibi faaliyetler sırasında kişisel bilgilerin toplanması, işlenmesi ve dağıtımı gizlilik ve mahremiyet sorunlarını gündeme getirmiştir.

Birçok insanın hayatının ayrılmaz bir parçası haline gelen internet, bir iletişim kanalı, sosyal çevre, bilgi kaynağı ve işlem ortamı olarak görülmektedir. Bu durum da insanların internet üzerinden daha fazla bilgi paylaşımında bulunmalarına neden olmaktadır. Öyle ki her birimiz günlük aktivitelerimizi (alışveriş, sosyal medya araçları ile iletişim, vergi ödeme, haberleri okurken, müzik dinlerken, fotoğraf paylaşırken) yerine getirirken kişisel bilgilerimizi bilinçli ya da bilinçsiz, istekli ya da isteksiz bir şekilde açığa çıkarmaktayız. Bunun yanı sıra, birçoğumuz sosyal medya araçlarını kullanırken de özel yaşantımıza dair birçok bilgimizi bilinçli ya da bilinçsiz bir şekilde paylaşabilmekteyiz. Bu durum kişisel verilerin açığa çıkarılmadan günlük işlerin yürütülmesini neredeyse imkânsız hale getirmektedir (Nissenbaum, 2010, s. 2).

Bireylerin dijital platformlarla etkileşim sürecinde açığa çıkardıkları kişisel bilgiler, bilgi ekonomilerinde alınıp satılan bir meta haline gelmiştir. Bireylerin daha iyi hizmetlere veya ürünlere erişmek adına çevrimiçi ortamlarda daha fazla kişisel veri paylaşmaları, söz konusu ortamda yaptıkları her şeyin toplu bir fotoğrafının kolaylıkla çekilmesine zemin hazırlamaktadır. Dahası büyük veri ve tahminsel analitik yöntemler, günlük yaşamda oldukça somutlaşan kavramlar olarak karşımıza çıkmaktadır. Bireylerin çevrimiçi etkileşime olanak tanıyan platformlardaki bütün iş ve işlemleri veri olarak toplanıp anlamlandırılabilmektedir. Daha da önemlisi bu anlamlandırmalar siyasal düşünce, cinsel yönelim, ırk, din, sağlık, finans, sosyal bağlantılar ve arkadaşlık döngüleri, istihbarat, sosyal ve mesleki statü, vb. gibi kişisel mahremiyetinizin ihlali boyutuna kadar gelebilmektedir. Çevrimiçi platformlara yönelik gizlilik ve mahremiyet endişeleri çoğunlukla izinsiz olarak kişisel verilerin paylaşımı, kişisel verilerin üçüncü parti kişi ve kuruluşlarca kullanılması gibi başlıkları içermektedir (Boyd ve Ellison, 2007). Yasal açıdan bakıldığında, mahremiyet temel olarak genel insan hakları, anayasal haklar ve daha spesifik olarak da veri koruma kuralları ile korunmaktadır (Tuunainen, Pitkänen ve Hovi, 2009). Bu çerçevede son dönemde kişisel verilerin gizliliğine yönelik çalışmalar yoğunlaşırken, konuya yönelik düzenlemeler de geliştirilmektedir. Birçok ülkede gizlilik kavramı veri koruma ile birlikte anılırken, gizlilik kavramı kişisel verilerin yönetimi açısından yorumlanmaktadır. Konuya yönelik literatürün de yaşanan gelişmeler doğrultusunda şekillendiği anlaşılmaktadır. Birçok çalışmada, gizlilik risklerine, kullanıcıların sosyal medya ve e-ticaret gibi farklı çevrimiçi ortamlardaki gizlilik farkındalığına yönelik analizler yapılmıştır (Dinev ve Hart, 2005; Aïmeur, Gambs ve Ho, 2010; Pitkänen ve Tuunainen, 2012; Buchenscheit vd., 2014; Almuhimedi vd., 2015). Bu konuda yapılan çalışmalar değerlendirildiğinde, farklı ortamlarda bireylerin kişisel bilgilerinin önemli bir bölümünü farkında olarak ya da olmayarak açıkladıkları anlaşılmaktadır. Çalışmalarda kullanıcıların bu paylaşımlarının risklerine yönelik farkındalık düzeylerinin düşüklüğü anlaşılırken, genç kuşaktaki farkındalık düzeyinin nispeten yüksek olmasına rağmen bu ortamlardaki gizliliğe yönelik ayarların ve ilgili politikaların büyük ölçüde anlaşılmadığı ya da göz ardı edildiği vurgulanmaktadır.

Temel bir insan hakkı olarak görülen mahremiyet kavramı üzerindeki algılar ve uygulamalar, teknolojinin yarattığı etkilerle değişim göstermektedir. Yaygın olarak teknoloji kullanımı çoğu zaman özel alan ile kamu alanı arasındaki dengeyi bozarak mahremiyet ve gizliliğe yönelik riskler yaratmaktadır. Bu bağlamda özellikle çevrimiçi ortam ile sürekli etkileşim halinde bulunan bireylerin mahremiyet ve kişisel verilere yönelik algıları, konuyla ilgili farkındalıkları ve kişisel verilerin kullanımına yönelik yeterlilikleri önemlidir. Çalışmada Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğrencilerinin çevrimiçi ortamlardaki mahremiyet ve kişisel veri algıları incelenmiştir. Bu çerçevede kullanıcıların farkındalıklarının kişisel verilerin mahremiyetine yönelik etkilerinin neler olduğunun ortaya konması amaçlanmaktadır. Bunun yanı sıra çalışma ile genç kuşağın kişisel veri ve mahremiyet algılarına yönelik

bir farkındalığın oluşturulması amaçlanmaktadır. Çalışmada ilk olarak mahremiyet ve dijital yaşamdaki mahremiyet ve kişisel veriler ile ilgili literatür değerlendirilmektedir. Daha sonra çalışma kapsamında araştırma metodolojisi sunularak Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğrencilerine uygulanan anket bulguları sunulmaktadır. Son bölümde ise çalışmanın sonuçları tartışılarak değerlendirmelere yer verilmektedir.

Dijital Yaşam ve Mahremiyet (Gizlilik)

Mahremiyet temel bir insan hakkıdır. İnsan onurunu destekleyen örgütlenme özgürlüğü ve ifade özgürlüğü gibi hakların temelini oluşturmaktadır. Mahremiyet kavramının modern çağın en önemli insan hakkı olduğu söylenmektedir. Diğer yandan tüm insan hakları arasında tanımlanması en zor kavramlardan biri mahremiyet olarak görülmektedir (Bennett, 2009). Mahremiyet ile ilgili tanımlar birçok bağlamda farklılık göstermesine ragmen, hukukta ortak ve yaygın mahremiyet tanımları bedensel, bölgesel, bilgi ve iletişim gizlilikleri üzerine yoğunlaşmaktadır. Kavram olarak mahremiyet, kişilerin yalnız kalabildikleri, düşünebildikleri, davranabildikleri, diğer bireylerle hangi sınırlarda ilişki ve iletişim kuracaklarına kendilerinin karar verdiği bir alanı ifade etmektedir (Yüksel, 2003). Bu bağlamda mahremiyet hakkı da bireylerin kendi hayat alanlarını diğerleri ile ne ölçüde paylaşacaklarını belirleme hakkı olarak düşünülebilir. Modern anlamda bilinen mahremiyet (gizlilik) hakkı, 1890'da iki avukatın girişimiyle başlatılmıştır (Bennett, 2009). Amerikalı yargıç Brandeis tarafından "yalnız bırakılma hakkı; hakların en kapsamlısı ve özgür insanlar tarafından en çok değer verilen hak" olarak tanımlanmıştır. (Bennett, 2009).

Mahremiyet kavramı kültürden kültüre hatta zaman zaman bireyden bireye değişiklik gösterebilen bir kavramdır. Bu nedenle kavramın tanımlanması, sınırlarının belirlenmesi güçleşmektedir. Mahremiyet yaklaşımları üç boyutta ele alınmaktadır. Bunlar (Kokolakis, 2017):

- Bölgesel mahremiyet: Bir insanı çevreleyen fiziksel alanla ilgili gizlilik.
- Kişi mahremiyeti: Bir bireyin fiziksel varlığına karşı gereksiz müdaheleyi temsil eder (örn: fiziksel arama).
- Bilgi mahremiyeti (gizliliği): Kişisel verilerin toplanması, depolanması veya nasıl işlenebileceğinin ve dağıtılabileceğinin kontrol edilmesi ile ilgilidir.

Bu boyutlar ilk olarak fiziksel alanın korunması, ardından haksız müdahalelere karşı kişilerin korunması, son olarak da kişilerin bilgi güvenliğinin korunması gerekliliğini içermektedir (Kokolakis, 2017). Mahremiyetin bütün ayrımlarına rağmen ortak olan noktasınının kişilerin kendi alanlarında kontrolü sürdürebilmesi olduğu anlaşılmaktadır. Bu noktada bireylerin kendi kontrollerini sürdürebildikleri miktarda mahremiyet alanlarının da arttığı söylenebilir.

Bilgi ve iletişim teknolojilerinde yaşanan hızlı değişimler ve içinde bulunduğumuz dijital yaşamda bireylerin mahremiyet haklarına saldırılar oldukça kolaylaşmış bulunmaktadır. Günümüzde bireylerin çalışırken, gündelik hayat aktivitelerini yerine getirirken veya boş zamanları değerlendirirken interneti kullanmaları neredeyse bir zorunluluk haline gelmiştir. Öyle ki kablosuz internet bağlantısına sahip olmak veya çevrimiçi olmak insanlar için temel bir gereksinim ve hak olarak düşünülmektedir (Tan ve Pivot, 2015). Bu süreçte bireylere yönelik olarak birçok formatta içerik üretilmekte ve bu içerik kayıt altına alınmaktadır. Söz konusu içerik dijital dünyada bireylerin özel hayatına ilişkin birçok bilgiyi de barındırabilmektedir. Bir bireyin çevrimiçi davranışları, kişisel mahremiyet de dâhil olmak üzere, bireyin gerçek hayatını büyük ölçüde yansıtmaktadır. Bu bağlamda geliştirilen büyük veri analiz yöntemleri bireylerin çevrimiçi ayak izlerini toplamak aracılığıyla bireylerin kişisel profillerini kolaylıkla açığa çıkarmaktadır. Bu ortamda, bireylerin, özel yaşamlarına ilişkin verilerin açığa çıkması, sağlık kayıtlarının güvenliği, finansal verilerin güvenliği, özel hayatın mahremiyeti vb. gibi kaygıları artmaktadır. Dijital çağda yaşanan bu durum George Orwell'in kaleme aldığı "1984" adlı eseri akla getirmektedir. Edebiyat tarihinin en çok akılda kalan sözlerinden birisi olan ve romanın da eksenini oluşturan "Büyük birader seni gözetliyor" (Big Brother is watching you) cümlesi her şeyi görebilen, her şeye kadir gözcünün tanımı olarak nitelendirilmektedir (Orwell, 1948). Aslında Orwell bu eserde, her şeyi görebilen bir göz olmanın gücünden bahsederken, bilginin gücünün de altını çizmektedir. Bu açıdan değerlendirildiğinde eserin büyük veri dünyasında yaşanan mevcut durumu yansıttığını da söylemek mümkündür.

Büyük veri uygulamalarıyla ortaya çıkan teknikler ve analizler bireylerin mahremiyetini korumak için geleneksel yolların artık etkili olmayacağını göstermektedir. Bu doğrultuda birçok ülke mahremiyet ve gizliliğe yönelik yasalar ve düzenlemeler geliştirmektedir. Söz konusu gizlilik yasaları kişinin rızasına ve kişisel bilgilerin toplanmasına odaklanmıştır. Fakat günümüzde bu durum yeterli olamamaktır. Çünkü kişisel verilerin toplanmasına yönelik birey onayı, verilerin toplanması esnasında gerçekleşmektedir, fakat çevrimiçi süreçlerde kullanılan birçok veri kişisel verilerle doğrudan ilgili olmamasına rağmen bireylere yönelik çok önemli ipuçlarını barındırabilmektedir. Bu noktada çevrimiçi davranışların kaydı, log kayıtları tutulması gibi yöntemlerle toplanan verilerin anlamlandırılması doğrultusunda da kişisel veriler elde edilebilmektedir (Tan ve Pivot, 2015). Bu durum mahremiyetin korunmasına yönelik kaygıların artmasına neden olmaktadır.

Literatürdeki birçok çalışma da bireylerin mahremiyete yönelik kaygılarını ortaya koymaktadır. Çalışmalarda genel olarak konuya yönelik bilgi eksikliğinin ve kontrolün bireylerin ellerinde olmadığı düşüncesinin mahremiyete yönelik kaygıları artırdığına değinilmektedir (Dinev ve Hart, 2005; Dwyer, Hiltz, ve Passerini, 2007; Goettke vd., 2007; Miltgen, 2009; Ridley-Siegert, 2015; Tan ve Pivot, 2015). Konuyla ilgili araştırmalarda öğrencilerin de analiz edildiği görülmektedir. Bu kapsamda yapılan bir çalışmada öğrencilerin mahremiyet kaygıları ve Facebook kullanımlarına yönelik farkındalıklarının yüksek olmasına ve kişisel olarak tanımlanabilecek bilgileri paylaşmanın olası sonuçlarından haberdar olmalarına rağmen, yine de kişisel bilgileri bu platformlarda kullanma konusunda yeterince rahat oldukları belirtilmektedir (Govani ve Pashley, 2007). Diğer yandan çevrimiçi sosyal ağlara yönelik birçok çalışma, gençlerin kendi özel bilgilerini korumadıkları şeklindeki yaygın varsayımlara meydan okumaktadır. Araştırmalar gençlerin bu ortamlarda kendi oluşturdukları çeşitli koruma stratejilerini kullandıklarını göstermektedir. Bu stratejiler; takma isimler kullanma ve yanlış bilgi verme, kişisel profillerine erişim ve gizliliğe yönelik ayarları yapma, arkadaşlık taleplerini sınırlandırma, etiket ve fotoğrafları silme gibi stratejiler olarak sıralanmaktadır (Boyd ve Hargittai, 2010; Miltgen ve Peyrat-Guillard, 2014; Young ve Quan-Haase, 2013).

Mahremiyet (gizlilik) koşullarına ilişkin bilgilendirme metinleri ile ilgili olarak kullanıcıların gittikçe daha fazla sorun yaşadıkları anlaşılmaktadır. Bu durum söz konusu metinlerin içeriklerinin okunmasının mahremiyet kaygılarını artırması veya okuma ve anlama zorlukları ile ilişkilendirilmektedir (Milne ve Culnan, 2004; Milne, Culnan, ve Greene, 2006). Nitekim yapılan birçok çalışma bireylerin çevrimiçi ortamlarda özellikle yarar sağladıklarını düşündükleri durumlarda (örneğin gerekli bir bilgiye ulaşmak için web sitesine kayıt olurken) söz konusu koşulları okumadan kolaylıkla kişisel verilerini paylaşbildiklerini göstermektedir.

Çalışmalar mahremiyet kaygıları ile koruma davranışı arasında pozitif bir ilişkinin olduğunu da göstermektedir (Lutz ve Strathoff, 2014). Sıkı gizlilik düzenlemeleri olan ülkelerde daha az mahremiyet (gizlilik) problemleri yaşandığı belirtilmekte; fakat bu durumun reklam ve diğer tüketici pazarlama etkinliklerinde dezavantajlara yol açtığı da ifade edilmektedir (Martin ve Murphy, 2017).

Dijital dünyada çevrimiçi süreçlerde tüm bilgiler takip edilebilmektedir. Çevrimiçi ayak izlerinin yanı sıra içinde bulunduğumuz toplumda, güvenlik kameraları, akıllı ev sistemleri, akıllı şehirler, RFID (Radio Frequancy Identification) sistemleri, GPS(Global Positioning) System), mobil araçlar, giyilebilir teknolojiler (akıllı saatler, akıllı bileklikler, akıllı giysiler vb.), sağlık gözlem aletleri gibi birçok sistem ve uygulama her an kişisel verilere erişebilmektedir. Söz konusu sensör ve sensör sistemleri kamu hizmetleri ve planlamalarında, trafik kontrolünde, kamu güvenliğinde, sağlık hizmeti verimliliğinde, ekonomik büyümede, günlük yaşamda büyük avantajlar sağlamasına rağmen, mahremiyet konusunda riskler oluşturmaktadır (Tan ve Pivot, 2015). Yaygın bir şekilde kullanılan internetin ve büyük veriye yönelik teknik ve uygulamaların, çevrimiçi ortamdaki verilere erişimi ve bu verileri toplamayı kolaylaştırdığını söylemek mümkündür. Bu ortamda gittikçe daha yoğun olarak üretilen kişisel veriler, insanlar, veri sağlama şirketleri veya yönetimler tarafından rahatça bulunabilmekte ve toplanabilmektedir. Günümüz dünyasında kişilik hakları, mahremiyet ihlalleri ile zarar görebilmektedir. Bu noktada özellikle büyük veri evreninde mahremiyet konusu üzerine oluşabilecek riskleri toplum farkındalığına sunmak, söz konusu risklere yönelik önemli korunma adımlarından birisi olarak düşünülülebilir.

Kişisel Veriler, Mahremiyet ve Konuya Yönelik Düzenlemeler

Mahremiyet kavramı bilgi ve iletişim çağında özellikle kişisel veriler bağlamında ele alınmaktadır. Bilgi teknolojilerinin hızla ilerlediği günümüz dünyasında, mahremiyet ihlalleri ile kişilik hakları zarar görebilmektedir. Söz konusu zararları engellemek ya da azaltmak adına, kişilik haklarının bir parçası olan kişisel verilerin elektronik ortamda işlenmesi ve paylaşımı noktasında birçok düzenleme yapılmaktadır. Bu bağlamda kişisel veri kavramının ayrıntılı olarak açıklanması önemlidir. Kişisel veri kavramı net olarak sınırları tanımlanamamış bir kavramdır. Kavram, ilgili mevzuatta kimliği belirli veya belirlenebilir kişilere ilişkin her türlü bilgi olarak ifade edilmektedir (Kişisel Verilerin Korunması Kanunu, 2016). Örneğin kişinin adı, adresi, doğum tarihi, telefon numarası vb. veriler kişisel verileri ifade etmektedir Kanun'da ayrıca 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 güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri gibi veriler, özel nitelikli kişisel veriler olarak tanımlanmaktadır.

Teknoloji ve bilgi sistemleri, çoğu insan için günlük yaşamın bir parçası olmasına rağmen, modern bilgi ve iletişim sistemleri çok karmaşık ve kafa karıştırıcı olabilmektedir. Bireyler genellikle söz konusu sistemlerde, onlar hakkında ne tür verilerin toplandığına ve nerede tutulduğuna, ne kadar süre tutulacağına ve ne için kullanılacağına dair hiçbir fikre sahip değildir (Almuhimedi vd., 2015). Mahremiyet ve gizliliğe yönelik risklerin önemli bir boyutu ise, internette ve sosyal ağ sitelerinde bireylerin paylaştıkları kişisel bilgilere kimlerin erişebildiğidir. Bu bağlamda çevrimiçi gizlilik ve mahremiyet tehditleri ve riskleriyle ilgili tartışmalarda kişisel olarak nitelendirilebilecek bilgilerin tanımlanması ve bu bilgilere yönelik farkındalığın oluşturulması önemli olmaktadır (Aïmeur, Gambs, ve Ho, 2010). Kişisel verilere kötü amaçlı üçüncü şahıslar tarafından erişildiğinde, mahremiyet ve gizliliğe yönelik risklerin de gerçekleşmesi olasılığı artmaktadır. Riskin niteliği ve niceliği, sağlanan verinin türü ve miktarına göre değişmektedir. Bu kapsamda erişilen veri, bazı durumlarda çok kapsamlı ve özel olabilmektedir. Bu durum, kimlik hırsızlığından, şantaja, ayrımcılıktan, çevrimiçi veya fiziksel takipe kadar uzanabilmektedir (Gross ve Acquisti, 2005; Hughes-Roberts ve Kani-Zabihi, 2014). Kişisel bilgilerin gizliliğinin ve kontrolünün kaybedilmesi, sosyal olarak telafisi mümkün olmayan zararlara neden olabilmektedir. Bu bağlamda konuya yönelik bireylerin çevrimiçi ortamda ortaya çıkabilecek mahremiyet ihlallerine karşı farkındalık kazanmaları ve bilgi sahibi olmaları önemlidir.

Bir verinin kişisel veri niteliği kazanması veya belirli bir kişiyi temsil etmesi ancak verinin işlenme sürecinde kesinlik kazanabilmektedir. Kişisel verilerin işlenmesi, verilerin elde edilmesi, kaydedilmesi, düzenlenmesi, uyarlanması, dönüştürülmesi, kullanımı, açıklanması, birleştirilmesi, silinmesi gibi süreçlerden oluşmaktadır (Kaya, 2011). 1980 yılında yayımlanmış ve 2013 yılında güncellenmiş olan Ekonomik İşbirliği ve Kalkınma Örgütü (Organisation for Economic Co-operation and Development-OECD) Rehber İlkeleri; kişisel verilerin korunması ve işlenme sürecinde dikkate alınması gereken prensipleri şu şekilde belirlemiştir (OECD, 2013):

- Sınırlılık: Kişisel veriler, hukuka uygun sebepler ve araçlarla toplanmalıdır, veri sahiplerinin toplama konusunda bilgilendirilmeleri ve bilinçli rızalarının alınması gerekmektedir.
- Kalite: Toplanan veriler kullanılan amaç doğrultusunda mümkün olduğunca tam, güncel ve doğru olmalıdır.
- Amaca Özgülük: Kişisel verilerin toplanma amacı belirlenmelidir. Veriler sadece belirlenen amaç için kullanılmalıdır.
- Kullanım Sınırlaması: Toplanan veriler belirtilen amaçlar dışında yayılamaz, bulundurulamaz veya başka amaçlarla kullanılamaz. Veri sahibinin bilinçli rızası ve kanuna dayalı yetkiler bu maddenin sınırlaması olabilir.
- Güvenlik: Toplanan verilere yönelik oluşabilecek tehlikelere karşı (kayıp, yetkisiz erişim, zarar verme, değiştirme, açıklama) uygun güvenlik tedbirleri ile korunmalıdır.
- Açıklık: Kişisel verilerle ilgili gelişmeler, uygulama ve politikalar hakkında genel bir açıklık ilkesi bulunmalıdır. Bireyler kendileri ile ilgili veri barındıran kurumların politikalarına kolayca ulaşabilmelidirler.
- Bireyin Rızası: Veri sahibinin rızası olmaksızın veriler erişilebilir hale getirilmemeli ve açıklanmamalıdır.

- Hesap Verebilirlik: Veri sahipleri veri toplayıcı ve yayınlayıcılarına karşı sayılan diğer ilkeler çerçevesinde hesap sorma hakkına sahip olabilmelidir.

Kişisel verilerin korunması uzun süredir üzerinde çalışılan bir konu olmakla beraber, teknolojinin hızlı evrimi çerçevesinde konu boyut değiştirerek farklı bakış açıları ile yorumlanmaya başlamıştır. Öyle ki küresel veri hareketleri ve ülkeler arasında yaşanan veri trafiği nedeniyle kişisel verilerin korunması uluslararası açıdan da önem kazanmıştır (Akıncı, 2017). Bunun yanı sıra son yıllarda ülkelerin konuya yönelik hukuki altyapılarını teknolojik gelişmelerle uyumlaştırma çabaları da artmıştır.

Yaşanan süreçlerde kişisel verilere yönelik tehditlere karşı hem bireysel hem toplumsal savunma mekanizmalarının varlığı değer kazanmaktadır. Kişisel verilerin korunması özel hayat ve aile hayatına saygı hakkı bakımından önemlidir. Kişisel verilerin korunmasının uluslararası belgelerde, mahremiyete yönelik düzenlemelerle yorumlandığı görülmektedir. Mahremiyet, özel hayatın gizliliği ve kişisel verilere yönelik uluslararası düzenlemelerde aşağıdaki gibi ele alınmıştır:

- Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi 12. Maddesi: *"Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır"* şeklinde düzenlenmiştir (İnsan Hakları Evrensel Beyannamesi, 1949)
- Birleşmiş Milletler'in *Kişisel ve Siyasal Haklar Sözleşmesi*'nin 17. maddesi *"Mahremiyet Hakkı" (Right to Privacy)* olarak düzenlenmiştir (Kişisel ve Siyasal Haklar Sözleşmesi, 1966)
- Ekonomik Kalkınma ve İşbirliği Örgütü (OECD-Organizatin for Economic Co-operation and Development-) 1980'de *"Mahremiyetin Korunması ve Sınıraşırı Veri Akışına Dair Rehber İlkeler"* başlıklı metni yayımlamıştır (OECD, 2013).
- Avrupa Konseyi'nin *Avrupa İnsan Hakları Sözleşmesi*'nin 8. Maddesi özel hayata ve aile hayatına saygı hakkı olarak tanımlanmıştır (Avrupa Konseyi, 1950).
- Avrupa Birliği'nin 95/46 sayılı *"Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımı"* isimli Yönergesi, Birlikteki her üye ülkede kişisel verilerin eşit seviyede korunmasının garanti altına alınması amaçlanmıştır. Avrupa Avrupa Komisyonu tarafından üye ülkelerde uygulanmakta olan AB veri koruma kurallarında, Veri Koruma Direktifi'nde benimsenen ilkelerin modernize edilmesi ve gelecekte vatandaşların mahremiyet hakkının garanti altına alınması amacıyla, kapsamlı bir reforma gidilmesi ihtiyacı ortaya çıkmıştır. Bu çerçevede Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihinde "Genel Veri Koruma Tüzüğü (General Data Protection Regulation–GDPR)" onaylanmıştır (Akıncı, 2017).

Uluslararası düzenlemelerin yanı sıra konuya ilişkin Türk hukuk düzenlemelerinde mahremiyet ve kişisel verilere yönelik düzenlemeler de bulunmaktadır. Bunlar:

- Anayasamızın 20, 21, ve 22. Maddeler "Özel Hayatın Gizliliği ve Korunması" başlığını düzenlemektedir (T.C. Anayasası, 1982).
- "Türk Medeni Kanunu"nda 24. Maddesinde mahremiyet hakkına yönelik düzenlemeler bulunmaktadır (Türk Medeni Kanunu, 2001).
- "Bilgi Edinme Kanunu" 21. Madde (Bilgi Edinme Kanunu, 2003) ile mahremiyet'e yönelik hususlar düzenlenmiştir.
- "Türk Ceza Kanunu"nun 10, 125, 134, 135, 136, 137 ve 280. Maddelerinde (Türk Ceza Kanunu, 2004) özel hayatın gizliliği ve mahremiyet konusu ile ilgili düzenlemeler bulunmaktadır.

Türkiye'de kişisel verilerin korunmasına yönelik yasal düzenleme çalışmaları 2000'li yıllardan itibaren gündeme gelmiştir. 2016 yılında ise konuya yönelik kanun çalışması tamamlanmıştır. "6698 sayılı Kişisel Verilerin Korunması Kanunu" 7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Kanun ile "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" amaçlanmaktadır.

Dünya'da ve Türkiye'de kişisel verilerin korunması ve mahremiyete yönelik yapılan düzenlemeler değerlendirildiğinde, kişisel verilerin korunmasının temel insan hak ve özgürlükleri olarak kabul edildiği

görüldüğü anlaşılmaktadır. Bugün artık küresel boyutlarda yapılan veri paylaşımının güvenliğine yönelik ülkelerin gerek bölgesel gerekse uluslararası boyutlarda çözüm aradıkları ve konuya yönelik çalışmaların düzenli olarak yapıldığı değerlendirilmektedir. Bu bağlamda Birleşmiş Milletler, Ekonomik Kalkınma ve İşbirliği Örgütü, Avrupa Konseyi, Avrupa Birliği gibi uluslararası oluşumların yetkin çalışmaları ortaya çıkmıştır. Türkiye'de de 2010 yılında yapılan bir Anayasa değişikliği ile birlikte kişisel verilerin korunması anayasal hak statüsüne kavuşmuştur. Kişisel verilerin korunmasına yönelik atılan bu önemli adım Avrupa birliği Temel Hakları Şartını da karşılamaktadır. Akabinde Avrupa Konseyince hazırlanan 108 sayılı Sözleşme ile AB Direktiflerine paralel bir şekilde hazırlanan Kişisel Verilerin Korunması Kanunu Tasarısı ve 2016 yılında çıkarılan Kişisel Verilerin Korunması Kanunu'yla, AB ülkeleri nezdinde veri koruma bakımından güvenilir ülke statüsüne kavuşulması konusunda önemli bir kriter karşılanmış bulunmaktadır. Söz konusu Kanun ile bağımsız ve özerk bir Veri Koruma Otoritesinin kurulması ve akabinde ikincil mevzuat düzenlemelerinin hazırlanması öngörülmektedir.

Yöntem

Araştırmada; aldıkları derslerle (Bilgi Hukuku, Bilgi Merkezleri Yönetimi, Etik gibi.) ve aldıkları derslerin yanı sıra mezun olduktan sonra çalışacakları alanlarda da kişisel verilerin yönetimi ile ilgili süreçlerde yer alma potansiyeline sahip Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğrencilerinin çevrimiçi ortamlardaki mahremiyet ve kişisel veri algılarının betimlenmesi; bu algıların çevrimiçi ortamdaki kişisel veri ve mahremiyete yönelik davranışlara etkilerinin neler olduğunun ortaya konması amaçlanmaktadır. Bu çerçevede araştırmada evreni temsil ettiği düşünülen bir gruba dayalı olarak genelleme yapmaya yarayan bir yöntem olan betimleme yöntemi kullanılmıştır. Bununla birlikte araştırma kapsamında aşağıdaki araştırma sorularına yanıt aranmıştır.

- Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğrencilerinin günlük yaşamlarında çevrimiçi ortamlarda mahremiyet ve kişisel veri algıları ne düzeydedir?
- Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğrencilerinin çevrimiçi ortamlara yönelik mahremiyet ve kişisel veri algıları davranışlarını nasıl etkilemektedir?

Araştırmada veriler, anket tekniği ile toplanmıştır. Bu süreçte literatürdeki çalışmalardan da hareketle açık uçlu, çoktan seçmeli ve beşli likert ölçekli 34 sorudan oluşan web tabanlı bir anket geliştirilmiştir. Geliştirilen anket, Bölüm Öğrenci Bilgi Sistemi üzerinden e-posta ile bütün öğrencilere gönderilmiş ve bu ankette öğrencilerin kişisel bilgilerine yönelik hiçbir veri tutulmamıştır. Araştırmanın gerçekleştirildiği dönemde Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü lisans programında öğrenim gören kayıtlı 280 öğrenci bulunmaktadır. İki haftalık bir süre için açık bırakılan ve katılımın gönüllülük esasına dayandığı ankete 151 öğrenci yanıt vermiştir. Ankete yanıt veren öğrencilerin evreni temsil oranı %53,9'dur. Bir başka deyişle bu oranın bölümdeki her 2 öğrenciden birini temsil ettiği söylenebilir. Anketlerden toplanan veriler, nicel veri analiz yazılımlarından Predictive Analytics Software (PASW) yazılımı ile tablolaştırılmıştır. Açık uçlu ve diğer seçenekli sorulardan elde edilen bulgular ise ayrıca kodlanarak yorumlanmıştır. Araştırmada diğer seçeneği kapsamında toplanan veriler nitel verilerin sayısallaştırılması ve analizinde kullanılan yöntemlerden biri olan, metindeki içerik ve anahtar kelimeleri sayan, karşılaştıran ve sonra da yorumlayan sonuçlandırıcı (summative) içerik analizi yöntemiyle sunulmuştur (Hsieh ve Shannon, 2005).

Anketin içsel tutarlılığının ölçümlenmesi için PASW yazılımında 74 değişken altında toplanan veriler üzerinde güvenilirlik testi uygulanmıştır. Bu kapsamda demografik ve açık uçlu sorulara yönelik değişkenler çıkartıldıktan sonra elde edilen Crombach Alpha değeri, 0,93 olarak ölçülmüştür. Bu değer araştırmada elde edilen verilerin içsel tutarlılığının çok yüksek olduğunu ve yüksek derecede güvenilir olduğunu ortaya koymaktadır.

Bulgular

Öğrencilerin kişisel veri ve mahremiyet algılarına yönelik verileri analiz edilirken öncelikle öğrencilerin okudukları sınıf bilgileri değerlendirilmiştir. Araştırmaya katılan öğrencilerin %11,9'u (18 öğrenci) 1.Sınıf, %27,8'i (42 öğrenci) 2. Sınıf, %31,8'i (48 öğrenci) 3. Sınıf ve %28,5 (43 öğrenci) 4.

Sınıfta okumaktadır. Araştırmaya katılan öğrencilerin %92,7'si (140 öğrenci) interneti her gün kişisel amaçlar için kullandıklarını belirtirken ayda birden az interneti kullanan öğrenci bulunmamaktadır. Öğrencilerin neredeyse tamamı interneti en az haftada 4 veya 6 kere ve üzeri kullanmaktadır.

Tablo 1: Kişisel Veri Kavramı Bilme Durumu

Bilme durumu	**f**	**%**
Evet	72	47,6
Hayır	19	12,5
Kısmen	60	39,7
Toplam	**151**	**100,0**

Araştırmada öncelikle öğrencilerin kişisel veri algıları üzerine değerlendirmelerde bulunan analizlere yer verilmektedir. Bu doğrultuda araştırmaya katılan öğrencilerin kişisel verinin ne olduğunu bilip bilmeme durumu değerlendirildiğinde (Tablo 1), öğrencilerin yaklaşık yarısı (%47,6) kişisel verilerin ne olduğunu bildiğini düşünmektedir. Bunun yanı sıra kişisel verileri kısmen bildiğini düşünen öğrencilerin oranı %39,7 (60 öğrenci), kişisel verinin ne olduğunu bilmediğini söyleyenlerin oranı ise %12,5'dir (19 öğrenci).

Konu kapsamında açık uçlu olarak sorulan kişisel verilerin neler olduğu sorusuna verilen yanıtlar incelendiğinde elde edilen veriler Şekil 1 kapsamında kelime bulutu olarak görselleştirerek sunulmuştur. Şekil 1'e göre 590 sözcük üzerinden değerlendirme yapılmış ve öğrencilerin en fazla kimlik numarasını kişisel veri olarak belirttikleri görülmüştür. Genel olarak öğrencilerin kredi kartı bilgileri, ad soyadı, ev adresi, kimlik bilgileri ve doğum tarihi gibi kelimeleri en fazla kişisel veri olarak nitelendirdikleri anlaşılmaktadır.

Şekil 1. Kişisel Veriler Kelime Bulutu

Tablo 2: Kişisel Verilerin Korunması Hakkı ve Özel Hayatın Gizliliği gibi Hakların Bilinme Durumu

Bilme durumu	**f**	**%**
Konuyu az biliyorum	100	66,1
Konuyu bilmiyorum	6	3,1
Konuyu yeterli seviyede biliyorum	45	29,8
Toplam	**151**	**100,0**

Öğrencilerin kişisel verilerin korunması hakkı ve özel hayatın gizliliği gibi hakların bilinme durumunu yansıtan Tablo 2'ye göre, öğrencilerin yarısından fazlasının (100 öğrenci, %66,2) konuyu az bildiklerini nitelendirdikleri görülmektedir. Konuya yönelik yeterli seviyede bilgisi olduğunu düşünen öğrenciler, yaklaşık üçte bir oranındadır (45 öğrenci, %29,8). Diğer yandan konuyu hiç bilmediğini belirten az sayıda öğrenci olduğu anlaşılmaktadır (6 öğrenci, %3,1). Bu durum öğrencilerin genel olarak kişisel verilerin korunması hakkı ve özel hayatın gizliliği gibi haklara yönelik haberdar olma eğiliminde oldukları olarak düşünülebilir.

Tablo 3: 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndan Haberdar Olma Durumu

Haberdarlık durumu	**f**	**%**
Evet	46	30,4
Hayır	44	29,2
Kısmen	61	40,4
Toplam	**151**	**100,0**

Tablo 3'e göre öğrencilerin üçte biri (46 öğrenci, %30,4) 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndan haberdar iken, yaklaşık üçte birinin ise (44 öğrenci, %29,3) haberdar olmadıkları anlaşılmaktadır. Bunun yanı sıra öğrencilerin yarıya yakını (61 öğrenci, %40,4) Kanun'dan kısmen haberdar olarak görülmektedir. Tabloya göre genel olarak öğrencilerin yüksek oranda (107 öğrenci, %70,8) kısmen ya da tamamen 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndan haberdar oldukları anlaşılmaktadır.

Tablo 4: Kanun'dan Haberdarsanız Hangi Kanallar Aracılığı ile Haber Oluğu Bilgisi

Haberdar olunan kanal	**f**	**%**
Firma bilgilendirmeleri (SMS, İnternet vs.)	**101**	**66,8**
İnternet	**60**	**39,7**
Dersler	**42**	**27,8**
Gazete	21	13,9
Mevzuat Bilgi Sistemi	1	0,6

Tablo 4'e göre 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndan haberdar olan öğrencilerin yarısından fazlası (101 öğrenci, %66,8) Kanun'dan firma bilgilendirmeleri sayesinde haberdar olmuşlardır. Bu durumun son dönemlerdeki mecburi firma blgilendirmeleri ile ilişkili olduğu düşünülmektedir. Öğrenciler ikinci sırada (60 öğrenci, %39,7) internet vasıtasıyla Kanundan haberdar olduklarını ifade ederken, üçüncü olarak da dersler vasıtasıyla (42 öğrenci, %27,8) haberdar olduklarını belirtmişlerdir. Tabloya göre öğrencilerin en az (11 öğrenci, %7,2) Mevzuat Bilgi Sistemi ve TV vasıtasıyla Kanun'a yönelik bilgi edindikleri anlaşılmaktadır. Genel olarak öğrencilerin interaktif ortam

iletişimlerininin daha fazla olmasının yeniliklerle bu platformlar aracılığı ile daha yoğun haberdar olmalarını etkilediği düşünülmektedir.

Tablo 5: Kişisel Verileri Toplayan Kurumların Toplanan Verileri Doğru Bir Şekilde Koruyup Korumadığı Düşüncesi

	Evet		**Hayır**		**Kararsızım**	
Kurumlar	**f**	**%**	**f**	**%**	**f**	**%**
Özel Şirketler	31	20,5	**71**	**47,0**	50	33,1
Yerel Yönetimler	39	25,8	58	38,4	54	35,7
Kamu Kurumları	**51**	**33,7**	40	26,4	**60**	**39,7**
Polis	**64**	**42,3**	41	27,1	46	30,4
Doğrudan Pazarlama Şirketleri	0	0	**112**	**74,1**	39	25,8
Sigorta Şirketleri	30	19,8	61	40,3	**60**	**39,7**
Bankalar	**52**	**34,4**	39	25,8	**60**	**39,7**
Telekomünikasyon operatörleri	18	11,9	**92**	**60,9**	41	27,1
Sağlık Kurumları	40	26,4	42	27,8	**69**	**45,8**

Kişisel verileri toplayan ve tabloda listelenen kurumlarda, verilerin doğru bir şekilde korunup korunmadığı düşüncesini analiz eden Tablo 5'e göre öğrencilerin üçte ikisinden fazlasının (112 öğrenci, %74,1) en az oranda doğrudan pazarlama şirketlerinin kişisel verileri koruyamadıklarını düşündükleri anlaşılmaktadır. Öğrencilerin yarıdan fazlası (92 öğrenci, %60,9) telekomünikasyon operatörlerinin toplanan kişisel verilerini doğru bir şekilde korumadıklarını düşündüklerini belirtmişlerdir. Tablo 5'e göre öğrenciler en fazla (64 öğrenci, % 42, 3) polis tarafından toplanan kişisel verilerinin doğru bir şekilde korunduğunu düşünmektedir. Katılımcılar ikinci sırada (52 öğrenci, %34,4) bankaların verilerini doğru koruduğunu düşünürken, üçüncü sırada ise kamu kurumlarının (51 öğrenci, %33,7) kişisel verilerini doğru koruduğunu düşündüklerini belirtmişlerdir. Tabloya göre öğrencilerin belirtilen kurumların kişisel verileri doğru bir şekilde koruyup korumadığına yönelik düşünceleri analiz edildiğinde, bilmiyorum diyenlerin oranlarının genel olarak öğrencilerin üçte birinden fazla olması dikkati çekmektedir. Öğrenciler kamu kurumları (51 öğrenci, %33,7) ve bankaların (52 öğrenci, %34,4) üçte birden fazla oranda kişisel verileri koruduklarını düşünmelerine rağmen, aynı başlıklarda kararsız öğrencilerin de üçte birden fazla olması (60 öğrenci, %39,7) olması çarpıcıdır. Tabloya göre öğrencilerin en fazla (69 öğrenci, % 45,8) sağlık kurumlarında tutulan kişisel verilerin doğru bir şekilde korunup korunmadığına yönelik belirsizler yaşadıkları anlaşılmaktadır.

Tablo 6: Kişisel Ayrıntıları Soran Formları veya Uygulamaları Doldururken, Genellikle Bu Durumlar Karşısında Nasıl Davranıldığı Durumu

Durumlar	**Fikrim yok**		**Kişisel veri paylaşmam**		**Kişisel verilerimi boş bırakırım ya da yanlış bilgi veririm**		**Sorulan her bilgiyi veririm**	
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**
Firma üyelik kartlarına başvururken	11	7,2	**40**	**26,4**	**55**	**36,4**	45	29,8
Tapu İşlemleri	12	7,9	2	1.3	0	0	**137**	**90,7**
Ürünlerin ücretsiz deneme sürümlerini denerken	8	5,2	**50**	**33,1**	**54**	**35,7**	39	25,8
Fikir Anketleri	1	0,6	**90**	**59,6**	**30**	**19,8**	30	19,8
İşvereninizin istediği bilgileri doldururken	1	0,6	7	4,6	3	1,9	**140**	**92,7**
Kamu hizmetleri için başvururken (elektrik, gaz vs.)	2	1,3	0	0	0	0	**149**	**98,6**
Banka hizmetleri	4	2,6	2	1,3	1	0,6	**144**	**95,3**
Sigorta hizmetleri	**40**	**26,4**	15	9,9	0	0	96	63,5
Mobil İletişim Sağlayıcıları	7	4,6	33	21,8	8	5,2	115	76,1
Spor kulübü üyeliği	**15**	**9,9**	16	10,5	**30**	**19,8**	90	59,6
Eğitim kurumları	0	0	0	0	15	9,9	136	90,0

Tablo 6'ya göre, kişisel ayrıntıları soran formları veya uygulamaları doldururken, öğrencilerin neredeyse tamamına yakın bir kısmının (149 öğrenci, %98,6) kamu hizmetleri için başvuru esnasında (elektrik, gaz vs.) kişisel verilerini paylaştıkları anlaşılmaktadır. Öğrenciler daha sonra sırasıyla banka hizmetleri (144 öğrenci, %95,3), işvereninizin istediği bilgileri doldururken (140 öğrenci, %92) ve tapu işlemleri gibi (137 öğrenci, 90,7) süreçlerde kişisel verilerini paylaşabileceklerini belirtmektedir. Bu durum öğrencilerin genel olarak resmi işlemlerde kişisel verilerini paylaşma eğiliminde olduklarına işaret edebilmektedir. Diğer yandan, öğrencilerin en az fikir anketlerini doldururken (90 öğrenci, %59,6) ve ürünlerin ücretsiz deneme sürümlerini denerken (50 öğrenci ,%33,1) kişisel verilerini vermekten kaçındıkları anlaşılmaktadır. Bunun yanı sıra öğrencilerin ankette yer alan durumlarda kişisel verilerini boş bırakma veya yanlış veri verme seçeneği incelendiğinde, en fazla firma üyelik kartlarına başvururken ve ürünlerin ücretsiz deneme sürümlerini denerken (109 öğrenci, %72,1) kişisel verileri boş bıraktıkları veya yanlış veri verdikleri görülmektedir.

Tablo 7: Kişisel verilerinizi soran birileri tarafından telefonda aranma durumu

		Evet	Hayır
Aranma durumu	**f**	120	31
	%	79,4	20,6
Arayan kişinin kendini tanıtması (N=120)	**f**	90	30
	%	74,3	25,7

Tablo 7'ye göre öğrencilerin üçte ikisinden fazlası (120 öğrenci, %79,4) kişisel verilerini soran birileri tarafından telefonda aranmıştır. Bunun yanı sıra aranan öğrencilerin üçte ikisinden fazlasının (90 öğrenci, %74,3) arayan kişi tarafından kim olduğuna dair bilgilendirildiği anlaşılmaktadır. Genel olarak kişisel verilerin istenme durumunun yüksek olması bu verileri kullanan platformların yoğunluğunun artmasına işaret etmekle birlikte söz konusu verilerin korunmasının da önemini ortaya çıkarmaktadır.

Tablo 8. Arayan Kişiyle Kişisel Verilerin Paylaşılma Durumu (N=120)

Kişisel veri paylaşımı	**f**	**%**
Evet	60	50
Hatırlamıyorum	4	3,4
Hayır	6	5,0
Kısmen paylaştım	50	41,6

Tablo 7'de gösterilenvekişisel verilerini soran birileriyle telefonda görüştüğünü belirten öğrencilerin, (120 öğrenci, %79,4) arayan kişiyle kişisel verilerini paylaşma durumu değerlendirildiğinde (Tablo 8), öğrencilerin neredeyse tamamının kişisel verilerini tamamen veya kısmen arayan kişiyle paylaştıkları anlaşılmaktadır (110 öğrenci, %91,6). Diğer yandan arayan kişiyle kişisel verilerini paylaşmadığını söyleyen 6 öğrenci (%5,0) bulunmaktadır. Tablo verileri Tablo 7 ile birlikte değerlendirildiğinde kişisel verilerin istenme durumu karşılığında öğrencilerin kişisel verilerin paylaşımına yönelik bilgilendirilmelerinin önemi anlaşılabilmektedir.

Tablo 9: Kişisel Verileri Nasıl Korudukları veya Kullandıkları Konusunda Kuruluşlara ve Oluşumlara Güven Düzeyi (N=151)

Kuruluş ve uygulamalar	**Fikrim yok**		**Az güveniyorum**		**Orta seviyede güveniyorum**		**Güveniyorum**		**Çok güveniyorum**	
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**
Finansal kurumlar (bankalar vs.)	0	0	36	23,8	**65**	**43,04**	**40**	**26,4**	**10**	**6,6**
Sigorta şirketleri	**30**	**19,8**	60	39,7	41	27,1	5	3,3	5	3,3
Yardım kuruluşları	**40**	**26,4**	41	27,1	40	26,4	14	9,2	7	4,6
Merkezi yönetim	4	2,6	70	46,3	37	24,5	**37**	**24,5**	3	1,9
Yerel yönetimler	5	3,3	40	26,4	**60**	**39,7**	**40**	**26,4**	6	3,9
Kamu sağlığı hizmetleri	0	0	80	52,9	40	26,4	30	19,8	1	0,6
Özel sağlık hizmetleri (özel klinikler vs.)	1	0,6	70	46,3	50	33,1	21	13,9	**9**	**5,9**
Pazar araştırması kurumları	4	2,6	**95**	**62,9**	27	17,8	20	13,2	5	3,3
Online satıcılar	0	0	**100**	**66,2**	30	19,8	19	12,5	2	1,3
Sosyal medya platformları	0	0	**96**	**63,5**	42	27,8	10	6,6	3	1,9
Arama motorları	0	0	75	49,6	55	36,4	15	9,9	6	3,9
Telefonunuzdaki mobil uygulamalar (IOS ya da Android)	0	0	88	58,2	34	22,5	20	13,2	**9**	**5,9**
Kullandığınız e-posta servisleri	0	0	44	29,1	**66**	**43,7**	35	23,1	6	3,9
Kullandığınız web tarayıcısı (Chrome, Edge, Mozilla, Opera gibi)	0	0	71	47,1	50	33,1	10	6,6	10	6,6

Tablo 9'a göre kuruluşların ve oluşumların kişisel verileri nasıl korudukları veya kullandıkları konusundaki güven düzeyleri değerlendirildiğinde, öğrencilerin yarıdan fazlasının pazar araştırması kurumları (95 öğrenci, %62,9), çevrimiçi satıcılar (100 öğrenci, %66,2) ve sosyal medya platformlarına (96 öğrenci, %63,5) kişisel verilerin korunması ve kullanılmasına yönelik olarak az güvendikleri görülmektedir. Orta seviyede güvendikleri kuruluş ve oluşumlar değerlendirildiğinde ise kullandıkları e-posta servislerine katılımcıların yarıya yakın bir kısmının (66 öğrenci, %43,7) orta seviyede güvendikleri anlaşılmaktadır. Tablo genel olarak değerlendirildiğinde, öğrencilerin en fazla (115 öğrenci, %76,0) finansal kurumlara (banka vs.) orta seviye ve üzerinde güvendikleri görülmektedir. Öğrenciler daha sonra kullandıkları e-posta servislerine (107 öğrenci, %70,7) ve yerel yönetimlere (106 öğrenci, %70) orta seviye ve üzerinde güvendiklerini belirtmişlerdir.

Tablo 10: Kişiler veya organizasyonların Talep Ettikleri Kişisel Verilere Yönelik Bilgilendirme Metnini Dikkatlice Okuma Durumu

Okuma durumu	**f**	**%**
Bazen	41	27,1
Evet	44	29,1
Hayır	66	43,7

Öğrencilerin kişiler veya organizasyonların talep ettikleri kişisel verilere yönelik bilgilendirme metnini dikkatlice okuma durumuna yönelik elde edilen bulgular değerlendirildiğinde (Tablo 10) öğrencilerin yarıya yakın bir kısmının (66 öğrenci, %43,7) bilgilendirme metinlerini okumadıkları anlaşılmaktadır. Bazen okuduklarını bildiren öğrenci oranı yaklaşık üçte birdir (41 öğrenci, %27,1). Tabloya göre, bilgilendirme metinlerini okuduklarını söyleyen öğrencilerin oranı yaklaşık %30 olarak görülmektedir. Tablonun kişisel verilerin korunmasının önemli bir ayağı olan bilgilendirme metinlerinin okunmasının önemine yönelik farkındalık eksikliğini işaret edebileceği düşünülmektedir.

Tablo 11: Bilgilendirme Metnini Okurken Genellikle Karşılaşılan Zorluklar (N=151)

Zorluklar	**f**	**%**
Kişisel verilerimin nasıl işleneceğine dair bilgiler bulunmuyor	40	26,4
Şartlar okumak için oldukça uzun ve karmaşık	**140**	**92,7**
Şartların neler olduğunu anlayamıyorum	74	49,1
Yazılar okumak için çok küçük	**143**	**94,7**

Kişiler veya organizasyonların talep ettikleri kişisel verilere ilişkin bilgilendirme metnininin okunmasında karşılaşılan zorluklara yönelik elde edilen veriler değerlendirildiğinde (Tablo 11), öğrencilerin neredeyse tamamına yakın kısmının yazıların okumak için çok küçük (143 öğrenci, %94,7) ve şartların da oldukça uzun ve karmaşık olduğunu (140 öğrenci, %92,7) düşündükleri görülmektedir. Birden çok seçeneğin işaretlenebildiği soruda öğrencilerin yarıya yakın bir kısmının (74 öğrenci, %49,1) şartların neler olduğunu anlayamadıkları ortaya çıkmaktadır. Genel olarak tablodabilgilendirme metinlerinin yazım karakterlerinin ve dillerinin anlaşılmayı zorlaştırdığına yönelik ortaya çıkan bulguların, bu metinlerin düzenlenmesinde dikkat edilecek hususları yansıttığı düşünülmektedir.

Tablo 12: Kişisel Verilerinizi Toplayan Kurumların Sizin Bildiğiniz Amaçlar Dışında Kişisel Verilerinizi Kullanmasında Herhangi Bir Sakınca Görüyor Musunuz?

Sakınca görme durumu	**f**	**%**
Hayır	9	5,9
Kararsızım	52	34,5
Sakınca görüyorum	90	59,6
Toplam	**151**	**100,0**

Tablo 12'ye göre araştırmaya katılan öğrencilerin yarısından fazlası (90 öğrenci, %59,6) kişisel verilerini toplayan kurumların, kişisel verileri bilinen amaçlar dışında kullanmasında sakınca görmektedir. Diğer yandan konuya yönelik kararsız olduğunu söyleyen üçte bir oranında (52 öğrenci, %34,5) öğrenci bulunması dikkat çekmektedir. Bu durum öğrencilerin konu hakkındaki bilgi eksikliklerinin bir kanıtı olarak değerlendirilebilir.

Tablo 13: Olaylar Karşısında Kişisel Verilerinizin Kötüye Kullanıldığını Düşünme Durumu

Durumlar	**f**	**%**
Belirli bir amaç için bir işletmeye sunduğunuz verilerinizin işletmede başka bir amaçlar için de kullanılması	**50**	**33,1**
Bir işletmenin internet sayfalarında gezinirken bilginiz olmadan sitede bıraktığınız kişisel bilgilerinizi kaydetmesi	18	11,9
İlginiz olmayan bir firmanın kişisel verilerinizi ele geçirmesi	**60**	**39,7**
Yaptığınız işlemin amacını yansıtmayan bir kişisel verinizin talep edilmesi	23	15,2
Toplam	**151**	**100,0**

Belirlenen olaylar karşısında kişisel verilerinin kötüye kullanıldığını düşünme durumunu gösteren Tablo 13'e göre, öğrencilerin en fazla ilgileri olmayan bir firmanın kişisel verilerini ele geçirmesi durumunu kötüye kullanım olarak adlettikleri görülmektedir. İkinci sırada belirli bir amaç için bir işletmeye sunulan verilerin işletmede başka amaçlar için de kullanılması durumu (50 öğrenci, %33,1) öğrenciler tarafından kötüye kullanım olarak nitelenmektedir. Bunun yanı sıra, bir işletmenin internet sayfalarında gezinirken bilginiz olmadan sitede bırakılan kişisel bilgilerin kaydetmesi durumunun en az (18 öğrenci, %11,9) oranda kötüye kullanım olarak değerlendirmesi dikkat çekicidir. Bu durumun, farkında olmadan toplanan verilerin ikincil kullanımlarına yönelik bilgi eksikliğine işaret edebileceği değerlendirilmektedir.

Tablo 14: Web Servislerini Kullanırken Şifrenizi Ayarlama Durumu (N=151)

Şifre belirleme	**f**	**%**
Birçok sistemde kullandığım ortak parolalarımdan birini kullanırım.	140	92,7
Doğum günüm, telefon numaram, öğrenci numaram gibi kolay hatırlayabileceğim bir şifre oluştururum.	90	59,6
Şifreleme yazılımı kullanarak güvenliği yüksek (bit olarak) şifre üretirim.	7	4,6
Tahmini zor bir şifre belirlerim.	50	33,1

Araştırmaya katılan öğrencilerin web servislerini kullanırken şifrelerini nasıl ayarladıklarını gösteren Tablo14'e göre, öğrencilerin neredeyse tamamının (140 öğrenci, %92,7) birçok sistemde kullandığı ortak parolalarından birini tercih ettikleri anlaşılmaktadır. Araştırmaya katılanlardan sadece 7 öğrenci (%4,6) şifreleme yazılımı kullanarak, güvenliği yüksek (bit olarak) şifre üreterek web servislerini kullandıklarını belirtmiştir. Bunun yanı sıra katılımcıların yarıdan fazlasının (90 öğrenci, %59,6) doğum günü, telefon numarası, öğrenci numarası gibi kolay hatırlayabileceği verilerini bir şifre oluşturmak için kullanması dikkat çekmektedir. Bu durum öğrencilerin kişisel veri olarak sayabileceğimiz verilerini şifre olarak kullanma eğiliminde olduklarına işaret etmektedir.

Tablo 15: Akrabalarınızın ve Arkadaşlarınızın Kişisel Bilgilerini, Onların Rızası Olmadan Ücretsiz Servis veya Ürünler Kullanmak için Açıklar Mısınız?

Açıklama durumu	**f**	**%**
Emin değilim	46	30,5
Evet	5	3,3
Hayır	100	66,2
Toplam	**151**	**100,0**

Tablo 15'e göre öğrencilerin üçte ikisine yakın bir kısmının (100 öğrenci, %66,2), akrabalarının ve arkadaşların kişisel bilgilerini, onların rızası olmadan ücretsiz servis veya ürünler kullanmak için

açıklamayacaklarını ifade ettikleri görülmektedir. Diğer yandan, konuya yönelik emin olmadığını belirten öğrenci oranı yaklaşık üçte birdir (46 öğrenci, %30,4). Akrabalarının ve arkadaşların kişisel bilgilerini, onların rızası olmadan ücretsiz servis veya ürünler kullanmak için açıklayabileceğini söyleyen öğrenci sayısı ise sadece 5 (%3,3)'dir.

Tablo 16: Belirtilen Kişisel Verilerin Blog, Sosyal Ağ Sitesi veya Kişisel Web Sitesinde Paylaşılma Durumu

	Cevaplamak istemiyorum		**Evet, Paylaştım**		**Hayır, Paylaşmadım**	
Kurumlar	**f**	**%**	**f**	**%**	**f**	**%**
Gerçek isim	5	3,3	**141**	**93,3**	5	3,3
Telefon	0	0	90	59,6	61	40,3
Fotoğraf ve videolar	0	0	**148**	**98,6**	13	8,6
İş yeri ismi	1	0,6	10	6,6	**140**	**92,7**
Okuduğunuz okul	0	0	**150**	**99,3**	1	0,6
Yaşadığınız şehir	1	0,6	138	91,3	12	7,9
Ev adresiniz	1	0,6	18	11,9	**132**	**87,4**
Plakanız	0	0	0	0	**151**	**100**
e-mail	20	13,2	110	72,8	21	13,9
Doğum tarihi	0	0	93	61,5	58	38,4
Eğitim bilgileriniz	0	0	128	84,7	23	15,2
Sevdiğiniz müzik	15	9,9	70	46,3	66	43,7
İlişki durumunuz	8	5,2	46	30,4	97	64,2
Politik görüşünüz	19	12,5	70	46,3	62	41,0

Öğrencilerin blogları, sosyal ağ siteleri veya kişisel web sitelerinde kişisel verilerini paylaşma durumunu gösteren Tablo 16'ya göre katılımcı öğrencilerin söz konusu ortamlarda en fazla okudukları okulu (150 öğrenci, %99,3), daha sonra fotoğraf ve videolarını (148 öğrenci, %98,6) ve gerçek isimlerini (141 öğrenci, % 93,3) ve paylaştıklarını belirttikleri anlaşılmaktadır. Buun yanı sıra tabloya göre öğrencilerin hiç birinin plakalarını söz konusu ortamlarda paylaşmadıkları anlaşılırken iş yeri isimleri (140 öğrenci, 92,7) ve ev adreslerini de (132 öğrenci, %87,4) yüksek oranlarda paylaşmadıkları anlaşılmaktadır. Genel olarak tabloda kimlikleri açık edebilecek kişisel verilerin paylaşımının varlığı görülmektedir.

Tablo 17: İnternette Yayınlanan Kişisel Veriler Nedeniyle Yabancılarla İletişim Kurma Durumu

İletişim kurma durumu	**f**	**%**
Emin değilim	18	11,9
Evet	75	49,6
Hayır	58	38,5
Toplam	**151**	**100,0**

Araştırmaya katılan öğrencilere internette yayınlanan kişisel verilerinin yabancılarla iletişim kurmalarına sebep olup olmadığı sorusu yöneltiğinde, öğrencilerin yaklaşık yarısı (75 öğrenci, %49,4) yayınlanan verilerinin yabancılarla iletişim kurmalarına neden olduğunu belirtmişlerdir. Bu durumun yabancılarla iletişim kurmalarına neden olmadığını söyleyen 58 öğrenci (%38, 5) bulunmaktadır. Yabancılarla kurdukları iletişime bu durumun neden olup olmadığına emin olmayan 18 öğrenci (%11, 9) bulunmaktadır. Bulgular öğrencilerin internette paylaşılan verileri ile birlikte değerlendirildiğinde (Tablo 16) kişisel verilerin paylaşılmasının istenmeyen iletişimlere sebebiyet verebileceğini düşündürmektedir.

Tablo 18. Kişisel Veriler İnternette Paylaşıldığında İnsanların Bunu Görüntüleyecek Olmasından Endişelenme Durumu

Endişe durumu	**f**	**%**
Az endişelenirim	45	29,7
Evet, endişelenirim	71	47,0
Hayır endişelenmem	35	23,3
Toplam	**151**	**100,0**

Araştırmaya katılan öğrencilerin, kişisel verileri internette paylaşıldığında pek çok insanın bunu görüntüleyecek olmasından endişelenme durumunu gösteren Tablo 18' göre, katılımcıların yarıya yakın bir kısmının (71 öğrenci, %47,0) bu durumdan endişeleceğini bildirdiği görülmektedir. Diğer yandan öğrencilerin yaklaşık yüzde otuzu (45 öğrenci) bu durumdan az endişeleneceklerini belirtirken, 35öğrencinin ise (%23,1) bu durumdan endişelenmeyeceklerini bildirdikleri görülektedir.

Tablo 19: Arkadaşlardan Birinin, İzniniz Olmadan, Size Ait Fotoğraf veya Videolarınızı Yüklediğinde Hissiyat

Hissiyat	**f**	**%**
Benim için bir sorun teşkil etmez	15	9,9
Bilmiyorum	10	6,7
Güvendiğim bir arkadaşımın paylaşımı ise bir sorun teşkil etmez	**70**	**46,3**
Kişisel verilerime saygı duyulmadığını hissederim	45	29,8
Mahremiyetimin ihlal edildiğini düşünürüm	11	7,3
Toplam	**151**	**100,0**

Tablo 19'a göre öğrencilerin yaklaşık yarıya yakın bir oranının (70 öğrenci, %46,3), arkadaşlarından birinin, kendisinin izni olmadan, fotoğraf veya videolarını paylaştığında, güvendiği bir arkadaşı ise bu durumun bir sorun teşkil etmeyeceğini söylediği görümektedir. Söz konusu duruma yönelik sorun teşkil etmediğini veya bilmediğini söyleyen 25 öğrenci (%16,5) bulunmaktadır. Bunun yanı sıra, nitelenen durum karşısında kişisel verilerine saygı duyulmadığını hissedeceğini söyleyen yaklaşık üçte bir oranında öğrenci (45 öğrenci, %29,8) bulunmaktadır. Bu durumun mahremiyetini ihlal edeceğini düşünen öğrencilerin azlığı (11 öğrenci, %7,2) dikkati çekmektedir. Söz konusu verinin kişisel verilerle mahremiyet arasındaki bağlatının farkındalığına yönelik bir sorunu işaret edebileceği değerlendirilmektedir.

Tablo 20. Kişisel Verileri Korumak için İnternet Güvenliği/ Gizlilik Ayarı Önlemi Alınma Durumu

Önlem alınma	f	%
Bu ayarların nasıl yapılacağını bilmiyorum	50	33,2
Evet	80	52,9
Hayır	21	13,9
Toplam	**151**	**100,0**

Araştırmaya katılan öğrencilerin kişisel verilerini korumak için internet güvenliği/gizlilik ayarı önlemi alma durumunu yansıtan Tablo 20'ye göre, öğrencilerin yarısından fazlasının (80 öğrenci, %52,9) güvenlik ve gizlilik ayarlarının yapılmasına yönelik önlemlerini aldıkları anlaşılmaktadır. Bunun yanı sıra öğrencilerin üçte birlik bir kısmının (50 öğrenci, %33,1) bu ayarların nasıl yapılacağına yönelik bilgi eksikliklerinin olduğu görülmektedir. Söz konusu ayarları yapmadığını söyleyen ise 21 öğrenci bulunmaktadır (%13).

Tablo 21. Kişisel Verilerin ve/ veya Kişisel Bilgilerin Korunması için Geçerli Olan Yasa, Kural, İlke, Rehber veya Diğer Düzenlemelerden Haberdar Olma Durumu

Haberdarlık	f	%
Evet	45	29,8
Hayır	75	49,6
Kısmen	31	20,6
Toplam	**151**	**100,0**

Araştırmaya katılan öğrencilerin kişisel verilerin ve/veya kişisel bilgilerin korunması için geçerli olan yasa, kural, ilke, rehber veya diğer düzenlemelerden haberdar olma durumunu gösteren Tablo 21'e göre, katılımcıların yarıya yakınının bu düzenlemelerden haberdar olmadıkları görülmektedir (75 öğrenci, %49,6). Düzenlemelerden ve kanunlardan kısmen haberdar olduğunu belirten öğlenciler ise %20,6 oranında görülmektedir. Öğrencilerin yaklaşık üçte biri (45 öğrenci, %29,8) düzenlemelerden haberdar olduklarını belirtmektedir. Genel olarak tablo kişisel verilerin korunmasına yönelik yasal çerçeve kapsamında öğrencilerin bilgi eksikliğini düşündürmektedir. Konuyla ilgili düzenlemelerden haberdar olduğunu belirten öğrencilerin oranının düşük olması konu ile ilgili farkındalıklarına yönelik de bilgi vermektedir.

Tablo 22: Kişisel Verilerin Geçmişte Kötüye Kullanılması

Kötü kullanım	f	%
Bilmiyorum	45	29,8
Evet	38	25,1
Hayır	68	45,0
Toplam	**151**	**100,0**

Tablo 22'ye göre, araştırmaya katılan öğrencilere kişisel verilerinin geçmişte kötüye kullanıp kullanılmadığı sorulduğunda, %25,1'inin (38 öğrenci) kişisel verlerinin geçmişte kötüye kullanıldığını belirttiği görülmektedir. Bunun yanı sıra öğrencilerin yaklaşık yarısını (68 öğrenci, %45,0) kişisel verilerinin geçmişte kötüye kullanılmadığını ifade etmiştir. Kişisel verilerinin geçmişte kötüye kullanılıp kullanılmadığını bilmediğini söyleyen öğrencilerin oranı ise yaklaşık %30'dur.

Kişisel verileri geçmişte kötüye kullanılan katılımcılara (38 öğrenci) konuyla ilgili şikâyette bulunup bulunmadıkları sorulduğunda, öğrencilerin yarısından fazlası (26 öğrenci, %68,6) konuya yönelik şikâyette bulunmadıklarını belirtmiştir. Şikâyette bulunan dokuz öğrenci (%23,6) bulunmaktadır. Diğer

seçeneğini işaretleyenler değerlendirildiğinde (3 öğrenci, %7,8), kişisel verilerini kötüye kullandıklarını düşündükleri kişi veya sayfalara kendilerinin uyarıda bulundukları yorumlanmıştır.

Şikâyette bulunan katılımcı öğrencilerin (9 öğrenci) şikâyetlerinin sonucunun ne olduğu sorulduğunda, 4 öğrenci (%44,5) işlemlerinin hala devam ettiğini belirtmiştir. 2 öğrenci konuya yönelik bir sonuç alamadığını belirtirken, yine 2 öğrenci daha konuya yönelik tatmin edici bir sonuç alamadıklarını belirtmişlerdir (%44,4). Şikâyet sonucunda tatmin edici bir sonuç aldığını söyleyen yalnız 1 öğrenci bulunmaktadır (%11,1).

Tablo 23: Kişisel Verileriniz Geçmişte Kötüye Kullanıldıysa ve Bir Şikâyette Bulunmadıysanız, Bunun Sebebi Nedir? (N=29)

Sebepler	**f**	**%**
Bunun önemsenecek bir konu olduğunu düşünmedim	8	27,5
Nasıl şikâyet edileceğini bilmiyordum	10	34,4
Nereye şikâyet edeceğimi bilmiyordum	9	31,0
Zamanım yoktu	2	6,8

Tablo 23'e göre, kişisel verileri geçmişte kötüye kullanılan ve bir şikâyette bulunmayan katılımcı öğrencilerin yaklaşık üçte birinin (8 öğrenci, %27,5), bunun önemsenecek bir konu olduğunu düşünmedikleri ve bu sebeple şikâyette bulunmadıkları görülmektedir. Katılımcılardan 10 tanesinin (%34,4) nasıl şikâyette bulunacaklarını bilmemeleri sebebiyle, dokuz tanesinin ise (%31,0) nereye şikâyet edeceklerini bilmeme sebebiyle şikâyette bulunmadıkları görülmektedir. Zamanı olmadığı için şikâyette bulunmadıklarını belirten iki öğrenci bulunmaktadır (%6,8).

Tablo 24: Kişisel Verileriniz İleride Kötüye Kullanılırsa, Şikâyette Bulunacak mısınız?

İleride şikâyette bulunma	**f**	**%**
Adaletin işlediğini görmek için şikâyette bulunurum	25	16,5
Hakkımı savunmak adına şikâyette bulunurum.	19	12,5
Karşı tarafa bir ders vermek amacıyla şikâyette bulunurum	15	9,9
Karşı tarafın davranışlarını değiştirebilmek amacıyla şikâyette bulunurum	**46**	**30,4**
Kaybımın tazminatı için şikâyette bulunurum	**36**	**23,8**
Resmi bir özür elde etmek için şikâyette bulunurum	10	6,6
Toplam	**151**	**100,0**

Tablo 24'e göre, öğrenciler ileride kişisel verileri kötüye kullanılırsa en fazla karşı tarafın davranışlarını değiştirebilmek amacıyla şikâyette bunabileceklerini (46 öğrenci, %30) belirtmektedir. Duruma ilişkin listenin ikinci sırasında kayıpların tazminatı için şikâyette bulunma (36 öğrenci, %23,8) gerekçesi yer almaktadır. Adaletin işlediğini görmek için şikâyette bulunacaklarını belirten %16,5 oranında (25 öğrenci) katılımcı bulunmaktadır. Öğrenciler en az (10 öğrenci, %6,6) resmi bir özür elde etmek için şikâyette bulunacaklarını belirtmektedir.

Tablo 25: Kişisel Verileriniz Gelecekte Kötüye Kullanılırsa ve Bir Şikâyette Bulunmazsanız, Bunun Nedeni Ne Olabilir?

Nedenler	**f**	**%**
Adaletin işleyeceğinden şüphe duymam	11	7,2
Dikkate alınacağını sanmıyorum	20	13,2
Kişisel verilerimi kötüye kullanan kişi bir psikopat olabileceğinden önce kendimi ve ailemi savcılık, polis yardımıyla koruma altına almam gerek. Kişisel verilerimin kötüye kullanımı için şikâyette bulunmak bundan sonra gelir.	**30**	**19,8**
Nasıl başvuracağını bilememe	**42**	**27,8**
Nereye başvuracağını bilememe	**30**	**19,8**
Önemli bir konu olduğunu düşünmediğimden	13	8,6
Zaman yetersizliği	5	3,3
Toplam	**151**	**100,0**

Araştırmaya katılan öğrencilerin, kişisel verilerinin gelecekte kötüye kullanılması durumunda eğer şikâyette bulunmazlarsa bunun nedeninin ne olabileceğine yönelik yanıtlarını içeren Tablo 25'e göre, öğrencilerin en fazla nasıl başvuracaklarını bilememekten dolayı şikâyet etmeyeceklerini söyledikleri görülmektedir (42 öğrenci, %27,8). Öğrenciler ayrıca yaklaşık %20 oranında nereye başvuracağını bilememe nedeninden dolayı şikâyette bulunmayacaklarını bildirmiştir. Bunun yanı sıra, aynı oranda öğrencinin (30 öğrenci, %19,8) "Kişisel verilerimi kötüye kullanan kişi bir psikopat da olabileceğinden önce kendimi ve ailemi savcılık, polis yardımıyla koruma altına almam gerek. Kişisel verilerimin kötüye kullanımı için şikâyette bulunmak bundan sonra gelir" şıkkında belirtilen nedenden dolayı şikâyette bulunmayacaklarını belirttikleri görülmektedir. Tabloya göre öğrenciler en az oranda (5 öğrenci, %3,3) "Zaman yetersizliği" dolayısıyla bu konuda şikâyette bulunmayacaklarını belirtmiştir. Genel olarak tablo bulgularının öğrencilerin kişisel verilerinin kötüye kullanılması durumunda nereye ve nasıl başvuracaklarını bilmemelerinden dolayı şikayette bulunmamalarının, konuyla ilgili bireysel hakların tanıtımında eksikliğe işaret ettiği düşünülmektedir.

Tablo 26: Kişisel Verileriniz Kötüye Kullanıldıysa ve Şikâyette Bulunmak İsterseniz, Kime veya Hangi Kuruma Şikâyet Edersiniz?

Kurum ve kişiler	**f**	**%**
Polis	**69**	**45,6**
Kişisel Verileri Koruma Kurulu	**48**	**31,7**
Cumhuriyet savcılığı	**26**	**17,4**
Veri sahipleri	7	4,6
Bilmiyorum	1	0,66
Toplam	**151**	**100,0**

Tablo 26, öğrencilerin kişisel verilerinin kötüye kullanılması durumunda başvuracakları kişi veya kurumları göstemektedir. Buna göre öğrencilerin en fazla (69 öğrenci, %45,6) söz konusu durumda polise başvuracakları anlaşılmaktadır. Öğrenciler ikinci sırada Kişisel Verileri Koruma Kuruluna (48 öğrenci, %31,7) başvuracaklarını belirtirken, üçüncü sırada ise (26 öğrenci, %17,4) Cumhuriyet Savcılığı bulunmaktadır. Kişisel verilerin kötüye kullanımı durumunda öğrencilerin daha çok kolluk kuvvetlerden destek almaya çalışmalarının konu kapsamındaki sorumlu birim ve kurumlar ile ilgili bilgi ve tanıtım eksikliğine işaret ettiği düşünülmektedir.

Sonuç ve Öneriler

Elektronik cihazların her alanda yoğun olarak kullanıldığı günümüzde, her türlü kişisel veri anlık olarak depolanmakta ve paylaşılmaktadır. İnternetin hayatımızın vazgeçilmez bir parçası olması bir yandan hayatımıza kolaylık sağlarken, diğer yandan da kişisel verilerimize istenmeyen yetkisiz erişimlerinin artmasına sebep olmaktadır. Kişisel verilerin dijital ortamdan gelen tehditlere ve saldırılara karşı korunması, kişisel verilerin gizliliği ve mahremiyetine yönelik farkındalığın gelişmesi, bilgi güvenliği konusunun da önemli bir ayağını oluşturmaktadır. Bu bağlamda konuya yönelik araştırmada elde edilen bulgular çerçevesinde sonuçlar değerlendirildiğinde; öğrencilerin büyük oranda kişisel verilerin ne olduğunu bildiklerini düşünmelerine rağmen, konu ayrıntılandırıldığında kişisel verilerin net ayrımlarla tanımlanması konusunda yetersiz oldukları anlaşılmaktadır. Öğrencilerin genel olarak kişilerin kimlik bilgileri, ad, soyadı, ev adresi, kredi kartı bilgileri ile kişisel verileri eşleştirdikleri görülürken, özel nitelikli kişisel verilere yönelik tanımlamalarda sıkıntılar yaşadıkları anlaşılmaktadır. Bunun yanı sıra, kişisel verilerin korunması hakkı ve özel hayatın gizliliği gibi hakların bilinme durumunu değerlendirildiğinde, öğrencilerin konuya yönelik bilgilerinin yetersiz seviyede olduğu tespit edilmiştir. Bulgulara göre öğrenciler genel olarak kişisel verilerin korunması hakkı ve özel hayatın gizliliği gibi haklardan haberdar olma eğiliminde olsalar da konu kapsamında ayrıntı ve yeterli bilgilerinin olmadığı ortaya çıkmaktadır. Daha özel anlamda, öğrencilerin kişisel verilere yönelik kullanılan temel yasa olan 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndan haberdar olma durumu değerlendirildiğinde, Kanun'un genel olarak bilinmediği veya sadece ismen bilindiği ortaya çıkmaktadır. Öğrencilerin söz konusu Kanun'dan en fazla internet yoluyla haberdar oldukları anlaşılırken, ikinci olarak ise dersler vasıtası ile haberdar oldukları ortaya çıkmaktadır. Bu sonuçla birlikte özellikle genç kuşağın etkin kullandığı bir platform olan internet vasıtasıyla kişisel verilere yönelik bilgilendirme yapılabileceği öngörülmektedir.

Araştırma bulgularına göre, öğrenciler kişisel verilerini toplayan kurumların, bildikleri amaçlar dışında bilgilerini kullanmasında sakınca görmektedirler. Diğer yandan konuya yönelik kararsız olduklarını söyleyen yaklaşık üçte bir oranında öğrenci olması, katılımcıların kişisel verilerin mahremiyeti ve gizliliğine yönelik algılarının güçlendirilmesi gerektiğini düşündürmektedir. Bu durumun aynı zamanda öğrencilerin konu kapsamında bilgi eksikliklerine işaret ettiği değerlendirilmektedir. Araştırmada öğrencilerin olaylar karşısında kişisel verilerinin kötüye kullanıldığını düşünme durumuna yönelik bulgular değerlendirildiğinde; genel olarak öğrencilerin ilgileri olmayan bir firmanın kişisel verilerini ele geçirmesi, belirli bir amaç için bir işletmeye sunulan verilerin işletmede başka amaçlar için de kullanılması gibi açık durumları verilerinin kötüye kullanımı olarak değerlendirdikleri sonucu çıkmıştır. Diğer yandan, bulgular öğrencilerin bireylerin farkında olmadan toplanan verilerine yönelik (örneğin bir internet sitesinde gezinirken) verilerinin toplanması durumu daha az oranda kötü kullanım olarak değerlendirdikleri görülmüştür. Söz konusu sonuç öğrencilerin farkında olmadan toplanan verilerin ikincil kullanımına yönelik bilgi eksikliğine işaret etmektedir. Sonuçlar öğrencilerin büyük oranda akrabalarının ve arkadaşlarının kişisel bilgilerini, onların rızası olmadan açıklamama eğiliminde olduklarını göstermektedir. Bunun yanı sıra katılımcıların arkadaşlarından birinin, izinleri olmadan, onlara ait fotoğraf veya videolarını paylaşması durumunu güvendikleri bir arkadaşları yaptığında sorun olarak algımayacaklarını düşünmeleri dikkat çekicidir. Belirtilen durumun kişisel verilere saygısızlık olduğunu düşünen öğrencilerin oranı yaklaşık üçte bir düzeyindedir. Bu durumun mahremiyet ihlali olduğunu düşünen oldukça az sayıda öğrencinin olmasının, öğrencilerin mahremiyet-kişisel veriler ve tanıdıklar arasındaki ilişki kurmalarında bir sorun olduğuna işaret ettiği düşünülmektedir. Diğer yandan, aynı öğrencilerin kişisel verilerinin internette paylaşılması ve pek çok insanın bunu görüntüleyecek olmasından çoğunlukla endişe duyacaklarını belirtmesi, katılımcıların konuyla ilgili algılarında farklılıklar olduğunu ortaya koymaktadır.

Sonuçlara göre, öğrenciler web servislerini kullanırken yüksek oranlarda birçok sistemde kullandıkları ortak parolalarından birini kullanmaktadırlar. Bu şifrelerin içerikleri genellikle doğum günü, telefon numarası, öğrenci numarası gibi kolay hatırlanabilecek şifre kodlarından oluşmaktadır. Bu durum kişisel verilerin mahremiyeti ve gizliliğine yönelik korunmanın önemini daha da açığa çıkarmaktadır. Araştıma sonuçlarına göre tahmini zor şifreler veya şifreleme yazılımları kullanan öğrencilerin sayıları azınlıktadır. Bu sonuçlar öğrencilerin bloglarında, sosyal ağ sitelerinde veya kişisel web sayfalarında

paylaştıklarını belirttikleri kişisel veriler ile birlikte değerlendirildiğinde anlamlanmaktadır. Söz konusu platformlarda açığa çıkarılan kişisel veriler vasıtası ile katılımcıların birçok şifresinin tahmin edilebilirliğinin yükseleceği anlaşılmaktadır. Bulgulara göre öğrencilerin gerçek isim, fotoğraflar videolar, yaşadıkları şehir, okudukları okul, telefon, e-mail, eğitim bilgileri, doğum tarihi vb. gibi kişisel verilerini özellikle sosyal medya platformlarında yoğun olarak paylaştıkları sonucu çıkmaktadır. Bu durumun kişisel verilerin korunmasına yönelik zaafiyet durumunu içerdiği düşünülmektedir. Nitekim internette yayınladıkları kişisel verileri vasıtasıyla öğrencilerin yarısının yabancı kişiler ile istenmeyen iletişim durumu ile karşılaştıkları ortaya çıkmıştır. Bu bağlamda çevrimiçi ortamlarda mahremiyet ve gizliliğe yönelik bilgilendirmelerin gerekli olduğu ortaya çıkmaktadır.

Araştırmada öğrencilerin yarısının kişisel verilerini korumak için internet güvenliği/gizlilik ayarı önlemi aldıkları görülürken, bu ayarları yapmayan ve nasıl yapılacağını bilmeyen öğrencilerin de aynı oranda olması dikkat çekicidir. Bu durum konuya yönelik bilgilendirme gerekliliklerini ortaya koymaktadır. Kişisel verilerin korunmasına yönelik önemli konulardan bir tanesi de bilgilendirme metinleridir. Bu bağlamda araştırmamızda ortaya çıkan sonuçlara göre öğrencilerin çoğunlukla kişiler veya organizasyonların talep ettikleri kişisel verilere yönelik bilgilendirme metnini dikkatlice okumadıkları veya bazen okudukları sonucu ortaya çıkmıştır. Söz konusu bilgilendirme metnini okurken genellikle karşılaşılan zorlukların başında, yazıların okumak için çok küçük ve şartların okumak için oldukça uzun ve karmaşık olması yer almaktadır.

Elde edilen sonuçlara göre, öğrencilerin kişisel ayrıntıları soran formları veya uygulamaları doldururken, genellikle söz konusu durum kamu hizmetleri, bankka hizmetleri için başvurmak ise kişisel verilerini verdikleri anlaşılmaktadır. Diğer yandan sonuçlarda öğrencilerin fikir anketleri doldururken veya ürünlerin ücretsiz deneme sürümlerini denerken kişisel verilerini vermekten kaçındıkları veya yanlış bilgilendirme yapabildikleri de ortaya çıkmaktadır. Bu durum farklı korunma stratejilerinin varlığına işaret etmektedir.

Araştırma sonuçlarında öğrencilerin, kişisel verileri toplayan kurumlar arasından en az doğrudan pazarlama şirketlerinin kişisel verilerini koruduklarını düşündükleri ortaya çıkmaktadır. En fazla ise emniyet kurumları ve bankaların kişisel verilerini koruduklarını düşündükleri ortaya çıkmıştır. Söz konusu duruma yönelik kamu kurumları, sağlık kurumları gibi organizasyonlara karşı kararsız oldukları dikkati çekmektedir. Bu durumun son zamanlarda kamu kurumlarının ve sağlık kurumlarının kişisel verilere yönelik ihlal haberleriyle ilintili olabileceği düşünülmektedir. Bu sonuçlara ilaveten öğrencilerin kuruluşların ve oluşumların kişisel verileri nasıl koruduklarını veya kullandıkları konusunda güven düzeyi değerlendirildiğinde; öğrencilerin pazar araştırması kurumları, online satıcılar ve sosyal medya platformlarına az güvendikleri görülmektedir. Öğrenciler finansal kurumlara (banka vs.), kullandıkları e-posta servislerine ve yerel yönetimlere ise daha fazla güvenmektedirler.

Öğrencilerin çoğunluğunun geçmişte kişisel verilerinin kötüye kullanılmadığı sonucu ortaya çıkmıştır. Diğer yandan, geçmişte kişisel verilerinin kötüye kullanıldığını ve henüz bu durumun olup olmadığını bilmediğini söyleyen öğrenciler beraber değerlendirildinde, kişisel verilerin kötüye kullanımının da yüksek miktarlarda olabileceği sonucu anlaşılmaktadır. Sonuçlara göre; kişisel verileri geçmişte kötüye kullanılan öğrencilerin yüksek oranda konuya yönelik şikâyette bulunmadıkları görülmektedir. Öğrencilerin konuya yönelik şikâyette bulunmama gerekçelerine yönelik bulgular değerlendirildiğinde ise nasıl ve nereye şikâyet edeceklerini bilmeme konusunda sıkıntı yaşadıkları sonucu ortaya çıkmıştır.

Gelecekte olası bir kötüye kullanım durumunda şikâyette bulunmama nedenlerinin ne olabileceği kapsamında elde edilen sonuçlara göre, daha önceki sonuçlarla paralel bir şekilde nasıl ve nereye başvuracaklarını bilememekten dolayı katılımcıların önemli bir bölümünün sorunu şikâyet etmeyecekleri sonucu ortaya çıkmaktadır. Bu durumun konuya yönelik bilgilendirme ve eğitim eksikliğine işaret ettiği açıktır. Bunun yanı sıra sonuçlardan kişisel verileri kötüye kullanan kişiden bireysel olarak kendilerini koruyamayacaklarını düşünmelerinin de şikâyet etmelerine engel olacağı anlaşılmaktadır. Son olarak öğrencilerin kişisel verilerinin kötüye kullanılması durumunda en fazla polise şikâyette bulunma eğiliminde oldukları dikkati çekerken, konun muhatabı sayılabilen Kişisel Verileri Koruma Kuruluna ve Cumhuriyet Savcılığına daha az başvuru olacağı araştırma sonuçlarından anlaşılmaktadır. Bu sonucun da yine konuya yönelik bilgilendirme ve eğitim ihtiyacını desteklediği düşünülmektedir.

Çalışmada elde edilen sonuçlar çerçevesinde geliştirilen öneriler aşağıda sıralanmaktadır;

- Kişisel verilerin mahremiyeti ve gizliliğine yönelik algıların ve farkındalığın güçlendirilmesi için internet vasıtasıyla kişisel verilere ve kişisel verilerin korunmasına yönelik bilgilendirme ve farkındalık çalışmaları yapılmalıdır.
- Gelecekte bilgi hizmeti verme potansiyeline sahip bilgi profesyoneli adaylarının söz konusu hizmetleri tasarlarken mahremiyet kavramı, mahremiyet ihlali, kişisel verilerin mahremiyeti, kişisel verilerin işlenme koşulları, kişisel verilerin doğrudan ve/veya ikincil kullanımından doğabilecek sorunlara yönelik farkındalıkla hareket etmelerine katkı sağlayacak içeriklerin derslerde daha etkin bir şekilde vurgulanması önerilmektedir.
- Kişisel verilerin kullanımına ilişkin sözleşme ve kuralları içeren bilgilendirme metinlerinin anlaşılabilirliğinin ve okunabilirliğine yönelik iyileştirmeler yapılması gereklidir.
- Kanunda Kişisel verilerden sorumlu kurum olarak adledilen Kişisel Verileri Koruma Kurulunun görev ve yetki alanına yönelik bilgilendirme çalışmalarınının yapılması gereklidir.

Günümüzde kişisel verilere yönelik mahremiyet ve gizlilik önlemlerinin artırılması veya konuya yönelik farkındalık çalışmalarının yapılandırılmaları gerek teknik anlamda gerek kültürel ve yasal alanlarda üzerinde çalışılması ve katkılar sunulması gereken güncel konulardır. Bu bağlamda gelecek çalışmalarda konuya yönelik farkındalık eğitimlerinin yapılandırılması, yasal yapıların görünürlüğünün artırılması, teknik önerilere yer verilmesi önerilmektedir.

Kaynakça

Aïmeur, E., Gambs, S. ve Ho, A. (2010). Towards a privacy-enhanced social networking site. *2010 International Conference on Availability, Reliability and Security* içinde (ss. 172-179). https://doi.org/10.1109/ARES.2010.97

Akıncı, A. N. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün getirdiği yenilikler ve Türk Hukuku bakımından değerlendirilmesi (Çalışma Raporu No. 2968*). Ankara: Kalkınma Bakanlığı. http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf adresinden erişildi.

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J. ve Agarwal, Y. (2015). Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* içinde (ss. 787–796). USA: ACM. https://doi.org/10.1145/2702123.2702210

Avrupa Konseyi. (1950). *Avrupa insan hakları sözleşmesi*. http://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf adresinden erişildi.

Bennett, L. (2009). Reflections on privacy, identity and consent in on-line services. *Information Security Technical Report*, *14*(3), 119-123. https://doi.org/10.1016/j.istr.2009.10.003

Bilgi Edinme Kanunu. (2003). T.C. *Resmi Gazete*, Sayı: 25269, 24 Ekim 2003.

Boyd, D. ve Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*(8). http://firstmonday.org/ojs/index.php/fm/article/view/3086 adresinden erişildi.

Boyd, D. M. ve Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Buchenscheit, A., Könings, B., Neubert, A., Schaub, F., Schneider, M., ve Kargl, F. (2014). Privacy Implications of Presence Sharing in Mobile Messaging Applications. *Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia* içinde (ss. 20–29). New York, USA: ACM. https://doi.org/10.1145/2677972.2677980

Dinev, T., ve Hart, P. (2005). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce*, *10*(2), 7-29. https://doi.org/10.2753/JEC1086-4415100201

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace, 13. AMCIS 2007 Prooceedings içinde (ss.71-110). Keystone: Colorado.

Goettke, R., Christiana, J., Prof, P., Smith, M. D., Waldo, D. J., Rosen, D. A., ve Friedman, A. (2007). Privacy and online networking websites. *Computer Science 199r: Special Topics in Computer Science Computation and Society* içinde (ss.51-70). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.92.1380&rep=rep1&type=pdf adresinden erişildi.

Govani, T., ve Pashley, H. (2007). Student awareness of the privacy implications when using Facebook. *Proceedings of The IEEE - PIEEE* içinde. http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf adresinden erişildi.

Gross, R., ve Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* içinde (ss. 71–80). New York, NY, USA: ACM. https://doi.org/10.1145/1102199.1102214

Hsieh, H.F. ve Shannon, S.E. (2005), Three Approaches to Qualitative Content Analysis, *Qualitative Health Research*, 15(9), 1277-1288. DOI: 10.1177/1049732305276687

Hughes-Roberts, T., ve Kani-Zabihi, E. (2014). On-Line privacy behavior: using user ınterfaces for salient factors. *Journal of Computer and Communications*, *02*, 220. https://doi.org/10.4236/jcc.2014.24029

İnsan Hakları Evrensel Beyannamesi. (1949). T.C. *Resmi Gazete*, Sayı: 7217, 27 Mayıs 2016.

Kaya, C. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde hassas veriler ve işlenmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 69* (1), 317-334.

Kişisel Verilerin Korunması Kanunu. (2016). T.C. *Resmi Gazete*, Sayı: 29677, 7 Nisan 2016.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Lutz, C., ve Strathoff, P. (2014). *Privacy concerns and online behavior – not so paradoxical after all? viewing the privacy paradox through different theoretical lenses* (SSRN Scholarly Paper No. ID 2425132). Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2425132 adresinden erişildi.

Martin, K. D., ve Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135-155. https://doi.org/10.1007/s11747-016-0495-4

Milne, G. R., ve Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15-29. https://doi.org/10.1002/dir.20009

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, *25*(2), 238-249.

Miltgen, C. L. (2009). Online consumer privacy concern and willingness to provide personal data on the internet. *International Journal of Networking and Virtual Organizations, Indersciences*, *6* (6), 574 - 603.

Miltgen, C. L., ve Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103-125. https://doi.org/10.1057/ejis.2013.17

OECD. (2013). *New data for understanding the human condition: international perspectives.* 12 Şubat 2017 tarihinde https://www.oecd.org/sti/sci-tech/new-data-for-understanding-the-human-condition.pdf adresinden erişildi.

Orwell, G. (1948). *Bin Dokuz Yüz Seksen Dört*, Çev: Nuran Akgören, İstanbul: Can Yayınları

Pitkänen, O., ve Tuunainen, V. K. (2012). Disclosing Personal Data Socially — An Empirical Study on Facebook Users' Privacy Awareness. *Journal of Information Privacy and Security*, *8*(1), 3-29. https://doi.org/10.1080/15536548.2012.11082759

Ridley-Siegert, T. (2015). Data privacy: What the consumer really thinks. *Journal of Direct, Data and Digital Marketing Practice*, *17*, 30-35. https://doi.org/10.1057/dddmp.2015.40

Tan, Q., ve Pivot, F. (2015). Big Data Privacy: Changing Perception of Privacy. *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*içinde (ss. 860-865). https://doi.org/10.1109/SmartCity.2015.176

T.C. Anayasası. (1982). *T. C. Resmi Gazete, 17863 (Mükerrer),* 9 Kasım 1982.

Tuunainen, V., Pitkänen, O., ve Hovi, M. (2009). Users' Awareness of Privacy on Online Social Networking Sites – Case Facebook. *BLED 2009 Proceedings*. içinde http://aisel.aisnet.org/bled2009/42 adresinden erişildi.

Türk Medeni Kanunu (2001). *T. C. Resmi Gazete, 24607*, 22 Kasım 2001.

Türk Ceza Kanunu (2004). *T. C. Resmi Gazete, 5237*, 26 Eylül 2004.

Young, A. L. ve Quan-Haase, A. (2013). Privacy Protection Strategies on Facebook. *Information, Communication & Society*, *16*(4), 479-500. https://doi.org/10.1080/1369118X.2013.777757

Yüksel, M. (2003). Mahremiyet Hakkı ve Sosyo - Tarihsel Gelişimi. *Ankara Üniversitesi SBF Dergisi*, *58*(01). https://doi.org/10.1501/SBFder_0000001619