BİYOMETRİK İMZALARIN TÜRK ADLİ BİLİMLER İNCELEMELERİNE KAZANDIRILMASI ÜZERİNE ARAŞTIRMA

RESEARCH ON BRINGING BIOMETRIC SIGNATURES INTO TURKISH FORENSIC SCIENCE STUDIES

ÖZAY DÖRTTEPE

DOÇ. DR. HARUN ARTUNER

Tez Danışmanı

Hacettepe Üniversitesi

Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin

Adli Bilimler Anabilim Dalı için Öngördüğü

YÜKSEK LİSANS TEZİ olarak hazırlanmıştır.

2023

ÖZET

BİYOMETRİK İMZALARIN TÜRK ADLİ BİLİMLER İNCELEMELERİNE KAZANDIRILMASI ÜZERİNE ARAŞTIRMA

ÖZAY DÖRTTEPE

Yüksek Lisans, Adli Bilimler Ana Bilim Dalı

Tez Danışmanı: Doç. Dr. Harun ARTUNER

HAZİRAN 2023, 61 sayfa

Teknolojinin hızla insan hayatının her aşamasına girmeye başlaması ve devam etmesinin sonucu olarak, insanların kalem ile kâğıt üzerine attıkları imzalar artık dokunmatik ekran özelliğine sahip tabletler sayesinde elektronik ortamda atılmaya başlanmıştır. Bunun sonucu olarak elektronik ortamda imzalanmış belgeler adli davalara konu olmaktadır. Söz konusu imzaların aidiyetinin tespit edilmesi için adli makamlarca kriminal laboratuvarlara inceleme istekleri gönderilmektedir. Ancak hâlihazırda söz konusu imzaların tam adının ne olması gerektiği, nasıl ve kimler tarafından inceleneceği vb. konularda belirsizlikler/boşluklar bulunmaktadır.

Bu tez çalışması ile adli makamların inceleme isteklerine cevap verebilmek, Jandarma kriminal laboratuvarlarının incelemelerine temel teşkil edecek talimatı ve gereklilikleri belirlemek ve söz konusu imzalarda mevcut isim karmaşasına son vermek amaçlanmıştır.

Biyometri, yakın zamana kadar birçok kişi tarafından bilinmeyen teknik bir konuydu ve daha çok bilişimle ilgiliydi. 6698 Sayılı Kişisel Verileri Koruma Kanunu'nun 2016 yılında yürürlüğe girmesi ve biyometrik verilerin özel bir nitelik olarak sınıflandırılması sonucunda bu alanda çalışan sayısı artış göstermiştir. Biyometri ve biyometrik veri artık tüm insanları ilgilendiren bir konu hâline gelmiştir. Bununla birlikte sadece teknik değil, yasal etki alanı da oluşturmaya başlamıştır. Neyin biyometrik veri olarak

değerlendirilebileceği, neyin değerlendirilemeyeceği ya da bir verinin ne zaman biyometrik veriye dönüştürüleceği konusundaki tartışmaların devam ettiği bilinmektedir.

Bu çalışmanın birinci bölümünde imzanın tanımı yapılmıştır. İmzanın neden yaygın olarak kullanıldığı ortaya konulmuş ve dijital imza denilince ilk akla gelen elektronik imza ele alınmıştır. Elektronik imza seviyeleri tanımlanarak elektronik imza hakkında yapılan hukuki düzenlemeler araştırılmıştır. İkinci bölümde ise dijital ortamlara atılan imzalar ele alınmıştır. Gelişmiş elektronik imza kapsamına giren biyometrik imza üzerinde durulmuştur. Biyometrik imza teknolojisinin avantajları ve biyometrik imza inceleme tekniklerinin adli bilimler açısından değerlendirmesi yapılmıştır. Biyometrik imzanın oluşturulması, ıslak imzaya denkliği, veri bütünlüğü, oluşturma güvenliği, doğrulama güvenliği ve kullanım kolaylığı üzerinde durulmuştur. Çalışmanın üçüncü bölümünde ise biyometrik imzanın detaylı incelemesi yapılarak bu kapsamda biyometrik imzanın veri gereksinimleri ortaya konulmuştur. Sayısal veriler olarak; X ve Y koordinatı, X ve Y yönünde hızı, X ve Y yönünde ivmesi, imzanın uzunluğu, imzanın yüksekliği, ilk noktadan itibaren geçen süre, kalem basıncı, kalem ucunun durumu ve eğimi, kalem kaldırma, kalem dönüşleri tanımlanmıştır. Biyometrik imzanın görüntüleri ve meta verileri üzerinde durulmuş, buna paralel olarak biyometrik imza çözüm gereksinimleri ele alınmıştır. Çözüm gereksinimleri kapsamında örneklem/işlemci hızı, zaman yakalama, basınç/kuvvet, hava hareketleri, biyometrik bir imzanın elektronik bir belgeye entegrasyonu tanımları yapılmıştır. Devamında ise imzalama koşulları üzerinde durulmuştur. Çalışmanın dördüncü bölümünde asıl çalışma konusu olan dijital ortamlara atılan imzaların kriminal incelemesi nasıl olmalı sorusu üzerinde yoğunlaşılmıştır. Öncelikle ıslak imzaların incelemesi yapılırken analiz edilen genel ve karakteristik özelliklerden bahsedilmiştir. Genel özelliklerden biçim, boyut, oranlar, boşluklar, eğim, ivme, hız, akıcılık, basınç, el kaldırma hareketi yörüngesi ele alınarak karakteristik özelliklerden de bahsedildikten sonra değerlendirme ve yorumlama yapılmıştır. En son bölümde ise dijital ortamlara atılı imzaların hukuki değerlendirmesi yapılarak bu hususstaki tartışmalara açıklık getirilmiştir. Sonuç olarak adli makamlardan kriminal laboratuvarlara gönderilen biyometrik imzaların incelemesi nasıl olmalı üzerinde bir açıklama geliştirilmiştir. Bu kapsamda Jandarma kriminal laboratuvarının altyapı çalışmaları ve eğitim hazırlıkları nasıl olmalı sorusunun cevabı da ortaya konulmuştur.

Anahtar Kelimeler: El Yazısı İmza, Biyometrik İmza, Biyodinamik İmza, Dijital İmza, Dijital Kriptolanmış İmza, Elektronik İmza, Online İmza

ABSTRACT

RESEARCH ON BRINGING BIOMETRIC SIGNATURES INTO TURKISH FORENSIC SCIENCE STUDIES

ÖZAY DÖRTTEPE

Master of Science, Department of Forensic Science

Supervisor: Harun Artuner

June 2023, 61 pages

As a result of the rapid penetration of technology into every stage of human life, people's signatures on paper with a pen have now begun to be made electronically, thanks to tablets with touch screen feature. As a result, documents signed electronically are subject to judicial proceedings. In order to determine the authenticity of the said signatures, requests for examination are sent to the criminal laboratories by the judicial authorities. However, the full name of the said signatures should be, how and by whom they will be examined, etc. there are uncertainties/gaps in matters.

In this study, to be able to respond to the investigation requests of the judicial authorities; to determine the instructions and requirements that will form the basis of the investigations of the Gendarmerie Criminal Laboratories.

Biometrics was a technical subject unknown to many until recently and was more about computing. As the Personal Data Protection Law No. 6698 came into force in 2016 and biometric data was classified as a special quality, the number of employees in this field increased. Biometrics and biometric data have now become a topic that concerns all

people. However, it has started to create not only a technical but also a legal domain. It is known that the debates about what can be considered as biometric data and what cannot be evaluated or when to convert a data into biometric data continue.

In the first part of this study, the definition of signature was made. It was revealed why the signature is widely used and the first thing that comes to mind when digital signature is mentioned is the electronic signature. Electronic signature levels were defined and legal regulations regarding electronic signature were investigated. In the second part, signatures on digital media were discussed. The focus was on biometric signature, which is within the scope of advanced electronic signature. The advantages of biometric signature technology and biometric signature examination techniques were evaluated in terms of forensic sciences. The creation of biometric signature, its equivalence to wet signature, data integrity, creation security, verification security and ease of use were emphasized. In the third part of the study, a detailed examination of the biometric signature was made. In this context, the data requirements of the biometric signature were revealed. As numerical data; X and Y coordinate, velocity in X and Y direction, acceleration in X and Y direction, length of signature, height of signature, time elapsed from the first point, pen pressure, pen tip state and tilt, pen lift, pen rotations were defined. Focused on images and metadata of biometric signature. In parallel with this, biometric signature solution requirements were discussed. Within the scope of solution requirements, definitions of sample/processor speed, time capture, pressure/force, air movements, integration of a biometric signature into an electronic document were made. Subsequently, the conditions for signing were discussed. In the fourth part of the study, the main subject of the study, how the criminal investigation of signatures on digital media should be focused on. First of all, the general and characteristic features analyzed while examining wet signatures were mentioned. General features such as form, size, proportions, spacing, slope, acceleration, speed, fluency, pressure, hand raising trajectory were discussed. After mentioning the characteristic features, evaluation and interpretation were made. In the last part, the legal evaluation of the signatures on digital media was made and the discussions on this issue were clarified. As a result, it was focused on how the biometric signatures sent from judicial authorities to criminal laboratories should be examined. In this context, the answer to the question of how the infrastructure works and training preparations of the Gendarmerie Criminal Laboratory should be was revealed.

Keywords: Handwritten Signature, Biometric Signature, Biodynamic Signature, Digital Signature, Digital Encrypted Signature, Electronic Signature, Online Signature

TEŞEKKÜR

Yüksek lisans danışmanım olarak, bu alanda bana yeni ufuklar açan ve her daim katkı ve desteklerini sunan tez danışmanım Doç. Dr. Harun ARTUNER'e teşekkürlerimi sunarım.

Başta eşim olmak üzere tüm aileme sevgi ve saygılarımla…

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

SİMGELER VE KISALTMALAR

AB : Avrupa Birliği

AMD : Amendment (Değişiklik)

AIIM : Akıllı Bilgi Yönetimi Derneği

BDIR : Dijital Biyometrik Veri Kaydı

BTK : Bilgi Teknolojileri İletişim Kurumu

CD : Veri Saklama Deposu (700 MB kadar)

CSV / TSV : Comma Seperated Values / Tab Seperated Values

DVD : Veri Saklama Deposu (4,7 GB kadar)

EC : European Commission

eIDAS : Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü

ESHS : Elektronik Sertifika Hizmet Sağlayıcısı

ETSI : Avrupa Telekomünikasyon Standartları Enstitüsü

GSM : Global System for Mobile

HMK : Hukuk Muhakemeleri Kanunu

IEC : Uluslararası Elektoteknik Komisyonu

ISO : International Organization for Standardization

JKDB-DOK-TL : Jandarma Kriminal Daire Başkanlığı Doküman Şube İnceleme Talimatı

NES : Nitelikli Elektronik Sertifika

PDF : Portable Document Format

PIN : Personal Identification Number

PKI : Ortak Anahtar Altyapısı

TBK : Türk Borçlar Kanunu

TDK : Türk Dil Kurumu

UNCITRAL : United Nations Commission on International Trade Law

XML : Veri Saklama Formatı

1. GİRİŞ

Teknolojik alandaki gelişmeler ile birlikte dijitalleşen dünyanın etkisi yaşamın her alanında görülmektedir. Dijitalleşmenin firmalara maliyet ve iş gücü tasarrufu sağlaması bu çalışmaları hızlandırmaktadır. Son yıllarda neredeyse her alanda işlemler akıllı telefon, tablet ya da bilgisayarlar aracılığı ile yapılmaktadır. Kullanımı giderek artan, firmalara maliyet tasarrufu sağlayan gelişmelerden bir tanesi de dijital ortamlara atılı imzalardır. Dijital ortamlara atılı imzalar akıllı telefon, tablet vb. cihazların dokunmatik ekranlarına kalem ya da parmak ile geleneksel ıslak imza gibi el hareketleri ile atılan imzalardır.

İmza, yüzyıllardır belgeleri onaylama ve kimlik tanımlama için kullanılan en basit ve maliyetsiz yöntemlerden birisidir. İmza kullanılan belgelerde anlaşmazlıklar ortaya çıktığında ise imza aidiyetinin tespiti için adli incelemelere başvurulmuştur. Kullanımı artan dijital ortamlara atılan imzaların anlaşmazlıklara konu olması durumunda da adli imza incelemeleri gerekli olacaktır. Dijital ortamlara atılan imzaların bazılarında sadece imza görüntüsü bazılarında ise görüntüsü ile birlikte imza atılış sürecinde imzanın zamana bağlı hareket verileri depolanır. Bu imzaların zemin ve imza atma aracının farklı olması, imzanın görüntüsü ile birlikte dinamik verilerinin de kaydediliyor olmasının incelemeyi yapacak el yazısı ve doküman inceleme uzmanlarına bazı avantaj ve dezavantajları olacaktır. İmzanın aidiyetini belirleyebilmek için geleneksel inceleme metotlarının dışında yeni yöntemlerin eklenmesi gerekmektedir.

1.1. Amaç ve Kapsam

Bu çalışmada elektronik imza, elektronik imzanın hukuki gelişimi, dijital ortamlara atılı imzalar, imzaların hukuki geçerliliği ve inceleme yöntemleri araştırılmış, Jandarma kriminal laboratuvarlarının dijital ortamlara atılı imzaları inceleyebilmesi için gereken altyapı ve eğitim hazırlıklılarının neler olması gerektiği tespit edilmiştir.

1.2. Araştırma Soruları

Türkiye'de iletişim sektöründen bankalara kadar birçok iş kolu hangi imza çeşidinin kullanılması konusunda ayrıntılı bir şekilde düzenlenmiş kurallara bağlı değildir. Aslında yasalar gereği bu durumu düzenleme yetkisi ülkemizde *Bilgi Teknolojileri İletişim Kurumu*na verilmiştir. *Bilgi Teknolojileri ve İletişim Kurumu*nun dijital olarak

yakalanmış imzaların düzenlenmesi konusunda yetersiz kalması, belgelere olan güven seviyesinin kuruluşların kendileri tarafından belirlenmesine sebep olmuştur. Tüm bunların yanında, hem ıslak imzanın hem de güvenli elektronik imzanın belgenin türüne bakılmaksızın birlikte kullanıldığı görülmektedir. Günümüzde alternatif imza türleri de ortaya çıkmıştır. Bunlardan en önemlisi de dijital ortamlara atılan imzalardan olan biyometrik imzadır.

Biyometrik imzaların adli soruşturmalara veya davalara konu olması durumunda ıslak imzalarda olduğu gibi aidiyetine yönelik rapor talep edildiği açıkça ortaya çıkmıştır. Bu çalışmada günlük yaşamda sıklıkla kullanılmaya başlanan biyometrik imzanın aidiyetinin tespitinin nasıl olması gerektiği, adli olarak inceleme yapan jandarma kriminal laboratuvarlarının izleyeceği yöntemin ne olması gerektiği üzerinde durulmuştur ve bu noktada oluşan inceleme taleplerinin karşılanması amaç edinilmiştir.

2. ALANYAZIN ÖZETİ

2.1. İmza Nedir?

İmzanın yaşamımızda yeri çok önemlidir. İmza atarak ya bizim için kritik öneme sahip bir borç veya yükümlülük altına gireriz ya da borç veya yükümlülükten kurtuluruz. İrademizi ortaya koyar, düşüncelerimizi beyan ederiz ve düşüncelerin bize ait olduğunu başka şahıslara veya kurumlara ifade ederiz [1]. Bu özelliği ile de imza; "hukuki alanda büyük önem ve değer taşımasının yanı sıra kişilerin kimliğini belirleyici bir unsur" olarak da değerlendirilmektedir [2]. Mühür, parmak izi, kesici diş gibi araçlar tarih boyunca vasiyetnamenin kime ait olduğunu göstermek için yaygın olarak kullanılmış olsa da adli imza incelemesi araştırmalarındaki gelişmelerin el yazısı imzaların yaygınlaşmasına yol açtığı söylenebilir.

İmzanın sözlük anlamı "*Bir kimsenin herhangi bir belgeyi yazdığını veya onayladığını belirtmek için her zaman aynı biçimde kullandığı işaret*" şeklindedir. Islak imza ise "*Kişinin kâğıt üzerine kalemle attığı imza*" olarak tanımlanmaktadır [3]. İmza ile ıslak imza/el yazısı imza birbirinden farklıdır. İmza geniş anlamda kullanılır ve faks, elektronik posta yoluyla da atılan imzalar dâhil tüm hepsini kapsar. Islak imza ise kişinin elektronik iletişim araçları kullanmaksızın kendi eliyle attığı imzadır.

El yazısı/ıslak imza, bir kişinin yazılı bir belgedeki metni yazdığını veya onayladığını gösteren biyometrik bir işaret olarak tanımlanabilir ve hemen hemen her zaman aynı şekilde kullanılır. Diğer bir deyişle, el yazısı imza, yazının kalıcı olarak korunmasına uygun bir nesne (örneğin kâğıt, tahta, deri) üzerinde kalemle kişinin karakteristik özelliklerini yansıtan bir işarettir. İmzalamak için kullanılan kalemin mutlaka mürekkepli olması gerekmez, kurşun kalemle atılan imza da kabul edilebilir.

Kişinin özelliklerini yansıtan bir işaretin el yazısı imza sayılabilmesi için bu istek ile yapılmış olması yeterlidir ve mutlaka adı ve soyadını içermesi gerekmez. *"...6098 Sayılı TBK'nin 15. maddesine göre, imzanın, borç altına giren kimsenin el yazısı olması gerekir. El yazısı ile atılacak imzanın şeklî konusunda yasada hüküm bulunmamaktadır. Kişi, kendisine özgü belli karakterleri içeren sembolleri belirterek imza atabileceği gibi, ad ve soyadını bizzat el yazısı ile yazmak suretiyle de imza atabilir. Ancak bu durumda borçlu, ad ve soyadını yazarken imza atmayı amaç edinmelidir. Bu durumda mahkemece, şikâyetçinin imzasını ad ve soyadı ile atıp atmadığı hususunun imzasının bulunabileceği*

resmî kuruluşlardan sorularak tespiti gerekir. Şayet şikâyetçinin imzasını ad ve soyadını yazmak sureti ile attığı tespit edilirse senet altına yazılan '...' ibaresinin şikâyetçi borçlunun eli ürünü olup olmadığının tespiti ile yukarda yapılan açıklamalar doğrultusunda oluşacak sonuca göre karar verilmesi gerekirken eksik incelemeye dayalı hüküm tesisi isabetsizdir..." [4].

21 Haziran 1934 tarihli ve 2525 sayılı Soyadı Kanunu'nun ikinci fıkrası "*Söyleyişte, yazışta, imzada öz ad önde, soy adı sonda kullanılır*" şeklindedir [5]. Zira bu madde, imzada ad ve soyadın hangi sırayla kullanılacağını gösteren bir düzenleyici hüküm niteliğindedir. Kişinin imza atarken eliyle yansıttığı bir işareti göstermesi önemli olduğu için imzayı imza olarak yorumlarken kişinin daha önce aynı amaçla kullandığı işaretler (imzalar) önemlidir. Ancak bunların kendi içinde yorumlanması gerekmektedir. Taklit edilmesi çok kolay olan basit el işaretleri imza olarak kullanılmaz, örneğin tipik yazım özelliklerini yansıtmayan ad baş harfleri veya basit bir çizgi çizmek gibi. Böyle bir durumda, alıcının söz konusu işaretin imza olarak sınıflandırılamayacağının farkında olması önemlidir. Aksine, kişinin ayırt edici yazılı özelliklerini yansıtmayan basit işaretlerin imza olarak alınması hukuki belirlilik ilkesine aykırı olacaktır. Bu gibi durumlarda, bu tür basit işaretlerin kişinin kendi ellerinden kaynaklanıp kaynaklanmadığını belirlemek mümkün değildir.

Aslında imza denilince akla ilk gelen, bir imzanın tüm fonksiyonlarını yerine getirme özelliğine sahip, "ıslak imza" olarak da bilinen elle atılan imzadır. Bu bağlamda ıslak imza tüm imza atma araç ve yöntemleri için ölçüt niteliğindedir. Öyle ki, diğer tüm araç ve yöntemler, bir niyet beyanının bağlayıcı niteliğini ortaya çıkarmak için el yazısı imza kadar yaygın olarak kullanılabilir.

2.2. İmza Neden Yaygın Olarak Kullanılıyor?

Elle atılan imzanın, yönetim kolaylığının yanı sıra, uzun süredir bir niyet beyanının kimliğini ortaya çıkarmanın en çok kullanılan yolu olmasını kriminal inceleme alanındaki gelişmelere bağlamak yanlış olmayacaktır. Diğer bir neden ise, hukuki açıdan bakıldığında, elle atılan bir imzanın gerçek olup olmadığının ve aidiyetinin belirlenmesinde yüksek doğruluklu bilirkişi raporlarıdır. Dolayısıyla el yazısı imza, kullanım kolaylığı ve yüksek isabet oranı ile doğrulanabilmesi nedeniyle çok genel bir kullanım alanına sahiptir.

İş ilişkilerinin yoğunlaşması ve günlük hayattaki olayların hızlanması nedeniyle imza kullanma ihtiyacının her geçen gün arttığını söylemek yanlış olmaz. Ayrıca günümüzde sanal ortamın önemi, el yazısı imza yerine başka araçların/yöntemlerin kullanımını gündeme getirmiştir. Bu değişiklik sonucunda "elektronik imza" ve "güvenli elektronik imza" gibi terimler günümüzde yeni terimler olarak kabul edilebilir. Güvenli elektronik imza, kullanım kapsamı ve hukuki niteliği ile ilgili ayrıntılı düzenlemelere sahip olmakla birlikte, dijital bir ekrana atılan imzanın hukuki niteliği konusunda açık bir tartışma mevcuttur.

2.3. Elektronik İmza

Türkiye'de 5 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu ile nitelikli elektronik imzanın kullanımına izin verilmiştir. Yasal olarak elektronik imza, *"Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"* olarak tanımlanmıştır [6]. Hukuki olarak elektronik imza, ıslak imzaya denk sayılabilmesi için güvenli elektronik imza türünde oluşturulmalıdır. Olması gereken şartlar kanunda aşağıdaki şekilde yer almaktadır:

a. *"Münhasıran imza sahibine bağlı olmalıdır."*
b. *"Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulmalıdır."*
c. *"Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlamalıdır."*
d. *"İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlamalıdır [7]."*

2.4. Elektronik İmza Seviyeleri

Avrupa Birliği'nin (AB) 1999/93/EC Direktifi temel alınarak 5070 sayılı Kanun yayımlanmıştır. Bu kanun, güven hizmetlerini elektronik imza ve zaman damgası ile sınırlamıştır. Detaylı incelendiğinde 5070 sayılı Kanun'da yapılan elektronik imza tanımı ile Avrupa Birliği'nin yayımlamış olduğu direktifteki tanım benzerlik göstermektedir. Avrupa Birliği (AB) tarafından 1999 yılında yayımlanan direktif, birlik içerisinde üye ülkeler arasındaki ticaretin artmasını hedeflemiştir. Hatta bu hedefini genel bir elektronik imza çerçevesi çizerek güçlendirmiştir. Yani AB üyesi ülkelere inisiyatif tanıyarak ulusal yasal düzenlemeler yapmasını istemiştir. Aslında bu direktif, teknolojik gelişmelere açık

olduğunu belirtmeyi amaç edinmiştir. Ancak bu durum, her ülkenin farklı uygulamalara gitmesine sebebiyet vermiştir. Sonuç olarak 1999 yılında yayımlanan Avrupa Komisyonu Direktifinin ihtiyacı tam olarak karşılayamaması üzerine 2014 yılında Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü (eIDAS) oluşturulmuştur. Türkiye'de Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü'nün bir karşılığı bulunmamaktadır. Bu tüzük, bir Avrupa Birliği tüzüğüdür. Böylece imza türleri için güven hizmetleri çeşitlendirilmiştir.

AB tarafından 2014 yılında yayımlanan Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü, 1999 yılında yayımlanan Avrupa Komisyonu Direktifi'nin yerini almıştır. Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü'nde üç farklı elektronik imza türü yer almaktadır (Şekil-2.1): *Basit, gelişmiş* ve *nitelikli* olmak üzere birbirini kapsayan elektronik imza türleri tanımlanmıştır. Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü'nde tanımlanan üç farklı elektronik imza türünün AB üyesi ülkelerde işlemlerdeki kullanımının, belgenin gerektirdiği güvenlik ihtiyacına göre belirlendiği görülmektedir.

2.4.1. Basit Elektronik İmza

Elektronik verilere eklenen veya elektronik formdaki bir imza değeriyle mantıksal olarak ilişkilendirilen imza türüdür. Taranmış bir imza görüntüsü eklemek veya "Kabul ediyorum" düğmesine basmak, basit elektronik imza örneklerindendir.

2.4.2. Gelişmiş Elektronik İmza

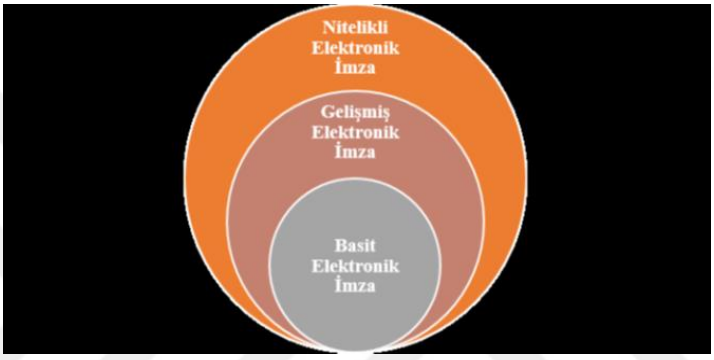
Belirli gereksinimleri karşılayan ve daha yüksek düzeyde imza doğrulama, güvenlik ve gizlilik sağlayan bir imza türüdür. Basit elektronik imzanın sağlaması gereken koşullara ek olarak;

a. İmzalayana benzersiz bir şekilde bağlanır.
b. İmza sahibini tanımlayabilir.
c. İmzalayanın kendi kontrolü altında benzersiz veriler kullanılarak oluşturulur.
d. İlişkili olduğu verilerle bağlantı kurar, böylece verilerdeki değişiklikler algılanabilir.

Bu çalışmanın konusu olan dijital ortamlara atılı imzalar bu kapsamda değerlendirilebilecek imzalardır.

2.4.3. Nitelikli Elektronik İmza

Onaylı bir elektronik imza sertifikasına dayalı olarak elektronik imza bilgileri kullanılarak onaylı bir elektronik imza oluşturma cihazı tarafından oluşturulur. Gelişmiş elektronik imza gereksinimlerine ek olarak, imzalayanın sertifikasının bir elektronik sertifika hizmet sağlayıcısı tarafından düzenlenmesini ve şifreleme anahtarlarının onaylı bir elektronik imza oluşturma aracında saklanmasını gerektirir. Kamu kurumlarında kullanılan elektronik imzalar nitelikli elektronik imzalara örnektir.



Şekil-2.1. Elektronik İmza Seviyeleri

2.5. Elektronik İmza Hakkında Hukuki Düzenlemeler

Elektronik ticaretin hızlanması ve teknolojinin gelişmesi sonucunda Birleşmiş Milletler Uluslararası Ticaret Örgütü, üye devletlerin düzenlemelerinde model olması amacıyla 1996 yılında Elektronik Ticaret Model Yasası'nı (UNCITRAL) hazırlamıştır. Bu kanunda, elektronik ortamda işlemlerin güvenli bir şekilde yürütülmesini sağlamak üzere, elle atılan imzanın işlevlerinin elektronik ortamda gerçekleştirilmiş sayılabilmesi için belirli koşullar getirilmiş ve elektronik imzanın imzayı kullanan kişinin kimliğinin tespit edilmesini sağlayan güvenilir bir yöntemle oluşturulması şartı getirilmiştir (m.7). Elektronik belgenin bütünlüğünün korunması için güvenilir bir garanti olması gerektiği de vurgulanmıştır (m.8) [8].

2.5.1. Birleşmiş Milletler Örgütü Tarafından Getirilen Düzenlemeler

Elektronik ticarete ilişkin özel bir model kanun olan Elektronik Ticaret Model Yasası hazırlanmış ve 05.07.2001 tarihinde onaylanmıştır. Söz konusu model kanun, elektronik

imzaların tanımı ve işlevleri konusunda AB Direktifine benzer hükümler getirmiştir. Bir elektronik imzayı güvenilir kılmak için, imzayı oluşturmak amacıyla kullanılan bilgilerin kullanılan belgeyle ilgili olarak imzalayana bağlı olması gerekir. Ayrıca imza anında, imza, sahibinin kontrolü altında ve imza anından sonra elektronik imzada yapılan tüm değişiklikler tanımlanabilir olmalı, imzaya eklenen bilgilerin de bütünlüğünü sağlamaya yönelik tedbirler uygulanmalıdır. Bu kanunda tanımlanan güvenli elektronik imzanın diğer imza tekniklerini kısıtlamayacağı ve hukuki olarak etkisiz kılamayacağı belirtilmiştir. Dolayısıyla gerekli şartları sağlayan tüm imza tekniklerinin eşit olarak değerlendirilmesi gerektiği öngörülmüştür. Model kanunun ıslak imza ile elektronik imzayı eşdeğer görmesi daha sonra çıkan mevzuatlarda da benimsenmiştir.

2.5.2. Avrupa Birliği Üyesi Ülkelerde Hukuki Düzenlemeler

Avrupa'da bulunan ülkelerde elektronik imza kullanımı uygulamada değişkenlik göstermektedir. Kira sözleşmesi imzalamak, kredi başvurusu yapmak gibi işlemler için nitelikli elektronik imza gerekirken; telekomünikasyon, bankacılık alanlarında genellikle gelişmiş elektronik imza kullanımı, yükseköğrenim veren okullardaki idari işlerde ise çoğunlukla basit elektronik imzanın kullanıldığı görülmektedir.

Ortak çerçeve koşullarının tanımına ilişkin 13 Aralık 1999 tarihli ve 1999/93/EC sayılı yönerge ile 2000/31 sayılı ve 8 Haziran 2000 tarihli elektronik ortamda yapılan ticari sözleşmelerin usul ve esaslarını belirlemek için bir Avrupa Birliği yönergesi yayımlandı [9].

1999 yılında yürürlüğe giren Avrupa Komisyonu Direktifi, AB'ye üye ülkelerde kullanılan elektronik imza yazılımları arasında yeknesaklığı sağlayamamıştır. Aslında bunun en büyük sebebi; bu direktifte elektronik imzanın yasal çerçevesi belirtilmesine rağmen bir AB üyesi ülkede oluşturulan elektronik imzanın başka bir AB üyesi ülkede de tanınacağının açık bir şekilde belirtilmemesidir. Bu karışıklığa son vermek ve elektronik imzaların AB genelinde kullanımını artırmak amacıyla 2014 yılında Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü yayımlanmıştır. 2014 yılından itibaren, bu tüzük AB'ye üye ülkeler için ayrıntılı bir yasal çerçeve sağlamıştır. Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü'nün yayımlanmasıyla birlikte her ülkenin kendi ülkesi içinde ayrı bir düzenleme yapmaksızın işlemlerin standart bir şekilde yapılması amaçlanmıştır.

AB bu direktifte güven hizmetlerini, zaman damgası ve elektronik imza ile sınırlandırmıştır. Ancak 2014'te Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü ile birlikte bu hizmetler çeşitlendirilmiştir. Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü 26'ncı maddesinde teknolojide meydana gelen gelişimin öngörülememesi nedeniyle bu tüzükte yeniliğe açık bir çerçeve benimsendiği belirtilmiştir. Aynı tüzüğün 27'nci maddesinde "*Bu tüzük teknolojiden bağımsız olmalıdır. Verdiği yasal etkiler, bu tüzüğün gerekliliklerinin yerine getirilmesi şartıyla herhangi bir teknik yolla sağlanmalıdır."* denilmektedir [10]. Takip eden yıllarda komisyon uygulama kararları ile bazı maddelerin kapsamı genişletilmiştir. Mesela, 2015 yılında alınan komisyon uygulama kararı ile gelişmiş elektronik imza için kullanılan formatlar ayrıca belirlenmiştir. Böylece günümüzde geçerli olan *Avrupa Telekomünikasyon Standartları Enstitüsü* standartları referans alınmıştır [11].

Akıllı Bilgi Yönetimi Derneği 2016 yılında AB üyesi ülkelerdeki elektronik imza kullanımı ile ilgili bir araştırmanın sonuçlarını yayımladı. Bu araştırmaya göre bazı ülkelerin farklı uygulamalara bile yer verdiğini tespit etti. Örneğin, İtalya'da elle dijital ekranlara atılan imzaların bazı alanlarda kullanıldığı görülmüştür. İtalya'da 2013 yılında Gelişmiş Elektronik İmza için Teknik Düzenlemeler Kararnamesi'nin yayımlanması bu durumun ortaya çıkmasının en büyük sebebidir [12]. İspanya ve Slovakya'da da dijital ekranlar üzerine elle atılan biyometrik imzaların yaygınlaştığı görülmektedir.

Almanya, Avusturya ve İsviçre'de ise kira sözleşmesi ve tüketici kredisi başvurusu imzalamak gibi bazı işlemler sadece nitelikli elektronik imzalar uygulandığı takdirde hukuki olarak geçerli sayılmaktadır. Bu işlemlerin haricinde, örneğin, Almanya'da kanunlar gereği evlilik, miras sözleşmeleri, ömür boyu tazminat taahhüdü, kefalet sözleşmesi gibi işlemlerde güvenli elektronik imza kullanılamamaktadır [13].

AB'ye üye ülkelerde özel bir hukuki statüsü olan tek elektronik imza türü nitelikli elektronik imzadır. AB Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü her ne kadar elektronik imzaları sınıflandırsa da sadece nitelikli elektronik imzayı yasal statüye kavuşturmuş ve diğer elektronik imza türleri ile ilgili herhangi bir düzenlemeye gitmemiştir. Tüzüğün, 25'inci maddesinin a. bendinde "*Bir elektronik imzanın, yalnızca elektronik biçimde olması ve nitelikli elektronik imza gerekliliklerini yerine getirmemesi tek başına yasal işlemlerde delil teşkil edemeyeceği veya kabul edilebilir sayılmayacağı*

anlamına gelmez." cümlesi ile diğer elektronik imzaların kabul edilebilirliğini değerlendirecek olan hukuki makama inisiyatif bıraktığı düşünülebilir [14].

2.5.3. Türkiye'de Hukuki Düzenlemeler

Türkiye'de elektronik imza konusunda gerekli araştırmalar yapıldıktan ve diğer kanun hükümleri düzenlendikten sonra Elektronik İmza Kanunu hazırlanmıştır. 5070 sayılı kanun olarak kabul edilmiştir ve 2004 yılında yayımlanarak yürürlüğe girmiştir. Kanunun içeriği 1999/93/EC sayılı AB Direktifi'ne ve Birleşmiş Milletler Uluslararası Ticaret Örgütünün Elektronik Ticaret Model Yasası'na uygun olarak hazırlanmıştır.

5070 sayılı kanunu incelediğimizde nitelikli elektronik imzadan güvenli elektronik imza olarak bahsedildiği anlaşılmaktadır. Hukuki olarak ıslak imzayla eşdeğer kabul edildiği de anlaşılmaktadır. Elektronik İmza Kanunu'nun "*Güvenli Elektronik İmza ve Sertifika Hizmetleri*" bölümünde ortaya konan şartlar nedeniyle, "güvenli elektronik imza; tekillik, inkâr edilemezlik, kimlik doğrulama ve veri bütünlüğü" sağlamalıdır. Nitelikli elektronik sertifika (NES) ile oluşturulması da zorunludur [15].

5070 sayılı Elektronik İmza Kanunu ile denetim ve kontrol yetkisi Telekomünikasyon Kurumuna verilmiştir. Telekomünikasyon Kurumu, 2008 yılında yapılan değişiklik ile *Bilgi Teknolojileri ve İletişim Kurumu (BTK)* adını almıştır.

5070 sayılı Elektronik İmza Kanunu ile güvenli elektronik imzanın özellikleri (AB Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü'nde nitelikli elektronik imza olarak geçen elektronik imza), imza oluşturma ve doğrulama araçları, hizmet sağlayıcıları, güvenli elektronik sertifikalar, sertifika sağlayıcıları ve yükümlülükleri düzenlenmiştir [16]. Hukuki olarak el ile atılan ıslak imza ile aynı yasal sonuçları doğuracağı ve bazı özel durumlarda kullanılamayacağı belirlenmiştir [17]. Diğer elektronik imza türleri ile ilgili bir düzenleme yapılmamıştır.

Elektronik İmza Kanunu'nun yürürlüğe girmesi ile ilgili kanunların imza şartı gerektiren maddelerinde güncelleme yapılarak güvenli elektronik imza, ıslak imza ile eşdeğer olarak kabul edilmiştir.

Türkiye'de faaliyet gösteren firmalar teknolojik gelişmelerden faydalanmak ve maliyetleri azaltmak gibi sebeplerle 5070 sayılı Kanun'da düzenlenmemiş elektronik imza türlerini de kullanmaya başlamışlardır. *Bilişim Teknolojileri ve İletişim Kurumu*

Hukuk Dairesi tarafından yapılan çalışmalarla 28.10.2017 tarihinde 30224 sayılı resmî gazetede yayımlanan Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği'nde *Bilişim Teknolojileri ve İletişim Kurumu* tarafından belirlenecek usuller ile elektronik ortamda abonelik sözleşmesi akdedilebileceği hükme bağlanmıştır.

Bu yönetmelikle birlikte, banka ve GSM operatörleri başta olmak üzere, birçok farklı sektörde elektronik ortamda sözleşmeler yapılarak elektronik imza türleri ile onaylama işlemi başlatılmıştır.

Ülkemizde, hemen hemen tüm işlemlerde güvenlik kıstaslarının tam olarak belirlenmemesi nedeniyle genellikle nitelikli elektronik imzanın kullanıldığı görülmektedir. Ancak son yıllarda alternatif imzalama türleri de ortaya çıkmıştır. Bunların içinde en yaygın olanı biyometrik imza ya da dijital ekranlara elle atılan imza olarak adlandırılan imza türüdür. Literatürde farklı isimlerle de anılmakla birlikte biyometrik imza, Türkiye'de cep telefonu hattı operatörleri ve bankalar tarafından kullanım kolaylığı ve tasarruf sağlaması nedeniyle birçok işlemde kullanılmaktadır. Dokunmatik ekranda parmak hareketleriyle veya yazmaya uygun kalemle atılan imzaya ilişkin mevzuatta açık hükümler bulunduğu söylenemez. Bu şekilde atılan imzaların güvenli elektronik imza kapsamında değerlendirildiği de söylenemez.

2.6. Dijital Ortamlara Atılı İmzalar

Dijital ortamlara atılı imzalarla ilgili alanyazın taraması yapıldığında farklı terimlerle karşılaşılmıştır. Bu terimler;

1. Biyometrik imza,
2. Biyodinamik imza,
3. El ile atılan dijital imza,
4. Dinamik imza,
5. El ile atılan elektronik imza,
6. Çevrimiçi (online) imzadır.

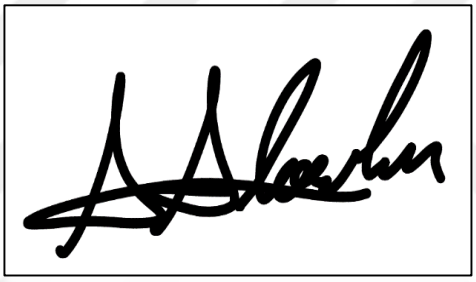
Dijital ortamlara atılı imzalar, atılmaları esnasında imzanın görüntüsü ile birlikte boyutsal koordinatlar, zaman ve baskı değerleri gibi daha detaylı bilgiler barındıran klasik el yazısı ve imza yazma davranışının bir ürünüdür. Bazı bilgisayar ve telefon uygulamalarının

cihaz ekranına atılan imzanın sadece görüntüsünü belgeye eklemesi ile atılan imzalar da bulunmaktadır.

Dijital ortamlara atılı imzanın diğer elektronik imzalama yöntemlerinden farkı; imzalama sürecine dair imza, imzalayan ve cihaza ait veri seti toplamasıdır. Toplanan veri, dokümanının içinde güvenli bir şekilde saklanır.

2.6.1. İmza Görüntüsü Saklanan İmzalar

Gelişen teknoloji ile insanların birçok işini akıllı telefon, tablet ve bilgisayarlardan sonuçlandırabilmesi sayesinde uzaktan erişim ile işlerin yapılması ön plana çıkmıştır. Bununla birlikte telefon ve bilgisayar uygulama geliştiricileri not ve belge oluşturma uygulamalarına imza ekleme seçenekleri koymuştur.



Şekil-2.2. Tablet Ekranına Kalem ile Adobe Reader Uygulamasında Atılan İmza

Şekil-2.3. Tablet Ekranına Kalem ile Adobe Reader Uygulamasında Atılan İmza

2.6.2. Biyometrik İmzalar

Biyometrik imzalar; imza pedi, tablet veya akıllı telefon gibi cihazlara kalem, parmak vb. bir araçla atılan, atılışı esnasında hareketlerin zamana bağlı sayısal veriler hâline dönüştürecek bir yazılım kullanılarak elde edilen imzalardır.

*Uluslararası Standartlar Teşkilatı*nın ISO/IEC 19794-7 standardı ile bu imzaların zaman serileri içinde farklı özellikleri toplayabileceği belirlenmiştir. Toplanan bu özellikler;

1. X, Y, Z koordinatı,
2. X, Y yönünde hız,
3. X, Y yönünde ivme,
4. İlk noktadan itibaren geçen süre,
5. Bir önceki noktadan itibaren geçen süre,
6. Kalem baskısı,
7. Kalem ucu anahtarı durumu,
8. X ve Y ekseni boyunca kalem ucu eğimi,
9. Kalem kaldırma ve
10. Kalem dönüşleri olabilir, şeklindedir.

Dijital olarak yakalanmış imza olarak da adlandırılan biyometrik imzada imzayı atan şahısların biyometrik verileri kullanılır. Bu veriler dijital bir ekrana imza atma esnasında kaydedilir ve çoğunlukla belgeyle birlikte şifrelenerek bütünleştirilir [18]. İmza atma esnasında kaydedilen biyometrik veriler; el yazısı ve belge inceleme uzmanları tarafından kişinin imzasını analiz ederken dikkat ettiği ayırt edici olan hız, basınç, ivme ve eğim gibi özelliklerdir. Açıkça anlaşılmaktadır ki biyometrik imza analizlerinin yapılabilmesi için biyometrik verileri dijital olarak yakalayabilecek bir donanıma ve yazılıma ihtiyaç vardır. Bu donanımların ve yazılımların oluşturacağı kombinasyon imzanın hem statik hem de dinamik verilerini belli standartlarda yakalayabilmeye ve kaydedebilmeye uygun olmalıdır. Ancak bu şekilde hem statik hem de dinamik veriler elektronik belgede saklanır ve kriminal inceleme için elverişli hâle gelir.

2.7. Biyometrik İmza İnceleme Alanında Yapılan Çalışmalar

"Dijital imza" fikri ilk olarak Diffie ve Hellman'ın çığır açan makaleleri "New Direction in Cryptography"de (1976) ortaya çıktı. Bu çalışmada bir A kullanıcısının bir M mesajı için imzasının mesaja ve kullanıcı tarafından gizli tutulan bilgilere bağlı bir değer olması gerektiğini, herkesin A'nın imzasının geçerliliğini doğrulayabileceğini, ancak hiç kimsenin A'nın imzasını herhangi bir mesajda taklit edemeyeceğini öne sürdüler. Dijital imza kavramı sağlam, kullanışlı ve hatta yasal olsa bile; tuzak kapı (trap door) işlevleri

kullanılarak uygulanmaları hâlinde birtakım teknik sorunlar ortaya çıkacağını savundular [19].

Dijital imza şeması kavramı da Diffie ve Hellman tarafından tasarlanmış ve tek yönlü kimlik doğrulama olarak adlandırılmıştır. Bu kavramın ilk örnekleri de 1978 yılında Rivest ve arkadaşları ile 1979 yılında Lamport tarafından verilmiştir. Dijital imza şemasının kanıtlanabilir güvenlik işlemleri de ilk defa Goldwasser ve arkadaşları tarafından 1995 yılında "Mesaj Saldırılarına Karşı Güvenli Bir Dijital İmza Şeması" çalışması ile tanımlanmıştır. Bu tanımda, kendi seçtiği mesajlarda hesaplanmış imzalara erişimi olan varsayımsal bir saldırgan, bazı yeni mesajlar için yeni bir imza oluşturmayı amaçlamıştır [20]. Canetti (2007) ile Pfitzmann ve Waidner (2001), kriptografik şemaların güvenliğini koruyan güvenlik çerçeveleri geliştirdi. Bu güvenlik çerçevelerinde, Dijital imza şeması gibi bir kriptografik şemanın güvenliği, algoritmalar ve güvenlik özellikleri idealize edilerek modellenmiştir [21].

Bir bütün olarak veya kısmen dijital olarak yakalanmış imzaların adli incelemesine ayrılmış çalışmalar ve dijital olarak yakalanmış verileri kullanan gerçek ve simüle edilmiş imzalar arasındaki adli ayrımcılığa odaklanan özel yayınların yanı sıra, çözümler arası karşılaştırmalarla ilgili olarak imza verilerinin güvenilirliğine odaklanan birkaç makale bulunmaktadır:

2009'da yayımlanan bir çalışmada Franke ıslak imzaları aynılarının dijital temsilleriyle karşılaştırdı [22]. Endüktif sensör teknolojisine sahip bir cihazda imzalama sırasında kalem eğiminin neden olduğu sözde yer değiştirme hatasını gözlemledi.

Smejkal ve arkadaşları da Signotec firmasının ürettiği çeşitli cihazları kullanarak 40 katılımcı tarafından sağlanan dijital olarak yakalanmış imzaların stabilitesini inceledi [23]. Signotec'in imza eşleştirme algoritmasını kullanarak, 38 katılımcıda, aynı cihazla yakalanıp karşılaştırılan iki imza için ≥ %60 yazar içi eşleşme oranı elde ettiler. Bu sonuç, yazarlara göre kullanılan cihazdan bağımsız olarak imzaların yüksek kararlılık sergilediğini gösterdi. Bununla birlikte, çalışma, kararlı ve kararsız imzaları ayırt etmek için neden ≥ %60'lık bir ölçek algoritması sonucunun ayarlandığını açıklamamaktadır ve ayrıca sonuçlar yalnızca cihaz içi karşılaştırmalar için gösterilmektedir. Cihazlar arası karşılaştırmalar için yapılan çalışma, yalnızca imza pedlerinin farklı tasarımının daha yüksek yazar içi imza değişkenliğine yol açabileceğini öngörmektedir.

Ayrıca, Heckeroth, Kerkhoff ve Weyermann kuvvet değerlerinin geçerliliği ile ilgili olarak bir çalışmayı yayımladılar [24]. Yazarlar, uygulanan kuvvet ile imzalama çözümü tarafından bildirilen değerler arasındaki fonksiyonun aynı sensör teknolojisini kullanan farklı cihazlar arasında bile değişiklik gösterdiği sonucuna varmıştır. Bu nedenle, kuvvet değerleri yorumlanırken dikkatli olunmalıdır. Aslında bu makale, sayısal verilerin kodlanması noktasında daha temel bir yöne odaklanmıştır: Çeşitli donanım ve yazılım kombinasyonlarının, yalnızca nicel (değişkenlerin sıklığı ve sayısı) ve nitel (bu değişkenlerin nasıl ölçüldüğü) tanımlamalarında değil, aynı zamanda verilerin kodlanma ve yapılandırılma biçiminde de farklılık gösteren veriler üretmesi nedeniyle imzaların karşılaştırmasını daha da karmaşık hâle getirmektedir. Bir adli yazılım çalışma ortamında farklı cihazlarla yakalanan dijital olarak yakalanmış imzaları analiz etmek ve karşılaştırmak için iki koşulun karşılanması gerektiği sonucuna ulaşmışlardır: (a) veriler uyumlu bir formatta olmalı ve (b) yakalanan değerler tek tip ölçeklere dayanmalıdır.

Dijital olarak yakalanmış imzaları bu tür birlikte çalışabilirliğini geliştirmeyi amaçlayan uluslararası bir standart olarak, ISO/IEC 19794–7, 2015 yılında yayımlandı [25]. Yayımlanan bu standart ile hangi verilerin yakalanabileceği açıklanmış, uyumlu veri formatları belirtilmiş ve veri kaydı içeriği örnekleri sunulmuştur. Dijital olarak yakalanmış imzaların birlikte çalışabilirliğini güvence altına alan temel meta veriler, ölçeklendirilmemiş sayısal değerleri ortak birimlere dönüştürmek için kullanılan oranlardır. Yani ISO standardına göre normalize edilen veriler için, boyutlar milimetre olarak verilir, kuvvet değerleri yüzde olarak ölçülür ve süreler saniye olarak rapor edilir.

3. GEREÇ VE YÖNTEM

3.1. Biyometrik İmzanın Oluşturulması

Günlük işlemlerin dijitalleştirilmesi, el yazısının kullanımını değiştirmiştir. Son yıllarda el yazısı imzalar, belgeleri kâğıda ihtiyaç duymadan imzalamak için imza atma sürecinde dijital ortama aktarılmaktadır. Biyometrik imzalar, dinamik imzalar, elektronik olarak yakalanan imzalar veya çevrimiçi imzalar olarak da bilinen bu dijital olarak yakalanan imzaların amacı, imzalanan belgelerin daha ucuz ve daha hızlı yönetimini sağlamaktır. Dijital olarak yakalanmış imzalar, tablet bilgisayar gibi bir sayısallaştırma cihazı ile tipik olarak bir PDF dosyasına imza yerleştiren bir yakalama yazılımı ile oluşturulur. Kâğıt üzerindeki belgelerde olduğu gibi, dijital olarak imzalanmış dosyalar da yasal bir ihtilafın konusu olabilir. Belgenin bütünlüğünün analizi yapılırken, örneğin belgenin imzalanmasından sonra olası değişiklikler konusu, adli bilişim uzmanlarının yetkisine girerken; tartışmalı dijital olarak yakalanmış imzaların yazarının kimliğinin tespiti, adli el yazısı incelemesi alanının konusudur.

Bir dijital olarak yakalanmış imzayı incelerken, el yazısı uzmanı genellikle PDF belgesinde görüntülenen bir imzanın iki boyutlu resimli temsili ile sınırlı değildir, aynı zamanda temel imzalama dinamiklerini yeniden yapılandırmak için gerekli olan dijital olarak yakalanmış imzanın sayısal verilerine erişim sağlayabilir. Uluslararası ISO/IEC 19794-7:2014/AMD 1:2015 standardına göre veriler, yazma işlemi sırasında belirli bir frekansta yakalanan en az uzamsal XY koordinatlarından, zaman bilgisinden ve kuvvet değerlerinden oluşmalıdır. Bazı yakalama çözümleri ayrıca "havadaki yörüngeler" veya "hava hareketleri" olarak adlandırılan bir imza pedinin yüzeyinin üzerindeki kalem ucunun yörüngesini de kaydeder. Dijital olarak yakalanmış imzalar; grafik ögelerin şekli ve yapısı, vuruş yönü ve sırası gibi kâğıt üzerinde yapılan yazılarda bulunan niteliksel özellikleri içerir. Bununla birlikte, dijital olarak yakalanmış imzalarda bulunan sayısal veriler, adli el yazısı incelemesi için ek fırsatlar da sunmaktadır. Dijital olarak yakalanan veriler, yalnızca ıslak imzalarda dolaylı olarak tahmin edilebilen, basınç ve zamanla ilgili özellikler -örneğin; imza süresi, yazma hızı ve hızlanma hakkında- nicel olarak ölçülen bilgileri içerir.

Dijital olarak yakalanmış imzalar ile ıslak imzaların karşılaştırıldığı çalışmalar, dijital olarak yakalanan imzalar ile geleneksel imzalar arasında istatistiksel olarak önemli

özellik farklarını ortaya koydu. Ancak, çalışmalara katılan el yazısı ve doküman inceleme uzmanlarının derecelendirmelerine göre, bu farklılıklar adli bağlamda hatalı sonuçlar riskini taşıyabilecek "açıkça farklı" bir imzalama davranışı göstermemektedir. Bu, imzalamanın değişen koşullar altında sabit kalan ve adli el yazısı inceleme disiplinindeki temel önermelerle uyumlu, oldukça otomatikleştirilmiş bir davranış olduğu varsayımıyla uyumludur [26].

Biyometrik imzanın oluşturulmasını ya da yakalanmasını sağlayan yazılımlar ülkemizde belli bir standart çerçevede olmadığından farklı niteliklere sahiptir. Başka bir deyişle, kişi dijital bir ekran üzerinde özel bir elektronik kalem kullanarak imzalama işlemini yapmaktadır. İşte tam bu esnada, uygun bir donanım ve yazılım kullanılarak oluşturulan imzadan şahsa ait biyometrik veriler elde edilebilmektedir.

Farklı kombinasyonlarda bir araya gelen yazılım ve donanım kurguları da farklı sonuçlar çıkarabilmektedir. Şöyle ki, kimi uygulamalar belge ile elektronik veri arasındaki bağlantıyı gösteren bir kanıt oluşturmak için belgenin özet değeri ile imzacıya ait biyometrik verileri birlikte şifreleyerek saklarken kimi uygulamalar şifrelemeden önce zaman damgası bilgisi de ekleyerek imza zamanının tespit edilebilmesine olanak sağlar [26]. Bazı kombinasyonlar ayrıca imzanın görseli, imzalanan belgenin özeti, belgenin tanımı, imzacıya ait kimlik bilgileri gibi birçok özelliği bir bütün hâline getirir ve bu şekilde saklar. Hatta bazıları ayrıca nitelikli elektronik sertifika ile imzalanarak tamamen korumaya alınır.

3.2. Islak İmzaya Denklik

5070 sayılı Elektronik İmza Kanunu'na göre ıslak imza ile denk olan elektronik imza türü sadece nitelikli elektronik imzadır. Avrupa Birliği'nin yayımladığı eIDAS tüzüğüne göre ise dijital olarak biyometrik verileri yakalanan imza hukuki olarak geçerli sayılmaktadır, ancak ıslak imza ile eşdeğer nitelikte görülmemektedir. Bu durum kimi el yazısı ve doküman inceleme uzmanları tarafından hukuki dayanak eksikliği olarak görülmektedir. Dolayısıyla adli inceleme yapılamayacağı görüşünü savunmaktadırlar.

3.3. Veri Bütünlüğü

Nitelikli elektronik imzada açık anahtarlı kriptografi kullanıldığı için belgede ya da sayısal verilerde yapılacak bir değişiklik imzanın orijinalliğinin kaybolmasına sebebiyet

verir. Nitelikli elektronik imza bünyesinde imzalanan belgenin özet değeri de yer aldığı için imza ile belgenin ilişkisi korunabilmektedir. Aynı şekilde uluslararası standartları benimseyen biyometrik imza yazılımı ve donanımı da belgenin özet değeriyle biyometrik verileri şifreleyerek bir bütün hâlinde koruma yeteneğine sahiptir. Fakat bu imkânı sağlayamayan kombinasyonlar için biyometrik imzanın yakalandığı donanımda şahsa gösterilen belgenin imzalandığı garanti altına alınamaz. Yani, imza ve belge bütünlüğü söz konusu olamaz. İmzanın transfer edilmesine olanak sağlayabilir. Ayrıca şifreli bir şekilde koruma olmadığında sonradan değişiklik yapılabilir.

3.4. İmza Oluşturma Güvenliği

Temel olarak nitelikli elektronik imza oluşturma verisine özel anahtar, nitelikli elektronik imza doğrulama verisine de açık anahtar denilmektedir. Açık anahtarlı kriptografi ile birlikte kullanılan özel anahtar sadece sahibi tarafından kullanılabilmektedir. Yani herkes tarafından erişime ve kullanıma imkân veren açık anahtarla özel anahtar arasında matematiksel bir bağlantı vardır. Özel anahtara erişim yalnızca PIN ile giriş yapıldığında mümkün olmaktadır. Biyometrik imzada ise güvenlik anlamında zayıf noktalar bulunmaktadır, çünkü kişilere ait olan biyometrik veriler donanım tarafından imzanın doğrulanması amacıyla kaydedilmektedir. Yani, özel anahtar olarak görebileceğimiz biyometrik veriler imza atma esnasında kaydedilmektedir.

3.5. İmza Doğrulama Güvenliği

Nitelikli elektronik imzada şifre girilerek işlem yapıldığı için doğrulama anlık olarak yapılabilmektedir. *Elektronik Sertifika Hizmet Sağlayıcısı (ESHS)* aracılığıyla nitelikli elektronik imzanın doğrulama bilgilerine ulaşılabilir. Biyometrik imza ya da dijital olarak yakalanmış imzada ise anında ve sonradan doğrulama yapmak mümkündür. Sonradan doğrulamaya itilaf konusu olması durumunda başvurulmaktadır. Böyle bir durumda imzacının inceleme konusu imzasıyla mukayese imzalarının karşılaştırılmasıyla doğrulama yapılır. Hatta bazı iş kolları, özellikle bankalar, kendi uygulamaları üzerinden imzacının biyometrik verilerini kaydederek çevrimiçi bir şekilde doğrulama yapmaktadır. Böylece farklı zamanlarda aynı kişinin oluşturduğu imzalar yerel veri tabanından sorgulanarak eşleştirme sağlanabilmektedir. Ancak bu uygulamanın da güvenlik zafiyeti yaratabileceği açıkça ortadadır.

Hangi biyometrik verilerin hangi ölçü biriminde yakalanacağı ile ilgili uluslararası standartlar belirlenmiştir. Kullanılan donanım ve yazılım ne olursa olsun bu standartlara uyulmalıdır. Aksi takdirde donanım ve yazılımın türüne göre biyometrik verilerin yakalanmasında farklılıklar oluşacaktır. El yazısı ve belge inceleme uzmanları tarafından karşılaştırma yapmak da mümkün olamayacaktır.

3.6. Kullanım Kolaylığı

Nitelikli elektronik imza sahibi olmak için kişinin öncelikle güvenirliği kabul edilen bir ESHS'ye nitelikli elektronik sertifika başvurusunda bulunması gerekmektedir. Ek olarak nitelikli elektronik imza kullanabilmek için kart okuyucu gibi bir donanım kullanmak zorunludur. Dolayısıyla nitelikli elektronik imza kullanıcısı için ek maliyet oluşmaktadır. Bu cihazların ortam bağımlılığı da kullanım kolaylığı noktasında sorunlar yaratmaktadır.

Biyometrik imzaya baktığımızda ise farklı bir durum karşımıza çıkmaktadır. Biyometrik imza tıpkı ıslak imza gibi oluşturulmaktadır. İmza pedi ya da tablet gibi dijital ekrana sahip bir cihaza biyometrik verileri yakalaması için yazılım yüklendiği zaman ortam bağımlılığı olmadan kişinin imzası her yerde alınabilmektedir. Böylece kolay bir şekilde imzacı tarafından imzalama işlemi yapılabilmektedir.

Nitelikli elektronik imza için oluşturulan değerler her belge için ayrı ayrı üretilmektedir. Gerekli koruma tedbirleri alındığı takdirde imzalanan belgeden imzanın alınıp başka bir belgeye transferi mümkün değildir. Bunun yanında biyometrik imza atılırken yakalanan biyometrik verilerin ele geçirilmesi ve başka bir belgeye transfer edilmesi daha mümkün görünmektedir.

Oluşturulduğu andan itibaren nitelikli elektronik imza kriptografik olarak korunmaktadır. Bu nedenle izinsiz transfer edilebilmesini engellemek için ek güvenlik tedbirlerine çok fazla ihtiyaç yoktur. Ancak biyometrik imzanın oluşturulması esnasında şifreleme genellikle bulunmamaktadır. Kullanılan donanımın özelliğine göre oluşturulan biyometrik imzanın başka bir ortama aktarılması gerekebilir. Bu aktarım esnasında biyometrik verinin ek güvenlik tedbirleri ile korunması gerekmektedir.

4. ANALİZ

Adli bakış açısından, dijital olarak yakalanan imzaların yakalanmasını ve kullanılmasını optimize etmek için teknoloji sağlayıcılar ve kullanıcı kurumlar için en iyi uygulama önerileri eksikliği vardır.

Adli el yazısı incelemesi yapılabilmesi için, dijital olarak yakalanan imza verileri, donanım ve yazılım meta verileri ve optimize edilmiş imzalama koşulları sağlanmalıdır.

Bir dijital olarak yakalanmış imzanın adli olarak incelenebilmesi için uygunluk kriterleri, üç ana başlık altında düzenlenmiştir: *veri gereksinimleri, dijital olarak yakalanmış imza çözüm gereksinimleri* ve *imzalama koşulları*.

4.1. Veri Gereksinimleri

Piyasada bulunan bazı dijital olarak yakalanmış imza çözümleri, imzanın yalnızca "düz" bir resmini, genellikle bir PDF dosyasına gömülü olarak kaydettiklerinden, el yazısı ve doküman inceleme uzmanlarına dijital olarak yakalanmış imza hakkında gerekli biyometrik bilgileri sağlamaz. Sınırlamalardan kaçınmak ve adli el yazısı incelemesini kolaylaştırmak için bir dijital olarak yakalanmış imza çözümü, ISO/IEC 19794-7:2014/AMD 1:2015 standardına uygun olarak verileri sağlamalıdır.

Birçok farklı firma *Uluslararası Standartlar Teşkilatı*nın ISO/IEC 19794-7 standardı ile sınırları belirlenmiş yazılımlar geliştirerek biyometrik imzaların saklanması, belgelerin imzalanması, belgeye eklenmesi ve belgeden çıkarılarak incelenmesi için programları piyasaya sürmektedir.

ISO/IEC 19794-7:2014 standartlarına göre alınmış bir imzanın verileri, Dijital Biyometrik Veri Kaydı'nda (BDIR) bayt dizileri şeklinde depolanır. Bu kayıt, imzanın tanıtıcı bilgilerini içeren bir başlık kısmı ve biyometrik verilerin saklandığı açıklama kısmı olarak iki parçadan oluşur.

Başlık Kısmı;

1. Dosyanın formatını,
2. Dosya formatının sürümünü,
3. Tam kayıt uzunluğunu,

4. Açıklama kısmında kayıtlı veri sayısını,
5. Bir sertifikasyonu varsa sertifikasyon bilgisini içerir.

Açıklama Kısmı;

1. Kısmın bayt sırasını,
2. Verilerin alındığı tarihi,
3. Yazılımın kayıtlı satıcı kimliğini,
4. İmzanın alındığı cihaz bilgilerini,
5. Kalite değerini,
6. Hangi verilerin kaydedildiğini,
7. Kaydedilen verilerin mümkün olan maksimum ve minimum değerlerini,
8. Değerlerin standart sapmasını,
9. Veri kanalının sabit olup olmadığını,
10. Kaydedilen imza verilerini,
11. Genişletilmiş veri uzunluğunu içerir [26].

Elektronik cihazlara atılarak elde edilen, kaydedilen ve transfer edilen imza verilerinin güvenilirliğini, bütünlüğünü ve gizliliğini korumak için aşağıdaki tekniklerin kullanılması gerekmektedir:

a) "Şifreleme yöntemleri,

b) Zaman damgası,

c) Loglama,

d) Erişim yetki ve kısıtlamaları"

Her ne kadar standartlarla sınırları belirlenmiş olsa da rekabeti önlememek adına bu sınırlar geniş tutulmuştur. Bazı firmaların yazılımları ise bu standartlara uymayan imza alma, saklama ve çıkartma yöntemleri kullanmaktadır.

Kullanılan yazılımlara göre imzanın sayısal verileri farklı formatlarda olabilir. Örnek olarak;

a) CSV/TSV formatları (Verilerin örnekleme anlarını ortak metin editöründe virgülle ya da sekmeyle ayırarak tek satırda gösteren formatlar)

b) ISO/IEC 19794-7 standardında belirtilen tam format, kompakt format, sıkıştırma format, XML formatı

c) Açık kaynak yazılımlarında okunabilen formatlar (XML formatı vb.)

d) Sadece belirli firmaların yazılımları ile okunabilen tescilli dosya formatları vb [27].

4.1.1. Sayısal Veri

Biyometrik imzaların atılması esnasında, yazılım özelliklerine göre farklı veriler zamana bağlı sayısal verilere dönüştürülerek toplanır (Çizelge 4.1.). Toplanabilen bazı özellikler;

(1) X, Y koordinatı

İmzanın atıldığı yüzey üzerindeki yatay ve dikey olarak konumu belirleyerek imzanın her noktasının sayısal olarak kayıt altına alındığı verilerdir.

(2) X, Y yönünde hız

İmzayı atan şahsın imzayı atarken yaptığı hareketlerdeki hızıdır.

(3) X, Y yönünde ivme

İmzayı atan şahsın imza atış esnasında kalem hareketlerini yaparken oluşan hız değişimlerinin kaydedildiği verilerdir.

(4) İmzanın Uzunluğu

İmzanın başlangıç ve bitiş noktası arasındaki mesafedir.

(5) İmzanın Yüksekliği

İmzanın Y ekseninde en alçak ve yüksek noktaları arasındaki mesafedir.

(6) İlk noktadan itibaren geçen süre

İmza atılan yüzey ve imza aracının birbiri ile ilk ve son teması arasında geçen süredir.

(7) Bir önceki noktadan itibaren geçen süre

İmza içerisindeki her nokta için kaydedilen zaman verileridir.

(8) Kalem basıncı

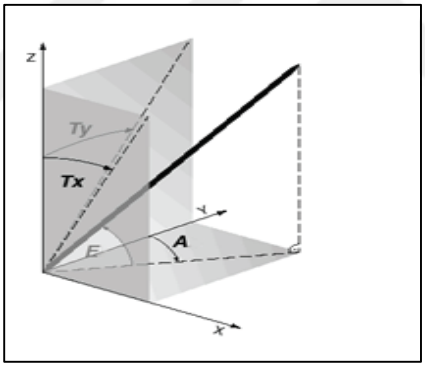
Uygun cihaz veya kalem ile atılan imzalarda yüzeye yapılan baskının ölçülerek kaydedildiği verilerdir.

(9) Kalem ucunun durumu ve eğimi

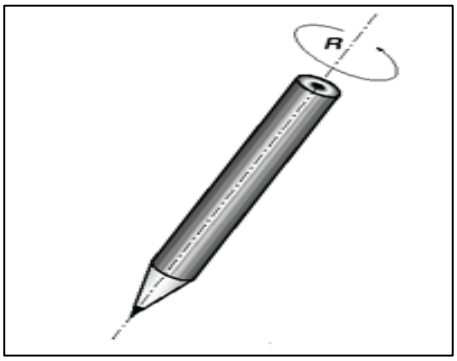
İmza atma aracının yüzeye dokunuş pozisyonuna göre kalem ile yüzey arasındaki açıların hesaplanarak oluşturulan verilerdir (Şekil 4.1.).

(10) Kalem kaldırma

İmza atılışı esnasında kalem ucunun yüzeyle temas kesilmelerini, uygun kalem ve yazılımlarla kalemin havada yaptığı hareketleri, tekrar temas noktası vb. verileri kaydedilebilir.



Şekil-4.1. İmza Kaleminin Hesaplanabilecek Açıları Sonuçları.



Şekil-4.2. Kalemin Kendi Ekseninde Dönüşleri

(11) Kalem dönüşleri

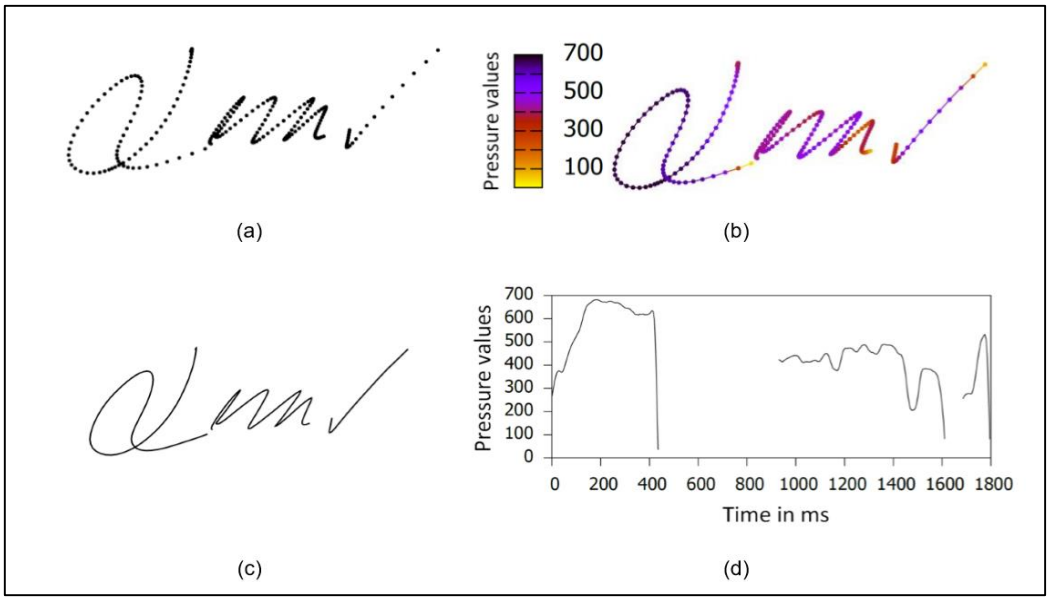
İmza atılışı esnasında kalemin x ve y düzlemlerinde yaptığı hareketlerde yön değişikliklerini kaydedilebilir (Şekil 4.2.). Toplanan bu özelliklerin zaman verilerinin tutulması ve zamana bağlı değişikliklerini gösterecek şekilde kaydedilmesi gereklidir. ISO/IEC 19794-7 standardına göre saniyede en az elli (50) veri toplanması gereklidir.

Parametre	Değer (İnceleme Konusu İmza)	Birim
İmza ID	MAYLtj8EJf7DPRADqM0swm7cD+GhD 1Cmv7DdEuti6X4=	-
İmza toplam süresi	4.2710	sn
El kaldırma sayısı	3	adet
Kalemin Temas Etmediği Süre	0.3830	sn
Ortalama X koordinatında hız	0.0044	m/sn
Uzunluk/En oranı	6.9019	kat / oran
Orta X noktası	0.0469	m
Orta Y noktası	0.0289	m
Hız korreleasyonu	14.8829	m2 / s2
Ortalama basınç	0.0000	N (newton)
Basınç standart sapması	0.0000	N (newton)
Toplam uzunluk	0.6729	m
Ortalama Hız	0.1657	m/sn
Toplam temas süresi	3.8880	sn
Uzunluk/Alan oranı	133.6049	kat / oran
En / Kayma oranı	2.5274	kat / oran
Toplam imza parçası	91.0000	adet

Çizelge-4.1. İmza İnceleme Yazılımından Alınan İmzanın Sayısal Verileri

(12) Biyometrik İmzaların Görüntüleri

Dijital ortamda hazırlanmış bir belgenin imzalanması sonucu belge görselinde imzanın geleneksel görüntüsüne benzer çizgisel görüntüsü oluşmaktadır. Ayrıca imzanın verilerine ulaşmak için kullanılan yazılım, verilerin zaman içerisindeki değişikliklerini farklı grafiklerle görüntüleyebilir (Şekil 4.3.).



Şekil-4.3. İmzanın Sayısal Verilerinin Farklı Şekillerde Görselleştirilmesi

***(a)** Noktadan Noktaya Gösterim, **(b)** Basınca Bağlı Renkli Noktasal Görüntüleme, **(c)** Çizgisel Görüntü, **(d)** Zaman Basınç Grafiği*

Bir dijital olarak yakalanmış imza çözümü, dijital olarak yakalanmış imzanın temel bilgisi olan zaman serisi veri noktalarını yakalayabilmelidir. En önemlileri, yazma işlemi sırasında belirli bir frekansta kaydedilen zaman ve basınç değerlerinin yanı sıra kalem ucunun uzaysal X ve Y koordinatlarıdır. Bu sayısal veriler, farklı formatlarda temsil edilebilecekleri adli analiz yazılımı kullanılarak adli inceleme için erişilebilir olmalıdır.

(13) Meta Veri

Dijital olarak yakalanmış imza çözümü meta verileri; imza yakalama donanımının (sayısallaştırıcı) türü/modeli, yazılım sürümü, işletim sistemi, imzalama zamanı ve kaydedilen verilerin ölçekleme bilgileri gibi bilgileri içermelidir. Farklı dijital olarak yakalanmış imza çözümleriyle yakalanan imzaların birlikte çalışabilirliğini sağlayan temel meta veriler, ölçeklendirilmemiş sayısal değerlerin ortak birimlere dönüştürülmesi için gerekli olan bilgilerdir. Bu ortak veriler aşağıdaki çizelgede belirtildiği gibi olmalıdır.

S.No		Karşılaştırma Kriterlerinin (Parametrelerin)		
		Adı	Birimi	Açıklaması
1	BİRİNCİL DERECE KİRİTERLER (PARAMETRELER)	El kaldırma sayısı	adet	İmza atma esnasında yapılan el kaldırma sayısını göstermektedir. El Kaldırmasız hareketlerde bu sayı 1 dir.
2		İmza toplam süresi	sn	İmzanın toplam atılma suresini göstermektedir. El kaldırmalı imzalarda kalemin havada kaldığı sürede bu sure içerisine dahildir.
3		Toplam temas süresi	sn	Kalemin imza atılma esnasında temas ettiği toplam süre.
4		Kalemin Temas Etmediği Süre	sn	El kaldırmalı hareketlerle atılan imzalarda kalemin el kaldırma hareketlerini yaptığı esnada havada kalma süresini göstermektedir.
5		Ortalama basınç	N (newton)	İmza atılması esnasında kalemin uyguladığı basıncın ortalamasını göstermektedir.
6		Basınç standart sapması	N (newton)	Her noktadaki basınç bilgisinin standart sapmasıdır.
7		Toplam uzunluk	m	İmzanın atılması esnasında kalemin izlediği yolun uzunluğunu göstermektedir. (Kalemin izlediği yola el kaldırma esnasında kalemin havada izlediği yol dahil)
8		Ortalama Hız	m/sn	İmza atılma esnasında kalemin yaptığı hızın genel ortalaması.
9		Ortalama hızlanma değeri	mikrosaniye	İmza atma esnasında kalemin ortalama hızlanma değeri, mikro metre / mikro saniye
10		İmza alanı	mm2	İmzanın kapladığı alanı göstermektedir.
11		İmzanın negatif ve pozitif bölgelerdeki alanı	X positive, Y positive, X negative, Y negative	İmzanın X (yatay) ve Y (dikey) ekseninin pozitif ve negatif bölgelerinde kapladığı alanı göstermektedir.
12		Uzunluk/En oranı	kat / oran	İmzanın X (yatay) eksen üzerindeki uzunluğunun, Y (dikey) eksen üzerindeki enine oranını göstermektedir.
13		Uzunluk/Alan oranı	kat / oran	İmzanın uzunluğunun, imzanın alanına oranını göstermektedir.
14		En/boy oranı	kat / oran	İmzanın Y (dikey) eksen üzerindeki eninin X (yatay) eksen üzerindeki uzunluğuna oranını göstermektedir.
15		En / Kayma oranı	kat / oran	İmzanın bitiş noktasının x eksendeki konumundan, başlangıç noktasının x eksenindeki konumunu çıkartıp kayma miktarına bölünmektedir
16		Yatay eksen(x) genişliği	mikrometre	İmzanın X (Yatay) eksendeki genişliğini göstermektedir.
17		Dikey eksen(y) yüksekliği	mikrometre	İmzanın Y (Dikey) eksendeki yüksekliğini göstermektedir.
18		Ort. Kare Ort. Karekök (RMS)	m/sn	Her noktadaki hız bilgisinin karelerinin ortalamasının karekökü bilgisidir.
19		Ortalama X koordinatında hız	m/sn	Kalemin imza atılması esnasında X (yatay) eksen üzerinde yaptığı hızın ortalamasını göstermektedir.
20		İmzanın başlangıç ve bitimi arasındaki kuş uçuşu mesafe	mikrometre	İmzanın başlıngıç noktası ile bitim nostası arasındaki kuş uçumu mesafeyi göstermektedir.
21	İKNİCİL DERECE KİRİTERLER (PARAMETRELER)	Hız korreleasyonu	m2 / s2	Her noktadaki yatay ve dikey hız bileşenlerinin korelasyonudur. (çarpımlarının toplamıdır)
22		Hız değişim sayısı	adet	İmzanın atılması esnasında kalemin yaptığı hızdaki değişik sayısını göstermektedir.
23		Y hızı standart sapması	m/sn	Y (DİKEY) eksende kalemin yaptığı hızın standart sapmasını göstermektedir.
24		X hızı standart sapması	m/sn	X (YATAY) eksende kalemin yaptığı hızın standart sapmasını göstermektedir.
25		Minimum X hızı	m/sn	İmza atılma esnasında kalemin kalemin X (yatay) eksen üzerinde yaptığı en düşük hız.
26		Minimum Y hızı	kat / oran	İmza atılma esnasında kalemin kalemin Y (dikey) eksen üzerinde yaptığı en düşük hız.
27		Maximum Y hızının ortalamadan uzaklığı	m/sn	Y (Dikey) eksende kalemin yaptığı maksimum hızın, ortalama hız ile arasındaki farkı göstermektedir.
28		Maximum - Minimum Y hızı farkı	m/sn	Y (Dikey) eksende kalemin yaptığı maksimum hız ile minimum hız arasındaki farkı göstermektedir.
29		Maximum X hızının ortalamadan uzaklığı	m/sn	X (YATAY) eksende kalemin yaptığı maksimum hızın, ortalama hız ile arasındaki farkı göstermektedir.
30		Maximum - Minimum X hızı farkı	m/sn	X (YATAY) eksende kalemin yaptığı maksimum hız ile minimum hız arasındaki farkı göstermektedir.

S.No		Karşılaştırma Kriterlerinin (Parametrelerin)		
		Adı	Birimi	Açıklaması
31	İKİNCİL DERECE KİRİTERLER (PARAMETRELER)	Ortalama Y hızı/Max Y hızı oranı	kat / oran	Y (DİKEY) eksende kalemin yaptığı hızın ortalamasının aynı eksendeki en yüksek hıza oranını göstermektedir.
32		Ortalama Pozitif Hız, X koordinatı	m/sn	Kalemin imza atılması esnasında X (yatay) eksen üzerinde pozitif yönde yaptığı hızın ortalamasını göstermektedir.
33		Ortalama Negatif Hız, X koordinatı	m/sn	Kalemin imza atılması esnasında X (yatay) eksen üzerinde negatif yönde yaptığı hızın ortalamasını göstermektedir.
34		Ortalama Pozitif Hız, Y koordinatı	m/sn	Kalemin imza atılması esnasında Y (dikey) eksen üzerinde pozitif yönde yaptığı hızın ortalamasını göstermektedir.
35		Ortalama Negatif Hız, Y koordinatı	m/sn	Kalemin imza atılması esnasında Y (dikey) eksen üzerinde negatif yönde yaptığı hızın ortalamasını göstermektedir.
36		Ortalama merkezkaç ivmelenmesi	m/sn2	Her noktadaki merkezkaç ivmesi değerinin ortalaması.
37		Ortalama tanjant ivmelenmesi	m/sn2	Her noktadaki tanjant ivmesi değerlerinin ortalaması
38		Yatay Span Oranı	kat / oran	İmzanın eninin, imzanın span bilgisine yani en ve boy vektörlerinin diyagonaline oranıdır.
39		Orta X noktası	m	İmzanın X (yatay) eksen üzerindeki orta noktasını göstermektedir.
40		Orta Y noktası	m	İmzanın Y (dikey) eksen üzerindeki orta noktasını göstermektedir.
41		Toplam imza parçası	adet	İmzanın atılması esnasında kalemin yaptığı hareket sayısını göstermektedir.
42		Dik uzun harflerin ort. yüksekliği	m	Yukarıya doğru uzun imza parçalarının (yukarı uzantısı olan h, l gibi harfler) ortlama uzunluğudur.
43		Dik alçak harflerin ort. alçaklığı	m	Aşağıya doğru uzun imza parçalarının (yukarı uzantısı olan g, p gibi harfler) ortlama uzunluğudur.
44		X-Y değişiklik / Kaymalar oranı	kat / oran	X-y eksenlerindeki toplam hareket alanının, toplam hareketliliğe oranını verir. X eksenindeki toplam farkın, Y eksenindeki hareketlilikle çarpılıp, Y eksenindeki toplam farka ve X eksenindeki hareketliliğe bölünmesiyle bulunur.
45		X max - min farkı	m	En yüksek x değeri ile en düşük X değeri arasındaki farktır. İmzanın enini verir.
46		İmza parçası / kalem hamlesi oranı	kat / oran	Kalem hareketi (her kalem kaldırmada yeni bir kalem hareketi başlar) başına düşen imza parçacık sayısıdır.
47		En / kalem hamlesi oranı	kat / oran	Enin kalem hareketi sayısına oranıdır.
48		Ortalama üstündeki X noktası sayısının oranı	kat / oran	X ekseninde, ortalamanın üstünde(sağında) olan noktaların oranını verir.
49		Ortalama üstündeki Y noktası sayısının oranı	kat / oran	Y ekseninde, ortalamanın üstünde (üzerinde) olan noktaların oranını verir.
50		Harf uzunluklarının toplam uzunluğa oranı	kat / oran	Başlangıç ve bitiş noktaları arasındaki mesafenin, toplam uzunluğa oranıdır.
51		Yüksek harf - alçak harf farkı	m	Yüksek harflerin en yüksek noktası ile alçak harflerin en alçak noktası arasındaki farkı verir.
52		Zaman biriminde oluşan ortalama x farkı	m	En yüksek ve en düşük x değerleri arasındaki farkın, toplam süreye oranıdır. Yatay hareketin ne kadar sürede gerçekleştiğini verir.
53		İmza hattının başlangıç noktasına mesafesi	mikrometre	İmzanın atılması sonucu oluşan imza hattının imzanın başlangıcına olan uzaklığını göstermektedir.
54		Yatay (x) eksen üzerinde pozitif yöndeki hareketlerinin mesafesi	mikrometre	Kalemin X (yatay) eksen üzerinde pozitif yönde yaptığı hareketlerin toplam mesafesini göstermektedir.
55		Dikey (y) eksen üzerinde pozitif yöndeki hareketlerinin mesafesi	mikrometre	Kalemin Y (dikey) eksen üzerinde pozitif yönde yaptığı hareketlerin toplam mesafesini göstermektedir.
56		Yatay (x) eksen üzerinde negatif yöndeki hareketlerinin mesafesi	mikrometre	Kalemin X (yatay) eksen üzerinde negatif yönde yaptığı hareketlerin toplam mesafesini göstermektedir.
57		Dikey (y) eksen üzerinde negatif yöndeki hareketlerinin mesafesi	mikrometre	Kalemin Y (dikey) eksen üzerinde nefatif yönde yaptığı hareketlerin toplam mesafesini göstermektedir.
58		X ekseni üzerinde ters yönde yapılan dönüş sayısı	adet	İmza atılması ensasında kalemin X (yatay) eksen üzerinde ters yönde yaptığı dönüş sayısını göstermektedir.
59		Y ekseni üzerinde ters yönde yapılan dönüş sayısı	adet	İmza atılması ensasında kalemin Y (yatay) eksen üzerinde ters yönde yaptığı dönüş sayısını göstermektedir.
60		Yatay eksen(x) genişliği, el kaldırmalar dahil	mikrometre	İmzanın X (yatay) eksen üzerindeki genişliğini el kaldırmalar dahil göstermektedir.

S.No		Karşılaştırma Kriterlerinin (Parametrelerin)		
		Adı	Birimi	Açıklaması
61	İKİNCİL DERECE KİRİTERLER (PARAMETRELER)	Dikey eksen(y) yüksekliği, el kaldırmalar dahil	mikrometre	İmzanın Y (DİKEY) eksen üzerindeki genişliğini el kaldırmalar dahil göstermektedir.
62		El kaldırma hareketlerinin başlangıç ve bitimi arasındaki mesafe	mikrometre	İmza içerisindeki el kaldırma hareketlerinin başlangıçları ile bitimleri arasındaki mesafelereni toplamı.
63		El kaldırma hareketinin imza başlangıcına mesafelerinin ve kalemin izlediği yol mesafeleri toplamı	mm	İmza içerisindeki el kaldırma hareketlerinin imzanın başlangıcına mesafelerinin ve kalemin izlediği yol mesafelerinin toplamını göstermektedir.
64		El kaldırma hareketi başlangıç vuruşlarının imza bitimine mesafeleri ve kalemin izlediği toplam düşey yol mesafeleri toplamı	mm	İmza içerisindeki el kaldırma hareketlerinin başlangıç vuruşlarının imzanın bitimine mesafelerini ve kalemin izlediği düşey yol mesafelerinin toplamını göstermektedir.
65		İmzanın başlangıç hareketi ile el kaldırma hareketleri arasındaki zaman	ms	İmzanın başlangıç hareketi ile ilk el kaldırma hareketi arasındaki zaman farkını gösterir. (El kaldırma hareketi yapılmayan imzalarda bu skor üretilemez)
66		İmzanın el kaldırma hareketleri ile bitim hareketi arasındaki zaman	ms	İmza içerisindeki son el kaldırma hareketinin imzanın bitim hareketi ile arasındaki zaman farkını gösterir. (El kaldırma hareketi yapılmayan imzalarda bu skor üretilemez.
67		Ağırlık merkezinin temel pozisyon değeri	ms	İmzanın ağırlık merkezinin poziyson değerini göstermektedir. (Temel pozisyon değeri bir kalıptır, herhangi noktasal bir pozisyona göre değer üretmez)
68		X ekseni ağırlık merkezi	mikrometre	X ekseni noktalarındaki ağırlık merkezi
69		Y ekseni ağırlık merkezi	mikrometre	Y ekseni noktalarındaki ağırlık merkezi
70		Kalemin aşağı yönde temas ederek oluşturduğu çizgilerin toplam uzunluğu	mikrometre	Kalemin aşağı yönde temas ederek oluşturduğu çizgilerin toplam uzunluğunun mikro metre cinsinden değeri.
71		Max Y değerinin 0 noktasına mesafesi	mikrometre	İmzanın dikey(y) ekseninde maksimum yaptığı değerinin 0 noktasına olan mesafesi.
72		Dikey uçlar arasındaki açı değeri	mikroderece	Soldan ve sağdan bulunan dikey uç noktaların oluşturduğu çizginin yatayla yaptığı açı
73		Dönüş hareketlerinin imzanın üst çizgisine olan açı değeri	mikroderece	Dönüş hareketlerinin imzanın üst çizgisine olan açı değerlerini belirtmektedir. Yukarı yönlü hareketler ile oluşturulan imza ise eksi değer, aşağı yönlü hareket ile oluşturulan imza ise artı değer olarak belirtilmektedir.
74		Dönüş hareketlerinin oluşturduğu açı değerlerinin toplamı	mikroderece	İmza içerisinde dönüş hareketlerinin oluşturduğu açı değerleri toplamını belirtmektedir. Yukarı veya sağa dönüşler yapılarak atılan imzalarda artı değer, aşağı veya sola dönüş yapılarak atılan imzalarda eksi değer olarak belirtilmektedir.
75		X ekseni genişliği / Y ekseni boyu	kat / oran	İmzanın yatay (x) eksenindeki genişliğinin dikey eksendeki(y) boyuna oranı
76		İmza bant aralığı	mm	İmzaların dikey(y) ve yatay (x) eksene göre kapladığı bant aralığı değeri
77		Tanjant histogram değeri (0-45°)	kat / oran	Arctanjant değeri 0-45 derece arasında olan noktaların toplam noktalara oranı
78		Tanjant histogram değeri (45-90°)	kat / oran	Arctanjant değeri 45-90 derece arasında olan noktaların toplam noktalara oranı
79		Tanjant histogram değeri (90-135°)	kat / oran	Arctanjant değeri 135-180 derece arasında olan noktaların toplam noktalara oranı
80		Tanjant histogram değeri (135-180°)	kat / oran	Arctanjant değeri 135-180 derece arasında olan noktaların toplam noktalara oranı
81		Tanjant histogram değeri (180-225°)	kat / oran	Arctanjant değeri 180-225 derece arasında olan noktaların toplam noktalara oranı
82		Tanjant histogram değeri (225-270°)	kat / oran	Arctanjant değeri 225-270derece arasında olan noktaların toplam noktalara oranı
83		Tanjant histogram değeri (270-315°)	kat / oran	Arctanjant değeri 270-315 derece arasında olan noktaların toplam noktalara oranı
84		Tanjant histogram değeri (315-360°)	kat / oran	Arctanjant değeri 315-360 derece arasında olan noktaların toplam noktalara oranı
85		Tanjant fark histogram değeri (0-90°)	kat / oran	İki nokta arasındaki arctanjant farkının 0-90 derece arasında olduğu noktaların toplam noktalara oranı
86		Tanjant fark histogram değeri (90-180°)	kat / oran	İki nokta arasındaki arctanjant farkının 90-180 derece arasında olduğu noktaların toplam noktalara oranı
87		Tanjant fark histogram değeri (180-270°)	kat / oran	İki nokta arasındaki arctanjant farkının 180-270 derece arasında olduğu noktaların toplam noktalara oranı
88		Tanjant fark histogram değeri (270-360°)	kat / oran	İki nokta arasındaki arctanjant farkının 270-360derece arasında olduğu noktaların toplam noktalara oranı

Çizelge-4.2. JKDB Biyometrik İmza Adli İnceleme Yazılımı Karşılaştırma Kriterlerinin (Parametreleri) Açıklama Çizelgesi.

4.2. Biyometrik İmza Çözüm Gereksinimleri

Bir iletide imzalayana, kimliğini doğrulamasını dijital imza şeması sağlar. Bu sayede orijinalliği herkes tarafından doğrulanabilir. İmzalayan, öncelikle asimetrik bir anahtar çifti oluşturur. Bu asimetrik anahtar, bir imzalama anahtarı ve bir doğrulama anahtarından oluşmaktadır. İmzalama anahtarı, imzalayan tarafından gizli tutulur ve mesajlar için imza oluşturulmasına olanak sağlar. Doğrulama anahtarı ise mesajı alacak kişiler için açık hâle getirilir. Böylece imzalama anahtarı kullanılarak o iletinin gerçekten imzalandığının doğrulanması sağlanabilir. Günümüzün kriptografik protokollerinin çoğunda önemli bir bileşen olarak dijital imza şeması karşımıza çıkmaktadır. Örneğin, kimlik doğrulama sağlamak için internet protokolünde kullanılan ortak anahtar altyapısının (PKI) temelini oluştururlar. Ayrıca elektronik postaların kimliğini doğrulamak için de kullanılırlar. Biyometrik imza çözümlemeleri de bu koşulları sağlayabilmelidir.

4.2.1. Örneklem\İşlemci Hızı

Örnekleme hızı esas olarak imza yakalama donanımına bağlıdır. Sonraki yakalama için dijital olarak yakalanmış imza uygulamasının sorunsuz bir şekilde yeniden üretmesine izin verecek kadar yüksek olmalıdır.

4.2.2. Zaman Yakalama

Dijital olarak yakalanmış imza çözümlerinin zamanı güvenilir bir şekilde yakalaması gerekir; buna, ekran kalemi havada olsa bile, bir imza içindeki vuruşlar arasındaki süreyi kaydetme de dâhildir.

4.2.3. Basınç\Kuvvet

Bir imza çözümü, bir dijital olarak yakalanmış imzanın yürütülmesi sırasında uygulanan basınç/kuvvet seviyeleri hakkında bilgi sağlamalıdır. Islak imza incelemesinden en ayırt edici özelliklerinden biri budur. Çünkü geleneksel imza incelemesi esnasında el yazısı ve doküman inceleme uzmanları tarafından kimi zaman kalem baskısı tespiti mümkün olamamaktadır. Bu noktada dijital olarak yakalanmış imza analizi güvenirlik sağlamaktadır.

4.2.4. Hava Hareketleri

Sayısallaştırıcıların aktif alana dokunmayan kalem ucu hareketini yakalaması gerekir. Böylece imza atma süresi tam olarak tespit edilebilir. Bu durum da imzanın taklit edildiği ya da baskı altında atıldığı konusunda el yazısı ve doküman inceleme uzmanlarına fikir verecektir.

4.2.5. Biyometrik İmzanın Bir Belgeye Entegrasyonu

Her dijital olarak yakalanmış imza çözümü, yakalanan imzaları ilgili elektronik belgeye güvenli ve benzersiz bir entegrasyonunu sağlamalıdır. Bunun tespitinin adli bilişim uzmanları tarafından yapılabileceği açıktır. Dolayısıyla el yazısı ve doküman inceleme uzmanları ile adli bilişim uzmanlarının koordineli çalışması gerekmektedir.

4.3. İmzalama Koşulları

İmza sahibine, mümkün olduğunca ıslak imza atma koşullarına yakın imza koşulları sağlanmalıdır.

Sayısallaştırıcı, imza sahibinin imzayı atarken (görsel geri bildirim) minimum gecikmeyle görselleştirmesine izin vermelidir.

İmzalama hareketini bozmamak için dijital olarak yakalanmış imzaları yakalama cihazının fiziksel özellikleri ve ergonomisi ile cihazın yerleşimi dikkate alınmalıdır.

Aktif alan, uzun imzaların atılmasına imkân sağlayacak kadar geniş olmalıdır. Ayrıca, aktif alan ekran çözünürlüğü, kalem ucunun ince hareketlerini hesaba katmalıdır.

Mümkünse, kâğıt üzerine bir mürekkepli kalem ile imza atılıyormuş gibi olmalıdır.

Sayısallaştırıcının aktif alanının parmaklara veya elin diğer kısımlarına değil, yalnızca kalemin ucuna duyarlı olması tercih edilir, aksi takdirde, bir imzanın yakalanmasında istenmeyen veriler ortaya çıkabilir. Aşırı veya şüpheli kesintiler, bir imzanın yürütülmesinin birden çok kez tekrarlanması veya kasıtlı olarak yavaş yürütülmesi gibi doğal olmayan herhangi bir imzalama davranışı engellenmelidir.

Bazı kurumlar, önceden kaydedilmiş referans dijital olarak yakalanmış imzalar aracılığıyla istemcilerin/imza sahiplerinin otomatik kimlik doğrulaması için yazılım

kullanır. Ancak, bir el yazısı ve doküman inceleme uzmanı tarafından yapılan profesyonel adli el yazısı incelemesinin yerini alamaz.

4.4. Dijital Ortamlarda Atılan İmzaların İncelenmesi

Dijital ortamlara atılı imzaların incelenmesinde, delilin fiziki durumunun değişmesi inceleme sürecini de değiştirecektir.

Dijital ortamlara atılı imzaların incelenmesinde, gelen delilin çıktısı alınarak inceleme yapılması; ıslak imza incelemelerinde dikkat edilmesi gereken bazı özelliklerin (kalem baskısı, çizgi kalitesi, mürekkep) tespit edilememesi sebebiyle incelemeleri olumsuz etkileyecektir. Dijital olarak gelen delilin, imzanın sadece son görüntüsünü değil, atılış sürecinde kaydedilmiş verileri de barındırması sebebiyle inceleme esnasında uzmana ek fayda sağlayacaktır.

4.4.1. İmza Görüntüsü Saklanan İmzaların İncelenmesi

Kullanılan akıllı telefonlar veya tabletler ile bir belgeyi taratıp üzerine önceden cihaza kaydedilen bir imza ya da o an atılacak bir imza eklenerek PDF formatında bir belge oluşturulmasına imkân tanımaktadır.

Bu imzalar PDF dosyasının imzalanmadan önceki son hâli ile birlikte belge içine entegre edilir. Zaman damgası, cihaz bilgisi gibi başlık bilgileri bulunsa da biyometrik sayısal verileri barındırmaz. Bu imzaların incelenmesi JKDB-DOK-TL-7.2-02 İmza İnceleme Deney Talimatı'nda belirlenmiş Kopya Belgelerin İncelenmesi ve Değerlendirmesi bölümündeki işlem basamaklarının uygulanmasını gerektirmektedir.

Dijital ortamlara atılı imzalar ayrık veri örneklemesi sistemi ile verileri toplaması sebebiyle çıktı alınmış belge üzerindeki dijital olarak yakalanmış imza görüntüsü, ıslak imzanın çizgi kalitesini sağlayamayacaktır [27]. Çizgi kalitesinin kötü olması ile birlikte imzaların atıldığı cihazların ekran kalitesi belgeye eklenirken büyütme küçültme oranları, alınan çıktı kalitesi incelemeleri olumsuz yönde etkileyecektir.

4.4.2. Biyometrik İmzaların İncelenmesi

Gelen delil bir belge ise; öncelikle veri bütünlüğü, imzanın belgeye eklenme süreci ile ilgili inceleme yapılmalıdır. Bir imzanın şahsın eli ürünü olması dijital bir belgenin orijinal olduğu sonucuna varmak için yeterli değildir. Belgenin orijinalliği, imzanın

belgeye ne zaman eklendiği ve imza eklendikten sonra belge üzerinde başka değişiklik yapılıp yapılmadığı incelenerek karar verilmelidir. Bu incelemeler veri inceleme uzmanlığı alanına girmektedir.

Dijital ortamlara atılı imza ile imzalı bir belgenin inceleme talebine el yazısı ve doküman inceleme ve bilişim laboratuvarlarının ortak çalışmaları sonucu doğru rapor verileceği değerlendirilmiştir. Veri inceleme uzmanınca belge bütünlüğü ve imzanın eklenmesinden sonra herhangi bir değişiklik yapılıp yapılmadığı incelendikten sonra el yazısı ve doküman inceleme uzmanı tarafından belge içerisinde bulunan imzanın incelenmesine geçilmelidir.

5. TARTIŞMA VE SONUÇ

Adli makamlar tarafından dijital olarak yakalanmış imzaların inceleme talepleri kriminal inceleme yapan laboratuvarlara gönderilmektedir. Fakat laboratuvar imkân kabiliyetleri yetersiz olduğundan inceleme talepleri kabul edilmemekteydi. Dolayısıyla oluşan ihtiyaç karşılanmamakta hatta adli süreç sağlıklı yürütülememekteydi. Jandarma kriminal daire başkanlığı bünyesinde bu ihtiyacı karşılamak için bu projeyi başlatmaya kararı verildi ve neticesinde olumlu bir sonuca ulaşıldığı görüldü.

Dijital olarak yakalanmış imzaları incelemeye başlarken el yazısı ve doküman inceleme uzmanları öncelikle imzanın dosya biçiminin şifreli olup olmadığını, biyometrik verilerin bulunup bulunmadığını ve ulaşılabilirliğini kontrol eder. Kullanılan adli yazılımlar imzanın atıldığı cihazın, yazılımın tanıtım bilgilerini ve imzanın atılma zamanını göstermelidir. İnceleme konusu imza ile mukayese konusu imzaların formatları ve benzer yazılım ve cihazlardan alınıp alınmadığı hususları kontrol edilir. Farklı yazılımlar ile veya farklı cihaz ile alınan imzaların sayısal verilerinin aynı şahıs eli ürünü olsa dahi farklı olma ihtimali ve kullanılan adli yazılımın farklı formatları düzenleyerek kendi formatına dönüştürmesinin verilerde değişikliğe sebep olabileceği mutlaka göz önünde bulundurulmalıdır.

07.03.2018 tarih ve 30353 sayılı resmi gazetede yayımlanan Kişisel Verileri Koruma Kurulu kararı ile imzaların davranışsal biyometrik veri olduğuna karar verilmiştir. Bu sebeple imzalar şifreli olarak saklanmalıdır. İnceleme talep eden makamdan gelen veriler şifreleri açılmış veya açma metotları ile birlikte gelmelidir.

5.1. İmzaların Özelliklerinin İncelenmesi

İnceleme konusu ve mukayese imzalar öncelikle kendi içinde özellikleri yönünden değerlendirilmeli ve daha sonra bu özellikleri yönünden birbirleri ile karşılaştırılarak imzanın aidiyeti ile ilgili bir karara varılmalıdır. Dijital ortamlara atılı imzaların özellikleri iki ana başlık altında değerlendirilebilir.

5.1.1. İmzaların Genel Özelliklerinin İncelenmesi

(1) Biçim

İmzanın ad, soyadı, harf karakterleri ya da çizgisel çekilişlerle oluşturulması yönünden değerlendirilmesidir. Karakteristik özellikler tespit edilmeye çalışılır. Harflerin bağlantı noktaları, dikey ve yatay çekilişler arasındaki farklılıklar üzerinde durulur.

(2) Boyut

İmzadaki karakterlerin boyutu, kapladığı alan ya da imza ile yazı satırları arasındaki ilişki gibi özelliklerin değerlendirilmesidir. İmzalarda etkin alanın ve ekrana yansıtılan görsel bilgilerin boyutları imza için ayrılan alanı sınırlandırabilir, bu durum da ıslak imzalarda da olduğu gibi imzalardaki ayırt edici özellikleri etkileyebilir.

Dijital ortamlara atılı imzalar ile geleneksel ıslak imzalar karşılaştırıldıklarında, dijital ortamlara atılı imzaların kaydedilen boyutu ile görsel çıktılarının oranlarının farklı olabileceği göz önünde bulundurulmalı ve imzanın alınma boyutları ile karşılaştırılma yapılmalıdır [27].

(3) Oranlar

İmza karakterlerinin yükseklik ve uzunlukları arasındaki oranların değerlendirilmesidir. İmzanın genel görüntüsü oranların değerlendirilmesinde ilk kanaati oluşturur. İncelemenin devamında imzanın parça parça değerlendirilmesi yapılır.

(4) Boşluklar

İmza karakterleri arasındaki boşlukların değerlendirilmesidir. Boşlukların imza boyutu gibi görüntü çıktılarında farklı oranlarda olabileceği değerlendirilmelidir.

(5) Eğim

İmza hatlarının atılan yüzeyin dikey eksenine açısal durumunun değerlendirilmesidir. Öne veya geriye eğik olması, dik olması ya da değişken eğilimli olması gibi durumlar incelenerek değerlendirilir.

(6) İvme

İmzanın atılması esnasında X ve Y koordinatlarındaki hareketi ve zaman değerleri ile atılması sırasında hız değişimleri hesaplanır.

Hız, ivme ve sarsıntı gibi veri türevleri biyometrik imzanın atılması sırasında doğrudan kaydedilmez, ancak veri noktalarına (X, Y koordinatları ve zaman değerleri) göre hesaplanabilir. Bu özellikler imzanın ortalama değeri, renk ölçeği veya zaman grafikleri kullanan ve farklı algoritmalarla işlenen resimler gibi çeşitli şekillerde analiz edilebilir.

(7) Hız

İmzanın atılması esnasında X ve Y eksenindeki birim zamandaki kalem hızı hesaplanır. İmzanın, imza sahibi tarafından otomatikleşmiş bir el hareketiyle atılmış olması göz önünde bulundurulur.

(8) Akıcılık

İmza atılışı esnasında geçen süre, imza hattında titreme, kalem kaldırma ya da aşırı baskı olup olmadığı değerlendirilir.

Dijital ortamlara atılı imzaların verileri genellikle toplam imza atma süresi, kalemin temas süresi ve el kaldırma süresinin hesaplanmasını ve karşılaştırılmasını sağlayacak verileri bulundurur. Ayrıca, seçilen bölümlerin süresi inceleme için yararlı olabilir.

Zamanla ilgili özellikleri incelerken, bazı imza yazılımlarının kalem kaldırmalarında zaman kaydetmeyi durdurduğu ve bunun da zamana bağlı özelliklerde sonuçları değiştirilebileceği göz önünde bulundurulmalıdır.

(9) Basınç

Bazı imza yazılımları ve imza atma araçları ile alınan imzalar basınç değerlerini içerebilir. Bu değerler geleneksel ıslak imzadaki kalem baskı izlerinin incelenmesi gibi değerlendirilmelidir. Kullanılan yazılımların özelliklerine göre imza, farklı basınçları renkli gösterimle veya basınç zaman grafikleri ile görüntülenebilir, çeşitli şekillerde analiz edilebilir ve karşılaştırılabilir. Basınç verileri incelenirken farklı imza yazılımlarında değişik ölçekler kullanılabileceği ve sayısal verilerdeki farklılıkların yazılımlardan kaynaklanabileceği göz önünde bulundurulmalıdır.

(10) El Kaldırma Hareketi Yörüngesi

Islak imzaların incelenmesinde olduğu gibi, el kaldırma sayısı, bir imza içindeki konumları ve karakterlerin bağlantı yolları analiz ve karşılaştırmanın bir parçası olmalıdır.

El Kaldırma hareketi içerisinde kalemin hareketi imzanın bir parçası gibi kişiye özel farklı bir şekil oluşturabilir. Geleneksel ıslak imzada göremediğimiz bu özellik, imzaların verileri arasında varsa gözlemlenmeli ve karşılaştırılmalıdır.

Bazı imza yazılımları havadaki hareketleri kaydetmez, bu nedenle bu özellikler kullanılamaz.

El kaldırma/havadaki hareketleri kaydeden bazı imza yazılımları, üzerinde hiçbir hareket kaydedilmeyen bir kesme yüksekliğine sahiptir. Kalem bu yüksekliğin üzerine çıktığında kesme noktasını ve dönüş noktasını tek bir düz çizgi ile bağlar. Farklı yazılımlardan alınan veriler ile karşılaştırma yapılırken bu durum göz önünde bulundurulmalıdır.

(11) Zaman

İmzada ilk temasın başladığı andan imzanın bitişine kadar geçen süre değerlendirilir. Bazı yazılımlar farklı süre hesaplamaları sunabilir. Toplam imza atma süresi, havada kalma süresi ve temas süresi iki el kaldırma arasında geçen süre vb. değerler incelenmeli ve değerlendirilmelidir.

Zamanla ilgili özellikleri incelerken el kaldırma hareketi süresindeki olası hatalar dikkate alınmalıdır. Ayrıca bazı yazılımların el kaldırma hareketlerini kaydetmediği ve toplam sürede değişiklik yaratabileceği, el kaldırma hareketini kaydetmesine rağmen kesme noktaları üzerinde zamanı kaydetmeyi durdurabileceği ve bu nedenle yapay bir toplam zaman sunabileceği göz önünde bulundurulmalıdır.

Yazma satırında ve alışılmadık derecede uzun imza atma süreleri ve belirgin sarsıntı izleri kopyalama ihtimalinin değerlendirilmesi gereken imzalardır.

5.1.2. İmzaların Karakteristik Özelliklerinin İncelenmesi

Geleneksel ıslak imzalarda olduğu gibi dijital ortamlara atılı imzalarda da barındırdığı kişisel karakteristik özellikler yönünden değerlendirme yapılmalıdır. Bu özellikler incelenirken imzaların sadece görüntülerinden değil, sayısal verilerinden faydalanmak sonuçları olumlu yönde etkileyecektir. İmzanın karakteristik özellikleri şu şekilde sıralanabilir;

a) Başlangıç hareketi (İmzanın başlangıcındaki harf veya semboller),

b) İmza içerisindeki harf karakterleri (İmza içerisindeki harflerin yapılışı, eğimi, oranı, konumu, önceki veya sonraki harf ile bağlantı durumları),

c) İmza içerisindeki el kaldırmalar (İmzanın atılması esnasındaki kalem kaldırmalar),

d) İmza içerisindeki dönüş hareketleri (Yuvarlak, sarmal, oval dönüşler),

e) İmza içerisindeki buklesel hareketler (Kıvrımların yapılışı, eğimi, oranı, konumu),

f) İmza içerisindeki yatay çekilişler ve dikey çıkışlar (Yapılışı, sayısı, eğimi, oranı, konumu),

g) İmzanın içerisindeki noktalama işareti (Şekli, konumu)

h) İmzanın bitimi (İmzanın bitimindeki figür, harf karakteri, çizgisel çekiliş veya buklesel hareketler)

İmzaları incelerken karakteristik özellikler değerlendirilmeli ve her özelliğin sayısal verileri ayrı ayrı incelenmelidir. İmzanın karakteristik parçalarının yapılış yönü ve görüntüsü kadar atılırken harcanan süre, uygulanan basınç, kalemin temas açıları, hızdaki değişim oranlarının incelenmesi ayırt edici bilgiler verecektir.

5.2. Dijital Ortamlara Atılan İmzaların Hukuki Bakımdan Değerlendirilmesi

Tarih boyunca ortaya çıkan gelişmeler ve yeni uygulamaların kullanımı sonucu yasal düzenleme ihtiyacı ortaya çıkmıştır. Bunun sonucunda kanun koyucu yasama organları yasal düzenlemeler yaparak kuralları, şartları ve kurallara uymanın veya uymamanın

sonuçlarını belirleyerek hukuki düzenlemeler yapmıştır. Yasal mevzuatlar ve hukuki gelişmeler genellikle ihtiyaçlar tespit edildikten sonra yani bir adım geriden gelmektedir. Dijital ortamlara atılı imzalarda da durum benzer olacaktır. Teknolojinin çok hızlı ilerlemesi ve kullanımla ortaya çıkacak olan ihtiyaçlar ve tespitler üzerine hukuki düzenlemelerin yapılacağı değerlendirilmektedir.

5070 sayılı Elektronik İmza Kanunu'nun yürürlüğe girmesi ile güvenli elektronik imza ile ilgili düzenlemeler yapılmış olsa da dijital ortamlara atılı imzalar ile ilgili herhangi bir düzenleme yapılmamıştır. UNCITRAL model kanunu ve eIDAS Tüzüğü benzer şekilde sadece nitelikli (5070 sayılı kanunda güvenli elektronik imza olarak belirtilmiş) elektronik imzayı düzenlenmiş olsa da hem UNCITRAL Model Kanunu'nda (md. 6) hem de eIDAS Tüzüğü'nde (md. 25) düzenlenmemiş olan diğer imza türlerinin delil niteliğini sağlayabileceği ve düzenlenmemiş olması geçersiz sayılacağı anlamına gelmediği belirtilmiştir [8][10]. 5070 sayılı Kanun'da ise bu şekilde bir madde yoktur.

Yürürlükteki kanunlarda dijital ortamlara atılı imzalarla ilgili bir hüküm bulunmasa da bu imzaların delil niteliği taşıyıp taşımadığı konusu dosyanın ceza hukuku ya da medeni hukuka konu olmasına göre değişebileceği değerlendirilmektedir.

Ceza yargılamalarında "delil serbestisi" ilkesi bulunmaktadır. Polisin Adli Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmelik'te delil; "meydana gelen bir suçun aydınlatılması ve suç sanıklarının tespitine yarayan her türlü ispat vasıtalarını ifade etmektedir" şeklinde tanımlanmıştır. Adil yargılamayı sağlayabilmek amacıyla, uyuşmazlığa konu olan olayı temsil eden ve hukuka uygun yollardan elde edilen, güvenilir, akla, mantığa, hayatın olağan akışına uygun, erişilebilir ve mevcut olan bulgular delil niteliği taşır. Bu kapsamda bakıldığında; her ne kadar hakkında bir düzenleme yapılmamış olsa da dijital ortamlara atılı imzalar ile imzalanmış belgeler delil olarak toplanıp Jandarma Kriminal Laboratuvarlarına incelenmek üzere gönderilmektedir.

Hukuk Muhakemeleri Kanunu (HMK) ile "uyuşmazlık konusu vakaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki verilerin ve bunlara benzer bilgi taşıyıcılarının belge olduğu" hükme bağlanmıştır [28]. Elektronik ortamlarda verilerin belge olarak kabul

edilmesi ve bu belgelerin delil olarak mahkemelere sunulabileceği düşünüldüğünde, belgelerin bazılarında dijital ortamlara atılı imzalar da bulunacaktır.

HMK'da bir belgede yer alan imzanın "ıslak imza" olması gerektiği belirtilmemiş, sadece imza veya güvenli elektronik imzadan bahsedilmiştir. Md. 208/f.1, kişinin bir belgede yer alan imzası veya yazısından bahsetmekte, ancak bu imzanın ıslak imza mı dijital ortama atılı bir imza mı olması gerektiği noktasında bir tespit yapmamaktadır. Fakat güvenli elektronik imzaya özellikle yer verilmesine rağmen diğer elektronik imza türleri ile ilgili bir atıfta bulunulmaması dijital ortamlara atılı imzaların kanunca kabul edilen imza türü olamayacağını göstermektedir (HMK Md. 205) [28].

6098 sayılı Türk Borçlar Kanunu'nda (Md. 14) "Yazılı şekilde yapılması öngörülen sözleşmelerde borç altına girenlerin imzalarının bulunması zorunludur. 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" ve (Md.15) "imzanın, borç altına girenin el yazısıyla atılması zorunludur. Güvenli elektronik imza, el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğurur…" imzanın şekil şartını belirtmiş ve sadece 5070 sayılı kanunda belirtilen güvenli elektronik imzayı ıslak imzaya eşdeğer bulmuştur [29].

6102 sayılı Türk Ticaret Kanunu'nda imzaların özellikleri ve elektronik imzanın kullanılıp kullanılamayacağı alanlar ayrıntılı bir şekilde belirlenmiştir. "(Md. 756) (1) Poliçe üzerindeki beyanların el ile imza edilmesi gerekir. (2) El ile atılan imza yerine, mekanik herhangi bir araç veya elle yapılan veya onaylanmış bir işaret veya resmî bir şahadetname kullanılamaz. (Md. 1526) (1) Poliçe, bono, çek, makbuz senedi, varant ve kambiyo senetlerine benzeyen senetler güvenli elektronik imza ile düzenlenemez. Bu senetlere ilişkin kabul, aval ve ciro gibi senet üzerinde gerçekleştirilen işlemler güvenli elektronik imza ile yapılamaz. (2) Konşimentonun, taşıma senedinin ve sigorta poliçesinin imzası elle, faksimile baskı, zımba, ıstampa, sembol şeklinde mekanik veya elektronik herhangi bir araçla da atılabilir. (3) Ticaret şirketleri ile gerçek ve tüzel kişi diğer tacirlere ilişkin olarak, bu kanunun zorunlu tuttuğu bütün işlemler elektronik ortamda güvenli elektronik imza ile de yapılabilir. (4) Şirket adına imza yetkisini haiz kişiler şirket namına kendi adlarına üretilen güvenli elektronik imzayla imza atabilirler [30]."

Türk Ticaret Kanunu'nun ilgili maddelerinde güvenli elektronik imzanın hangi şartlarda ve nasıl kullanılacağının ayrıntılı bir şekilde bilgisi verilmesine rağmen dijital ortamlara atılı imzalardan hiç bahsedilmemiş ve dijital ortamlarda atılı imzalar tamamen kapsam dışında bırakılmıştır.

Kanunları incelediğimizde medeni usul hukukunda imzanın daha ayrıntılı anlatıldığı, taşıması gereken özellikler ve geçerli olabilecek belge türlerinin belirlendiği görülmektedir. Bu kapsamda 5070 sayılı Kanun'da açıkça belirlenmiş şartları sağlayan güvenli elektronik imzanın geçerliliği tanınmıştır. Diğer imza türleri ile ilgili herhangi bir açıklama yapılmamıştır. Yeni bir yasal düzenleme yapılmadan dijital ortamlara atılı imzaların medeni usul hukukunda geçerli olup olmayacağı gerçekleşen durumlar ve yargı içtihatları ile netleşecektir.

Dijital ortamlara atılı imzaların geçerliliği ile ilgili bir yasal düzenleme olmasa da hukukçular arasında geçerli olduğuna dair görüşler de mevcuttur. Türk Borçlar Kanunu Md.15'te "imzanın borç altına girenin elle atılmasını zorunlu tutması ve imzanın mürekkepli kalemle, dijital kalemle ya da parmakla atılmasının, atılan yüzeyin kâğıt ya da tablet ve akıllı telefon ekranı olmasının kanun açısından fark etmeyeceği, esas şart olan elle atılmayı sağlayan imzaların geçerli olacağı görüşü savunulmaktadır [29].

28.10.2017 tarihinde 30224 sayılı resmî gazetede yayımlanan Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği'nde BTK tarafından belirlenecek usuller ile elektronik ortamda abonelik sözleşmesi akdedilebileceği hükme bağlanmış olup, GSM operatörleri başta olmak üzere birçok farklı sektörde elektronik ortamda sözleşmeler bu yönetmeliğe dayanılarak dijital ortamlara atılı imza ile onaylanmaktadır. Bu yönetmelikte sadece sözleşmenin yapılabileceği hükme bağlanmış olsa da tarafların sözleşmeyi nasıl onaylayacağı kısmı açık bırakılmıştır [31].

6698 Sayılı Kişisel Verilerin Korunması Kanunu incelendiğinde; bu kanun kapsamında inceleme ve değerlendirme yapan Kişisel Verilerin Korunması Kurulu 27.08.2020 tarihli ve 2020/649 sayılı kararında; biyometrik verileri genel itibariyle ömür boyu değişmeyen, müdahaleye gerek kalmadan kolayca elde edilen özellikler olarak tanımlamış ve fizyolojik ve davranışsal biyometrik veriler olarak sınıflandırmıştır. Dijital ortamlara atılı imzaları, imzanın oluşturulma esnasındaki dinamik verileri kaydetmesi sebebiyle davranışsal biyometrik veriler olduğunu belirtmiştir. Bu karar ile dijital ortamlara atılı

imzaların kişisel veri olarak kabul edilmesi gerektiği ve yapılacak işlemlerde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun dikkate alınması gerektiği vurgulanmıştır [32]. Kişisel Verilerin Korunması Kanunu'nda; verilerin hangi usul ve esaslarla işlenebileceği (md.4), işlenme şartları belirtilmiştir (Md. 5). Kişisel verilerden "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir." (Md.6/(1)) tanımlaması ile biyometrik özellikler barındıran dijital ortamlara atılı imzaların özel nitelikli kişisel veri olduğu anlaşılmaktadır. Kanun gereğince kişinin açık rızası olmaksızın kanunlarda öngörülen hâllerde işlenebilir (Md.6/(3)). Kanunun 28. maddesinde bazı hâller istisna olarak kabul edilmiş ve bu hâllerde kanunun uygulanmayacağı belirtilmiştir. "Soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi (Md.28/(1)/d), kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması (Md.28/(2)/a, kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması (Md.28/(2)/d) hâlleri istisna kapsamındadır [33]."

Jandarma kriminal laboratuvarları olarak inceleme talebi ile gelen imzaların gerekli kanuni şartları oluşturduğu, yargılama işlemlerinin bir parçası olduğu düşünülerek yapılacak bir incelemede bu kanun kapsamındaki istisnalardan olacağı değerlendirilmektedir. Yapılacak işlemlerde kanundan muaf olunsa dahi kanunun temel ilkelerine uygun ve orantılı işlemler tesis etmek gerekliliği Jandarma Kriminal Laboratuvarlarına veri güvenliği konusunda yükümlülükler getirmektedir. Veri güvenliğine ilişkin yükümlülükler kanunun 12. maddesinde aşağıdaki şekilde açıklanmıştır:

"Madde 12- (1) Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. (2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci

fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur. (3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. (4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder. (5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir [33]."

Kanun'da belirtilen "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır" (Md.6/(4)) maddesi gereğince Kişisel Verileri Koruma Kurulu 7 Mart 2018 tarihli ve 30353 Sayılı Resmî Gazete'de yayımlanan 31.01.2018 tarihli ve 2018/10 sayılı kararında "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" belirlemiştir. Bu önlemler;

I. Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kurallı, yönetilebilir ve sürdürebilir bir politika ve prosedür hazırlanmalıdır.

II. Erişim sağlayan çalışanlara güncel eğitim verilmesi ve bu çalışanların hukuken hesap verebilir hâlde tutulması gereklidir.

III. Verinin yüksek kimlik doğrulaması önlemlerinin ve kriptografik altyapının bulunduğu sanal ortamlarda depolandığına ve erişimin yalnızca yetkilendirilen personel tarafından yapıldığına dikkat edilmelidir.

IV. Verinin transferinin şifrelenmiş, güvenli ve yalnızca yetkililerce izlenebilir bir hâlde gerçekleşmesi gerekmektedir.

V. Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır [33].

Yürürlükte olan mevzuatlarda yapılan inceleme sonucu dijital ortamlara atılı imzaların kullanılmasını engelleyici bir husus olmadığı, medeni usul açısından imzanın borç yükümlülüğü getirip getirmeyeceğinin düzenlenmemiş olduğu, fakat ceza hukuku alanında delil niteliği taşıyacağı değerlendirilmiştir.

Teknoloji kullanımının maliyetleri düşürmesi ve arşiv, belge yönetimini kolaylaştırması dijital ortamlara atılı imzaların ve dijital çözümlerin daha fazla alanda kullanılmasını sağlayacaktır. Bu alandaki düzenleme ihtiyaçlarının da yeni çıkarılacak mevzuatlar ile giderileceği düşünülmektedir.

Jandarma kriminal laboratuvarlarının adli sürecin bir parçası olduğu, soruşturma ya da kovuşturma aşamasında delillerin laboratuvara gönderildiği düşünüldüğünde, uygun veri güvenlik süreçlerinin oluşturulmuş şekilde dijital ortamlara atılı imzaların incelenmesinin önünde kanuni bir engel olmadığı görülmüştür.

5.3. Değerlendirme

Mukayese konusu ve inceleme konusu imzalar kendi içerisinde incelenir. Yazılımda ortaya konulan tüm verileri karşılaştırarak anlamlı bir sonuç ortaya koymak zor olacaktır. Bu sebeple kendi içerisinde tutarlı olduğu görülen verilerin değerlendirmeye alınması gerekir. İmzanın genel ve karakteristik özelliklerini inceledikten sonra tespit edilen uyum ve uygunsuzluklar not alınarak karar verilir.

Hangi özelliklerin incelenebileceği ile ilgili yeterli çalışma olmaması ve imzayı atan kişinin alışkanlıklarına göre tutarlı olan verilerin değişebileceği değerlendirilerek özelliklere bir önem ve öncelik sırası verilmekten kaçınılmalıdır.

Özellikle farklı cihazlar ve yazılımlar ile alınan imzaların sayısal verilerinde; cihazların farklı hassasiyette olmaları ve yazılımların farklı değer ölçekleri kullanması gibi sebeplerle farklılıklar oluşabilecektir. Aynı zamanda cihazların çok küçük zaman aralıklarında küçük değer farklarını yakalayabilecekleri değerlendirildiğinde; imzaların sayısal verileri incelenirken verilerin aynı ya da benzer değerler olup olmadığı, imza içerisindeki değişimlerin karşılaştırılması kanaate ulaşmada uzmanlara yardımcı olabilecektir. Bu değişimlerin görülebilmesi için değerleri görselleştiren grafiklerden faydalanılabilir.

Karışık ve yüksek zorluk derecesindeki imzaların parçalara ayrılarak incelenmesi belirli bir özelliği ya da hareketi daha ayrıntılı inceleme imkânı sunabilir. Bu inceleme şeklinin daha fazla zaman alması, aynı şahıs eli ürünü imzalardaki doğal saplamaların uygunsuzluk olarak değerlendirilmesi gibi tehlikeleri olduğu göz ardı edilmemelidir [34].

İmza inceleme yazılımları genellikle her veri için ve genel imza için bir skor üretebilmektedir. Fakat kullanılan yazılımların algoritmaları ve skorları nasıl ürettiği ile ilgili yeterli çalışma olmaması sebebiyle bu skorlar ile kanaate gidilmemesi, inceleme yapan uzmana yardımcı olabilecek bir veri olarak kabul edilmesi ve imzayı inceleyen uzmanın görsel ve verisel incelemeyi birleştirerek kesin kanaatini oluşturması gereklidir.

Yapılan alanyazın taraması çalışmalarında bazı sayısal verilerin daha anlamlı olabileceği üzerine tespitler olduğu görülmüştür. Fakat çalışmaların anlamlı istatistiksel sonuçlar verebilmesi için örneklemlerin kısıtlı tutulan basit imzalarda çalışılmasının tercih edildiği görülmüştür. Linden'in yaptığı çalışmada görsel grafiklerin ufak sapmalara rağmen üst üste oturduğu ve atılan imzaların tekrar edilebilirliğinin yüksek olduğunu tespit edilmiştir [26].

Heckeroth ve Boywitt yaptıkları çalışmada biyometrik imzaların geleneksel ıslak imzalara karşı bir avantajının olmadığını fakat imzalama sürecine ait videoların bulunması uzmanların daha kolay kanaat bildirmelerini sağladığını tespit etmişlerdir. Ayrıca ıslak imza incelemeleri ile ilgili çok fazla çalışma olmasının ve uzmanların bu konuda tecrübeli olmalarının, biyometrik imza incelemelerinde ise tecrübesiz olmalarının ve dinamik verileri değerlendirme konusunda henüz yeterli çalışma olmamasının avantaj sağlanamamasına sebep olabileceğine değinmişlerdir [24].

Geleneksel ıslak imza incelemelerinde basit tersim imza türleri ile, yani kişiyle, ilişkilendirebilecek karakteristik özellik tespit edilemeyen, kolaylıkla taklit edilebilecek imzalar ile karşılaşılmaktadır. Dolayısıyla müspet ya da menfi bir kanaat verilememektedir. Biyometrik imzalarda ise barındırdıkları dinamik veriler, imzanın atılış hızı, kalem basıncı, açısı gibi özellikler değerlendirilerek basit tersim imza türlerinde bile aidiyetinin tespit edilebilme ihtimali vardır [34].

Tablet ve diğer cihazların yüzeylerinin kâğıda göre daha pürüzsüz olması kullanıcıların hızını ve kalem basıncını etkilediği, kâğıda göre yazarların hızlı yazarken harf

karakterlerinin ve buklesel hareketlerin boyutlarının büyüdüğü ve genişlediği tespit edilmiştir [34].

6. YORUM

Biyometrik imzalar, dinamik imzalar, elektronik olarak yakalanan imzalar veya *çevrimiçi imzalar* olarak da adlandırılan dijital olarak yakalanan imzalar son zamanlarda elektronik belgeleri yetkilendirmenin daha çok tercih edilen bir yöntemi olmuştur. Bu arada bu imza türü için ülkemizde dijital imza tabirinin yaygınlaştığını görmekteyiz. Kanaatimizce dijital biyometrik imza tabiri daha doğru olacaktır. Çünkü el yazısı ve doküman inceleme uzmanları tarafından analiz edilebilecek imzanın dijital olması yanında mutlaka biyometrik verileri barındırması gerekmektedir. Ayrıca bu tür imzaların yok sayılması artık mümkün değildir. Herhangi bir kimlik doğrulamada yaygın olan parola kullanımını değiştirme ihtiyacından doğmuştur [35]. Sonucunda da insanların bu ihtiyacını karşılama noktasında başarılı olmuştur ve günlük hayatın bir parçası hâline gelmiştir.

Islak imzalarda olduğu gibi, dijital olarak yakalanan imzaların yazarlığı yasal ihtilafların konusu olabilmektedir. Dijital verilerden oluşmasına rağmen, yazarlıklarının değerlendirilmesi, konuyla ilgili ek bilgi ve eğitim edinmeleri tavsiye edilen adli el yazısı ve doküman inceleme uzmanlarının yetkinliği dâhilindedir.

Her örneklem, kalem ucunun uzamsal koordinatlarını, yakalama zamanını ve uygulanan kuvveti belirten sayısal veriler içerir. Bazı yakalama çözümlerinin daha da fazla değişken kullandığı, bazılarının ise yalnızca imzanın görüntüsünü koruduğu ve sayısal verileri attığı bilinmektedir. Dijital olarak yakalanan imzalar, bir sayısallaştırma aygıtı ve imza verilerini kaydeden ve bunları elektronik bir belgeye, tipik olarak bir PDF dosyasına yerleştiren bir kontrol yazılımından oluşan bir yakalama çözümü tarafından üretilir. Piyasada çok sayıda donanım ve yazılım ürünü mevcuttur ve genellikle birleştirilebilir, bu da çeşitli farklı yakalama çözümleriyle sonuçlanır. Bu nedenle, adli el yazısı uzmanlarının, farklı sayısallaştırıcılar ve yazılımlar kullanılarak yakalanan tartışmalı ve bilinen örnekleri karşılaştırma görevi ile karşı karşıya kalacağı tahmin edilebilir.

Dijital olarak yakalanan imzalarla yetkilendirilen elektronik belgelerin artan popülaritesi ile birlikte, kriminal inceleme uzmanlarının önüne bu tür kanıtlar içeren dosyalar gelmeye başladı. Birçok farklı satıcı, değişen özelliklere sahip imza atma pedleri sunmaktadır. Bu nedenle, tamamen veya kısmen farklı donanım ve yazılım

kombinasyonlarıyla yakalanan imza örneklerini karşılaştırmak için adli el yazısı uzmanlarının çağrılması gerekmektedir. Çeşitli ekipmanlar tarafından üretilen sayısal el yazısı verileri, yalnızca yakalanan bilgilerin türü ve kalitesi açısından değil, aynı zamanda yapısı ve kodlaması açısından da farklılık gösterebileceğinden, bu tür durumlar zor olabilir. Bir çalışmada, kodlama özelliklerini incelemek için 26 farklı donanım ve yazılım kombinasyonu ile el yazısının sayısal verileri – yani uzamsal koordinatlar, kuvvet ve zaman değerleri – elde edilmiştir [24]. Örneklerin analizi, sayısal verilerin ölçeklendirilmesinin yalnızca donanıma değil, aynı zamanda yazılıma da bağlı olduğunu ortaya çıkardı. Bu nedenle, verilerin birlikte çalışabilirliğini geliştirmek için ISO/IEC 19794–7 standardına uygunlukları önerilmektedir. Bu standart, kullanılan imzalama çözümünün ölçekleme oranlarıyla sayısal imza verilerinin belirtilmesinin önemini vurgulamaktadır.

Sonuçlar, aynı yakalama donanımı ve yazılım kombinasyonunun kullanılmasının veri ön işleme ve normalleştirmeye ihtiyaç duymadan imzaların güvenilir bir şekilde karşılaştırılmasını sağlayan uzamsal koordinatlar, zaman ve kuvvet için ölçeklendirme bilgisi sağladığını göstermektedir. Ancak, farklı donanım ve yazılım kombinasyonları kullanıldığında, verilerin ölçeklenmesinde ve kodlanmasında önemli farklılıklar meydana gelmektedir. En önemlisi, ölçekleme bilgisinin sadece donanıma değil, yazılıma da bağlı olduğu gözlemlenmiştir. Bu nedenle, farklı çözümlerle elde edilen imzalar karşılaştırırken, el yazısı ve doküman inceleme uzmanları ölçekleme bilgilerini dikkate alarak sayısal verileri işlemeye başlamalı ve ölçeklenmiş imza verilerinin analizini destekleyen bir yazılım kullanmalıdır. Yakalanan imza verilerinde yoksa, ölçeklendirme bilgileri imza yakalama çözümü yöneticisi tarafından sağlanabilmeli veya deneysel olarak elde edilebilmelidir. Ölçekleme bilgileri, yakalanan verileri milimetreye dönüştürerek imza boyutunu normalleştirmeye olanak tanır. Ayrıca seviyeleri yüzdeye çevirerek kuvvet bilgisini ölçeklendirmeyi ve zaman bilgisini saniyeye dönüştürmeyi sağlar. Ek gözlemler, imza verileri ölçekleme oranları kullanılarak normalleştirildiğinde bile, çeşitli çözümlerle yakalanan verilerin, çeşitli kuvvet yakalama teknolojilerinden, kalemi kaldırmalarına, zaman veya hava hareketlerini yakalamaya yönelik farklı yaklaşımlardan kaynaklanan farklılıklar gösterebileceğini gösterdi. Verilerin hatalı yorumlanmasından kaçınmak için bunun el yazısı ve doküman inceleme uzmanları tarafından not edilmesi gerekir.

Normal şartlarda, el yazısı ve doküman inceleme uzmanları genellikle imza sahibinin duruşu veya sayısallaştırıcının konumu gibi imzalama koşulları hakkında bilgi edinmeye çalışır. Bu çalışma, el yazısı ve doküman inceleme uzmanlarının incelenen imzaları elde etmek için kullanılan imza yakalama çözümlerinin özellikleri ve parametreleri hakkında bilgi araması gerekliliğini vurgulamaktadır. Bu özellikler ve parametreler geleneksel imza incelemesinde değerlendirilenlerden farklı olmalıdır.

Geleneksel imza inceleme deney metodunda temel anlamda dikkat edilen kriterler şunlardır:

Style / legibility - Biçim

Size - Boyut

Vertical proportions – Dikey Oranlar

Spacing (horizontal) – Yatay Boşluklar

Slant - Eğim

Alignment - Hizalama

Number of pen lifts – Kalem Kaldırma Sayısı

Pressure level – Kalem Baskısı

Pressure variation – Çizgi Kalitesi

Fluency (speed) – İşleklik

Character / element construction – Harflerin Yapılışı

Character / element shape – Harflerin Şekli

Dijital olarak yakalanmış imzaların karşılaştırılmasında da uluslararası standartlara göre yazılımların sağlaması gereken kriterler şu şekildedir:

Pressure profiles - Basınç profilleri

Average pressure - Ortalama basınç

Speed profiles - Hız profilleri

Average speed - Ortalama hız

Stroke length - İmza uzunluğu

Time in contact - Temas süresi

Time in air - Havadaki zaman

Total time - Toplam zaman

Dijital ortamlara atılı imzaların her alanda olmasa da bazı alanlarda kullanılmasına engel bir durum olmaması, kullanılmaya başlanan bu imzanın anlaşmazlıklara ve hukuki sürece konu olması ve imzanın aidiyeti ile ilgili bir bilirkişi raporuna ihtiyaç duyulmasıyla laboratuvarlara inceleme talepleri gelmektedir.

İnceleme taleplerine karşılık verebilmek için gerekli kanuni ve teknolojik altyapının kurulması ve uzman personelin bilgi seviyesinin arttırılması doğru raporlar hazırlanabilmesi için önem arz etmektedir.

Dijital ortamlara atılı imzaların Jandarma Kriminal Laboratuvarlarında incelenebilmesi için yapılması gereken hazırlıkları iki başlık altında incelenebilir:

6.1. Altyapı Hazırlıkları

Dijital ortamlara atılı imzaların incelenmesi için farklı donanımsal cihazlara ihtiyaç yoktur. Laboratuvara inceleme talebiyle gönderilen dijital delilin bilgi ve özelliklerine ulaşabilecek imza verilerini birbirleri ile karşılaştırma yapılabilecek adli imza inceleme yazılımına ihtiyaç vardır. Sağlıklı bir inceleme yapabilmek için temin edilecek yazılımların;

a) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak tutulması,

b) Verilerin bulunduğu ortamlara ait güvenlik güncellemeleri yapılabilmesi,

c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanabilmesi,

d) İçerisinde tutulan verilere yetkisiz personelin ulaşmasını engelleyici şifreleme yöntemleri kullanması,

e) İmzanın başlık bilgilerine ulaşarak imzanın alındığı tarih, saat, hangi cihaz ve yazılımla alındığına dair bilgileri çıkarması,

f) Aynı anda en az iki imzanın görüntüsünü, özelliklerini ve grafiklerini açabilmesi,

g) İmzaların atılışının adım adım izleneceği videoları gösterebilmesi ve videoyu gerçek zamanlı ya da daha hızlı/daha yavaş oynatabilmesi,

h) İmzaların basınç verilerini renkli grafiklerde ve zaman basınç grafiklerinde gösterebilmesi,

i) İncelenen imzaları farklı pencerede açma, büyütme açısal döndürme yapabilmesi,

j) İmzaları parçalara ayırarak belirli kısımları inceleyip karşılaştırabilmesi,

k) Yazılımın verdiği değerler haricinde imza üzerinde düzlemsel ve açısal ölçümler yapılabilmesi,

l) ISO/IEC 19794-7, ISO/IEC 19794-11 standartlarına uygun olan, farklı cihaz ve yazılımdan alınan imzaların sayısal verilerini açabilmesi, dökümü ve karşılaştırmasını yapabilmesi,

m) PDF belgelere eklenmiş dijital ortamlara atılı imzaları, şifreleri mevcut ise çıkarabilmesi ve verileri okuyabilmesi gereklidir.

6.2. Eğitim Hazırlıkları

Personelin uzmanlık eğitimi içeriğine dijital ortamlara atılı imzalar imza inceleme yazılımları ve karşılaştırmaları ile ilgili eğitim eklenmelidir. İnceleme esnasında yapılacak karşılaştırmaların geleneksel ıslak imzada dikkat edilen hususlara benzeyen

unsurların olması planlanan eğitimin imza inceleme eğitiminden sonra yapılmasının daha verimli olacağı değerlendirilmektedir.

El Yazısı ve Doküman İnceleme uzmanlık eğitimi;

a) Dijital delillerin teslim alınması, saklanması,

b) Dijital ortamlara atılı imzalar ve teknolojik terminolojiye hâkimiyet,

c) Dijital ortamlara atılı imzaları tanımlayabilme,

d) Dijital ortamlara atılı imzaları adli incelemeleriyle ilgili kısıtlamaları bilme,

e) Dijital ortamlara atılı imzaları atmak, ayıklamak ve analiz etmek için tasarlanmış yazılımların kullanımı,

f) Dijital ortamlara atılı imzaların sayısal verilerini işleme,

g) Dijital ortamlara atılı imzaların grafiklerinin çizilmesi,

h) Genel ve özel karakteristik özelliklerin değerlendirilmesi,

i) Değerlendirilen özelliklerin yorumlanarak raporlanması, konularını içermelidir [27].

İnceleme çalışmalarının başlangıcında uzman ve uzman yardımcılarının sayısal verilerin analizi konusunda pratik eksiklikleri, ıslak imza incelemelerinde dikkate alınan bazı özelliklerin (çizgi kalitesi vb.) net olmaması sebebiyle incelemelerin daha uzun zaman alacağı ve sınırlı kalabileceği değerlendirilmektedir.

Adli imza inceleme yazılımının tedariki sonrası laboratuvar içerisinde yapılacak testler ve eğitimler ile uzman ve uzman yardımcılarının eksiklerini hızla giderebileceği düşünülmektedir.

Doğrulanabilir ve tekrarlanabilir sonuçlar ortaya çıkarabilmek maksadıyla karşılaşılabilecek inceleme konusu imzalar ortaya konularak farklı projelerde benzer durumların simüle edilerek çalışılması uzmanlık eğitimlerinin ve personelin gelişimini hızlandıracaktır.

Kalite Yönetimi kapsamında, özel nitelikli kişisel verilerin güvenliğine yönelik verilerin kimler tarafından erişilebileceğini, raporlamadan sonra ne kadar süre tutulacağını, hangi şartlarda imha edileceğini içeren kötüye kullanılmasını engelleyici, sistemli, kuralları net, yönetilebilir ve sürdürülebilir bir prosedürün belirlenmesi gerekmektedir.

Jandarma Kriminal Daire Başkanlığı olarak gerekli yazılım tedariki ve eğitim hazırlıklarını tamamladıktan sonra kalite prosedürlerinin tamamlanması ve inceleme deney metodunun oluşturulması sonrasında inceleme taleplerine cevap verilebileceği değerlendirilmektedir.

Sonuç olarak dijital olarak yakalanmış imzalar ile şahıs/şahısların (mağdur/şüpheli/müşteki) mukayese imzalarının inceleme ve karşılaştırmasının yapılabilmesi için aşağıdaki hususların sağlanması gerekmektedir.

(1) Öncelikle; olay/soruşturma/davaya konu olmuş inceleme konusu elektronik belge (abonelik sözleşmesi, cihaz taahhüt belgesi, araç kiralama belgesi vb.) üzerinde atılı bulunan dijital (biyometrik) imzaya itiraz eden şahıs ve varsa diğer şahısların dijital (biyometrik) mukayese imzalarının alınması gerekmektedir.

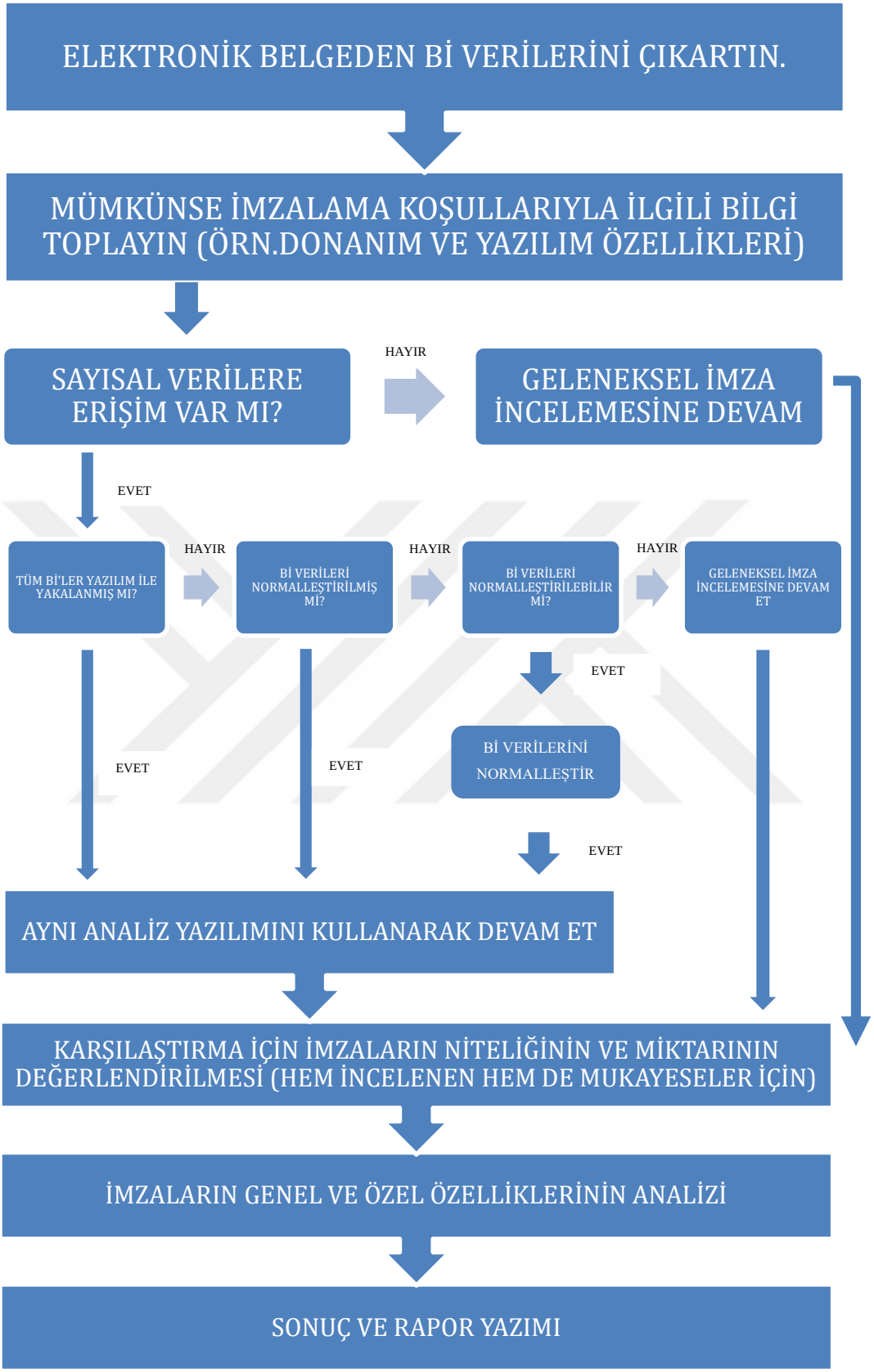
(2) Biyometrik İmza Adli İnceleme Yazılımına yükleyerek inceleme ve karşılaştırma yapmak için; inceleme konusu elektronik belge üzerinde atılı bulunan dijital (biyometrik) imzanın, şahıs/şahısların mukayese olarak attıkları dijital (biyometrik) imzaların ve varsa şahıs/şahısların farklı elektronik belgeler üzerinde atılı bulunan dijital (biyometrik) mukayese imzalarının sayısal verilerini içeren "ISO 19794-7 2014" standardındaki *.sig uzantılı dosyaları talep edilmelidir.

(3) Ayrıca imzalar üzerinde geleneksel imza incelemesi yapmak için de inceleme konusu elektronik belgenin ve şahısların atmış oldukları dijital (biyometrik) mukayese imzaların yüksek çözünürlükte *.pdf formatındaki dosyalarının ŞİFRESİZ bir şekilde, inceleme konusu belge üzerindeki imzalar ve mukayese imzalar ayrı dosyalarda olacak şekilde CD/DVD içerisinde söz konusu kurum/kuruluştan talep edilmesi gerekmektedir

(4) Söz konusu şahısların özellikle üzerinde imza incelemesi yapılacak belgenin düzenlenme tarihine yakın ve önceki tarihli bol miktarda samimi imza (kimlik

kartı veya ehliyet talep belgesi, adres beyan formu, resmi evrak, noter belgesi, tapu senedi, sandık seçmen listesi, banka sözleşmeleri, askerlik belgeleri, ifade tutanakları, dilekçe vb.) mukayeseleri temin edilmelidir. (Şahısların yabancı uyruklu olması ve samimi imza mukayesenin bulunamaması durumunda en az iki defa farklı tarihlerde huzurda mukayese alınmalıdır.)

Tüm bunlar değerlendirildiğinde dijital biyometrik imzaların incelemesi şematik olarak şu şekilde gösterilebilir:



Şekil-6.1. Biyometrik İmzaların İncelenmesi ve Karşılaştırılmasının Şematik Gösterimi

Yukarıdaki maddelerde belirtilen hususların TAM OLARAK sağlanıp gönderilmesi ve oluşturulan şemanın sırasıyla takip edilmesi hâlinde incelemeye elverişli dijital (biyometrik) imzaların incelemesi yapılarak hangi şahıs eli ürünü olup olmadığı hususunda müspet ya da menfi bir kanaat bildirmek mümkün olabilecektir.

Biyometrik imza günlük yaşamı kolaylaştıran bir unsur olduğu için yaygınlaşmıştır. Başta telefon operatörleri ve bankalar olmak üzere araç kiralama şirketleri, oteller, hastaneler, kargo firmaları gibi birçok iş kolu tarafından kullanılmaktadır. Aslında biyometrik imzaların, ıslak imzaların ya da nitelikli elektronik imzaların yerini almak gibi bir amacı yoktur. Tamamen insan ihtiyaçlarını karşılamak için ortaya çıkmıştır. Kredi kartlarının ilk çıktığı zamanı hatırlayalım. En başta kredi kartının alışveriş sonrası verilen çıktısını imzalıyorduk. Sonrasında şifre ile doğrulamaya başladık. Şimdilerde ise temassız bir şekilde kredi kartımızı kullanarak alışveriş yapmaya başladık. Bu süreç tamamen insan ihtiyaçlarına göre ilerledi. Biyometrik imzada da durumun böyle olduğunu değerlendiriyorum. Islak imzadan nitelikli elektronik imzaya geçilen durumlar olmakla birlikte, artık alternatif imza türlerinden biri olan biyometrik imzanın kullanıldığı çok sayıda işlemle karşılaşmaktayız.

Avrupa Birliği, birliğe üye ülkeler arasında elektronik ticaretin artırılması amacıyla 1999 yılında bir direktif yayınlamıştır. Bu direktif ile birlikte biyometrik imzaların kullanımı Avrupa ülkelerinde yaygınlaşmıştır. Ancak biyometrik imza kullanımında ülkeler arasında çeşitlilik olması ve ihtiyacı tam olarak karşılayamaması nedeniyle 2014 yılında AB tarafından Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü(eIDAS) oluşturulmuştur. Bu tüzüğün mantığına uygun olarak 2015 yılında da Uluslararası Standartlar Enstitüsü tarafından biyometrik imzaları da kapsayan ISO 19794 yayımlandı. Dolayısıyla biyometrik imzaların verilerinin uyumlu bir formatta olması gerektiği ve yakalanan değerlerin tek tip ölçeğe dayandırılması gerektiği ortaya kondu.

Türkiye'de 5 Ocak 2004 tarihinde, Avrupa Birliği'nin 1999 yılında yayımladığı direktifin esas alındığı Elektronik İmza Kanunu kabul edildi. Bu kanuna göre elektronik imzaları denetim ve kontrol yetkisi Bilgi Teknolojileri ve İletişim Kurumuna verilmiştir. Bilgi Teknolojileri ve İletişim Kurumu Hukuk Dairesi tarafından 2017 yılında yayımlanan Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliğinde elektronik ortamda abonelik sözleşmesi yapılabileceği hükme bağlanmıştır. Böylece 2017 yılından itibaren ülkemizde dokunmatik ekranda kalemle atılan imza yaygınlaşmaya başlamıştır.

Biyometrik imzanın diğer elektronik imzalama yöntemlerinden farkı; imzalama sürecine dair imza, imzalayan ve cihaza ait veri seti toplamasıdır. Dolayısıyla bu tür imzaların aidiyetini belirleyebilmek için geleneksel imza inceleme metotlarının yanında yeni yöntemlerin eklenmesi gereklidir.

Biyometrik imzaların adli yönden incelenebilmesi için hukuki altyapının tam olarak oluşmadığı ortadadır. Ancak incelenmesi hukuki değildir diyemeyiz. Avrupa Birliği ülkelerindeki hukuk altyapısı ülkemize göre daha iyi bir şekilde oluşturulmuştur. Nitekim 1999 yılında yayımlanan direktif ve 2014 yılında yayımlanan Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü esas alınarak hukuki düzenlemeler yapılmıştır. Ülkemizde ise 2004 yılında yayımlanan Elektronik İmza Kanunu ile ilk düzenleme yapılmıştır. Basit, gelişmiş ve nitelikli elektronik imza tanımları yapılmıştır. Biyometrik imza da gelişmiş elektronik imza kapsamında değerlendirilmektedir. 2017 yılında çıkarılan yönetmelikle de abonelik sözleşmelerinde biyometrik imza yaygın olarak kullanılmaya başlanmıştır.

Genellikle hukuki düzenlemeler bir adım geriden gelmektedir. Ülkemizde de böyle olacağını değerlendirmekteyim. Nitekim mevcut yasalarımıza baktığımızda; Hukuk Muhakemeleri Kanunu, Medeni Usul Hukuku ve Türk Ticaret Kanunu nitelikli elektronik imzanın hangi şartlarda ve nasıl kullanılacağını ayrıntılı bir şekilde belirtmesine rağmen biyometrik imzadan bahsetmemiştir. Ancak Türk Borçlar Kanunu'nda esas şart olarak imzanın elle atılması vurgulanmıştır. Bu durum biyometrik imzayı destekler niteliktedir. Yine Polisin Adli Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmelik'te delil; meydana gelen bir suçun aydınlatılması ve suç sanıklarının tespitine yarayan her türlü ispat vasıtaları olarak ifade edilmiştir. Biyometrik imzanın kullanıldığı dokümanlar da adli davalara konu olmakta, suçun aydınlatılması ve suç sanıklarının tespiti için kriminal inceleme yapılmak üzere bilirkişilere gönderilmektedir. 2017 yılında Bilgi Teknolojileri ve İletişim Kurumu da çıkardığı yönetmelikle biyometrik imza kullanımını desteklemiş olmuştur. Tüm bunlar değerlendirildiğinde biyometrik imza ile ilgili detaylı bir hukuki düzenlemenin tam olarak olduğunu söyleyemeyiz ama biyometrik imzanın varlığını inkar edecek bir düzenleme de olmadığı ortadadır. Kaldı ki biyometrik imzanın adli inceleme talepleri savcılıklar tarafından Jandarma Kriminal Laboratuvarlarına gönderilmektedir. Bu çalışma

biyometrik imzanın adli inceleme ihtiyacını karşılamak ve adli makamların inceleme taleplerini yerine getirebilmek için yapılmıştır.

Biyometrik imzanın tanımının tam olarak yapılması ve kanun koyucu tarafından düzenleyici kanunlarla desteklenmesi, hangi şartlarda kullanılmasının ortaya konması gerekmektedir. Ayrıca yasalar gereği Türkiye'de kullanılan imza çeşitlerini düzenleme yetkisi Bilgi Teknolojileri İletişim Kurumuna verilmiştir. Bu kurumun biyometrik imza özelinde yetersiz kalması, belgelere olan güven seviyesinin kuruluşların kendileri tarafından belirlenmesine sebebiyet vermiştir. Dolayısıyla ülkemizde biyometrik imza yazılımlarında birliktelik mevcut değildir. Bu durum yazılım yapan firmaların Uluslararası Standartlar Enstitüsü'nün belirlemiş olduğu standartlara uyum zorunluluğu ile sağlanabilir. Böylece biyometrik imza analiz yazılımı kullanan bir kriminal laboratuvar tarafından tüm Türkiye'de hatta dünyada kullanılan standartları sağlayan bütün biyometrik imzalar incelenebilir ve aidiyeti tespit edilebilir.

Yapılan çalışmada benim de mensubu olduğum Jandarma Kriminal Daire Başkanlığı El Yazısı ve Doküman İnceleme Şube Müdürlüğü personeli ile sürekli fikir alışverişinde bulunulmuş ve çalışma bu çerçevede yürütülmüştür. Yapılan bu çalışma biyometrik imzaların adli bilimler incelemelerine kazandırılmasında temel oluşturmaktadır. Güncel bilimsel gelişmeler ve yeni teknolojiler takip edilerek çalışmanın kapsamı arttırılabilir. Ayrıca bu çalışma esas alınarak inkâr kastıyla atılan biyometrik imzaların, üstten kopya yöntemiyle atılan biyometrik imzaların, farklı pozisyonlarda atılan biyometrik imzaların sayısal değerleri yönünden incelenmesi gibi çalışmalar yapılabilir.

7. KAYNAKLAR

[1] Kerimoğlu, D. ,"İmza nedir, nasıl atılmalıdır?", Çağın Polisi Dergisi, **2006.**

[2] Gümüşsoy, A. , İmzaların Zamana Bağlı Değişkenliği, Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü Adli Bilimler Anabilim Dalı, **2011.**

[3] Türk Dil Kurumu Sözlüğü.

[4] Yargıtay 12. Hukuk Dairesinin 28.11.2017 tarihli ve E. 2016/23838, K. 2017/14734 sayılı kararı.

[5] 21 Haziran 1934 tarihli ve 2525 sayılı Soyadı Kanununun ikinci fıkrası.

[6] Elektronik İmza Kanunu, Madde 3/b.

[7] Elektronik İmza Kanunu, Madde 4.

[8] Birleşmiş Milletler Elektronik Ticaret Model Yasası(UNCITRAL) madde 7 ve madde.

[9] https://www.eur-lex.europa.eu/legal-content/EN / Son Erişim 22 Ekim 2022.

[10] AB Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü, Madde 27, eIDAS, **2014.**

[11] Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute – ETSI) Commission Implementing Decision, **2015.**

[12] The Association for Intelligent Information Management – www.aiim.org, Son Erişim 10 Nisan 2022.

[13] The Association for Intelligent Information Management – www.aiim.org, Son Erişim 10 Mayıs 2022.

[14] AB Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü, Madde 25, eIDAS, **2014.**

[15] Elektronik İmza Kanunu, Güvenli Elektronik İmza ve Sertifika Hizmetleri Bölümü, **2004.**

[16] Elektronik İmza Kanunu, Madde 4-12, **2004.**

[17] Elektronik İmza Kanunu, Güvenli Elektronik İmza ve Sertifika Hizmetleri, **2004.**

[18] Kamu Sertifikasyon Merkezi Duyurular, www.bilgemtubitak.gov.tr, 23 Aralık 2019, Son Erişim 04 Haziran 2022.

[19] Diffie, W. , Hellman, M., New Directions in Cryptography, IEEE Transactions On Information Theory, Vol. IT-22, No:6, **1976.**

[20] Goldwasser, S. , Micali, S. ,Rivest, R., A Digital Signature Scheme Secure Against Adaptive Chosen Message Attacks, Revision 23 Mart **1995.**

[21] Canetti, R. , A Forward Secure Public Key Encryption Scheme, Journal of Cryptology 20, 265-294, **2007.**

[22] K. Franke, Capturing Reliable Data for Computer-Based Forensic Handwriting Analysis II: Penposition Activations, in: Proceedings of the 10th International Conference on Document Analysis and Recognition (ICDAR), Barcelona, Spain, **2009**, pp. 1310.

[23] V. Smejkal, J. Kodl, L. Sieger, F. Hortai, P. Tesař, Stability of a dynamic biometric signature created on various devices, in: Proceedings of the 51st International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, **2017**, pp. 1–5.

[24] J. Heckeroth, A. Kerkhoff, C. Weyermann, German BKA's Project „Esign" – How valid are pressure values, in: Proceedings of the 12th Conference of the European Network of Forensic Handwriting Experts, Porto, Portugal, **2019**, p. 19.

[25] International Organization for Standardization ISO/IEC 19794–7:2014/AMD 1:2015, Information technology, Biometric data interchange formats, Part 7: Signature/sign time series data, Amendment 1: XML encoding.

[26] ENFSI Best Practice Manual for the Forensic Examination of Digitally Captured Signatures, **2021.**

[27] JKDB-DOK-TL-7.2-02 İmza İnceleme Deney Talimatı.

[28] Hukuk Mahkemeleri Kanunu, Madde 199, 208, 205.

[29] 6098 Sayılı Türk Borçlar Kanunu, Madde 14,15.

[30] 6102 Sayılı Türk Ticaret Kanunu, Madde 756,1526.

[31] 30224 Sayılı Resmi Gazete, Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği, **2017.**

[32] Kişisel Verilerin Korunması Kurulu 27.08.2020 tarihli ve 2020/649 sayılı kararı, **2020.**

[33] 6698 Sayılı Kişisel Verilerin Korunması Kanunu, Madde 5,6, 12, 28.

[34] Linden, J., et all. Forensic Analysis of Digital Dynamic Signatures: New Methods for Data Treatment and Feature Evaluation, Journal of Forensic Science **2017.**

[35] Aksarı, Y., Artuner, H., Active Authentication by Mouse Movements, Ulakbım UASL, Hacettepe Üniversitesi, **2009**.