BİLGİ DÜNYASI
INFORMATION WORLD

e-ISSN: 2148-354X

Uzaktan Eğitim Sistemlerinde Kişisel Hakların Korunması: Türkiye'deki Üniversitelerin Koronavirüs Salgını (COVID-19) Sürecine Yönelik Değerlendirme

Protection of Personal Rights in Distance Education Systems: Evaluation of Universities Regarding Coronavirus Disease (COVID-19) Process

Türkay HENKOĞLU, Halise ŞEREFOĞLU HENKOĞLU

Makale Bilgisi / *Article Information*
Bu makaleye atıf yapmak için/ *To cite this article:*
Henkoğlu, T. ve Şerefoğlu Henkoğlu, H. (2021). Uzaktan eğitim sistemlerinde kişisel hakların korunması: Türkiye'deki üniversitelerin koronavirüs salgını (COVID-19) Sürecine yönelik değerlendirme. *Bilgi Dünyası, 22*(1), 65-98. doi: 10.15612/BD.2021.552

Makale türü / *Paper type:* Hakemli / *Refereed*
Araştırma Makalesi / *Research Article*

Doi: 10.15612/BD.2021.552

Geliş Tarihi / *Received:* 12.07.2020
Kabul Tarihi / *Accepted:* 16.05.2021
Elektronik Yayınlanma Tarihi / *Online Published:* 30.06.2021

İletişim / Communication
Üniversite ve Araştırma Kütüphanecileri Derneği / University and Research Librarians Association
Posta Adresi / Postal Address: Marmara Sok. No:38/17 06420 Yenişehir, Ankara, TÜRKİYE/TURKEY
Tel: +90 312 430 03 61; Faks / Fax: +90 312 430 03 61; E-posta / E-mail: bilgi@bd.org.tr
Web: http://www.bd.org.tr/index.php/bd/index

Araştırma Makalesi

Uzaktan Eğitim Sistemlerinde Kişisel Hakların Korunması: Türkiye'deki Üniversitelerin Koronavirüs Salgını (COVID-19) Sürecine Yönelik Değerlendirme

Türkay HENKOĞLU, Halise ŞEREFOĞLU HENKOĞLU***

Öz

Koronavirus salgını (COVID-19) nedeniyle üniversitelerde eğitim ve öğretime uzaktan eğitim sistemleri (UES) aracılığıyla devam edilmektedir. Bu süreçte UES kullanıcılarının kişisel hakların korunması ve bu sistemlere güven duymalarının sağlanması, UES'nin etkinliği ve başarısının ön koşulu olarak görülmektedir. Bu çalışmada, kişisel hakların korunması çerçevesinde UES'de kullanılan içeriğin eser sahibi, öğretim elemanları ve öğrencilere ilişkin yansımaları ile uzaktan eğitim merkezlerinin ve uzaktan eğitim faaliyetlerinde görev alan bilgi profesyonellerinin bu konudaki sorumluluklarının incelenmesi amaçlanmaktadır. Bu amaç doğrultusunda, UES'nin kullanımına yönelik kişisel haklar incelenmiş ve Türkiye'deki tüm üniversitelerin kullanmakta oldukları UES'lerin hukuksal koşullar ile uyumluluğu araştırılmıştır. Araştırma kapsamında Türkiye'deki 200 üniversitenin web sitelerinde yer alan uzaktan eğitim sürecine ilişkin açıklamalar, haber ve duyuru metinleri, kullanım kılavuzları (rehberler) ve uzaktan eğitim uygulama usul ve esaslarına ilişkin dokümanlar ile kullanıcıların kişisel haklarına yönelik hukuksal düzenlemeler incelenerek veri toplanmıştır. Elde edilen verilere bağlı olarak, kişisel hakların korunmasına ilişkin üniversitelerin sergilediği tutum, UES'de kişisel hakların korunmasına yönelik yaklaşımın hukuksal düzenlemeler ile uyumluluğu ve COVID-19 salgını sürecinde kişisel hakların korunmasına yönelik hukuksal sorumluluklar çerçevesinde alınan güvenlik önlemlerinin yeterliliği değerlendirilmiştir. Çalışmada elde edilen sonuçlar, hızlı bir geçiş süreci içinde geliştirilen UES çözümlerinin kişisel hakların korunması konusunda yetersiz olduğunu ve özellikle verilerin saklanmasına yönelik asgari güvenlik standartlarının belirlenmesine ihtiyaç duyulduğunu göstermektedir. Çalışmanın son bölümünde, uzaktan eğitim sürecine katılım sağlayan ve farklı hukuksal sorumlulukları bulunan öğrenciler, öğretim elemanları, veri sorumlusu, bilgi profesyonelleri, uzaktan eğitim merkezi yetkilileri ve Yükseköğretim Kurulu'nun göz önünde bulundurması gereken birçok farklı noktaya dikkat çekilerek önerilerde bulunulmuştur.

Anahtar sözcükler: *COVID-19, uzaktan eğitim, kişisel veriler, kişisel haklar, telif hakları.*

* Sorumlu Yazar, Dr. Öğr. Üyesi, Aydın Adnan Menderes Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, turkay.henkoglu@adu.edu.tr

** Dr. Öğr. Üyesi, Aydın Adnan Menderes Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, halise.serefoglu@adu.edu.tr

Research Article

Protection of Personal Rights in Distance Education Systems: Evaluation of Universities Regarding Coronavirus Disease (COVID-19) Process

*Türkay HENKOĞLU**, *Halise ŞEREFOĞLU HENKOĞLU***

Abstract

Because of coronavirus (COVID-19) pandemic, universities have begun distance education through learning management systems (LMS). Protecting the personal rights of LMS users and ensuring their trust to these systems are seen as a prerequisite for the effectiveness and success of LMS. In this study, it is aimed to investigate the reflections of content used in LMS on the author, academic staff and students within the framework of personal rights protection, and to examine the responsibilities of distance education centers and information professionals taking part in these centers. For this purpose, personal rights for the use of LMS were examined and different LMS used by all universities in Turkey were compared with the legal conditions. In the study data were collected by examining the explanations, news and announcements, user manuals/guides, documents on the principles and procedures of distance education and the legal regulations regarding the personal rights of users published on web sites of 200 universities in Turkey. Based on collected data, the attitudes of universities towards the protection of personal rights, the compatibility between the approach for the protection of personal rights in the LMS is and legal regulations, and adequacy of security measures taken within the context of legal responsibilities for the protection of personal rights during the COVID-19 pandemic were investigated. The findings of the study show that, LMS solutions developed in the rapid transition to distance education are insufficient for protecting personal rights and there is an urgent need to set minimum security standards especially for data storage. In the final part of the study, attention was drawn to many different points that should be taken into consideration by the participants of LMS, who have different legal responsibilities, including students, academic staff, data controller, information professionals, distance education center officials and the Council of Higher Education.

Keywords: *COVID-19, distance education, personal data, personal rights, copyright.*

* Corresponding author, Asst. Prof., Aydın Adnan Menderes University, Department of Management Information Systems, turkay.henkoglu@adu.edu.tr

** Asst. Prof., Aydın Adnan Menderes University, Department of Management Information Systems, halise.serefoglu@adu.edu.tr

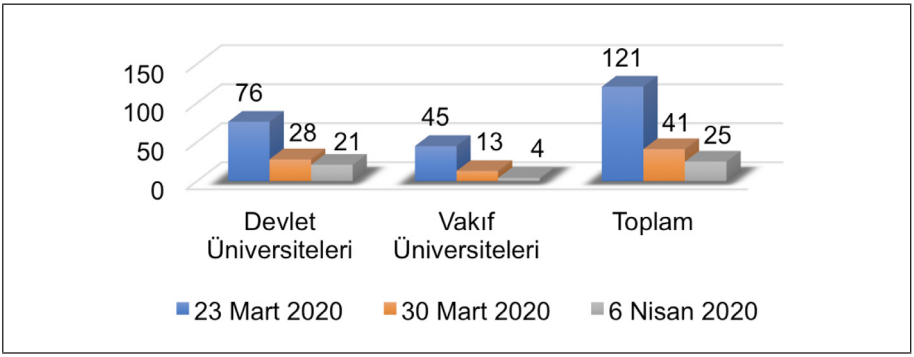
Giriş

Bilgi ve iletişim çağında elektronik ortamda yer alan bilgilerin gizliliğinin sağlanmasına yönelik risklerin ve bu ortamlarda işlenen bilgiler üzerinden kişisel haklara yönelik tehditlerin arttığı görülmektedir. Bu durum bilgi yönetim süreçlerinin her aşamasında veri koruma hukukunu da dikkate almayı zorunlu hale getirmektedir. Koronavirüs (COVID-19) salgını ile birlikte bütün eğitim kurumlarının uzaktan eğitim sürecine zorunlu olarak dahil olması, eğitim kurumlarındaki bilgi yönetim süreçlerine yeni bir boyut kazandırmış ve bu kurumlara veri koruma hukuku çerçevesinde yeni sorumluluklar getirmiştir.

Asya, Avrupa, Orta Doğu ve Amerika'da hızla yayılan COVID-19, 11 Mart 2020 tarihinden itibaren Türkiye'de de görülmeye ve yayılmaya başlamıştır. Tüm dünya ülkelerinde olduğu gibi (Dwivedi ve diğerleri, 2020; He ve diğerleri, 2021) Türkiye'de de sürecin başında bulaşı risklerini azaltmak amacıyla eğitim kurumlarında yüz yüze eğitime ara verilmesi kararı alınmıştır. Türkiye'de COVID-19 önlemleri kapsamında Yükseköğretim Kurulu (YÖK) tarafından üniversiteler 16 Mart 2020 tarihinden itibaren üç hafta süreyle tatil ilan edilmiştir (YÖK, 2020a, s.1). Salgının gelişimine bağlı olarak da 23 Mart 2020 tarihinden itibaren uzaktan eğitim kapasitesine sahip olan üniversitelerin uzaktan eğitim sürecine başlamaları kararı alınmıştır (YÖK, 2020b, s.4). Aynı zamanda sürecin desteklenmesi amacıyla YÖK'ün "Açık Bilim ve Açık Erişim" politikasının da ürünü olan "YÖK Dersleri Platformu" üniversite öğrencilerinin erişimine açılmıştır (YÖK, 2020c). Bu kararın ardından, Türkiye genelinde birçok üniversite 30 Mart 2020 tarihinden itibaren etkileşimli derslerin de yapılmasını sağlayacak uzaktan eğitim sistemleri (UES) için oldukça yoğun bir yapılanma sürecine girmiş ve dijital imkânlar ile uzaktan öğretim süreci başlamıştır. Bununla beraber, YÖK'ün (2020d) sürece ilişkin almış olduğu kararlar çerçevesinde, örgün öğretimde uzaktan öğretimle verilebilecek ders oranı %40'a çıkarılmış, örgün öğretimdeki her bir programın derslerinin en az %10'unun uzaktan öğretim ile verilmesi tavsiye edilmiş ve uzaktan eğitim merkezlerinde görevlendirilmek üzere ek kadro tahsisi yapılabileceği belirtilmiştir. YÖK (2020e) tarafından küresel salgın sürecinde üniversitelerdeki uzaktan öğretim uygulamalarına ilişkin yapılan bir anketten elde edilen verilere göre; Türkiye'deki 187 üniversite 23 Mart 2020 ve 6 Nisan 2020 tarihleri arasında uzaktan öğretime başlamıştır (Şekil 1). Bununla beraber, aynı anketten elde edilen verilere göre uzaktan öğretime geçiş yapan bu üniversitelerde, 2019-2020 eğitim öğretim yılı bahar dönemindeki derslerin %90,1'i uzaktan öğretim yoluyla verilmiştir.

Şekil 1

Üniversitelerin Uzaktan Eğitim Uygulamalarına Başlama Tarihleri (YÖK, 2020e)



UES'lerde öncelikli amaç, meşru erişim hakkı bulunan öğrencilerin sisteme istedikleri yerden ve istedikleri zamanda erişimlerinin sağlanmasıdır. Bu sistemlerin hukuka aykırı erişimleri reddetmesi ve sisteme giriş yapabilen kişilerin ise sadece yetkilendirildiği bilgilere erişebilmesi gerekmektedir (Romansky, 2014). COVID-19 salgını nedeniyle tüm dünyada eğitim kurumlarının, eğitim ve öğretim faaliyetlerini kesintisiz devam ettirebilmeleri amacıyla öncelikle derslerin senkron/etkileşimli (eş zamanlı) ya da asenkron (eş zamanlı olmaksızın) yöntemlerle yapılabilmesi için güvenilir altyapıya sahip araçlara ihtiyaç duyduklarını söylemek mümkündür. Bu süreçte Türkiye'de de birçok yükseköğretim kurumunun uzaktan eğitim altyapılarının geliştirilmesi gereken yönlerinin olduğu görülmektedir (YÖK, 2020d). Bazı üniversiteler[1] COVID-19 sürecini, "acil durum uzaktan öğretim" dönemi olarak tanımlamaktadır. Türkiye'deki üniversitelerde birkaç haftalık hazırlığın ardından UES'lere hızlı bir geçiş yapılma zorunluluğunun oluşması nedeniyle, birçok eğitim kurumu Google, Microsoft gibi güçlü ve küresel çapta altyapı sunan dijital şirketlerin çözümlerine yönelmişlerdir.

COVID-19 salgınının öğrenciler ve üniversiteler üzerindeki olumsuz etkisini en aza indirgemek için kritik bir öneme sahip olan UES'ler, kişisel verileri yöneten bilgi sistemleri olarak kişisel hakların korunmasına yönelik hukuksal düzenlemelere uygun olarak kullanılmalıdır (Pehlivanova ve Kanchev, 2020, s.291). Uzaktan eğitime hızlı geçiş sürecinin gizliliğin korunmasına yönelik kalıcı etkilerinin olabileceği alanyazındaki birçok çalışmada ele alınmış ve duyulan endişe ortaya konulmuştur (Dwivedi ve diğerleri, 2020). Uzaktan eğitim sürecinde sıklıkla başvurulan Microsoft Teams, Zoom ve Google Meet, Google Classroom gibi platformlar, asgari düzeyde öğrenci ve öğretim elemanlarının isimleri, e-posta adresleri, çerezlerle elde edilen verileri ve/veya diğer çevrimiçi tanım-

1 http://www.huzem.hacettepe.edu.tr/files/HUZEM_B%C4%B0LG%C4%B0LEND%C4%B0RME_%C3%96GR_ELM.pdf

layıcılar aracılığıyla toplanan verileri kullanabilmektedir (Orchison ve Rigg, 2020). COVID-19 sürecinde Google Classroom ve Zoom gibi uygulamalara ilişkin "hukuka aykırı olarak kişisel verileri topladığı" gerekçesiyle açılan ve sayısı giderek artan davalar, bu konudaki risk ve zorlukların önemli bir göstergesidir. Örneğin, Amerika Birleşik Devletleri (ABD)'nin New York gibi bazı şehirlerinde bahsi geçen bu uygulamalara bağlı video konferans araçlarının, artan bu tür endişeler nedeniyle yasaklandığı görülmektedir. Öğrenci yaklaşımına bakıldığında da kişisel hakların ihlal edildiği yönünde algı oluştuğu gözlenmektedir. Florida Eyalet Üniversitesi'nde 5.000'den fazla öğrencinin vermiş olduğu dilekçede, öğrencilerin "web etkinliğine ve mobil cihazlara yönelik bilgiler ile sınav etkinliğinde kamera/mikrofon donanımına erişim işlemlerinin" kayıt altına alınmasının mahremiyetin ihlali olduğu öne sürülmektedir (Ballard Spahr LLP, 2020). Benzer şekilde, ABD'de Aile Eğitim Hakları ve Gizlilik Yasası (Family Educational Rights and Privacy Act – FERPA) gereğince öğrencilerin video konferans görüntülerinin işlenmesine ilişkin ebeveyn izni ya da 18 yaş üzerinde olma durumuna bağlı olarak öğrencinin onayının alınması gerekmektedir (Mannino, 2018; Student Privacy Policy Office, 2020).

Üniversitelerin, uzaktan eğitim uygulamalarının ve bunları kullanan kişilerin gizlilik düzenlemelerine uymasını sağlayarak, öğrencilerin ve öğretim elemanlarının verilerini koruma sorumluluğu bulunmaktadır. Bunun için en uygun yöntemin ise, doğru yazılımın seçilmesi ve bu yazılımın hukuksal düzenlemelere uygun olarak kullanılması olduğu görülmektedir (Manfuso, 2020; Pehlivanova ve Kanchev, 2020, s.291). UES'ler bir dizi hukuka aykırı eylem için uygun bir ortam oluşturmaktadır. Bunlardan bazıları; öğrenci ve öğretim elemanlarının kişisel verilerine yönelik tehditler, kimlik hırsızlığı, fikir ve yeniliklerin çalınması, sistem üzerindeki verilerde yapılan değişiklikler, sosyal mühendislik etkinlikleri, temel güvenlik tehditleri (virüsler, casus yazılımlar, kimlik avı, reklam yazılımları, truva atları vb.), telif haklarına yönelik hususlar ve etkileşimli derslerin yapıldığı UES'lere hukuka aykırı olarak girme işlemleridir (Romansky, 2014, s.4-5). Genel olarak UES üzerinde kişisel verilerin korunması için veri sorumlusu, öğretim elemanları ve öğrencilerin dikkate almaları gereken birtakım hususlar bulunmaktadır (Poland Personal Data Protection Office, 2020a; 2020b). Bunların UES'nin erişimi, kullanımı ve verilerin saklanması açısından farklı sonuçları olabilmektedir. UES'lerin birçoğunun arayüzü üniversiteler tarafından geliştirilirken, özellikle veri depolama amacıyla sosyal medya ve bulut tabanlı diğer farklı uzaktan eğitim araçları yaygın olarak tercih edilmektedir (Institute of Electrical and Electronics Engineers, 2014; Romansky, 2014).

Uzaktan eğitim faaliyetlerine ilişkin hukuksal koşulların incelendiği ve alınan kararlarla hukuksal düzenlemelerin uzaktan eğitim faaliyetlerin yürütülmesinde nasıl karşılık bulduğuna yönelik önemli ipuçları sunan bu çalışmanın, kurumlarında uzaktan eğitim faaliyetlerinde görev alan bilgi profesyonelleri ile birlikte, üniversitelerin uzaktan eğitim merkezleri ve bilgi ve belge yönetimi bölümlerinin hem uygulama hem de uzaktan eğitim süreçlerine yönelik çalışmaları için temel teşkil edecek yeni bir bakış açısı sunacağı düşünülmektedir. Bilginin elde edilmesinden imhasına kadar olan tüm bilgi yönetim

süreçlerinde olduğu gibi, uzaktan eğitim süreçlerinde de hukuka aykırı işlemlerin bir seçenek olarak değerlendirilmesi ya da uygulanması mümkün olamamaktadır. Bu nedenle çalışmanın alanyazına katkı sağlayarak, uzaktan eğitim birimi personeli, uzaktan eğitim süreçlerinde veri sorumlusu adına ya da doğrudan verilerin işlenme süreçlerinde sorumluluklar alan bilgi profesyonelleri ve UES kullanıcılarında farkındalığı ve duyarlılığı arttıracağı düşünülmektedir.

Uzaktan Eğitim Sistemlerinde İşlenen Verilerin Hukuksal Koşulları

UES, öğrencilere uzaktan erişim imkânı ve farklı türlerdeki öğretim materyalleri kullanılarak farklı mekânlardan öğrenme sürecine katılma fırsatı sunmaktadır. Buna bağlı olarak, bu sistemlerin ve prosedürlerinin gizlilik ve güvenlik sorunlarının öneminin artırdığını söylemek mümkündür. Birçok UES'de, kişisel olarak tanımlanabilir bilgilerin toplanması, işlenmesi, bakımı, paylaşılması ve korunmasına ilişkin karar verilmesi gereken sorunlar bulunmaktadır. ABD ve Avrupa Birliği (AB)'nin uzaktan eğitim sistemlerinde kişisel hakların korunmasına yönelik hukuksal koşullarına genel olarak bakıldığında, yapılan düzenlemelerin uygulanması ve etki alanları açısından farklılıkların olduğu görülmektedir. AB içinde konuya ilişkin tüm uygulamalar, veri koruma mevzuatının özünü oluşturan AB Genel Veri Koruma Tüzüğü (General Data Protection Regulation – GDPR) kapsamında yapılmakta ve her AB vatandaşı bu çerçevede kendisine ait verilerin GDPR'a uygun olarak işlenmesini talep edebilmektedir (Anwar, 2020, s.12). Bununla beraber Avusturya'daki Graz Teknoloji Üniversitesi örneğinde olduğu gibi, GDPR'a katı bir şekilde uyulması nedeniyle, e-öğrenme hizmetleri, kullanılan teknolojiler ve uygulamalara ilişkin dokümantasyonun da ayrıntılı olarak hazırlandığı görülmektedir (Ebner ve diğerleri, 2020). ABD'de ise eyaletlerin çoğunun GDPR yönelimli olarak eyalet düzeyinde kişisel gizlilik korumalarını geliştirmeye çalıştıkları görülmektedir. Örneğin Maryland'ın 2020 yasama oturumunda, eyaletteki kamu yüksek öğrenimi için GDPR benzeri beklentilere yanıt veren Maryland Yüksek Öğretim Veri Gizliliği Yasası kabul edilmiştir. Ancak ABD'de eyaletler arası yasaların düzensiz olduğu ve eyaletlerin yükümlülüklerini açık olarak belirleyen kapsayıcı bir federal yasanın olmadığı görülmektedir. Bu durumda bir üniversitede aynı dersi alan farklı eyaletlerdeki öğrencilerin, üniversite tarafından tutulan bilgilere yönelik olarak kendi eyaletlerindeki hukuksal düzenlemelerin uygulanacağı beklentisi oluşmaktadır (Spicer, 2020, s.2).

UES erişimi, içerik yönetimi ve bulut hizmetlerinin kullanımı gibi konularda veri koruma mevzuatına uygun işlemlerin yapılması gerekmektedir (Romansky, 2014). UES üzerinde ders sunumları, ders notları ve yardımcı dokümanların oluşturduğu içeriğin yanı sıra etkileşimli ders videoları da bulunabilmektedir. Bu sistemler üzerinde işlenen verilerin özelliğine bağlı olarak farklı hukuksal düzenlemeler kapsamında dikkate alınması gereken sorumluluklar bulunmaktadır. Bu sorumluluklar, ilgili öğretim elemanlarının dikkate alması gerekenler ile UES'nin işleme amaçlarını ve vasıtalarını belirleyen,

veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan veri sorumlularının dikkate alması gereken sorumluluklar açısından iki temel yaklaşım altında sınıflandırılabilmektedir.

Öğretim Elemanları ve Öğrencilere İlişkin Hukuksal Sorumluluklar

Öğretim elemanlarının ve öğrencilerin UES üzerinde kullanmış oldukları ders içeriğine yönelik hukuksal sorumluluklar ağırlıklı olarak telif hakları hukuku ve 5846 Sayılı Fikir ve Sanat Eserleri Kanunu (FSEK, 1951) çerçevesinde değerlendirilmektedir. Bununla beraber, etkileşimli derse katılım sağlayan öğrencilerin derste hazır bulunma durumuna yönelik bilgiler de kişisel verilerin korunması açısından ilgili öğretim elemanı ve üniversite tarafından dikkate alınması gereken hususlar arasında yer almaktadır.

FSEK (1951) çerçevesinde eser sahibinin haklarına yönelik olarak değerlendirilebilecek izin ve/veya ihlaller, yüz yüze eğitim ve/veya uzaktan eğitim açısından genel olarak yaklaşımda herhangi bir farklılık oluşturmamaktadır. Ancak eser sahiplerini korumaya yönelik güçlü eğilim, FSEK'de yer alan eğitim istisnasına yönelik uygulamalarda bazı tereddütlerin oluşmasına neden olmaktadır. FSEK eser sahipliğinden doğan hakları korumakla birlikte, kamu yararı içinde değerlendirilen eğitim alanına yönelik bazı istisnalar içermektedir. Bu istisnalardan biri olan "temsil serbestisi" FSEK'in 33'üncü Maddesinde düzenlenmiştir. Temsil serbestisi, "yayımlanmış bir eserin; tüm eğitim ve öğretim kurumlarında, yüz yüze eğitim ve öğretim maksadıyla doğrudan veya dolaylı kâr amacı gütmeksizin temsili, eser sahibinin ve eserin adının mutat şekilde açıklanması şartıyla" serbest olmasıdır (FSEK, 1951, s.2402). Ancak bu temsilin gerçekleşmesi için gerekli şartlar arasında "yüz yüze eğitim ve öğretim maksadının" bulunuyor olması dikkat çekicidir. Mevcut haliyle uzaktan eğitim yönteminin, Kanun'un ilgili maddesinde belirtilen temsil serbestisinden yararlanamayacağı değerlendirilmektedir (Yıldız, 2019, s.859). Eğitimin yüz yüze ya da uzaktan yapılması temsil açısından önem taşımaktadır. Normal koşullarda UES ile eğitim veren bir kurumun yüz yüze yapılmasını öngördüğü derslerde bir eserin temsile konu olmasında herhangi bir sorun olmadığı görünmektedir. Ancak, tam tersi bir durumda normal koşullarda yüz yüze eğitim yapan bir eğitim kurumunda internet vb. iletişim araçları üzerinden eserin temsile konu olmasının, ilgili madde açısından tartışmalı olduğu görülmektedir. Bununla beraber, temsil serbestisinin oluşabilmesi için eserin yayımlanmış olması, temsilin eğitim kurumunda gerçekleşmesi, doğrudan veya dolaylı kâr amacı güdülmemesi ve eser sahibinin ve eserin adının mutat şekilde açıklanması şartlarının da yerine getirilmesi gerekmektedir (FSEK, 1951).

FSEK'in (1951) 35'inci Maddesinde düzenlenmiş olan "iktibas serbestisi" de eğitim ve öğretime ilişkin dikkate alınması gereken bazı istisnaları içermektedir. İktibas (alıntı), bir eserin değiştirilmeden başka bir esere alınması, parçalarından yararlanılmasıdır (alıntı, t.y.). FSEK'de, yeni bir eser oluşturulurken, yararlanılan eserden sınırlı ölçüde ve belir-

tilen kurallara uygun bir şekilde yararlanmanın mümkün olabileceği belirtilmektedir. İktibasın amacı aşması ya da yararlanılan eser sahiplerinin isimlerinin ve yararlanılan kısımların belirtilmemesi halinde "yolsuz iktibas" ortaya çıkmaktadır. İktibasın amacı aşmamasına rağmen şekle yönelik olarak usulüne göre kaynak gösterilmeden yapılan yolsuz iktibas, aynı zamanda başkasına ait bir eseri kısmen ya da tamamen kendisine mâl etmek ya da kendisininmiş gibi göstermek şeklinde tanımlanan (aşırma, t.y.) intihal (aşırma) suçunu da oluşturmaktadır (Fikrî ve Sinaî Haklar Araştırma ve Uygulama Merkezi [FİSAUM], 2003, s.7-8). İktibas, derleyen kişiye başka bir eserden sınırlı bir ölçüde yararlanma imkânı sunmaktadır. FSEK'in 34'üncü Maddesinde ise maksadın haklı göstereceği bir nispet (oran) dahilinde iktibaslar yapılmak suretiyle eğitim ve öğretim amacıyla "seçme ve toplama" eserlerin vücuda getirilmesinin mümkün olduğu görülmektedir (Arslanlı, 1954, s.138). Başka bir ifadeyle, eğitim ve öğretim amacıyla maksadın haklı göstereceği nispetin aşılmaması önem taşımaktadır. Örneğin; derste kullanımının faydalı olacağı düşünülen bir eserin eğitim ve öğretim amacıyla da olsa kopyalanarak öğrencilere dağıtılması bu serbestinin dışında kalmaktadır. Nitekim bu tür uygulamalara yönelik farklı bir örnek niteliğinde olan Yargıtay (2000) kararında, bir şairin her kitabından örnek şiirler seçilirken %90'ın üzerinde iktibas yolunda işleme yapıldığı ve bunun FSEK'in 34'üncü Maddesindeki maksadın haklı göstereceği nispetin aşılması anlamına geldiği vurgulanmaktadır. Bununla beraber, FSEK'in 35'inci Maddesi kapsamında eser niteliği taşıyan bilimsel konferans ve derslerde iktibas yapılırken kullanılabilecek vasıtalara açıklık getirilmektedir (Arslanlı, 1954, s.139). Buna göre alenileşmiş güzel sanat eserlerinin, ilmi konferans veya derslerde, konuyu aydınlatmak için projeksiyon ve buna benzer vasıtalarla gösterilmesi mümkündür. Ayrıca verilen ders eser niteliğinde olmasa dahi, bir güzel sanat eserinin eğitim ve öğretim amacıyla FSEK'in 33'üncü Maddesinde belirtilen koşullara uygun olarak da temsili (projeksiyon vasıtasıyla gösterilmesi vb.) yapılabilmektedir. FSEK'in 35'inci Maddesi kapsamında kendisine iktibas yapılacak eser yararlanılan eser ile kıyaslandığında bağımsız/müstakil bir eser niteliğinde iken, FSEK'in 34'üncü Maddesi kapsamında eğitim ve öğretim amacıyla vücuda getirilen seçme ve toplama eser, yararlanılan eser ile kıyaslandığında bağımsız bir eser niteliği taşımamaktadır (FİSAUM, 2003, s.5).

FSEK (1951) kapsamında "münhasıran eser sahibine ait olan haklar" arasında yer alan işleme (Madde 21), çoğaltma (Madde 22), yayma (Madde 23), temsil (Madde 24), umuma iletme (Madde 25) hakkı, eğitim ve öğretime ilişkin olarak öğretim elemanlarının ve derse katılım sağlayan öğrencilerin dikkate almaları gereken başlıca maddeler arasında yer almaktadır. Eserlerin eğitim ve öğretim amacıyla kullanılması, sahibinin meşru menfaatlerine zarar vermemeli ve/veya eserden normal yararlanmaya aykırı olmamalıdır. Ancak bununla beraber, eğitim ve öğretim kavramlarının oldukça kapsamlı olması ve farklı yorumlanabilmesi nedeniyle, eğitim ve öğretim istisnasının kullanımı da tartışmalı hale gelebilmektedir (Bozgeyik, 2015, s.34). Örneğin, COVID-19 salgınına bağlı bir zorunluluk nedeniyle UES üzerinden yapılan eğitim ve öğretim faaliyetlerinin fiziksel olarak eğitim kurumu çatısı altında yürütülmemesi, bu düzenlemenin katı bir

şekilde yorumlanması halinde bir sorun olarak görülebilmektedir. Bu nedenle uzaktan eğitim açısından FSEK'in yeterince açık ve kapsamlı olmadığı düşünülmektedir.

Öğrencilerin ders içeriğine ilişkin her türlü bilgiyi eğitim ve öğretim amacı dışında kullanmaları ya da sosyal medya gibi ortamlarda paylaşmaları da kişilik hakkı ihlalini oluşturmaktadır. Bu tür paylaşımların hukuka uygun olarak yapılabilmesi için ilgili öğretim elemanının rızasının olması ve ilgili eğitim kurumuna ilişkin izin almayı gerektirecek herhangi bir içeriği barındırmaması gerekmektedir. Bu noktada öğretim elemanı tarafından hazırlanan dersin içeriğine ilişkin olarak ortaya çıkan hak ihlaliyle, öğrencilerin bu içeriği hukuka aykırı olarak yayımlaması neticesinde ortaya çıkan hak ihlalinin farklı suçların konusu olduğu göz ardı edilmemelidir. UES'lerin kullanımına bağlı olarak işlenen suçlar, Türk Ceza Kanunu'nun (TCK, 2004) 9'uncu bölümünde "özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altında düzenlenmiştir. Özellikle özel hayatın gizliliğini ihlal (134'üncü Madde), kişisel verilerin kaydedilmesi (135'inci Madde), verileri hukuka aykırı olarak verme veya ele geçirme (136'ncı Madde) ve bu suçların nitelikli halinin düzenlendiği (137'nci Madde) maddelerin, UES'lerin kullanımında dikkate alınması önem taşımaktadır. Bunun dışında Kanun'da düzenlenen, bilişim sistemine hukuka aykırı olarak girme (243'üncü Madde) ve sistemi engelleme, bozma, verileri yok etme veya değiştirme (244'üncü Madde) yoluyla işlenen suçlar da kişilik haklarının sisteme girme yetkisi bulunmayan kişiler tarafından ihlaline neden olabilecek fiiller arasında yer almaktadır. TCK'daki düzenlemelerin yanı sıra, kişilik haklarının zedelenmesinden zarar gören kişiler, Türk Borçlar Kanunu'nun (TBK, 2011) 58'inci Maddesi gereğince de uğradığı manevi zarara karşılık manevi tazminat ödenmesini isteyebilmektedirler.

Uzaktan Eğitim Sistemi Yöneticileri ve Veri Sorumlularına İlişkin Hukuksal Sorumluluklar

UES'lerde, öğrencilere yönelik kişisel verilerle ses ve görüntü gibi biyometrik veri kapsamında değerlendirilebilecek hassas veriler (özel nitelikli kişisel veriler) işlenmektedir (Kişisel Verileri Koruma Kurulu [KVK Kurulu], 2020). Bu nedenle, UES'lerin kullanımı için üniversiteler tarafından benimsenen teknik tercihler, kişisel hakların korunmasına yönelik farklı sonuçlara neden olabilmektedir. Etkileşimli ders videolarının kayıtlarının nerede tutulacağı, kimlik doğrulama işlemlerinin nasıl ve nerede yapılacağı, kullanıcılara sunulacak güvenlik seçeneklerinin kapsamı gibi birçok unsur için yapılan tercihler, kişisel hakların ihlaline yönelik riskler oluşturabilmektedir. Her ne kadar birçok üniversite yazılı ya da elektronik ortamda UES'nin kullanımına yönelik bir taahhütnameyle bazı hukuksal sorumlulukları öğretim elemanları ile paylaşma yöntemini tercih etse de 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK, 2016) kapsamındaki tüm hukuksal sorumlulukların bu yöntemle öğretim elemanlarına devredilmesi mümkün olmamaktadır. Veri sorumluları ve üniversiteyi temsilen UES veri işleme faaliyetlerinden sorumlu uzaktan eğitim merkezi; UES üzerinde işlenecek veri türleri, işlenme amacı, kullanım amaçları, veriyi kimlerin işleyeceği, verinin paylaşılıp paylaşılmayacağı, paylaşılacaksa kimlerle

paylaşılacağı ve ne kadar süreyle saklanacağının belirlenmesine yönelik hususlara karar vermektedir. Bu çerçevede KVKK'nın 12'nci Maddesi gereğince veri sorumlusunun, UES üzerinden kaydedilen kişisel verilere hukuka aykırı olarak erişilmesini önleme ve yeterli düzeyde güvenliği temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma zorunluluğu bulunmaktadır (Kişisel Verileri Koruma Kurumu [KVK Kurumu], 2018a; KVKK, 2016).

Google, Microsoft gibi yurt dışı kaynaklı şirketlerin bulut hizmet sağlayıcılar aracılığıyla sunmakta olduğu web arayüzü ve veri depolama hizmetleri üzerinde, uzaktan eğitim merkezlerinin ve öğretim elemanlarının tam olarak denetimi ve kapsamlı güvenlik seçeneklerini kullanabilmesi mümkün olamamaktadır. Örneğin, Google Meet uygulamasında etkileşimli oturum linkine sahip olan herhangi bir kişinin, derse katılım sağlayan herhangi bir öğrencinin onayı ile derse girebilmesi mümkün olabilmektedir. Bu tür UES'lerde kullanılan toplantı yazılımlarının çoğunun güvenliği öncelemediği (O'Leary, 2020, s.5), istenmeyen misafirlerin etkileşimli derslere dâhil olabildiği (Morris, 2020) ve uygulamaların kullanıcıları bilgilendirmeksizin verileri diğer şirketlerle paylaştığına (Hamilton, 2020) yönelik düşünce ve endişelerin de arttığı görülmektedir. COVID-19 salgını sürecinde bu uygulamalarla ilgili olarak birçok zafiyetin ortaya çıktığı bildirilmektedir (Brough ve Martin, 2020, s.109). KVKK'nın (2016) 12'nci Maddesi ile ilişkili olarak bu tür bulut hizmetlerinin kullanımı göz önüne alındığında, veri sorumlusunun "…uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak…" yükümlülüğünü yerine getirebilmesi de mümkün olamamaktadır. Hukuksal açıdan bakıldığında, UES içinde sıklıkla veri işleyen durumunda olan bulut hizmet sağlayıcıların, KVKK kapsamında kişisel veri işleme faaliyetlerini veri sorumlusundan aldığı talimatlar doğrultusunda gerçekleştirmesi gerekmektedir. Kişisel veri işleme faaliyetlerine ilişkin hukuki yükümlülüklerin yerine getirilmesi konusunda KVKK veri sorumlusunu dikkate almaktadır (KVK Kurumu, 2018b, s.33-35). Uzaktan eğitim merkezi tarafından seçilerek sisteminin bir parçası haline getirilmiş olan bu servislere yönelik hukuksal sorumluluğun, alınan idari karar ya da taahhütname ile öğretim elemanlarına ve öğrencilere devredilmesinin KVKK düzenlemeleriyle bağdaşmadığı düşünülmektedir. Farklı teknik seçenekler sunulması ve öğretim elemanlarının kendi güven duydukları sistemleri tercih edebilmeleri halinde ise sorumluluğun öğretim elemanlarına bırakılmasının mümkün olabileceği değerlendirilmektedir.

UES üzerinden işlenen verilerin yurt dışı kaynaklı şirketlerin bulut hizmet sağlayıcılarına aktarılması konusunda hassasiyet gösterilmesi, kişisel hakların korunması açısından önem taşımaktadır. Verilerin yurt dışına aktarılmasına yönelik koşullar KVKK'nın (2016) 9'uncu Maddesinde düzenlenmiştir. Buna göre ilgili kişinin açık rızasının bulunması halinde kişisel verilerin yurt dışına aktarılması mümkün olabilmektedir. Bunun dışında, KVKK'nın 5'inci maddesinin 2'nci fıkrası ile 6'ncı maddesinin 3'üncü fıkrasında belirtilen, ilgilinin açık rızası aranmaksızın kişisel verilerin işlenebileceği şartların varlığı halinde "yeterli korumanın bulunduğu ülkelere" veri aktarımının yapılması ya da yeterli

korumanın bulunmadığı ülkelere veri aktarımı için Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve KVK Kurulu'nun izninin bulunması gerekmektedir. KVKK' nın 9/3 Maddesinde, yeterli korumanın bulunduğu ülkelerin Kurulca belirlenerek ilan edileceği belirtilmektedir. Kurul bu konuda karar verirken; Türkiye'nin taraf olduğu sözleşmeleri, iki ülke arasındaki karşılıklılık durumunu, her aktarımdaki kişisel verinin niteliği ile işlenme amaç ve süresini, verinin aktarılacağı ülkedeki mevzuatın uygulanmasını ve verinin aktarılacağı ülkedeki veri sorumlusunun alınacak önlemlere ilişkin taahhüdünü değerlendirmektedir. KVKK'nın bu maddesinde belirtilen yeterli korumanın bulunduğu ülkelerin KVK Kurulu tarafından henüz belirlenmemiş olduğu dikkate alındığında, Kanun'da belirtilen hallerin varlığı halinde yurt dışı kaynaklı bulut ortamlarına veri aktarımı yapılabilmesi için KVK Kurulu'nun izninin alınması zorunlu hale gelmektedir. Bu nedenle öncelikli olarak UES'lerin kullanmakta olduğu bulut hizmet sağlayıcılara yönelik bilgilendirmelerin yapılması ve açık rızanın alınması önem taşımaktadır.

Belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki açık rızalar battaniye rızalar olarak kabul edilmekte ve hukuken geçersiz sayılmaktadır (KVK Kurumu, 2018b, s.27). Yöntem olarak açık rızanın hukuken geçerli olabilmesi için sistemin kullanımına yönelik işaretlenmesi zorunlu bir onay kutusu/butonu sunulmasının ötesinde, KVKK'nın 3'üncü Maddesi gereğince UES'in kullanımı ile sınırlı ve özgür irade ile karar verilmesine imkân sağlanan bilgilendirmeye dayalı bir rıza metni sunulmalıdır (KVK Kurumu, t.y., s.4) Elektronik ortam üzerinden de alınabilen açık rıza ile öğretim elemanları; işlenmesine izin verdiği verinin sınırı, kapsamı, gerçekleştirilme şekli ve süresini de belirleyebilmelidir. Açık rızanın temel unsurlarından biri olan belirli bir konu ile sınırlandırılma zorunluluğu; etkileşimli derslerin kayıt altına alınması, kaydın aktarılması, saklanması ve kaydın UES üzerinden yayınlanması açısından ayrı süreçler olarak değerlendirilmelidir. Öğretim elemanı ve öğrencilerin derse katılım sağlaması ve başlatılan ses ve/veya görüntü kayıt işleminin katılımcıların bilgisi dahilinde yapılmasına ilişkin açık rızanın normal süreç içinde yer aldığı değerlendirilebilir. Ancak kaydın saklanması ve tekrar izlenebilmesi amacıyla erişime açılması işlemleri gibi farklı süreçlere ilişkin kişisel hakların korunması için açık rızanın alınması ya da bu süreçlere yönelik tercihin öğretim elemanına bırakılmasının daha doğru bir yaklaşım olacağı değerlendirilmektedir. Bununla beraber açık rızanın verilmesinin kişiye sıkı sıkıya bağlı bir hak olması nedeniyle, ilgili kişinin elektronik ortamda vermiş olduğu açık rızasını sistem üzerinden geri alabilme imkânı sağlanmalıdır (KVK Kurumu, 2018b, s.26).

UES ile kaydedilen ders videolarının öğrencilerin ders sonrasında da erişimine açık olabilmesi için merkezi veri depolama ortamlarının tercih edilmesi zorunluluk haline gelmektedir. Bu durumda, kullanılan bulut vb. depolama alanındaki kayıtlar üzerinde uzaktan eğitim merkezi teknik personelinin de tam erişim yetkisi bulunmaktadır. UES'yi kullanan öğretim elemanı, ilgili teknik personel grubu içinde kendisi ile aynı işlem yetkilerine sahip, ancak kendisi tarafından yetkilendirilmemiş ve çoğunlukla kimlerin erişim

sağlayabildiğini bilmediği ya da anlayamadığı bir depolama ortamını kullanmaktadır. Bu durum, KVKK'nın (2016) 11'inci Maddesinde düzenlenen, ilgili kişinin işlenen verileri hakkında bilgi talep etmesi halinde açıklanabilir olmalıdır. UES içinde yer alan içeriğin teknik olarak üçüncü şahısların erişimine açılması, öğretim elemanı ve/veya uzaktan eğitim merkezi teknik ekibinin kullanıcı yetkisi ile mümkün olabilmektedir. Depolama ortamlarındaki bu dosyalar üzerindeki teknik işlem yetkisini elinde bulunduran teknik personelin, KVKK kapsamında bu dosyaların güvenliğinin sağlanması sorumluluğu da bulunmaktadır. Başka bir ifadeyle, taahhütnameler ile öğretim elemanları ve öğrencilere hatırlatılan kişisel hakların ve kişisel verilerin korunması sorumluluğunun, KVKK kapsamında uzaktan eğitim merkezlerinin de sorumluluğu olduğu görülmektedir. Bu çerçevede ilgili uzaktan eğitim merkezinin KVKK kapsamındaki sorumluluklarının da taahhütnamelerde yer alması ve KVKK'nın 10'uncu Maddesinde düzenlenmiş olan aydınlatma yükümlülüğünün yerine getirilmesi önem taşımaktadır. Aydınlatma yükümlülüğü çerçevesinde veri sorumlusu, veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ve KVKK'nın 11'inci maddesinde sayılan diğer haklara ilişkin bilgileri ilgili kişiye sağlamakla yükümlüdür. Bununla beraber, Kişisel Veri Güvenliği Rehberi (KVK Kurumu, 2018a) çerçevesinde teknik ve idari tedbirler alınmalıdır (KVK Kurulu, 2020).

Veri sorumluları ve veri sorumlusu adına UES üzerinde tasarım ve geliştirme işlemleri yapan uzaktan eğitim merkezi personeli ya da bilgi profesyonelleri tarafından alınması gereken önlemlere ilişkin olarak, KVK Kurulu (2020) tarafından alınan kararlara uyulması önem taşımaktadır. KVK Kurulu tarafından alınan bu kararlarda UES'lerde öğrencilerin ad ve soyadları gibi kişisel verileri ile ses ve görüntü gibi biyometrik veri kapsamında değerlendirilebilecek özel nitelikli kişisel verilerinin işlendiğine dikkat çekilerek, bu konuya ilişkin rehberlerin ve KVK Kurulu kararlarının göz önünde bulundurulması gerektiği vurgulanmaktadır. Bu çerçevede KVKK'nın (2016) 6'ncı Maddesinin 4'üncü Fıkrası ile 22'nci Maddesinin 1'inci Fıkrasının "ç" bendine istinaden KVK Kurulu'nun 31/01/2018 tarihli ve 2018/10 sayılı kararında, alınmasının gerekli olduğu vurgulanan önlemlerden bazıları şunlardır (KVK Kurulu, 2018);

- Verilerin güvenliğine yönelik sistemli, kuralları açık, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,
- Verilerin işlenme süreçlerinde çalışan personel ile gizlilik sözleşmesi yapılması,
- Verilere erişim yetkisi bulunan personelin yetki kapsam ve sürelerinin açık olarak tanımlanması ve yetki kontrollerinin periyodik olarak yapılması,
- Verilerin kriptografik yöntemler kullanılarak saklanması ve kriptografik anahtarların güvenli ve farklı ortamlarda bulundurulması,

- Veriler üzerinde gerçekleştirilen tüm işlemlerin güvenli olarak işlem kayıtlarının oluşturulması,
- Verilerin bulunduğu ortamlara yönelik güvenlik testlerinin yapılması/yaptırılması ve test sonuçlarının kayıt altına alınması,
- Verilere erişim sağlamak için kullanılan UES'e ait kullanıcı yetkilendirmelerinin yapılması, güvenlik testlerinin düzenli olarak yapılması/yaptırılması ve test sonuçlarının kayıt altına alınması,
- Verilere uzaktan erişim sağlanırken en az iki kademeli kimlik doğrulama sisteminin kullanılması,
- Verilerin bulunduğu ortamlara yönelik fiziksel güvenlik önlemlerinin alınması,
- Verilerin aktarılması gerektiğinde şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılmasıdır.

Uzaktan eğitim sürecinde veri işleme konusunda izin ya da emir veren hukuk kurallarına dayanarak yapılan işlemlerde, ilgili hukuk kuralının amacına göre veri işlenmesi ve veri sorumlularının ilgili kişilerin öngöremeyeceği biçimde hareket etmemeleri gerekmektedir. Aksi halde Türk Medeni Kanunu'nun (2001) 2'nci Maddesinde düzenlenen "dürüstlük kuralının" kişisel verilerin işlenmesi esnasında ihlal edilmesi söz konusu olabilmektedir. Dürüstlük kuralı gereğince veri sorumluları, ilgili kişilerin çıkarlarını ve makul beklentilerini göz önüne almalıdırlar (KVK Kurumu, 2018b, s.43). UES'lerin kalitesinin değerlendirildiği araştırmalarda (Çakmak, 2013); öğrencilerin en çok üniversitenin söz verdiği hizmeti doğru ve güvenilir olarak yerine getirmesi özelliğini önemli bulmaları, dürüstlük kuralının uygulama açısından önemini ortaya koymaktadır. Kapsayıcı bir özelliğe sahip olan dürüstlük ilkesi uyarınca, veri işleme faaliyetinin şeffaf olması ve veri sorumlusunun bilgilendirme ve uyarı yükümlülüklerine uygun hareket etmesi gerekmektedir (KVK Kurumu, 2018b).

UES'lerin öğrenci başarısı üzerinde etkili olan bir diğer unsuru da sınav süreçleri ile ilgilidir. YÖK (2020f) tarafından alınan kararda, üniversitelerde 2019-2020 eğitim ve öğretim yılı sınavlarının yüz yüze gerçekleştirilmeyeceği, üniversite yetkili kurullarınca tercih edilecek "dijital imkânlar" veya "ödev, proje gibi alternatif yöntemler uygulanarak" yapılacağı bildirilmektedir. Bununla beraber, YÖK (2020g) tarafından üniversitelerde dijital ortamda gerçekleştirilebilecek sınavların temel ilkeleri belirlenerek üniversitelere duyurulmuştur. Ancak bu kararlarda "şeffaflık ve denetlenebilirliğe" ilişkin olarak sadece dijital ortamların izin verdiği sınav güvenlik tedbirlerinin (soruların rastgele seçilmesi, tam ekran ve tarayıcı kilidinin işlevselleştirilmesi vb.) uygulanması ve ödev, proje ve araştırma raporlarının değerlendirilmesinde intihal tespit programlarının kullanılması önerilmektedir. Ancak sınava, ilgili öğrenci dışındaki kişilerin katılım sağlayarak soru-

ları cevaplandırması ile ödev ve projelerin öğrenci tarafından yapılmamış olma risklerinin göz ardı edildiği görülmektedir. Bu durumda, ücret karşılığı ve benzeri şekilde sınav ya da ödevini üçüncü kişilerin yardımıyla tamamlayan öğrenciler ile sadece kendi imkânlarıyla başarılı olmaya çalışan öğrencilerin, yukarıda belirtilen tedbirlere rağmen eşit koşullarda değerlendirilemeyeceği açıktır. Sınavlarda öğrenci kameralarının açık olma zorunluluğu ve öğrencinin önceden bildirmiş olduğu coğrafi konumdan sınava girmesinin sağlanması ile alınan önlemlerin bir üst seviyeye taşınması mümkün olmakla birlikte, bu zorunlulukların tüm üniversiteler tarafından katı bir şekilde uygulanması ve takibinin teknik olarak sağlanması mümkün olamamaktadır. UES'de web kameralı çevrimiçi gözetleme sistemlerinin kullanımına yönelik katı kuralların uygulandığı ABD'de, öğrencilerin mahremiyet ile notları arasında seçim yapmaya zorlandığı yönünde görüşler bulunmaktadır (Harwell, 2020). Zira YÖK'ün (2020f) kararında da benzer bir vurgulama yapılarak, şeffaf ve denetlenebilir olmanın yanı sıra, öğrencinin bedeni ve ruhi sağlıklarını dikkate alan bir yaklaşım içinde olunması gerektiğinin de altı çizilmektedir. Ancak hukuksal açıdan sözlü sınavlarda olduğu gibi (Sezer ve Bilgin, 2010), çevrimiçi sınavlarda da öğrenci görüntü kaydının oluşturulması ve ödevlerin yüz yüze eğitimde olduğu gibi öğrenciler tarafından etkileşimli derslerde sunularak kaydının oluşturulmasının gerekli olduğu düşünülmektedir. Böylelikle her ne kadar kopya çekmenin engellenmesi mümkün olmasa da en azından sınava doğru kişilerin katılımı ve hazırlanan ödev üzerinde öğrencinin mutlaka çalışması sağlanabilecektir. Diğer taraftan, uzaktan eğitimde bu tür ölçme değerlendirme sorunları dikkate alınarak, COVID-19 öncesinde "Yükseköğretim Kurumlarında Uzaktan Öğretime İlişkin Usul ve Esaslar"ın YÖK (2014) tarafından düzenlendiği görülmektedir. Bu düzenlemenin 12'nci Maddesinde, dönem sonu sınavları ile bütünleme sınavlarının gözetimli olarak canlı veya elektronik ortamda yapılmasının esas olduğu ve gözetimsiz ara sınavların genel başarıya etkisinin uzaktan öğretimde %20'den fazla olamayacağı vurgulanmaktadır. Ancak COVID-19 sürecinde YÖK (2020f, 2020g) tarafından alınan kararlarla bu yaklaşımın daha esnek hale getirildiği görülmektedir.

Araştırmanın Amacı ve Soruları

Bu çalışmada, COVID-19 salgını sürecinde yükseköğretim kurumlarının kullanmış oldukları UES'lerin kullanıcı hakları açısından ne tür riskleri oluşturduğu incelenmiştir. Üniversitelerin uzaktan eğitim konusunda yapmış oldukları duyurular, bilgilendirme metinleri ve uyarılar göz önüne alındığında, hukuksal açıdan özellikle telif haklarının ve kişisel verilerin korunması konularına dikkat çekildiği ve risklerin bu konular üzerinde yoğunlaştığı görülmektedir. Bu çerçevede, çalışmada UES uygulamalarının hukuksal koşulları değerlendirilerek mevcut durumun ortaya konulması ile birlikte, eğitim kurumları, uzaktan eğitim süreçlerinde sorumluluk üstlenen bilgi profesyonelleri ve kullanıcılara yönelik farkındalığın oluşturulması amaçlanmıştır. Bu amaç doğrultusunda aşağıdaki araştırma sorularına yanıt aranmaktadır:

1. COVID-19 salgını sürecinde Türkiye'deki üniversitelerin UES'ye geçişi ve bu süreci yönetimi nasıl olmuştur?
2. UES'lerde öğretim elemanları ve öğrencilere ilişkin hukuksal sorumluluklar nelerdir?
3. UES'lerde, UES yöneticileri, UES süreçlerinde sorumluluk alan bilgi profesyonelleri ve/veya veri sorumlularına ilişkin hukuksal sorumluluklar nelerdir?
4. Üniversitelerin UES'lerinde kişisel hakların korunmasına yönelik yaklaşımı ve izlemiş olduğu yöntemler, hukuksal sorumluluklar ve mevzuat ile uyumlu mudur?
5. Üniversiteler COVID-19 salgını sürecinde kişisel hakların korunmasına yönelik hukuksal sorumluluklara ilişkin yeterli güvenlik önlemlerini almışlar mıdır?
6. COVID-19 salgını sürecinde Türkiye'deki üniversiteler kişisel hakların korunmasına yönelik olarak nasıl bir tutum izlemiştir?

Yöntem

Araştırma Deseni

COVID-19 salgını sürecinde yükseköğretim kurumlarının kullanmış oldukları UES'lerin kullanıcı hakları açısından ne tür riskler oluşturduğunun ortaya konulmasını sağlayan bu çalışmada betimleme/tarama yöntemi kullanılmıştır. Betimleme/tarama modeli, araştırmaya konu olan ve geçmişte veya halen var olan bir durumu herhangi bir müdahalede bulunmadan var olduğu haliyle betimlemeyi amaçlayan araştırma modelidir (Karasar, 2012, s.77).

Araştırma Evreni ve Örneklem

Araştırmanın evrenini, Türkiye'de 2019-2020 eğitim-öğretim yılında aktif olarak eğitim-öğretim faaliyetlerine devam eden 70 vakıf ve 126 devlet üniversitesi ile 4 vakıf meslek yüksek okulu olmak üzere toplam 200 üniversite oluşturmaktadır. Araştırmada örneklem seçme yöntemine başvurulmamış, araştırma konusu ile ilgili tüm birimlerin araştırmaya dahil edilmesi olarak tanımlanan tam sayım yöntemi (Lin, 1976, s.164) kullanılmıştır. Bu kapsamda araştırma evreninde yer alan üniversitelerin belirlenmesinde YÖK (2020h) tarafından hazırlanan "COVID-19 Bilgilendirme" platformundan yararlanılmıştır. Pandemi sürecinde üniversitelerimizdeki çalışmalar başlığı altında üniversite isimlerinin ve ilgili üniversitenin çalışmalarına erişimi sağlayan bağlantının yer aldığı bu platformda toplam 207 üniversiteye yer verilmektedir. Ancak bu platformda yer alan 7 üniversitenin 2019-2020 eğitim-öğretim yılı itibariyle aktif olarak eğitim-öğretim faaliyetlerine devam etmediği belirlenmiştir. Bu nedenle, bu 7 üniversite araştırma evreninden çıkartılmış ve pandemi sürecinde aktif olarak eğitim-öğretim faaliyetlerine devam eden 200 üniversite araştırma kapsamında ele alınmıştır.

Verilerin Toplanması

Elektronik ortamlarda kişilik haklarının ihlaline neden olan birçok unsur bulunmaktadır. UES özelinde ise kişilik haklarına ilişkin kişisel verilerin korunması ve haksız fiil boyutu ile telif hakları hukukuna yönelik ihlallerin öne çıktığı görülmektedir. Bu nedenle çalışmada öncelikle UES'lerde işlenen, kişinin üzerinde hak sahibi olduğu ve aynı zamanda kişisel değer olarak görülen bilgilerin hukuksal koşullarına ilişkin detaylı bilgi verilmiştir. Bu kapsamda öğretim elemanları ve öğrencilere ilişkin hukuksal sorumluluklar ile UES yöneticileri ve veri sorumlularına ilişkin hukuksal sorumluluklar ayrı alt başlıklar halinde irdelenmiştir. YÖK tarafından konuya ilişkin olarak alınan kararlar ve yönetmelikler ile KVK Kurumu tarafından alınan kararlar ve rehberler incelenerek, araştırmada ağırlıklı olarak dikkate alınacak hususlar belirlenmiştir. Çalışmada hukuksal koşullar ve ilgili kurumların almış olduğu kararlar ile üniversitelerin uzaktan eğitim uygulamaları karşılaştırılarak değerlendirilmiş ve kişisel hakların korunmasına yönelik eksiklikler ortaya konulmuştur. Çalışma kapsamında kurumların zarar görmemesi amacıyla isimleri gizli tutulmuş, sadece örnek yaklaşımların olduğu üniversitelerin uzaktan eğitim merkezi portallarının adresleri dipnot bölümünde verilmiştir.

Araştırma kapsamında 200 üniversiteden verilerin toplanması için, üniversitelerin uzaktan eğitim merkezleri ya da ilgili birimleriyle e-posta ve telefon aracılığıyla irtibat kurularak bilgi alınması amaçlanmıştır. Bu amaç doğrultusunda öncelikle araştırma evreninde yer alan üniversitelerden rastgele örnekleme yöntemi ile seçilen 20 üniversite ile telefon aracılığıyla irtibata geçilmiştir. Bu görüşmelerde kendilerinden e-posta üzerinden belge paylaşım yoluyla ya da telefon ile araştırmanın amaçları doğrultusunda veri toplanıp toplanamayacağı sorulmuştur. Ancak bu yöntemlerle ulaşılan 20 üniversitenin 18'i, araştırma amaçlı olarak uzaktan eğitim sistemleri ve uygulamalarına ait verebilecekleri tüm bilgilere, bilgilendirme sayfaları üzerinden çevrimiçi erişim sağlanabileceğini belirtmişler ve bu nedenle araştırmaya herhangi bir ilâve bilgi sunarak katkı sağlamayı reddetmişlerdir. Görüşme yapılan 20 üniversitenin ikisi ise bilgilendirme sayfalarında yer alan bilgilerden daha fazlasını (kurum içi yazışmalar vb.), sistem güvenliği ve gizlilik nedeniyle paylaşamayacaklarını belirtmişlerdir. Bu nedenle araştırma verilerinin tamamının üniversite uzaktan eğitim merkezleri ya da ilgili birimlerin hazırlamış oldukları ve herkesin erişimine açık çevrimiçi bilgilendirme sayfaları üzerinden elde edilmesine karar verilmiştir.

Araştırma kapsamında verilerin toplanması amacıyla öncelikle YÖK (2020h) tarafından hazırlanan "COVID-19 Bilgilendirme" platformundan yararlanılarak, araştırma evreninde yer alan üniversitelerin COVID-19 sürecinde yaptıkları çalışmalara ilişkin bilgilerin sunulduğu web sitelerinin adresleri belirlenmiştir. Bu işlemin ardından araştırma evreninde yer alan her üniversite için ilgili web sitesi ziyaret edilmiş, bu sitede "Uzaktan Eğitim Faaliyetleri" başlığı altında üniversitede yürütülen senkron ve asenkron eğitim faaliyetlerine ilişkin açıklamalar incelenmiştir. Bu aşamada üniversitenin uzaktan eğitim

sürecinde kullandığı UES ve bu sistem kapsamında kullanılan uygulamalara (yazılımlara) ilişkin veriler toplanmıştır. Üniversiteler tarafından hazırlanmış olan bu web sitelerinde üniversitelerin uzaktan eğitim süreçlerine ilişkin genel açıklamalar sunulmakla birlikte, bu açıklamaların tamamında uzaktan eğitim uygulama esasları gibi detaylara yer verilmediği görülmüştür. Bu nedenle, bu aşamada elde edilen verilerin teyit edilmesinin yanı sıra, uzaktan eğitim sürecine ilişkin detayların elde edilebilmesi amacıyla araştırma evreninde yer alan her üniversitenin UES ve uzaktan eğitim uygulama ve araştırma merkezi web sitesi ziyaret edilerek bu sitelerde uzaktan eğitim sürecine ilişkin yer alan açıklamalar, haber ve duyuru metinleri, öğrenci ve öğretim elemanlarına yönelik hazırlanmış kullanım kılavuzları (rehberler) ve uzaktan eğitim uygulama usul ve esaslarına ilişkin dokümanlar incelenmiştir. Bu kapsamda kullanılan UES türlerine ve senkron ders (canlı sınıf) platformlarına ve bu sistemlerin kullanımında kişisel verilerin korunması ve telif haklarına yönelik herhangi bir açıklamanın sunulup sunulmadığına ilişkin veriler toplanmıştır.

Verilerin Analizi

Araştırma kapsamında toplanan verilerin analizinde yüzde (%) ve frekans (f) gibi betimsel istatistiklerden yararlanılmış, analiz sürecinde "Microsoft® Excel® 2019" programı kullanılmıştır. Değerlendirmeler sonucunda, üniversitelerde kullanılan UES türleri, üniversitelerde kullanılan senkron ders platform türleri, üniversite taahhütnamelerinde UES veya senkron ders platformlarında paylaşılan içeriklere ilişkin fikri mülkiyet haklarının korunması konusuna doğru bir yaklaşımla yer verilip verilmediği, üniversitelerin bilgilendirme platformlarında UES üzerinde işlenen kişisel verilerin korunmasına yönelik gerekli ve yeterli uyarıların yapıp yapılmadığı, UES'ye ilişkin olarak alınması istenen önlemlerin ve uygulamaların kişisel hakların korunması açısından hukuka uygun olup olmadığı ortaya konulmaya çalışılmıştır.

Sınırlılıklar

Araştırma kapsamında elde edilen verilerin yer aldığı çevrimiçi bilgilendirme sayfalarının bağlantı adresleri uzaktan eğitim süreci içinde değişebilmekte ve ilgili dokümanlara erişim açısından sorunlar meydana gelebilmektedir. Çalışma içinde verilen örneklere ilişkin erişim adresleri, araştırmanın yapıldığı tarih itibariyle aktif olan erişim adresleridir. Çalışmanın ana veri kaynağı olan çevrimiçi bilgilendirme sayfalarında da devam eden uzaktan eğitim süreci içinde güncellemelerin olabileceği düşünülmektedir. Ayrıca gizlilik ve güvenlik gerekçeleriyle çevrimiçi bilgilendirme sayfalarında ve duyurularda yer almadığı için bu çalışmada incelenemeyen kurum içi yazışma ve bilgilendirmelerin olabileceği düşünülmektedir. Bu çalışma ile dikkat çekilen hususlar ve çalışmada sunulan öneriler, araştırma kapsamında çevrimiçi bilgilendirme sayfalarından elde edilen bulgulara dayanmaktadır.

Bulgular ve Tartışma

Üniversitelerde Kullanılan Uzaktan Eğitim Sistemleri ve Senkron Ders Platform Türleri

COVID-19 salgını sürecinde üniversitelerde kullanılan UES türlerine ilişkin tanımlayıcı istatistikler Tablo 1'de gösterilmektedir.

Tablo 1

Üniversitelerde Kullanılan Uzaktan Eğitim Sistemi (UES) Türleri

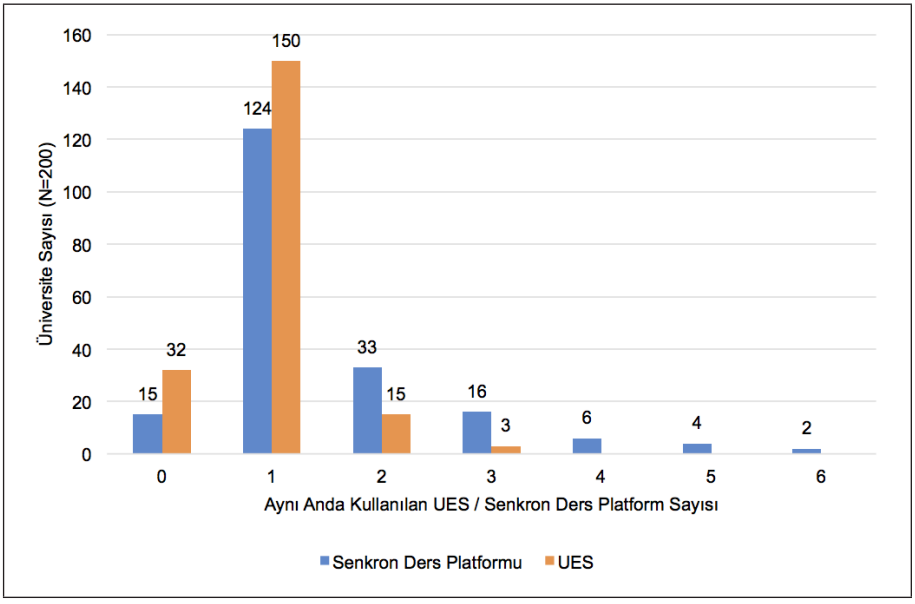
UES Türü	n	%
Moodle	70	35,0
ALMS	55	27,5
Üniversitenin geliştirdiği UES[a]	23	11,5
Google Classroom	21	10,5
Canvas	11	5,5
Sakai	5	2,5
Edmodo	5	2,5

[a] "Uzaktan Eğitim Uygulama ve Araştırma Merkezi" veya "Bilgi İşlem Daire Başkanlığı" tarafından geliştirilmiş olan öğrenme yönetim sistemleri veya öğrenci bilgi sitemlerini UES olarak kullanan üniversiteler

Tablo 1 incelendiğinde; üniversiteler tarafından en fazla tercih edilen UES'nin, açık kaynak kodlu bir yazılım olan Moodle sistemi (n=70, %35,0) olduğu görülmektedir. Moodle, dünyada pek çok ülkede ve Türkiye'de birçok eğitim kurumu ve eğitimci tarafından kullanılan ve küresel çapta yükseköğretim kurumlarının %60'ından daha fazlası tarafından tercih edilen bir UES'dir (Moodle, 2020). Moodle sistemini sırasıyla; ALMS (n=55, %27,5), üniversitelerin kendi bünyelerinde uzaktan eğitim merkezleri veya bilgi işlem daire başkanlıkları tarafından geliştirilmiş/uyarlanmış UES'ler (n=23, %11,5) ve Google Classroom (n=21, %10,5) takip etmektedir.

Şekil 2

Üniversitelerde Kullanılan UES ve Senkron Ders Platformlarının Dağılımı



Bu noktada, Şekil 2'de gösterildiği üzere, Tablo 1'de yer alan UES'lerden sadece birini (n=150) veya birkaçını (n=18) aynı anda kullanan üniversiteler olduğu gibi, bu UES'lerden herhangi birini kullanmayan üniversiteler (n=32) de bulunmaktadır. Herhangi bir UES kullanmayan üniversiteler, uzaktan eğitim sürecinde sadece senkron ders platformlarını kullanmaktadır. Bu nedenle uzaktan öğretim sürecinde UES kullanmayan üniversitelerin sayısı ile Tablo 1'de yer alan UES'lerden herhangi birini kullanan üniversitelerin sayıların toplamı, araştırma evreninde yer alan toplam üniversite sayısından farklıdır.

COVID-19 salgını sürecinde üniversitelerde kullanılan senkron ders platformu türlerine ilişkin tanımlayıcı istatistikler Tablo 2'de gösterilmektedir.

Tablo 2

Üniversitelerde Kullanılan Senkron Ders Platform Türleri

Senkron Ders Platformu	n	%
Zoom	57	28,5
Perculus	46	23,0
Microsoft Teams	45	22,5
Adobe Connect	43	21,5
BigBlueButton	32	16,0
Google Meet	29	14,5
Blackboard Collaborate	17	8,5
Skype	12	6,0
Youtube	10	5,0
Whatsapp	3	1,5

Tablo 2 incelendiğinde; üniversiteler tarafından en fazla tercih edilen senkron ders platformunun Zoom (n=57, %28,5) olduğu görülmektedir. Zoom, bulut bilişim teknolojisi ile kullanıcılarının ses ve/veya görüntü paylaşarak çevrimiçi görüşmeler, toplantılar vb. etkinliklerin düzenlemesine imkân tanıyan bir uygulamadır. Zoom uygulamasını sırasıyla; Perculus Plus (n=46, %23,0), Microsoft Teams (n=45, %22,5), Adobe Connect (n=43, %21,5) ve BigBlueButton (n=32, %16,0) uygulamaları takip etmektedir.

Bu noktada, Şekil 2'de gösterildiği üzere ve Tablo 1'de gösterilen UES'lerin kullanımına benzer şekilde, Tablo 2'de yer alan senkron ders platformlarından sadece birini (n=124) veya birkaçını (n=61) aynı anda kullanan üniversiteler olduğu gibi, bu platformlardan herhangi birini kullanmayan ve sadece UES üzerinden asenkron şekilde uzaktan eğitim sürecine devam eden üniversitelerin de (n=15, %7,5) bulunduğunu belirtmekte fayda vardır. Bu nedenle uzaktan öğretim sürecinde senkron ders platformu kullanmayan üniversitelerin sayısı (n=15) ile Tablo 2'de yer alan platformlardan herhangi birini kullanan üniversitelerin sayılarının toplamı, araştırma evreninde yer alan toplam üniversite sayısından farklıdır.

Web tabanlı UES'ler COVID-19 salgını süreci öncesinde de kullanılmakla birlikte, araştırmadan elde edilen bulgular doğrultusunda bu süreçte UES'lerden beklentilerde bazı farklılıkların oluştuğunu söylemek mümkündür. Örneğin; ideal UES modellerinin senkron/etkileşimli eğitim özelliği olmakla birlikte, sunduğu en önemli avantajlar arasında sanal bir kampüs oluşturulması ve asenkron eğitim imkânının olması gösterilmektedir (Al ve Madran, 2004). COVID-19 salgını sürecinde ise kaynaklara asenkron erişim konusunda sağlanan esnekliğin yanı sıra, mümkün olduğunca yüz yüze eğitimde sağlanan senkron ders işleme koşullarının sağlanmasının hedeflendiği görülmektedir.

Tablo 2'de de görüldüğü üzere, üniversitelerin %82,5'i (n=185) en az bir senkron bir ders platformunu kullanmaktadır. Bununla beraber, YÖK (2020e) tarafından yapılan bir araştırmanın sonuçlarında da COVID-19 salgını sürecinde canlı ders uygulaması gerçekleştiren üniversitelerin %37'sinin tüm derslerde, %18'inin de belli derslerde canlı ders uygulamasını zorunlu tuttuğu görülmektedir. Salgın süreci öncesinde kıyasla UES'lerden beklentideki bu değişimin, günümüz iletişim teknolojileri ile artan bant genişliği kullanımına bağlı olarak şekillendiği değerlendirilmektedir. Bununla beraber, 2004 yılı itibariyle 79 üniversitenin 5'i uzaktan eğitim programına sahip iken (Al ve Madran, 2004), COVID-19 salgını sürecindeki ilk iki haftada 200 üniversitenin 187'sinin (%93,5) uzaktan öğretime geçiş süreçlerini tamamlamış olması (YÖK, 2020e), uzaktan eğitimin bir zorunluluğa dönüştüğünü göstermektedir. Diğer taraftan, Tablo 1 ve Tablo 2'de sunulan araştırma bulguları ile YÖK (2020e) tarafından yapılan anket çalışmasının bulguları arasındaki farklılık dikkate alındığında, üniversitelerin COVID-19 salgını sürecinde uzaktan eğitim platformlarındaki güncelleme ve iyileştirme çalışmalarını aralıksız devam ettirmiş olduklarını söylemek mümkündür.

Uzaktan Eğitim Sistemlerinde Telif Haklarının Korunması

UES'lerde senkron ve asenkron eğitim için üretilen ders içeriklerine yönelik telif haklarının korunması amacıyla ne tür önlemlerin alındığına ilişkin düzenlemeler incelendiğinde; araştırma evreninde yer alan 200 üniversitenin %11'inin (n=22) öğrenci ve öğretim elemanlarına yönelik hazırlanmış kullanım kılavuzlarında veya uzaktan eğitim uygulama usul ve esaslarına ilişkin dokümanlarda konuya ilişkin bir taahhütnameye yer verdikleri görülmektedir. Bu üniversitelerin UES kullanım taahhütnameleri gereğince, öğretim elemanları ve öğrenciler FSEK (1951) hükümlerine uygun olarak UES'nin kullanılmasını kabul etmiş sayılmaktadırlar. Buna göre öğretim elemanları ve öğrencilerin, FSEK kapsamına giren hiçbir içeriği sahiplerinden izin almaksızın kullanamayacağı, içeriğin kullanılması halinde ise doğacak sorumluluğun öğretim elemanları ve öğrencilere ait olduğu belirtilmektedir. Ancak bu taahhütnamelerde eğitim ve öğretim amacıyla eser sahibinin meşru menfaatlerine zarar vermeden ve/veya eserden normal yararlanmaya aykırı olmamak şartıyla hangi ölçüde yararlanılabileceğine yönelik herhangi bir açıklama bulunmamaktadır. Bu nedenle, bu taahhütnamelerde genel menfaat gerekçesiyle eğitim ve öğretime yönelik olarak FSEK içinde düzenlenen istisnaların göz ardı edildiği görülmektedir. Bu eksikliğin nedeninin, UES'nin altyapısını tasarlayan ve/veya bu sistemleri işleten personelin, içeriğe yönelik hukuksal sorumlulukları içeriği sağlayan ders sorumlusuna bırakmak istemesinin olabileceği düşünülebilir. Ancak bu çerçevede oluşturulan taahhütname, FSEK kapsamında öğretim elemanlarına tanınan eğitim istisnasının önüne geçerek, eser sahibinin haklarını korumaya yönelik katı yaklaşımın bir örneği haline gelebilmektedir. Buna karşın bazı üniversitelerin[2], mümkün olduğunca dış kaynaklı doküman ve resimler için sadece ve doğrudan bağlantı adresinin verilmesini

2 http://www.uludag.edu.tr/dosyalar/bilgiislem/ukey/ukey_c.pdf

önererek bu konudaki risklerin en aza indirilmesini amaçladıkları görülmektedir. Bununla beraber, bazı üniversitelerin[3] uzaktan eğitim sürecine ilişkin hukuksal çerçevede yayımlamış oldukları uygulama esaslarında FSEK ve veri koruma konusundaki uyarılara yer verdiği görülürken, bazı üniversitelerin[4] FSEK dışında herhangi bir bilgilendirme ya da uyarıya yer vermedikleri görülmektedir. Bunun yanı sıra hukuksal sorumluluklarla etik kurallara uyum arasında ikilemde kalan, telif haklarına uyum sağlamanın etik çerçevede değerlendirildiği ve bu konudaki yasal yükümlülüğün öğretim elemanına ait olduğunu ifade eden uyarı metinlerinin yayınlandığı görülmektedir. Araştırma evreninde yer alan 200 üniversitenin 22'si (%11) öğretim elemanlarını, uzaktan eğitim sürecinde öğrencilerin dersleri takip edebilmesi amacıyla kullanılan video, resim vb. görsel ve işitsel ders materyallerinin oluşturulmasında ve uzaktan öğretim sürecinde kullanılan UES veya senkron ders platformlarında paylaşılmasında fikri mülkiyet haklarının korunmasına yönelik gerekli özeni göstermeleri gerektiği konusunda uyarmaktadır.

Uzaktan Eğitim Sistemlerinde Kişisel Verilerinin Korunması

UES'lerde senkron ve asenkron eğitim kapsamında öğretim elemanlarının ve/veya öğrencilerin kişisel verilerinin korunması amacıyla ne tür önlemlerin alındığına ilişkin düzenlemeler incelendiğinde; araştırma evreninde yer alan 200 üniversitenin sadece 30'unun (%15) uzaktan eğitim sürecinde KVKK'ya (2016) özen göstermeleri gerektiği konusunda öğrenci veya öğretim elemanlarını uyardıkları görülmektedir. Bu kapsamda öğretim elemanlarına, öğrencilerin görüntülerinin olduğu video gibi ders materyallerinin, öğrencilerin açık rızası alınmadan hiçbir sanal ortamda paylaşılmaması gerektiği konusunda uyarılar yapılmaktadır. Benzer şekilde, öğrencilere de uzaktan öğretim süresince oluşturulan tüm ders materyalleri ile video, ses ve görüntü kayıtlarının, KVKK kapsamında öğretim elemanının kişisel verisi olduğu ve bu verilerin COVID-19 salgını sürecinde öğrenciler ile paylaşılmış olduğu hatırlatılmaktadır. Öğrencilere, ders anlatım sürecinde kendileri ile paylaşılmış olan ve öğretim elemanlarına ait kişisel verilerin korunmasına özen göstermeleri ve bu verilerin herhangi bir sanal ortamda paylaşılmaması ve tedavüle sokulmaması gerektiği konusunda uyarılar yapılmaktadır. Ancak, kişisel verilerin korunması yönünde öğrenci veya öğretim elemanlarına bilgilendirme yapan 30 üniversitenin 12'sinde bu tür haklara yönelik ihlallerinin oluşması halinde üniversitenin herhangi bir hukuki/cezai sorumluluğunun olmadığı ve bu hususta tüm sorumluluğun ilgili kişi/kişilerde bulunacağı belirtilmektedir. KVKK'nın (2016) 12'nci Maddesi gereğince veri sorumlusu tarafından alınması gereken teknik ve idari önlemlerin alınmadığı her koşulda, bu tür ifadelerle üniversitelerin risk ve sorumlulukları tamamen transfer edemeyecekleri açıktır. Çalışmada hukuksal koşulların açıklandığı bölümde belirtildiği gibi, öğrencilerin ve veri sorumlularının kişisel verilerin korunmasına yönelik farklı sorumlulukları bulunmaktadır. Örneğin; bazı üniversitelerin[5] UES kullanım esasla-

3 https://www.eskisehir.edu.tr/duyurular/i-1585906283
4 https://erbakan.edu.tr/evdekal/sayfa/9231
5 https://egeders.ege.edu.tr/mod/page/view.php?id=299&lang=en

rında belirtildiği gibi KVKK'ya aykırı olan bilgilerin sistem üzerinde bulunduğu fark edildiğinde, sistem yöneticileri tarafından içeriğin yayından kaldırılması, üst yönetime bilgi verilmesi ve gerekli hallerde işlem kayıtlarının adli mercilere verilmesi gibi sorumlulukların belirlenmiş olması önem taşımaktadır. Bunun yanı sıra, kişisel verilerin korunmasına ilişkin sorumlulukları tamamen transfer etme arayışında olan üniversitelerin bilgilendirme metinlerinde kullanılan ifadelerin aynı cümlelerden oluştuğu görülmektedir. Bu durum, üniversitelerin birbirinden etkilenerek bu metinleri oluşturdukları izlenimini oluşturmaktadır.

KVKK'ya (2016) uygun olarak UES'lerde işlenen verilerin amacını ve işlenme vasıtalarını belirterek, veri sahibinin haklarına ilişkin bilgilerin sunulduğu uzaktan eğitim aydınlatma metnini yayımlayan az sayıda da olsa üniversiteler[6] bulunmaktadır. Benzer şekilde, sorumluluğu transfer etme amacında olmayan bazı üniversitelerin[7] de öğrencilere yönelik olarak hazırlamış olduğu taahhütnameler ile uzaktan eğitim kapsamında hazırlanan ve paylaşılan tüm ders materyallerin kişisel veri niteliğinde olduğunu ve bunların açık rıza olmadan üçüncü kişilerle paylaşılamayacağını belirttikleri görülmektedir. Bu kapsamda kişisel verilerin korunmasına yönelik öğretim elemanlarına ve/veya öğrencilerine bilgilendirme yapan bazı üniversitelerin[8]; özellikle KVK Kurulu'nun (2020) uzaktan eğitim platformları hakkındaki kamuoyu duyurusuna atıfta bulunarak bilgilendirme yapmış olmasını, KVK Kurulu'nun bu duyurusunun yarattığı farkındalığın önemli bir yansıması olarak değerlendirmek mümkündür.

Öğretim elemanlarına ve öğrencilere yönelik olarak kişisel verilerin korunması konusunda yapılan bazı bilgilendirme metinlerinde, kurumsal e-posta hesapları üzerinden uzaktan eğitim amacıyla erişilen platformlara ilişkin kullanım istatistikleri arasında özel görüşmelerin kayıtlarının da tutulduğu bilgisi yer almaktadır. Bu bilgilendirme metinlerinde özel görüşmeler için kişisel e-posta hesaplarının kullanılması önerilirken, kurumsal e-posta hesaplarındaki kişisel verilerden üniversitenin sorumlu olmadığı belirtilmektedir. Bu durumda veri sorumlusunun, kullanım istatistiklerini özel görüşmelere ilişkin bilgilerden nasıl ayrı bir şekilde koruyacağının ve meydana gelen veri hırsızlığına bağlı olarak mı kendisini sorumlu hissedeceğinin belirsiz olduğu görülmektedir. Diğer taraftan bu konuya ilişkin olarak KVK Kurulu'nun (2018) kararında, UES üzerinden işlenen verilerin aktarılma süreçlerinde kurumsal e-posta adresi ya da KEP hesabının kullanılması gerektiği belirtilmektedir. Ancak bazı üniversitelerin kullanmakta olduğu kurumsal e-posta hesaplarının da yurt dışı merkezli hizmet sunucuları (Google Gmail vd.) üzerinden oluşturulmuş olması, bu gerekliliğin nasıl sağlanacağı açısından düşündürücüdür.

6 https://api.hacibayram.edu.tr/files/1/Hac%C4%B1bayram%20AHBV/uzaktan-egitim(tr-TR)/HBV%20UZAKTAN%20E%C4%9E%C4%B0T%C4%B0M%20ayd%C4%B1nlatma%20metni%20(1).pdf

7 https://www.thk.edu.tr/wp-content/uploads/2020/04/TAAHH%C3%9CTNAME-1.docx

8 https://uzem.usak.edu.tr/menu/6478#kisisel_verilerin_korunmasi_kanunu

UES'lerde kişisel verilerin korunmasına ilişkin bir diğer önemli hususun da üniversitelerin verilerin depolanması için tercih ettikleri ortamlara ilişkin olduğu görülmektedir. Bu kapsamda, araştırma evreninde yer alan bazı üniversitelerin yerel sisteme (sunuculara) yük getirdiği gerekçesiyle çekilen ders videolarının Youtube, Google Drive ve Microsoft One Drive gibi yurt dışı kaynaklı ortamlara taşınması konusunda tercih yaparken, hukuksal koşulları ve kişisel hakları göz önünde bulundurmadıklarını söylemek mümkündür. Bununla birlikte, öğretim elemanlarına ders videolarının yurt dışı kaynaklı bu tür ortamlara taşınması konusunda herhangi bir uyarıda bulunmayan, ancak UES'ye ilişkin sık sorulanlar bölümünde sisteme eklenecek olan videoların nerede barındırıldığının/depolandığının bir önemi olmadığını ifade eden üniversitelerin bulunduğu görülmektedir. Bundan farklı olarak, boyutu 100 MB'ı aşan verilerin yurt dışı kaynaklı ortamlara taşınması konusunda öğretim elemanlarına yönlendirme yapan, ancak içeriğin kişisel verilerin korunması konusunda ihlal oluşturmayacak şekilde hazırlanmasına dikkat çeken üniversiteler de bulunmaktadır. Bazı üniversitelerin[9] ise ders materyallerinin Youtube vb. sosyal paylaşım sitelerinde herkese açık şekilde paylaşılmaması ve aynı zamanda sınıf ve öğrenci görüntüsü olan videoların KVKK (2016) kapsamında öğrencilerin açık rızası alınmadan hiçbir sanal ortamda paylaşılmaması hususuna özen gösterilmesine dikkat çektikleri görülmektedir. Benzer şekilde; Microsoft Teams, Zoom gibi veri merkezi yurt dışında olan platformlar kullanılarak veri aktarımı yapılması halinde bu durumun KVKK'nın 9'uncu Maddesinin ihlali anlamına gelebileceğine dikkat çeken üniversiteler[10] olduğu gibi bu koşulları göz önüne alarak UES kapsamındaki tüm verileri üniversite kontrolündeki sunucularda bulunduran üniversiteler[11] de bulunmaktadır. Bu çerçevede, daha önce bahsi geçen Tablo 1'de de görüldüğü üzere, araştırma evreninde yer alan 200 üniversitenin 23'ü (%11,5), UES sunucularını kendi kontrolünde yapılandırmaktadır. Şüphesiz UES'ler üzerinde kişisel verilerin bulunduğu ve kişisel hakların ihlaline yönelik en fazla risk içeren unsurlar, yurt dışı kaynaklı olarak hizmet sunan ve canlı ders videolarının işlendiği platformlardır. Daha önce bahsi geçen Tablo 2'de de görüldüğü üzere Perculus platformu haricinde, üniversiteler tarafından tercih edilen senkron ders platformlarının tamamının yurt dışı kaynaklı olarak hizmet sunan platformlar olduğunu söylemek mümkündür.

Genel itibariyle senkron dersler için yurt dışı kaynaklı olarak hizmet sunan platformlar tercih edilirken; birçok üniversite tarafından kullanılan Google Meet gibi uygulamaların bulut ortamlarına aktarmış olduğu verilerin saklanma koşulları (Google Cloud, 2020a) incelendiğinde, ilgili kuruluşlar tarafından gerekli güvenlik önlemlerinin ISO 27001, ISO 27017, ISO 27018 ve SSAE16 / ISAE 3402 gibi uluslararası bilgi güvenliği standartlarına uygun olarak alındığı ve güvenlik stratejisinin bir parçası olarak kriptografik yöntemlerin kullanıldığı görülmektedir. Bununla beraber, varsayılan olarak kullanımda olmayan verilerin kriptografik yöntemlerle saklanması, kimliğe duyarlı

9 https://its.metu.edu.tr/uzaktanegitim/
10 https://www.gtu.edu.tr/kategori/3687/0/display.aspx?languageId=1
11 http://korona.test.gelisim.edu.tr/uzaktan-ogretim-faaliyetleri#accordion_100

vekil sunucu kullanım seçenekleri ve 24 Ekim 1995 tarihli 95/46/EC sayılı Veri Koruma Direktifi'nin yerini alarak 25 Mayıs 2018'de yürürlüğe giren GDPR'a uyum taahhüdünde bulunması (Google Cloud, 2020b) nedeniyle bu tür platformların kullanımı tercih sebebi olabilmektedir (Google Cloud, t.y.). Ancak yeterli korumanın bulunduğu ülkeler KVK Kurulu tarafından belirlenmediği sürece, yeterli bir korumanın sağlandığının ilgili platform tarafından yazılı olarak taahhüt edilmesi gerekmektedir. Bu nedenle KVK Kurumu (2020a) tarafından örneği sunulan ve asgari şartların belirtildiği bir sözleşmenin 6698 sayılı Kanun'un 12'nci Maddesinin 2'nci fıkrasına istinaden yapılması önem taşımaktadır. KVK Kurumu'nun (2020b) yayımlamış olduğu "Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru" ile bu konuya açıklık getirdiği görülmektedir. Ancak araştırmada Türkiye'deki üniversiteler ile UES'ler üzerinden işlenen kişisel verilerin yurt dışı kaynaklı bulut ortamlarına aktarılmasına yönelik özel bir sözleşmenin yapılmadığı görülmektedir. Bununla beraber, UES üzerinden işlenen verilerin başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde veri sorumlularının da gerekli tedbirlerin alınmasına yönelik olarak bu kişilerle birlikte müştereken sorumluluğu bulunmaktadır (KVK Kurumu, 2018a). KVK Kurulu'nun (2020) dikkat çektiği gibi, veri depolama işlemlerinin yurt dışı kaynaklı bulut ortamlarında yapılmasına bazı üniversitelerin[12] mesafeli olduğu görülmektedir. Veri güvenliğinin sağlanmasına yönelik sorumluluk bilinciyle bu üniversitelerin, kendi UES altyapısını oluşturmak amacıyla Bilgi Teknolojileri ve İletişim Kurumu ile iş birliği içinde UES'nin teknik altyapısını kullanıma sunan üniversitelerden destek aldıkları görülmektedir.

UES üzerinden oluşturulan verilere yönelik tüm erişim işlemleri, sistemin kullanım amacına uygun olarak uzaktan yapılmaktadır. Bu tür uzaktan erişimin gerekli olduğu uygulamalarda, KVK Kurulu'nun (2018) kararı gereğince en az iki kademeli kimlik doğrulama sisteminin sağlanması gerekmektedir. Ayrıca kişisel veri güvenliği rehberinde (KVK Kurumu, 2018a) de bulut ortamında depolanan verilere uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanması önerilmektedir. Bununla birlikte, birçok üniversitenin kullanmakta olduğu Google Meet vb. platformların sunduğu güvenlik seçenekleri arasında erişim için iki kademeli kimlik doğrulama sisteminin kullanılabileceği belirtilmektedir (Lakshminarayanan ve Hashim, 2020). Ancak araştırma kapsamında incelenen üniversitelerin uzaktan eğitim sürecine ilişkin bilgi ve belgelerinden, iki kademeli kimlik doğrulama sisteminin kullanıldığına yönelik herhangi bir bulgu elde edilememiştir. Buna karşın, araştırma evreninde yer alan 200 üniversitenin 44'ünde (%22) UES veya senkron (canlı) ders platformlarına giriş için öğrenci ve/veya öğretim elemanlarına tanımlanan kullanıcı adlarında ve şifrelerinde öğrencinin/öğretim elemanının adı ve soyadı, öğrenci numarası, sicil numarası veya T.C. kimlik numarası gibi kolaylıkla ulaşılabilir ya da tahmin edilebilir kişisel verilerin tamamına veya bir kısmına yer verildiği görülmektedir. Bazı üniversiteler kullanıcı adı ve şifresi olarak T.C. kimlik numaralarının kullanımı için altyapı değişikliği yaparken, bu kararı KVKK (2016) kapsamında yapılan

12 http://www.ohu.edu.tr/oidb/manset/12429

çalışmalar sonucunda almış olduklarını belirtmektedirler. UES'lere erişim konusunda KVK Kurulu'nun (2018) kararında belirtilen hususlara uyum konusunda bu üniversitelerin gerekli hassasiyeti göstermedikleri açıktır. Ayrıca veri sorumlularının almaları gereken güvenlik önlemleri kapsamında değerlendirildiğinde, bu tür yaklaşımların sistem erişimi açısından güvenlik zafiyetlerine neden olabileceği düşünülmektedir.

Araştırma kapsamında incelenen uzaktan eğitim portalları ve kullanıcı taahhütnamelerinde, UES üzerinde verilere erişim yetkisine sahip kullanıcıların kimler olduğu, yetki kapsamlarının ve sürelerinin nasıl tanımlandığının açık olarak belirtilmediği görülmektedir. KVK Kurulu'nun (2018) "özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler" ile ilgili almış olduğu 31/01/2018 tarihli ve 2018/10 sayılı kararı gereğince; veri sorumluları tarafından bu sistemler üzerinde çalışanlar ile gizlilik sözleşmelerinin yapılması, yetki tanımlamalarının yapılması ve yetki kontrollerinin periyodik olarak yapılması gerekmektedir.

Uzaktan eğitim sürecinde sınavların yapılması hususunda ise birçok üniversitenin, çalışmanın "uzaktan eğitim sistemlerinde işlenen verilerin hukuksal koşulları" başlığı altında belirtilen sınav güvenliğinin sağlanmasına ve bu çerçevede kişisel hakların korunmasına yönelik herhangi bir bilgi sunmadığı görülmektedir. Ancak bazı üniversitelerin[13], bilgisayarı geçici olarak bir sınav istasyonuna dönüştürerek sınav esnasında diğer web sayfaları, pencereler ve programlara erişimi kısıtlayan çözümleri tercih ettiği görülmektedir. Bazı üniversitelerin de UES'den kaynaklanan hak kayıplarının önüne geçebilmek amacıyla COVID-19 sürecindeki değerlendirme puanların öğrencinin isteğine bağlı olarak genel not ortalamasına dahil etmeme kararı aldıkları görülmektedir.

Sonuç

Kişinin varlığına yönelik ve kişi ile sıkı sıkıya bağlı mutlak haklardan olan kişilik hakları, hukuk düzeni tarafından korunan ve üzerinde tasarruf edilemeyen haklardır. Tüm elektronik ortamlarda olduğu gibi UES ve bu sistemler üzerinden yürütülen uzaktan eğitim süreçlerinde de kurumların ve bilgi profesyonellerinin kişisel hakların korunmasına ilişkin hukuksal sorumlulukları bulunmaktadır. Hukuksal düzenlemeler ve bu düzenlemelere bağlı olarak alınan kararların göz ardı edilerek UES üzerinde verilerin işlenmesi, kişisel hakların ihlaline neden olabilecek riskleri barındırmaktadır. Kişisel hakların korunmasına yönelik hukuksal düzenlemeler ile KVK Kurumu tarafından alınan kararlar ve yapılan duyurular, UES'lerde veri işlerken kişisel hakların korunması ve güvenli veri işleme yöntemlerinin geliştirilmesi için önemli bir rehber niteliğindedir.

COVID-19 salgını sürecindeki YÖK (2020a, 2020b, 2020c, 2020d, 2020e, 2020f, 2020g) kararları ve buna bağlı olarak üniversitelerdeki uzaktan eğitim uygulamaları genel olarak değerlendirildiğinde, eğitim sürecinde kesinti yaşanmaması ve aynı zamanda

13 https://its.metu.edu.tr/uzaktanegitim/

salgın risklerinin en aza indirilmesinin öncelikli olarak hedeflendiği görülmektedir. UES üzerinden binlerce öğrenci ile aynı anda etkileşimli dersin yapılmasını sağlayabilmek için güçlü bir bilişim sistemi altyapısına ihtiyaç duyulmaktadır. Bu koşullara hazırlıksız olan üniversitelerin birçoğu, hızlı bir şekilde uzaktan eğitime geçiş yapmak zorunda kalmış ve bilişim sistemleri altyapılarını süreç içinde uygun hale getirmeye çalışmışlardır. Farkındalığı daha üst seviyede olan bazı kurumların, verilerin güvenli olarak saklanmasına yönelik öneme atıfta bulunarak gerekli altyapı düzenlemelerini çok hızlı bir şekilde yaptıkları ve verileri yerel sunuculara transfer ettikleri görülmektedir. Yeterli teknik ve hukuki altyapıya sahip olmayan üniversitelerde ise bu eksikliklerin giderilemediği görülmektedir. Altyapı yetersizliğine bağlı olarak giderilemeyen en önemli eksikliğin verilerin saklanması konusunda oluştuğu görülmektedir. Kısa süre içinde yeni ve yerel bir altyapının oluşturulamaması ve kullanıcıların eş zamanlı olarak bu sistemlere uyum sağlayamaması nedeniyle, eğitim kurumları çoğunlukla yurt dışı kaynaklı bulut hizmet sunucuları üzerinden sağlanan çözümlere yönelmişlerdir (KVK Kurulu, 2020).

Verilerini yurt dışı kaynaklı bulut ortamlarında depolayan üniversitelerin kişisel veri güvenliğini sağlama konusunda sınırlılıklarının olduğu görülmektedir. Ayrıca araştırma bulguları dikkate alındığında, UES erişimi için kullanılan güvenli kimlik doğrulama yöntemlerinin kullanımına ilişkin gerekli hassasiyetin gösterilmediği anlaşılmaktadır. Bu durum kişisel hakların ihlaline neden olabilecek şartları oluşturmaktadır.

Araştırma bulguları, FSEK (1951) ile ilgili hususların hukuksal düzenleme yönüyle anlaşılmasının zor bir yapıda olduğunu ve bu nedenle uygulamada yorum farkının çeşitliliğe neden olduğunu göstermektedir. Üniversitelerin bazıları telif hakları ve kişisel verilerin korunması konusunda öğrencilere yönelik uyarılarda bulunurken bazıları öğretim elemanlarını uyarmayı tercih etmektedir. Bu duruma bağlı olarak, üniversitelerin telif hakları ve kişisel verilerin korunması konusuna yaklaşımında büyük farklılıkların olduğunu söylemek mümkündür. FSEK, yazar haklarının korunmasına yönelik önemli düzenlemeler içerirken, eserlerin üçüncü kişiler tarafından kullanımına yönelik istisnaları da içermektedir. Ancak çalışmanın "uzaktan eğitim sistemlerinde işlenen verilerin hukuksal koşulları" başlığı altında açıklandığı gibi, bu istisnaların uzaktan eğitim süreçleri ve kullanılan UES'ye yönelik olarak güncellenerek, daha anlaşılır ve uygulanabilir hale getirilmediği görülmektedir.

COVID-19 salgını süreci sonrasında YÖK (2020d) ve üniversite senatolarının kararları gereğince, 2020-2021 güz döneminden itibaren örgün öğretimdeki her bir programın derslerinin asgari %10'unun uzaktan öğretim ile verilmesi kararlaştırılmıştır. Bu karar ile bundan sonraki yıllarda da kullanılacak olan UES'lerin kullanıcıları ve içerik sağlayıcıları olan öğrenciler ile öğretim elemanlarında farkındalığın oluşacağı ve bu sistemler üzerinde kişisel hakların korunması konusunda gelecek yıllarda daha fazla hassasiyet gösterileceği düşünülmektedir.

Öneriler

COVID-19 salgını sürecinde UES'ler eğitimde büyük kolaylık sağlamış olsa da bu sistemler üzerindeki kişisel hakların korunmasını sağlayan hukuksal düzenlemelerin askıya alınamayacağı unutulmamalıdır. UES'lerde kişisel verilerin hukuka aykırı olarak işlenmesi ve erişilmesi önlenerek hukuka uygun olarak muhafazasının sağlanabilmesi için verilerin niteliği ve muhafaza edildiği ortam göz önünde bulundurularak kişisel veri güvenliği rehberi (KVK Kurumu, 2018a) çerçevesinde teknik ve idari tedbirler alınmalıdır. Ayrıca bu çerçevede, UES'lere ilişkin bazı çalışmaların YÖK tarafından başlatılması gerektiği düşünülmektedir. Örneğin, uzaktan eğitim standartları YÖK tarafından COVID-19 salgını süreci de dikkate alınarak yeniden belirlenmeli ve uygulamaların belirlenen standartlara uygunluğu izlenmelidir. İlgili kurumlarla iş birliği yapılarak üniversitelerin uzaktan öğretim altyapısı desteklenmeli ve belirli düzeyde güvenlik standardının sağlanması için mümkün olması halinde YÖK tarafından merkezi veri depolama ortamları oluşturularak üniversitelerin kullanımına sunulmalıdır. Bununla beraber UES üzerinde işlenen hassas verilere yönelik olarak, KVK Kurulu'nun (2018) "özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler" ile ilgili almış olduğu 31/01/2018 tarihli ve 2018/10 sayılı kararı dikkate alınmalıdır. Bunun yanı sıra UES'lerdeki eksikliklere bağlı kişisel hak ihlallerinin önüne geçilebilmesi amacıyla uzaktan eğitim sürecinde tüm üniversitelerin dikkate alacakları ve temel kavramları da açıklayan bir uygulama rehberinin oluşturulması için çalışmaların başlatılması önem taşımaktadır. Söz konusu rehberlerin oluşturulmasında, İngiltere'deki eğitim kurumları için hazırlanan benzer taslakların da (United Kingdom Department for Education, 2018) örnek alınabileceği düşünülmektedir. Bu kapsamda tüm üniversitelerin uzaktan eğitim sürecinde sağlamaları gereken asgari standartların belirlenmesi sürecinde KVK Kurulu'nun da görüşleriyle katkı sunması önem taşımaktadır.

Araştırmadan elde edilen bulgulara bağlı olarak UES'lerin veri koruma gereksinimlerine uyması ve bu kapsamda bireylerin gizlilik haklarının korunabilmesi için UES'yi tasarlayan ve yöneten birimlerin yanı sıra bu sistemlere ilişkin bilgi yönetim süreçlerinde sorumluluk alan bilgi profesyonellerinin öncelikli olarak dikkate almaları gereken hususlar şunlardır;

- UES'lerin veri koruma gereksinimlerine uyması ve bireylerin gizlilik haklarının korunabilmesi için hukuksal amaçlar doğru olarak belirlenmelidir.
- Üniversitelerde KVKK'ya (2016) uygun olarak geliştirilen veri koruma ve bilgi güvenliği politikaları, UES'yi de kapsayacak şekilde gözden geçirilmelidir.
- UES'lerde veri sahibinin haklarının korunabilmesi için öncelikle bu süreçteki katılımcıların rolleri ("Veri Denetleyicisi", "Veri İşlemcisi", "Veri Konusu") açık olarak tanımlanmalıdır.

- Verilerin depolanması ve erişim işlemlerinde KVK Kurulu'nun (2018) da dikkat çektiği gibi kriptografik yöntemler kullanılmalıdır. Özellikle sistem erişimi için gerekli şifreler tahmin edilebilir ya da elde edilebilir bilgilerden oluşturulmamalı ve kullanıcıların da bu tür bilgileri kullanmamaları için gerekli teknik önlemler alınmalıdır.
- UES üzerinden oluşturulan ders kayıtlarına sadece dersi alan öğrencilerin kurumsal kimlik denetimi sonrasında girişleri sağlanmalıdır.
- Öğrencilerin dersleri takip edebilmesi amacıyla oluşturulan video vb. materyallerinin sosyal paylaşım siteleri gibi sanal ortamlar üzerinden herkese açık şekilde paylaşılmaması konusunda uyarılar yapılmalıdır.
- UES'lerdeki veriler üzerinde gerçekleştirilen tüm işlemler güvenliği sağlanarak kayıt altına alınmalıdır. Gerekli hallerde bu kayıtlar adli mercilere verilebilecek şekilde korunmalı ve saklanmalıdır.
- Senkron (canlı) derslerin kaydedildiği ortamlar ve kayıt ortamının güvenliğinin sağlanmasına yönelik risk değerlendirmesi yapılmalıdır.
- Senkron ders videolarının öğrenciler tarafından indirilebilmesi ve uzun bir zaman aralığından sonra farklı platformlardan (yurt dışı vb.) paylaşılması halinde, izlenecek yöntemlerin (hukuksal hakların korunması açısından) neler olduğuna yönelik belirsizlikler giderilmelidir.
- Uzaktan öğretimle yürütülen derslere yönelik ölçme ve değerlendirme yöntemleri gözden geçirilerek, asgari güvenlik standartları belirlenmelidir.
- Öğrenci ve öğretim elemanları UES'nin riskleri ve kişisel hakların korunması konusunda üniversitelerin uzaktan eğitim merkezleri tarafından bilgilendirilmeli ve gerekli uyarılar yapılmalıdır.
- Üniversiteler çevrimiçi kaynakları kullanmak istediklerinde, hukuksal gerekliliklere bağlı olarak veri sahibinin onayını almalıdırlar.

Çıkar Çatışması

Bu araştırmada, verilerin toplanması, sonuçların yorumlanması ve makalenin yazılması süreçlerine ilişkin yazarlar arasında herhangi bir çıkar çatışması bulunmamaktadır. Ayrıca çalışmada veri kaynağı olarak kullanılan kurumları herhangi bir maddi veya manevi zarara uğratacak açıklamalara yer verilmemiştir.

Yazarlık Katkısı

Makalenin yazarları; araştırmanın planlanması, verilerin toplanması, istatistiksel analiz ve verilerin yorumlanması, makalenin yazımı, makalenin içeriğinin gözden geçirilmesi ve denetlenmesine eşit katkıda bulunmuşlardır.

Etik Kurul Kararları ve İzinler

Makale, etik kurul izin belgesi gerektirmeyen bir çalışmadır.

Kaynakça

Al, U. ve Madran, O. (2004). Web tabanlı uzaktan eğitim sistemleri: Sahip olması gereken özellikler ve standartlar. *Bilgi Dünyası, 5*(2), 259-271. https://bd.org.tr/index.php/bd/article/view/491/487

Alıntı. (t. y.). *Türk Dil Kurumu Güncel Türkçe Sözlük* içinde. https://sozluk.gov.tr/

Anwar, M. (2020). Supporting privacy, trust, and personalization in online learning. *International Journal of Artificial Intelligence in Education*, 1-15. https://doi.org/10.1007/s40593-020-00216-0

Arslanlı, H. (1954). *Fikri hukuk dersleri II: Fikir ve sanat eserleri*. İstanbul Üniversitesi Hukuk Fakültesi Yayınları.

Aşırma. (t. y.). *Türk Dil Kurumu Güncel Türkçe Sözlük* içinde. https://sozluk.gov.tr/

Ballard Spahr LLP. (2020, 27 Nisan). *Remote learning – privacy and data security challenges.* https://www.jdsupra.com/legalnews/remote-learning-privacy-and-data-66888/

Bozgeyik, H. (2015). Telif hukukunda eğitim istisnası. *Ticaret ve Fikri Mülkiyet Hukuku Dergisi, 1*(2), 23-36. http://dergipark.org.tr/tr/download/article-file/199324

Brough, A. R. ve Martin, K. D. (2020). Consumer privacy during (and after) the COVID-19 pandemic. *Journal of Public Policy & Marketing, 40*(1), 108-110. https://doi.org/10.1177/0743915620929999

Çakmak, A. Ç. (2013). Uzaktan eğitim hizmetinin öğrenciler tarafından değerlendirilmesi: Karabük Üniversitesi'nde bir uygulama. *İstanbul Ticaret Üniversitesi Sosyal Bilimleri Dergisi, 12*(23), 263-287. https://ticaret.edu.tr/uploads/yayin/sosyal23/15_263_287_Sosyal_23.pdf

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., Gupta, B., Lal, B., Misra, S., Prashant, P., Raman, R., Rana, N.P., Sharma, S.K. ve Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management, 55*, 102211. https://doi.org/10.1016/j.ijinfomgt.2020.102211

Ebner, M., Schön, S., Braun, C., Ebner, M., Grigoriadis, Y., Haas, M., Leitner, P. ve Taraghi, B. (2020). COVID-19 epidemic as e-learning boost? Chronological development and effects at an Austrian University against the background of the concept of "e-learning readiness". *Future Internet, 12*(6), 94. https://doi.org/10.3390/fi12060094

Fikrî ve Sinaî Haklar Araştırma ve Uygulama Merkezi. (2003). *Üniversitelerde fikir ve sanat eserleri: Yolsuz iktibas*. Ankara Üniversitesi Fikrî ve Sınaî Haklar Araştırma ve Uygulama Merkezi.

Fikir ve Sanat Eserleri Kanunu. (1951, 5 Aralık). *Resmi Gazete* (Sayı: 7981). https://www.mevzuat.gov.tr/MevzuatMetin/1.3.5846.pdf

Google Cloud. (2020a). *How Google uses encryption to protect your data.* https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf

Google Cloud. (2020b). *Google Cloud & the General Data Protection Regulation (GDPR).* https://cloud.google.com/security/gdpr#tab2

Google Cloud. (t. y.) *Ravelin: Embracing open with Google Cloud platform.* https://cloud.google.com/customers/ravelin

Hamilton, I. A. (2020, 31 Mart). *Zoom is being sued for allegedly handing over data to Facebook.* https://www.businessinsider.com/zoom-sued-allegedly-sharing-data-with-facebook-2020-3

Harwell, D. (2020, 1 Nisan). *Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance*. https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/

He, W., Zhang, Z. J. ve Li, W. (2021). Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. *International Journal of Information Management, 57*, 102287. https://doi.org/10.1016/j.ijinfomgt.2020.102287

Institute of Electrical and Electronics Engineers. (2014). Students' data privacy: How far it is protected? (Ethical Percpective). *2014 International Conference on Interactive Collaborative Learning (ICL)* (ss. 619-622) içinde. IEEE. https://doi.org/10.1109/ICL.2014.7017843

Karasar, N. (2012). *Bilimsel araştırma yöntemi* (23. bs). Nobel Akademi Yayıncılık.

Kişisel Verilerin Korunması Kanunu. (2016, 24 Mart). *Resmî Gazete* (Sayı: 29677). http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

Kişisel Verileri Koruma Kurulu. (2018). *"Özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 sayılı kararı.* https://www.kvkk.gov.tr/Icerik/4110/2018-10

Kişisel Verileri Koruma Kurulu. (2020, 7 Nisan). *Uzaktan eğitim platformları hakkında kamuoyu duyurusu.* https://www.kvkk.gov.tr/Icerik/6723/Uzaktan-Egitim-Platformlari-Hakkinda-Kamuoyu-Duyurusu

Kişisel Verileri Koruma Kurumu. (2018a). *Kişisel veri güvenliği rehberi (teknik ve idari tedbirler)*. KVKK Yayınları. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf

Kişisel Verileri Koruma Kurumu. (2018b). *Kişisel verilerin korunması kanunu hakkında sıkça sorulan sorular*. KVKK Yayınları. https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular

Kişisel Verileri Koruma Kurumu. (2020a, 9 Mart). *Taahhütnameler*: *Veri sorumlusundan veri işleyene aktarım.* https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler

Kişisel Verileri Koruma Kurumu. (2020b, 7 Mayıs). *Yurt dışına kişisel veri aktarımında hazırlanacak taahhütnamelerde dikkat edilmesi gereken hususlara ilişkin duyuru.* https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU

Kişisel Verileri Koruma Kurumu. (t. y.). *Açık rıza*. KVKK Yayınları. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf

Lakshminarayanan, K. ve Hashim, S. (2020, 8 Nisan). *Secure connections: How Google Meet keeps your video conferences protected.* Google Cloud. https://cloud.google.com/blog/products/g-suite/how-google-meet-keeps-video-conferences-secure

Lin, N. (1976). *Foundations of social research*. McGraw-Hill.

Manfuso, L. G. (2020, 30 Nisan). *Protecting data privacy in a remote learning landscape.* https://edtechmagazine.com/higher/article/2020/04/protecting-data-privacy-remote-learning-landscape

Mannino, N. (2018, 14 Haziran). *What is FERPA and how does it impact guardians and college students?* Azusa Pacific University. https://www.apu.edu/articles/what-is-ferpa-and-how-does-it-impact-parents-and-college-students/

Moodle. (2020). *Higher education*. https://moodle.com/solutions/higher-education/

Morris, D. Z. (2020, 2 Nisan). *Zoom meetings keep getting hacked. Here's how to prevent 'Zoom bombing' on your video chats.* https://fortune.com/2020/04/02/zoom-bombing-what-is-meeting-hacked-how-to-prevent-vulnerability-is-zoom-safe-video-chats/

O'Leary, D. E. (2020). Evolving information systems and technology research issues for COVID-19 and other pandemics. *Journal of Organizational Computing and Electronic Commerce, 30*(1), 1-8. https://doi.org/10.1080/10919392.2020.1755790

Orchison, M. ve Rigg, K. (2020, 27 Mart). *Data protection and privacy implications of online and remote learning.* https://www.cois.org/about-cis/news/post/~board/perspectives-blog/post/data-protection-and-privacy-implications-of-online-and-remote-learning

Pehlivanova, T. ve Kanchev, K. (2020). Data privacy aspects of e-learning. *Proceedings of the 15th International Conference On Virtual Learning ICVL 2020* içinde (ss.291-296). University of Bucharest. http://www.c3.icvl.eu/papers2020/37.pdf

Poland Personal Data Protection Office. (2020a). *Good practices that help keep data secure during online lessons.* https://uodo.gov.pl/en/file/401

Poland Personal Data Protection Office. (2020b). *Security of personal data during remote learning.* https://uodo.gov.pl/en/file/402

Romansky, R. (2014). *Problems of privacy and data protection in online learning based on the network space.* http://e-university.tu-sofia.bg/e-publ/files/2897_Privacy%20%26%20Online%20learning.pdf

Sezer, Y. ve Bilgin, H. (2010). Sözlü sınavların yargısal denetimi. *Türkiye Barolar Birliği Dergisi, 86*(1), 168-187. http://tbbdergisi.barobirlik.org.tr/m2010-86-580

Spicer, D. Z. (2020). New privacy legislation and online education. *International Journal on Innovations in Online Education, 4*(2). https://doi.org/10.1615/IntJInnovOnlineEdu.2020032793

Student Privacy Policy Office. (2020). *FERPA & Coronavirus disease 2019 (COVID-19): Frequently asked questions (FAQs).* https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20and%20Coronavirus%20Frequently%20Asked%20Questions_0.pdf

Türk Borçlar Kanunu. (2011, 11 Ocak). *Resmî Gazete* (Sayı: 27836). https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6098.pdf

Türk Ceza Kanunu. (2004, 26 Eylül). *Resmî Gazete* (Sayı: 25611). http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf

Türk Medeni Kanunu. (2001, 22 Kasım). *Resmî Gazete* (Sayı: 24607). https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf

United Kingdom Department for Education. (2018). *Data protection: A toolkit for schools.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf

Yargıtay. (2000). *Yargıtay kararı* (Esas No: 2000 / 7065, Karar No: 2000 / 9425). https://www.hukukturk.com/yargitay-kararlari?EsasNo1=2000&EsasNo2=7065&KararNo1=2000&KararNo2=9425

Yıldız, H. (2019). FSEK kapsamında korunan eserlerin eğitim-öğretim amacıyla kullanımı. *Terazi Hukuk Dergisi, 14*(152), 855-867. https://jurix.com.tr/article/18827#

Yükseköğretim Kurulu. (2014). *Yükseköğretim Kurumlarında Uzaktan Öğretime İlişkin Usul ve Esaslar.* https://www.yok.gov.tr/Documents/Kurumsal/egitim_ogretim_dairesi/Uzaktan_ogretim/yuksekogretim_kurumlarinda_uzaktan_ogretime_iliskin_usul_ve_esaslar.pdf

Yükseköğretim Kurulu. (2020a). *Koronavirüs (Covid-19) bilgilendirme notu: 1.* https://covid19.yok.gov.tr/Documents/alinan-kararlar/02-coronavirus-bilgilendirme-notu-1.pdf

Yükseköğretim Kurulu. (2020b). *YÖK başkanı Saraç üniversitelerde verilecek olan uzaktan eğitime ilişkin açıklama yaptı.* https://covid19.yok.gov.tr/Documents/alinan-kararlar/03-uzaktan-egitime-iliskin-alinan-karar.pdf

Yükseköğretim Kurulu. (2020c). *"YÖK Dersleri Platformu" öğrencilerin erişimine açıldı.* https://covid19.yok.gov.tr/Documents/alinan-kararlar/04-yok-dersleri-platformu-erisime-acildi.pdf

Yükseköğretim Kurulu. (2020d, 4 Haziran). *Küresel salgın ile mücadele sürecinde yeni düzenlemeler - II.* https://www.yok.gov.tr/Sayfalar/Haberler/2020/kuresel-salgin-surecinde-yapisal-duzenlemeler-2.aspx

Yükseköğretim Kurulu. (2020e, 3 Mayıs). *Üniversitelerdeki uzaktan eğitime yönelik değerlendirme: Salgın sürecinde üniversitelerdeki uzaktan eğitimin bir aylık durum tespiti.* https://www.yok.gov.tr/Sayfalar/Haberler/2020/uzaktan-egitime-yonelik-degerlendirme.aspx?fbclid=IwAR2KzZwUqqjE6InsGV1Ocbtz8pWDimPhI6arTMYEbVss2YtjuMUOs7WBrNM

Yükseköğretim Kurulu. (2020f, 11 Mayıs). *YÖK'ten üniversitelerdeki sınavların yüz yüze gerçekleştirilmeyeceğine ilişkin karar.* https://www.yok.gov.tr/Sayfalar/Haberler/2020/yok-ten-sinavlara-iliskin-karar.aspx

Yükseköğretim Kurulu. (2020g, 27 Mayıs). *YÖK, üniversitelerde dijital ortamda gerçekleştirilebilecek sınavların temel ilkelerini açıkladı.* https://www.yok.gov.tr/Sayfalar/Haberler/2020/universitelerde-dijital-sinavlarin-temel-ilkeleri.aspx

Yükseköğretim Kurulu. (2020h). *COVID-19 bilgilendirme: Pandemi sürecinde üniversitelerimizdeki*