İSTANBUL BİLGİ ÜNİVERSİTESİ
BİLİŞİM VE TEKNOLOJİ HUKUKU ENSTİTÜSÜ

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitümüz öğretim üyelerinden Leyla Keser Berber tarafından kaleme alınan "**BİYOMETRİK İMZA VE TÜRK BORÇLAR KANUNU'NDAKİ YAZILI ŞEKİL ŞARTI İLE HUKUK MUHAKEMELERİ KANUNUNDAKİ İMZA AÇISINDAN YERİ**" başlıklı çalışmayı bilgilerinize sunarız.

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitümüzün çalışmalarını **https://itlaw.bilgi.edu.tr** adresinden takip edebilirsiniz.

BİYOMETRİK İMZA VE TÜRK BORÇLAR KANUNU'NDAKİ YAZILI ŞEKİL ŞARTI İLE HUKUK MUHAKEMELERİ KANUNUNDAKİ İMZA AÇISINDAN YERİ

Leyla Keser Berber*

* İstanbul Bilgi Üniversitesi Hukuk Fakültesi Bilişim ve Teknoloji Hukuku Ana Bilim Dalı Öğretim Üyesi

I. Giriş

Günümüzde elektronik ortamda yapılan tüm işlemler tek bir klik ile gerçekleşmektedir. Elektronik ticaret sitelerinden alışveriş yapmak için, mesafeli satış sözleşmesini kliklemek, kullandığımız cep telefonu veya sosyal medya uygulamasının yenilediği sözleşmeleri tek tuşla kabul etmek, istediğimiz bir mobil uygulamayı ilgili platformlardan tek tuşla indirmek mümkündür. Tüm bu işlemlere ilişkin olarak taraflar arasında söz konusu olabilecek uyuşmazlıklar ise imza ile değil "log"larla ispatlanmaktadır. İmza şartı arayan işlemlerin çoğu açısından ise; güvenli elektronik imza yerine daha çok docusign[1] veya Adobe Signature[2] gibi elektronik imzalar kullanılmaktadır. Avrupa Birliği'nin 2014 tarihli İç Pazarda Elektronik İşlemler için Kimlik Tespiti ve Güven Hizmetlerine İlişkin Regülasyonu ((eIDAS)[3] kapsamında Gelişmiş Elektronik İmza başlığı altında değerlendirebileceğimiz biyometrik imza, 2000'li yılların başından beri kullanılan bir imzalama yöntemidir.

Bu çalışmada tablet, cep telefonu veya bilgisayar gibi cihazlara"elle atılan" biyometrik imzanın, Türk Borçlar Kanunu'ndaki "*elle atılma*" ve "*yazılı şekil*" şartını ve Hukuk Muhakemeleri Kanunu'ndaki "*imza*" şartını nasıl ve hangi koşul ve kriterlerle yerine getirebildiği analiz edilmiştir.

Yine bu çalışmada Türkiye'de biyometrik imza dışında halihazırda "yazılı şekil" ve "ispat hukuku" anlamında yürürlükte olan teknolojilerin neler olduğunu açıklamaktadır. Çalışmada öncelikle terminolojik olarak biyometrik imza ele alındıktan sonra, 6698 Sayılı Kişisel Verilerin Korunması Kanunu anlamında özel nitelikli bir kişisel veri niteliğinde olduğu tespit edilerek, bu Kanun uyarınca tabi olduğu hukuksal durum açıklanmıştır. Biyometrik imzanın o imzayı atan kişiye ait olup olmadığının kriminal polis laboratuarı veya adli tıp kurumu tarafından incelenmesinde esas alınacak ISO/IEC 19794 standardına değinildikten sonra, biyometrik imza ve ıslak imza arasındaki ortak ve farklı yönler doğuracağı sonuçlar ile birlikte irdelenmiştir. Biyometrik imzanın Türk Borçlar Kanunu'nda öngörülen yazılı şeklin unsurlarından imza şartını nasıl karşıladığı tartışıldıktan sonra, Hukuk Muhakemeleri Kanunu'nda öngörülen bir belgedeki imzanın inkar edilmesi halinde söz konusu olacak süreçler açısından ne anlama geldiğine de yer verilmiştir. Son olarak; bir elektronik veri olarak biyometrik imzanın, ıslak imzaya nazaran daha güçlü bir delil olmasını sağlamak amacıyla kullanılabilecek olan diğer teknolojiler ve çözümlerden bahsedilmiştir.

[1] https://www.docusign.com
[2] https://helpx.adobe.com/acrobat/using/signing-pdfs.html
[3] https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014

II. Genel Değerlendirme

Biyometrik İmza'yı irdelemeye başlamadan önce; el yazısı ile atılan (ıslak) imza dışında, Türk Hukuk'unda yazılı şekil şartını karşılayan teknolojileri değerlendirmek gerekir. Bu teknolojiler ve hukuki sonuçlarını aşağıdaki gibi özetlemek mümkündür:

- Güvenli Elektronik İmza: 5070 Sayılı, 2004 tarihli Elektronik İmza Kanunu (EİK) ile hayatımıza giren güvenli elektronik imza, EİK'nun atfına istinaden; Türk Borçlar Kanunu md. 14 ve 15 uyarınca yazılı şeklin unsurlarından olan el yazısı ile "imza" gibi imza atanı bağlayan ve aynı hukuki sonuçları doğuran bir etkiye sahiptir. Aynı hüküm EİK md. 5/f.1'de de tekrarlanmaktadır. EİK tarafından yapılan ikinci atıf ise Hukuk Muhakemeleri Kanununa (HMK) ilişkin olup, güvenli elektronik imza ile oluşturulan veriler "senet" hükmünde kabul edilmektedir (HMK md. 205/f.1 ve 2). EİK'nun 5. Maddesinin 2. Fıkrasının ilk versiyonunda mevcut olan ve finans dünyası için güvenli elektronik imza kullanımını daraltan "teminat sözleşmeleri" ibaresi de, 15.7.2016 tarihli 6728 sayılı Kanunun 45. Maddesiyle "teminat mektupları dışındaki banka teminat sözleşmeleri" şeklinde değiştirilerek, finans dünyasında güvenli elektronik imzanın uygulama alanı genişletilmeye çalışılmıştır.

- Server Signing: Güvenli elektronik imzanın, kullanıcıya ait bir token (konvansiyonel elektronik imza) veya cep telefonunun SIM'i tarafından atılması uygulaması (mobil imza) yerine; server tarafından atılabilmesi olarak özetleyebileceğimiz bu teknolojinin dayanağını, Avrupa Birliği'nin 910/2014 sayılı "*Elektronik İşlemler İçin Elektronik Kimlik ve Güven Hizmetleri Regülasyonu (eIDAS)" ve "TSE CEN/TS 419241*" numaralı standart oluşturmaktadır. Sistem kısaca halihazırda flash memory'lere yüklenerek imza sahibinin kullanımına sunulan konvansiyonel elektronik imzadan veya cep telefonunun SIM kartına yüklenerek kullanılan mobil imzadan farklı olarak; elektronik imzanın açık ve gizli anahtar çiftinin oluşturulduğu server'da kalması ve kullanıcının imzalama istemi server tarafından alındığında, imza sahibinin en az iki faktörlü kimlik doğrulama yöntemleri ile doğrulaması yapıldıktan sonra, elektronik imzanın imza atılmak istenen dokümana veya platforma bizzat server tarafından atılması işlemidir. Elektronik imza kullanıcılarını flash memory veya mobil imzada olduğu gibi SIM kart gibi bir donanıma bağımlı olmaktan kurtaran ve elektronik imza kullanımını son derece hızlı bir şekilde yaygınlaştıracak olan bu teknolojinin Ülkemizde kullanımı için Bilgi Teknolojileri ve İletişim Kurumu tarafından EİK'nun değiştirilmesi gerekmektedir.

III. Biyometrik İmza

A. Terminoloji ve Kişisel Verilerin Korunması Kanunu Açısından Değerlendirme

İlgili kişinin el yazısı ile tablete, cep telefonuna veya bilgisayara atılan biyometrik imza, tıpkı normal bir kalem kullanılarak kağıda atılan ıslak imzada olduğu gibi, bir biyometrik veridir. Bu nedenle öncelikle hukuk sistemimizde bu veriye atfedilen değeri ve bu verinin hukuksal açıdan niteliğini incelemek gerekir. 7 Nisan 2016 tarihinde yürürlüğe giren 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) md. 6/f.1 bir gerçek kişiye ait biyometrik veriyi "özel nitelikli kişisel veri" olarak kabul etmektedir.

KVKK'nın tanımlar bölümünde biyometrik veri tanımlanmamaktadır. Ancak Avrupa Birliği'nin Genel Veri Koruması Tüzüğü (General Data Protection Regulation- GDPR)[4] biyometrik veri tanımını ihtiva etmektedir. Bu kapsamda md. 4/14 biyometrik veriyi şöyle tanımlamaktadır: "Biyometrik veri; yüz görüntüsü veya daktiloskopik veri gibi benzersiz tanıtıcılarla bir bireyin fiziksel, psikolojik veya davranışsal özelliklerine ilişkin olan tüm verileri ifade etmektedir".

95/46 Sayılı Veri Koruması Direktifinde olmayan, ancak GDPR'da ilk defa düzenlenen, biyometrik veriyi de ilgilendiren bir diğer konu ise; Mahremiyet Etki Değerlemesidir (Privacy Impact Assessment). GDPR md. 35'e göre; veri işleme operasyonu, verinin doğası gereği ilgili kişinin hak ve özgürlükleri açısından spesifik riskler ortaya çıkarıyorsa, veri sorumlusu veya veri sorumlusu adına hareket eden veri işleyenin, kişisel verinin korunması açısından öngörülen veri işleme operasyonu açsından bir etki değerlemesi yapması gerekmektedir (f.1). Bu madde kapsamında özellikle "spesifik bir risk ortaya çıkaran işleme operasyonları" arasında etki değerlemesi yapılması öngörülen bir veri kategorisi olarak da; çocuklar, genetik veriler veya biyometrik verilere ilişkin büyük ölçekli dosyalama sistemlerinde yer alan kişisel veriler girmektedir.

Özel nitelikli kişisel verilerden olan biyometrik verinin işlenebilmesini[5] hukuka uygun kılan sebeplerden biri ilgili kişinin "*açık rızası*"dır (KVKK md. 6/f.2).KVKK md. 6/f.3 ise; açık rıza dışında biyometrik verinin işlenebileceği diğer bir hukuka uygunluk sebebi olarak, "kanunlarda öngörülen haller"e atıf yapmaktadır. Kanunların özel nitelikli kişisel verilerin işlenmesini öngördüğü durumlarda bu veriler, ilgili kişinin açık rızası olmadan da işlenebilmektedir. Örneğin;

[4] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
[5] KVKK md. 3/f.1, e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, ifade eder.

Türk Borçlar Kanunu (TBK) yazılı şekilde yapılması öngörülen sözleşmelerde, imzanın borç altına girenlerin "el yazısı ile" atılmasını zorunlu kılmaktadır". Islak imza da, biyometrik imza da el yazısı ile atıldığı için KVKK anlamında bir biyometrik veridir ve aşağıdaki açıklamalarımız çerçevesinde TBK'da öngörülen yazılı şeklin unsurların olan el yazısı ile atılma zorunluluğunu yerine getirdiği için, KVKK md. 6/f.3 uyarınca ilgili kişinin açık rızasına gerek olmadan kişisel veri işlenebilecek bir hukuka uygunluk sebebi oluşturmaktadır.

KVKK özel nitelikli kişisel verinin işlenebilmesi için, yukarıda belirttiğimiz hukuka uygunluk sebeplerinin dışında ayrıca, Kişisel Verileri Koruma Kurulu tarafından belirlenecek yeterli önlemlerin alınmasını da şart koşmaktadır (md. 6/f.4). Bu önlemler arasında şu hususlara dikkat çekmek gerekir:

- **Hareketsiz veriler (Data at rest):** Özel nitelikli verinin bir sunucuda saklanması durumunda aşağıdaki güvenlik önlemleri alınır:
    - **Erişim hakları:** Kişisel verinin sadece ilgili kişisel veriye tanımlı iş için ihtiyacı olan kişiler tarafından erişebilmesi, diğer bilgisayar kullanıcılarının erişmesinin engellenmesi için, gerekli erişim hakları planlanır, gerçekleştirilir ve veri sorumlusu tarafından önemli değişikliklerden sonra, ve her durumda en az yılda bir kez kontrol edilir.
    - **Şifreleme:** Verinin sadece durduğu sunucuda değil, alınan yedeklerin de güvenli olması için sabit olarak depolandığı yerde kriptografik yöntemlerle şifrelenmesi gereklidir. Söz konusu kriptografik yöntemler simetrik algoritmalar söz konusu olduğunda en az 256 bit (örn: AES), asimetrik algoritmalar söz konusu olduğunda en az 2048 bit (örn: RSA) şifrelemesi ile güvenli hale getirilir. Şifreleme yapıldığı zaman, ilgili şifrelere ait anahtarların, ISO/IEC27001 standardında belirtildiği gibi anahtar yönetimi içinde ele alınması gereklidir.
    - **Loglama:** Özel nitelikli kişisel verinin durduğu ortamda gerçekleşecek işlem hareketlerinin zaman damgası ile kayıt altına alınması.
- **Aktarılan veriler (Data at transit):** Özel nitelikli verinin farklı bilgisayar sistemleri arasında aktarılması durumunda aşağıdaki güvenlik önlemleri alınır:
    - **Şifreleme:** Verinin tüm yolculuğu boyunca, kriptografik yöntemlerle şifrelenmesi gereklidir. Söz konusu kriptografik yöntemler simetrik algoritmalar söz konusu olduğunda en az 256 bit (örn: AES), asimetrik algoritmalar söz konusu olduğunda en az 2048 bit (örn: RSA) şifrelemesi ile güvenli hale getirilir. Gerçekleştirilen veri aktarımı, iki ayrı kurum arasında, bir seferlik ise, veri ile anahtarlar ayrı yöntemler ile (örn: veri Internet üzerinden, anahtar SMS ile) karşı tarafa gönderilir. Düzenli veri aktarımı söz

konusu olduğu zaman, ilgili şifrelere ait anahtarların, ISO/IEC27001 standardında belirtildiği gibi anahtar yönetimi içinde ele alınması gereklidir.

- **Loglama:** Biyometrik verinin durduğu ortamda gerçekleşecek işlem hareketlerinin zaman damgası ile kayıt altına alınması.

B. Teknik Değerlendirme

Biyometrik imzanın teknolojik nitelikleri ve bu imzanın imza atan kişi tarafından atılıp atılmadığının tespitine yarayacak teknik kriterler ve parametreler, "*ISO/IEC 19794-7:2014 Biometric data interchange formats — Part 7: Signature/sign time series*" ve "*ISO/IEC 19794-11:2013 Information technology -- Biometric data interchange formats -- Part 11: Signature/sign processed dynamic data*" standardında düzenlenmiştir.

Belirtmek gerekir ki; ISO/IEC 19794:2014 standardı biyometrik imzanın üzerine atılacağı tabletin, cep telefonunun veya bilgisayarın teknik özelliklerinden daha çok; biyometrik imzanın kimin tarafından atıldığını tespit etmek amacıyla inceleme yapacak olan kriminal polis laboratuarı veya adli tıp kurumu gibi yerlerin, bu incelemeyi nasıl yapacaklarını standarda bağlamaktadır. Kriminal polis laboratuarı veya adli tıp kurumları gibi el yazısı ile kağıda kalem kullanılarak atılan imzanın, imza atan kişiye ait olup olmadığını teknik olarak inceleyen yerler açısından ISO/IEC 19794 standardının mevcudiyeti; artık bu kurumların biyometrik imzayı da teknik olarak nasıl inceleyeceklerinin açığa kavuşmuş olduğu anlamına gelmektedir. ISO/IEC 19794-11'in 2013 tarihinde yayımlanmış olduğunu dikkate alacak olursak, aslında bu tarihten itibaren biyometrik imzanın teknik olarak incelenmesinin mümkün olduğu görülecektir.

Bir konuda standart yayımlanmış olması, o konuda bilişim dünyasında ortak bir terminoloji, yöntem, teknik ve güvenlik kriterleri ile süreçler belirlendiği anlamına gelmektedir. Bilişim teknolojisinin ortak dili standartlardır. Standartlar düzenledikleri konuya ilişkin olarak, bu standardı benimseyen ülkelerde teknik olarak harmonizasyon yaratmaktadır. Standartlar hukuk dünyası açısından da önem taşımaktadır. Zira bir konuda standardın mevcudiyeti, ilgili kamu kurum ve kuruluşunun veya düzenleyici otoritenin çok rahat bir şekilde kanun ve/veya ikincil mevzuat çıkarmasına yardımcı olmaktadır. ISO/IEC 19794 standardı da biyometrik imza konusunda, 2013 tarihinden önce biyometrik imzanın incelenmesinde kendi yaklaşım ve tekniklerini kullanarak incelemeyi yapan kriminal polis laboratuarı ve adli tıp kurumuna artık daha standardize bir yol göstermektedir.

ISO/IEC 19794-7:2014 dijital tablet veya gelişmiş kalem sistemleri kullanılarak atılan, çok boyutlu zaman serisi formunda tespit edilmiş davranışsal imza/işaret verisi için veri değişim formatlarının neler olduğunu belirlemektedir.

Veri değişim formatları, el yazısı ile atılan işaret veya imzaların da dahil olduğu oldukça geniş bir kapsamdaki uygulama alanlarında kullanılabilecek ve uygulanacak şekilde jeneriktir.

ISO/IEC 19794-7:2014 biyometrik imzanın incelenmesi işlemi sonucunda;

1. Ne tür verinin elde edilebileceğine ilişkin bir açıklamayı,
2. Veri içeren üç farklı formatı:
    a. genel kullanım için tam format
    b. tam formatın ihtiva ettiği aynı miktardaki, veriyi sıkıştırılmış formda tutmaya elverişli sıkıştırılmış format, ve
    c. tam formata göre daha az bilgi taşıyan, sıkıştırma/genişletme gerektirmeyen akıllı kartlar veya diğer token'larla kullanım için kompakt format
3. Veri elde edilirken veri kayıt içerikleri ve iyi uygulama örnekleri

ihtiva etmektedir.

Elektronik cihazlara atılan ve yukarıdaki formatlarda elde edilen, kaydedilen ve transfer edilen biyometrik verinin; güvenilirliğini, bütünlüğünü ve gizliliğini korumak için aşağıdaki tekniklerin kullanılması gerekmektedir:

a. Şifreleme yöntemleri,
b. Zaman damgası,
c. Loglama,
d. Erişim yetki ve kısıtlamaları (ID management)

Biyometrik karşılaştırma için ise ISO/IEC 19794-11:2013 standardı; tablet, dijital kalem veya gelişmiş kalem sistemleri kullanılarak elde edilen, bir zaman serisinden çıkartılan imza/işaret şeklinde işlenen davranışsal veri için, veri değişim formatını belirlemektedir. Burada da veri değişim formatı jenerik olup, ISO/IEC 19794-11:2013'te adreslenen uygulama spesifik isterler ve özellikler mevcut değildir.

C. Tablet, bilgisayar veya cep telefonu gibi ortamlara elle atılan Biyometrik İmza ve Islak İmzanın Karşılaştırılması

Biyometrik imza ve ıslak imzanın en büyük ortak özellikleri "ilgili kişinin el yazısı ile" atılmalardır. Her iki imza türü arasındaki en önemli fark ise; ıslak imza mürekkepli veya mürekkepsiz kalem

kullanılarak kağıt üzerine "elle" atılırken, biyometrik imza ise tablet, bilgisayar veya cep telefonu üzerine yine "elle" atılmaktadır. Islak imza veya biyometrik imzayı atan kişi, imzasını inkar ettiğinde; imza incelemesi için kriminal polis labotaruarı veya adli tıp kurumu devreye girecektir.

Islak imzanın kriminal polis laboratuarları veya adli tıp kurumu tarafından incelenmesinde kullanılan teknikler, "mürekkep yaşı" yani kağıt belgenin "ne zaman imzalanmış" olduğunun tespiti ile birlikte, söz konusu imzanın ilgili kişiye ait olup olmadığını belirlemektedir. Biyometrik imzada ise, yukarıda belirttiğimiz ISO/IEC 19794-7 ve 11 standardı çerçevesinde yapılacak bir incelemede sadece "mürekkep yaşı" tespit edilemeyecek, ancak o belgenin ne zaman imzalandığı sorusunun cevabı aşağıda değineceğimiz üzere, mürekkep yaşı üzerinden belgenin imzalandığı tarihi yaklaşık olarak tespit etmeye nazaran, daha güçlü bir teknoloji olan "zaman damgası" teknolojisi ile verilecektir.

İmza inkarı bir yargılama sırasında söz konusu olduğunda, Hukuk Muhakemeleri Kanunu md. 211/f.1, a bendi hakime nasıl inceleme yapılması gerektiğini açıklamaktadır. Aynı maddenin "b" bendi ise; "a" bendine göre yaptığı inceleme sonucunda bir neticeye varamamışsa hakimin bilirkişiye yani kriminal polis laboratuarı veya adli tıp kurumuna başvuracağını düzenlemektedir.

IV. Biyometrik İmza ve Yazılı Şekil Şartı

Çalışmamızın bu bölümünde, Sözleşmelerin şekline ilişkin olarak Türk Borçlar Kanununda (TBK) yer alan hükümler ışığında biyometrik imzanın "*yazılı şekil şartını*" yerine getirip getirmediği değerlendirilecektir.

Yazılı şeklin unsurlarını düzenleyen TBK md. 14/f.1; yazılı şekilde yapılması öngörülen sözleşmelerde borç altına girenlerin imzalarının bulunmasının zorunlu olduğunu; 2. fıkrasında ise güvenli elektronik imzanın, yazılı şeklin unsurlarından olan "imza" unsurunu karşılayacağını ifade etmektedir. TBK md. 15/f.1 ise; imzanın "el yazısıyla" atılmasının zorunlu olduğunu, güvenli elektronik imzanın da, el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğuracağını hükme bağlamaktadır.

Güvenli elektronik imza; gerek TBK gerek HMK'da yer alan ve maddi hukuk ve ispat hukuku açısından son derece bağlayıcı ve güçlü hukuki sonuçlar ihtiva etmesine rağmen; uygulamada 2004 yılından günümüze kadar yaygınlaşma anlamında istenilen başarıyı elde edememiştir. Bunun nedeni ise; bireyleri konvansiyonel elektronik imzada bir donanıma yani token'a, mobil imzada ise bir SIM'e bağlı kılmasıdır. Güvenli elektronik imzanın sadece Server Signing şeklinde atılması durumunda, kullanıcının imza atmak için herhangi bir donanıma ihtiyacı kalmayacak olup, sadece "imzala" butonu tıklanarak imza atılması mümkün olabilecektir. Server Signing için de Bilgi

Teknolojileri ve İletişim Kurumu tarafından EİK'da değişiklik yapılması şart olduğu için, bu teknoloji ve ona hayat veren standart henüz iç hukukumuzda uygulama alanı bulamamıştır.

TBK yazılı şeklin unsurlarından olan imzanın, el yazısıyla atılmasını öngörmektedir. Ancak ilgili maddelerde el yazısıyla imzanın hangi ortama ve hangi medya kullanılarak atılacağına dair herhangi bir tespit mevcut değildir. Böyle bir tespitin yapılmamış olması da, aslında kanun koyucunun bu alandaki teknolojik gelişmeleri engellemek istemediğini, teknoloji nötr yaklaşımını benimsediğini göstermektedir. Geçmişte sadece kağıt ortam ve bu kağıda, sadece kalem kullanılarak imza atmak mümkün iken; bugün artık elektronik ortamda, herhangi bir elektronik medyada yer alan bir belgeye biyometrik imza şeklinde el yazısıyla imza atmak mümkündür. Biyometrik imzanın, yukarıda değindiğimiz ISO/IEC 19794-7/11 standardı uyarınca normal kalem kullanılarak atılan el yazısıyla imzadan tek farkı sadece imza atmakta kullanılan teknolojilerin "dijital" olması ve imzanın atıldığı ortamın kağıt değil de "elektronik" olmasıdır. İster normal kalem ister elektronik ortama atılsın, imza ilgili kişinin "el yazısı ile" atılmaktadır. TBK'nun da yazılı şekil için aradığı tek kriter budur! Dolayısıyla TBK'daki yazılı şekil şartını yerine getirmek bakımından el yazısı ile atılan ıslak imza ile, yine el yazısı ile atılan biyometrik imza arasında herhangi bir bir fark mevcut değildir.

Islak imza ve biyometrik imza "*biyometrik*"tir. Zira tanım olarak biyometri, bireyin ölçülebilir biyolojik izlerini ifade etmektedir. Kriminal polis laboratuarları veya adli tıp kurumları kağıda kalem ile el ile atılan imzanın da, elektronik ortama yine el ile atılan imzanın da analizini ilgili teknolojileri ve standartları kullanarak gerçekleştirebilmekte ve ister kağıt belgedeki ister elektronik belgedeki el yazısı ile atılan imzanın kime ait olduğunu tespit edebilmektedir. Diğer bir ifade ile; bir kişinin el yazısı ile atıldığı ölçüde; kağıda veya elektronik medya üzerine imza atılması arasında bir fark mevcut değildir. Dolayısıyla imzanın atıldığı materyalin veya ortamın ıslak imza/biyometrik imza ayrımında herhangi bir önemi yoktur. Bu husus ise; yazılı şekle ilişkin olarak; TBK md. 15/f.1'in aradığı "imzanın borç altına girenin el yazısıyla atılmasının zorunlu olduğu'"na ilişkin koşulu biyometrik imzanın da karşıladığını göstermektedir. Hatta biyometrik imza; elektronik bir veri olması dolayısıyla bizatihi ihtiva ettiği teknik nitelikler (yardımcı veri-metadata) dikkate alındığında, ıslak imzadan daha güçlü bir delil değerine sahiptir. Biyometrik imza ayrıca aşağıda değineceğimiz teknolojiler ile de birleştiğinde de, kalem kullanılarak el yazısı ile kağıda atılan ıslak imzadan daha güçlü bir hukuki delil vasfını kazanmaktadır.

V. Biyometrik İmza ve Hukuk Muhakemeleri Kanunu

Hukuk Muhakemeleri Kanunu (HMK) 199. Maddesinde "belge" kavramını düzenlemektedir. Kanunda yer alan tamına göre; "Uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki

veriler ve bunlara benzer bilgi taşıyıcıları bu Kanuna göre belgedir" (HMK md. 199/f.1). Görüldüğü üzere HMK elektronik ortamdaki verileri "belge" kapsamında değerlendirmektedir. Adi senetlere ilişkin 208. Madde ise; adi senetlerde yer alan yazı veya imzanın inkarına ilişkindir. Md. 208/f.1 incelendiğinde; taraflardan birinin, kendisi tarafından düzenlendiği iddia edilen bir "*belgedeki*" yazı veya imzasını inkar etmesi durumunda nasıl hareket edileceği anlatılmaktadır. HMK md. 208'de yer alan "*belge*" kavramı, md. 199/f.1 ile birlikte değerlendirilmelidir. Buna göre; adi senet kağıt formatta olabileceği gibi, elektronik ortamda da düzenlenebilir. HMK'da adi senedin kağıtta olmasına ilişkin herhangi bir zorunluluk mevcut olmadığı gibi, md. 208/f.1 hükmü ile de belgenin elektronik ortamda da olabileceği teyit edilmiştir. Yine HMK'da yer alan hiçbir hüküm, bir belgede yer alan imzanın "*ıslak imza*" olması gerektiğini öngörmemektedir. HMK sadece imza veya güvenli elektronik imzadan bahsetmektedir. Md. 208/f.1 kişinin bir belgede yer alan imzası veya yazısından bahsetmekte, ancak bu imzanın ıslak imza mı biyometrik imza mı olması gerektiği noktasında bir tespit yapmamaktadır. Aynen TBK gibi HMK'da gelişen teknolojiler karşısında kanunun güncelliğini koruması amacıyla "teknoloji nötr" davranmaktadır. Dolayısıyla HMK uygulamasında bir adi senet elektronik ortamda düzenlenebileceği gibi, bu adi senedin imzası da biyometrik imza şeklinde olabilecektir.

VI. Biyometrik İmzanın, Elektronik Bir Veri Olarak Değerlendirilmesi

Biyometrik imza bir elektronik veri olarak ihtiva ettiği yardımcı veriler (metadata) dışında; aşağıda değindiğimiz diğer teknolojiler ve veriler ile birleştiğinde, kağıt üzerindeki ıslak imzanın kesinlikle sahip olmayacağı özellikler taşıyacaktır. Bu da mahkemeye sunulan sadece kağıt üzerinde yer alan ıslak imzaya oranla, biyometrik imzanın daha güçlü bir delil olması sonucunu doğuracaktır:

Biyometrik İmza ve Zaman Damgası: Kriminal polis laboratuarı veya adli tıp kurumu tarafından biyometrik imza incelemesinde, "belgenin yaşı" veya "belgenin ne zaman imzalandığı" hususunun tespit edilebilmesini sağlamak için; ilgili kişi tablet, cep telefonu veya bilgisayara imza atarken bu biyometrik veriye "*zaman damgası*"nın ilave edilmesi gerekecektir. Bu sayede elektronik belgenin "*ne zaman*" imzalandığı tartışmasız bir kesinlikle kanıtlanabilecektir. Zaman damgasının EİK ve ikincil mevzuatında öngörülen hukuki sonuçları doğurabilmesi ve bağlayıcı olabilmesi için, EİK md. 3/h bendinde tanımlanan ve mutlaka ve sadece BTK tarafından yetkilendirilen Elektronik Sertifika Hizmet Sağlayıcılardan[6] temin edilebilecek olan zaman damgasının biyometrik imza verisine eklenmesi gerekli olacaktır. Biyometrik imzaya eklenen zaman damgası ile öncelikle; biyometrik imzanın ne zaman atıldığı, elektronik ortamdaki belgenin ne zaman imzalandığı tespit

[6] https://www.btk.gov.tr/tr-TR/Sayfalar/e-imza-Elektronik-Sertifika-Hizmet-Saglayicilari.

edilmekte ve bu teknoloji sayesinde kağıt belgenin ne zaman imzalandığının tespitinde kullanılan mürekkep yaşını hesaplama uygulamasından daha kesin bir durum yaratılmış olmaktadır. Yine zaman damgası teknolojisi, biyometrik imzaya eklendiğinde; artık imzayı atan kişinin imzayı o tarihte atmadığını iddia etmesi, diğer bir ifadeyle elektronik ortamdaki verinin imzalandığı tarihi inkar etmesi olanaksız hale gelmektedir.

Log Tutulması: İlgili kişi biyometrik imza atarken, elektronik ortamda gerçekleştirilen her işlemde olduğu gibi log tutulması önem taşıyacaktır. Bu log, biyometrik imza atılma işleminin gerçekleştiğini gösteren bir kayıt olarak muhafaza edilmeli ve biyometrik imzanın atılıp atılmadığına ilişkin herhangi bir uyuşmazlıkta delil olarak kullanılmalıdır. Özellikle imzalama işleminin ilgili kişiye ait tablet, cep telefonu veya bilgisayardan yapılması durumunda, ilgili kurumun/kuruluşun yer sağlayıcı ve içerik sağlayıcı sıfatıyla, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun md. 2/f.1, j bendi uyarınca trafik bilgisini yani; taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini de loglaması ve bu logları da mutlaka "zaman damgası ile bilişim sistemlerinde muhafaza etmesi gerekli olacaktır". Biyometrik imza atma işleminin ilgili kurum/kuruluşun kendisine ait tablet, cep telefonu veya bilgisayarda yapılması durumunda da yine aynı şekilde biyometrik imza verisine zaman damgası atılması ve trafik verilerinin az önce belirttiğimiz şekilde yine zaman damgası atılarak loglanması gerekmektedir.

Şifreleme Teknolojileri Kullanımı: Biyometrik imzanın, bir elektronik veri olarak gizliliği, güvenliği ve bütünlüğünü sağlamak için zaman damgası ve log dışında, bu veri muhafaza edilirken uygun şifreleme teknolojilerinin kullanılması da tavsiye edilmektedir. Bu sayede biyometrik imza, bilgi güvenliği tedbirlerine uygun şekilde bilişim sistemlerinde saklanabilecektir.

Erişim Yetkileri, Kısıtlamaları (ID Management) Uygulanması ve Erişim Kayıtlarının Tutulması: Biyometrik imzanın zaman damgası atılması ve şifrelenmesi dışında, bilişim sistemlerinde muhafaza edildiği ortamlara erişime yetkili olacak kişilerin ve bu kişilerin erişim yetkilerinin kapsamının belirlenmesi gereklidir (erişim yetki kontrol matrisi). Belirlenen bu kapsamda sistemde gerçekleştirilen her erişimin mutlaka zaman damgalı loglarının tutulması önem taşımaktadır.

VII. Sonuç

Yukarıda yer alan açıklama ve değerlendirmelerimize istinaden aşağıdaki noktaların altını çizmek mümkündür:

1. Yazılı şeklin unsurlarından olan imzanın, hangi ortama ve hangi teknoloji ile atılacağı konusunda bir tercih yapmayan, bilakis bu konuda teknoloji nötr bir yaklaşım belirleyen Türk Borçlar Kanunu'na göre; imzanın yazılı şekil şartının yerine getirilmesi bakımından sadece "elle atılması" önem taşımaktadır. Biyometrik imza da elle atılmaktadır ve ıslak imzadan bu noktada hiçbir farkı mevcut değildir.

2. Elle atılan ıslak imza gibi, biyometrik imza da imza inkarı halinde kriminal polis laboratuarı veya adli tıp kurumu tarafından ISO/IEC 19794 standardında öngörülen şekilde incelenmektedir.

3. Biyometrik imza, ıslak imzadan Hukuk Muhakemeleri Kanunu anlamında delil gücü bakımından da daha üstündür. Özü itibariyle bir elektronik veri niteliğindeki biyometrik imzanın;

- imzanın atıldığı zamanın tartışmasız şekilde ispatına yarayan zaman damgası teknolojisi ile,
- güvenlik, bütünlük ve kullanılabilirlik açısından şifreleme yöntemleri ile,
- imzalama işleminin kanıtlanması bakımından loglama ile,
- bilişim sistemlerinde bu elektronik veriye erişimin kontrolünü sağlayan ID Management teknolojileri ile

birlikte muhafaza edilmesi ve bu sayede halihazırda sahip olduğu delil gücünün daha da güçlendirilmesi mümkündür.