Bölüm 13

BİLİŞİM SUÇLARINA YÖNELİK HUKUKSAL VE ETİK KABULLENME: YÖNETİM BİLİŞİM SİSTEMLERİ BÖLÜMÜ ÖĞRENCİLERİ ÜZERİNE BİR DEĞERLENDİRME

Türkay HENKOĞLU[1]
Halise ŞEREFOĞLU HENKOĞLU[2]

GİRİŞ

Bilgi ve iletişim teknolojileri vasıtasıyla işlenen suçlara ya da bu konudaki düzenlemelere ilişkin olarak "bilişim suçları" ve "bilişim hukuku" kavramları yaygın olarak kullanılmaktadır (Karagülmez, 2009, s. 37). Bilişim sözcüğü, Türkiye'nin kalkınması için bir araç olarak kullanılması öngörülen yeni bir teknik bilimin adı olarak 1968 yılında Prof. Dr. Aydın Köksal tarafından Almanca ve Fransızca karşılıkları ile birlikte (informatik ve informatique) verilerek kullanılmış ve Türkçe'ye kazandırılmıştır (Köksal, 2006). 765 Sayılı eski Türk Ceza Kanunu'nda[3] "Bilişim Alanında Suçlar" başlığı altında yapılan düzenlemeler ile birlikte bilişim kavramının bilişim suçları ile birlikte hukuk kaynaklarında yer aldığı görülmektedir. 765 Sayılı Kanun'da bilişim alanındaki suçların düzenlendiği 525. maddenin tüm fıkralarında yer alan "bilgileri otomatik işleme tabi tutma" ifadesi, bu kanun kapsamında bilişim kavramına hukuksal açıdan nasıl yaklaşıldığını göstermektedir. 1990'lı yıllardan itibaren iletişim teknolojileri ve bilgisayar ağlarının gelişiminin de etkisiyle artan ve veri depolama ortamları arasında daha fazla yer değiştiren bilgi, hukuksal çerçevede daha fazla gündem haline gelmekte ve çoğunlukla "bilişim hukuku" adı altında değerlendirmeye alınmaktadır. Bu nedenle hukuk literatüründe bilgi hukuku ya da bilişim hukuku arasında ayrım yapılmaksızın, bilişim hukuku kavramının kullanımı yaygın olarak tercih edilmektedir.

[1] Dr. Öğr. Üyesi, Aydın Adnan Menderes Üniversitesi, Söke İşletme Fakültesi, Yönetim Bilişim Sistemleri AD, turkay.henkoglu@adu.edu.tr
[2] Dr. Öğr. Üyesi, Aydın Adnan Menderes Üniversitesi, Söke İşletme Fakültesi, Yönetim Bilişim Sistemleri AD, halise.serefoglu@adu.edu.tr
[3] 13/11/2005 tarih ve 25642 S.R.G. de yayımlanan 04/11/2004 tarih ve 5252 sayılı Kanun'un 12. maddesi ile, 1 Haziran 2005 tarihi itibariyle tüm ek değişiklikleriyle birlikte yürürlükten kaldırılmıştır.

Bilgi ve iletişim çağında bilgi sistemlerinin kullanımı, tüm yaşam alanlarında (ekonomi, sağlık, savunama, enerji, eğitim iletişim vd.) hızla yaygınlaşmaktadır. Buna bağlı olarak artan bilişim suçları, her geçen yıl doğrudan bilgi ve bilgi sistemlerine ya da bilgi teknolojilerinin kullanımıyla hedef haline getirilen kurum ve kuruluşlara daha fazla zarar vermektedir. Kısa süreli kesintilerin dahi büyük sorunlara neden olduğu bilgi ve iletişim çağında, bilgi sistemlerine yönelik tehdit ve saldırılarla mücadelenin yanı sıra, bu sistemleri kullanan kullanıcıların da sorumluluklarının bilincinde ve çok daha dikkatli olması gerektiği aşikardır. Özellikle bilgi merkezleri ve sistem yönetim birimlerinde çalışan profesyonellerin, artan elektronik bilgi işleme miktarı ile birlikte hukuksal sorumluluklarını yerine getirme konusunda daha dikkatli olmaları gerekmektedir.

Bu çalışmanın amacı Yönetim Bilişim Sistemleri Bölümü 4. Sınıf öğrencilerinin bilişim suçlarına yönelik hukuksal ve etik yaklaşımlarını / farkındalıklarını belirlemek ve konuya ilişkin düzenlenen bir eğitim programının ardından öğrencilerin düşüncelerindeki değişimi gözlemlemektir. Bu amaç doğrultusunda çalışmada aşağıda belirtilen sorulara yanıt aranmıştır.

- Bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları ile yasak cihaz veya programlara yönelik suçlara ilişkin katılımcıların hukuksal ve etik açıdan yaklaşımları nasıldır?
- Katılımcıların internet ortamında yapılan yayınlar yoluyla işlenen suçlara hukuksal ve etik açıdan yaklaşımları nasıldır?
- Özel hayata ve hayatın gizli alanına karşı suçlara yönelik olarak katılımcıların hukuksal ve etik kabullenme durumlarında ne tür farklılıklar bulunmaktadır?
- Katılımcıların fikir ve sanat eserlerine ilişkin hukuksal ve etik kabullenme durumları nasıldır?
- Bilişim suçları ve bilişim hukukuna yönelik olarak verilen eğitim sonrasında katılımcıların hukuksal sorumlulukları benimseme düzeyinde ve etik yaklaşımlarında herhangi bir değişiklik olmuş mudur?

BİLİŞİM SUÇLARINA GENEL BAKIŞ

Bilgisayar sistemlerinin kullanımının yaygınlaşması, daha az yer kaplayan transistörlü bilgisayarların 1960'lı yıllardan itibaren vakum tüplü bilgisayarların yerini almasıyla mümkün olmuştur. 1970'li yıllardan itibaren bilgisayarların işlemleri otomatikleştirerek birim zamanda üretim sayısını ve üretim kalitesini

standartlaştırması sayesinde kullanımı yaygınlaşırken, aynı zamanda bu sistemlere yönelik tehditler de artmaya başlamıştır. Bu yıllarda bilgisayar sistemlerine ilişkin saldırıların, doğrudan iletişim altyapısını oluşturan telefon ağına, fiziksel olarak bilgisayar sistemlerine ve/veya üzerinde bulunan bilgilerin bütünlüğüne zarar verme şeklinde olduğu görülmektedir (Hodeghatta & Nayak, 2014, s. 6 ve 13; International Telecommunication Union, 2012, s. 12-13). Bilgisayarla ilgili suçların evrilerek gelişmeye başlaması ve bu suçlara yönelik ilk hukuksal düzenlemelerin yapılması ise 1970'li yıllara dayanmaktadır. Bu yıllarda bilgisayar sistemlerinin kötü amaçlı kullanımına ilişkin örneklerin de artmaya başladığı görülmektedir (Hodeghatta & Nayak, 2014, s. 13-14; Murphey, 2019). 1970 ve 1977 yıllarında Almanya ile 1973 yılında İsveç'te düzenlenmiş olan ulusal veri koruma direktifleri, bilgisayarlar ile işlenen ve kişi haklarını hedef alan suçlara yönelik ilk ve öncü hukuksal düzenleme olma özelliğini taşımaktadırlar (Öman, 2010, s. 390; Riccardi, 1983, s. 247). 1980'li yıllardan itibaren bilgisayarların, bilişim suçlarının öznesi, nesnesi, aracı ve korkutma ya da aldatma amacıyla kullanılan bir sembol haline geldiği görülmektedir (Casey, 2011, s. 40). Günümüzde doğrudan bilgisayar ve bilgisayar sistemlerine yönelik suçların yanı sıra bilgisayarların kullanımıyla gerçekleştirilen suçların da bulunması nedeniyle, bilgisayarlar aracılıyla işlenen suçlar için "bilgisayar suçları" ya da bu tür suçların büyük bölümünün bilgisayar ağlarıyla da ilişkili olması nedeniyle "siber suçlar" şeklinde kullanımlar bulunmaktadır (Casey, 2011, s. xxv). Bu noktada bilişim suçlarının varlığı yaygın olarak kabul edilmiş ve üzerinde uzlaşılmış olsa da bilişim suçu kavramının net bir tanımının olmadığını, kapsamı ve sonuçları hakkında muğlaklık yaşandığını söylemek mümkündür (Balajanov, 2018, s. 4). Bu nedenle bilişim suçu kavramı; "bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suçlar", "bilgisayarla ilgili suçlar", "içerik ile ilgili suçlar" ve "telif hakkı ve ilgili hakların ihlaliyle ilgili suçlar" gibi farklı boyutlarda geniş bir çerçevede tanımlanmaktadır (Avrupa Konseyi, 2001a, s. 4).

Bilgi ve iletişim teknolojilerinin modern yaşamda daha yaygın kullanımı ve özellikle internet altyapısına bağımlılığın artması ile birlikte, bilişim suçları içinde siber suçların daha fazla öne çıktığı görülmektedir. Bu nedenle güvenlik yazılım şirketleri siber suçların oluşumunda önemli derecede rol oynayan internet kaynaklı risk ve tehditler üzerinde daha fazla yoğunlaşmaktadırlar. Güvenlik yazılım şirketlerine göre siber suç, bir bilgisayarın suçun nesnesi olduğu veya suç işlemek için bir araç olarak kullanıldığı bir suç olarak tanımlanmakta-

dır (PandaSecurity, 2018). Birçok farklı etkisi bulunan siber tehditler, internet kullanıcılarını özellikle bilgilerinin çalınması yönüyle sosyal medya üzerinden etkilemektedir. Bu nedenle, bilişim suçları ve siber güvenliğe ilişkin yaklaşımlar içinde veri korumaya yönelik hukuksal sorumluluklar da daha fazla yer bulmaktadır. Bir şirketin siber tehdidi algılama ve önlem alabilmesi için ortalama 200 güne ihtiyaç duyulan bu çağda, güvenlik yazılım şirketleri (PandaSecurity, 2018) dahi kullanıcıların bilinçli ve duyarlı olabilmeleri için gerekli olan eğitimin önemine dikkat çekmektedirler.

Bilişim suçlarının önemli bir bölümü veri koruma hukuku çerçevesinde ya da veri koruma hukuku ile ilişkili olarak açıklanabilmektedir. Ancak hukuksal çerçevede ele alınması gereken bu konu, çoğu zaman iç içe olduğu bilginin gizliliğinin korunması ile aynı koşullarda değerlendirilerek, bilişim hukukuna ilişkin önemli bir farklılık göz ardı edilebilmektedir. Bilişim suçlarıyla hukuksal mücadelenin başlangıcı kabul edilen 1970'li yıllardan günümüze kadar olan süreçte, gizliliğin korunmasından mahremiyetin korunmasına evrilen bir yaklaşımdan söz etmek mümkündür[4]. Mahremiyet, belirli bir sosyal işlev için hangi kişisel verilerin toplanması veya saklanması gerektiği sorusuyla ilgilidir. Bu nedenle bireyin kişisel verisi üzerindeki karar yetkisinin dayandırılacağı hukuksal koşulları da kapsamaktadır. Gizlilik ise toplanan kişisel verilerin kurum ya da kuruluş tarafından nasıl tutulacağı, nasıl kullanılacağı ve kişinin rızasının ne zaman gerekeceği ile ilgilidir (Westin, 1976, s. 6). Bu nedenle "bilgi gizliliği" (informational privacy) ile "veri koruma" (data protection) kavramları için farklı tanımlamalar yapılmaktadır. Duncan & Ark. (1993, s. 22-23) bilgi gizliliğini; bireyin bilgi arayışı, davranışları, fikirleri ve tutumları ile ilgili paylaşımlarının kapsam ve koşullarını seçme yeteneği olarak tanımlamaktadır. Bununla birlikte, bireysel bir hak olan mahremiyetten farklı olarak gizlilik, bireylere ait verilerle sınırlı değildir ve genellikle kuruluşlardaki verileri de kapsamaktadır. Veri koruma ise verilere asgari düzeyde müdahale sağlanması için geliştirilen politika ve prosedürlere uygulanmaktadır. Bunun için veri korumaya yönelik bir dizi güçlü kurallar belirlenerek, bireylerin kişisel verileri üzerinde daha fazla kontrole sahip olmasının sağlanması hedeflenmektedir (Avrupa Komisyonu, 2020).

Verilerin korunmasına yönelik süreçler, bilginin elektronik ortamlara taşınması ile birlikte daha karmaşık hale gelmiş ve farklı birçok bilim alanının dikkatini çekmeye başlamıştır. Kayıtlara göre bilişim suçlarıyla ilgili tarihsel süreç

[4] Çalışma genelinde İngilizce "privacy" karşılığı olarak mahremiyet, "confidentialy" karşılığı olarak gizlilik kavramlarının kullanımı tercih edilmiştir.

1820'li yıllarda başlamaktadır. Ancak 1820 yılında tarihe ilk siber suç olarak geçen olay, özel kumaş serilerinin dokumasında adım dizisinin tekrarlanmasına izin veren Joseph Marie Jacquard'ın dokuma tezgahına yönelik bir sabotaj girişimidir (Kaur & Ark., 2015, s. 21). Bugünkü koşullarda ise bilişim suçları adı altında ifade edilen suçların tamamı bilgisayarlar üzerinde ve/veya bilgi teknolojilerinin kullanımıyla gerçekleşen suçlardır (Karagülmez, 2009, s. 35-38). Teknoloji ve hukuk alanlarını birbirine yaklaştıran bilişim suçları; sınırlarının olmaması, delillerinin elde edilmesinin zorluğu ve uluslararası yargı faaliyetlerinin daha zor yürümesi nedeniyle diğer klasik suçlardan ayrışmaktadır. Bununla beraber bilişim suçlarında faillerin kullandıkları suç enstrümanlarının farklı olması, mağdur ile failin çoğu zaman karşı karşıya gelmemesi ve kolay işlenebilir suçlar olduğu için küçük yaştaki faillerin daha fazla olması, durumu daha zor ve karmaşık hale getirmektedir. Bilişim suçlarına özgü bu durum, suçun gerçekleşmesi için gerekli maddi unsurlardan biri olan nedensellik bağının[5] kurulamamasının en önemli nedeni olarak görülmektedir. Bilişim teknolojilerinin kullanımına yönelik bağımlılığın artması ile birlikte, bilişim suçlarının çeşitliliği ve her geçen yıl etkileri artmaktadır. Bilişim suçları bazen diğer suçların işlenmesi için bir ön araç olarak kullanılmakta, bazen de milyarlarca dolarlık maddi kayıplarının, müşteri kayıplarının ve/veya itibar kaybının doğrudan nedeni olarak ortaya çıkabilmektedir (Radware, 2020; Statista, 2017).

BİLİŞİM HUKUKU VE BİLİŞİM SUÇLARI KAPSAMINDA YER ALAN HUKUKSAL DÜZENLEMELER

Türk Ceza Kanunu (TCK)'nun 243. maddesinin gerekçesinde bilişim sistemi, "verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler" şeklinde tanımlanmıştır (Türk Ceza Kanunu Gerekçesi, 2004). Avrupa Konseyi (2001b, s. 5) Siber Suç Sözleşmesi'nde ise daha kapsamlı olarak "verilerin otomatik işlenmesi için geliştirilmiş donanım ve yazılım unsurlarından oluşan, bir bilgisayar programı aracılığıyla verileri işleyen, girdi, çıktı ve depolama olanaklarını içeren, tek başına veya benzer diğer cihazlar ile bağlantılı olarak çalışan sistem" olarak ifade edilmiştir. Bu nedenle bilişim kavramının hukuksal düzenlemeler ve koşulların değerlendirilmesinde bu kapsamda dikkate alınması önem taşımaktadır.

[5] Nedensellik bağı, meydana gelen netice ile fail arasındaki neden-sonuç ilişkisidir (Boz, 2016, s. vi).

Türkiye'de bilişim suçlarına ilişkin özel bir hukuksal düzenleme bulunmamaktadır. Bilişim hukukuna konu olan bilişim suçlarıyla ilgili hükümler mevcut kanunlara eklenerek oldukça geniş ve dağınık bir şekilde mevzuat içinde yer almaktadır. Türk Hukuk Mevzuatı'nda bilişim suçları ile ilgili düzenlemelerin büyük bölümü 5237 Sayılı TCK, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 5846 Sayılı Fikir ve Sanat Eserleri Kanunu, 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu, 5070 Sayılı Elektronik İmza Kanunu ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun kapsamı içinde yer almaktadır. Bununla beraber, Avrupa Konseyi Siber Suçlar Sözleşmesi gibi uluslararası sözleşmelerin de bilişim hukukuna doğrudan etkileri bulunmaktadır. Bu çerçevede içeriği suç teşkil eden web sitelerinin oluşturulması, dolandırıcılık, fikri mülkiyet ihlali, özel hayatın gizliliği ve kişisel verilerin hukuka aykırı olarak işlenmesi gibi birçok klasik suçun işlenmesi için internetin ya da daha geniş anlamda bilgi ve iletişim teknolojilerinin kullanılması, bu tür klasik suçları bilişim hukuku kapsamında değerlendirilen suçlar haline getirmiştir (Kaya & Çakır, 2020, s. 39-40).

Bilişim suçları birçok ülkede özel kanunlarla ya da ceza kanunları içerisinde düzenlenmiştir (Dülger, 2004). Ülkemizde bilişim suçlarına ilişkin hukuksal düzenlemelerin büyük bölümü TCK içerisinde bulunmaktadır. TCK (2004)'da bilişim suçları "Bilişim Alanında Suçlar" adı altında yer alan bir bölüm olarak ve aynı zamanda bilişim sistemlerinin kullanılmasıyla nitelikli olarak gerçekleşebilecek hırsızlık ve dolandırıcılık gibi suçlara ilişkin maddeler içinde[6] düzenlenmiştir. TCK kapsamında bilişim sistemleri vasıtasıyla işlenebilen suçlara ilişkin düzenlemelerin yapıldığı başlıca maddeler; 124 (haberleşmenin engellenmesi), 125/2 (bilişim sistemi kanalıyla hakaret), 132 (haberleşmenin gizliliğini ihlâl), 135 (kişisel verilerin kaydedilmesi), 136 (verileri hukuka aykırı olarak verme veya ele geçirme), 138 (verileri yok etmeme), 142/2 (nitelikli hırsızlık), 158/1 (nitelikli dolandırıcılık), 163 (karşılıksız yararlanma), 243 (bilişim sistemine girme), 244 (sistemi engelleme, bozma, verileri yok etme veya değiştirme), 245 (banka ve kredi kartlarını kötüye kullanma), 245/A (yasak cihaz veya programlar), 246 (tüzel kişiler hakkında güvenlik tedbiri uygulanması), 228/3 (kumar oynanması için yer ve imkan sağlama) ve 226. (müstehcenlik) maddelerdir.

[6] Dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi (TCK:158-f) ve hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi (TCK:142-e), suçun işlenmesindeki kolaylık ve takibindeki zorluk nedeniyle nitelikli hal olarak görülmüştür.

Bilişim hukuku kapsamında göz önünde bulundurulması gereken diğer bir husus ise özel hukuk çerçevesinde kişilik haklarının korunmasıdır. Kişilik haklarının ihlali halinde koruyucu ve tazminat davalarının açılması mümkündür. Kişi (davacı) ihlalin gerçekleşme durumuna göre; saldırı tehlikesinin önlenmesi, sürmekte olan saldırıya son verilmesi ya da etkileri devam eden saldırının hukuka aykırılığının tespit edilmesi isteyebilir (Türk Medeni Kanunu, 2001). Kişilik haklarının korunmasına yönelik özel hukuk kapsamındaki başlıca düzenlemeler arasında; Türk Medeni Kanunu (m23, 24, 25, 26, 27, 158/2, 174, 304 ve 305), Fikir ve Sanat Eserleri Kanunu (m14-19, 70-71 ve 80-83), Türk Ticaret Kanunu (m56) ve Türk Borçlar Kanunu (m45, 46, 47, 48 ve 49) bulunmaktadır.

ARAŞTIRMANIN ÖNEMİ

Bilişim suçları ile mücadele edebilmek ve bilgi güvenliğinin sağlanması için hukuksal, teknik ve idari yöntemlerin birlikte kullanılması önem taşımaktadır. Ancak bununla birlikte, kullanıcılarda gerekli ve yeterli düzeyde farkındalık oluşmadığında kullanılan yöntemlerin etkisi azalmakta ya da tümüyle ortadan kalkabilmektedir. Bu nedenle bireysel ya da kurumsal ayrım yapılmaksızın, tüm kullanıcıların bilişim suçları ve olası risk ve tehditler hakkında bilgi sahibi olması önem taşımaktadır. Diğer taraftan teknik önlemlerin alınmasına yönelik asgari standartların yanı sıra, herhangi bir ihlal ile karşı karşıya kalındığında sahip olunan hukuksal hakların bilinmesi de sorunların aşılması ya da çözümsüz kalmasında belirleyici olabilmektedir. Basılı belgeler üzerinde olduğu gibi elektronik ortamlarda üretilen bilgilerin ve bilişim teknolojileri kullanılarak yapılan tüm işlemlerin hukuka uygun olma zorunluluğu bulunmaktadır. Bilgi toplumlarında bilişim suçlarını işleme yaşının her geçen yıl küçüldüğü (Aiken & ark., 2016; Eriş, 2011, s. 39; News Room, 2015) dikkate alındığında; bilişim suçlarına yönelik bilinçlenme ve hukuksal sorumlulukların öğrenilmesine katkı sağlayan öğrenme süreçlerinin de daha küçük yaşlarda başlamasının önemli olduğu düşünülmektedir (Balajanov, 2018). Böylelikle, yapılan araştırmalarda da belirtildiği gibi (Henkoğlu, 2015, s. 173), ilgi ve meraka bağlı olarak gerçekleşen bilişim suçlarının sayısında azalma olacağı ve aynı zamanda bireylerin bilişim suçları karşısında daha bilinçli yaklaşımlarda bulunmalarının sağlanabileceği değerlendirilmektedir.

Günümüzde kullanılan en kapsamlı bilgi güvenliği modellerinden biri olan McCumber (2005, s. 106) modelinde ve kuruluşların bilgi varlıklarına yönelik tüm potansiyel risk yelpazesini belirlemek ve bunlarla mücadele etmek için

sistematik bir yaklaşım sağlayan ISO 27001 (2013) standardı içinde önemi vurgulanan eğitim ve farkındalığın, teknik ve hukuksal boyutta önlemlerin alınmasına yönelik bütünlüğü tamamlamada büyük ölçüde etkisi bulunmaktadır (Calder & Watkins, 2020, s. 129). Her ne kadar gerekli hukuksal düzenlemeler doğru zamanda yapılmış olsa da bilginin elde edilmesi, işlenmesi, saklanması, transferi ve imha edilmesine yönelik süreçlerin hukuka uygun olarak izlenmesi, bilgi profesyonellerinin bilişim hukukuna ilişkin farkındalığının sağlanması ile mümkün olabilmektedir.

Klasik suçlarda olduğu gibi bilişim suçlarına yönelik olarak da hukuksal düzenlemeler önleyici tedbirler arasında öne çıkmaktadır. Bununla beraber, hukuksal düzenlemeler hakkında yeterli düzeyde bilgi sahibi olmayan bilgisayar kullanıcılarının, zaman zaman etik değerleri dikkate alarak da suç ve ihlallerden kaçınarak benzer tutum ve davranış özellikleri gösterdikleri bilinmektedir. Bu nedenle, bu çalışmada bilişim suçlarına yönelik hukuksal düzenlemelere ilişkin farkındalığı görmenin yanı sıra, hukuksal düzenlemeler hakkında fikri olmayan kullanıcıların etik değerleri dikkate alarak benzer sonuçlara ne kadar yaklaşabildiklerinin de görülmesi amaçlanmaktadır. Literatürde katılımcıların bilişim suçlarına yönelik hukuksal ve etik yaklaşımın değerlendirildiği ve sonrasında katılımcılara bilişim hukuku eğitimi verilerek hem hukuksal hem de etik yaklaşımdaki değişimin ortaya konulduğu bir araştırma bulunmamaktadır. Bu çalışmadan elde edilen sonuçlara bağlı olarak, bilişim suçlarına yönelik farkındalığın nasıl arttırılabileceği ve bilişim suçları ile mücadelede bilinçlenme düzeyinin artmasıyla en etkin sonucun nasıl alınabileceği konusunda somut çıkarımlarda bulunulabilmektedir.

YÖNTEM

Araştırma Deseni

Bilişim hukuku mevzuatına ve etiğine ilişkin geliştirilen bir eğitim programının etkililiğinin değerlendirilmesi amacıyla gerçekleştirilen bu çalışmada tek grup öntest-sontest yarı deneysel model kullanılmıştır. Bağımsız bir değişkenin bağımlı bir değişken üzerindeki etkisini ölçmek amacıyla yürütülen bu modelde seçilmiş bir çalışma grubuna uygulanan öntest ve sontest ölçümleri arasındaki olası farklılığın, iki ölçüm arasında ilgili bağımsız değişkene ilişkin gerçekleştirilen işlemden kaynaklandığı öngörülmektedir (Babbie, 2010; Rubin & Babbie, 2011). Mevcut araştırmada da bilişim hukuku mevzuatına ve etiğine ilişkin geliştirilen bir eğitim programının, çalışma grubunda yer alan lisans öğrenci-

lerinin bilişim hukuku farkındalığına ve bu konudaki etik algılarına etkisi değerlendirilmek istenmiştir. Bu amaç doğrultusunda bir grup lisans öğrencisine geliştirilen eğitim programı uygulanmış, programın etkili olup olmadığı aynı grup üzerinde uygulama öncesinde yapılan öntest ile uygulama sonrasında yapılan sontest ölçümleri arasındaki farkın manidarlığı ile belirlenmiştir. Bununla birlikte, bu çalışma etik kurul izin/onay belgesi gerektirmeyen bir çalışmadır.

Çalışma Grubu

Araştırmanın çalışma grubunu, 2020-2021 eğitim-öğretim yılında Yönetim Bilişim Sistemleri Bölümü'nde öğrenim gören ve çalışmaya gönüllü olarak katılan 62 son sınıf öğrencisi oluşturmaktadır. Çalışma grubunun seçiminde gönüllü katılım esas alınmış ve amaçlı örnekleme yöntemine başvurulmuştur. Sınırlı kaynakların etkin kullanımı için bilgi açısından zengin deneklerin belirlenerek seçilmesi şeklinde tanımlanan amaçlı örnekleme yönteminde ele alınan problem durumuna ilişkin bilgi ve deneyim sahibi ve araştırmaya en çok katkı yapacağı öngörülen bireylerin çalışma grubuna dahil edilmesi söz konusudur (Patton, 2002, s. 230). Bu kapsamda çalışma grubunun oluşturulmasında araştırmacıların da görev yaptığı üniversitede Yönetim Bilişim Sistemleri Bölümü son sınıf öğrencilerinin tamamına araştırmacılar tarafından çalışmanın amacı ve kapsamı hakkında bilgilendirme yapılmış ve tamamen gönüllülük esasına bağlı olarak öğrenciler çalışmaya katkı sağlamaya davet edilmişlerdir.

Yaş aralığı dikkate alındığında, bilişim suçlarının işlenme oranlarının en yüksek olduğu yaş grubunun 21-30 yaş grubu olduğunu görülmektedir (Aiken ve diğerleri, 2016, s. 2; Boateng & ark., 2010; Eriş, 2011, s. 39; News Room, 2015). Bu grubunun bilgi ve iletişim teknolojilerini en yoğun kullanan grup olmasının yanı sıra (Johnson, 2021; Türkiye İstatistik Kurumu, 2021), bu yaştaki bireylerin bir bilişim sistemine izinsiz girilmesi ya da programın kırılmasına yönelik ilgi ve merakları, dijital ortamın sunduğu imkânlar ile yasal olmayan eylemleri teşvik edici içeriğe maruz kalmaları ve bu tür suçlarla ilişkili kişilerle kolayca iletişim kurabilmeleri, etik ve yasal değerlere ilişkin düşük farkındalıkları ve tüm bu nedenlere bağlı olarak suç işlemeye daha fazla meyilli olmalarının; bilişim suçlarının bu yaş grubunda daha fazla işlenmesine neden olduğunu söylemek mümkündür (Balajanov, 2018, s. 15; Yılmaz & Güllüpınar, 2020, s. 5380-5381). Diğer taraftan yaş faktörü ile birlikte, çalışma grubunda yer alan öğrencilerin öğrenim gördükleri Yönetim Bilişim Sistemleri Bölümü'nün mesleki hedefleri dikkate alındığında, bu bölümün öğrencilerinin son sınıfa kadar

bilgi ve iletişim teknolojileri odaklı birçok ders aldıkları, bilişim etiği konusunda görece daha fazla farkındalığa sahip oldukları ve gördükleri öğrenim doğrultusunda sistem ve veri analizi bilgileri ile bilişim hukuku bilgisini temel alan adli bilişim süreçlerine daha fazla ilgi duyan öğrenci grupları arasında yer aldıkları görülmektedir (Henkoğlu & Şerefoğlu, 2019, s. 596).

Veri Toplama Aracı

Bu çalışmada veri toplama aracı olarak araştırmacılar tarafından geliştirilen "Bilişim Hukuku ve Etiği Farkındalık Anketi" kullanılmıştır. İlgili anket; 6'sı katılımcıların demografik özelliklerini ve bilgi ve iletişim teknolojilerini kullanım alışkanlıklarını, 29'u ise 3'lü likert tipinde hazırlanmış ve katılımcıların bilişim suçlarına ve etik değerlere ilişkin farkındalıklarını belirlemeye yönelik toplam 35 sorudan oluşmaktadır. Ankette yer alan likert tipi sorular, katılımcıların ilgili maddede ifade edilen bilişim suçunu yasal ve etik açıdan değerlendirmelerine imkân verecek biçimde "hukuksal olarak suçtur" ve "ahlaki açıdan uygun değildir" olmak üzere iki ayrı kategori altında ve "katılıyorum", "katılmıyorum" veya "fikrim yok" seçenekleri ile yanıt vermelerini sağlayacak şekilde düzenlenmiştir. Likert tipi sorular 4 temel başlık altında gruplandırılmıştır. Bu ana başlıklar ve her bir başlık altında yer alan soru sayıları aşağıda belirtildiği şekildedir.

1. Bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları ile yasak cihaz veya programlara yönelik suçlar (10 Soru)
2. İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlar (6 Soru)
3. Özel hayata ve hayatın gizli alanına karşı suçlar (9 Soru)
4. Fikir ve sanat eserlerine ilişkin suçlar (4 Soru)

Anket geliştirme sürecinde öncelikle alanyazındaki ilgili çalışmalar incelenerek bu çalışmalar kapsamında en sık ifade edilen ve gündelik hayatta en fazla karşılaşılabilecek bilişim suçları ve etik ihlaller belirlenmiştir. Bu kapsamda belirlenen ilgili suçlara ve ihlallere ilişkin ifadeler temel alınarak bir madde havuzu oluşturulmuştur. Bu işlemin ardından hazırlanan taslak anket formu kapsam geçerliliğinin değerlendirilmesi amacıyla uzman görüşüne sunulmuştur. Uzman görüşleri doğrultusunda taslak form üzerinde gerekli düzeltmeler yapılarak nihai anket formu oluşturulmuştur.

Eğitim Programının Uygulanması ve Veri Toplama Süreci

Çalışma kapsamında bilişim hukuku mevzuatına ve etiğine ilişkin geliştirilen eğitim programı, çalışma gurubunda yer alan gönüllü öğrencilerine 12 haftalık bir süreç içerisinde çevrimiçi olarak uygulanmıştır. Yapılan uygulama ile eğitim programının kazanımları çerçevesinde öğrencilere eğitim verilerek öğrencilerin temel bilişim hukuku mevzuatına ve etik değerlere ilişkin bilgi ve farkındalık düzeylerinin artırılması amaçlanmıştır.

Eğitim programı içinde bilişim hukukuna ve etiğine ilişkin aşağıda belirtilen konu başlıklarına yer verilmiştir:

1. TCK'nın genel hükümleri, temel ilkeler ve tanımlar
2. Bilişim hukukunda suç teorisi, suçun unsurları ve hukuka aykırılığı ortadan kaldıran sebepler
3. Bilişim suçlarında soruşturma ve kovuşturma
4. Bilişim sisteminin kendisine karşı ve bilişim sistemi kullanılarak işlenen suçlar
5. Avrupa Konseyi Siber Suçlar Sözleşmesi'nde tanımlanan bilişim suçları
6. Adliyeye, özel hayata ve hayatın gizli alanına karşı suçlar
7. İnternet ortamında yapılan yayınlar yoluyla işlenen suçlar
8. Fikri mülkiyet hakları ihlalleri ve internet yayıncılığı
9. Elektronik ortamda yer alan belgelerin hukuksal niteliği ve elektronik imza
10. Avrupa Birliği ve Türk Hukuk Mevzuatında kişisel verilerin korunmasına ilişkin düzenlemeler

Eğitim uygulaması, araştırmacıların kendi sorumluluğu altında ve gönüllü öğrencilerin görüşleri de alınarak belirlenen gün ve saatlerde çevrimiçi yapılmıştır. Bu kapsamda, her hafta bir ders oturumu yaklaşık 2 saat olarak düzenlenen uygulamada her bir öğrenci 12 farklı çevrimiçi oturuma katılmış ve böylece bu süreç içerisinde toplam 24 saatlik bir eğitime tabi tutulmuştur. Bununla birlikte, eğitim uygulamasının ilk haftasında araştırmada veri toplama aracı olarak kullanılan anket çevrimiçi ortamda öntest olarak uygulanmıştır. Ancak öntest uygulamasından önce araştırma süreci ve uygulanacak eğitim programı hakkında öğrencilere tekrar sözlü olarak bilgi verilmiş ve katılımlarının tamamen gönüllülük esasına bağlı olduğu hatırlatılmıştır. Bu kapsamda öğrencilerden

öntest uygulamasındaki anket sorularını cevaplamadan önce anketin ilk sayfasında yer alan bilgilendirme bölümünü okuyarak ve bölüm sonundaki onay/izin seçeneğini işaretleyerek çalışmaya gönüllü katılımlarını beyan etmeleri istenmiştir. Benzer şekilde uygulamanın son haftasında eğitim programı tamamlandıktan sonra eğitim öncesinde öntest olarak uygulanan anket sontest olarak tekrar çevrimiçi ortamda uygulanmış ve ardından öğrencilerin eğitim programına ilişkin görüş ve önerileri alınmıştır.

Verilerin Analiz Edilmesi

Çalışmada elde edilen verilerin analizinde betimleyici istatistiklerden yararlanılmıştır. Bu kapsamda ankette yer alan her bir soru için öntest ve sontest olmak üzere iki ayrı grup altında yüzde ve sıklık değerleri hesaplanmıştır. Bu kapsamda ankette yer alan her bir sorudan elde edilen veriler, diğer sorulardan bağımsız olarak ilgili soruda ifade edilen tekil duruma ilişkin katılımcıların fikrinin belirlenmesi amacıyla kullanılmıştır. Bu nedenle katılımcılardan öntest ve sontest olmak üzere iki aşamada elde edilen verilerin karşılaştırılmasında yüzde ve sıklık değerleri temel alınmıştır ve ankette yer alan likert tipi sorulardan her bir katılımcının farkındalığını belirlemeye yönelik toplam ölçüm değeri (puan) elde edilmemektedir. Bu noktada hazırlanan anketin 71 katılımcıya uygulandığını, ancak öntest veya sontest aşamasında eksik verilerin ve özensiz işaretlemelerin olduğu 9 anketin değerlendirme dışı bırakılarak, veri analizinin 62 katılımcı üzerinde yapıldığını belirtmekte fayda vardır.

Çalışmada belirtilen veri analizlerinin gerçekleştirilmesi amacıyla Microsoft Excel 2019 ve IBM SPSS Statistics 20 programlarından yararlanılmıştır.

BULGULAR VE YORUM

Çalışmada kapsamında elde edilen bulgular veri toplama aracı olarak kullanılan ankette yer alan soruların gruplandırıldığı ana başlıklar altında sunulmaktadır.

Katılımcıların Demografik Özellikleri

Çalışma grubunda yer alan katılımcıların tamamı her gün internet kullandıklarını ve %77,41'i (n=48) bilgi ve iletişim teknolojileri hakkındaki gelişmeleri yakından takip ettiklerini belirtmektedir. Yaş ortalaması 21,50 olan katılımcıların %98,38'i (n=61) 6 yıldan daha uzun süredir internet kullanıcısı olduğunu belirtirken, 10 yıldan daha uzun süredir internet kullanıcısı olduğunu belirten katılımcı oranı ise %64,51 (n=40)'dir. Katılımcıların tamamı internete evden,

okuldan ya da mobil hatlar üzerinden bağlanarak, interneti derslerle ilgili konuları araştırma, iletişim kurma, güncel gelişmeleri takip etme, oyun ve eğlence amacıyla kullandıklarını belirtmektedirler. Bununla birlikte, katılımcıların tamamı bu araştırma öncesinde bilişim hukuku ve etiğine ilişkin herhangi bir eğitim, ders, kurs, seminer vb. etkinliğe katılmadıklarını belirtmişlerdir.

Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları ile Yasak Cihaz veya Programlara Yönelik Suçlar

Bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme, banka veya kredi kartlarının kötüye kullanılması ve yasak cihaz veya programlara yönelik suçlar, TCK'nın 243., 244., 245. ve 245/A maddelerinde düzenlenmektedir. Bu suçlara ilişkin olarak katılımcılara yöneltilen sorular ve bu sorulara "katılıyorum" yanıtını veren katılımcıların hukuksal ve etik kabullenme durumlarına ilişkin betimsel istatistikler Tablo 1'de sunulmaktadır.

Tablo 1 incelendiğinde; bilişim alanındaki suçlara ilişkin olarak yöneltilen sorulara katılımcıların öntest aşamasında verdikleri yanıtların %60'ında etik kabullenmenin hukuksal kabullenmeden daha yüksek olduğu görülmektedir. Sontest aşamasında ise katılımcıların tüm sorularda etik kabullenmeden ziyade hukuksal düzenlemelere uygun bir yaklaşım içinde oldukları görülmektedir. Sontest aşamasında katılımcılardan sadece "aynı konutta yaşayan kardeşlerden birinin, diğerine ait kredi kartını kullanarak zarara neden olması" ve "TCK'da tanımlanan bilişim alanındaki suçları işleme amacı ile geliştirilmemiş bir yazılımın bulundurulması" ile ilgili fiillerin hukuksal olarak suç olduğunu düşünenlerin oranlarında büyük ölçüde azalma olduğu görülmektedir. Böylece verilen eğitim ile katılımcıların bahsi geçen fiillere ilişkin hukuksal düzenlemeler kapsamında doğru düşünüş biçimini edindiklerini söylemek mümkündür. Bu kapsamda genel olarak öntest aşamasında katılımcıların bilişim alanındaki suçlara ilişkin soruları bilgi eksiklikleri nedeniyle etik algıları üzerinden yanıtladıkları, eğitim sonrası yapılan sontest aşamasında ise bilişim suçlarına ilişkin değerlendirmeyi hukuksal ve etik algılarını birlikte kullanarak yaptıkları görülmektedir. Sontest aşamasında özellikle "aynı konutta yaşayan kardeşlerden birinin, diğerine ait kredi kartını kullanarak zarara neden olması" ile ilgili olarak hukuksal ve etik yaklaşım arasındaki büyük farklılık, eğitim sonrasındaki bilinçlenmeye bağlı olarak katılımcıların hukuksal açıdan doğru bir yaklaşım içinde olduğunu ve bununla beraber beklendiği gibi bu fiilin etik açıdan uygun bulunmadığını göstermektedir. Tablo 1'de yer alan verilerde dikkat çeken diğer bir nokta ise sontest aşamasında "bir ülke aleyhinde yayın yapan bir web sitesinin, bir hac-

Tablo 1. Bilişim Alanında Suçlara İlişkin Hukuksal ve Etik Kabullenme Durumu

Bilişim suçu / Etik ihlali	Hukuksal olarak suç olduğunu düşünüyorum				Etik olarak uygun bulmuyorum			
	Öntest		Sontest		Öntest		Sontest	
	n	%	n	%	n	%	n	%
Bir bilişim sistemindeki verilere yetkisiz olarak erişip herhangi bir zarar vermeden sistemden çıkılması	39	62,90	56	90,32	35	56,45	52	83,87
Başkasına ait bir bilişim sistemindeki güvenlik açıklarının gerekli izinler alınmaksızın araştırılması	33	53,22	50	80,64	40	64,51	47	75,80
Bir ülke aleyhinde yayın yapan bir web sitesinin, bir hacker grubu tarafından kapatılması	38	61,29	56	90,32	22	35,48	39	62,90
Şifreli yayın yapan ve abonelik gerektiren bir yayının, bedel ödemeksizin /çeşitli yazılımlar aracılığıyla) izlenmesi	47	75,80	54	87,09	40	64,51	48	77,41
Bir web sitesine genel erişimi engelleyici teknikler kullanmak	40	64,51	56	90,32	40	64,51	55	88,70
Bir program ya da güvenlik kodunun bir bilişim sistemindeki verileri değiştirmek amacıyla başkasına gönderilmesi	49	79,03	60	96,77	54	87,09	61	98,38
Bir bilişim sistemine hukuka aykırı olarak girmek amacıyla hazırlanmış kodların sabit disk üzerinde bulundurulması	39	62,90	49	79,03	42	67,74	50	80,64
Aynı konutta yaşayan kardeşlerden birinin, diğerine ait kredi kartını kullanarak zarara neden olması	44	70,96	6	9,67	56	90,32	55	88,70
Bir internet sitesi üzerinde kayıtlı bulunan kredi kartı bilgilerinin elde edilmesi amacıyla geliştirilmemiş, ancak bu amaçla da kullanılabilecek bir kodun (farklı bir kullanım amacı için) bulundurulması	37	59,67	4	6,45	39	62,90	13	20,96
Bir banka çalışanı tarafından müşterilerin hesap bilgileri kullanılarak yetkisiz para transferi yapılması	61	98,38	62	100	62	100	62	100

ker grubu tarafından kapatılmasını" katılımcıların büyük bir çoğunluğu (n=56, %90,32) suç olarak tanımlamasına karşın, aynı zamanda %37,1 (n=23)'inin bu fiili etik olarak kabul edilebilir bulmasıdır. Bu durum, eğitim hedefi doğrultusunda bilişim suçlarına ilişkin hukuksal koşulların öğrenilmiş olduğunu, ancak böyle bir durumda dahi katılımcıların bir bölümünün etik değerler kapsamında bu konuya duyarsız kalabileceğini göstermektedir.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlar

İnternet üzerinde içerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcıların yükümlülükleri ile internet ortamında işlenen belirli suçlarla mücadeleye ilişkin esas ve usuller 5651 Sayılı Kanun ile düzenlenmiştir. 5651 Sayılı Kanun'un 8. Maddesinde düzenlenen suçlara ilişkin katılımcılara yöneltilen sorular ve bu sorulara "katılıyorum" yanıtını veren katılımcıların hukuksal ve etik kabullenme durumlarına ilişkin betimsel istatistikler Tablo 2'de sunulmaktadır.

Tablo 2 incelendiğinde, eğitim öncesi ve sonrasındaki hukuksal kabullenme oranlarındaki değişimle birlikte, 5651 Sayılı Kanun'un 8. Maddesinde düzenlenen suçlara yönelik olarak tüm katılımcılarda farkındalığın arttığı görülmektedir. Tablo 2'de yer alan verilerde dikkat çeken nokta ise sontest aşamasında katılımcıların yarısından fazlasının (%54,83) "daha önce Facebook üzerinden yayımlanmış ve kaldırılmış resimlerin veri sahibinin rızası dışında yayımlanması" fiilinin hukuksal olarak suç olduğu konusunda tereddüt yaşarken, neredeyse tamamının (%95,16) bu fiili etik olarak doğru bulmamasıdır. Bu durum, bilişim suçlarına ilişkin hukuksal bilgi eksikliğinin devam ettiği hususlarda etik kabullenmenin bu açığı kapattığını göstermektedir. Bununla beraber, eğitim sonrasında Tablo 2'de yer alan tüm suçlara yönelik olarak sadece hukuksal kabullenmede değil, etik kabullenme oranlarında da artış olduğu görülmektedir.

Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar

Haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğini ihlal, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmemeye ilişkin suçlar, TCK'nın 9. bölümünde 132 ila 140. maddeleri arasında düzenlenmiştir. Bu kapsamda katılımcılara yöneltilen sorular ve bu sorulara "katılıyorum" yanıtını veren katılımcıların hukuksal ve etik kabullenme durumlarına ilişkin betimsel istatistikler Tablo 3'te sunulmaktadır.

Tablo 2. İnternet Ortamında Yapılan Yayınlar Yoluyla İşlenen Suçlara İlişkin Hukuksal ve Etik Kabullenme Durumu

	Hukuksal olarak suç olduğunu düşünüyorum				**Etik olarak uygun bulmuyorum**			
Bilişim suçu / Etik ihlali	**Öntest**		**Sontest**		**Öntest**		**Sontest**	
	n	**%**	**n**	**%**	**n**	**%**	**n**	**%**
Daha önce Facebook üzerinden yayımlanmış ve kaldırılmış resimlerin veri sahibinin rızası dışında yayımlanması	18	29,03	34	54,83	52	83,87	59	95,16
Facebook ya da Twitter üzerinden bir kişiye yönelik hakaret içerikli yayın yapılması	42	67,74	58	93,54	55	88,70	61	98,38
İnternet sitesi üzerinden kumar oynamaya imkân sağlanması	52	83,87	56	90,32	43	69,35	51	82,25
İnternet sitesi üzerinden intihara teşvik eden yayınların yapılması	52	83,87	62	100	60	96,77	62	100
Uyuşturucu kullanma yöntemleri konusunda bilgi veren bir internet sitesinin oluşturulması	48	77,41	62	100	55	88,70	61	98,38
Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukların ya da temsili çocuk görüntülerinin kullanılması	56	90,32	62	100	61	98,38	62	100

Tablo 3. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlara İlişkin Hukuksal ve Etik Kabullenme Durumu

	Hukuksal olarak suç olduğunu düşünüyorum				Etik olarak uygun bulmuyorum			
Bilişim suçu / Etik ihlali	**Öntest**		**Sontest**		**Öntest**		**Sontest**	
	n	**%**	**n**	**%**	**n**	**%**	**n**	**%**
Hizmetler için daha sonra ihtiyaç duyulabileceği gerekçesiyle mümkün olan tüm kişisel bilgilerin kaydedilmesi	14	22,58	57	91,93	23	37,09	38	61,29
Kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis ve tedavi hizmetlerinin yürütülmesi amacıyla özel nitelikli kişisel verilerin, yetkili kurum tarafından veri sahibinin açık rızası aranmaksızın işlenmesi	47	75,80	1	1,61	44	70,96	3	4,83
Kurum ve ilgili birimde sorumlu olunan ve kullanım süresi sona eren evrakların yok edilmeyerek daha sonra ihtiyaç duyulabileceği düşüncesiyle muhafaza edilmesi	29	46,77	44	70,96	28	45,16	34	54,83
Hukuka uygun olarak elde edilen müşteri bilgi ve belgelerinin açıklanması	22	35,48	41	66,12	32	51,61	48	77,41
Kamu görevlisi tarafından görevinin verdiği yetki kullanılmak suretiyle kurum kayıtlarında yer alan kişisel verilerin başkasına verilmesi	58	93,54	61	98,38	61	98,38	62	100

Kişinin tarafı olduğu haberleşmenin (telefon görüşmesi WhatsApp vb.) içeriğini diğer tarafın rızası olmaksızın açıklaması	46	74,19	62	100	59	95,16	62	100
Kişinin kendisi ile birlikte en az üç kişinin bulunduğu ortamda diğerlerinin rızası dışında yapılan konuşmaları kaydetmesi	46	74,19	62	100	55	88,70	62	100
İki kişi arasında yapılan görüşmeye ilişkin ses kayıtlarının müşterek bir arkadaşa dinletilmesi	27	43,54	62	100	45	72,58	62	100
Sonradan kanıt elde etme imkânının olmadığı ve yetkili makamlara başvurma olanağının bulunmadığı ani gelişen durumlarda ses ya da görüntü kaydı yapmak	33	53,22	1	1,61	32	51,61	1	1,61

Tablo 3 incelendiğinde; katılımcıların kişisel verilerin işlenmesi, kaydedilmesi ve muhafaza edilmesine yönelik hukuksal farkındalıkları eğitim öncesinde görece düşükken, eğitim sonrasında bu fiillere ilişkin farkındalıklarının arttığı görülmektedir. Kişisel verilerin işlenmesine yönelik düzenlemeler TCK'nın bahsi geçen ilgili maddelerinin yanı sıra, 6698 Sayılı Kanun'un 2. bölümünde 4 ila 9. maddeleri arasında da yer almaktadır. Her ne kadar 6698 Sayılı Kanun hakkında farkındalığı oluşturmaya yönelik olarak Kişisel Verileri Koruma Kurumu (2021) tarafından tüm konu başlıklarına özel rehberler oluşturulmuş ve kamu spotları yayımlanmış olsa da katılımcıların eğitim öncesinde veri koruma hukuku hakkında yeterince bilgi sahibi olmadıkları görülmektedir. Sadece "kamu görevlisi tarafından görevinin verdiği yetki kullanılmak suretiyle kurum kayıtlarında yer alan kişisel verilerin başkasına verilmesi" konusunda katılımcıların tamamına yakını öntest ve sontest aşamasında hukuksal ve etik olarak beklenen yaklaşımı gösterdikleri görülmektedir. Bu kapsamda katılımcılara verilen eğitimin, genel olarak katılımcıların veri korumaya ilişkin etik yaklaşımlarında

da hukuksal algı ile benzer değişikliğe neden olduğu söylemek mümkündür. Örneğin "hukuka uygun olarak elde edilen müşteri bilgi ve belgelerinin açıklanması" konusunda öntest aşamasında etik açıdan fikrinin olmadığını belirten 16 katılımcının 14'ünün sontest aşamasında bu fiili etik olarak uygun bulmadığını belirtmesi katılımcıların etik yaklaşımlarının olumlu yönde değiştiğini göstermektedir.

Haberleşmenin gizliliğini ihlal ve kişiler arasındaki konuşmaların dinlenmesi ve kayda alınmasına ilişkin TCK'nın 132. ve 133. maddelerinde düzenlenen suçlarla ilgili olarak yöneltilen sorulara (6., 7. ve 8. sorular) katılımcıların tamamı sontest aşamasında hem hukuksal hem de etik olarak uygun bulmadıklarını belirten yanıtlar vermişlerdir. Ancak katılımcıların yaklaşık yarısının örnekler üzerinden yöneltilen üç soruya öntest aşamasında hukuksal olarak aynı yaklaşımı göstermediği, başka bir ifadeyle hukuksal olarak suç olup olmadığı konusunda yeterince bilgi sahibi olmadıkları görülmektedir. Eğitim sonrasında yapılan sontest verileri ise katılımcıların hukuksal kabullenme durumlarında belirgin bir artış olduğunu göstermektedir.

Tablo 3'te yer alan ve özel hayata ve hayatın gizli alanına karşı suçlara ilişkin 9. soru doğrudan hukuksal düzenlemelerde yer almamakla birlikte günlük hayatta sıkça karşılaşılan ve Yargıtay kararları (2012, 2014b, 2014c, 2014a) ile açıklık kazanan konulara yönelik olarak hazırlanmıştır. Bu soru katılımcıların verilerin işlenmesi ile ilgili hukuksal ve etik algılarının ölçülebilmesi amacıyla yöneltilmiştir. Soruda verilen örneğe ilişkin olarak öntest aşamasında katılımcıların yaklaşık olarak yarısının (n=33, %53,22) hukuksal olarak suç olduğunu düşündüğü ve bu fiili etik olarak da uygun bulmadığı görülmektedir. Bununla birlikte, katılımcıların bir bölümü (n=17, %27,42) konuya ilişkin fikrinin olmadığını belirtmişlerdir. Ancak eğitim sonrasında katılımcıların neredeyse tamamının (n=61, %98,38) hem hukuksal hem de etik açıdan düşüncelerinin beklendiği gibi değişmiş olduğu görülmektedir.

Fikir ve Sanat Eserlerine İlişkin Suçlar

Fikir ve Sanat Eserleri Kanunu'nun 71/1. maddesinde, bir eserin hak sahibi kişilerin yazılı izni olmaksızın işlenmesi, çoğaltılması, yayımlanması ya da ödünç vermek suretiyle yayılması hakkında cezaya hükmedilmesi düzenlenmiştir. Bu kapsamda katılımcılara yöneltilen sorular ve bu sorulara "katılıyorum" yanıtını veren katılımcıların hukuksal ve etik kabullenme durumlarına ilişkin betimsel istatistikler Tablo 4'te sunulmaktadır.

Tablo 4. Fikir ve Sanat Eserlerine İlişkin Hukuksal ve Etik Kabullenme Durumu

Bilişim suçu / Etik ihlali	Hukuksal olarak suç olduğunu düşünüyorum				Etik olarak uygun bulmuyorum			
	Öntest		Sontest		Öntest		Sontest	
	n	%	n	%	n	%	n	%
Genel Kamu Lisansına (GPL) sahip işletim sistemlerinin (Linux vb.) bireysel amaçlar için kullanılması	17	27,41	7	11,29	15	24,19	9	14,51
Bilimsel kitapların kütüphane sistemleri üzerinden ücretsiz olarak ödünç verilmesi	13	20,96	0	0	9	14,51	0	0
Belgesel türündeki bir filmin orijinal DVD'sinin ödünç verilmesi	7	11,29	58	93,54	10	16,12	18	29,03
Başkasına ait eser mahiyetinde olmayan mektup ve hatıraların yayınlanması	32	51,61	54	87,09	49	79,03	56	90,32

Tablo 4 incelendiğinde; öntest aşamasında genel kamu lisansının kullanımının, katılımcıların %27,41'i (n=17) hukuksal olarak suç olabileceğini, %24,19'u (n=15) ise etik açıdan doğru bulmadıklarını belirtmişlerdir. Bunun yanı sıra bu soruya ilişkin hem hukuksal hem de etik açıdan fikrinin olmadığı belirten %30,64 (n=19) oranında bir katılımcı olduğu görülmektedir. Eğitim sonrasında uygulanan sontest aşamasında ise fikrinin olmadığını belirten katılımcı bulunmamaktadır. Benzer şekilde "bilimsel kitapların kütüphane sistemleri üzerinden ücretsiz olarak ödünç verilmesi" ve "belgesel türündeki bir filmin orijinal DVD'sinin ödünç verilmesi" fiillerini de öntest aşamasında hukuksal açıdan suç olarak değerlendiren ya da etik açıdan doğru olmadığını düşünen az sayıda katılımcı olmasına karşın, verilen eğitim ile edindikleri bilgiler doğrultusunda sontest aşamasında bu fiilleri suç olarak değerlendiren ya da etik açıdan doğru bulmayan katılımcı bulunmamaktadır. Özel hayata ve hayatın gizli alanına karşı suçlar genel olarak TCK'nın 9. bölümünde 132 ila 140. maddeleri arasında düzenlenmiş olmakla birlikte, hukuka uygunluk nedeni olmaksızın kişinin gizli ya da özel hayata ilişkin bilgileri içeren mektup ve hatıraların alenileştirilmesi Fikir ve Sanat Eserleri Kanunu'nun 85. maddesi gereğince kişilik hakkını ihlal etmektedir (Yıldız, 2019, s. 467-468). Bu çerçevede katılımcılara fikir ve sanat eseri

niteliği olmayan başkasına ait mektup ve hatıraların yayınlanması hakkındaki düşünceleri sorulmuştur. Öntest aşamasında katılımcıların sadece %51,61'i (n=32) bu fiilin hukuksal açıdan suç olduğunu belirtirken, %27,41'i (n=17) bu konuya ilişkin fikrinin olmadığını belirtmiştir. Sontest aşamasında ise fikri olmayan katılımcıların büyük bölümünün bu davranışı suç olarak değerlendirdiği ve suç olarak değerlendiren katılımcı oranının %87,09'a (n=54) yükseldiği görülmektedir. Etik algı açısından değerlendirildiğinde ise hem öntest (n=49, %79.03) hem de sontest (n=56, %90,32) aşamasında katılımcıların çok büyük bir bölümünün bu davranışı etik bulmadığı görülmektedir.

DEĞERLENDİRME VE SONUÇ

Üniversitelerde bilişim hukuku eğitiminin verilmesi; özellikle bilginin elde edilmesi, işlenmesi, saklanması, muhafaza edilmesi, transfer edilmesi ve imha edilmesine yönelik süreçleri yakından takip eden bilişim sistemleri ve bilgi yönetimi alanlarından mezun olacak öğrenciler için büyük önem taşımaktadır. Zira elektronik ortamda bilginin işlenmesine yönelik tüm süreçlerin bilişim hukukuna uygun olarak işlemesi temel bir zorunluluktur. Bu nedenle bilgi yöneticilerinin ve bilişim sistemleri personelinin etik kabullenmenin de ötesinde, bilişim hukuku mevzuatı çerçevesinde uymak zorunda oldukları sorumluluklar bulunmaktadır.

Çalışma kapsamında elde edilen bulgular ışığında genel bir değerlendirme yapıldığında; uygulanan eğitim sonrasında katılımcıların tüm bilişim suçlarına yönelik düşüncelerinin değişmiş olduğu ve hukuksal çerçevede bilişim suçlarını tanımlayabildikleri görülmektedir. Sontest aşamasında katılımcıların ankette yer alan sorularda tanımlanan eylemleri bilişim suçu olup olmadıkları konusunda ayrıştırabilmeleri, hukuksal çerçevede verilen eğitimin ana hedefine ulaştığını ve katılımcılarda istendik davranış değişikliğini oluşturduğunu göstermektedir. Bununla beraber katılımcıların eğitim sonrasında hukuksal açıdan düşünceleri değişmesine karşın, bazı fiillere karşı etik açıdan yaklaşımında belirgin bir değişim olmamıştır. Örneğin, katılımcıların fikir ve sanat eserlerine ilişkin hukuksal yaklaşımları eğitim sonrasında büyük oranda değişirken, özellikle "belgesel türündeki bir filmin orijinal DVD'sinin ödünç verilmesini" katılımcıların büyük bölümünün etik açıdan yanlış bir davranış olarak nitelendirmedikleri görülmektedir. Ancak bu etik yaklaşım, katılımcılarda istenilen hukuksal farkındalığın oluşmasına engel olmamıştır. Elde edilen bulgular, katılımcıların sontest aşamasında yöneltilen sorulara hem hukuksal hem de etik

açıdan bilinçli bir şekilde yanıt verdiklerini göstermektedir. Uygulanan eğitim öncesinde bazı eylemlerin hukuksal olarak suç olup olmadığı ya da etik açıdan uygunluğu konusunda fikrinin olmadığını beyan eden katılımcıların, eğitim sonrasında büyük oranda fikir sahibi olduğu görülmektedir. Özellikle sorularda belirtilen eylemlerin hukuksal olarak suç olup olmadığı konusunda tereddüt yaşayan katılımcıların hemen hemen tamamı, eğitim sonrasında bu eylemleri suç olarak tanımlayabilmişlerdir.

Bu çalışmada uygulanan öntest ve sontest sonuçları arasındaki farklılıklar, genel olarak şu çıkarımların elde edilmesini sağlamıştır:

Bilişim hukuku eğitimi katılımcıların hem hukuksal yaklaşımlarında hem de etik yaklaşımında büyük ölçüde istendik değişiklikler yaratmıştır.

Eğitim öncesinde genel olarak hukuksal açıdan fikri olmayan ya da bilgi sahibi olmayan katılımcı oranının çok yüksek olması, özellikle meslek alanı ile ilgili olarak seçilen katılımcı grubunun meslek hayatında bilişim hukukuna ilişkin sorunlarla karşılaştıklarında zorlukların yaşanabileceğini göstermektedir.

Eğitim öncesinde katılımcılar bazı bilişim suçları hakkında fikrinin olmadığını belirtmesine karşın, etik algılarıyla beklenen yaklaşımı göstermektedirler. Katılımcıların, çalışmanın bulgularında örnekleri verilen bu suçlara ilişkin etik açıdan doğru yaklaşımı benimsemeleri ise bu suçlara ilişkin hukuksal açıdan da doğru davranış biçimini sergilemesini sağlamaktadır. Bu durumun etik algının önemini işaret etmesi nedeniyle, özellikle mesleki etik ilkelerinin de katılımcıların bilişim hukuku algısına katkı sağlayacağı değerlendirilmektedir.

Eğitim sonrasında katılımcıların genel olarak hukuksal yaklaşımlarında bilişim hukuku mevzuatına uygun olarak değişim görülmesine rağmen, bazı fillere karşı etik kabullenmelerinde değişikliğin olmadığı görülmektedir. Bu durum ise etik kabullenmenin bilişim hukukuna ilişkin eksik ya da yanlış bilgiyi her koşulda ikame edemeyeceğini göstermektedir. Dolayısıyla, bilişim hukukuna ilişkin bilgi eksikliğinin devam etmesi halinde, etik algıya bağlı olarak katılımcıların belirli konularda hukuksal olarak hatalı işlem yapma olasılığının da bulunduğu göz ardı edilmemelidir. Bu çerçevede bilişim hukuku eğitimleri ile mesleki etik ilkelerine ilişkin eğitimlerin birbirini tamamladığı, ancak tek başına yeterli olmadığı düşünülmektedir.

Bu çalışmanın katılımcıları, mesleki hayatları boyunca bilişim hukukuna ilişkin mevzuatı bilmek ve uygulamak zorunda olan ve nispeten daha bilinçli olması gerektiği düşünülen gruplardan biri olan Yönetim Bilişim Sistemle-

ri Bölümü son sınıf öğrencileri arasından seçilmiştir. Çalışmada çok geniş bir mevzuat içinden temel ve sınırlı sayıda bilişim suçuna ilişkin sorular örneklendirilerek katılımcılara yöneltilmiş ve hem hukuksal hem de etik açıdan yaklaşımları değerlendirilmiştir. Bilişim hukuku mevzuatı çok geniş olmakla birlikte, dijitalleşen dünyada belirli oranlarda bilgi toplumunun tüm kesimlerini ilgilendirmekte ve etkilemektedir. Bu nedenle, benzer araştırmaların toplumun diğer kesimlerinde de yapılmasının ve elde edilen sonuçlara bağlı olarak görülen bilgi eksikliği sorununun yaşam boyu öğrenme stratejisi kapsamında değerlendirilmesinin faydalı olacağı değerlendirilmektedir.

KAYNAKLAR

Aiken, M., Davidson, J. & Amann, P. (2016). *Youth pathways into cybercrime*. Erişim adresi: https://www.ucd.ie/geary/static/publications/Pathways_White_Paper.pdf

Avrupa Komisyonu. (2020). *Data protection: Better rules for small business*. Erişim adresi: https://ec.europa.eu/justice/smedataprotect/index_en.htm

Avrupa Konseyi. (2001a). *Explanatory report to the convention on cybercrime*. Erişim adresi: https://rm.coe.int/16800cce5b

Avrupa Konseyi. (2001b). *Siber suç sözleşmesi*. Erişim adresi: https://rm.coe.int/1680081561

Babbie, E. (2010). *The practice of social research* (12 bs.). USA: Wadsworth, Cengage Learning.

Balajanov, E. (2018). Setting the minimum age of criminal responsibility for cybercrime. *International Review of Law, Computers & Technology, 32*(1), 2-20.

Boateng, R., Longe, O. B., Mbarika, V. W., Avevor, I. & Isabalija, S. R. (2010). *Cyber crime and criminality in Ghana: Its forms and implications.* Erişim adresi: https://t.ly/RtaR

Boz, B. (2016). *Ceza hukukunda nedensellik bağı.* (Yayımlanmamış yüksek lisans tezi). Yıldırım Beyazıt Üniversitesi, Ankara.

Calder, A. & Watkins, S. (2020). *IT governance: An international guide to data security and ISO 27001/ISO 27002* (7 bs.). United Kingdom: Kogan Page.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet*. United States: Elsevier Science Publishing Co Inc.

Duncan, G. T., Jabine, T. B. & Wolf, V. A. (1993). *Private lives and public policies: Confidentiality and accessibility of government statistics*. Washington, D.C.: National Academy Press.

Dülger, M. V. (2004). *Bilişim suçları*. Ankara: Seçkin Yayıncılık.

Eriş, U. (2011). Türkiye'de kırıcı (hacker) kültürü. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi, 2*, 22-44.

Henkoğlu, T. (2015). *Bilgi güvenliği ve kişisel verilerin korunması*. Ankara: Yetkin Hukuk Yayınları.

Henkoğlu, T. & Şerefoğlu, H. (2019). Yönetim bilişim sistemleri bölümü öğretim programlarının bilgi yönetimi açısından değerlendirilmesi. *Yükseköğretim ve Bilim Dergisi*, 9(3), 587-602.

Hodeghatta, U. & Nayak, R. (2014). *The infosec handbook: An introduction to information security*. Berkeley, CA: Apress.

ISO. (2013). *ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements*. Erişim adresi: https://t.ly/kIhA

International Telecommunication Union. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. Erişim adresi: https://t.ly/Fo1t

Johnson, J. (2021). *Internet use by age group worldwide as of November 2019*. Erişim adresi: https://t.ly/my5e

Karagülmez, A. (2009). *Bilişim suçları ve soruşturma - kovuşturma evreleri* (2 bs.). Ankara: Seçkin Yayıncılık.

Kaur, S., Sharma, S. & Singh, A. (2015). Cyber security: Attacks, implications and legitimations across the globe. *International Journal of Computer Applications, 114*(6), 21-23.

Kaya, İ. S. & Çakır, A. (2020). Yasak cihaz veya programlar suçu. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 19*(2020/2), 32-55.

Köksal, A. (2006). Eniac'ın 60. yılında TBD 35 yaşında. *Bilişim Kültürü Dergisi, 35*(93), 24-28.

Kişisel Verileri Koruma Kurumu. (2021). *Rehberler*. Erişim adresi: https://www.kvkk.gov.tr/Icerik/2030/Rehberler

McCumber, J. (2005). *Assessing and managing security risk in IT systems: A structured methodology*. United States: Auerbach Publications.

Murphey, D. (2019). *A history of information security*. Erişim adresi: https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

News Room. (2015). *Average age of cyber-crime suspects falls to 17*. Erişim adresi: https://t.ly/NfpR

Öman, S. (2010). *Implementing data protection in law*. Erişim adresi: https://t.ly/s9VK

PandaSecurity. (2018). *Types of cybercrime*. Erişim adresi: https://t.ly/Eevz

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3 bs.). Thousand Oaks, CA: Sage.

Radware. (2020). *The 2019–2020 global application & network security report*. Erişim adresi: https://t.ly/qOf4

Riccardi, J. L. (1983). The German Federal Data Protection Act of 1977: Protecting the right to privacy? *Boston College International and Comparative Law Review, 6*(1), 243-271.

Rubin, A. & Babbie, E. R. (2011). *Research methods for social work* (7 bs.). Belmond: Cengage Learning.

Statista. (2017). *Consumer loss through cyber crime worldwide in 2017, by victim country (in billion U.S. dollars)*. Erişim adresi: https://t.ly/1Fj0

TCK. (2004). Türk Ceza Kanunu. Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf

TMK. (2001). Türk Medeni Kanunu. Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf

Türkiye İstatistik Kurumu. (2021). *Bireylerin yaş grubuna ve cinsiyetine göre bilgisayar ve internet kullanım oranları*. Erişim adresi: http://www.tuik.gov.tr/PreIstatistikTablo.do?istab_id=2600

Türk Ceza Kanunu Gerekçesi. (2004). *Türk Ceza Kanunu Genel Gerekçesi*. Erişim adresi: https://t.ly/G8Lv

Westin, A. F. (1976). *Computers, health records, and citizens rights*. Washington, D.C.: Government Printing Office.

Yargıtay. (2012). *Yargıtay 12 CD E.2012/20608, K.2012/18217*. Erişim adresi: https://t.ly/X6MO

Yargıtay. (2014a). *Yargıtay 12 CD E.2013/13614, K.2014/5809*. Erişim adresi: https://t.ly/MLEx

Yargıtay .(2014b). *Yargıtay 12 CD E.2013/22599, K.2014/12706.* Erişim adresi: https://t.ly/kajQ

Yargıtay. (2014c). *Yargıtay 12 CD E.2013/26087, K.2014/10205*. Erişim adresi: https://t.ly/Bp5A

Yıldız, O. A. (2019). Mektup, hatıra ve benzeri yazıların kişilik hakkı kapsamında korunması. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 25*(1), 450-470.

Yılmaz, F. & Güllüpınar, F. (2020). Türkiye'de bilişim suçlarının kriminolojik açıdan değerlendirilmesi: Bilişim suçlarının hukuksal ve sosyolojik boyutlarının analizi. *OPUS Uluslararası Toplum Araştırmaları Dergisi, 15*(10. Yıl Özel Sayısı), 5371-5409.