

PAPER DETAILS

TITLE: Bilgi ve İletişim Teknolojileriyle Özel Hayata Karşı İşlenen Suçların Değerlendirilmesi

AUTHORS: Trkay HENKOGLU

PAGES: 143-170

ORIGINAL PDF URL: <https://dergipark.org.tr/tr/download/article-file/2364178>

Bilgi ve İletişim Teknolojileriyle Özel Hayata Karşı İşlenen Suçların Değerlendirilmesi

Türkay Henkoğlu^{*1}

Anahtar Sözcükler

Özel hayat
Gizlilik
Bilgi ve iletişim
teknolojileri
Sosyal medya

Makale Hakkında

Gönderim Tarihi

09 Nisan 2022

Kabul Tarihi

22 Haziran 2022

Yayın Tarihi

28 Aralık 2022

Makale Türü

Araştırma Makalesi

Öz

Elektronik ortamda yer alan bilgilerin işleme süreçlerinde bilginin gizliliğinin korunmaya ihtiyacı olduğu kadar, bu bilgilerin sahipleri olarak kişilerin gizliliğinin de korunmaya ihtiyacı vardır. Elektronik ortamda bilginin işlenmesiyle ilişkili olarak bireylerin özel hayatının korunması hedef alındığında, özel hayata ve hayatın gizli alanına karşı işlenebilecek suçlara yönelik önlemlerin alınması ve/veya bu konudaki hukuksal sorumlulukların yerine getirilmesi önem taşımaktadır. “Özel hayata ve hayatın gizli alanına karşı suçlar” Türk Ceza Kanunu’nun (TCK) dokuzuncu bölümünde 132 ila 140. maddeleri arasında düzenlenmiştir. Bu çalışmada, elektronik ortamlarda özel hayata ve hayatın gizli alanına karşı işlenebilecek suçlara dikkat çekilmesi ve çoğunlukla bilgi teknolojilerinin yardımıyla gerçekleşen bu suçlara ilişkin Yargıtay kararları üzerinden mevcut durumun ortaya konulması amaçlanmıştır. Çalışmada betimleme yöntemi kullanılmış ve çalışma kapsamında, TCK’da “özel hayata ve hayatın gizli alanına karşı suçlar” başlığı altında tanımlanan suçlara yönelik Hukuk Türk bilgi bankası üzerinden erişim sağlanan toplam 129 Yargıtay kararı incelenmiştir. Elde edilen bulgular sonucunda, ilgili suçların bilgi ve iletişim teknolojilerinden yararlanılarak işleme oranlarının yüksek olduğu görülmektedir. Çalışmada bu suçlara ilişkin uygulama, yorumlama ve karar verme süreçlerindeki yanlışlar Yargıtay kararları üzerinden değerlendirilerek, konuya ilişkin karar vericiler ve bilgi profesyonellerine yönelik farkındalığa katkı sağlayacak hususlara dikkat çekilmiştir.

Assessment of Crimes Committed Against Private Life Through Information and Communication Technologies

Keywords

Private life
Privacy
Information and
communication
technologies
Social media

Article Info

Received

April 09, 2022

Accepted

June 22, 2022

Published

December 28,
2022

Article Type

Research Paper

Abstract

In the process of information processing in an electronic environment, the privacy of individuals as the owners of the information need to be protected, as well as the privacy of this information. When it is aimed to protect the private life of individuals in relation to information processing in the electronic environment, it is important to take measures against crimes committed against private life and the secret sphere of private life and/or to fulfill legal responsibilities in this regard. Crimes against private life and the secret sphere of private life are regulated in Section 9 of the Turkish Penal Code (TPC) between Articles 132 and 140. This study, it is aimed to draw attention to the crimes committed against private life and the secret sphere of private life in electronic environments, and to reveal the current situation regarding these crimes, which are mostly committed with the help of information technologies, through the decisions of the Court of Cassation. For this purpose, in the study a total of 129 decisions of the Court of Cassation defined under the title of crimes against private life and secret sphere of private life were analyzed through the descriptive survey research method. As a result of the findings, it is seen that the rate of committing these crimes by using information and communication technologies is high. In the study, by evaluations of mistakes in the implementation, interpretation, and decision-making processes regarding these crimes within the framework decisions of the Court of Cassation, attention is drawn to the issues that will contribute to the awareness of decision-makers and information professionals on the subject.

Atf: Henkoğlu, T. (2022). Bilgi ve iletişim teknolojileriyle özel hayata karşı işlenen suçların değerlendirilmesi. *Bilgi ve İletişim Teknolojileri Dergisi*, 4(2), 143-170. <https://doi.org/10.53694/bited.1100987>

Cite: Henkoğlu, T. (2022). Assessment of crimes committed against private life through information and communication technologies. *Journal of Information and Communication Technologies*, 4(2), 143-170. <https://doi.org/10.53694/bited.1100987>

^{*} Sorumlu Yazar/Corresponding Author turkay.henkoglu@adu.edu.tr

¹ Assist. Prof. Dr., Aydın Adnan Menderes University, Department of Management Information Systems, Aydın/Turkey, turkay.henkoglu@adu.edu.tr, <https://orcid.org/0000-0002-0567-5408>

Introduction

Today, a large part of the information is processed in electronic media, and a large part of "crimes against private life and the confidential sphere of private life" is committed in electronic environment and through information systems. In the process of information processing in an electronic environment, the privacy of individuals as the owners of the information needs to be protected, as well as the privacy of this information. Within the scope of information security, it is possible to say that protecting the privacy of information, it contributes to the protection of individuals' private lives. However, when it is aimed to protect the private life of individuals in relation to information processing in the electronic environment, is necessary to take measures against crimes committed against private life and the secret sphere of private life and/or to fulfill legal responsibilities in this regard. While professional organizations point out the legal regulations on the subject by drawing attention to the increasing threats against private life and the confidential sphere of life in their social media policies, there is no explanatory information about how these crimes are committed and how the legal regulations should be interpreted. In order to respect the private life and the secret sphere of private life in daily life and to reduce the crime rates committed in this regard, it is important to include information on the legal approach to this issue in the daily information that people use practically in their daily lives.

In the study, it is aimed to increase the awareness of decision-makers and information professionals on the subject by revealing the current situation within the framework of the Supreme Court decisions, which facilitate the interpretation of legal regulations and guide in terms of implementation. For this purpose, answers to the following research questions are sought:

- What are the "crimes against private life and the confidential sphere of life" in electronic media?
- Which methods are used to commit crimes against privacy violation, and how many of these crimes are committed by using information and communication technologies?
- What kind of misconceptions or different opinions are encountered in practice regarding crimes committed against private life and the secret sphere of private life by using information and communication technologies?
- What are the decisions and evaluations of the Court of Cassation regarding the crimes against violation of the confidentiality of communication in electronic media, listening of private conversations between individuals by a listening device or recording these conversations, privacy violation, recording personal data, unlawful delivery or acquisition of data, and failing to destroy all copies of the data?

Method

Crimes against private life and the secret sphere of private life are regulated the Section 9 of the Turkish Penal Code (TPC) between Articles 132 and 140. This study, it is aimed to draw attention to the crimes committed against private life and the secret sphere of private life in electronic environments, ad to reveal the current situation regarding these crimes, which are mostly committed with the help of information technologies, through the decisions of the Court of Cassation which are facilitating the interpretation of legal regulations and guiding in terms of their application. For this purpose, in the study a total of 129 decisions of the Court of Cassation defined under the title of crimes against private life and secret sphere of private life were analyzed through descriptive

survey research method. In this way, it is also aimed to increase the awareness of decision makers and information professionals on the subject.

In this context, answers were sought about what are the crimes committed against private life and secret sphere of private life in electronic media, what are the effects of the use of social media and information technologies in violation of privacy of private life and related decision-making processes, how the Court of Cassation made decisions regarding the crimes of violation of privacy of communication in electronic media, listening and recording of conversations between individuals, recording of personal data, and unlawful acquisition or disclosure of data.

As a result of the findings, the extent of the effects of the use of information and communication technologies and social media in the decision-making processes regarding these crimes were revealed. In the study, by revealing the current situation within the framework decisions of the Court of Cassation, which are a guide for interpretation and implementation of legal regulations, attention is drawn to the issues that will contribute to the awareness of decision makers and information professionals on the issues like the crimes of violating the confidentiality of communication, listening and recording of conversations between individuals, violating the privacy of private life, recording personal data, unlawfully giving or obtaining data, and not destroying data.

Discussion and Conclusion

In order not to become a part of the crimes committed against private life and the secret sphere of life or to take adequate measures against these crimes, it is important to have information about the crimes regulated in Section 9 of the Turkish Penal Code (TPC) between Articles 132 and 140. Nowadays, it is possible to say that examining these crimes through information and communication media has become a necessity. It is observed that the rate of these crimes committed with the help of information and communication technologies is very high in the decisions of the Court of Cassation. Also, it is seen that there is an increase in the rate of crimes against private life and the secret sphere of life being committed through social network providers with the widespread use of social media in all institutions and organizations. Legal responsibilities are becoming more important and their reflections on both the person and the relevant institution may be more severe if people who tend to share their private life on social media are public employees. The fact that crimes committed against the privacy of private life are committed mostly through information and communication technologies today leads to make more mistakes in application, interpretation, and criminal decision-making processes. For this reason, it is thought that it would be beneficial for information professionals who process, manage and develop information policies about the information processing in electronic media to take into account the legal conditions and increasing risks regarding the protection of privacy.

Giriş

İnsanoğlu sosyalleşmenin ve paylaşma gereksiniminin bir yansıması olarak toplum içinde iletişim halinde kalmaya çalışırken, aynı zamanda kendisine ait olan ve sadece sınırlı sayıda kişi tarafından bilinmesini istediği bilgilerin korunmasına yönelik arayışını sürdürmektedir. İletişim ve sanal gruplarla etkileşim gereksinimi kişisel kullanımların ötesinde, kurumsal çözüm ve politika geliştirme arayışlarında da hissedilmektedir (Akbaş & Fenerci, 2016; Gülaslan, 2018, s. 180-200; Yalçınkaya, 2020, s. 25). Bu tür çözümler sunulurken, mahremiyetin korunmasının hukuksal sorumluluklar kapsamında garanti altına alınması ya da garanti edilemiyorsa politikalarda bunun açık bir şekilde belirtilmesi gerekmektedir (American Library Association [ALA], 2018, s. 6-7).

Bilgi ve iletişim teknolojilerindeki gelişmeler, sosyalleşme ve sanal gruplarla etkileşimi kolaylaştırırken, özel hayatın gizliliğine yönelik riskleri arttırmaktadır. Elektronik ortamlarda bilginin işleme süreçlerindeki tüm aşamalarda, bilgi ve iletişim teknolojileri kullanılarak özel hayatın gizliliğini hedef alan suçların arttığı bilinmektedir. Bu risklerin azaltılabilmesi için hukuksal düzenlemelerin bilgi ve iletişim teknolojilerindeki gelişmelere bağlı olarak güncellenmesi ve var olan düzenlemelere ilişkin farkındalığın artırılması gerekmektedir. 5237 Sayılı Türk Ceza Kanunu'ndaki (TCK) özel hayata ve özel hayatın gizli alanına karşı işlenen suçlara ilişkin Yargıtay kararlarının bulunduğu 2006-2021 yılları arasındaki süreç dikkate alındığında, bu suçların işlenmesinde kullanılan ve bu suçların işlenmesini kolaylaştıran bilgi ve iletişim teknolojilerine ilişkin durum ortaya konulabilmektedir.

Sosyal medya kullanımının yaygınlaşmasıyla birlikte, “özel hayata ve hayatın gizli alanına karşı suçların” sosyal ağ sağlayıcılar üzerinden işlenmesinin daha kolay hale geldiği görülmektedir. Bu durum, bilginin işlendiği ortamlardaki değişikliğin ve bireylerin bilgi davranışının² doğal bir sonucudur. Sosyal medya kullanımı konusunda bireylerin iş yaşantısı ile özel yaşantısı arasındaki sınırın belirlenerek birbirinden ayrılması da çoğu zaman mümkün olamamaktadır (Gülaslan, 2018, s. 175, 248).

Bilginin kullanılabilirliği için, toplanması, saklanması, paylaşılması ve erişilebilir hale getirilmesi önem taşımaktadır. Bu amaca uygun olarak saklanan ve erişilebilir hale getirilen bilgiler tarihsel süreç içinde değerli hale gelirken, hukuka aykırı olarak elde edilen, saklanan ve dağıtılan bilgiler yaşanmakta olan süreç için sorun haline gelebilmektedir. TCK gerekçesinde de (2004) 135. maddeye ilişkin olarak belirtildiği gibi, çağımızda kişilerle ilgili kayıtlar, kurumlar tarafından bilgisayar ortamlarına aktarılmakta ve muhafaza edilmektedir. Bu bilgilerin önceden belirtilmiş amacın dışında kullanılması ya da üçüncü şahıslar tarafından hukuka aykırı olarak yararlanılması nedeniyle, söz konusu bilgilerin sahipleri telafisi mümkün olmayan zararlara uğrayabilmektedirler. Bu nedenle gündelik yaşamda özel hayata ve özel hayatın gizli alanına karşı saygılı olunması ve bu konuda işlenen suç oranlarının azaltılabilmesi için, kişilerin günlük yaşamlarında pratik olarak kullanmış oldukları ve sezgi ya da sağduyuya dayalı günlük bilgileri³ içinde, günlük yaşamın parçası olarak bu konudaki hukuksal yaklaşıma ilişkin bilgilerin de olması önem taşımaktadır. Böylece kişisel hakların ihlâline neden olmayan, olumlu sonuçlara yol açan kullanımın da desteklenebileceği düşünülmektedir (Junco, 2011, s. 60). Konuya ilişkin kurumsal risklerin arttığı son yıllarda, Türk Kütüphaneciler Derneği (TKD) gibi meslek kuruluşları bünyesinde oluşturulan sosyal

² Bilgi davranışı, bireylerin bilgiye nasıl yaklaştığını ve işlediğini ifade eder. Bireyin bilgiyi araması, kullanması, değiştirmesi, paylaşması, depolaması ve hatta görmezden gelmesi bilgi arama davranışı kapsamında değerlendirilebilir (Davenport, 1997, s. 83).

³ Gündelik bilgi, insanın düşüncelerine, duyu verilerine, kendine özgü yaşam deneyimine, içinde bulunduğu çevrenin geleneklerine bağlı olarak edindiği, çoğunlukla pratik ihtiyaçlarını gidermeğe yönelik olarak ve yaşama uyum sağlamak için kullandığı bilgi türüdür (Gürkan, 2019, s.1).

medya politikalarında da özel hayatın gizliliğine ilişkin hukuksal düzenlemelere dikkat çekildiği görülmektedir (TKD, 2018, s. 6).

Çalışma kapsamında irdelenen ve gündemde sıklıkla yer alan bilgi ve iletişim teknolojileri ile “özel hayata ve özel hayatın gizli alanına karşı işlenen suçlara” ilişkin Yargıtay kararları, elektronik ortamda üretilen bilgilere yönelik olarak nasıl bir tutumun gösterilmesi gerektiği hakkında fikir vermekte ve yol gösterici olabilmektedir. Hukuk ve ceza mahkemeleri kararlarının son merci tarafından karara bağlanmış hali olan Yargıtay kararları, somut olayın özelliğine bağlı olarak uygulamaya yönelik en kapsamlı değerlendirme örneklerini sunan hukuksal kaynaklardır. Yargıtay içtihat metinlerinde yer alan açıklamalar, özel hayatın gizliliğine ve bu konuya yönelik olarak uygulamada tereddütlerin bulunduğu hususların yorumlanmasına yardımcı olan önemli bir kaynak niteliği taşımaktadır. Bu nedenle çalışma kapsamında TCK’nın dokuzuncu bölümünde “özel hayata ve özel hayatın gizli alanına karşı suçlar” şeklinde düzenlenen suçlara yönelik Yargıtay kararları incelenmiştir. Çalışmada öncelikle “özel hayata ve hayatın gizli alanına karşı suçlar” hakkında genel bilgi sunulmuş ve araştırmada kullanılan hukuk bilgi bankası üzerinden erişilen konuya ilişkin tüm Yargıtay kararları incelenerek bu çerçevede değerlendirilmiştir.

Çalışmanın Amacı ve Soruları

Bu çalışmada, “özel hayata ve hayatın gizli alanına karşı suçlara” ilişkin Yargıtay kararları incelenerek, elektronik ortamlarda özel hayata karşı işlenen suçlarda bilgi ve iletişim teknolojilerinin rolü ortaya konulmuştur. Günümüzde bilginin çok büyük bir bölümü elektronik ortamlarda işlendiği gibi, “özel hayata ve özel hayatın gizli alanına karşı işlenen suçların” da büyük bölümü elektronik ortamda ve bilişim sistemleri aracılığıyla işlenmektedir (Tripathi ve diğerleri, 2016, s. 24). Bu durum, yapılacak hukuksal düzenlemelerde, mevcut düzenlemelere ilişkin karar verme süreçlerinde ve bilgi yönetim süreçlerinde, elektronik ortamlarda ve bilişim sistemleri aracılığıyla işlenen bilginin özel hayata yönelik durumunun dikkate alınmasını gerektirmektedir. Bazı mesleki kuruluşlar (TKD, 2018, s. 6) özel hayata ve hayatın gizli alanına karşı artan tehditlere sosyal medya politikalarında dikkat çekerek konuya ilişkin hukuksal düzenlemeleri işaret ederken, bu suçların nasıl işlendiği ve hukuksal düzenlemelerin nasıl yorumlanması gerektiği konusunda açıklayıcı bilgiler bulunmamaktadır. Bu çerçevede, çalışmada doğrudan Yargıtay kararlarını merkeze alarak Ceza Hukuku çerçevesinde değerlendirme yapılmamış, araştırma evreninde yer alan Yargıtay kararları kapsamında bilgi ve iletişim teknolojileriyle özel hayata karşı işlenen suçların incelenmesi hedef alınmıştır.

Çalışmada, hukuksal düzenlemelerin yorumlanmasını kolaylaştıran ve uygulama açısından yol gösterici olan Yargıtay kararları çerçevesinde mevcut durum ortaya konularak, konuya ilişkin karar vericilerin ve bilgi profesyonellerinin farkındalığının artırılması amaçlanmıştır. Bu amaç doğrultusunda aşağıdaki araştırma sorularına yanıt aranmaktadır:

- Elektronik ortamlarda özel hayata ve hayatın gizli alanına karşı işlenen suçlar nelerdir?
- Özel hayatın gizliliğinin ihlâline yönelik suçlar hangi yöntemlerle ve ne kadarı bilgi ve iletişim teknolojileri ile birlikte elektronik ortamlar kullanılarak işlenmektedir?
- Özel hayata ve hayatın gizli alanına karşı bilgi ve iletişim teknolojileri kullanılarak işlenen suçlara ilişkin uygulamada ne tür yanılgılar ya da farklı görüşlerle karşılaşılmaktadır?
- Elektronik ortamlarda haberleşmenin gizliliğini ihlâl, kişiler arasındaki konuşmaların dinlenmesi ve kaydedilmesi, özel hayatın gizliliğini ihlâl, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak

verme ya da ele geçirme ve verileri yok etmeme suçlarına yönelik Yargıtay'ın karar ve değerlendirmeleri nasıldır?

Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar

Özel hayat, kişinin göz önünde olmayan, kamuya kapalı ve diğer insanlardan gizlediği hayatıdır. Bir kişinin gizliliğine her ne şekilde olursa olsun girilmesi, özel hayatın gizliliğinin ihlali olarak değerlendirilmektedir (Hafizoğulları & Özen, 2009). Özel hayat kavramı, kişinin diğer insanlarla paylaşmadığı yaşantısı ve mahremiyeti ile sınırlı olmayıp, herkesin bilmemesi gereken ve/veya istenildiğinde başkalarına açıklanabilen bilgilerin tamamını içermektedir.

Özel hayatın gizliliği ve korunması hakkı, “kişilerin kendi kişiliklerini geliştirmek, manevi değerlerine güvence sağlamak amacıyla diğer insanlar tarafından bilinmesini istemediği hususların oluşturduğu ve buna bağlı olarak da korunması hukuken gerekli olan hayat alanına yönelik temel şahsiyet hakkı” şeklinde tanımlanmaktadır (Yargıtay, 2012b). Bu nedenle, bir görüntü ya da sesin dinlenmesi ve/veya kaydedilmesinin kamuya açık alanda yapılmış olması, buna rıza gösterildiği anlamını taşımamaktadır. Kamuya açık alanlarda kişinin başkalarınca bilinmesini ve/veya görülmesini istemeyeceği tüm faaliyetler özel hayat kavramı kapsamında değerlendirilmektedir. Bir bilginin, özel hayat kavramı kapsamında yer alıp almadığı belirlenirken, içinde bulunulan çevrenin özelliklerinin yanı sıra, kişinin toplum içindeki konumu, mesleği, tanınırlığı, rıza ve öngörülerini ile müdahalenin derecesi de göz önüne alınmalı ve somut olayın özelliğine göre hukuka uygunluk sebeplerinin bulunup bulunmadığı araştırılmalıdır (Yargıtay, 2012a, 2013b).

Özel hayatın gizliliğine yönelik olarak “herkesin özel ve aile yaşamına saygı gösterilmesini isteme hakkı” Anayasa'nın (1982) 20. maddesinde düzenlenmiş ve bu hak Türk Medeni Kanunu'nun 24. ve 25. Maddeleriyle koruma altına alınmıştır. Kişilik haklarına saldırılması durumunda uygulanacak yaptırımlar ise Borçlar Kanunu'nun 49. maddesinde düzenlenmiştir (Yargıtay, 2010).

Bilgi ve iletişim teknolojilerindeki gelişmeler, hukuka aykırı olarak kişilerin özel konuşmalarının dinlenmesine, özel görüntülerinin izlenmesine ve kaydedilmesine olanak sağlamaktadır. Buna yönelik olarak da Anayasa'nın 22. maddesinde haberleşme hürriyeti düzenlenmiş ve korumaya alınmıştır. Anayasa ile garanti altına alınan özel hayata yönelik eylemlerle, kişinin görüntü ve sesinin bilgi ve rızası dışında gizlice kaydedilerek kişilik hakkına zarar verilmesine ilişkin eylemler, TCK'nın 132, 133. ve 134. maddelerinde “haberleşmenin gizliliğinin ihlali”, “kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması”, “özel hayatın gizliliğinin ihlali” başlıkları altında ayrı ayrı suç olarak düzenlenmiş ve yaptırıma bağlanmıştır. Bu kayıtların medya yoluyla kamuoyuna sunulması ise kişilik haklarına yönelik ikinci bir saldırı niteliği taşımaktadır (Yargıtay, 2007). TCK'nın 135. ve 136. maddelerinde ise “kişisel verilerin kaydedilmesi”, “verilerin hukuka aykırı olarak verilmesi ya da ele geçirilmesine” yönelik suçlar tanımlanarak yaptırıma bağlanmıştır.

Avrupa İnsan Hakları Sözleşmesi'nin (1950) 8. maddesinde de kişilerin aile ve özel yaşamına, konutuna ve haberleşmesine saygılı olunmasını isteme hakkının bulunduğu hükmü yer alırken, bu hakkın sınırlandırılmasının “ulusal ve/veya kamu güvenliği, ülkenin ekonomik refahı, suç işlenmesinin önlenmesi, düzenin korunması, sağlığın veya başkalarının hak ve özgürlüklerinin korunması için gerekli olması durumunda mümkün olabileceği” belirtilmiştir.

Haberleşmenin Gizliliğini İhlal

Haberleşmenin gizliliğini ihlâl suçu TCK'nın 132. maddesinde düzenlenmiştir. 132. maddenin birinci fıkrasında kişiler arasındaki haberleşmenin gizliliğinin ihlâli, ikinci fıkrasında ifşası (açığa çıkarılması) yaptırım altına alınmıştır. İlgili maddenin üçüncü fıkrasında ise kişinin tarafı olduğu haberleşmenin içeriğinin açığa çıkarılması suç olduğu düzenlenmiştir. Haberleşme içeriğinin öğrenilmesi, görülmesi, duyulması, dinlenmesi ya da kayıt edilmesi eylemlerinin tamamlanması halinde suç oluşurken, yarım kalması fiili bu suça yönelik teşebbüsü oluşturmaktadır (Hafizoğulları & Özen, 2009, s. 11). Suçun sadece kastla (bilerek ve isteyerek) işlenebilmesi nedeniyle, dikkatsizlik ve özensizlik sonucunda haberleşmenin gizliliğinin ihlâl edilmesi halinde suç oluşmayacaktır.

132. maddenin birinci fıkrasında, en az iki kişinin, diğer insanların bilmemeleri gerektiğini düşünerek ve gizliliği sağlamaya çalışarak, uygun araç (internet, telefon, mektup, kâğıt vd.) ve sembollerle (söz, yazı, işaret vd.) paylaştıkları bilgi ve düşüncelerinin, özel hayata yönelik olsun veya olmasın, özel bir çaba sarf edilerek, doğrudan veya dolaylı şekilde, başka kişiler tarafından, okunmak veya dinlenmek suretiyle öğrenilmesi eylemi suç olarak tanımlanmıştır. Buna göre haberleşenler dışında herkesin bu suçun faili olabilmesine karşın, haberleşmenin tarafı olan kişiler suçun faili olamamaktadır. Haberleşme kişiler arasında sınırlı olduğu için, suçun mağdurları haberleşen kişilerdir (Hafizoğulları & Özen, 2009, s. 10). Birinci fıkrada aynı zamanda, anlaşılabilir olsun ya da olmasın, yazı, ses, görüntü, özel işaretler gibi başkalarının haberleşme içeriklerinin, kâğıt, manyetik bant, bellek vb. nesne üzerine aktararak kaydedilmesi suçun nitelikli şekli olarak tanımlanmıştır. Bu nesneler üzerindeki haberleşmeye ilişkin gizlilik, nesne üzerinde yer alan bilgi ve bu bilginin alıcısı dışında başkaları tarafından öğrenilmesi ile ilgilidir.

132. maddenin ikinci fıkrasında, ilgililerin rızası dışında haberleşme içeriğinin öğrenme yetkisi bulunmayan kişilere yayılması, açığa vurulması ve/veya kamuoyuna duyurulması eylemi suç olarak düzenlenmiştir. Haberleşme içeriği hukuka uygun olarak öğrenilmiş olsa dahi, bu içeriklerin yetkisiz kişilerce öğrenilmesinin sağlanması suçun oluşması için yeterlidir. TCK gerekçesinde de (2004), soruşturma aşamasında haberleşme içeriklerinin televizyonlarda ya da gazetelerde yayınlanmasının, hukuka uygun olarak kayda alınmış olsalar dahi bu suçu oluşacağı belirtilmektedir.

132. maddenin üçüncü fıkrasında ise kişinin kendisiyle yapılan haberleşme içeriğini, ilgililerinin rızası dışında, en az iki kişi tarafından algılanabilme olanağı bulunan aleni ortamda açığa çıkarması eylemi “haberleşmenin gizliliğini ihlâl” suçu çerçevesinde düzenlenmiştir. Bu düzenleme kapsamında suçun oluşması için açığa çıkarmanın alenen yapılmış olması önem taşımaktadır. Bu nedenle TCK gerekçesinde (2004), öğrenilen bilginin ilgili kişinin rızası olmaksızın alenen duyurulması ya da sosyal medya vd. ortamlardan başkalarının erişimine sunulması halinde suçun oluşacağı belirtilmektedir. Açığa çıkarmanın basın ve yayın aracılığıyla yapılması halinde, 132. maddenin dördüncü fıkrası gereğince verilecek cezanın artırılması öngörülmüştür.

Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması

Anayasanın (1982) 22. maddesi gereğince haberleşmenin gizliliği esastır ve hukuksal zorunluluklar olmadıkça, başkaları ile olan konuşmalarının alenileştirilmesine kişiler sadece kendileri karar verirler. “İki veya daha fazla kişinin, belirli sayıda dinleyici çevresi dışına çıkmayacağını düşünerek yüz yüze gerçekleştirdikleri sesli düşünce ve açıklamaları, konuşmanın tarafı olmayan kişilerce, ilgilisinin rızası olmadan, uygun bir aletle (duyulabilir ve/veya algılanabilir hale getirmeye yarayan bir düzenekle) dinlenmesi ya da kaydedilmesi”, TCK'nın 133/1. madde ve fıkrasında suç olarak tanımlanmıştır (Yargıtay, 2014d, 2014c). Burada tanımlanan suç seçimlik hareketli

olmasına karşın, dinleme ve kaydetmenin birlikte yapılması halinde tek bir suç işlenmiş olmaktadır ve temel ceza yüksek tutulmaktadır (Hafizoğulları & Özen, 2009, s. 14). TCK gerekçesinde (2004) aleni olma durumuna ilişkin olarak konuşmanın yapıldığı yerin öneminin olmadığı, özel çaba harcanarak duyulabilmesi durumunda aleni olmayan konuşmanın söz konusu olacağı belirtilmektedir. Bu suçu konuşmanın tarafı olmayan kişi işleyebilmektedir. Kast ile dinleme ya da kaydetme işlemi başladığı anda suç tamamlanmış olarak kabul edilmektedir. Ancak konuşmaları dinlemenin ya da kaydetmenin, bunu mümkün kılan bir aletle yapılmış olması önemlidir. Suçun mağdurları ise aralarındaki konuşmanın dinlenmesi ya da kaydedilmesine rıza göstermeyen kişilerdir. Konuşmayı yapanlardan birinin rızasının olmaması suçun oluşması için yeterli iken, taraflardan birinin rızasının olması suçun oluşmasına engel değildir. Konuşma esnasında hakaret, tehdit veya şantaj içeren sözlerle karşı karşıya kalan ve buna bağlı olarak konuşmaları kaydeden mağdurların bu şekilde elde ettiği delil ise hukuka uygun olarak kabul edilmektedir. Bu noktada kaydetme işleminin gerçekleşmekte olan bir haksız saldırıya karşı yapıldığı, kayıtları takip organlarına verme işlemininse tekrarı mümkün olan haksız saldırıya yönelik olarak yapıldığı düşünülmekte ve her iki hareketin de meşru savunma sınırları içinde gerçekleştiği değerlendirilmektedir (Tezcan ve diğerleri, 2013, s. 545).

TCK'nın 133/2. madde ve fıkrasında ise üç ya da daha fazla kişinin, yüz yüze yapılan ve aleni olmayan söze dayalı düşünce paylaşımının, ilgililerinin rızası bulunmamasına karşın, konuşmanın tarafı olan kişilerce bir ses alma cihazıyla kaydedilmesi suç olarak tanımlanmıştır. Söyleşiye katılanlardan birinin, kayda elverişli bir cihaz ile söyleşinin bir parçasını dahi diğer katılanların rızası olmaksızın kaydetmiş olması, suçun oluşması için yeterlidir.

Kişiler arasındaki aleni olmayan konuşmanın kaydedilmesi yoluyla elde edilen bilgilerin hukuka aykırı olarak açığa çıkarılması eylemi TCK'nın 133/3. madde ve fıkrasında suç olarak düzenlenmiştir (Yargıtay, 2014f, 2014c). TCK gerekçesine (2004) dayalı başka bir ifadeyle, TCK'nın 133/1. ve 133/2. maddesinde tanımlanan suçların işlenerek elde edildiği verilerden yarar sağlanması, üçüncü kişilere verilmesi ya da başkalarının bilgi edinmesinin sağlanması suç olarak tanımlanmıştır. Örneğin birçok kurum ve kuruluşun yardım masası vb. isimler altında destek sunan birimlerinde kaydedilen konuşmaların e-posta vb. araçlarla başkalarına verilmesi bu suç kapsamında değerlendirilmektedir. Bu konuşmaların bir web sayfası üzerinden yayınlanması ise basın ve yayın yoluyla yayımlanması suçunu oluşturmaktadır (Avşar & Öngören, 2010, s. 153). Verilerin basın ve yayın yoluyla yayımlanmasına yönelik olarak TCK'nın 133/3. madde ve fıkrasında belirtilen ceza ile TCK gerekçesinde (2004) öngörülen ceza arasında çelişkiler olmakla birlikte, asıl olan TCK'nın 133/3. madde ve fıkrasında aynı cezaya hükmolunacağı belirtilmektedir. TCK'nın 133. maddesi kapsamında işlenen suçların takibi şikâyeteye bağlıdır.

Özel Hayatın Gizliliğini İhlâl

“Özel hayatın gizliliğini ihlâl” suçları TCK'nın 134. maddesinde düzenlenmiştir. 134. maddenin birinci fıkrasında “özel hayatın gizliliğini ihlâl ve gizliliğin görüntü ve/veya seslerin kayda alınmasıyla ihlâl” suç olarak tanımlanmıştır. İkinci fıkrada kişilerin “özel hayatına yönelik görüntü ya da seslerin hukuka aykırı olarak açığa çıkarılması” suç olarak tanımlanmıştır.

TCK gerekçesinde (2004), hukuka aykırı olarak açığa çıkarılan görüntü ya da seslerin hukuka uygun olarak kayda alınmış olabileceği gibi, birinci fıkrada ifade edilen suçun işlenmesi suretiyle de elde edilmiş olabileceği belirtilmektedir. İkinci fıkrada belirtilen suçun oluşabilmesi için, hukuka aykırı olması ve ses ya da görüntü kayıtlarının açığa çıkarılarak yetkisiz kişiler tarafından öğrenilmesinin sağlanması yeterlidir. Hata ile farklı bir

kişinin özel hayatına yönelik görüntü ve/veya seslerin ihlâl edilmesi halinde, suçun varlığı ortadan kalkmamaktadır.

Özel hayatın gizliliğini ihlâl suçu kastla işlenen, yani failin, bir kişinin özel hayatını ihlâl ettiğini bilerek ve isteyerek davranışına devam ettiği bir suçtur. Gizliliğin görüntü ya da seslerin kayda alınarak ihlâl edilmesi durumunda cezanın alt sınırının ağırlaştırılması öngörülmüştür. Suçun takibi şikâyeteye bağlıdır.

Kişisel Verilerin Kaydedilmesi

Kişisel verilerin korunmasına yönelik düzenlemelerin amacı, kişisel veriler işlenirken özel hayatın gizliliğini ve kişilerin temel haklarını korumaktır. Bunun için kişisel verileri işleyenlerin yükümlülükleri ile uyulması gereken usul ve esaslar düzenlenmektedir (Kişisel Verilerin Korunması Kanunu [KVKK], 2016). TCK gerekçesinde (2004) ve KVKK'nın (2016) 3. maddesinde tanımlanan, “kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilginin hukuka aykırı olarak kaydedilmesi”, TCK'nın 135. maddesinde suç olarak tanımlanmıştır. KVKK'nın gerekçesinde (Kişisel Verileri Koruma Kurumu [KVK Kurumu], 2019) 3. maddeye ilişkin açıklamalarda belirtildiği gibi, ad, soyad ve doğum tarihi gibi kesin teşhisi sağlayan verilerin yanı sıra, kişi ile ilişkilendirilen ve kişiyi belirlenebilir kılan fiziksel, ailevi, psikolojik, ekonomik, sosyal ve kültürel kimliği ifade eden veriler de kişisel veri olarak nitelendirilmektedir. Bilgi ve iletişim teknolojinin gelişimine bağlı olarak, elektronik ortamlarda belirli hizmetleri almak amacıyla edinilen kimlik bilgileri de (e-posta adresi, kullanıcı hesap bilgileri vb.) kişi ile ilişkilendirilmesi halinde bu kapsamda değerlendirilmektedir.

TCK gerekçesinde (2004) belirtildiği gibi, kişisel verilerin bilgisayar ya da kâğıt üzerinde kayda alınması, suçun oluşması açısından önem taşımamaktadır. Suçun meydana gelmesi için kişisel verilerin hukuka aykırı olarak kaydedilmesi gerekirken, ilgili kişinin rızasının bulunması ya da kamu hizmetlerinin gereği olarak kanun hükümlerine istinaden kişisel bilgilerin kayda alınması halinde suç oluşmamaktadır. TCK'nın 135/2. madde ve fıkrasında ise özel nitelikli kişisel veri olarak da nitelendirilen (KVKK, 2016), kişilerin ahlaki eğilimlerine, siyasi, felsefi ya da dini görüşlerine, cinsel yaşamlarına, ırkı kökenlerine, sağlık durumlarına ya da sendikal bağlantılarına yönelik bilgilerin kaydedilmesi suç olarak tanımlanmıştır. Hassas verilerin kaydedilmesine yönelik olarak hukuka aykırılık vurgusunun yapılmamış olması, bu bilgilerin kaydedilmesinin her koşulda hukuka aykırı olduğunu göstermektedir. TCK gerekçesinde (2004), bu bilgilerin suçlulukla mücadelede, suçluların ortaya çıkarılmasını sağlamak amacıyla belli ölçüde kaydedilmesine izin verilebileceği ifade edilmektedir.

Kişisel verilerin hukuka aykırı olarak kayıt altına alınması işlemiyle suç tamamlanmaktadır. Ayrıca bir neticesinin olması gerekmemektedir. “Kişisel verilerin hukuka aykırı olarak kaydedilmesi” suçu kastla işlenen suçlardan olup, eylemin kamu görevlisi tarafından görevin sağladığı yetki kötüye kullanılarak ya da bir mesleğin/sanatın sunduğu kolaylıktan yararlanılarak gerçekleşmesi halinde, TCK'nın 137. maddesi gereğince cezada artırım uygulanması gerekmektedir. Kişisel verilerin kaydedilmesine ilişkin suçlar TCK'nın 139. maddesi gereğince resen takip edilmektedir.

Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme

“Verilerin hukuka aykırı olarak verilmesi ya da ele geçirilmesi”, TCK'nın 136/1. madde ve fıkrasında suç olarak düzenlenmiştir. Bu madde hükmüne göre kişisel verilerin hukuka uygun olarak kaydedilmiş olup olmadığına bakılmaksızın hukuka aykırı olarak elde edilmesi, başkalarına verilmesi ya da yayılması suç olarak tanımlanmıştır (Türk Ceza Kanunu Gerekçesi, 2004; Yargıtay, 2018f). “TCK'nın 135. maddesinde olduğu gibi, 136. maddesinde

de genel olarak korunan hukuki değer kişilerin özel hayatı iken özelde kişisel verilerdir. Kişisel verilerin korunmasına yönelik suçlarda korunan hukuki değer "sır" değil, veri sahibinin kişilik haklarıdır (Dülger, 2004, s. 579). TCK'nın 135. ve 136. maddelerinde sadece sır niteliğini taşıyan kişisel verilerin korunacağına dair bir hüküm bulunmamaktadır. Bununla beraber TCK'nın 135. maddesinin gerekçesinde gerçek kişiye ilişkin tüm bilgilerin kişisel veri olarak kabul edileceği belirtilmektedir. Bu nedenle her türlü kişisel verinin hukuka aykırı olarak ele geçirilmesi, verilmesi veya yayılması halinde TCK'nın 136. maddesinde tanımlanan suçun oluştuğu söylenebilir (Yargıtay, 2018h).

“Kişisel verilerin hukuka aykırı olarak ele geçirilmesi, başkalarına verilmesi ya da yayılması” suçu, genel kastla işlenen suçlardandır (Yargıtay, 2017f). Bu suçlar TCK'nın 139. maddesi gereğince resen takip edilmektedir.

“Haberleşmenin gizliliğini ihlâl”, “kişiler arasındaki konuşmaların kayda alınması ve/veya dinlenmesi”, “kişisel verilerin kaydedilmesi”, “özel hayatın gizliliğini ihlâl” ve “verileri hukuka aykırı olarak verme ya da ele geçirmeye” yönelik suçların kamu görevlisi tarafından görevinin verdiği yetki kötüye kullanılarak ya da bir mesleğin/sanatın sağladığı kolaylıktan yararlanılarak işlenmesi, TCK'nın 137. Maddesi gereğince cezada artırım nedenleri arasında sayılmıştır.

Verileri Yok Etmeme

Kullanılma amaçları yönünden bazı kişisel verilerin saklanma süresi kanunla sınırlandırılabilir. Belirlenen süre sonunda, özel hayata ilişkin gizliliğinin korunması kapsamında bu verilerin yok edilmesi gerekmektedir. Hukuka uygun bir şekilde kaydedilmesine karşın kanunlarda belirlenen süresi geçmiş olan “kişisel verilerin yok edilmemesi”, TCK'nın 138. maddesinde bağımsız bir suç olarak tanımlanmıştır. Elektronik ortamda yer alan verilerin yok edilmesi için tüm kopyalarının kalıcı olarak silinmesi ve bir örneğinin kalmaması gerekmektedir (Akdağ, 2013, s. 148). Verilerin, kullanım süresi aşıldıktan sonra yok edilmesi, suçun varlığını ortadan kaldırmamaktadır. Bunun yanı sıra, suçun tamamlanmış sayılması için bir zararın oluşması şartı bulunmamaktadır.

Verileri yok etmeme suçu, silinme koşulları gerçekleşmesine rağmen bu görevi yerine getirmekle yükümlü kişilerin görevlerini ihmal etmeleri ile gerçekleşmektedir (Şen, 2006, s. 611). Bu nedenle suçun faili, süresi geçmiş olan kişisel verileri yasalar çerçevesinde yok etmekle yükümlü kişilerdir (Akdağ, 2013, s. 144). KVKK'nın (2016) 7. maddesinde, kişisel verilerin işlenmesini gerektiren nedenler ortadan kalktığında, veri sorumlusu⁴ tarafından resen ya da veri sahibinin isteği nedeniyle yok edileceği belirtilmektedir. Bu kanunun 17. maddesinde ise 7. maddeye aykırı olarak bu verileri silmeyen veya anonimleştirmeyenler için TCK'nın 138. maddesinin uygulanacağı belirtilmektedir. Mağdurun bu konuda rıza göstermesi de kastla işlenen bu suçun oluşumuna engel değildir. Süresi geçen verilerin yok edilmemesine ilişkin suçlar TCK'nın 139. maddesi gereğince resen takip edilmektedir.

Yöntem

Araştırmanın Deseni

Özel hayatın gizliliğinin ihlâline yönelik suçların hangi yöntemlerle ve ne kadarının bilgi ve iletişim teknolojileri kullanılarak işlendiğinin, özel hayata ve hayatın gizli alanına karşı bilgi ve iletişim teknolojileri kullanılarak

⁴ Kişisel Verilerin Korunması Kanunu'nun (2016) 3. Maddesinde veri sorumlusu; “kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi” olarak tanımlanmaktadır.

işlenen suçlara ilişkin uygulamada ne tür yanlışların ya da farklı görüşlerin bulunduğu ve Yargıtay'ın bu suçlara ilişkin karar ve değerlendirmelerinin neler olduğunun, HukukTürk bilgi bankası üzerinden erişim sağlanan toplam 129 Yargıtay kararı üzerinden ortaya konulmasını sağlayan bu çalışmada betimleme yöntemi (modeli) kullanılmıştır. Betimleme modeli, geçmişte ya da halen var olan ve araştırma konusunu oluşturan bir durumu herhangi bir müdahalede bulunmaksızın mevcut haliyle betimlemeyi hedefleyen araştırma modelidir (Karasar, 2012, s.77).

Evren ve Örneklem

Araştırmanın evrenini, TCK'da “özel hayata ve hayatın gizli alanına karşı suçlar” başlığı altında tanımlanan suçlara yönelik olarak HukukTürk bilgi bankası üzerinden erişim sağlanan toplam 129 Yargıtay kararı oluşturmaktadır. Yargıtay kararları, hukuk ve ceza mahkemeleri kararlarının son merci tarafından karara bağlanmış hali olması ve uygulama için referans sağlayan hukuksal kaynaklar olması açısından önem taşımaktadır. Çalışmada Yargıtay kararları içinde yer alan açıklamalar, dikkate alınması gereken en önemli kaynaklardan biri olarak özel hayata karşı işlenen suçlara yönelik uygulamada yanlışların ya da farklı görüşlerin olduğu görülen hususların yorumlanmasına yardımcı olmaktadır.

Araştırma evreninde yer alan Yargıtay kararlarının belirlenmesinde HukukTürk bilgi bankasından yararlanılmıştır. HukukTürk bilgi bankası, çalışmanın araştırma amacına uygun olarak kararların madde bazında sınıflandırılmasında kolaylık sağlaması ve madde bazında yapılan aramalarda ilgililiğin yüksek olması nedeniyle tercih edilmiştir. TCK'nın yürürlüğe girdiği 2005 yılından 2022 yılına kadar olan sürece ilişkin olarak, HukukTürk bilgi bankasında bulunan “özel hayata ve hayatın gizli alanına karşı suçlara” yönelik 129 Yargıtay kararı araştırma kapsamında ele alınmıştır. Araştırmada örneklem seçme yöntemine başvurulmamış, araştırma konusu ile ilgili HukukTürk bilgi bankası üzerinde yer alan 129 Yargıtay kararı araştırmaya dahil edilerek tam sayım yöntemi (Lin, 1976, s. 164) kullanılmıştır.

Veri Toplama Süreci

Özel hayata ve hayatın gizli alanına karşı suçların, TCK'nın 132,133,134,135,136. ve 138. maddelerinde düzenlendiği görülmektedir. “Özel hayata ve hayatın gizli alanına karşı suçlar” başlığı altında tanımlanan bu suçlar;

- Haberleşmenin gizliliğinin ihlali,
- Kişiler arasındaki konuşmaların dinlenmesi ve/veya kayda alınması,
- Özel hayatın gizliliğini ihlâl,
- Kişisel verilerin kaydedilmesi,
- Verileri hukuka aykırı olarak verme ya da ele geçirme ve
- Verileri yok etmeme suçlarıdır.

Araştırmada öncelikle bu suçların hangi eylemlerin sonucunda oluşacağı, suçun nasıl ve kimler tarafından işlenebileceği, suçun mağdurunun kim ya da kimler olabileceği, suçun takibinin nasıl yapılacağı ve suça ilişkin yaptırımları içeren hukuksal koşullar hakkında temel bilgi sunulması amaçlanmıştır. Bu nedenle çalışmanın ilk bölümünde TCK madde gerekçeleri ve Yargıtay kararları içindeki açıklamalar ağırlıklı olmak üzere, konuya ilişkin literatürden yararlanılarak bilgi sunulmuştur. Bu kapsamda, yukarıda belirtilen suçlar ayrı alt başlıklar halinde

yapılandırılmıştır. Yargıtay kararları içindeki açıklamalar için, araştırma evrenini oluşturan 129 Yargıtay kararlarına hukuk bilgi bankası üzerinden erişim sağlanmıştır.

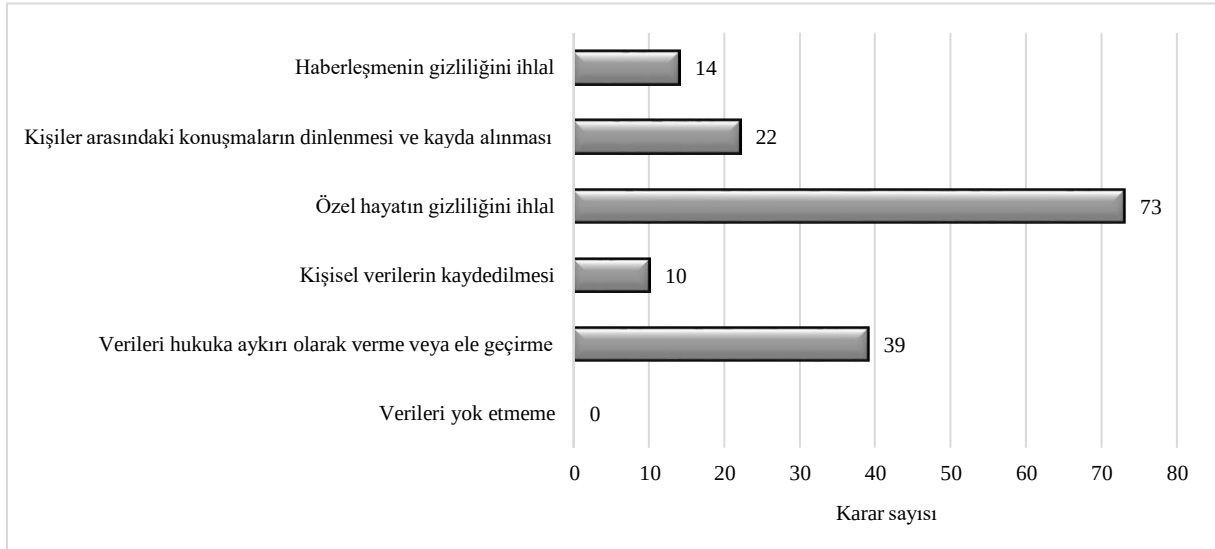
Yargıtay kararlarının araştırma soruları çerçevesinde incelenmesi için, bu çalışmada yararlanılan hukuk bilgi bankası üzerinden erişim sağlanan ve TCK'da “özel hayata ve hayatın gizli alanına karşı suçlar” başlığı altında düzenlenen maddelere ilişkin içeriğe sahip olan 129 Yargıtay kararı tespit edilmiştir. Bu işlem esnasında her madde için ayrı ayrı tespitler yapılmış ve ilgili Yargıtay kararları değerlendirilmek üzere her madde için ayrı ayrı sınıflandırılmıştır. TCK'da ilgili başlık altında yer alan düzenlemelerin madde isimleri, veri toplama ve değerlendirme işlemlerinin daha anlaşılır olması için yapılan sınıflandırmada ve alt başlıkların oluşturulmasında herhangi bir değişiklik yapılmadan kullanılmıştır. Bu aşamada elektronik ortamlarda özel hayata karşı bilgi ve iletişim teknolojileri vasıtasıyla işlenen suçların Yargıtay kararları içindeki ağırlığı ve Yargıtay kararlarında konunun bu yönüne dikkat çeken değerlendirmelerine ilişkin veriler toplanmıştır.

Verilerin Analizi

Araştırma kapsamında toplanan verilerin analizinde yüzde (%) ve frekans (f) gibi betimsel istatistiklerden faydalanılmış, analiz sürecinde “Microsoft® Excel® 2019” programı kullanılmıştır. Değerlendirmeler sonucunda, elektronik ortamlarda “haberleşmenin gizliliğini ihlâl”, “kişisel verilerin kaydedilmesi”, “kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması”, “özel hayatın gizliliğini ihlâl”, “verileri hukuka aykırı olarak verme veya ele geçirme” ve “verileri yok etmeme” suçlarına ilişkin Yargıtay'ın görüş ve değerlendirmeleri ortaya konulmaya çalışılmıştır. Yargıtay öncesindeki süreçlerde, bu suçların nasıl değerlendirildiği ve bu suçların oluşumuna neden olan eylemlere yönelik hangi yaklaşımlar sonucunda yanlışların olduğu tespit edilmiştir. Bununla beraber, incelenen Yargıtay kararları üzerinden, özel hayatın gizliliğinin ihlâlinde ve buna ilişkin karar süreçlerinde, bilgi ve iletişim teknolojilerinin kullanımının hangi boyutlarda olduğuna yönelik fikir edinilmeye çalışılmıştır.

Bulgular

TCK'nın 9. Bölümünde “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlığı altında düzenlenen suç türleri ve her bir suç türünün konusu ile ilgili çalışma kapsamında incelenen kaç adet Yargıtay kararı bulunduğu ilişkin bilgiler Şekil 1 üzerinde gösterilmektedir.



Şekil 1. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlara İlişkin Yargıtay Karar Sayıları

Çalışma bulguları genel olarak suç türlerine ilişkin alt başlıklarda ortak noktalar üzerinden verilirken, konuya ilişkin öğretici bilgi içeren ya da yanlıya neden olan yaklaşımlara ilişkin açıklamaların bulunduğu Yargıtay kararları özel olarak belirtilmiştir.

Haberleşmenin Gizliliğini İhlâl

Haberleşmenin gizliliğinin ihlâl edilmesi ile kişiler arasındaki konuşmaların dinlenmesi ve kayda alınmasına yönelik eylemlerin birçok Yargıtay kararında birlikte değerlendirildiği görülmektedir. Bu nedenle her iki eylem için de geçerli olan ve iç içe geçen açıklamaların bulunduğu Yargıtay kararlarının, "Haberleşmenin Gizliliğini İhlâl" ve "Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması" başlıklı bölümlerde birlikte incelenmesi gerektiği düşünülmektedir. Şekil 1 üzerinde yer alan "haberleşmenin gizliliğini ihlâl" ve "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçlarına yönelik toplam 36 Yargıtay kararının 18'inde (%50), detaylı ve standart bir açıklamanın yapıldığı görülmektedir. Yargıtay (2012e, 2014f, 2014g, 2014b) kararlarından açıkça anlaşıldığı gibi, TCK'nın 132. ve 133. maddesi kapsamında düzenlenen "haberleşmenin gizliliğini ihlâl" ve "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçlarına ilişkin olarak, "kişinin, sonradan kanıt elde etme imkânının olmadığı ve yetkili makamlara başvurma olanağının bulunmadığı ani gelişen durumlarda (örneğin; kendisine karşı işlenmekte olan cinsel saldırı, tehdit, hakaret, şantaj, iftira vb. bir suç söz konusu olduğunda)" hukuka aykırılık bulunmamaktadır. Benzer şekilde, "kendisini ya da aile birliğini hedef alan haksız bir saldırıyı önlemek için, kaybolma riski bulunan kanıtların kaybolmasını engelleyerek ve yetkili makamlara ulaştırarak güvence altına almak için, saldırıyı yapan tarafın rızası ve bilgisi dışında, haberleşme içeriklerini ya da özel hayata yönelik ses ve görüntülerini kaydetme, dinleme ya da izleme eylemleriyle kişisel verileri ele geçirme, kaydetme ve yayma eylemleri" hukuka aykırı olarak kabul edilmemektedir. Esasen bu durumda, kişinin hukuka aykırı olduğu bilinciyle hareket ettiğinden de söz edilemeyeceği belirtilmektedir. TCK'nın 132. maddesi kapsamında haberleşmenin gizliliğini ihlâl suçuna yönelik 14 Yargıtay kararının 6'sında (%43) ve TCK'nın 133. maddesi kapsamında "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçuna ilişkin 22 Yargıtay kararının 7'sinde (%32) bu hususa ilişkin açıklamanın yer aldığı görülmektedir. Ancak bir Yargıtay (2014d) kararında belirtildiği gibi, "önceden hazırlıklı ve planlı şekilde, kaybolma riskleri olan mevcut delilin korunmasını sağlamak için değil, yeni bir delil elde etmek amacıyla hareket edilmesi karşısında TCK'nın

133/2. madde ve fıkrasında tanımlanan kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu oluşmaktadır”.

TCK'nın 132. maddesinde düzenlenen haberleşmenin gizliliğini ihlâl suçu, bir Yargıtay (2014e) kararında da açıklandığı gibi genel kast ile işlenebilen suçlardandır. Bu nedenle 132. maddenin ilk fıkrasındaki suçun manevi unsurunun oluşabilmesi için, “haberleşmenin gizliliğini ihlâl etme” neticesinin bilinmesi ve istenmesi; 132. maddenin ikinci fıkrasındaki suçun manevi unsurunun oluşabilmesi için, kişiler arasındaki haberleşme içeriklerinin taksirle veya tamamen hukuka uygun olarak elde edilmiş olsa dahi, bilerek ve isteyerek açığa çıkarılmış olması gerekmektedir. Bununla beraber, farklı Yargıtay (2012e, 2012d, 2012c, 2014e) kararlarında vurgulandığı gibi, kişinin kendisiyle gerçekleştirilen haberleşme içeriğini kaydetmesi eylemi 132. maddede suç olarak tanımlanmamış olmasına karşın, koşullara bağlı olarak 134. maddenin birinci fıkrasında tanımlanan “özel hayatın gizliliğini ihlâl” suçunu oluşturabildiği görülmektedir. Kişinin tarafı olduğu haberleşmenin içeriğini diğer tarafın rızasını almaksızın açığa çıkarmasına yönelik bir Yargıtay (2014h) kararında ise eylemin TCK'nın 132/3. maddesinde tanımlanan “haberleşmenin gizliliğini ihlâl” suçunu oluşturduğu dikkate alınmadan, uygulama yeri olmayan TCK'nın 134/1. Maddesine göre hüküm⁵ kurulmuş olduğu belirtilmektedir. Buna yönelik Yargıtay kararları üzerinde yapılan detaylı incelemede, Yargıtay süreci öncesinde verilen kararlarda, suçun TCK'nın 132/3. maddesi kapsamında mı yoksa 134/1. maddesi kapsamında mı değerlendirileceğine yönelik tereddütlerin yaşandığı görülmektedir. Haberleşmenin gizliliğini ihlâl suçuna yönelik Yargıtay kararlarının 6'sının (%43) aynı zamanda özel hayatın gizliliğini ihlâl suçu ile ilgili açıklamalar içerdiği görülmektedir. Ayrıca bu 6 kararın Yargıtay tarafından bozulmasına ilişkin sunulan gerekçeler incelendiğinde, 2 kararda suçun nitelendirilmesinde yanlışlığa düşülerek hüküm kurulduğunun açık olarak ifade edildiği görülmektedir.

Haberleşmenin gizliliğini ihlâl suçuna ilişkin olarak incelenen Yargıtay kararlarının sadece ikisinin (%14) eski nesil telsiz ve teyp cihazı ile ilgili olduğu, diğer 12 (%86) kararın ise günümüzde yoğun bir şekilde kullanılan bilgi ve iletişim teknolojileri aracılığıyla ve Facebook, Twitter, MSN gibi sosyal medya araçları da kullanılarak işlenen suçlara yönelik olduğu görülmektedir.

Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması

“Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçuna” ilişkin olarak toplam 22 Yargıtay kararı bulunmaktadır. Bu suça yönelik bir Yargıtay (2014g) kararında, TCK'nın 133/2. madde ve fıkrasında “kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması” başlığı altında tanımlanan suçun oluşabilmesi için, söyleşinin, “aleni olmamasının” gerekli ve yeterli olduğu belirtilmektedir. Başka bir ifadeyle, “belirsiz sayıda kişinin, özel bir çaba harcamadan kolaylıkla duyabileceği şekilde konuşulmaması” yeterli olmakla birlikte, suçun oluşması bakımından konuşma içeriğinin bir önemi bulunmamaktadır. Buna göre, söyleşinin özel yaşam alanı içinde yer alan ve gizlilik taşıyan konular hakkında olabileceği gibi, herkesin bildiği hususlar hakkında da olabileceği belirtilmektedir. Örneğin bir Yargıtay (2018g) kararında belirtildiği gibi, bir kişinin makam odasına gelen ziyaretçilerle yapmış olduğu konuşmalarının gizlice ses alma cihazı ile kayda alınması, TCK'nın 133/1. maddesinde tanımlanmış olan kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçunu oluşturmaktadır.

⁵ Hüküm, mahkemenin önüne getirilmiş olan davayı çözen karardır. Davayı doğrudan çözmesi nedeniyle, bu karar mahkemenin ara karar ı değil son karardır (Çınar, 2009, s. 32).

Söyleşi dışında, iki kişi arasında gerçekleşen bir konuşmada, tarafların kendi aralarında geçen sözleri kayda alması, TCK'nın 133/1. madde ve fıkrası kapsamında değil, koşulları bulunduğu takdirde aynı Kanun'un 134/1. madde ve fıkrasında tanımlanan “özel hayatın gizliliğini ihlâl” suçu kapsamında değerlendirilebilmektedir (Yargıtay, 2014i, 2014f, 2014c, 2018e). Örneğin, sanık ile mağdurun yüz yüze değil, telefon vasıtasıyla görüşmüş olmaları ve sanığın tarafı olduğu haberleşme içeriğini kaydetmesi şeklinde gerçekleşen eylemin, TCK'nın 134/1. madde ve fıkrasındaki “özel hayatın gizliliğini ihlâl” suçu kapsamında değerlendirilebileceği düşünülmektedir (Yargıtay, 2017i). Benzer şekilde diğer Yargıtay (2015g, 2015f) kararlarında, “sanığın, katılan⁶ ile yüz yüze yaptığı, içeriği özel, aleni olmayan konuşmaları katılanın bilgisi ve rızası dışında kaydetmesi eyleminde, bir üçüncü kişinin dahil olmaması ve sanığın tarafı olduğu konuşmayı kaydetmesi sebebiyle”, TCK'nın 134/1. madde ve fıkrasındaki “özel hayatın gizliliğini ihlâl” suçunu oluşturduğu görüşüne yer verilmiştir.

Haberleşmenin gizliliğini ihlâl suçunda olduğu gibi, “kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması” suçuna yönelik olarak yapılan incelemede de Yargıtay süreci öncesinde verilen kararlarda, suçun TCK'nın 133/1. maddesi kapsamında mı yoksa 134/1. maddesi kapsamında mı değerlendirileceğine yönelik tereddütlerin yaşandığı görülmektedir. Bu nedenle “kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması” suçuna yönelik Yargıtay kararlarının 10'unun (%45) aynı zamanda “özel hayatın gizliliğini ihlâl” suçu ile ilgili açıklamalar içerdiği görülmektedir. Bu 10 davada kararın Yargıtay tarafından bozulmasına yönelik gerekçeler incelendiğinde, 6 kararda yasal olmayan gerekçelerle ve suçun vafında yanılığa düşülerek, TCK'nın 134. maddesi yerine TCK'nın 133. maddesi kapsamında hüküm kurulmuş olduğu ya da sanığın tarafı olduğu haberleşme içeriğini kaydetmesi karşısında eylemin TCK'nın 134. maddesinde düzenlenen “özel hayatın gizliliğini ihlâl” suçu kapsamında değerlendirilebileceği açık olarak ifade edilmektedir.

“Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması” suçuna ilişkin olarak incelenen Yargıtay kararlarının 6'sında (%27) sadece ses alma cihazıyla, diğer 16 (%73) kararda ise bilgi ve iletişim teknolojilerinin önemli bir unsuru olarak cep telefonu aracılığıyla konuşmaların dinlendiği ve kayda alındığı görülmektedir. Bununla beraber, 7 kararda (%32) ses kayıtlarının CD ortamına aktarılması amacıyla bilgisayardan faydalanılmış olduğu görülmektedir.

Özel Hayatın Gizliliğinin İhlâl Edilmesi

TCK'nın 9. Bölümünde “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlığı altında düzenlenen suçlara yönelik en fazla Yargıtay kararının (N=73), TCK'nın 134. maddesinde düzenlenen “özel hayatın gizliliğini ihlâl” suçu ile ilgili olduğu görülmektedir. “Özel hayatın gizliliğini ihlâl” suçuna ilişkin toplam 73 Yargıtay kararının 66'sının (%90) bilgi ve iletişim teknolojileri aracılığıyla işlenen suçlara yönelik olduğu ve sosyal medya araçlarının da bu suçların işlenmesinde yoğun bir şekilde kullanıldığı görülmektedir. Diğer 6 (%10) Yargıtay kararında ise suçun işlenmesinde kullanılan araca yönelik açık ifade bulunmadığı için kesin bir bulgu elde edilememiştir. Bu çerçevede, günümüzde özel hayatın gizliliğinin ihlâline yönelik suçların hemen hemen tamamının, bilgi ve iletişim teknolojileri ile birlikte elektronik ortamların kullanılarak işlendiğini söylemek mümkündür.

⁶ “Kamu davasına katılma (müdahale) isteminin yetkili makam (merci) tarafından kabul edilmesi durumunda, istemde bulunan kişiye, katılan (müdahil) denir” (Çınar, 2019).

Özel hayatın gizliliğini ihlâl suçunun ne şekilde işlendiğine ilişkin olarak Yargıtay kararları incelendiğinde, genel olarak güvenlik kameralarının kullanımı ile görüntü veya seslerin kayda alınması ve açığa çıkarılması konularına yönelik suçların internet ortamının sağladığı kolaylıktan yararlanılarak işlendiği dikkat çekmektedir. TCK'nın 134. maddesi kapsamında incelen tüm Yargıtay kararlarında, suçun işlenme şeklini açıklayan konu başlıklarının dağılımı Tablo 1’de görülmektedir.

Tablo 1. Özel hayatın gizliliğini ihlâl suçuna ilişkin Yargıtay kararlarının (n=73) konusunu oluşturan başlıklar

Suçun konusu	n	%
Kişilerin özel hayatına yönelik görüntü ve/veya seslerinin hukuka aykırı olarak açığa çıkarılması.	21	28.7
Gizliliğin görüntü ve/veya seslerin kayda alınarak ihlâl edilmesi.	21	28.7
Kişilerin özel hayatına ilişkin gizliliğin ihlâl edilmesi. Başkalarının görülmesi ve bilinmesi istenmeyen özel yaşantıya müdahalede bulunma.	14	19.1
Kişilerin tarafı olduğu konuşmaların cep telefonu vd. ses alma cihazları kullanılarak gizlice kaydedilmesi.	9	12.3
Olumsuz tutum ve davranışlara yönelik iddiaları ispat etme ve kaybolma riskleri bulunan delillerin korunmasını sağlama amacı ile görüntü veya seslerin kayda alınması.	7	9.5
Güvenlik kamerasının gözetleme amacıyla takılması ve kullanılması.	1	1.3

TCK'nın 134. maddesinde düzenlenen “özel hayatın gizliliğini ihlâl” suçuna ilişkin Yargıtay kararlarının konusunu 6 temel işlenme şekli ile tanımlamak ve sınıflandırmak mümkündür. 134. madde kapsamında işlenen suçların incelenmesi Yargıtay sürecinde bu konu başlıkları kapsamında yapılmasına karşın, doğrudan TCK'nın 134. maddesi ile ilgili olmayan özel hayata ve hayatın gizli alanına karşı diğer suçlara atıfta bulunan kararlar da bulunmaktadır. Örneğin bir Yargıtay (2018e) kararında dinleyicilerin de hazır olduğu bir ortamdaki kişiler arasında aleni olmayan konuşmaların özel hayatın gizliliğini ihlâl edecek bir husus içermediği, benzer bir Yargıtay (2018g) kararında da “suç vasfında yanılığa düşülerek TCK’nın 134/1. maddesi gereğince mahkûmiyet kararının verilmiş olduğu” belirtilmektedir. Bir Yargıtay (2016) kararında ise suç vasfında yanılığa düşmenin yanı sıra suçun nitelikli halini oluşturan mesleğinin sağladığı kolaylıktan yararlanma durumunun dikkate alınmamış olduğu belirtilmektedir. Bu örneklerde olduğu gibi özel hayatın gizliliğini ihlâl suçuna yönelik olarak yapılan incelemelerde Yargıtay süreci öncesinde verilen kararlarda, suçun TCK’nın 132, 133, 135. ve 136. maddeleri kapsamında mı yoksa 134/1. maddesi kapsamında mı değerlendirileceğine yönelik tereddütlerin yaşandığı görülmektedir. Bu nedenle özel hayatın gizliliğini ihlâl suçuna ilişkin Yargıtay kararlarının 29’unun (%40) aynı zamanda TCK’nın 132, 133, 135. ve 136. maddeleri ilgili açıklamalar içerdiği görülmektedir.

TCK’nın 134/1. maddesinde düzenlenen “özel hayatın gizliliğini ihlâl” suçuna yönelik toplam 73 Yargıtay kararları incelendiğinde, bunların 19’unun (%26) sosyal medya üzerinden işlenmiş olduğu görülmektedir. Aynı zamanda elektronik ortamlarda özel hayatın gizliliğine yönelik ihlâl suçlarını konu alan Yargıtay kararları içindeki sosyal medya kullanımı hakkında da fikir veren bu oran, özel hayatın gizliliğinin korunması konusunda sosyal medya ortamının önemini ortaya koymaktadır. TCK’nın 134. maddesine ilişkin suçların sosyal medya ve özellikle yurtdışı kaynaklı yer sağlayıcılar üzerinden işlenmiş olması, zamana bağlı kısıtlılıklar nedeniyle bu suçlara yönelik olarak yapılan adli incelemeler için de zorluklar oluşturmaktadır (Drewer ve Ellermann, 2018, s. 141; Shaw ve diğerleri, 2016, s. 315). Bir Yargıtay (2014k) kararında bu hususa dikkat çekilerek, “Google, Yahoo, Facebook,

Skype, Hotmail, Twitter, Youtube gibi internet ortamında yaygın olarak kullanılan yer sağlayıcı firmaların merkezinin Amerika Birleşik Devletleri'nde (ABD) bulunduğu, ABD mevzuatına göre internet ortamında işlenen suçlara ilişkin trafik bilgilerinin yer sağlayıcılar ya da erişim sağlayıcılar tarafından 90 gün süreyle saklandığı ve bu süre içinde resmi otoritelerce başvurulduğunda anılan saklama süresine 90 gün daha ilave edildiği” belirtilmektedir.

TCK’nın 134. maddesine ilişkin bazı Yargıtay (2015c, 2017a, 2018b) kararları incelendiğinde, Yargıtay öncesi süreçlerde verilen kararlarda, gerçekleşen eylemin TCK’nın 226/3 maddesinde düzenlenen “müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları, temsili çocuk görüntülerini veya çocuk gibi görünen kişileri kullanan kişilerle” ilgili olduğu halde, suç vasfının tayininde yanılığa düşülmüş olduğu ve yazılı şekilde TCK’nın 134/2. maddesiyle mahkumiyete karar verilmiş olduğu görülmektedir. Ancak TCK’nın 44. maddesinde düzenlenen fikri içtima⁷ kuralına göre, “tek eylemle birden fazla suçun oluşması” ya da başka bir ifadeyle gerçekleşen eylemin “müstehcenlik” ve “özel hayatın gizliliğini ihlâl” suçlarını oluşturması nedeniyle, TCK’da bu suçlara dair en ağır cezanın tanımlandığı 226/3 maddesinin uygulanması gerekmektedir.

Özel hayatın gizliliğinin ihlâline yönelik suçlarda, ilgilinin rızasına ilişkin hususların da dikkate alınması önem taşımaktadır. Bir Yargıtay (2017c) kararında, görüntü ve seslerin gizlice kaydedilerek sonradan çekim izninin alınmış olmasının, mağdurun izni öncesinde gerçekleşen eyleme rıza gösterdiği sonucunu doğurmadığı belirtilmektedir.

TCK’nın 134. maddesine ilişkin suçların soruşturulması ve kovuşturulması, TCK’nın 139/1. maddesi gereğince şikâyet tabidir. Bu konuya ilişkin örnek Yargıtay (2015d, 2017e, 2017b) kararlarında, “kovuşturmada şikâyet koşulunun gerçekleşmemesi sebebiyle sanık hakkındaki davanın düşmesine karar verilmesi gerektiği” belirtilmektedir.

TCK’nın 134. maddesine ilişkin Yargıtay kararlar incelendiğinde, olumsuz tutum ve davranışlara yönelik iddiaları ispat etme ve kaybolma riskleri bulunan delillerin korunmasını sağlama amacı ile görüntü veya seslerin kayda alınması durumuna dikkat çekilen Yargıtay kararları olduğu görülmektedir. Örneğin bir Yargıtay (2015e) kararında, “sanığın iddiasını ispatlama amacını taşıyan eyleminde hukuka aykırı hareket ettiği bilinciyle hareket etmediğinin anlaşılması nedeniyle, özel hayatın gizliliğini ihlâl suçundan beraatına karar verilmesi” gerektiğine dikkat çekilmiş, benzer bir Yargıtay (2015b) kararında da bu gerekçeyle sanığın beraatına karar verilmesinde isabetsizlik görülmemiştir.

Kişisel Verilerin Kaydedilmesi

TCK’nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesine yönelik 10 Yargıtay kararının 5’inin (%50), TCK’nın 134. ve 136. maddelerinde tanımlanan suçlarla ilişkili olduğu görülmektedir. Bu nedenle kişisel verilerin kaydedilmesine yönelik eylemlerin, “özel hayatının gizliliğini ihlâl” ve “kişisel verilerin hukuka aykırı olarak verilmesi ya da ele geçirilmesi” suçları ile birlikte değerlendirilmesi gerektiği düşünülmektedir. Bununla beraber incelenen Yargıtay kararlarının 9’unda (%90), söz konusu eylemlerin elektronik ortamlar ve bilgi

⁷ Fikri içtima: “İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişinin, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılmasıdır” (TCK, 2004, s. 8974).

teknolojileri kullanılarak gerçekleştirildiği görülmektedir. Bu durum, kişisel verilerin kaydedilmesine yönelik suçlarda elektronik ortamların kullanımına yönelik tercihler ve kullanım kolaylığı hakkında fikir vermektedir.

TCK'nın 135. maddesinde “hukuka aykırı olarak kişisel verilerin kaydedilmesi” suçu düzenlenmiş olmakla birlikte, eylemin TCK'nın 134. maddesinde düzenlenen “özel hayatın gizliliğini ihlâl” suçu kapsamında da değerlendirilmesi önem taşımaktadır. Nitekim bir Yargıtay (2015a) kararında mahremiyete ilişkin görüntülerin kaydedilmesi ve açığa çıkarılması eyleminin “kişisel verilerin kaydedilmesi” suçunu değil, TCK'nın 134/1. maddesinin 2. cümlesi ve 134/2. maddesine uyan “özel hayatın gizliliğini ihlâl” suçlarını oluşturacağı belirtilmektedir. Bununla beraber, bu suçların soruşturulması ve kovuşturulmasının TCK'nın 139. maddesi gereğince şikâyetle bağlı olduğunun göz ardı edilmemesi gerekmektedir.

Yargıtay kararları TCK'nın 135. maddesi kapsamında incelendiğinde, eylemin hangi durumlarda TCK'nın 134/1. ve 134/2. maddesi kapsamında değerlendirileceği ve TCK'nın 135. maddesinde tanımlanan suçtan nasıl ayırt edileceği konusunda örneklerin bulunduğu görülmektedir. Bir Yargıtay (2014a) kararında, “özel hayata ilişkin görüntü ya da seslerin kişisel veri olarak nitelendirilmesinde şüphe bulunmamakla birlikte, kişinin özel hayatına ilişkin görüntü veya sesinin kaydedilmesi suretiyle ihlâl edilmesi ya da rızası dışında yayılması, açığa çıkarılması, ilan edilmesi yoluyla içeriği öğrenme yetkisi olmayan kişilerin bilgisine sunulmasının özel hayatın gizliliğini ihlâl suçu kapsamında TCK'nın 134. maddesinde düzenlendiği” ifade edilmektedir. Bu nedenle anılan kararda, “kişinin özel hayatına ilişkin görüntüsü, fotoğrafı ya da sesinin, yasal anlamda TCK'nın 135. maddesi kapsamında kişisel veri olarak değerlendirilemeyeceği” belirtilmektedir. Ayrıca, “kişinin özel yaşam alanı içerisinde yer almayan görüntüsü, fotoğrafı ya da sesinin rızaya aykırı olarak kaydedilmesi veya kullanılmasının kişilik hakkının ihlâli olarak değerlendirilmesi ve bu tür eylemlerin özel hukuk yaptırımlarına konu olabileceği” ifade edilmektedir.

TCK'nın 135, 136. ve 138. maddelerine ilişkin suçların soruşturulması ve kovuşturulması, TCK'nın 139/1. maddesi gereğince şikâyetle tabi değildir. Bu konuya ilişkin örnek bir Yargıtay (2013a) kararında, verileri hukuka aykırı olarak verme veya ele geçirme suçunun, soruşturulması ve kovuşturulmasının şikâyetle bağlı olmadığı gözetilmeden, kovuşturma aşamasında mağdurların şikâyetlerinden vazgeçtiklerinden bahisle davanın düşmesine karar verilmesinin kanuna aykırı olduğu belirtilmektedir.

Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme

Araştırmada elde edilen veriler doğrultusunda, verileri hukuka aykırı olarak verme ya da ele geçirmeye yönelik Yargıtay öncesi süreçlerde verilen kararlarda, bu çalışmada incelenen özel hayata ve hayatın gizli alanına karşı işlenen diğer suçlarla ilgili daha fazla yanlışlığa düşüldüğü görülmektedir. Örneğin bir Yargıtay (2018d) kararında, gündelik elbiselerle çekilmiş fotoğrafın ve ad-soyadı bilgilerinin kişisel veri niteliğinde olması nedeniyle bu verilerin hukuka aykırı olarak verilmesine ilişkin eylemde “TCK'nın 136. maddesi kapsamında hüküm kurulması gerekirken, delillerin takdirinde hataya düşülerek TCK'nın 134/2. maddesinde düzenlenen özel hayatın gizliliğini ihlâl suçuna ilişkin hüküm kurulmuş olduğu” belirtilmektedir. Başka bir Yargıtay (2018c) kararında da buna ilâve olarak, daha önce Facebook üzerinden yayımlanmış olmasının kişisel veri olma özelliğini değiştirmeyeceği ve üçüncü kişilere veri sahibinin rızası dışında bu resimleri yayımlama hakkı tanımayacağı vurgulanmaktadır. Benzer şekilde TCK'nın 136. maddesi ile ilgili olarak araştırma kapsamında incelenen 39 Yargıtay kararının 9'unda (%23), Yargıtay süreci öncesinde verilen kararlarda yanlışlığa düşülmüş olduğu ifade edilmektedir.

“Verileri hukuka aykırı olarak verme veya ele geçirme” suçuna yönelik olarak incelenen 39 Yargıtay kararının 28’inde (%72), söz konusu eylemlerin elektronik ortamlar ve bilgi teknolojileri kullanılarak gerçekleştirildiği görülmektedir. Banka veya kredi kartlarının kötüye kullanılması suçları doğrudan bu çalışma konusu ile ilgili olmamakla birlikte, kredi kartı kopyalama araçları da bu orana dahil edildiğinde, elektronik ortamların bu suçun işlenmesindeki kullanım oranının %98’e çıktığı görülmektedir. Bu verilere bağlı olarak, “kişisel verilerin hukuka aykırı olarak verilmesi ya da ele geçirilmesine” ilişkin suçların hemen hemen tamamının elektronik ortamlarda gerçekleştiğini söylemek mümkündür.

TCK’nın 136/1. madde ve fıkrasının, “bu madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır” şeklindeki gerekçesi dikkate alındığında, kişisel verilerin verilmesi ya da ele geçirilmesi için kaydedilmiş olması ve bu haliyle başkalarına verilmesi ya da ele geçirilmesi gerekmektedir (Yargıtay, 2018f). Bu çerçevede kişisel verilerin kaydedilmiş olarak bellek vb. nesne üzerine taşınması gibi istenildiğinde tekrar kullanılabilmesine olanak sağlayan faaliyetler, “kişisel verileri ele geçirme” kapsamında değerlendirilebilmektedir. Ancak kişisel verilerin kaydedilmeden önce öğrenilerek, yazılı/basılı ve elektronik ortamlara aktarılmadan başkalarına açıklanması ve bu verilere sadece duyu organlarıyla vâkıf olunması, TCK’nın 134/1. madde ve fıkrasında düzenlenen “özel hayatın gizliliğini ihlâl” suçu kapsamında değerlendirilmektedir (Yargıtay, 2018f).

“Verileri hukuka aykırı olarak verme veya ele geçirme” suçu, seçimlik hareketli bir suç olarak düzenlendiği için, kişisel verilerin hukuka aykırı olarak başkasına verilmesi, ele geçirilmesi ve yayılması şeklindeki seçimlik hareketlerin birinin gerçekleştirilmesiyle suç oluşmaktadır. Bu soyut tehlike suçunun oluşabilmesi için herhangi bir neticenin gerçekleşmesi gerekmemektedir. Seçimlik harekette elden, internet üzerinden ya da diğer elektronik ortamlarda başkalarına (gerçek ya da tüzel kişilere) verilen verilerin hukuka aykırı veya uygun olarak elde edilmiş olmasının bir önemi bulunmamaktadır. Bu noktada verme eyleminin hukuka aykırı olması önem taşımaktadır (Yargıtay, 2017h). Bunun yanı sıra, bir Yargıtay (2018a) kararında kolaylıkla ulaşılabilecek ya da bilinmesi mümkün olan kişisel bilgilerin de “kişisel veri” olarak kabul edildiğine dikkat çekilerek, uygulamada belirsizlik oluşturmaması ve her eylemin suça dönüşmemesi için somut olayın özelliklerinin dikkate alınmasının ve “sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerektiğinin” önemine vurgu yapılmaktadır. Örneğin bir kişinin nüfus cüzdanını ele geçirmedeki kastının kişisel verileri depolama ve yaymak olup olmaması, suçun yasal unsurlarının oluşması açısından önem taşımaktadır.

TCK’nın 134/1. ya da 136. maddelerinin uygulanması açısından dikkat edilen önemli unsurlardan biri de rızanın varlığıdır. Bir Yargıtay (2017g) kararında, “bazı fotoğrafların daha önce mağdurun rızasına uygun olarak sosyal paylaşım sitesinde yayımlanmış olması nedeniyle, özel yaşam alanına ilişkin ve özel hayatının gizliliğini ihlâl edecek nitelikte görüntüler olarak kabul edilemeyeceği” vurgulanmaktadır. Daha sonra bu fotoğrafların rızaya aykırı olarak (söz konusu fotoğrafların mağdur tarafından silinmesinin istenmesine rağmen) yayımlanmaya devam edilmesi durumunda ise TCK’nın 136/1. maddesindeki “kişisel verileri hukuka aykırı olarak yayma” suçunu oluşturacağı belirtilmektedir.

“Verileri hukuka aykırı olarak verme veya ele geçirme” suçunun internet ve sosyal medya üzerinden işlenme durumuna yönelik olarak, daha önce veri sahibi tarafından paylaşılmış olması ve paylaşılan verinin kişisel veri niteliğinin dikkate alınması önem taşımaktadır. Sosyal medya ile ilgili en sık karşılaşılan sorun, sosyal ağ profili

sayfalarında yayınlanan materyaldir (Lenartz, 2012, s. 29). Bu hususa ilişkin bir Yargıtay (2014j) kararında, “Facebook’taki herkes tarafından görülebilen profil resminin hukuk tarafından gizliliği ve korunması temel bir şahsiyet hakkı kabul edilmiş özel yaşam alanına dair bir görüntü olarak kabul edilemeyeceği” vurgulanmaktadır. Bununla beraber, bir kişiye ait herkese açık Facebook profil resminin kopyalanarak başka bir kişi tarafından rıza olmaksızın kendi Facebook hesabında yayımlanmasına yönelik olarak, başkaca bir kişisel bilgiye yer verilmemesi halinde, hukuka aykırı olarak ele geçirme ve yaymadan da söz edilemeyeceği belirtilmektedir. Ancak hukuka aykırı yöntemlerle profil resminin sahte Facebook hesabı üzerinden yayımlanması, TCK’nın 136/1. maddesinde tanımlanan “verileri hukuka aykırı olarak verme veya ele geçirme” suçunu oluşturmaktadır. Ayrıca resimlerin Facebook gibi görsel, işitsel ve elektronik kitle iletişim araçları üzerinden belirsiz sayıda kişinin görgüsüne sunulması, TCK’nın 6/1-g maddesi uyarınca cezada artırım yapılmasını gerektirmektedir (Yargıtay, 2017d).

TCK’nın 136. maddesi kapsamında yapılan incelemelerde, kredi kartı ile ilişkili olarak bilgilerin kopyalanması, sahte kredi kartının oluşturulması ve bu kartların kullanılarak yarar sağlanması konusunda, Yargıtay süreci öncesinde tereddütlerin bulunduğu görülmektedir. Bu konuya açıklık getiren bir Yargıtay (2018i) kararında, ele geçirilen kopyalama cihazında kart bilgileri kopyalanarak bir kart oluşturulmasına ilişkin delillerin bulunması halinde ilgili bankanın suçtan zarar gören taraf olduğu dikkate alınarak TCK’nın 245/2. Maddesi kapsamında uygulama yapılması gerektiği belirtilmektedir. Anılan kararda, kart bilgilerinin kopyalanması suretiyle yeni bir kart oluşturulmamasına karşın ele geçirilen ilgili kopyalama cihazı üzerinde bilgi bulunması durumunda, TCK’nın 136. maddesi uyarınca “kişisel verileri hukuka aykırı olarak ele geçirme” suçunu oluşturacağı belirtilmektedir.

Verileri Yok Etmeme

TCK’nın 137. maddesi kapsamında yapılan Yargıtay kararlarına ilişkin incelemede, suçun bir kamu görevlisi tarafından ve görevinin sağladığı yetkinin kötüye kullanılmasıyla veya belli bir sanatın/mesleğin sağladığı kolaylıktan yararlanılarak işlendiği toplam 7 Yargıtay kararının olduğu görülmektedir. Bu kararların, TCK’nın 132, 133, 134. ve 135. maddeleri ile ilişkili olarak verildiği anlaşılmaktadır.

Araştırma kapsamında incelenen Yargıtay kararlarında, TCK’nın 138. maddesinde düzenlenen “verileri yok etmeme” suçuna yönelik bir Yargıtay kararının bulunmadığı görülmektedir. Bu suçun ihmal yoluyla işlenebileceği göz önüne alındığında, verilerin yok edilmesi konusunda yükümlülüğü bulunan bilgi profesyonellerinin ya da diğer veri sorumlularının bu konuda ihmallerinin bulunmadığı yönünde bir çıkarımda bulunulabilir. Ancak diğer taraftan, verilerin yok edilmesi konusuna son yıllarda kişisel verilerin korunmasına yönelik çalışmalarla dikkatlerin yoğunlaştığı da göz ardı edilmemelidir. Başka bir ifadeyle, araştırmada bu konuda Yargıtay kararlarına ulaşılmamış olması, kanaatimizce verilerin süresi içinde yok edildiğini ve bu konuda sorunların bulunmadığını söylemek için yeterli değildir.

Tartışma ve Sonuç

TKD (2010) mesleki etik ilkelerinde de belirtildiği gibi, çalışanların uyması gereken norm ve kurallar çerçevesinde kurum ve kuruluşlarda özel hayatın gizliliğinin korunması için bilgi güvenliğine ilişkin önlemler alınmaktadır. Ancak bilgi güvenliği önlemleri kapsamında bilginin gizliliğinin korunması, veri sahiplerine yönelik özel hayatın korunmasına dolaylı ve sınırlı olarak katkı sağlamaktadır. Bu nedenle son yıllarda mesleki kuruluşlarda sosyal medya politikalarının geliştirilmesine yönelik çalışmalar (TKD, 2018) yürütülürken, “özel hayata ve hayatın gizli alanına karşı suçlarla” ilgili hukuksal düzenlemelere de dikkat çekildiği görülmektedir. “Özel hayata ve hayatın

gizli alanına karşı işlenen suçların” bir parçası haline gelmemek ya da bu suçlara karşı yeterli önlemleri alabilmek için, TCK’nın 9. Bölümünde 132 ila 140. maddeleri arasında düzenlenen suçlara yönelik bilgi sahibi olmak önem taşımaktadır. Ancak hukuksal düzenlemelerde, kişisel verilerin kaydedilmesi gibi örneklere ilişkin olarak her eylemin suç oluşturmaması ve uygulamada belirsizlik yaratılmaması amacıyla, düzenlemelerin amacından fazla genişletilmemesine özen gösterildiği görülmektedir. Bu nedenle eylemlerin suç olarak nitelendirilmesi ya da uygun suç tanımı ile eşleştirilmesi, somut olayın özelliklerinin titizlikle değerlendirilmesini gerektirmektedir. Literatürde kullanılan özel hayatın gizliliğine yönelik fiziki koşullarda gözetleme, karıştırma vb. örneklerin aksine, günümüzde bu suçların bilgi ve iletişim ortamları üzerinden incelenmesinin zorunlu hale geldiği görülmektedir. Özel hayatın gizliliğine yönelik suçların günümüzde daha çok bilgi ve iletişim teknolojileri aracılığıyla işlenmesi, uygulama, yorumlama ve suça yönelik karar verme süreçlerinde daha fazla yanılgıya düşülmesine neden olabilmektedir. Bu nedenle, örneklere bağlı olarak Yargıtay’ın görüş ve değerlendirmeleri hem hukuksal işlemlerin takibi hem de benzer durumlarla karşılaşma olasılığı bulunan bilgi profesyonelleri için önem taşımaktadır.

Çalışmada incelenen Yargıtay kararlarının dağılımı dikkate alındığında, özel hayatın gizliliğinin ihlâl edilmesi ve haberleşmenin gizliliğini ihlâl suçlarının bilgi ve iletişim teknolojilerinden yararlanılarak işlenme oranlarının çok yüksek olduğu görülmektedir. Sosyal medya kullanımının tüm kurum ve kuruluşlarda yaygınlaşmasıyla birlikte, “özel hayata ve hayatın gizli alanına karşı suçların” sosyal ağ sağlayıcılar üzerinden işlenme oranında da artış olduğu görülmektedir (Bahar, 2018, s.25; FBI, 2021). Junco’nun (2011, s. 60) da belirttiği gibi, sosyal medya üzerinden yapılan paylaşımlardaki içeriğin kişisel haklara yönelik ihlaller içermesi ve internet üzerinde hızla yayılması, yüz yüze yapılan iletişime göre daha kolay ve olağan bir durumdur. Buna karşın, bireylerin sosyal medya üzerindeki ifade özgürlüğü ile çevrimiçi saldırılar karşısındaki hakları arasındaki dengenin sağlanması ya da sınırların belirgin olarak çizilebilmesi çoğu zaman kurumlar için zorlayıcı olabilmektedir (Lenartz, 2012, s. 32). Sosyal medya üzerinden özel hayata ilişkin paylaşım eğilimleri olan kişilerin kamu çalışanı olması halinde, hukuksal sorumluluklar daha önemli hale gelmekte ve hem kişiye hem de ilgili kuruma yansımaları daha ağır olabilmektedir. Bu nedenle, elektronik ortamlarda işlenen bilgi ve bu bilgileri işleyen, yöneten ve bilgi politikaları geliştiren bilgi profesyonellerinin, özel hayatın gizliliğinin korunmasına yönelik hukuksal koşulları ve artan riskleri dikkate almalarının yararlı olacağı düşünülmektedir.

Yargıtay kararlarına dayalı bulgular mutlak doğrular olarak kabul edilmemekle birlikte, farklı zamanlarda verilen kararlarda belirgin hale gelen görüşlere dayalı çıkarımda bulunulabilmektedir. Bu çalışmada erişim sağlanan Yargıtay kararları üzerinden yapılan incelemeye bağlı olarak, elektronik ortamlarda özel hayatın ve hayatın gizli alanının korunması amacıyla zaman ve mekân sınırı olmaksızın herkes tarafından göz önüne alınmasının faydalı olacağı düşünülen başlıca hususlar şunlardır;

- Kişinin daha sonra kanıt elde etme imkânının olmadığı ve yetkili makamlara başvurma olanağının bulunmadığı ani gelişen durumlarda yapmış olduğu kayıtlar için, haberleşmenin gizliliğine yönelik hukuka aykırılık bulunmamaktadır.
- Haksız saldırıyı önlemek ve kaybolma ihtimali bulunan delillerin yetkili makamlara ulaştırılarak güvence altına almak amacıyla, haberleşme içeriklerini izleme, dinleme ya da kaydetme eylemleri ile kişisel verileri ele geçirme, kaydetme ve/veya yayma eylemlerinde hukuka aykırılık bulunmamaktadır.
- Bilerek ve isteyerek haberleşmenin gizliliği ihlâl edilmemeli ve kişiler arasındaki haberleşme içerikleri açığa çıkarılmamalıdır.

- Özel bir çaba harcamadan rahatlıkla duyulamayan ve algılanamayan kişiler arasındaki konuşmalar, özel bir çaba ile dinlenmemeli ve kayda alınmamalıdır.
- Söyleşi dışında iki kişi arasında gerçekleşen bir konuşmada, konuşan taraflardan birinin konuşma içeriğini diğerinin izni olmadan kaydetmesi özel hayatın gizliliğinin ihlâline neden olmaktadır.
- Görüntü ve seslerin gizlice kaydedilerek sonradan çekim izninin alınmış olması, mağdurun izni öncesinde gerçekleşen eyleme rıza gösterdiği anlamını taşımamaktadır.
- Kişinin özel hayatına ilişkin görüntü ya da sesinin kayda alınarak ihlâl edilmesi ya da rızası dışında yayılması, açığa çıkarılması, ilan edilmesi yoluyla içeriğe erişim yetkisi olmayan kişilerle paylaşılması, özel hayatın gizliliğinin ihlâline neden olmaktadır.
- Kişisel verilerin hukuka aykırı olarak ele geçirilmesi, kaydedilmesi, verilmesi ya da ve süresi geçmiş olan verileri yok etmeme suçlarının takibi şikâyetle bağlı değildir. Bu nedenle mağdurların şikâyetlerinden vazgeçmesi takibi sona erdirmeyecektir.
- Kişisel verilerin kaydedilmesi, bir yerden başka bir yere transfer edilmesi vd. işlemlere ilişkin hukuka aykırılığı ortadan kaldıran hususlar KVKK'da detaylı olarak düzenlenmiştir.
- Gündelik yaşama ait ve kişisel veri niteliği taşıyan verilerin hukuka aykırı olarak verilmesine ilişkin eylemler “özel hayatın gizliliği” değil, “verileri hukuka aykırı olarak verme veya ele geçirme” suç kapsamında değerlendirilmektedir.
- Daha önce sosyal medyada yayınlanan bir kişisel veri, veri sahibinin rızası dışında üçüncü kişilere yayımlanmamalıdır.
- Sosyal medyada herkes tarafından görülebilen içerik, özel yaşam alanına dair bir içerik olarak kabul edilmemektedir.

Yayın Etiği Bildirimi / Research Ethics

Yazar araştırmanın etik dışı bir sorunu olmadığını, araştırma ve yayın etiği konusunu gözlemlediğini beyan etmektedir. / The author declares that the research has no unethical problem, and observe the research and publication ethics.

Araştırmacıların Katkı Oranı / Contribution Rate of Researchers

Çalışmanın her aşamasına yazar katkı sunmuştur. / The author provide the contribution rates to each stage of the study.

Çıkar Çatışması / Conflict of Interest

Çalışmada herhangi bir çıkar çatışması bulunmamaktadır. / The study has no conflict of interest.

Fon Bilgileri / Funding

Bu çalışmada herhangi bir fon kullanılmamıştır. / There is no funding for this study.

Etik Kurul Onayı / The Ethical Committee Approval

Etik kurul kararı: Bu arařtırmada, tüm arařtırmacılara açık, uluslararası veri tabanında yer alan veriler kullanıldığından etik kurul kararı gerektirmemektedir. / The Ethical Committee Approval: This research does not require an ethics committee decision, since data in an international database open to all researchers are used.

Kaynakça / References

- American Library Association [ALA]. (2018). Social media guidelines for public and academic libraries. <http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/smg2018.pdf>
- Akbaş, M. ve Fenerci, T. (2016). Üniversite kütüphanelerinde sosyal medya politikaları [Social media policies in university libraries]. *Bilgi Dünyası / Information World*, 17(2), 201-231. <https://www.bd.org.tr/index.php/bd/article/download/63/57>
- Akdağ, H. (2013). *Türk Ceza Kanunu kapsamında kişisel verilerin korunması*. Adalet Yayınevi.
- Avrupa Konseyi. (1950). Avrupa İnsan Hakları Sözleşmesi. http://www.echr.coe.int/Documents/Convention_TUR.pdf
- Avşar, Z. ve Öngören, G. (2010). *Bilişim hukuku*. Türkiye Bankalar Birliği.
- Bahar, A. (2018). Bilişim suçları, iletişim ve sosyal medya [Cyber crimes, communication and social media]. *İstanbul Aydın Üniversitesi Dergisi*, 10(3), 1-36. https://iaud.aydin.edu.tr/wp-content/uploads/2018/07/iaud_v10i3001.pdf
- Çınar, A. (2009). Hükmün konusu ve eylemi (fiili) değerlendirmede mahkemenin yetkisi. *Türkiye Barolar Birliği Dergisi* (84), 31-62. <http://tbbdergisi.barobirlik.org.tr/m2009-84-542>
- Çınar, A. R. (2019). Ceza yargılamasında kamu davasına katılma [Participation in the trial in criminal procedure]. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 21(Özel S.), 2801-2836. <https://hukuk.deu.edu.tr/wp-content/uploads/2019/09/ALI-RIZA-CINAR.pdf>
- Davenport, T. H. (1997). *Information ecology: Mastering the information and knowledge environment*. Oxford University Press.
- Drewer, D. ve Ellermann, J. (2018). The Online Environment as a Challenge for Privacy and the Suppression of Crime. M. B. J. Biasiotti M., Cannataci J., Turchi F. (Ed.), *Handling and Exchanging Electronic Evidence Across Europe* (Cilt. 39, s. 141-148) içinde. Springer. https://doi.org/10.1007/978-3-319-74872-6_8
- Dülger, M. V. (2004). *Bilişim suçları ve internet iletişim hukuku*. Seçkin Yayınevi.
- FBI (2021). Internet crime report. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
- Gülaslan, T. (2018). Kamu yönetiminde sosyal medya kullanımı ve yönetimi: Temel ilkeler ve öneriler [Usage and administration of social media in public administration: Basic principles and recommendations]. [Hacettepe Üniversitesi]. Ankara. http://www.openaccess.hacettepe.edu.tr:8080/xmlui/bitstream/handle/11655/5022/Kamu%20Y%c3%b6netiminde%20Sosyal%20Medya%20Kullan%c4%b1m%c4%b1%20ve%20Y%c3%b6netimi_Temel%20c4%b0lkeler%20ve%20c3%96neriler.pdf?sequence=1&isAllowed=y
- Gürkan, Ü. (2019). *Hukuk sosyolojisine giriş* (10 bs.). Siyasal Kitabevi.
- Hafizoğulları, Z. ve Özen, M. (2009). Özel hayata ve hayatın gizli alanına karşı suçlar. *Ankara Barosu Dergisi*, 67(4), 9-22. <https://dergipark.org.tr/en/download/article-file/397650>

- Junco, R. (2011). The need for student social media policies. *EDUCAUSE Review*, 46(1), 60-61.
<https://er.educause.edu/-/media/files/article-downloads/erm1118.pdf>
- KVK Kurumu. (2019). Madde ve gerekçesi ile kişisel verilerin korunması kanunu (bilgi notu) ve kişisel verilerin korunmasına ilişkin terimler sözlüğü. KVKK Yayınları.
- KVKK. (2016). Kişisel Verilerin Korunması Kanunu. <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>
- Lenartz, A. J. (2012). All my rowdy “friends”: The use of social media in higher education [Northern Arizona University]. San Francisco.
<https://www.proquest.com/docview/1019989172/fulltextPDF/76CC47A714C14120PQ/1?accountid=11248>
- Lin, N. (1976). *Foundations of Social Research*. McGraw-Hill.
- Shaw, U., Das, D. ve Medhi, S. P. (2016). Social network forensics: Survey and challenges. *International Journal of Computer Science and Information Security*, 14(11), 310-316.
https://www.academia.edu/30916542/Social_Network_Forensics_Survey_and_Challenges
- Şen, E. (2006). *Yeni Türk Ceza Kanunu Yorumu*, Cilt 1. Vedat Kitapçılık.
- T.C. Anayasası. (1982). Türkiye Cumhuriyeti Anayasası.
<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf>
- TCK. (2004). Türk Ceza Kanunu. <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf>
- Tezcan, D., Erdem, M. R. ve Önok, R. M. (2013). *Teorik ve pratik ceza özel hukuku*. Seçkin Yayıncılık.
- Tripathi, E., Tripathi, A. ve Yadav, M. K. S. (2016). Role of information technology in cyber crime and ethical issues in cyber ethics. *International Journal of Business and Research*, 10, 21-25.
http://www.ijber.in/list_volume10.html
- Türk Ceza Kanunu Gerekçesi. (2004). Türk Ceza Kanunu Genel Gerekçesi. <https://legalbank.net/belge/madde-1-ila-345-turk-ceza-kanunu-genel-gerekce/2677278>
- Türk Kütüphaneciler Derneği [TKD]. (2010). Türk Kütüphaneciler Derneği Mesleki Etik İlkeleri.
<http://kutuphaneci.org.tr/wp-content/uploads/2019/11/Mesleki-Etik-%C4%B0lkeleri.jpg>
- Türk Kütüphaneciler Derneği [TKD]. (2018). Kütüphaneler için sosyal medya politikası.
<http://kutuphaneci.org.tr/wp-content/uploads/2018/03/K%C3%BCt%C3%BCphaneler-%C4%B0%C3%A7in-Sosyal-Medya-Politikas%C4%B1-TKD-Sosyal-Medya-Politikalar%C4%B1-%C3%87a%C4%B1%C5%9Fma-Grubu.pdf>
- Yalçınkaya, B. (2020). Geleceğin arşivlerinin inşası: Sosyal medyanın arşivlenmesi hakkında bir değerlendirme [Building archives of the future: An evaluation of archiving social media]. *Bilgi Yönetimi / Information Management*, 3(1), 25-38. <https://dergipark.org.tr/tr/download/article-file/1112219>
- Yargıtay. (2007). Yargıtay kararı (Esas No: 2006 / 13723, Karar No: 2007 / 13089).
<https://www.hukukturk.com/Goster?v=GE95G5nVYZ6>

- Yargıtay. (2010). Yargıtay kararı (Esas No: 2009 / 8119, Karar No: 2010 / 7573).
<https://www.hukukturk.com/Goster?v=GE95G6nuHmC>
- Yargıtay. (2012a). Yargıtay kararı (Esas No: 2011 / 7345, Karar No: 2012 / 8936).
<https://www.hukukturk.com/Goster?v=GE95G8XoKe0>
- Yargıtay. (2012b). Yargıtay kararı (Esas No: 2011 / 20872, Karar No: 2012 / 9834).
<https://www.hukukturk.com/Goster?v=GE95G8dUJFI>
- Yargıtay. (2012c). Yargıtay kararı (Esas No: 2012 / 13117, Karar No: 2012 / 14791).
<https://www.hukukturk.com/Goster?v=GE95G77Ima8>
- Yargıtay. (2012d). Yargıtay kararı (Esas No: 2012 / 13228, Karar No: 2012 / 14787).
<https://www.hukukturk.com/Goster?v=GE95G9OmzmC>
- Yargıtay. (2012e). Yargıtay kararı (Esas No: 2012 / 20608, Karar No: 2012 / 18217).
<https://www.hukukturk.com/Goster?v=GE95G5UCHku>
- Yargıtay. (2013a). Yargıtay kararı (Esas No: 2012 / 22005, Karar No: 2013 / 24489).
<https://www.hukukturk.com/Goster?v=GE95G5Z0uno>
- Yargıtay. (2013b). Yargıtay kararı (Esas No: 2012 / 32005, Karar No: 2013 / 15770).
<https://www.hukukturk.com/Goster?v=GE95G6AQfJo>
- Yargıtay. (2014a). Yargıtay kararı (Esas No: 2013 / 9669, Karar No: 2014 / 3760).
<https://www.hukukturk.com/Goster?v=GE95G7TIhIO>
- Yargıtay. (2014b). Yargıtay kararı (Esas No: 2013 / 13614, Karar No: 2014 / 5809).
<https://www.hukukturk.com/Goster?v=GE95G7Rp80e>
- Yargıtay. (2014c). Yargıtay kararı (Esas No: 2013 / 15779, Karar No: 2014 / 7263).
<https://www.hukukturk.com/Goster?v=GE95G7VEJZQ>
- Yargıtay. (2014d). Yargıtay kararı (Esas No: 2013 / 20481, Karar No: 2014 / 10220).
<https://www.hukukturk.com/Goster?v=GE95G74VXyC>
- Yargıtay. (2014e). Yargıtay kararı (Esas No: 2013 / 21755, Karar No: 2014 / 13367).
<https://www.hukukturk.com/Goster?v=GE95G7jzSKm>
- Yargıtay. (2014f). Yargıtay kararı (Esas No: 2013 / 22599, Karar No: 2014 / 12706).
<https://www.hukukturk.com/Goster?v=GE95G7gru4>
- Yargıtay. (2014g). Yargıtay kararı (Esas No: 2013 / 26087, Karar No: 2014 / 10205).
<https://www.hukukturk.com/Goster?v=GE95G7oX2Po>
- Yargıtay. (2014h). Yargıtay kararı (Esas No: 2014 / 1714, Karar No: 2014 / 18859).
<https://www.hukukturk.com/Goster?v=GE95G77YjYG>
- Yargıtay. (2014i). Yargıtay kararı (Esas No: 2014 / 2511, Karar No: 2014 / 17251).
<https://www.hukukturk.com/Goster?v=GE95G7FVVC4>

- Yargıtay. (2014j). Yargıtay kararı (Esas No: 2014 / 4081, Karar No: 2014 / 19490).
<https://www.hukukturk.com/Goster?v=GE95G7bFSwC>
- Yargıtay. (2014k). Yargıtay kararı (Esas No: 2014 / 7409, Karar No: 2014 / 24197).
<https://www.hukukturk.com/Goster?v=GE95G7MJsJc>
- Yargıtay. (2015a). Yargıtay kararı (Esas No: 2014 / 11530, Karar No: 2015 / 584).
<https://www.hukukturk.com/Goster?v=GE95G7sJsBM>
- Yargıtay. (2015b). Yargıtay kararı (Esas No: 2014 / 13474, Karar No: 2015 / 3).
<https://www.hukukturk.com/Goster?v=GE95G85qZLk>
- Yargıtay. (2015c). Yargıtay kararı (Esas No: 2014 / 19535, Karar No: 2015 / 4333).
<https://www.hukukturk.com/Goster?v=GE95G8IKv4a>
- Yargıtay. (2015d). Yargıtay kararı (Esas No: 2014 / 22101, Karar No: 2015 / 2153).
<https://www.hukukturk.com/Goster?v=GE95G8JTJaq>
- Yargıtay. (2015e). Yargıtay kararı (Esas No: 2015 / 81, Karar No: 2015 / 7817).
<https://www.hukukturk.com/Goster?v=GE95G7uYBma>
- Yargıtay. (2015f). Yargıtay kararı (Esas No: 2015 / 14885, Karar No: 2017 / 3121).
<https://www.hukukturk.com/Goster?v=GE95G75uzWS>
- Yargıtay. (2015g). Yargıtay kararı (Esas No: 2015 / 17241, Karar No: 2017 / 4259).
<https://www.hukukturk.com/Goster?v=GE95G6Eb9Ye>
- Yargıtay. (2016). Yargıtay kararı (Esas No: 2015 / 5128, Karar No: 2016 / 10207).
<https://www.hukukturk.com/Goster?v=GE95G9Oi360>
- Yargıtay. (2017a). Yargıtay kararı (Esas No: 2014 / 9227, Karar No: 2017 / 4650).
<https://www.hukukturk.com/Goster?v=GE95G7xDBC4>
- Yargıtay. (2017b). Yargıtay kararı (Esas No: 2015 / 10834, Karar No: 2017 / 192).
<https://www.hukukturk.com/Goster?v=GE95G9aI1nE>
- Yargıtay. (2017c). Yargıtay kararı (Esas No: 2015 / 11084, Karar No: 2017 / 636).
<https://www.hukukturk.com/Goster?v=GE95G9bQQJU>
- Yargıtay. (2017d). Yargıtay kararı (Esas No: 2015 / 11112, Karar No: 2017 / 637).
<https://www.hukukturk.com/Goster?v=GE95G6kJpLM>
- Yargıtay. (2017e). Yargıtay kararı (Esas No: 2015 / 12554, Karar No: 2017 / 413).
<https://www.hukukturk.com/Goster?v=GE95G9dhDM0>
- Yargıtay. (2017f). Yargıtay kararı (Esas No: 2015 / 13248, Karar No: 2017 / 3108).
<https://www.hukukturk.com/Goster?v=GE95G5wNFb6>
- Yargıtay. (2017g). Yargıtay kararı (Esas No: 2017 / 150, Karar No: 2017 / 6231).
<https://www.hukukturk.com/Goster?v=GE95G5YOyFk>

- Yargıtay. (2017h). Yargıtay kararı (Esas No: 2017 / 829, Karar No: 2017 / 363).
<https://www.hukukturk.com/Goster?v=GE95G7lmY9w>
- Yargıtay. (2017i). Yargıtay kararı (Esas No: 2017 / 4667, Karar No: 2018 / 3187).
<https://www.hukukturk.com/Goster?v=GE95G6Db0VM>
- Yargıtay. (2018a). Yargıtay kararı (Esas No: 2015 / 1659, Karar No: 2018 / 2748).
<https://www.hukukturk.com/Goster?v=GE95G8OicW8>
- Yargıtay. (2018b). Yargıtay kararı (Esas No: 2016 / 13170, Karar No: 2018 / 439).
<https://www.hukukturk.com/Goster?v=GE95G9SZHe4>
- Yargıtay. (2018c). Yargıtay kararı (Esas No: 2017 / 2960, Karar No: 2018 / 1541).
<https://www.hukukturk.com/Goster?v=GE95G7qbSK0>
- Yargıtay. (2018d). Yargıtay kararı (Esas No: 2017 / 7385, Karar No: 2018 / 3977).
<https://www.hukukturk.com/Goster?v=GE95G6JGz6e>
- Yargıtay. (2018e). Yargıtay kararı (Esas No: 2017 / 10732, Karar No: 2018 / 9468).
<https://www.hukukturk.com/Goster?v=GE95G8jD2TA>
- Yargıtay. (2018f). Yargıtay kararı (Esas No: 2017 / 12083, Karar No: 2018 / 2539).
<https://www.hukukturk.com/Goster?v=GE95G5zyGGG>
- Yargıtay. (2018g). Yargıtay kararı (Esas No: 2018 / 2226, Karar No: 2018 / 8746).
<https://www.hukukturk.com/Goster?v=GE95G8kNuQi>
- Yargıtay. (2018h). Yargıtay kararı (Esas No: 2018 / 3318, Karar No: 2018 / 9281).
<https://www.hukukturk.com/Goster?v=GE95G8TH1kG>
- Yargıtay. (2018i). Yargıtay kararı (Esas No: 2018 / 6171, Karar No: 2018 / 10436).
<https://www.hukukturk.com/Goster?v=GE95G9KfXXc>
-