

PART 20

**THE COMMITTABILITY
OF FORGERY OFFENCES
IN THE DIGITAL
ENVIRONMENT**

BELGEDE SAHTECİLİK
SUÇLARININ DİJİTAL
ORTAMDA İŞLENEBİLİRLİĞİ

CENK TELLİ
MERVE ÖRKMEZ ÇAYIR
RUMEYSA SAMSA

PART 20

ABSTRACT | ÖZET

Article 204 et seq. of the Turkish Criminal Code No. 5237 (“TCC”) defines the offences of document forgery according to the nature of the document that is the subject of the offence and the manner in which the act of forgery is committed, and in this context, the issue of the document forgery in the digital environment is assessed.

5237 sayılı Türk Ceza Kanunu’nun (“TCK”) 204. maddesi ve devamında düzenlenen belgede sahtecilik suçları suçun konusu olan belgenin niteliğine ve sahtecilik eyleminin gerçekleşme biçimine göre tanımlanmakta olup bu bağlamda belgede sahtecilik suçlarının dijital ortamda işlenebilirliği hususu ele alınmaktadır.

KEYWORDS | ANAHTAR KELİMELELER

Document, Forgery, Electronic Signature, Forgery of Document, The Principle of Legality.

Belge, Sahtecilik, Elektronik İmza, Evrakta Sahtecilik, Kanunilik İlkesi.

I. INTRODUCTION

As a result of the digitalization of our age with each passing day, it is obligatory for the regulations in the law to catch up with these innovations and to be updated. However, since it is not possible for the legislator to catch up with these innovations rapidly, it is a common solution to interpret and apply the existing legal regulations in accordance with the age. In this particular context, when forgery offences are under consideration, there are a multitude of elements that need to be evaluated with great precision.

The provisions in the penal codes are interpreted strictly due to their nature. This is based on the principle of legality, which is also explained as “no punishment without law/ nulla poena sine lege”¹. Consequently, it is not possible to criminalize and punish an act that is not clearly defined by law. The principle of legality, derived from Roman Law, has been incorporated into a broader framework encompassing Human Rights Law and constitutional principles². In this article, we evaluate document forgery in digital environments within the framework of the limits set by the Constitution and criminal laws.

I. GİRİŞ

Çağımızın gün geçtikçe dijitalleşmesinin bir sonucu olarak hukukta yer alan düzenlemelerin de bu yenilikleri yakalaması ve güncellenmesi mecburiyeti doğmaktadır. Ancak kanun koyucunun bu yenilikleri hızla yakalayabilmesi imkanının düşük olmasından ötürü var olan hukuki düzenlemelerin çağa uygun bir biçimde yorumlanarak uygulanması yaygın bir çözüm olarak karşımıza çıkmaktadır. Bu bağlamda belgede sahtecilik suçları ele alındığında ise detaylıca değerlendirilmesi gereken birçok unsur mevcuttur.

Ceza kanunlarında yer alan hükümler nitelikleri gereği dar yorumlanır. Bunun dayanağı ise “kanunsuz ceza olmaz/ nulla poena sine lege” şeklinde de açıklanan kanunilik ilkesinden doğmaktadır¹. Dolayısıyla kanunda açıkça tanımlanmamış bir fiilin suç teşkil ederek cezalandırılması mümkün değildir. Kanunilik ilkesi esasında Roma Hukuku’ndan günümüze kadar gelmiş olmakla birlikte İnsan Hakları Hukuku’ndan anayasalara kadar geniş bir çerçevede kendisine yer edinmektedir². Bu makalemizde belgede sahtecilik suçlarının dijital ortamlarda işlenebilirliğini Anayasa ve ceza kanunları tarafından çizilen sınır çerçevesinde değerlendirmekteyiz.



II. FORGERY CRIMES

Offences pertaining to forgery are subject to regulations as outlined in Article 204 and the following articles of the TCC. These offences include forgery of an official document (Article 204 of the TCC), corruption, destruction or concealment of an official document (Article 205 of the TCC), false statement in the issuance of an official document (Article 206 of the TCC), forgery of a private document (Article 207 of the TCC), corruption, destruction or concealment of a private document (Article 208 of the TCC) and misuse of blank signature (Article 209 of the TCC). The distinguishing characteristics that differentiate these offences from each other are the nature of the document that is subject to forgery and the manner in which the act of forgery is committed.

The committability of these offences in the digital environment must be examined separately according to the concept of the document and the act constituting forgery.

A. The Concept of Document

Notwithstanding the fact that the document, which is the subject of the offences under Article 204 et seq. of the TCC, is not defined

II. BELGEDE SAHTECİLİK SUÇLARI

Belgede sahtecilik suçları TCK’nın 204. maddesi ve devamında düzenlenmektedir. Bu suçlar; resmi belgede sahtecilik (TCK m.204), resmi belgeyi bozmak, yok etmek veya gizlemek (TCK m.205), resmi belgenin düzenlenmesinde yalan beyan (TCK m.206), özel belgede sahtecilik (TCK m.207), özel belgeyi bozmak, yok etmek veya gizlemek (TCK m.208) ve açığa imzanın kötüye kullanılması (TCK m.209) fiilleridir. Bu suçları birbirinden ayırt eden unsurlar sahtecilik konusu belgenin niteliği ve sahtecilik fiilinin işleniş biçimine haiz hareketlerdir.

Bu suçların dijital ortamda işlenebilirliğinin ise belge kavramı ve sahtecilik teşkil eden harekete göre ayrı ayrı incelenmesi gerekmektedir.

A. Belge Kavramı

TCK madde 204 vd. yer alan suçların konusunu oluşturan belge TCK’da tanımlanmamakla birlikte; bir hukuki olay, olgu veyahut bir

DİPNOT

¹ Kemal Gözler, Yorum İlkeleri, s. 81, <https://www.anayasa.gen.tr/yorum-ilkeleri-kitaptan.pdf>. (Erişim Tarihi, 12.01.2025).

² Ümit Kılınc, Avrupa İnsan Hakları Sözleşmesinde Sınırlamanın Dar Yorumu İlkesi, YÜHFD Cilt: XVII Sayı: 2, İstanbul 2020 s. 601’den naklen; Marc Touiller, “L’interprétation stricte de la loi pénale et l’article 7 de la Convention européenne des droits de l’Homme”, RDLE, 2014, n°08.

FOOTNOTE

¹ Kemal Gözler, Comment Principles, p. 81, <https://www.anayasa.gen.tr/yorum-ilkeleri-kitaptan.pdf>. (Last Accessed, 12.01.2025).

² Ümit Kılınc, The Principle of Narrow Interpretation of Restriction in the European Convention on Human Rights, YÜHFD Cilt: XVII Sayı: 2, İstanbul 2020 p. 601; Marc Touiller, “L’interprétation stricte de la loi pénale et l’article 7 de la Convention européenne des droits de l’Homme”, RDLE, 2014, n°08.

PART 20

in the TCC, it is a written instrument used to prove a legal event, fact or a declaration of intent. Consequently, it is imperative to recognize that not all data qualifies as a document, and not all information on paper qualifies that document as a document in the sense of criminal law. A fundamental component of the term "document" is the information contained within it³. In this context, the content of the document must necessarily have the characteristic of evidencing an event or phenomenon in the legal realm. Therefore, the primary function of the document is to serve as a reliable source of ev-

irade beyanını ispata yarayan yazılı araçlardır. Dolayısıyla her veri belge niteliği taşımamakta olup kâğıt üzerinde yer alan her bilgi de evrakı ceza hukuku anlamında belge niteliğine getirmemektedir. Belge teriminden ne anlaşılacağı hususunda önemli unsurlardan biri belgenin içeriğinde yer alan bilgilerdir³. Bu bağlamda belgenin muhtevası mutlaka hukuk alanında bir olay veya olguya delalet etme özelliğini taşımalıdır. Dolayısıyla belgenin en büyük amacı ispata yarar olmasıdır. Belgenin muhtevası bir irade beyanını içerebileceği gibi hukuk düzleminde önem arz eden olay ve olgulara yönelik gerçekliğin



idence. The content of the document may include a declaration of intent, or it may be in the form of writing down the reality regarding the events and facts that are important in the legal plane. In this regard, contracts containing the declarations of intent of the parties, petitions in court files, trial records, and records maintained by state institutions such as health reports, SSI records, and land registry records, are considered as documents as well.

In addition to the content of the document, another element that constitutes its identity as a document is the certainty of its issuer. The rationale behind this assertion is that the value of the content of the document originates from the person of the issuer. The issue is to be understood from the fact that the issuer of the document is certain to whom

yazıya dökülmesi biçiminde de olabilmektedir. Bu biçimiyle ele alındığında tarafların irade beyanlarını içeren sözleşmeler; mahkeme dosyalarında yer alan dilekçeler, duruşma zaptları vb. evrak ve hatta sağlık raporları, SGK kayıtları, tapu sicil kayıtları gibi devlet kurumlarının kayıtları da belge niteliğini taşımaktadır.

Belgenin içeriği ile birlikte belgeyi belge yapan diğer bir unsur ise düzenleyicisinin belirli olmasıdır. Bunun sebebi ise belgenin içeriğinin değerinin düzenleyen şahsından kaynaklanmasıdır. Düzenleyenin belirli olmasından anlaşılacak husus belge içeriğinde yer alan irade beyanının kime ait olduğudur. Belgede yer alan imzanın değeri ise bu noktada ortaya çıkmaktadır⁴. Ancak bu durum bir evrakın ceza hukuku bakımından belge niteliği kazanabilmesi

the declaration of intent contained in the content of the document belongs. The significance of the signature in the document thus arises⁴. However, it is important to note that the requirement for a document to be signed or physically signed does not apply to the characteristics of the document in the context of criminal law.

In consideration of all these elements, it seems possible to create, modify or falsify the document in the digital environment, due to its nature. The most significant issue to be addressed in this respect is that the relevant document must meet all validity requirements. Indeed, it is not possible to forge a document that is not legally valid. Consequently, the criminal offence of forgery of a document that will not be legally valid if issued in a digital environment will not apply in cases such as forgery, alteration, distortion, destruction, concealment, etc. in a digital environment.

1. Being Written

The fundamental principle to be grasped from the fact that the document is written is that it contains writing in its content⁵. Documents that comprise solely visual elements or data recorded for storage purposes do not meet the criteria for being designated as documents. While these data possess the quality of evidence, they do not meet the criteria for document status.

The method by which the content of the document is written is inconsequential. In this respect, the quality of the document is unaffected by the method of writing employed, whether by hand or by computer. However, it is imperative to consider any validity conditions pertaining to the document's composition. To illustrate this point, consider a handwritten will, which is required by law to be written in full by hand from beginning to end. Conversely, if a handwritten will is created using a computer or typewriter, it is not subject to the same legal validity conditions as a traditional document. Consequently, if it lacks any content that would be deemed legally protected in its current state, it would not possess the requisite legal quality. Therefore, if a handwritten will is prepared in a computer environment or on a typewriter, the act of forgery on this document will not constitute an offence. In essence, the document in question lacks legal validity.

için mutlaka imzalanmış olması veya fiziken imzalanmış olması gerektiği anlamına gelmemektedir.

Tüm bu unsurlar ele alındığında belgenin niteliği gereği dijital ortamda düzenlenmesi, değiştirilmesi veya tahrif edilmesi mümkün görünmektedir. Elbette bu açıdan ele alınması gereken en önemli husus ilgili belgenin tüm geçerlilik şartlarını taşıması gerekliliğidir. Nitekim hukuken geçerli olmayan bir belgede sahtecilik yapılması da mümkün olmayacaktır. Bu bakımdan dijital ortamda düzenlenmesi halinde hukuken geçerlilik kazanmayacak bir belgenin dijital ortamda gerçeğe aykırı şekilde düzenlenmesi, değiştirilmesi, bozulması, yok edilmesi, gizlenmesi vs. gibi durumlar halinde belgede sahtecilik suçu oluşmayacaktır.

1. Yazılı Olması

Belgenin yazılı olmasından anlaşılacak husus, içeriğinde yazıyı barındırmasıdır⁵. Salt görsel içeren evrak veyahut depo edilmek amacıyla kaydedilen veriler belge niteliği taşımamaktadır. Bu veriler delil niteliği taşımakla birlikte belge niteliğinde olmayacaklardır.

Belge içeriğinde yer alan yazının hangi vasıta ile yazıldığına bir önemi bulunmamaktadır. Bu bakımdan belgenin elle yazılması veya bilgisayar ortamında yazıya aktarılması belge niteliğini etkilememektedir. Ancak unutmamak gerekir ki düzenlenen belgede yazıya ilişkin bir geçerlilik şartı bulunması halinde bu geçerlilik şartının da göz önünde bulundurulması gerekmektedir. Örneğin el yazılı vasiyetnamenin kanunda belirlenen şekil şartı olarak baştan sona elle yazılması gerekmektedir. Bu durumda el yazılı vasiyetnamenin bilgisayar ortamında veya daktilo ile yazılması halinde bu evrak kanuni geçerlilik şartlarına sahip olmadığından ötürü, mevcut şekli ile hukuken korunmaya değer başka bir içeriği de bulunmuyor ise, belge niteliğini haiz olmayacaktır. Bu sebeple el yazılı vasiyetnamenin bilgisayar ortamında veya daktilo üzerinde düzenlenmesi halinde bu evrak üzerinde yapılacak sahtecilik hareketi suç teşkil etmeyecektir. Nitekim ortada geçerli bir belge bulunmamaktadır.

FOOTNOTE

³ Ahmet Gökçen, Document Forgery Crimes (m.204-212), 4th Edition, Ankara 2016, p. 76.

⁴ Gökçen, Document Forgery Crimes, p. 84-101.

⁵ Mert Asker Yüksektepe, Document Forgery Crimes with Case Law, 2nd Edition, İstanbul 2021, p. 6.

DİPNOT

³ Ahmet Gökçen, Belgede Sahtecilik Suçları (m.204-212), 4. Baskı, Ankara 2016, s. 76.

⁴ Gökçen, Belgede Sahtecilik Suçları, s. 84-101.

⁵ Mert Asker Yüksektepe, İçtihatlarla Belgede Sahtecilik Suçları, 2. Baskı, İstanbul 2021, s. 6.

PART 20

2. The Presence of Legally Significant Content

In order to discuss the existence of a document within the context of criminal law, it is necessary for the document to contain content that is capable of producing results within the legal realm. Consequently, if a document lacks legally significant content, it cannot be considered a subject relevant to the forgery offence⁶.

It is imperative that the content of the document is comprehensible to all relevant parties, or the intended recipient. The main reason for this is that the document is a means of proof. Indeed, if the content of a text is incomprehensible, the text's legally enforceable content cannot be mentioned⁷.

3. The Significance of the Issuer

Given that the document in question is reflective of a declaration of intent due to its nature, the person whose declaration it reflects must be certain⁸. Despite the fact that it contains a legally binding will, an anonymous document does not qualify as a document within the meaning of the TCC. Consequently, the identity of the document's issuer must be discerned during the examination process. As a matter of fact, Ahmet Gökçen explains; *"The issuer of the document can be understood from its content as well as from the signature on the document"*⁹. However, in cases where the document must be signed according to the conditions of validity, it will not be sufficient to even initialize the document. However, in the absence of any such validity requirement, the existence of the document should be accepted if the issuer of the document is understood from its content.

B. The Acts Which State Forgery (Material Element)

The following acts constitute the material elements of the offence: forging a document, altering an original document in a way to deceive others, using a forged document, corrupting, destroying, concealing the document, making a false statement in the issuance of an official document, filling in a signed and partially or completely blank paper, which is filled in a certain way and delivered to him for use, in a way different from the reason for which it was given. In this re-

2. Hukuken Anlamı Olan Bir İçeriğinin Olması

Ceza hukuku anlamında bir belgenin varlığından söz edilebilmesi için belgenin hukuk aleminde sonuç doğurma yeteneğini kabil bir içeriğe sahip olması gerekmektedir. Dolayısıyla hukuken anlamı olan bir içeriğe sahip olmaması halinde belgede sahtecilik suçu konusunu oluşturan bir belgeden söz edilemeyecektir⁶.

Belgede yer alan yazıların herkes tarafından veya muhatabı tarafından anlaşılabilir olması gerekir. Bunun en temel sebebi belgenin ispat aracı olmasıdır. Nitekim muhtevasının anlaşılmadığı metinler söz konusu olduğunda hukuken anlamı olan bir içerikten bahsedilemeyecektir⁷.

3. Düzenleyicisinin Belirli Olması

Belgenin niteliği gereği irade beyanını yansıtmasından ötürü beyanını yansıttığı kişinin belirli olması gerekir⁸. Hukuken bir anlama sahip olan irade beyanı içermekle birlikte anonim olarak kaleme alınan evrak TCC anlamında belge niteliğine sahip değildir. Bu sebeple belgenin düzenleyicisinin belge incelendiğinde anlaşılması gerekmektedir. Nitekim Ahmet Gökçen; *"Belgenin düzenleyicisi muhtevastan da anlaşılabilir gibi belgede yer alan imzadan da anlaşılabilir"* şeklinde açıklamaktadır⁹. Elbette ki belgenin geçerlilik şartlarına göre imzalanmasının zorunlu olduğu hallerde belgeye paraf dahi atılmış olması yeterli olmayacaktır. Ancak imzalı olmasına yönelik bir geçerlilik şartı olmaması halinde belgenin düzenleyicisinin içeriğinden anlaşıldığı durumlarda da belgenin varlığı kabul edilmelidir.

B. Sahtecilik Teşkil Eden Fiiller (Maddi Unsur)

Suçun maddi unsuru olan fiiller; belgenin sahte olarak düzenlenmesi, gerçek olarak düzenlenen bir belgenin gerçeğe aykırı olarak başkalarını aldatacak biçimde değiştirilmesi, sahte bir belgenin kullanılması, belgenin bozulması, yok edilmesi, gizlenmesi, resmi bir belgenin düzenlenmesinde yalan beyanda bulunulması, belirli bir tarzda doldurulup kullanılmak üzere kendisine teslim olunan imzalı ve kısmen veya tamamen boş bir kâğıdın verilme nedeninden farklı bir şekilde doldu-

gard, it is imperative to consider the committability of these actions within the context of the digital environment, as they bear distinct characteristics that must be duly assessed.

1. Issuing the Document as Forged

The forgery of a document is classified as an offence under Article 204 of the TCC or Article 207 of the TCC, depending on whether the document is of an official or private nature. While forgery alone is sufficient for the commission of the offence in official documents, forgery alone is not sufficient in private documents, and the forged document must also be used for the commission of the offence. The crux of the matter pertains to the conceptualization of forgery, which is understood to be contrary to the declaration of intent of the document's issuer or contrary to the events or facts reflected in reality. An alternative opinion posits that forgery entails the imitation of document-issuing¹⁰.

In order for this particular offence to be committed in the digital environment, it is necessary for the issuing activity to take place in said environment. Given that the drafting of documents in a computer environment is not subject to any restrictions, provided that it does not contradict the validity conditions, it can be concluded that this offence can be committed in the digital environment if the document issued in the computer environment is issued in a false manner.

2. The Alteration of an Original Document

The alteration of an original document with the intent to deceive others is considered an offence¹¹. It is important to note that, in contrast to the act of modifying an official document, the use of a private document, in addition to the modification itself, must also take place for the offence to occur, as in the act of editing. In the digital environment, the commission of this offence varies according to the form in which the document is issued.

In the event of the physical issuance of the original document, any subsequent digital alterations to that document would require the transfer of the document to the digital environment, followed by a deliberate alteration of the document in a manner that is contrary to the truth. Conversely, if an original document is produced in a digital environment

ruled. Bu bakımdan söz konusu fiillerin dijital ortamda gerçekleştirilebilirliğinin ayrı ayrı ele alınması gerekmektedir.

1. Belgenin Sahte Olarak Düzenlenmesi

Belgenin sahte olarak düzenlenmesi, resmi veya özel niteliğe sahip olmasına göre TCC madde 204 veya TCC madde 207'ye göre suç teşkil etmektedir. Resmi belgede suçun oluşması için sahte olarak düzenleme tek başına yeterli değilken özel belgede düzenleme tek başına yeterli olmayıp suçun oluşması için sahte belgenin kullanılması da gerekmektedir. Burada ele alınması gereken husus sahtelikten ne anlaşılacağıdır ki sahtelik, belgenin düzenleyicisinin irade beyanına veya gerçek dünyada yansıttığı olay veya olgulara aykırı olmasıdır. Diğer bir görüşe göre sahtelikten anlaşılacak husus taklit suretiyle belgenin düzenlenmesidir¹⁰.

Bu fiilin dijital ortamda işlenebilmesi için düzenleme faaliyetinin dijital ortamda gerçekleşmesi gerekmektedir. Belgelerin bilgisayar ortamında kaleme alınmasında, geçerlilik şartlarına aykırılık oluşturmadığı sürece, bir engel olmadığından ötürü bilgisayar ortamında düzenlenen belgenin gerçeğe aykırı bir biçimde düzenlenmesi halinde bu suçun dijital ortamda işlenebileceği aşikardır.

2. Gerçek Olarak Düzenlenen Bir Belgenin Değiştirilmesi

Gerçek olarak düzenlenen bir belgenin başkalarını aldatacak biçimde değiştirilmesi suç teşkil etmektedir¹¹. Tabii burada özel bir belgeden bahsediliyor ise, resmi belgeden farklı olarak yine düzenleme eyleminde olduğu gibi suçunun oluşması için değiştirme eylemine ilaveten kullanmanın da gerçekleşmesi gerekmektedir. Burada bu suçun dijital ortamda işlenmesi gerçek olarak düzenlenen belgenin hangi biçimde düzenlendiğine göre değişiklik göstermektedir.

Gerçek belgenin fiziki olarak düzenlenmiş olması ihtimalinde bu belgenin dijital ortamda değiştirilebilmesi için belgenin dijital ortama aktarılması, akabinde gerçeğe aykırı bir biçimde değiştirilmesi söz konusu olacaktır. Ancak gerçek bir belgenin dijital ortamda üretilmiş olması halinde bu belge çoğunluk-

DİPNOT

6 Yüksektepe, Belgede Sahtecilik Suçları, 2. Baskı, İstanbul 2021, s. 10.

7 Gökçen, Belgede Sahtecilik Suçları, s. 91; **Doğan Soyaslan**, Ceza Hukuku Özel Hükümler, 8. Baskı, Ankara 2010, s. 488.

8 Mahmut Koca/ İlhan Üzülmez, Türk Ceza Hukuku Özel Hükümler, 2. Baskı, Ankara 2015, s. 671.

9 Gökçen, Belgede Sahtecilik Suçları, s. 95.

10 Gökçen, Belgede Sahtecilik Suçları, s. 168. "Taklit, varakanın düzenleneni gözüken kişiden başka bir kimse tarafından yeniden düzenlenmesi demektir. Bu halde sahte olarak oluşturulan evraktan önce ortada gerçek bir belgenin bulunması ve sahtekarlık sonucunda yine bu belgenin varlığını koruması gerekir." Ayrıca bkz. **Sahir Erman**, Ticari Ceza Hukuku C.: III, Sahtekarlık Suçları, İstanbul 1987, s. 442.

11 Koca/ Üzülmez, Özel Hükümler, s. 685.

FOOTNOTE

6 Yüksektepe, Document Forgery Crimes, 2nd Edition, İstanbul 2021, p. 10.

7 Gökçen, Document Forgery Crimes, p. 91; **Doğan Soyaslan**, Special Provisions of Criminal Law, 8th Edition, Ankara 2010, p. 488.

8 Mahmut Koca/ İlhan Üzülmez, Turkish Criminal Law Special Provisions, 2nd Edition, Ankara 2015, p. 671.

9 Gökçen, Document Forgery Crimes, p. 95.

10 Gökçen, Document Forgery Crimes, p. 168. "Forgery means that the document is issued by a person other than the person who appears to be the issuer of the document. In this case, a real document must exist before the forged document and this document must still exist as a result of the forgery." Also look: **Sahir Erman**, Commercial Criminal Law, C.: III, Fraud Crimes, İstanbul 1987, p. 442.

11 Koca/ Üzülmez, Special Provisions, p. 685.

PART 20

since this document is usually stored in the database where it was produced, document verification systems can easily reveal whether the document has been forged.

3. The Use of a Forged Document

The use of a forged document constitutes another act that forms the crime of document forgery¹². There is a distinction between whether the document subject to the crime is an official document, i.e. a document issued by a public official in accordance with certain regulations as part of their duty, or a private document in terms of this act that gives rise to crime. In case the document in question is an official document, the legislator considers the acts of forging, altering in a way to deceive others, using, and issuing contrary to the truth by a public official as separate crimes. In other words, the mere occurrence of either forging or using an official document alone is sufficient for the crime to be committed. However, if the document subject to the crime is a private document, both the acts of forging and using must occur together for the crime to be committed. Furthermore, the legislator has also criminalized the act of knowingly using a forged private document. Moreover, the environment in which the document is used is important in terms of this crime being committed in the digital realm. Therefore, in case a forged document is used in digital environments, it may be possible for document forgery crimes to be committed in the digital realm as well.

4. Corrupting, Destroying or Concealing the Document

The act of destroying, corrupting, or concealing a document constitutes a crime as it aims to prevent the document from fulfilling its primary purpose of providing evidence, effectively amounting to tampering with evidence¹³. The subject of this crime can only be official documents. With regard to documents created in physical form, it is not possible to commit this act in the digital environment. Indeed, it is contrary to the ordinary course of life to digitally alter a document that has a physical existence.

However, it is possible to commit this crime with respect to documents prepared in the digital environment. For documents digitally

la belgenin üretildiği veri tabanında da saklandığından, belge doğrulama sistemleri ile belge üzerinde sahtelik yapıp yapılmadığı kolaylıkla ortaya çıkabilecektir.

3. Sahte Olarak Düzenlenen Bir Belgenin Kullanılması

Belgede sahtecilik suçunu oluşturan diğer bir fiil de sahte olarak düzenlenen bir belgenin kullanılmasıdır¹². Suça vücut veren bu eylem bakımından suça konu belgenin resmi belge niteliğini haiz olması, yani bir kamu görevlisi tarafından görevi gereği belirli mevzuatlara göre düzenlenen bir belge olması ile özel belge niteliğini haiz arasında fark bulunmaktadır. Söz konusu belgenin resmi bir belge olması halinde kanun koyucu; sahte olarak düzenleme, başkalarını aldatarak şekilde değiştirme, kullanma ve kamu görevlisi tarafından gerçeğe aykırı şekilde düzenleme eylemlerini ayrı ayrı suç olarak kabul etmektedir. Bir diğer ifade ile, resmi belgenin sadece sahte olarak düzenlenmesi ve sadece kullanılması eylemlerinden birinin gerçekleşmesi, suçun oluşması için tek başına yeterlidir. Ancak suça konu belgenin özel belge olması halinde suçun oluşması için düzenleme ve kullanma eyleminin birlikte gerçekleşmesi gerekir. Öte yandan kanun koyucu, özel belgenin sahte olduğunu bilecek kullanma eylemini de cezaya bağlamıştır. Bununla birlikte bu suçun dijital ortamda işlenebilmesi bakımından belgenin kullanıldığı ortam önem arz etmektedir. Dolayısıyla sahte olarak üretilen bir belgenin dijital ortamlarda kullanılması halinde de belgede sahtecilik suçlarının dijital ortamda işlenebilmesi söz konusu olabilecektir.

4. Belgenin Bozulması, Yok Edilmesi veya Gizlenmesi

Belgenin bozulması, yok edilmesi veya gizlenmesi fiili belgenin esas amacı olan ispatı önlemek yani delil karartmak anlamını taşıdığından suç teşkil etmektedir¹³. Bu suçun konusu ancak resmi belgeler olabilmektedir. Fiziki ortamda düzenlenen belgeler bakımından bu fiilin dijital ortamda işlenebilmesi mümkün olmamaktadır. Nitekim fiziki varlığa sahip bir belgenin dijital olarak tahrif edilmesi hayatın olağan akışına aykırıdır.

Ancak dijital ortamda düzenlenen belgeler bakımından bu suçun işlenmesi mümkün olabilir. Dijital ortamda düzenlenerek veri tabanlarına kaydedilen belgeler bakımından belgeyi tahrif etme suçunun gerçekleştiril-

created and stored in databases, the crime of document forgery can be committed through hacking activities carried out on the sources of these databases. However, this also constitutes the crime of obstructing, disrupting, destroying or altering data in a system as regulated in Article 244 of the TCC¹⁴. According to Article 244(2) of the TCC, this crime is defined as: "A person who corrupts, destroys, alters or renders inaccessible the data in an information system, inserts data into the system, or sends existing data to another place shall be sentenced to imprisonment from six months to three years". Therefore, such activities directed at the information system where a digitally created document is stored may constitute both the crime specified in Article 205 or 208 of the TCC and the crime in Article 244 of the TCC, depending on whether the document is official or private. However, real concurrence as per Article 212 of the TCC cannot be applied here. Indeed, Article 212 of the TCC states: "In case of using a forged official or private document during the commission of another crime, separate penalties shall be imposed for both forgery and the related crime." The application of real concurrence provisions requires that the act of forgery be in the form of using a forged document¹⁵. Consequently, in the case of Article 244 of the TCC as explained above, real concurrence provisions cannot be applied since there is no new crime committed using a forged document. Nevertheless, as multiple different crimes under Article 244 of the TCC and Article 204 et seq. of the TCC are committed simultaneously through the same act, the provisions of ideal concurrence will be applied, and the penalty will be imposed based on the crime type that requires a more severe punishment between these two crime types.

5. The False Declaration in the Issuance of an Official Document

False declaration in the issuance of an official document constitutes another type of document forgery crime. In this regard, it is necessary to address the differences between official documents and private documents. An official document refers to a document issued by a public official in the course of their duty¹⁶. In this context, identity documents, driver's licenses, passports, graduation certificates and diplomas, documents issued by courts, land registry records, and all similar documents are considered

lebilmesi, bu veri tabanlarının kaynaklarında gerçekleştirilecek korsanlık faaliyetleri ile mümkün olacaktır. Ancak bu husus TCK madde 244'te düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu da oluşturmaktadır¹⁴. TCK madde 244'ün 2. fıkrasına göre bu suç; "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır." şeklinde düzenlenmektedir. Bu sebeple dijital ortamda düzenlenen bir belgenin muhafaza edildiği bilişim sistemine yönelik bu faaliyetler belgenin resmi veya özel belge niteliğini haiz olmasına göre hem TCK madde 205 ya da TCK madde 208'de yer alan suçu hem de TCK madde 244'te yer alan suçu oluşturabilmektedir. Ancak burada TCK madde 212 gereğince gerçek içtima uygulanamayacaktır. Nitekim TCK madde 212; "Sahte resmi veya özel belgenin bir başka suçun işlenmesi sırasında kullanılması halinde hem sahtecilik hem de ilgili suçtan dolayı ayrı ayrı cezaya hükmolunur." şeklinde düzenlenmekte olup gerçek içtima hükümlerinin uygulanabilmesi için sahtecilik konusu fiilin sahte belgenin kullanılması şeklinde olması gerekecektir¹⁵. Dolayısıyla yukarıda açıkladığımız TCK md.244'ün söz konusu olduğu durumda sahte belge kullanılarak işlenmiş yeni bir suçtan bahsedilemeyeceği için gerçek içtima hükümleri uygulama alanı bulamayacaktır. Ancak bununla birlikte aynı eylem ile TCK m.244'teki ve TCK md.204 ve devamındaki birden çok farklı suç birlikte işlenmiş olacağından fikri içtima hükümleri uygulanarak, bu iki suç tipinden daha ağır ceza verilmesi gerektiren suç tipi üzerinden ceza verilecektir.

5. Resmi Bir Belgenin Düzenlenmesinde Yalan Beyanda Bulunulması

Resmi bir belgenin düzenlenmesinde yalan beyanda bulunulması diğer bir belgede sahtecilik suçudur. Bu hususta resmi belge ile özel belge arasındaki farklara değinmek gerekmektedir. Resmi belge, kamu görevlisi tarafından görevi gereği düzenlenen belge anlamına gelmektedir¹⁶. Bu bağlamda kimlik belgeleri, sürücü belgeleri, pasaportlar, mezuniyet belgeleri ve diplomalar, mahkemeler tarafından düzenlenen belgeler, tapu kayıtları vb. tüm belgeler resmi belge niteliğindedir. Resmi belge niteliğini haiz olmayan tüm

FOOTNOTE

¹² Gökçen, Document Forgery Crimes, p. 193.

¹³ Koca/ Üzülmöz, Special Provisions, p. 702.

¹⁴ Mehmet Can Karagöz, Blocking the Information System with an Introduction to Information Systems Theory, Crime of Corruption, Destruction or Alteration of Data, 1st Edition, İstanbul 2020, p. 151.

¹⁵ Gökçen, Document Forgery Crimes, p. 305.

¹⁶ Soyaslan, Special Provisions, p. 489.

DİPNOT

¹² Gökçen, Belgede Sahtecilik Suçları, s. 193.

¹³ Koca/ Üzülmöz, Özel Hükümler, s. 702.

¹⁴ Mehmet Can Karagöz, Bilişim Sistemleri Teorisine Giriş İle Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, 1. Baskı, İstanbul 2020, s. 151.

¹⁵ Gökçen, Belgede Sahtecilik Suçları, s. 305.

¹⁶ Soyaslan, Özel Hükümler, s. 489.

PART 20

official documents. All documents that do not possess the characteristics of an official document fall under the definition of private documents. In this context, documents prepared by public officials independently of their duties are also considered private documents¹⁷. Furthermore, Article 210 of the TCC enumerates documents that are considered equivalent to official documents. This provision states: "(1) If the subject of private document forgery is a negotiable instrument payable to order or bearer, a document representing goods, a share certificate, a bond, or a will, the provisions relating to forgery of official documents shall apply. (2) A physician, dentist, pharmacist, midwife, nurse, or other healthcare professional who issues a false document shall be sentenced to impris-



onment from three months to one year. If the issued document provides an unjust benefit to a person or has the nature of causing harm to the public or individuals, the penalty shall be determined according to the provisions of forgery of official documents." This article stipulates documents that, although private in nature, are considered official documents. Moreover, it would be beneficial to add a note regarding the crime of forgery in official documents in the form of certification, separate from the act of false declaration. Specifically, when a private document acquires the status of an official document through notarization, the nature of the forgery will vary depending on which part of the document

belgeler ise özel belge tanımına girecektir. Bu bağlamda kamu görevlisinin görevinden bağımsız olarak düzenlediği belgeler de özel belge niteliğindedir¹⁷. Bununla birlikte TCK madde 210 ise resmi belge niteliğinde sayılan belgeleri sıralamaktadır. Bu hüküm; "(1) Özel belgede sahtecilik suçunun konusunun, emre veya hamile yazılı kambiyo senedi, emtiayı temsil eden belge, hisse senedi, tahvil veya vasiyetname olması halinde, resmi belgede sahtecilik suçuna ilişkin hükümler uygulanır. (2) Gerçeğe aykırı belge düzenleyen tabip, diş tabibi, eczacı, ebe, hemşire veya diğer sağlık mesleği mensubu, üç aydan bir yıla kadar hapis cezası ile cezalandırılır. Düzenlenen belgenin kişiye haksız bir menfaata sağlaması ya da kamunun veya kişilerin zararına bir sonuç doğurucu nitelik taşıması ha-

linde, resmi belgede sahtecilik hükümlerine göre cezaya hükmolunur." şeklinde düzenlenmiş olup özel belge olmakla birlikte resmi belge olarak sayılan belgeleri hükme bağlamıştır. Öte yandan bu konuya yalan beyan eyleminden ayrı olarak onaylama şeklindeki resmi belgelerde sahtecilik suçu konusunda bir ilavede bulunmak faydalı olacaktır. Şöyle ki; özel niteliğe haiz bir belgenin noterde onaylanma suretiyle resmi belge vasfı kazanması halinde sahtecilik faaliyetinin belgenin hangi kısmında gerçekleştiğine göre niteliği değişiklik gösterecektir. Sahtecilik faaliyetinin bu biçimde düzenlenen bir belgenin içerik kısmında gerçekleştirilmesi halinde bu durumda oluşan suç özel belgede sahtecilik

the forgery occurs. If the forgery activity is carried out in the content section of a document prepared in this manner, the resulting crime will be forgery of a private document. However, if the forgery activity relates to the notarization process (date, journal number, seal, signature, etc.) performed by the notary, the resulting crime will be the forgery of an official document.

The act of making a false declaration will only constitute a crime if the document being issued is an official document. Consequently, the person to whom the false declaration is made must be a public official. In this context, it is evident that this crime will materialize if the false declaration is transmitted digitally to a public official. In other words, if a false declaration is submitted while creating a document request in a digital environment, for example through the E-Devlet Portal, and this document is generated as a result of a public official's evaluation, this crime will have been committed. However, if the document request is created automatically by the digital system without being evaluated by a public official when it is submitted, or if the person to whom it is submitted for evaluation is not a public official, then this crime will not occur.

6. Misuse of Blank Signature

The act of misusing a blank signature occurs when a signed paper, either partially or completely blank, which has been entrusted to someone to be filled out in a specific manner, is instead completed in a way that differs from its intended purpose. A document can be signed physically, electronically, or digitally. This matter is stipulated in Article 15 of the Turkish Code of Obligations ("TCO") No. 6098, which states: "The signature must be handwritten by the person undertaking the obligation. A secure electronic signature also produces all the legal consequences of a handwritten signature." Consequently, for an electronically signed document to produce all the legal effects of a handwritten signature, the signature must be a secure electronic signature. The primary reason for this requirement is to prevent the forgery, copying, or alteration of electronic signatures.

According to Article 4 of the Electronic Signature Law No. 5070 ("Law No. 5070"), a secure electronic signature is defined as an electronic signature that: "a) Is exclusively

suçu olacaktır. Ancak sahtecilik faaliyetinin noter tarafından gerçekleştirilen onay işlemine ilişkin (tarih, yevmiye no, mühür, imza, vs.) olması halinde gerçekleştirilecek suç resmi belgede sahtecilik suçu olacaktır.

Yalan beyanda bulunulması fiili ancak düzenlenen belgenin resmi belge olması halinde suç teşkil edecektir. Dolayısıyla yalan beyanda bulunulan kişi bir kamu görevlisi olacaktır. Bu bağlamda kamu görevlisine iletilen yalan beyanın dijital olarak iletilmesi halinde bu suçun vücut bulacağı aşikardır. Yani dijital ortamda, örneğin E-Devlet Portalı üzerinden, belge talebi oluşturulduğu esnada yalan beyan sunularak bu belgenin bir kamu görevlisinin değerlendirmesi sonucu oluşturulması halinde bu suç gerçekleşmiş olacaktır. Ancak belge talebi oluşturulduğunda bu talep bir kamu görevlisinin değerlendirmesinden geçmeksizin, yani dijital sistem tarafından otomatik olarak oluşturuluyorsa veyahut değerlendirilmesine sunulan kişi kamu görevlisi değilse bu halde bu suç oluşmayacaktır.

6. Açığa İmzanın Kötüye Kullanılması

Açığa imzanın kötüye kullanılması fiili belirli bir tarzda doldurulup kullanılmak üzere kendisine teslim olunan imzalı ve kısmen veya tamamen boş bir kağıdın verilme amacından farklı bir şekilde doldurulması şeklinde gerçekleşmektedir. Belge fiziki olarak imzalanabileceği gibi elektronik veya dijital olarak da imzalanabilmektedir. Bu husus 6098 sayılı Türk Borçlar Kanunu'nun ("TBK") 15. maddesinde; "İmzanın, borç altına girenin el yazısıyla atılması zorunludur. Güvenli elektronik imza da, el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğurur." şeklinde hüküm altına alınmıştır. Dolayısıyla elektronik ortamda imzalanan belgenin el yazısı ile atılan imzanın bütün hukuki sonuçlarını doğurabilmesi için imzanın güvenli elektronik imza olması gerekir. Bunun en temel sebebi elektronik imzanın sahte olmasının veya kopyalanmasının, değiştirilmesinin önlenmesidir.

Güvenli elektronik imza 5070 sayılı Elektronik İmza Kanunu'nun ("5070 sayılı Kanun") 4. maddesine göre; "Güvenli elektronik imza; a) Münhasıran imza sahibine bağlı olan, b)

FOOTNOTE

¹⁷ Devrim Güngör, Crime of Forgery of Official Documents, 1st Edition, Ankara 2010, p. 62.

DİPNOT

¹⁷ Devrim Güngör, Resmi Belgede Sahtecilik Suçu, 1. Baskı, Ankara 2010, s. 62.

PART 20

linked to the signatory, b) Is created using a secure electronic signature creation device that is solely under the control of the signatory, c) Enables the identification of the signatory based on a qualified electronic certificate, d) Allows for the detection of any subsequent changes made to the signed electronic data.” Consequently, signatures on documents signed with a secure electronic signature can be examined for any type of forgery activity¹⁸. For instance, if any alterations are made to a document signed with a secure electronic signature, the signatures recorded on the document are automatically deleted.

If an unsecured electronic signature is used as required by legislation, it cannot be considered a signature within the meaning of Article 15 of the TCO. Consequently, if the signature is a condition for the validity of the document in question, a valid document cannot be established, and therefore, the crime of document forgery will not occur as a result of the forgery activity. However, it is evident that the crime of forgery will occur in the event that the alteration of data in the document cannot be traced using technological means when a secure electronic signature is used. In this case, the forgery activity will have taken place on the electronic signature itself. In other words, the crime that will materialize in terms of forgery activity here is not the misuse of a blank signature, but forgery of the signature itself.

Article 17 of Law No. 5070 stipulates: “Those who create wholly or partially forged electronic certificates or who counterfeit or alter validly created electronic certificates, as well as those who knowingly use these electronic certificates, shall be punished with imprisonment from two to five years and a judicial fine of not less than one hundred days. If the crimes mentioned in the above paragraph are committed by employees of an electronic certificate service provider, these penalties shall be increased by up to half.” This provision regulates the crime of forgery in electronic signatures. In this context, a forgery activity carried out on a document with an electronic signature will also constitute forgery within the scope of this provision¹⁹. The answer to the question of which provisions should be applied - the acts specified in the TCC or the penal provisions in Law No. 5070 - is provided in Article 212 of the TCC. Consequently, to the extent applicable, real concurrence should be applied, and the penalty should be calculated based on both types of crimes.

Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespiti ni sağlayan, d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapıp yapılmadığının tespitini sağlayan, elektronik imzadır.” şeklinde tanımlanmaktadır. Dolayısıyla güvenli elektronik imza ile imzalanan belgelerde yer alan imzalar her türlü sahtecilik faaliyeti bakımından incelenebilmektedir¹⁸. Örneğin güvenli elektronik imza ile imzalanan bir belge üzerinde değişiklik yapılması halinde belge üzerinde kayıtlı imzalar otomatik olarak silinmektedir.

Mevzuat gereği güvenli olmayan elektronik imza kullanılması halinde ise TBK madde 15 anlamında bir imzadan söz edilemeyeceğinden dolayı, imzanın söz konusu belgenin geçerlilik şartı olması halinde geçerli bir belgeden söz edilemeyeceğinden gerçekleştiren sahtecilik faaliyeti sonucu belgede sahtecilik suçu oluşmayacaktır. Ancak kullanılan güvenli elektronik imzanın teknolojik imkanlar kullanılarak belgede yer alan verilerin değiştirilmesinin izlenemediği ihtimalde sahtecilik suçunun gerçekleşeceği aşikardır. Ancak bu durumda gerçekleşecek sahtecilik faaliyeti elektronik imza üzerinde gerçekleşmiş olacaktır. Yani burada sahtecilik faaliyeti bakımından vücut bulacak suç açığa imzanın kötüye kullanılması suçu değil, imzada sahtecilik suçudur.

Bununla birlikte 5070 sayılı Kanun’un 17. maddesi; “Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taktit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adli para cezasıyla cezalandırılır. Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.” şeklinde düzenlenmiş olup elektronik imzada sahtecilik suçunu düzenlemiştir. Bu bağlamda elektronik imzalı bir belgede gerçekleştirilen sahtecilik faaliyeti aynı zamanda bu hüküm bağlamında da sahtecilik anlamına gelecektir¹⁹. Bu hükümler arasında TCK’da yer alan fiiller veyahut 5070 sayılı Kanun’da yer alan cezai hükümlerden hangisinin uygulanacağı sorusunun cevabı ise yine TCK madde 212’de yer almaktadır. Dolayısıyla, uygun düştüğü ölçüde gerçek içtima uygulanarak her iki suç tipi üzerinden de cezanın hesaplanması gerekecektir.

C. The Ability to Mislead

Undoubtedly, the most crucial aspect to consider regarding document forgery crimes is the deceptive capability of the forged document. The deceptive capability, although not explicitly stated among the elements in the law, is one of the material elements of the crime of document forgery. In this respect, the deceptive capability is an element related to the forged document’s ability to be convincing about its authenticity, and the determination of this aspect is left to the discretion of the judge.

In the commission of document forgery crimes in the digital environment, attention must be paid to whether this element is also present²⁰. Indeed, a forged document that does not convince its recipient of its authenticity does not constitute the subject of this crime.

The examination of whether this element is realized in terms of documents produced in the digital environment can be understood through electronically generated documents with QR codes. Since documents produced with QR codes can be verified in the digital environment, the deceptive capability of these documents will be realized when the document is verified. The QR code verification process is carried out by opening the obtained document with the QR code and matching it through the system. In other words, along with the content being contrary to the truth, the matching of the document displayed on the system with the document in hand through the QR code on the document will ensure the realization of the deceptive capability element. However, it is evident that if the document opened through the system with the QR code does not match, the element of deceptive capability will not be realized. Moreover, if the content is also genuine and the document is verified with the QR code, there is no issue to be discussed in terms of the crime of forgery.

The determination of whether this element is realized in terms of electronic signatures can be made by examining the validity of the certificates in secure electronic signatures. Secure electronic signatures are subject to the supervision of the Information and Communication Technologies Authority as per Law No. 5070. The certification processes of secure electronic signatures are carried out by electronic signature providers. These certifi-

C. İğfal Kabiliyeti Hususu

Belgede sahtecilik suçları bakımından ele alınması gereken en önemli husus hiç şüphesiz sahte belgenin iğfal kabiliyetini haiz olmasıdır. İğfal kabiliyeti, kanunda yer alan unsurlar arasında açıkça yazmamakla birlikte, belgede sahtecilik suçunun maddi unsurlarındandır. Bu bakımdan iğfal kabiliyeti sahte düzenlenen belgenin gerçek olduğu konusunda inandırıcılık yeteneğine sahip olmasına yönelik bir unsur olup, bu hususun tespiti hâkimin takdir yetkisine bırakılmıştır.

Belgede sahtecilik suçlarının dijital ortamda işlenmesi esnasında da bu unsurun oluşup oluşmadığına dikkat edilmesi gerekecektir²⁰. Nitekim muhatabını gerçek olduğuna inandırmayan sahte bir belge bu suçun konusu olmamaktadır.

Dijital ortamda üretilen belgeler bakımından bu unsurun gerçekleşip gerçekleşmediğinin incelemesi ise karekodlu olarak düzenlenen elektronik belgeler üzerinden anlaşılabilir. Karekodlu biçimde üretilen belgelerin yine dijital ortamda doğrulanması yapılabileceğinden dolayı bu belgelerin iğfal kabiliyetinin bulunması belgenin doğrulanması halinde gerçekleşmiş olacaktır. Karekod ile doğrulama işlemi, elde edilen belgenin karekod ile açılıp sistem üzerinden eşleştirme yapılması ile gerçekleştirilmektedir. Yani içeriğinin gerçeğe aykırı olmasıyla birlikte belge üzerinde yer alan karekod sayesinde sistem üzerinde görüntülenen belge ile elde bulunan belgenin eşleştirilmesi iğfal kabiliyeti unsurunun gerçekleşmesini sağlayacaktır. Ancak karekod ile sistem üzerinden açılan belgenin eşleşmemesi halinde iğfal kabiliyeti unsurunun gerçekleşmeyeceği aşikardır. Kaldı ki içeriğinin de gerçek olması ve belgenin karekod ile doğrulanması halinde zaten sahtecilik suçu bakımından tartışılacak bir husus bulunmamaktadır.

Elektronik imza bakımından bu unsurun gerçekleşip gerçekleşmediğinin tespiti için ise güvenli elektronik imzalarda yer alan sertifikaların geçerliliğine bakılabilecektir. Güvenli elektronik imza 5070 sayılı Kanun gereği Bilgi Teknolojileri ve İletişim Kurumu’nun denetimine tabidir. Güvenli elektronik imzanın sertifikalanması işlemleri elektronik imza yer sağlayıcıları tarafından gerçekleştirilmektedir. Bu sertifikalar imza sahiplerinin kimliğini, imzalanan belgede değişiklik yapıp yapılmadığını, belgenin ne zaman imzalandığını vb. tüm verilerin sorgulanmasını sağlamaktadır.

FOOTNOTE

¹⁸ Mehmet Emin Özgül, Rights and Obligations of the Secured Electronic Signature Holder, InÜHFD 12(2): 539-556 (2021), p. 547.

¹⁹ Özhan Sağlık, Forgery of Electronic Signed Documents: A Review in the Context of Supreme Court Decisions, <https://acikerisim.uludag.edu.tr/server/api/core/bitstreams/499f2a00-753d-4764-9f23-c954c9e3dc5a/content#:~:text=%E2%80%9C-Bir%20resmi%20belgeyi%20sahte%20olarak,kadar%20hapis%20cezas%C4%B1%20ile%20cezaland%C4%B1r%C4%B1lmaktad%C4%B1r,> (Last Accessed, 12.01.2025).

²⁰ Soyaslan, Special Provisions, p. 498 et seq.

DİPNOT

¹⁸ Mehmet Emin Özgül, Güvenli Elektronik İmza Sahibinin Hakları ve Yükümlülükleri, InÜHFD 12(2): 539-556 (2021), s. 547.

¹⁹ Özhan Sağlık, Elektronik İmzalı Belgelerin Sahteciliği: Yargıtay Kararları Bağlamında Bir İnceleme, <https://acikerisim.uludag.edu.tr/server/api/core/bitstreams/499f2a00-753d-4764-9f23-c954c9e3dc5a/content#:~:text=%E2%80%9C-Bir%20resmi%20belgeyi%20sahte%20olarak,kadar%20hapis%20cezas%C4%B1%20ile%20cezaland%C4%B1r%C4%B1lmaktad%C4%B1r,> (Erişim Tarihi 12.01.2025).

²⁰ Soyaslan, Özel Hükümler, s. 498 vd.

PART 20

cates enable the verification of all data such as the identity of the signatories, whether any changes have been made to the signed document when the document was signed, etc. Document formats capable of being electronically signed also have a certificate viewing feature. Therefore, the characteristics of the electronic signature can be examined using this certificate viewing feature in these documents, and the forgery activity can be investigated accordingly²¹. In cases where the forgery activity has also been carried out on the certificate itself, it is evident that this would constitute a crime under Article 17 of Law No. 5070, as explained above.

III. CONCLUSION

The rapidly evolving and changing era brings certain challenges to the legal realm, and the resolution of these issues is limited to the interpretation of existing law. While considering this matter in terms of document forgery crimes, the problem of forgery in digitalized documents persists alongside the digitalization of the world. The legislator's inadequacy in keeping pace with the times in lawmaking leaves no alternative but to produce casuistic solutions to end these problems.

When examined in terms of current law, the feasibility of committing document forgery crimes in the digital environment has been evaluated separately for each type of crime. According to this assessment, the feasibility of committing each act constituting forgery

Elektronik ortamda imzalanabilme kabiliyetine sahip belge formatlarında aynı zamanda sertifika görüntüleme özelliği bulunmaktadır. Dolayısıyla bu belgelerde yer alan sertifika görüntüleme özelliği kullanılarak elektronik imzanın özellikleri incelenebilmekte, bu doğrultuda yapılan sahtecilik faaliyetini incelenebilmektedir²¹. Sahtecilik faaliyetinin sertifika üzerinde de gerçekleştirilmiş olması halinde ise yukarıda da açıklandığı üzere 5070 sayılı Kanun'un 17. maddesi gereğince suç teşkil edeceği aşikardır.

III. SONUÇ

Büyük bir hızla gelişen ve değişen çağın hukuk alemine taşıdığı birtakım sorunlar bulunmakta olup bu sorunların çözümü için yürürlükte olan hukukun yorumlanmasından öteye gidilememektedir. Belgede sahtecilik suçları bakımından bu husus ele alındığında dijitalleşen dünya ile birlikte dijitalleşen evrakin sahteliği sorunu varlığını sürdürmektedir. Kanun koyucunun yasa yapma konusunda çağa ayak uydurmak konusundaki yetersizliği bu problemlerin sona erdirilmesi için kazistik çözümler üretilmesinden başka çare bırakmamaktadır.

Yürürlükte olan hukuk bakımından ele alındığında belgede sahtecilik suçlarının dijital ortamda işlenebilirliği her suç tipine göre ayrı ayrı değerlendirilmiştir. Bu değerlen-

in the digital environment varies. When considered as a whole, it is clearly understood that the current law is inadequate in solving such problems occurring today. Although a type of crime in the form of forgery in electronic signatures has been enacted with Law No. 5070, this innovation is only regulated in terms of electronic signatures. However, due to the gap in legislation regarding electronic documents, it is evident that the current law is insufficient in this regard. Indeed, considering the judicial processes that occur in the form of, so to speak, fitting the act to the type of crime, the laws have struggled to fully meet the need for punishing such acts. For this reason, integrating technology into legal systems in order to adapt the law to the age and quickly fill the gaps in the laws will eliminate this problem.

dirmeye göre sahtecilik oluşturan her fiilin dijital ortamda işlenebilirliği değişiklik göstermektedir. Bir bütün halinde ele alındığında ise yürürlükte olan hukukun günümüzde gerçekleşen bu tarz problemleri çözmekte yetersiz kaldığı açıkça anlaşılmaktadır. Her ne kadar elektronik imzada sahtecilik biçiminde bir suç tipi 5070 sayılı Kanun ile yürürlüğe girmiş ise de bu yenilik yalnızca elektronik imza bakımından düzenlenmiştir. Ancak elektronik belgeler bakımından mevzuatta boşluk bulunduğundan dolayı yürürlükteki hukukun bu hususta yetersiz kaldığı aşikardır. Nitekim tabiri caizse fiili suç tipine uydurmak biçiminde gerçekleşen yargılama süreçleri de göz önünde bulundurulduğunda bu tarz fiillerin cezalandırılması hususunda kanunlar ihtiyacı tam anlamıyla karşılamakta zorlanır bir duruma gelmiştir. Bu sebeple hukukun çağa uyum sağlayabilmesi ve kanunlarda yer alan boşlukların hızla dolabilmesi amacıyla teknolojinin hukuk sistemlerine entegre edilmesi söz konusu problemi ortadan kaldıracaktır.

BIBLIOGRAPHY

AHMET GÖKÇEN, Document Forgery Crimes (m.204-212), 4th Edition, Ankara 2016.

DEVİRİM GÜNGÖR, Crime of Forgery of Official Documents, 1st Edition, Ankara 2010.

DOĞAN SOYASLAN, Special Provisions of Criminal Law, 8th Edition, Ankara 2010.

KEMAL GÖZLER, Comment Principles, <https://www.anayasa.gen.tr/yorum-ilkeleri-kitaptan.pdf>. (Last Accessed, 12.01.2025).

MAHMUT KOCA/ İLHAN ÜZÜLMEZ, Turkish Criminal Law Special Provisions, 2nd Edition, Ankara 2015.

MEHMET CAN KARAGÖZ, Blocking the Information System with an Introduction to Information Systems Theory, Crime of Corruption, Destruction or Alteration of Data, 1st Edition, İstanbul 2020.

MEHMET EMİN ÖZGÜL, Rights and Obligations of the Secured Electronic Signature Holder, InÜHFD 12(2): p. 539-556 (2021).

MERT ASKER YÜKSEKTEPE, Document Forgery Crimes with Case Law, 2nd Edition, İstanbul 2021.

ÖZHAN SAĞLIK, Forgery of Electronic Signed Documents: A Review in the Context of Supreme Court Decisions., <https://acikerisim.uludag.edu.tr/server/api/core/bitstreams/499f2a00-753d-4764-9f23-c954c9e3dc5a/content#:~:text=%E2%80%9C-C-Bir%20resmi%20belgeyi%20sahte%20olarak,kadar%20hapis%20cezas%C4%B1%20ile%20cezaland%C4%B1r%C4%B1lmak-tad%C4%B1r,> (Last Accessed, 12.01.2025).

ÜMİT KILINÇ, The Principle of Narrow Interpretation of Restriction in the European Convention on Human Rights, YÜHFD Cilt: XVII Sayı:2, İstanbul 2020.

KAYNAKÇA

AHMET GÖKÇEN, Belgede Sahtecilik Suçları (m.204-212), 4. Baskı, Ankara 2016.

DEVİRİM GÜNGÖR, Resmi Belgede Sahtecilik Suçu, 1. Baskı, Ankara 2010.

DOĞAN SOYASLAN, Ceza Hukuku Özel Hükümler, 8. Baskı, Ankara 2010.

KEMAL GÖZLER, Yorum İlkeleri, <https://www.anayasa.gen.tr/yorum-ilkeleri-kitaptan.pdf>. (Erişim Tarihi, 12.01.2025).

MAHMUT KOCA/ İLHAN ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, 2. Baskı, Ankara 2015.

MEHMET CAN KARAGÖZ, Bilişim Sistemleri Teorisine Giriş İle Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, 1. Baskı, İstanbul 2020.

MEHMET EMİN ÖZGÜL, Güvenli Elektronik İmza Sahibinin Hakları ve Yükümlülükleri, InÜHFD 12(2): s. 539-556 (2021).

MERT ASKER YÜKSEKTEPE, İçtihatlarla Belgede Sahtecilik Suçları, 2. Baskı, İstanbul 2021.

ÖZHAN SAĞLIK, Elektronik İmzalı Belgelerin Sahteciliği: Yargıtay Kararları Bağlamında Bir İnceleme, <https://acikerisim.uludag.edu.tr/server/api/core/bitstreams/499f2a00-753d-4764-9f23-c954c9e3dc5a/content#:~:text=%E2%80%9C-C-Bir%20resmi%20belgeyi%20sahte%20olarak,kadar%20hapis%20cezas%C4%B1%20ile%20cezaland%C4%B1r%C4%B1lmaktad%C4%B1r,> (Erişim Tarihi 12.01.2025).

ÜMİT KILINÇ, Avrupa İnsan Hakları Sözleşmesinde Sınırlamanın Dar Yorumu İlkesi, YÜHFD Cilt: XVII Sayı:2, İstanbul 2020.

FOOTNOTE

²¹ Sağlık, Forgery of Electronic Signed Documents, p. 4.

DİPNOT

²¹ Sağlık, Elektronik İmzalı Belgelerin Sahteciliği, s. 4.