Adli Bilimler ve Suç Araştırmaları Dergisi

ISSN: 2687-3397
Yıl: 2, Cilt: 2, Sayı: 1, Haziran 2020 s.24-34 Makale Türü: Araştırma
Makalenin Geliş Tarihi: 30/04/2020 Makalenin Kabul Tarihi: 14/05/2020

Covıd-19 İnfeksiyonu Nedeni ile Kullanımı Artan Elektronik İmzanın Adli Bilimler Açısından Önemi

Emrah Emiral[*], Dilek Kiliç[**], Nergis Cantürk[***]

Öz: Dünya Sağlık Örgütü tarafından pandemi ilan edilen Covid-19 enfeksiyonu nedeni ile alınan tedbirler kapsamında kişiler arası ilişkilerin büyük bir bölümü elektronik ortama taşınmıştır. Sosyal ilişkilerimize engel getiren karantina uygulaması, esnek mesai sistemi ile çalışılan ortamlar elektronik imzanın daha yaygın bir şekilde kullanılmasına neden olmuştur. 15.01.2004 tarihli 5070 sayılı Elektronik İmza Kanunu ile yaşamımıza girmiştir. Elektronik ortamda yapılan yazılı işlemler sahtecilik suçlarına yeni bir boyut kazandırma potansiyeline sahiptir. Yapılan işlemi yürüten kişinin kimliklendirmesi sorunu siber suç alanında görev yapan birimlerin alanına dâhil olmuştur. HMK'nın 210. maddesi; "güvenli elektronik imzayla oluşturulmuş verinin inkârı hâlinde, hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılamamışsa, bilirkişi incelemesine başvurulur." hükmünü içermektedir. (Hukuk Muhakemeleri Kanunu, Madde:210) .1086 Sayılı Hukuk Usulü Muhakemeleri Kanunu ("HUMK") yürürlükte iken bu hususta açık bir hüküm bulunmadığından, güvenli elektronik imzanın inkârı durumunda HUMK'nın 308. Maddesi uyarınca imza incelenmekteydi. Kamusal alanda e-imzanın kullanım alanları; KPSS, YDS, ALES gibi başvurular, sağlık uygulamaları, vergi ödemeleri, elektronik beyannameler, pasaport başvurularıdır. Bu çalışmamızda günlük yaşantımızda yeri olan ve pandeminin etkisi ile kullanımı artan elektronik imzanın adli bilimlerdeki önemine dikkat çekilmesi amaçlanmıştır.

Anahtar kelimeler: Covid-19, Elektronik İmza, Belge İnceleme, Siber Suçlar, Elektronik İmza Kanunu

[*] Öğretim Görevlisi Dr., Ankara Üniversitesi Tıp Fakültesi Adli Tıp Anabilim Dalı, Adli Tıp Uzmanı, 5326428164, dr.emrahemiral@gmail.com, ORCİD ID: 0000-0003-2464-7039.

[**] Gülhane Eğitim ve Araştırma Hastanesi Çocuk Cerrahisi AD. Keçiören Ankara, kilic06dilek@gmail.com, ORCİD ID; 0000-0003-2685-6774.

[***] Profesör Dr., Ankara Üniversitesi Adli Bilimler Enstitüsü, Adli Tıp Uzmanı, 5367902390, nergiscanturk@yahoo.com, ORCİD ID; 0000-0001-8739-0723.

Turkish Journal of Forensic Science and Crime Studies

ISSN: 2687-3397
Year: 2, Volume: 2, Issue: 1, June 2020 p.24-34 Article Type: Research Article
Received Date: 30/04/2020 Accepted Date: 14/05/2020

The Importance of ElectronIc Signature Which has an Increasing Usage Due to the Covid-19 Infection With Regards to the Forensic Science

Emrah Emiral, Dilek Kiliç, Nergis Cantürk

Abstract: As part of the measures taken due to the Covid-19 infection, which has been declared as a pandemic by WHO (World Health Organization), most of the interpersonal relations have been transferred to the electronic environment. Quarantine application, which obstructs our social relations in environments with flexible schedules, has enabled the use of electronic signature more widely. It has started to have an impact in our lives with the Electronic Signature Law No.5070 dated 15.01.2004. The written procedures in electronic form have the potential to bring in a new dimension to fraud crimes. The matter of identification of the person who carries out the transition is included in the units that are dealing with the field of cybercrime. Article no.210 of the CPL contains the provision stating; "in case of a denial of a data created with a secure electronic signature, if no conclusion is reached by the judge after the party has been heard denying the data, an expert investigation is to be applied." (Civil Procedures Law, Article no:210) While the Code of Civil Procedure No.1086 was in force, in case of a denial of a secure electronic signature, since there was no explicit provision indicating this matter, the signature was to be investigated in accordance with Article no. 308 of the Code of Civil Procedure. The use of e-signature in public spaces are like; applications for KPSS, YDS, ALES, health practices, tax payments, electronic statements and passport applications. In this study, it is aimed to draw attention to the importance in the forensic science of electronic signature which has a place in our daily lives and also has an increasing usage due to the pandemic.

Key words: Covid-19, Electronic Signature, Document Review, Cybercrime, Electronic Signature Law

Giriş

İlk defa Aralık ayında Çin'in Wuhan, Hubei şehrinde etkeni daha önce tanımlanmamış şiddetli pnömoni vakaları bildirilmiştir. Yapılan çalışmalar sonucunda 7 Ocak 2020'de yeni bir koronavirüs tanımlanmıştır ("WHO, Novel Coronavirus (2019-nCoV) SITUATION REPORT - 1 21 JANUARY 2020,"). 11 Şubat 2020'de Dünya Sağlık Örgütü hastalığı koronavirüs hastalığı 2019 (COVID-19) olarak adlandırmıştır. Aynı günlerde Uluslararası Virüs Taksonomisi Komitesi'nin Koronavirus Çalışma Grubu (CSG), hastalık etkenini ciddi akut solunum sendromu koronavirüs 2 (SARS-CoV-2) olarak isimlendirmiştir (Jiang et al., 2020). Çok kısa sürede Çin dışında 113 ülkeye yayılan hastalık 11 Mart 2020 de DSÖ tarafından pandemi ilan edilmiştir ("WHO, Coronavirus disease 2019 (COVID-19) Situation Report – 51,"). Ülkemizde de aynı tarihte ilk pozitif olgunun duyurulmasıyla başlayan salgın sürecinin etkisi halen devam etmektedir. 07.06.2020 tarihi itibariyle ülkemizde 169.218 pozitif vaka ve 4.669 ölüm sayısı bildirilmiştir ("Coronavirus disease (COVID-19) Situation Report – 139. 07/06/2020,")

11 Mart 2020 tarihinden sonra tüm dünyayı tehdit etmeye devam eden Covid-19 enfeksiyonunun Türkiye'deki vaka sayılarının artışıyla; 14 Mart 2020 itibariyle hudut kapılarından Türkiye'ye giriş çıkışlar kapatıldı ("81 İl Valiliği ve Hudut İdare Mülki Amirliklerine Genelge 13/03/2020,"). Tiyatro, sinema gibi sosyal alanlarda yapılan toplu etkinlikler yasaklandı. Restorant, çay bahçesi gibi kalabalık olabilecek işletmelerin faaliyetleri durduruldu ("81 İl Valiliğine Coronavirüs Tedbirleri Konulu Ek Bir Genelge Daha Gönderildi. 16/03/2020,"). Sosyal temasın en aza indirilmesi amaçlanmıştır. Ayrıca 21 Mart 2020 itibariyle 65 yaş üstü ve kronik hastalığı olan kişilere, 3 Nisan 2020 itibariyle 20 yaş altına dışarı çıkma yasağı getirilmiştir ("Şehir Giriş/Çıkış Tebirleri ve Yaş Sınırlaması 03/04/2020,"). Alınan bu tedbirler nedeniyle fiziksel olarak bir araya gelemeyen taraflar, hukuki işlemlerini uzak mesafelerden çözmek amacı ile kendilerine elektronik imza gibi alternatif yöntemler bulmuşlardır. Bu yöntemler değer kazanmış olup elektronik ortamlarda hazırlanan belgelerin korunması sorunu ortaya çıkmıştır.

Türk Dil Kurumu imzayı "Bir kimsenin herhangi bir belgeyi yazdığını veya onayladığını belirtmek için her zaman aynı biçimde kullandığı işaret" şeklinde tanımlamıştır ("İmza, Türk Dil Kurumu Sözlükleri"). Çeşitli resmi veya özel belgelerin hukuki bakımdan geçerli olabilmesi için üzerinde bulunması gereken en önemli unsurlardan biri imzadır. Bu açıdan kişiye hak sağlayan ve sorumluluk altına alan bir araçtır (Bengshir ve Topcan, 2008).

Elektronik imza kanununun 16. maddesinde "İmza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar." denilmiştir ("Elektronik İmza Kanunu"). Islak imza sahteciliklerinde kullanılan el yazısı ve imza karakteristik özellikleri elektronik imza

incelemelerinde yapılamamaktadır (Delipınar, 2012). Güvenli elektronik imzalı bir belge üzerinde sonradan yapılan herhangi bir değişiklik belgenin hash değerinin değişmesine neden olur ve belgede bulunan elektronik imzanın kalkmasına sebep olur. Hash değeri, bir dosyanın parmak izi gibidir. Dosyalar, karmaşık algoritmalarla taranarak özgün bir parmak izi yığını oluşturulur (Gözel, 2015). Avrupa Siber Suçları Sözleşmesi'nin 7. maddesinde elektronik verilerde sahtecilik fiili düzenlenmiştir ("TBMM Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu 3/9/2012,") Bu sözleşmenin resmi çevirisi "Sanal Ortamda İşlenen Suçlar Sözleşmesi" olarak bilinmektedir. ("Sanal Ortamda İşlenen Suçlar Sözleşmesi,"). Sözleşme ülkemizde 22/04/2014 tarihinde 6533 sayılı kanunla kabul edilmiştir. ("Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun,"). Elektronik belgeler üzerinden işlenen suçlara verilecek cezalar da Türk Ceza Kanunun 244. Maddesinde düzenlenmiştir ("Türk Ceza Kanunu ").

Elektronik İmza

Elektronik imza, Avrupa Birliği Direktifi doğrultusunda pek çok ülkenin kanunlarında tanımlanmıştır. 5070 sayılı Elektronik İmza Kanunu'nda elektronik imza "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" olarak tanımlanmıştır ("Elektronik İmza Kanunu,"). Bu tanım ile elektronik imzanın elektronik veriden farklı olduğu ve elektronik belgeye eklendiği, eklendiği veriyle mantıksal bağlantı kurulması gerektiği ve bu mantıksal bağlantı kurulmasının kimlik doğrulama için yapıldığı vurgulanmıştır (Yalçınkaya, 2008). Ayrıca kanunda güvenli elektronik imzanın, elle atılan ıslak imza ile aynı hukukî sonuçları doğuracağı vurgulanmıştır. Elektronik imzaya ihtiyaç duyulmasındaki en önemli sebep gelişen teknolojik şartlarda elektronik ortamda yapılan hukuki işlemleri güven altına almak, belgeleri düzenleyen kişileri tespit etmek ve imzaların inkâr edilmesini önlemektir (Erturgut, 2004). Elektronik imzalar birçok farklı formatlarda karşımıza çıkmaktadır. Bunlar; biyometrik yöntemler (yüz taraması, retina taraması ve parmak izi taraması gibi), PIN kodları, ıslak imzanın tarayıcıda taranarak elektronik ortama aktarılması, bilgisayar ekranlarına özel kalemlerle atılan imza ve çift anahtarlı kriptografiyle yapılan dijital imzalar şeklinde sayılabilir (Gözel, 2015). Elektronik imzalar; idareye yapılan başvurularda (YDS, ALES gibi sınavlar, pasaport işlemleri), kurum içi işlemlerde (personel izinleri, vergi ödemeleri, bordro işlemleri personel kimlik kartı, bina giriş sistemleri, yönetim kurulu kararları, sözleşme yapma vb), kurumlar arası ilişkilerde (Emniyet Müdürlükleri, Nüfus ve Vatandaşlık İşleri Müdürlükleri vb), sağlık hizmetlerinde (sağlık personeli, e-nabız, e-reçete gibi), belediye hizmetleri sosyal güvenlik uygulamaları, üniversite hizmetleri ve daha birçok alanda kullanılmaktadır (Yılmaz, 2016).

Elektronik İmza Çeşitleri

Elektronik imzaların; basit elektronik imza, gelişmiş elektronik imza, güvenli elektronik imza ve akredite edilmiş sertifika hizmet sağlayıcısı tarafından verilen imza olmak üzere 4 farklı çeşidi bulunmaktadır.

Basit Elektronik İmza

Basit elektronik imza, elektronik formlarda bulunan verilere eklenen veya mantıksal olarak bağlı bulunan ve bir kişi tarafından imza atmak amacıyla kullanılan elektronik form verilerdir. Tarayıcıdan geçirilerek elektronik belgelere eklenen elle atılmış imza, 'KABUL EDİYORUM' sekmesine tıklanması, PIN kodu girilmesi, elektronik posta sonuna eklenen imzalar basit elektronik imzaya örnek olarak gösterilebilir (Şimşek vd,, 2019).

Gelişmiş Elektronik İmza

Yalnızca imzayı atan kişiye bağlı olan; kişinin kimliğinin belirlemesinde olanak sağlayan; yalnızca imzayı atan kişinin kontrolünde tutulacağı araçlar ile meydana getirilen ve üzerinde sonradan meydana gelen değişikliklerin anlaşılmasına olanak veren elektronik imza çeşididir (Yılmaz, 2016).

Güvenli Elektronik İmza

Güvenli elektronik imzalar, gelişmiş elektronik imzanın bütün özelliklerini içermekle birlikte nitelikli bir elektronik sertifikaya sahip olan ve güvenli imza oluşturma araçları kullanılarak üretilmiş imzalardır (Yalçınkaya, 2008). Islak imzanın kişi aidiyeti gibi elektronik imza da herhangi bir elektronik belgeye atılan imzalanın verisinin atan kişi tarafından atılıp atılamadığını. Karşılaştırılmalı hukuktaki mevzuatta bulunan tanım elektronik imza tanımı ile uyumludur. Bazı kaynaklarda elektronik imza dijital imza olarak da isimlendirilmektedir (Belgin, 2009).

Güvenli elektronik imzanın unsurları Elektronik İmza Kanunu'nun 4. Maddesinde;

> *"a. Münhasıran imza sahibine bağlı olan,*
> *b. Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,*
> *c. Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,*
> *d. İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan, elektronik imzadır."*
> şeklinde tanımlanmıştır. *("Elektronik İmza Kanunu,").*

Akredite Edilmiş Sertifika Hizmet Sağlayıcısı Tarafından Verilen İmza

Elektronik imzanın doğrulanmasında gerekli olan veriyi ve imza sahibine ait kimlik bilgilerini içeren elektronik ortamda bulunan kayıt elektronik sertifika olarak

tanımlanmaktadır. Kişilerin ve kurumların bilgileri güvenli bir şekilde iletilmesini sağlamaktadır (Durak, 2016). Akreditasyon sistemi Türk hukukumuzda sertifika hizmet programı sağlayıcılar bakımından kabul edilmemiştir (Arslan, 2015).

Elektronik İmzaya İlişkin Uluslararası Gelişmeler

Birleşmiş Milletler

Birleşmiş Milletler Uluslararası Ticaret Komisyonu (UNCITRAL) 16 Aralık 1996 tarihinde "Elektronik Ticaret Model Kanunu" yayınlamıştır. Oluşturulan model zaman içerisinde geliştirilmiştir. Model kanun Singapur ve Güney Kore tarafından kanunlaştırılmış ve birçok ülkenin yasama organlarını etkilemiştir ("Basic facts about the United Nations Commission on International Trade Law," 2013). Model kanunda elektronik, optik veya benzeri araçlar ile oluşturulan, gönderilen, alınan veya depolanan bilgi "veri iletisi" olarak tanımlanmıştır. Model kanuna göre "veri iletisi" daha sonra ulaşılabilir formda olmak şartıyla yazılı bir belgenin hukuki etkisine sahiptir. Yine bu modele göre elektronik belge oluşturulması ve belge içeriğinin onaylanması aşamasında güvenilir elektronik bit yöntem kullanılması yazılı imzaya eşdeğerdir (Uncitral Model Law On Electronic Signatures, 2001).

Avrupa Birliği

Avrupa Konseyi, 13 Aralık 1999 tarihinde 1999/93 sayılı Elektronik İmza Yönergesini kabul etmiştir. Yönerge, elektronik imza işlemleri ve güvenlik standartları konusunda alınması gerekli asgari tedbirleri belirtmektedir ("Community Framework For Electronic Signatures," 1999; Keserberber, 2000). Yönergede elektronik imza, mantıksal olarak bir elektronik veriye eklenen veya bir belgeye iliştirilen ve doğrulama şekli olarak isimlendirilmiştir. Yönergede bulunan hükümler, elektronik imza sertifikasyon servis sağlayıcılarının kurulmasına ve denetlenmesini kapsamaktadır. Yönerge kamusal alanda elektronik imzanın kullanılmasında gereken alt yapının oluşturmasının gerekli olduğuna vurgu yapılmakta olup, üye ülkelerin hukuksal olarak ıslak imza ve elektronik imzayı eş değer tutan düzenlemeleri şart koşmaktadır. Bunun yanı sıra yönerge usul hukuk açısından elektronik belgeyi delil olarak kabul etmektedir.

Amerika Birleşik Devletleri

ABD'de dijital imzayı ilgilendiren ilk kanun 1994 yılında Utah'ta çıkarılmıştır (Richards, 1998). Tüm kamu hizmetlerinin elektronik ortamdan sürdürülmesi amaçlanan "Access America" adlı program ise 1993 yılında başlatılmıştır (Keserberber, 2000). Elektronik imzanın konumu Amerika Birleşik Devletlerinde temel olarak üç kanunla belirtilmiştir. Bu kanunlar "Standart Elektronik İşlemler Yasası", "Ulusal ve Uluslararası Ticarette Elektronik İmza Yasası" ve "Devlette Kırtasiyeciliğin Azaltılması Hakkında Yasa"'dır (Guler, 2008).

Türk Hukuku Açısından Elektronik İmza

Türkiye'de 1997 yılında Bilim ve Teknoloji Yüksek Kurulu'nun Türkiye'de elektronik ticaret ağının kurulmasına ilişkin 97/3 sayılı Kararı ile e-imza çalışmaları başlamıştır. Dış Ticaret Müsteşarlığı'nın başkanlığında kurulan "Elektronik Ticaret Koordinasyon Kurulu" 1998 tarihinde ilk toplantısını gerçekleştirerek hazırladıkları raporu "ETKK Değerlendirme Komisyonu"'na bildirmişlerdir. Bu koordinasyon kurulunda teknik, hukuk ve finans grupları bulunmaktadır. Bu komisyonun hazırladığı kanun tasarısı ile hazırlanan kanun 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de "Elektronik İmza Kanunu" yayınlanmıştır (Sağıroğlu ve Alkan, 2005).

Bu kanun'un "Tanımlar" başlıklı 3. Maddesinde elektronik imza kavramı "başka bir veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacı ile kullanılan veri" şeklinde tanımlanmaktadır. Elektronik imza; sadece iki kişinin erişimine açık olan bir ortamda, bilginin üçüncü tarafların erişimine kapalı, bütünlüğü bozulmadan (bilgiyi ileten kişinin oluşturmuş olduğu ilk ve orijinal haliyle) ve tarafların kimlikleri doğrulanarak iletildiğini, elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşur.

Elektronik imzanın türlerinden biri olan "Güvenli Elektronik İmza" ise Kanun'un 4. Maddesinde tanımlanmıştır. Kanun'un 4. Maddesinde yer alan maddelere göre güvenli elektronik imzada bulunması gerekli olan özellikler aşağıda sıralanmıştır:

- Münhasırın (yalnızca ve özellikle) imza sahibine bağlı olmak,
- Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturmak,
- Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlamak,
- İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlamak.

Kanun'un 5. Maddesinin 1. Fıkrası uyarınca "Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur". Bu kuralın istinası, aynı maddenin 2. Fıkrasında yer almaktadır. Buna göre "Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile banka teminat mektupları dışındaki teminat sözleşmeleri, güvenli elektronik imza ile gerçekleştirilemez".

Kanun'un 22. ve 23. Maddeleri ile Borçlar Kanunu ve Hukuk Usulü Muhakemeleri Kanunu'nun ilgili maddelerinde yapılan değişikliklerle ıslak imza ile imzalanan bir belgenin delil niteliği elektronik imza ile imzalanan belgenin delil olma niteliği ile aynı ölçüdedir. Bunun için, 22. Madde ile Borçlar Kanununun 14 üncü Maddesinin birinci Fıkrasına "Kanunda aksi öngörülmedikçe, imzalı bir mektup, asılları borç altına girenlerce imzalanmış telgraf, teyit edilmiş olmaları kaydıyla faks veya buna benzer iletişim araçları ya da güvenli elektronik imza ile

gönderilip saklanabilen metinler de yazılı şekil yerine geçer" hükmü eklenmiştir ("Borçlar Kanunu,"). 23. Maddeyle ise, Hukuk Usulü Muhakemeleri Kanununa 295/A maddesi eklenmiş ve bu maddede "usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar. Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkâr ederse, bu Kanunun 308 inci maddesi kıyas yoluyla uygulanır." hükmü düzenlenmiştir ("Hukuk Usulü Muhakemelerİ Kanunu"). Türk Ceza Kanunu'nun 244. Maddesi 2. Bendinde "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır." denilmiştir.

Elektronik İmzanın Delil Olarak Değeri

Avrupa Birliği Direktifinin 5. maddesi ıslak imzanın hukuki karşılığı ve delil olma değeri ile gelişmiş elektronik imza kullanılarak oluşturulan veri ve belgelerin etkisinin eşit olduğunu vurgulayarak üye devletlere yargılamada delil olarak kabul edilmesi yükümlülüğünü yüklemiştir; ancak bu yükümlülüğün geçerliliği; elektronik imzanın gelişmiş elektronik imza olması, nitelikli sertifikaya sahip olması ve güvenli imza oluşturma araçları ile oluşturulması şartlarına bağlanmıştır (Yılmaz, 2016). Elektronik İmza Kanunu'nun 5. Maddesinde de "Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur." denilmiştir. Hukuk Usulü Muhakemeleri Kanunun 295/A maddesinde de usulüne uygun olarak oluşturulmuş elektronik verilerin senet niteliğinde olduğu ve aksi ispatlanıncaya kadar kesin delil olduğu vurgulanmıştır ("Hukuk Usulü Muhakemeleri Kanunu"). Elektronik belgelerin delil olarak kabul edilmesi elektronik ticaretin gelişmesi ve internet aracılığıyla yapılan hukuki işlemlerin tercih edilmesi içinde son derece önemlidir. Bu belgelerin delil olarak kabul edilmesindeki ana faktör güvenli elektronik imza ile imzalanmış olmalarıdır (Belgin, 2009).

Elektronik İmzalı Belgeler Hakkında Sahtelik İddiası

Güvenli elektronik imza ile hazırlanan bir veri dava sırasında davalı tarafından inkâr edilebilir. Bu durumda Hukuk Muhakemeleri Kanunu'na göre hâkim veriyi inkâr eden tarafı dinledikten sonra bir kanaate varamaması halinde bu konuda bilirkişi incelemesine karar verecektir ("Hukuk Muhakemeleri Kanunu").

Sahtelik İncelemesi

Hâkim, mahkemeye sunulan elektronik belgenin, güvenli elektronik imza ile imzalanıp imzalanmadığı konusunda kendiliğinden araştırma yapması gerekir. Islak imza ile imzalanan belge ve senetlerde hâkim gözle görülür olan kâğıt üzerinde bir değerlendirme yapabilir. İmzanın sahte olup olmadığı konusunda adli belge in-

celemesi için bilirkişi görüşü isteyecektir. Kâğıt üzerinde yapılan el yazısı ve imza incelemelerinde tersim tarzı, işleklik derecesi, istif (sıkışıklık), eğim, doğrultu, seyir, hız, alışkanlıklar ve baskı derecesi gibi tanıda kullanılan temel unsurlar değerlendirilmektedir (Aşıcıoğlu, 2019). Elektronik belgelerde ise fiziki bir belge ve imza bulunmadığından bu unsurlar kullanılamamaktadır. Bu duruma Hukuk Usulü Muhakemeleri Kanununun 308. maddesi kıyas yoluyla uygulanacaktır. Bu maddenin kıyas yoluyla uygulanması için bakılacak ilk şey elektronik belgenin güvenli elektronik imza ile imzalanmış olup olmadığının tespit edilmesidir. Fakat elektronik belge güvenli elektronik imza dışında bir imza kullanılması durumda, Kanunun 308. maddesinin uygulanması mümkün olmayacaktır.

Sonuç

Covid-19 enfeksiyonu nedeni ile Cumhurbaşkanlığı kararları ve İçişleri Bakanlığı Genelgeleriyle 65 yaş üstü ve 20 yaş altının bireylerin dışarı çıkma yasağı, sosyal ve fiziksel mesafe konulması, kamu ve özel iş yerlerinde dönüşümlü mesai uygulaması gibi önlemler sosyal hayatımız kadar iş hayatımızı da derinden etkilemektedir. Bu dönemde elektronik iletişimin önemi hukuki ve resmi işlemlerde daha da artmıştır. Elektronik alanda yazılan belgeler ve atılan imzalar adli belge niteliği kazanma potansiyeli taşımaktadır.

Sözleşme ve beyan gibi belgelerin internet aracılığıyla uzaktan imzalanmasına olanak verdiği için pratik bir çözüm yolu olarak kullanılabilen elektronik imzaların sıkça kullanılması, ileride oluşabilecek anlaşmazlıklar dikkate alındığında, elektronik imza kullanımının arttığı bu dönemde tarafların hukuki açıdan güvenliklerini sağlanması oldukça önemlidir. Kişilerin kendini hukuki açıdan koruma altına alabilmesi için kullanacakları elektronik imzaları mutlaka Bilgi Teknolojileri ve İletişim Kurumu tarafından yetkilendirilmiş bir Elektronik Sertifika Hizmet Sağlayıcısı tarafından temin etmelidir (Çal vd., 2020). Elektronik belgelerin ve imzaların kullanımının sosyal izolasyonu bir sağlık tedbiri olarak yaygın şekilde kullandığımız Covid-19 enfeksiyonu döneminde artması nedeni ile bu alanda da sahteciliğin artış gösterebileceği dikkate alındığında; kullanıcıların güvenliği için elektronik imza başvurularının mutlaka Bilgi Teknolojileri ve İletişim Kurumu tarafından ilan edilen e-imza hizmet sağlayıcılarının kendi internet sitelerinden yapılması gerekmektedir. Güvenli elektronik imza şartlarına uymayan e-imzaların kullanımı sonucunda yapılan bilirkişi incelemeleri de ıslak imza incelemeleri ile karşılaştırıldığında daha kompleks ve fiziki verinin olmaması sebebiyle tespiti zorlaştırmaktadır.

Kaynakça

81 İl Valiliği ve Hudut İdare Mülki Amirliklerine Genelge 13/03/2020. https://www.icisleri.gov.tr/81-il-valiligi-ve-hudut-idare-mulki-amirliklerine-genelge

81 İl Valiliğine Coronavirüs Tedbirleri Konulu Ek Bir Genelge Daha Gönderildi. https://www.icisleri.gov.tr/81-il-valiligine-koronavirus-tedbirleri-konulu-ek-genelge-gonderildi (E.T.: 16.03.2020).

Arslan, Z. (2015). Electronic signature and current advancements. *GSI Articletter.* C. 13, S.103.

Aşıcıoğlu, F. (2019). *El yazısı incelemesinde temel tanı unsurları (dokuzlar kaidesi). In adli belge inceleme ve sahtecilik alanındaki bilirkişi raporlarının incelikleri*. ss. 25-45. Ankara: Seçkin.

Belgin, D. (2009). Elektronik imzali belgelerin delil değeri (HUMK M. 295/A). *Hukuk Gündemi Dergisi*. C. 2, ss. 37-54.

Bengshir, T., Topcan, F. (2008). Türkiye'de e-imza altyapısı ve kamu kurumlarında uygulamalar. *Amme İdaresi Dergisi.* C. 41, S. 1, ss. 95-111.

Borçlar Kanunu. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6098.pdf

Çal, A., Gündeş, H. ve Gödekoğlu, K. (2020). Elektronik imzanın küresel salgın covid-19 perspektifinden değerlendirilmesi, https://www.ozbek.av.tr/covid-blog/elektronik-imzanin-kuresel-salgin-covid-19-perspektifinden-degerlendirilmesi/ (E.T.: 30 Nisan 2020).

Community framework for electronic signatures. (1999). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=EN

Coronavirus disease (COVID-19) Situation Report – 139. 07/06/2020. In.

Delipinar, A. E. (2012). *Medeni muhakeme hukukunda elektronik imzali belgelerin delil niteliği*. (Yayınlanmamış Yüksek Lisans Tezi). İstanbul Üniversitesi. İstanbul.

Durak, Y. (2016). Elektronik sertifika hizmet sağlayıcısının sorumluluğu. Sirene Belek Hotel, Antalya, Turkey, 14(16), 72.

Elektronik İmza Kanunu. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf

Erturgut, M. (2004). Elektronik imza kanunu bakımından e-belge ve e-imza. *Bankacılar Dergisi*. C. 43, ss. 66-79.

Gözel, A. (2015). Belgede sahtecilik suçlarinin konusu olarak belge ve elektronik belge. *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*. C. 5, S. 1, ss. 143-201.

Guler, M. (2008). Türkiye'de e-imza alanindaki hukuki düzenlemelerin ve kamu kurumlarinda bazi e-imza uygulamalarinin incelenmesi. (Yayınlanmamış Yüksek Lisans Tezi). Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü. Ankara.

Hukuk Muhakemeleri Kanunu. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6100.pdf

Hukuk Usulü Muhakemeleri Kanunu. https://www.mevzuat.gov.tr/MevzuatMetin/5.3.1086.pdf.

İmza. Türk Dil Kurumu Sözlükleri. https://sozluk.gov.tr/

Jiang, S., Shi, Z., Shu, Y., Song, J., Gao, G. F., Tan, W. ve Guo, D. (2020). A distinct name ıs needed for the new coronavirus. *Lancet (London, England).* C. 395, S. 10228, ss. 949-949.

Keserberber, L. (2000). İmzalıyorum o halde varım. Dijital imza hakkındaki yasal düzenlemeler. *Dijital İmzalı Hukuki Belgelerin Hukuki Değeri*. C. 200, S. 2.

Richards, R. J. (1998). The utah digital signature act as model legislation: A critical analysis. *J. Marshall J. Computer & Info. L.* C. 17.

Sağıroğlu, Ş., Alkan, M. (2005). Her yönüyle elektronik imza (e-imza). *Grafiker. Ankara*, C. 3, S, 5.

Sanal Ortamda İşlenen Suçlar Sözleşmesi. https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5-1.pdf

Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun. https://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm

Şehir Giriş/Çıkış Tebirleri ve Yaş Sınırlaması. https://www.icisleri.gov.tr/sehir-giriscikis-tebirleri-ve-yas-sinirlamasi (E.T.: 03 Nisan 2020).

Şimşek, M. M., Özcan, T., Ergun, T. ve Çelik, V. (2019). Elektronik imza seviyeleri. *Bilgi Yönetimi*. C. 2, S. 2, ss. 136-144.

TBMM Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu. https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf (E.T.: 3 Eylül 2012).

Türk Ceza Kanunu. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf

Uncitral Model Law On Electronic Signatures. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf

United Nations. (2013). Basic facts about the united nations commission on ınternational trade law. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/12-57491-guide-to-uncitral-e.pdf

WHO, Coronavirus disease 2019 (COVID-19) Situation Report - 51. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200311-sitrep-51-covid-19.pdf?sfvrsn=1ba62e57_10

WHO, Novel Coronavirus (2019-nCoV) Situation Report - 1. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200121-sitrep-1-2019-ncov.pdf?sfvrsn=20a99c10_4 (E.T.: 21 Ocak 2020).

Yalçınkaya, B. (2008). *Elektronik imzalı belgelerin yönetimi ve arşivlenmesi*. (Yayınlanmamış Yüksek Lisans Tezi). Marmara Üniversitesi, İstanbul.

Yılmaz, M. (2016). Elektronik imzalı belgelerin karşılaştırmalı hukukta ve idarî yargılama hukukunda delil niteliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*. C. 22, S. 3, ss. 3435-3486.