

**T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

**TÜRK CEZA HUKUKUNDA
BİLİŞİM SİSTEMİNE
GİRME SUÇU**

YÜKSEK LİSANS TEZİ

Ahmet Alper AYDIN

Tez Danışmanı: Doç. Dr. E. Eylem AKSOY RETORNAZ

HAZİRAN 2022

**T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

**TÜRK CEZA HUKUKUNDA
BİLİŞİM SİSTEMİNE
GİRME SUÇU**

YÜKSEK LİSANS TEZİ

Ahmet Alper AYDIN

Tez Danışmanı: Doç. Dr. E. Eylem AKSOY RETORNAZ

HAZİRAN 2022

ÖNSÖZ

Bu çalışmada Türk Ceza Kanunu'nun 243. maddesinde düzenlenen bilişim sistemine girme suçu incelenmiştir. Bilişimle ilişkili teknik tanım ve açıklamaların yanı sıra doktrindeki görüşler ve yargı kararlarına da çalışmada yer verilerek incelenen suç tüm yönleriyle açıklanmaya çalışılmıştır.

Gerek konu belirleme gerekse tezin yazım sürecinin her aşamasında yanımda olarak benden hiçbir zaman desteğini esirgemeyen değerli danışmanım Doç. Dr. E. Eylem AKSOY RETORNAZ'a en içten teşekkürlerimi sunarım. Kuşkusuz ki kendisinin emeği, desteği ve sabrı olmasaydı bu çalışma da olmazdı. Prof Dr. Pınar MEMİŞ KARTAL ve Dr. Öğr. Üyesi Osman Gazi GÜÇLÜTÜRK'e ise hem tez jürime katılarak beni onurlandırdıkları hem de verdikleri geri bildirimlerle tezime sundukları katkılar için teşekkür ederim.

Beraber çalıştığımız süreçte bana her türlü desteği gösteren ve tezime vakit ayırabilmem için ellerinden geleni yapan kıymetli mesai arkadaşlarım Av. Açelya YÜKSEL, Av. Aslı KOÇAK KALDIRIM, Av. Helin Dilar ÇETİN ve Av. Timur Arif ÇAPKIN'a verdikleri destekler için şükranlarımı sunuyorum. Tezimi baştan sona okuyarak hatalarımı düzeltmeme yardımcı olan Mehmet Emre KANAT'a da ayrıca teşekkür ederim. Benim için çok stresli ve zorlu geçen bu süreçte sıklıkla başlarımı ağrıttığım değerli dostlarım Mahmut YATI, Mustafa YILDIZ ve Sencer AYDEMİR'e ise gösterdikleri dostluk için minnettarım.

Beni bu günleri getiren sevgili annem Mine AYDIN ve babam Selami AYDIN'a ise ne kadar teşekkür etsem yetersiz kalır. Gösterdikleri sevgi, emek ve özveri olmasaydı ne bugün olduğum insan olabilirdim ne de bu çalışmayı yapabilirdim. Sevgili kardeşim Mehmet Eren AYDIN'a da gerek yüksek lisans yaptığım süreçte verdiği destek için teşekkür ederim. Son olarak ise ihtiyacım olan her zaman yanımda olan ve hayatı benim için anlamlı kılan sevgili eşim ve yol arkadaşım Ayşenur Kanat AYDIN'a tüm kalbimle teşekkür ederim.

İÇİNDEKİLER

ÖNSÖZ.....	i
İÇİNDEKİLER.....	ii
KISALTMALAR.....	v
LE RÉSUMÉ	vii
ABSTRACT	xii
ÖZET	xvii
GİRİŞ.....	1
I. TEMEL KAVRAMLAR	5
A. Bilişim.....	5
B. Bilişim Sistemi ve Bilgisayar.....	6
1. Bilgisayar.....	6
2. Bilişim Sistemi	8
C. Bilişim Suçu.....	11
1. Terim Sorunu.....	11
2. Bilişim Suçlarının Tanımlanması ve Sınıflandırılması	15
D. Veri.....	18
E. İnternet	20
II. TARİHİ GELİŞİM.....	22
A. Uluslararası Hukukta Bilişim Suçlarının Tarihi Gelişimi.....	22
1. Bilgisayar ve Bilişim Suçlarının Tarihi Gelişimi	22
2. Avrupa Konseyi Siber Suç Sözleşmesi	24
B. Türkiye’de Bilişim Suçlarının Tarihi Gelişimi	27
1. 765 Sayılı Türk Ceza Kanunu Dönemindeki Durum	27
2. 5237 Sayılı Türk Ceza Kanunu Hazırlık Süreci.....	29
3. 5237 Sayılı TCK’da Bilişim Sistemine Girme Suçu.....	32

III. KORUNAN HUKUKİ DEĞER	35
IV. SUÇUN UNSURLARI	38
A. Maddi Unsur.....	38
1. Fail.....	38
2. Mağdur	41
3. Suçun Konusu.....	43
4. Hareket	48
5. Netice.....	57
6. Teşebbüs.....	59
B. Manevi Unsur.....	61
C. Hukuka Aykırılık Unsuru.....	66
1. Genel Olarak.....	66
2. Kanun Hükmünün Yerine Getirilmesi.....	71
3. Meşru Savunma.....	75
4. Hakkın Kullanılması.....	78
5. İlgilinin Rızası	79
D. Suçu Etkileyen Nedenler.....	85
1. Hafifletici Nedenler.....	86
2. Ağırlaştırıcı Nedenler	91
E. Suçun Netice Sebebiyle Ağırlaşmış Hali	92
V. SUÇLARIN BİRLEŞMESİ VE İŞTİRAK	95
A. Suçların Birleşmesi	95
B. İştirak.....	102
VI. YAPTIRIM VE YARGILAMA.....	103
A. Yaptırım	103
B. Yargılama.....	105
SONUÇ.....	108

KAYNAKÇA	122
ÖZGEÇMİŞ.....	140



KISALTMALAR

ABD.:	Amerika Birleşik Devletleri
a.g.e.:	Adı Geçen Eser
a.g.m.:	Adı Geçen Makale
AİHM:	Avrupa İnsan Hakları Mahkemesi
AİHS:	Avrupa İnsan Hakları Sözleşmesi
Alm.:	Almanca
AKSSS:	Avrupa Konseyi Siber Suç Sözleşmesi
AYM:	Anayasa Mahkemesi
C.:	Cilt
CD.:	Ceza Dairesi
Der.:	Derleyen
CMK:	Ceza Muhakemeleri Kanunu
DEÜHFD:	Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi
E.T.:	Erişim Tarihi
E.:	Esas Numarası
Fra.:	Fransızca
FSEK:	Fikir ve Sanat Eserleri Kanunu
İÜHFM:	İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
İng.:	İngilizce
K.:	Karar Numarası
PVSK:	Polis Vazife Ve Salâhiyet Kanunu
s.:	Sayfa

S.:	Sayı
T.:	Tarih
TBMM:	Türkiye Büyük Millet Meclisi
TCK:	Türk Ceza Kanunu
TDK:	Türk Dil Kurumu
TÜİK:	Türkiye İstatistik Kurumu
Yar.:	Yargıtay
YCGK:	Yargıtay Ceza Genel Kurulu
YHGK:	Yargıtay Hukuk Genel Kurulu

LE RÉSUMÉ

Le sujet de cette thèse est le crime d'accès non autorisé au système informatique réglementé à l'article 243 du Code pénal turc n° 5237. Dans le premier paragraphe de l'article, la forme simple du crime, dans le deuxième paragraphe, la situation nécessitant moins de peine, et dans le troisième paragraphe, le crime aggravé en raison du résultat est réglementé. Afin de comprendre les cybercrimes et de prendre une décision équitable dans des événements concrets, il est d'une importance vitale de définir les systèmes d'information soumis au crime et les éléments de ces systèmes. Pour cette raison, les concepts d'ordinateur, de système d'information, de données et d'internet de notre étude ont été examinés. Les caractéristiques techniques de ces concepts sont précisées ; puis les définitions faites dans la doctrine et la législation ont été examinées. Afin de mieux comprendre la situation dans la pratique de ces concepts, qui sont apparus comme l'objet ou les outils de la cybercriminalité, les décisions de la Cour suprême sont également incluses dans cette section. Toujours dans cette section, l'accent est mis sur le concept de cybercriminalité, qui peut être considéré comme un nouveau concept de droit pénal. Tout d'abord, des approches différentes dans la littérature internationale et dans la doctrine de notre pays sur la dénomination de ces crimes ; Ensuite, les définitions et classifications faites sont examinées.

Dans la section suivante, il s'agit d'examiner l'évolution historique de l'informatique et des délits informatiques. Tout d'abord, le développement des cybercrimes qui ont émergé aux États-Unis, qui sont aussi la patrie des ordinateurs, et les études menées par les pays pour prévenir ces crimes sont mentionnés. Ensuite, le processus de préparation de la Convention du Conseil de l'Europe sur la cybercriminalité, qui est le document international le plus important et le plus complet préparé sur la cybercriminalité, et les articles liés au crime que nous examinons sont soulignés. Ensuite, les études réalisées pour l'entrée des cybercrimes dans la législation de notre pays et les articles relatifs aux cybercrimes ajoutés au Code pénal turc n° 765 ont été examinés. Les projets préparés pour faire un nouveau code pénal dans le cadre de la réforme pénale turque et les articles liés à la cybercriminalité dans ceux-ci ont également été inclus dans notre étude. Enfin, le processus de préparation du Code pénal turc n° 5237, dans lequel le délit d'accès non autorisé au système informatique a été réglementé pour la première fois dans notre pays, et les modifications apportées à cette loi ont été soulignées.

Sur le transfert des informations de base sur les concepts et le contexte historique au lecteur ; L'analyse de l'accès non autorisé au système informatique réglementé à l'article 243 du Code pénal turc a été lancée. Différents points de vue ont été exprimés dans la doctrine quant à la valeur juridique que l'on cherche à protéger par le délit d'accès non autorisé au système informatique. Les auteurs ont affirmé qu'il visait à protéger ensemble une ou plusieurs des valeurs telles que la propriété, la vie privée, la liberté de communication, les données personnelles et la sécurité du système. A notre avis, la valeur juridique à protéger par ce crime est uniquement la sécurité des systèmes d'information. Le législateur a protégé d'autres intérêts avec différents crimes dans le

Code pénal turc. La valeur que l'on veut protéger dans des formes simples est la sécurité du système d'information. En raison de la nature du troisième paragraphe, la valeur protégée sont les données dans le système.

Toute personne réelle peut être l'auteur de ce crime. Les personnes morales, en revanche, ne peuvent pas être des auteurs au sens du droit pénal. Toutefois, les mesures de sécurité prévues à l'article 60 du CPP peuvent être prononcées pour les personnes morales qui tirent profit de la commission de l'infraction. Bien qu'il n'y ait aucune obligation dans la loi d'avoir une profession ou un statut particulier pour commettre des délits informatiques, on constate que ces délits sont généralement commis par des pirates informatiques appelés "hackers". La victime du crime est la personne qui a des droits sur le système et qui a un accès direct au système. Les personnes qui ont été légalement autorisées à accéder au système par le propriétaire du système peuvent également être victimes de ce crime. Sans aucun doute, des personnes réelles peuvent être victimes de ce crime. Le statut des personnes morales est controversé. Certains auteurs soutiennent que les personnes morales ne peuvent pas être des victimes, mais peuvent être lésées par le crime. Les auteurs, auxquels nous avons également participé, ont affirmé qu'aucune disposition du Code pénal turc n'empêche les personnes morales d'être victimes ; affirment qu'ils peuvent aussi être des victimes. Dans la mesure où cela convient à la nature du délit, les personnes morales peuvent également être victimes du délit d'accès non autorisé au système informatique.

qui ne peuvent faire qu'un certain travail, comme les lecteurs de codes-barres, les appareils électroménagers et les distributeurs de café. L'objet du délit d'accès non autorisé au système informatique est celui des systèmes d'information. Ces systèmes, qui peuvent être utilisés à des fins générales, peuvent traiter, transférer et stocker des données entre eux. Les appareils machines, ne sont pas considérés comme des systèmes d'information. Aujourd'hui, les guichets automatiques, qui peuvent se connecter à Internet et effectuer de nombreuses transactions bancaires, sont considérés comme des systèmes d'information. Ordinateurs, smartphones, tablettes sont les systèmes d'information les plus courants. Sont également considérés comme des systèmes d'information les sites Internet, les applications de médias sociaux, les adresses e-mail, les bases de données en ligne et les plateformes qui fournissent des services de jeux vidéo, qui ne sont pas connectés à un certain matériel et accessibles à distance. Les serveurs de cloud computing, qui sont entrés dans la vie de l'humanité ces dernières années, et les systèmes intelligents fonctionnant avec l'internet des objets sont également considérés comme des systèmes d'information. Dans l'article 243 du Code pénal turc, il est réglementé que l'infraction peut être commise à l'encontre de tout ou partie du système d'information ; par conséquent, une certaine partie du système ou un appareil connecté au système peut également faire l'objet de ce crime. Par exemple, un certain dossier dans le système d'information ou une mémoire externe connectée au système peut également faire l'objet du crime. Le sujet du crime qui nécessite moins de punition est les systèmes d'information qui peuvent être utilisés pour un prix. Le sujet de l'aggravation du crime en conséquence est les données du système.

Un crime sera commis si l'auteur accomplit l'un des actes d'entrée ou de séjour dans le système d'information. L'acte d'entrer peut être effectué en touchant physiquement le système ; Il peut également être effectué à distance à l'aide de réseaux ou de câbles Internet. Le système n'a pas besoin d'être spécialement protégé pour que l'acte d'entrer soit considéré comme un crime ; Il suffit que l'entrée soit illégale. En d'autres termes, le propriétaire du système ne doit pas avoir donné son consentement

explicite ou implicite pour que l'auteur entre dans le système. Si un système est accessible à tous, il n'y aura pas de crime. Il est nécessaire d'entrer dans la zone de travail virtuelle / numérique, et non dans la structure physique du système. L'auteur peut commettre ce crime en appuyant sur le bouton du système d'information, ainsi qu'utiliser différentes méthodes et logiciels. Divers logiciels peuvent être utilisés par des hackers qui en ont fait leur métier pour commettre des délits informatiques. Les pirates qui détectent les vulnérabilités du système par la méthode de numérisation ; Il essaie d'entrer dans le système avec des logiciels malveillants tels que des virus, des vers, des chevaux de Troie. Les méthodes de manipulation psychologique telles que l'ingénierie sociale et le phishing sont également fréquemment utilisées par les pirates. En particulier avec des programmes tels que Pegasus Spyware développés ces dernières années, on constate que les propriétaires du système ne peuvent entrer dans le système d'information cible qu'en envoyant un fichier. Pour que l'acte de suspension soit exécuté, l'auteur doit d'abord entrer dans le système. Bien que l'auteur soit entré dans le système conformément à la loi, la raison de se conformer à la loi peut avoir disparu. Si l'agresseur qui se rend compte de cette situation ne quitte pas immédiatement le système, il aura commis l'acte de rester dans le système. L'auteur qui entre dans le système à la suite d'une erreur, mais qui n'en sort pas malgré la réalisation de son erreur, aura également commis ce crime.

Il n'est pas nécessaire qu'une conséquence ou un préjudice spécial se produise pour que le crime soit commis. Un crime sera commis dès que l'auteur entrera ou restera dans le système. Pour l'état aggravé du crime, le législateur a réglementé l'atteinte aux données en conséquence. La tentative est possible en termes de délit d'accès non autorisé au système informatique. Si l'auteur, qui a entamé des actions exécutives pour entrer dans le système, ne peut pas entrer dans le système pour des raisons indépendantes de sa volonté, il sera puni selon les dispositions de la tentative. Pour ce qui est de l'acte de continuer à rester, il est possible de tenter. Lorsque la tentative est possible, les dispositions d'abandon volontaire réglementées à l'article 36 du Code pénal turc seront également appliquées. L'auteur, qui interrompt volontairement l'exécution du crime, ne sera puni que pour les crimes qu'il a commis jusque-là.

Le crime d'accès non autorisé au système informatique ne peut être commis qu'intentionnellement. En cas d'entrée dans un système par négligence ou par erreur, l'auteur ne sera pas puni. Le but de l'auteur n'a aucune importance en termes de formation du crime et de punition de l'auteur. En présence de situations qui éliminent la faute de l'auteur, le crime ne se produira pas, puisque la capacité de faute n'existera pas. Pour commettre l'infraction régie par l'article 243/3 du Code pénal turc, l'auteur doit avoir délibérément pénétré dans le système d'information et endommagé les données du système par un acte de négligence.

La signification de l'expression « illégalement » dans l'article réglementant le crime que nous examinons est discutée dans la doctrine. Certains auteurs soutiennent qu'avec ce choix du législateur, la conscience de l'illégalité est également acceptée comme élément du crime. Selon le point de vue auquel nous souscrivons, le but du législateur ici est d'attirer l'attention sur les raisons de respect de la loi qui peuvent survenir lors de la commission du crime. L'important est de savoir s'il y a un état de conformité avec la loi. Même si l'auteur n'agit pas spécifiquement avec la conscience de l'illégalité, si d'autres éléments du crime sont réalisés, l'auteur sera puni. Une personne qui entre dans le système d'information d'une autre personne dans le cadre de l'application d'une loi ne sera pas punie. Les principaux exemples à donner à cet

égard sont la recherche dans les journaux informatiques et le contrôle des mesures de communication. L'auteur qui utilise le système d'information en état de légitime défense pour prévenir un crime ne sera pas non plus puni. L'auteur qui s'introduit dans le système d'information dans le cadre de l'exercice d'un droit ne sera pas non plus sanctionné. Par exemple, le contrat d'abonnement peut donner aux personnes le droit d'accéder aux systèmes de communication d'autrui. La personne qui entre dans le système conformément au consentement du propriétaire du système ne sera pas pénalisée. Le consentement peut être donné explicitement ou implicitement. Le consentement donné à des tiers par une personne qui entre dans le système avec le consentement du propriétaire du système ne sera pas valide. Le consentement peut être donné sous certaines conditions ; Il peut également être donné pour l'exécution d'un certain objectif. Il est également possible de donner son consentement pour une certaine période de temps. Étant donné que les actions des hackers white hat qui testent la sécurité du système avec des tests de pénétration seront dans le cadre du consentement, aucun crime ne se produira. Il a donné à ses employés le consentement de les utiliser dans l'établissement qui attribue des ordinateurs à ses employés. Il est également important de savoir si c'est un crime pour les institutions d'accéder à des ordinateurs et à des adresses électroniques afin de contrôler leurs employés. Selon les décisions de la Cour européenne des droits de l'homme et de la Cour constitutionnelle, les employeurs doivent informer leurs employés de la portée et des limites de ces inspections et obtenir leur accord avant de procéder à des inspections. Dans le cas contraire, l'audit constituera le délit d'accès non autorisé au système informatique.

La peine à imposer sera réduite si le délit d'accès non autorisé au système informatique est commis contre les systèmes qui peuvent être utilisés contre un prix. Il ne s'agit pas ici de lieux où sont loués des systèmes d'information tels que des cybercafés. Pour arriver à cet état de délinquance, il faut qu'un service soit offert sur la structure virtuelle du système d'information. Les sites Web qui offrent divers services à leurs membres, les plateformes où l'on joue à des jeux vidéo et les applications qui fonctionnent avec un système de paiement à l'utilisation sont des exemples de ces systèmes. L'utilisation non autorisée du service Internet sera également considérée dans le cadre de ce paragraphe. Regarder des émissions cryptées sur Internet telles que IPTV et WEBTV entre également dans le champ d'application de l'article 243/2 du Code pénal turc. L'utilisation du service de diffusion cryptée et des distributeurs automatiques fournis par les lignes téléphoniques et magnétiques sans en payer le prix constituera le délit de profit sans paiement réglementé à l'article 163 du Code pénal turc. Si le délit d'accès non autorisé au système informatique est commis dans le cadre des activités de une organisation terroriste, la peine sera aggravée. En outre, certains auteurs soutiennent que les crimes commis contre des systèmes appartenant à des institutions publiques et liés à la sécurité de l'État et des systèmes protégés par des mesures de sécurité privées devraient être punis plus sévèrement. Dans le cas où les données du système sont modifiées ou détruites en raison d'un délit d'accès non autorisé au système informatique, l'article 243 du Code pénal turc sera appliqué. Ici, l'auteur sciemment et volontairement un accès non autorisé au système informatique endommage par inadvertance les données du système. Si l'auteur nuit intentionnellement aux données, l'article Code pénal turc sera puni conformément à l'article 244. Dans la justification de la loi, les données sont définies comme tous les éléments abstraits du système.

Si le délit d'accès non autorisé au système informatique est commis comme circonstance aggravante ou élément d'un autre délit, il s'agit d'un délit combiné. Par

exemple, dans les délits de vol par utilisation de systèmes d'information (article 142/2-e du CGI) et d'escroquerie par l'utilisation du système d'information comme outil (article 158/1-f du CGI), l'auteur commet le délit réglementé à l'article 243 du Code pénal turc comme l'élément du crime qu'il vise réellement. Dans ce cas, l'auteur ne sera pas puni pour le délit d'accès non autorisé au système informatique. Si le crime d'accès non autorisé au système informatique est commis plus d'une fois contre la même personne à des moments différents, il y aura une infraction successive. La même situation sera également en cause si le crime est commis contre plus d'un système avec un seul acte. Ici, une pénalité unique sera prononcée et ladite pénalité sera augmentée conformément à l'article 43 du Code pénal turc. Si plus d'un crime est commis avec un seul acte, l'auteur ne sera puni que pour le crime le plus grave. La personne qui commet le délit d'accès non autorisé au système informatique peut parfois commettre les délits de violation de la confidentialité des communications, de violation de l'intimité de la vie privée ou de saisie de données personnelles par le même acte. Si l'acte dans lequel ces crimes sont commis est le même, une seule peine sera donnée à l'auteur. Cependant, si l'acte qui cause chaque crime est différent, l'auteur doit être puni séparément pour chaque crime. Une discussion similaire est également en question en ce qui concerne les crimes régis par l'article 244 du TPC. Si l'auteur commet le crime d'accès non autorisé au système informatique afin de commettre le crime de l'article 244 du Code pénal turc, en tant que crime outil, il ne sera pas puni conformément à l'article 243 du Code pénal turc. Code pénal turc de l'auteur. S'il est inévitable d'entrer dans le système d'information pour commettre le crime en 244, la sanction ne doit être prononcée que conformément à cet article. Cependant, l'auteur, qui entre dans le système d'information même s'il n'y est pas obligé, sera également puni conformément à l'article 243 du Code pénal turc. Parfois, l'auteur, qui veut commettre le délit d'accès non autorisé au système informatique, peut commettre le délit d'appareils et de programmes interdits réglementés par l'article 245A du Code pénal turc afin de faciliter son travail. Ici, l'auteur doit être puni conformément à l'article 243 du Code pénal turc et à l'article 245A du Code pénal turc.

Le délit d'accès non autorisé au système informatique peut être commis par une seule personne ; Il est possible que plusieurs personnes commettent ce crime ensemble. Rien ne s'oppose à la mise en œuvre de ce crime par les dispositions relatives à la perpétration indirecte, à l'aide et à l'instigation. L'auteur qui commet le délit d'accès au système d'information sera jugé par le tribunal correctionnel de première instance du lieu où le délit a été commis. À partir de 2021, certains tribunaux ont commencé à fonctionner comme des tribunaux spécialisés dans le domaine de l'informatique dans les endroits où il existe deux ou plusieurs tribunaux pénaux de première instance.

ABSTRACT

The subject of this thesis is the crime of unauthorised access to computer system regulated in Article 243 of the Turkish Crime Code(TCC) No. 5237. In the first paragraph of the article, the simple form of the crime, in the second paragraph, the situation requiring less punishment, and in the third paragraph, the aggravated crime due to the result is regulated. In order to understand cyber crimes and to make a fair decision in concrete events, it is of vital importance to define the information systems subject to the crime and the elements of these systems. For this reason, the concepts of computer, information system, data, and the internet of our study were examined. The technical features of these concepts are mentioned; then the definitions made in the doctrine and legislation were examined. In order to better understand the situation in practice of these concepts, which emerged as the subject or tools of cybercrime, the decisions of the Supreme Court are also included in this section. Again in this section, the concept of cyber crime, which can be considered as a new concept for criminal law, is emphasized. First of all, different approaches in the international literature and in our country's doctrine on the naming of these crimes; then, the definitions and classifications made are examined.

In the next section, it is aimed to examine the historical development of informatics and IT crimes. First of all, the development of cyber crimes that emerged in the USA, which is also the homeland of computers, and the studies done by countries to prevent these crimes are mentioned. Then, the preparation process of the Council of Europe Cybercrime Convention, which is the most important and comprehensive international document prepared on cybercrime, and the articles related to the crime we are examining are emphasized. Afterwards, the studies carried out for the entry of cyber crimes into our country's legislation and the articles related to cyber crimes added to the TCC No. 765 were examined. The drafts prepared to make a new penal code within the scope of the Turkish penal reform and the articles related to cyber crimes in these were also included in our study. Finally, the preparation process of the TCC No. 5237, in which the crime of unauthorised access to computer system was regulated for the first time in our country, and the amendments made in this law were emphasized.

On transferring the basic information about the concepts and the historical background to the reader; The analysis of the unauthorised access to computer system regulated in Article 243 of the TCC has been started. Different views have been expressed in the doctrine about the legal value that is sought to be protected by the crime of unauthorised access to computer system. It has been claimed by the authors that it is aimed to protect one or more of the values such as property, privacy, freedom of communication, personal data and security of the system together. In our opinion, the legal value to be protected by this crime is only the security of information systems. The legislator has protected other interests with different crimes in the TCC. The value that is wanted to be protected in simple forms is the security of the information system. Due to the nature of the third paragraph, the protected value is the data in the system.

Every real person can be the perpetrator of this crime. Legal persons, on the other hand, cannot be perpetrators in the sense of criminal law. However, the security measures stipulated in Article 60 of the TCC may be adjudicated for legal entities that derive benefit from the commission of the crime. Although there is no requirement in the law to have a special profession or status in order to commit computer crimes, it is seen that these crimes are usually committed by computer hackers called "hackers". The victim of the crime is the person who has rights over the system and has direct access to the system. Persons who have been legally authorized to access the system by the system owner may also be victims of this crime. Undoubtedly, real persons may be victims of this crime. The status of legal entities is controversial. Some authors argue that legal entities cannot be victims, but may be harmed by crime. The authors, to whom we also participated, asserted that there is no provision in the TCC that prevents legal persons from being victims; argue that they may also be victims. As long as it is suitable for the nature of the crime, legal entities may also be victims of the crime of unauthorised access to computer system.

The subject of the crime of unauthorised access to computer system is information systems. These systems, which can be used for general purposes, can process, transfer and store data between each other. Devices that can only do a certain job, such as barcode readers, white goods and coffee vending machines, are not considered information systems. Today, ATMs, which can connect to the internet and perform many banking transactions, are considered information systems. Computers, smart phones, tablets are the most common information systems. Internet sites, social media applications, e-mail addresses, online databases and platforms that provide video game playing services, which are not connected to a certain hardware and can be accessed remotely, are also considered as information systems. Cloud computing servers, which have entered the life of humanity in recent years, and smart systems working with the internet of things are also considered as information systems. In Article 243 of the TCC, it is regulated that the crime can be committed against the whole or a part of the information system; therefore, a certain part of the system or a device connected to the system may also be the subject of this crime. For example, a certain folder in the information system or an external memory connected to the system may also be the subject of the crime. The subject of the crime that requires less punishment is the information systems that can be used for a price. The subject of the aggravation of the crime as a result is the data in the system.

A crime will be committed if the perpetrator performs one of the acts of entering or staying in the information system. The act of entering can be performed by physically touching the system; It can also be performed remotely with the help of internet networks or cables. The system does not need to be specially protected for the act of entering to be considered a crime; It is sufficient that the entry is illegal. In other words, the system owner must not have given explicit or implicit consent for the perpetrator to enter the system. If a system is accessible to everyone, there will be no crime. It is necessary to enter the working virtual / digital area, not the physical structure of the system. The perpetrator can commit this crime by pressing the button

of the information system, as well as use different methods and software. Various software can be used by hackers who have made it their profession to commit computer crimes. Hackers who detect the vulnerabilities of the system by scanning method; It tries to enter the system with malicious software such as viruses, worms, Trojan horses. Psychological manipulation methods such as social engineering and phishing are also frequently used by hackers. Especially with programs such as Pegasus Spyware developed in recent years, it is seen that the system owners can enter the target information system only by sending a file. In order for the act of staying to be executed, the perpetrator must first enter the system. Although the perpetrator has entered the system in accordance with the law, the reason for compliance with the law may have disappeared. If the perpetrator who realizes this situation does not leave the system immediately, he will have committed the act of staying in the system. The perpetrator who enters the system as a result of error, but does not exit the system despite realizing his mistake, will also have committed this crime.

There is no need for a special consequence or harm to occur for the crime to be committed. A crime will be committed as soon as the perpetrator enters or remains in the system. For the aggravated state of the crime, the legislator has regulated the damage to the data as a result. Attempt is possible in terms of the crime of unauthorised access to computer system. If the perpetrator, who started executive actions to enter the system, cannot enter the system for reasons beyond his control, he will be punished according to the provisions of the attempt. In terms of the act of continuing to stay, it is possible to attempt. Where the attempt is possible, the voluntary *abandonment* provisions regulated in Article 36 of the TCC will also be applied. The perpetrator, who voluntarily interrupts the execution of the crime, will be punished only for the crimes he has committed until then.

The crime of unauthorised access to computer system can only be committed intentionally. In case of entering into a system by negligence or mistake, the perpetrator will not be punished. The purpose of the perpetrator is of no importance in terms of the formation of the crime and the punishment of the perpetrator. In the presence of situations that eliminate the fault of the perpetrator, the crime will not occur, since the ability to fault will not exist. In order to commit the crime regulated in TCC Article 243/3, the perpetrator must have deliberately entered the information system and damaged the data in the system with a negligent act.

The meaning of the expression “unlawfully” in the article regulating the crime we are examining is discussed in the doctrine. Some authors argue that with this choice of the legislator, the awareness of illegality is also accepted as an element of the crime. According to the view we agree with, the purpose of the legislator here is to draw attention to the reasons for compliance with the law that may arise during the commission of the crime. The important thing is whether there is a state of compliance with the law. Even if the perpetrator does not act specifically with the awareness of illegality, if other elements of the crime are realized, the perpetrator will be punished. A person who enters another person's information system within the scope of

enforcement of a law will not be punished. The main examples to be given in this regard are search in computer logs and control of communication measures. The perpetrator who uses the information system in self-defense to prevent a crime will not be punished either. The perpetrator who enters the information system within the scope of exercising a right will not be punished either. For example, the subscription agreement may give people the right to access the communication systems of others. The person who enters the system in accordance with the consent of the system owner will not be penalized. Consent can be given either explicitly or implicitly. The consent given to third parties by a person who enters the system with the consent of the system owner will not be valid. Consent can be given subject to certain conditions; It can also be given for the performance of a certain purpose. It is also possible to give consent for a certain period of time. Since the actions of white hat hackers who test the security of the system with penetration tests will be within the scope of consent, no crime will occur. It has given its employees consent to use them in the institution that allocates computers to its employees. It is also an important issue whether it is a crime for institutions to access computers and e-mail addresses in order to control their employees. According to the decisions of the ECtHR and the Constitutional Court, employers must inform their employees about the scope and limits of these inspections and obtain their approval before conducting inspections. Otherwise, the audit will constitute the crime of unauthorised access to computer system.

The penalty to be imposed will be reduced if the crime of unauthorised access to computer system is committed against the systems that can be used for a price. What is meant here is not places where information systems such as internet cafes are rented. In order to achieve this state of crime, there must be a service offered over the virtual structure of the information system. Websites that offer various services to their members, platforms where video games are played, and applications that work with a pay-as-you-go system are examples of these systems. Unauthorized use of the Internet service will also be considered within the scope of this paragraph. Watching internet-based encrypted broadcasts such as IPTV and WEBTV is also within the scope of TCC article 243/2. Using the encrypted broadcast service and vending machines provided by telephone and magnetic lines without paying the price will constitute the crime of benefiting without payment regulated in TCC article 163. If the crime of unauthorised access to computer system is committed within the framework of the activities of a terrorist organization, the penalty will be increased. In addition, some authors argue that crimes committed against systems belonging to public institutions and related to the security of the state and systems protected by private security measures should be punished more severely. In case the data in the system is changed or destroyed due to the crime of unauthorised access to computer system, TCC article 243 will be applied. Here, the perpetrator knowingly and willingly unauthorised access to computer system inadvertently damages the data in the system. If the perpetrator intentionally harms the data, TCC article will be punished in accordance with 244. In the justification of the law, data is defined as all abstract elements in the system.

If the crime of unauthorised access to computer system is committed as an aggravating factor or element of another crime, it is a combined crime. For example, in the crimes of theft through the use of information systems (TCC article 142/2-e) and fraud through the use of the information system as a tool (TCC article 158/1-f), the perpetrator commits the crime regulated in TCC article 243 as the element of the crime he really targets. In this case, the perpetrator will not be punished for the crime of unauthorised access to computer system. If the crime of unauthorised access to computer system is committed more than once against the same person at different times, there will be a successive offense. The same situation will also be in question if the crime is committed against more than one system with a single act. Here, a single penalty will be given and the said penalty will be increased according to article 43 of the TCC. If more than one crime is committed with a single act, the perpetrator will be punished only for the most serious crime. The person who commits the crime of unauthorised access to computer system can sometimes commit the crimes of violating the confidentiality of communication, violating the privacy of private life or seizing personal data with the same act. If the act in which these crimes are committed is the same, only one punishment will be given to the perpetrator. However, if the act that causes each crime is different, the perpetrator should be punished separately for each crime. A similar discussion is also in question in terms of the crimes regulated in TPC article 244. If the perpetrator commits the crime of unauthorised access to computer system in order to commit the crime in TCC article 244, as a tool crime, he will not be punished in accordance with TCC article 243. TPC of the perpetrator. If it is unavoidable to enter the information system in order to commit the crime in 244, punishment should be given only in accordance with this article. However, the perpetrator, who enters the information system even though he is not obliged, will also be punished in accordance with TCC article 243. Sometimes, the perpetrator, who wants to commit the crime of unauthorised access to computer system, can commit the crime of prohibited devices and programs regulated in TCC article 245A in order to facilitate his work. Here, the perpetrator should be punished in accordance with both TCC article 243 and TCC article 245A.

The crime of unauthorised access to computer system can be committed by a single person; It is possible for more than one person to commit this crime together. There is no obstacle to the implementation of this crime by the provisions regarding indirect perpetration, aiding and instigation. The perpetrator who commits the crime of entering the information system will be tried in the criminal court of first instance in the place where the crime was committed. As of 2021, certain courts have started to work as specialized courts in the field of informatics in places where there are two or more criminal courts of first instance.

ÖZET

Bu tezimin konusu, 5237 sayılı Türk Ceza Kanunu'nun 243. maddesinde düzenlenen bilişim sistemine girme suçudur. Maddenin ilk fıkrasında suçun basit hali, ikince fıkrasında daha az cezayı gerektiren hali, üçüncü fıkrasında ise neticesi sebebiyle ağırlaşmış hali düzenlenmiştir. Bilişim suçlarının anlaşılması ve somut olaylarda adaletli bir karar verilebilmesi için suça konu bilişim sistemlerinin ve bu sistemlerin unsurlarının tanımlanması hayati bir öneme sahiptir. Bu nedenle çalışmamızın bilgisayar, bilişim sistemi, veri ve internet kavramları incelenmiştir. Bu kavramların teknik özelliklerine değinilmiş; ardından doktrinde ve mevzuatta yapılan tanımlar incelenmiştir. Bilişim suçlarının konusu ya da araçları olarak ortaya çıkan bu kavramların uygulamadaki durumunun daha iyi anlaşılabilmesi için Yargıtay kararlarına da bu bölümde yer verilmiştir. Yine bu bölümde ceza hukuku için yeni bir kavram olarak sayılabilecek bilişim suçu kavramının üzerinde durulmuştur. İlk olarak bu suçların adlandırılması konusunda uluslararası literatürde ve ülkemiz doktrinindeki farklı yaklaşımlar; ardından ise yapılan tanımlar ve sınıflandırmalar incelenmiştir.

Sonraki bölümde ise bilişim ve bilişim suçlarının tarihi gelişiminin incelenmesi amaçlanmıştır. İlk olarak bilgisayarın da ana vatanı olan Amerika'da ortaya çıkan bilişim suçlarının gelişimi ve bu suçların engellenmesi için ülkeler tarafından yapılan çalışmalara değinilmiştir. Ardından bilişim suçları ile ilgili olarak hazırlanan en önemli ve geniş kapsamlı uluslararası belge olan Avrupa Konseyi Siber Suç Sözleşmesi'nin hazırlanma süreci ve incelemekte olduğumuz suç ile ilgili maddelerinin üzerinde durulmuştur. Devamında ise bilişim suçlarının ülkemiz mevzuatlarına girişi için yapılan çalışmalar ile 765 sayılı TCK'ya eklenen bilişim suçları ile ilgili maddelerin incelemesi yapılmıştır. Türk ceza reformu kapsamında yeni bir ceza kanunu yapmaya yönelik hazırlanan tasarılar ile bunlarda yer alan bilişim suçlarına ilişkin maddeler de yine çalışmamızda yer almıştır. Son olarak bilişim sistemine girme suçunun ülkemizde ilk defa düzenlendiği 5237 sayılı TCK'nın hazırlanış süreci ve bu kanunda yapılan değişiklikler üzerinde durulmuştur.

Kavramlar ile ilgili temel bilgiler ve tarihi arka planın okuyucuya aktarılması üzerine TCK m. 243'te düzenlenen bilişim sistemine girme suçu incelenmesine başlanmıştır. Bilişim sistemine girme suçu ile korunmak istenen hukuki değer ile ilgili doktrinde farklı görüşler dile getirilmiştir. Malvarlığı, özel hayatının gizliliği, haberleşme özgürlüğü, kişisel veriler ve sistemin güvenliği gibi değerlerin birinin ya da birkaçının birlikte korunmasının amaçlandığı yazarlarca öne sürülmüştür. Bize göre ise bu suç ile korunmak istenen hukuki değer yalnızca bilişim sistemlerinin güvenliğidir. Kanun koyucu sayılan diğer menfaatleri TCK'da yer alan farklı suçlarla korumuştur. TCK m. 243'ün basit hali ile korunmak istenen değer bilişim sisteminin güvenliğidir. Üçüncü fıkradaki niteliği sebebiyle ağırlaşmış halde ise korunmak istenen değer sistemde bulunan verilerdir.

Her gerçek kişi bu suçun faili olabilecektir. Tüzel kişiler ise ceza hukuku anlamında fail olamayacaklardır. Bununla birlikte suçun işlenmesi ile menfaat temin eden tüzel kişiler hakkında TCK m. 60'da öngörülen güvenlik tedbirlerine hükmedilebilecektir. Her ne kadar kanunda bilişim suçlarının işlenebilmesi için özel bir meslek ya da statü sahibi olmak gibi bir şart aranmasa da bu suçların genellikle "hacker" olarak adlandırılan bilişim korsanlarınca işlendiği görülmektedir. Suçun mağduru ise sistem üzerinde hak sahibi olan ve sisteme doğrudan erişim yetkisine sahip kişidir. Sistem sahibi tarafından hukuka uygun bir şekilde sisteme erişim yetkisi

verilmiş kişiler de bu suçun mağduru olabilirler. Kuşkusuz ki gerçek kişiler bu suçun mağduru olabileceklerdir. Tüzel kişilerin durumu ise tartışmalıdır. Kimi yazarlar tüzel kişilerin mağdur olamayacaklarını, ancak suçtan zarar gören olabileceklerini savunmaktadır. Bizim de katıldığımız yazarlar ise TCK'da tüzel kişilerin mağdur olmalarına engel bir hüküm olmadığını öne sürerek; bunların da mağdur olabileceklerini savunmaktadır. Suçun niteliğine uygun düştüğü sürece tüzel kişiler de bilişim sistemine girme suçunun mağduru olabileceklerdir.

Bilişim sistemine girme suçunun konusu bilişim sistemleridir. Genel amaçlı olarak kullanılabilen bu sistemler verileri işleyebilir, birbirleri arasında aktarabilir ve depolayabilirler. Barkod okuyucular, beyaz eşyalar ve kahve otomatları gibi sadece belli bir işi yapabilen cihazlar bilişim sistemi olarak kabul edilmemektedirler. Bununla birlikte son yıllarda ortaya çıkan nesnelerin interneti ile diğer nesneler ile bilişim sistemlerine veri gönderebilen ya da bunlardan veri alabilen beyaz eşyalar ya da akıllı saatler gibi giyilebilir teknoloji ürünleri bilişim sistemi olarak kabul edilmelidir. Günümüzde artık internete bağlanabilen ve birçok bankacılık işleminin yapılabilirdiği ATM'ler ise bilişim sistemi sayılmaktadır. Bilgisayarlar, akıllı telefonlar, tabletler en yaygın bilişim sistemleridir. Belli bir donanıma bağlı olmayan ve uzaktan erişilebilen internet siteleri, sosyal medya uygulamaları, e-posta adresleri, online veri tabanları ve video oyunu oynama hizmeti veren platformlar da yine bilişim sistemi olarak kabul edilmektedir. Son yıllarda insanlığın hayatına giren bulut bilişim sunucuları ile nesnelerin interneti ile çalışan akıllı sistemler de yine bilişim sistemi olarak kabul edilmektedirler. TCK m. 243'te suçun bilişim sisteminin tamamına ya da bir kısmına karşı işlenebileceği düzenlenmiştir; bu nedenle sistemin belli bir parçası ya da sisteme bağlı bir aygıt da bu suçun konusu olabilir. Örneğin bilişim sisteminin içerisinde bulunan belli bir klasör ya da sisteme bağlanmış bir harici bellek de suçun konusu olabilir. Suçun daha az cezayı gerektiren halinin konusu bedeli karşılığı yararlanılabilen bilişim sistemleridir. Suçun netice itibarıyla ağırlaşan halinin konusu ise sistemin içerisindeki verilerdir.

Failin bilişim sistemine girme veya sistemde kalmaya devam etme hareketlerinden birini yapması ile suç işlenmiş olacaktır. Girme eylemi fiziksel olarak sisteme temas edilerek icra edilebileceği gibi; internet ağları ya da kablolar yardımıyla uzaktan da icra edilebilecektir. Girme eyleminin suç olarak kabul edilebilmesi için sistemin özel olarak korunmasına gerek yoktur; girişin hukuka aykırı olması yeterlidir. Bir başka failin sisteme girme eyleminin hukuken geçerli bir hak ya da rızaya dayanmaması gerekmektedir. Herkesin erişimine açık bir sisteme girilmesi halinde suç oluşmayacaktır. Sistemin fiziksel yapısına değil çalışan sanal/dijital alana girilmesi gerekmektedir. Fail bilişim sisteminin düğmesine basarak bu suçu işleyebileceği gibi farklı yöntemler ve yazılımlar da kullanabilecektir. Bilişim suçlarını işlemeyi meslek haline getirmiş hackerlar tarafından bu suçların işlenebilmesi için çeşitli yazılımlar kullanılabilmektedir. Tarama yöntemi ile sistemin açıklarını tespit eden bilişim korsanları; virüsler, solucanlar, Truva atları gibi zararlı yazılımlar ile sisteme girmeye çalışmaktadır. Sosyal mühendislik ve olta gibi psikolojik manipülasyon yöntemleri de yine bilişim korsanlarınca sıkça kullanılmaktadır. Özellikle son yıllarda geliştirilen Pegasus yazılımı gibi programlarla sistem sahiplerine sadece dosya gönderilerek hedef bilişim sistemine girilebildiği görülmektedir. Kalma eyleminin icra edilebilmesi için ilk olarak failin sisteme girmiş olması gerekmektedir. Fail sisteme hukuka uygun bir şekilde girmiş olmasına rağmen hukuka uygunluk sebebi ortada kalmış olabilir. Bu durumu fark eden fail hemen sistemden çıkmazsa sistemde

kalmaya devam etme fiilini işlemiş olacaktır. Hata sonucu sisteme girdiği sistemden hatasını fark etmesine rağmen çıkmayan fail de bu suçu işlemiş olacaktır.

Suçun işlenmesi için özel bir neticenin ya da zararın meydana gelmesin gerek yoktur. Fail sisteme girdiği veya kalmaya devam ettiği anda suç işlenmiş olacaktır. Suçun neticesi sebebiyle ağırlaşmış hali için ise kanun koyucu verilere zarar gelmesini netice olarak düzenlemiştir. Bilişim sistemine girme suçu bakımından teşebbüs mümkündür. Sisteme girmek için icrai hareketlere başlayan fail elinde olmayan nedenlerle sisteme giremezse teşebbüs hükümlerine göre cezalandırılacaktır. Kalmaya devam etme eylemi bakımından ise teşebbüs mümkündür. Teşebbüsün mümkün olduğu hallerde TCK m. 36'da düzenlenen gönüllü vazgeçme hükümleri de uygulanacaktır. Gönüllü olarak suçun icra hareketlerini yarıda bırakan faile sadece o zamana kadar işlediği suçlardan dolayı ceza verilecektir.

Bilişim sistemine girme suçu sadece kasten işlenebilmektedir. Taksirle ya da hata sonucu bir sisteme girilmesi halinde faile ceza verilmeyecektir. Suçun oluşumu ve failin cezalandırılması açısından failin amacının bir önemi yoktur. Failin kusurluluğunu ortadan kaldıran hallerin varlığında ise kusur yeteneği mevcut olmayacağı için suç da oluşmayacaktır. TCK m. 243/3'te düzenlenen suçun işlenmesi için ise fail kasten bilişim sistemine girmiş olmalı ve taksirli bir hareketle sistemdeki verilere zarar vermelidir.

İncelemekte olduğumuz suçu düzenleyen maddedeki “*hukuka aykırı olarak*” ifadesinin anlamı doktrinde tartışılmaktadır. Kimi yazarlar kanun koyucunun bu tercihi ile hukuka aykırılık bilincini de suçun bir unsuru olarak kabul ettiğini savunmaktadır. Bizim katıldığımız görüşe göre ise kanun koyucunun buradaki amacı suçun işlenmesi sırasında ortaya çıkabilecek hukuka uygunluk nedenlerine dikkat çekmektir. Önemli olan hukuka uygunluk halinin bulunup bulunmadığıdır. Failin özel olarak hukuka aykırılık bilinciyle hareket etmiyor olsa bile suçun diğer unsurları gerçekleştiği takdirde fail cezalandırılacaktır. Bir kanun hükmünün icrası kapsamında bir başkasına ait bilişim sistemine giren kişi cezalandırılmayacaktır. Bu konuda verilecek başlıca örnekler bilgisayar kütüklerinde arama ve iletişimin denetlenmesi tedbirleridir. Bilişim sistemini bir suçu önlemek için meşru müdafaa kapsamında işleyen fail de cezalandırılmayacaktır. Bir hakkın kullanılması kapsamında bilişim sistemine giren fail de cezalandırılmayacaktır. Örneğin abonelik sözleşmesi kişilere başkalarına ait ilişim sistemlerine erişme hakkı verebilmektedir. Sistem sahibinin verdiği rızaya uygun bir şekilde sisteme giren kişi de cezalandırılmayacaktır. Rıza açık bir şekilde verilebileceği gibi örtülü olarak da verilmiş olabilir. Sistem sahibinden aldığı rıza ile sisteme giren bir kimsenin üçüncü kişilere vereceği rıza geçerli olmayacaktır. Rıza belli bir şarta bağlı olarak verilebileceği gibi; belli bir amacın ifasına yönelik olarak da verilebilecektir. Ayrıca belli bir süreliğine rıza verilmesi de mümkündür. Sızma testleri ile sistemin güvenliğini test eden beyaz şapkalı hackerların eylemleri rıza kapsamında olacağı için suç oluşmayacaktır. Çalışanlarına bilgisayar tahsis eden kurumda bunları kullanabilmeleri için çalışanlarına rıza göstermiştir. Kurumların, çalışanlarını denetlemek amacıyla bilgisayarlar ve mail adreslerine erişmelerinin suç olup olmadığı da önemli bir konudur. AİHM ve Anayasa Mahkemesi kararlarına göre işverenlerin denetim yapmadan önce bu denetimlerin kapsamı ve sınırları hakkında çalışanlarını bilgilendirmeleri ve onaylarını almaları gerekmektedir. Aksi halde yapılan denetim bilişim sistemine girme suçunu oluşturacaktır.

Bilişim sistemine girme suçunun bedeli karşılığı yararlanılabilen sistemlere karşı işlenmesi halinde verilecek ceza azaltılacaktır. Burada kastedilen internet kafeler

gibi bilişim sistemlerinin kiralandığı mekanlar değildir. Suçun bu halinin ulaşması için bilişim sistemini sanal yapısı üzerinden sunulan bir hizmet söz konusu olmalıdır. Üyelerine ücret karşılığı çeşitli hizmet sunan internet siteleri, video oyunu oynama platformları ve kullandığın kadar öde sistemi ile çalışan uygulamalar bu sistemlere örnek olarak gösterilebilir. İnternet hizmetinin yetkisiz bir şekilde kullanılması da bu fıkra kapsamında değerlendirilecektir. IPTV ve WEBTV gibi internet tabanlı sunulan şifreli yayınların izlenmesi de yine TCK m. 243/2 kapsamındadır. Telefon ve manyetik hatlar ile sunulan şifreli yayın hizmeti ile otomatların bedeli ödenmeksizin kullanılması ise TCK m. 163'te düzenlenen karşılıksız yararlanma suçunu oluşturacaktır. Bilişim sistemine girme suçunun bir terör örgütünün faaliyetleri çerçevesinde işlenmesi halinde verilecek ceza artırılacaktır. Ayrıca kimi yazarlar kamu kurumlarına ait ve devletin güvenliği ile ilgili sistemler ile özel güvenlik önlemleri ile korunan sistemlere karşı işlenen suçların daha ağır bir şekilde cezalandırılmasını savunmaktadır. Bilişim sistemine girme suçunun işlenmesi nedeniyle sistemdeki verilerin değişmesi ya da yok olması halinde ise TCK m. 243 uygulanacaktır. Burada bilerek ve isteyerek bilişim sistemin giren fail istemeden sistemdeki verilere zarar vermektedir. Kasten verilere zarar veren fail ise TCK m. 244 gereğince cezalandırılacaktır. Kanunun gerekçesinde veri sistemdeki tüm soyut unsurlar olarak tanımlanmıştır.

Bilişim sistemine girme suçu bir başka suçun ağırlaştırıcı sebebi ya da unsuru olarak işlenmişse bileşik suç söz konusudur. Örneğin bilişim sistemleri kullanılması yoluyla hırsızlık (TCK m. 142/2-e) ve bilişim sisteminin araç olarak kullanılması yoluyla dolandırıcılık (TCK m. 158/1-f) suçlarında fail asıl hedeflediği suçun unsuru olarak TCK m. 243'te düzenlenen suçu işlemektedir. Bu durumda faile bilişim sistemine girme suçundan dolayı ceza verilmeyecektir. Bilişim sistemine girme suçunun aynı kişiye karşı farklı zamanlarda birden fazla kere işlenmesi halinde zincirleme suç söz konusu olacaktır. Suçun tek fiille birden fazla sisteme karşı işlenmesi halinde de yine aynı durum söz konusu olacaktır. Burada tek bir ceza verilecek ve söz konusu ceza TCK m. 43'e göre artırılacaktır. Tek bir fiil ile birden fazla suçun işlenmesi halinde faile yalnızca en ağır suç için ceza verilecektir. Bilişim sistemine girme suçunu işleyen kişi kimi zaman aynı fiille haberleşmenin gizliliğini ihlal, özel hayatın gizliliğini ihlal veya kişisel verilerin ele geçirilmesi suçlarını işleyebilmektedir. Eğer bu suçların işlendiği fiil aynıysa faile yalnızca tek bir ceza verilecektir. Buna rağmen her suça sebebiyet veren fiil farklıysa fail her suç bakımından ayrı ayrı cezalandırılmalıdır. Benzer bir tartışma TCK m. 244'te düzenlenen suçlar bakımından da söz konusudur. Fail TCK m. 244'teki suçu işlemek için bilişim sistemine girme suçunu bir araç suç olarak işlemişse TCK m. 243 gereğince cezalandırılmayacaktır. Failin TCK m. 244'teki suçu işlemesi için bilişim sistemine girmesi kaçınılmaz ise sadece bu madde gereğince ceza verilmelidir. Bununla birlikte zorunda olmamasına rağmen bilişim sistemine giren faile ayrıca TCK m. 243 gereğince de ceza verilecektir. Kimi zaman bilişim sistemine girme suçunu işlemek isteyen fail, işini kolaylaştırmak amacıyla TCK m. 245A'da düzenlenen yasak cihaz ve programlar suçunu işleyebilmektedir. Burada faile hem TCK m. 243 hem de TCK m. 245A gereğince ceza verilmelidir.

Bilişim sistemine girme suçu tek kişi tarafından işlenebileceği gibi; birden fazla kişinin de bu suçu birlikte işlemesi mümkündür. Dolaylı faillik, yardım etme ve azmettirmeye ilişkin hükümlerin de bu suçu uygulanması önünde herhangi bir engel yoktur. Bilişim sistemine girme suçunu işleyen fail, suçun işlendiği yerdeki asliye ceza mahkemesinde yargılanacaktır. 2021 yılından itibaren iki veya daha fazla asliye ceza

mahkemesi olan yerlerde belli mahkemeler biliřim alanında ihtisas mahkemesi olarak alıřmaya bařlamıřtır.



GİRİŞ

1946 yılında geliştirilen ve tarihteki ilk bilgisayar olarak kabul edilen ENIAC¹ ile hayatımıza giren bilişim sistemleri; günümüze değin geçen sürede çok hızlı bir şekilde değişmiş ve gelişmiştir. Bilişim teknolojileri profesyonel iş hayatından, eğitime; eğlenceden, alışverişe kadar birçok alanda hayatın vazgeçilmez bir parçası olmayı başarmıştır. Öyle ki TÜİK verilerine göre 2021 yılında Türkiye’deki hanelerin %80,5’i bilişim sistemleri ve internet düzenli olarak kullanmaktadır². Hayatın her alanına sirayet eden bilişim sistemleri aynı zamanda yeni suç tiplerinin ortaya çıkması ve işlenmesi için uygun bir ortam olmuştur.

İlk defa altmışlı yıllarda Amerika’da ortaya çıkan³ bilişim suçları; kişisel bilgisayarlar ve internetin yaygınlaşarak evlerde kullanılmaya başlandığı doksanlı yıllara gelinmesiyle birlikte yaygınlaşmıştır⁴. Bilişim suçlarının işlenme şekillerinin ve sayılarının arttığı bu yıllarda devletler de bu suçlar ile ilgili cezai düzenlemeleri yürürlüğe koymaya başlamıştır⁵. Yine bu yıllarda uluslararası örgütler tarafından da bilişim suçları üzerine çeşitli çalışmalar yapılmış; 2001 yılında ise bilişim suçları alanındaki ilk ve en önemli uluslararası belge olarak kabul edilen Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS) hazırlanarak imzaya açılmıştır⁶.

Ülkemizde ise 1991 yılında 765 sayılı TCK’da yapılan değişikliklerle birlikte bilişim suçları ceza kanunumuza girmiştir⁷. Ancak bu değişiklik ile kanuna eklenen maddeler arasında bu çalışmanın konusu olan bilişim sistemine girme suçunu düzenleyen bir madde bulunmamaktaydı. Bilişim sistemine girme eylem ilk defa 5237

¹ Ahmet Caner Yenidünya/Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul: Legal Yayıncılık, 2003 s. 13-14.

² TÜİK, **2021 Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması** [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanim-Arastirmasi-2021-37437](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2021-37437) (E.T. 11.04.2022)

³ Emin Doğan Aydın, **Bilişim Suçları ve Hukukuna Giriş**, Ankara: Doruk Yayınları, 1992 s. 25.

⁴ Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 8. Baskı, Ankara: Seçkin Yayıncılık, 2020 s. 93-94.

⁵ Levent Kurt, **Açıklamalı İctihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara: Seçkin Yayınevi, 2005 s. 115.

⁶ Murat Önok, “*Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği*”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Prof. Dr. Nur Centel’e Armağan, C.9, S. 2, 2013 s. 1241.

⁷ Akbulut, **Bilişim Alanında Suçlar**, 2. Baskı, Ankara: Adalet Yayınevi s. 96-97. Kurt, **a.g.e.** s. 118-121.

sayılı TCK'nın 243. maddesinde suç olarak düzenlenmiştir⁸. 2016 yılında ise TCK m. 243'te çeşitli değişiklikler yapılmıştır. Maddenin güncel hali şu şekildedir:

Bilişim sistemine girme

Madde 243- “(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.

(2) Yukarıdaki fıkra da tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

(4) (Ek: 24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.”

Maddenin ilk fıkrası bilişim sistemine girme suçunun basit halini, ikinci fıkrası cezanın azaltılmasını gerektiren halini, üçüncü fıkrası ise suçun ortaya çıkan netice nedeniyle ağırlaşan halini düzenlemektedir. Maddeye 2016 yılında eklenen dördüncü fıkra da ise “veri nakillerini izleme suçu” düzenlenmiştir. Bu suç her ne kadar TCK m. 243 içerisinde düzenlenmiş olsa da bilişim sistemlerine girmeksizin işlenen bir suçtur. Doktrinde de bu suçun ayrı bir maddede düzenlenmesinin daha sağlıklı olacağı ifade edilmiştir⁹. Koruduğu hukuki değer, suçun konusu ve icra edilen fiiller yönünden bilişim sistemine girme suçu ile arasında önemli farklar bulunan dördüncü fıkra bu çalışma kapsamında incelenmeyecektir.

Çalışmamızda TCK m. 243'ün ilk üç fıkrasında düzenlenmiş olan bilişim sistemine girme suçu incelenecektir. İşlenen bir fiilin TCK'da düzenlenmiş olan suç tipinin kapsamına girip girmediğinin tipiklik unsuru yönünden değerlendirilebilmesi için ilk olarak bilişim, bilişim sistemi ve ilgili kavramların sınırlarının açık ve net bir şekilde tespit edilebilmesi gerekmektedir. Bilişim sistemleri ve bu sistemlerin

⁸ Akbulut, **a.g.e.** s. 112. Kurt, **a.g.e.** s. 136.

⁹ Akbulut, **Ba.g.e. Suçlar** s. 158-159. Dülger, **a.g.e.** s. 237. Ahmet Gül, **Doğrudan-Dolaylı Bilişim Suçları**, 3. Baskı, Ankara: Seçkin Yayıncılık, 2021 s. 91.

bileşenlerinin tanım ve özellikleri, gelişen teknolojiyle de bağlantılı olarak, her geçen gün gelişmekte ve değişmekte; bu değişim ise aşağıda değinilecek kavramların tanımlanmasını daha da zorlaştırmaktadır¹⁰. Öte yandan bu kavramlara kanuni düzenlemelerle yapılacak tanımlar zaman içinde yetersiz kalacak, bu durum ise ortaya çıkan yeni suç işleme biçimlerinin kanunun kapsamı dışında kalmasına neden olacaktır¹¹. Bu nedendir ki bazı yazarlar bilişim kavramlarının tanımını yapmaktan kaçınıp özelliklerini saymakla yetinirken¹² bazı yazarlar ise teknik ayrıntı ve terimlerden arındırılmış kısa ve öz tanımlar yapmayı tercih etmiştir¹³. Suçun unsurlarının incelenmesi sırasında meydana gelebilecek olası karışıklıkların önüne geçilebilmesi maksadıyla; çalışmamızın ilk bölümünde doktrinde yapılan tanımlar yargı kararları ile birlikte bütüncül bir şekilde ele alınacaktır. Bu bölümde çoğunlukla incelemekte olduğumuz suçun konusu olacak bilgisayar ve bilişim sisteminin yanında; veri ve internet gibi suçla yakın ilişkili kavramlara da değinilecektir. Ayrıca bilişim kavramının isimlendirilmesi, tanımlanması ve sınıflandırılmasına ilişkin doktrindeki yaklaşımlara değinilmiştir.

Kavramların tanımlanmasının ardından, okuyucunun kavramların tarihi arka planına hâkim olması amacıyla, bilişim ve bilişim suçlarının tarihi gelişimine değinilecektir. Ardından ülkemizin de taraf olduğu AKSSS'nin hazırlanış süreci ile incelemekte olduğumuz suçla ilgili hükümlerinden bahsedilecektir. Akabinde ise 765 sayılı TCK döneminde bilişim suçları ile ilgili hazırlanan tasarılar ve yapılan kanun değişiklikleri ele alınacaktır. Bu sırada 5237 sayılı TCK'nın hazırlık süreci ile bu dönemde yapılan tartışmaların üzerinde durulacaktır.

Çalışmanın devamında ise suçla korunan hukuki değer doktrindeki farklı görüşler ve yargı kararları ışığında incelenecektir. Ardından suçun maddi unsurları, manevi unsuru ve hukuka aykırılık unsuru tek tek incelenerek bu konularda doktrinde ve yargı kararlarında belirtilen önemli hususların üzerinde durulacaktır. Yine aynı başlık altında; suçun cezasını hafifleten ve ağırlaştıran nedenler ile suçun neticesi sebebiyle ağırlaşmış hali incelenecektir. Suçların birleşmesi başlığı altında ise bilişim sistemine girme suçunun farklı suçlarla beraber işlenmesi halinde failin nasıl

¹⁰ Dülger, **a.g.e.** s. 58.

¹¹ Büşra Özçelik, **Bilişim Sistemine Girme Suçu**, İstanbul: On İki Levha Yayınları: İstanbul Ceza Hukuku ve Kriminoloji Arşivi, 2021 s. 3-4.

¹² Yenidünya/Değirmenci **a.g.e.** s. 31

¹³ Dülger, **a.g.e.** s. 64-65.

cezalandırılacağı sorusunun üzerinde durulacaktır. Bu kapsamda TCK'nın ilgili maddelerinde düzenlenen bileşik suç, zincirleme suç ile aynı ve farklı neviden fikri içtima hallerine ayrı ayrı değinilecek; bu hallerde hakim tarafından uygulanacak kurallar örnekler, doktrin görüşleri ve yargı kararları ile belirlenmeye çalışılacaktır. İştirak başlığı altında ise birden fazla fail olması veya faile yardım edilmesi yahut failin suça azmettirilmesi durumlarında uygulanacak hükümlerin üzerinde durulacaktır. Yaptırım bölümünde suçun basit hali ve nitelikli halleriyle neticesi sebebiyle ağırlaşmış haline verilecek ceza ve bu cezanın nasıl belirleneceği üzerinde durulacaktır. Yargılama başlığı altında ise yakın zamanda CMK'da yapılan değişiklikler de ele alınarak bilişim sistemine girme suçunun soruşturma ve kovuşturma evrelerinin nasıl yürütüleceği açıklanacaktır.

Bu çalışmada gerek suçla ilgili temel kavramlar gerekse suçun unsurlarına ilişkin tartışmalarda ilgili Yargıtay Ceza Genel Kurulu ve ceza dairesi kararlarına değinilerek uygulamadaki güncel durum da okuyucuya aktarılacaktır. Konu ile ilgisi bulunan hallerde ise Avrupa İnsan Hakları Mahkemesi ile Anayasa Mahkemesi kararlarına yer verilecektir. Yargı kararlarının yanı sıra doktrindeki farklı görüşlere de değinilerek işlenen konuların olabildiğince geniş bir perspektiften incelenmesi amaçlanmaktadır.

I. TEMEL KAVRAMLAR

A. Bilişim

Fransızca “*informatique*¹⁴” sözcüğünün karşılığı olarak Türkçe’de ilk başlarda “*enformatik*¹⁵” olarak da kullanılan bilişim: “*verinin saklanması, saklanan verinin elektronik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgilenen bir bilim dalı*¹⁶” olarak tanımlanabilir. Bu tanım ve doktrinde yapılmış olan diğer tanımlar¹⁷ incelendiğinde bilişim kavramının; verilerin bir bilişim sistemine yüklenerek işlenip çıktı haline getirilmesini kapsayan veri işleme ile birlikte bu verilerin bilişim sistemleri arasında çeşitli ağlar vasıtasıyla aktarılması anlamına gelen veri iletişimini de kapsadığı görülmektedir¹⁸.

Yargıtay kararlarına bakıldığında ise bilişim kavramı doktrindeki tanımlara paralel olarak “*bilgisayardan da faydalanılmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesine konu olan akademik ve mesleki disipline verilen ad... bilgisayar kullanma ilmi.*¹⁹” şeklinde tanımlanmıştır. Yine aynı kararda “*Her ne kadar çoğunlukla ‘bilişim’ ile ‘bilgisayar’ terimleri aynı anlamda kullanılmaktaysa da gerçekte bunlar aynı şey demek değildir. Zira, ‘bilişim’ sözcüğü ‘bilgisayar’ kelimesine oranla daha geniş kapsamlıdır.*” denilerek bilgisayar ve bilişim arasında kapsayıcılık yönünden bir ayrım yapılmıştır. Doktrindeki kimi yazarlarca²⁰ da benimsenmiş olan bu ayrım, bir makine olan bilgisayar ile bir bilim dalı olan bilişimi kıyaslamamanın mümkün olmayacağını gerekçesiyle eleştirilmiştir²¹.

¹⁴ Bu sözcük 1962 yılında Philippe Dreyfus tarafından information ve automatique sözcüklerinden yola çıkılarak türetilmiştir. Georges Ifrah, **Bilgisayar Ne Sayar: Rakamların Evrensel Tarihi XI**, (Çev. Kurtuluş Dinçer), Ankara: Tübitak Popüler Bilim Kitapları, 2002 s.69.

¹⁵ Kavram İngilizce’de “*informatics*”, Almanca’da “*informatiks*”, İtalyanca ve İspanyolca’da ise “*informatica*” olarak ifade edilmektedir.

¹⁶ Yenidünya/Değirmenci, **a.g.e.** s. 27.

¹⁷ Tanımlar için bkz. Dülger, **a.g.e.** s. 68. Recep Yılmaz Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile**, İstanbul: Alfa Yayınevi, 1997 s. 131. Akbulut, **a.g.e.** s. 13. Aydın, **Bilişim Suçları ve Hukukuna Giriş** s. 3. İsmail Ergün, **Siber Suçların Cezalandırılması ve Türkiye’de Durum**, Ankara: Adalet Yayınları, 2008 s. 10. Metin Turan, **Bilişim Hukuku**, 5. Baskı, Ankara: Seçkin, 2021 s. 48-49. Yüksel Ersoy, “*Genel Hukuki Koruma Çerçevesinde Bilişim Suçları*”, **Prof. Dr. Yılmaz Günel’a Armağan**, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayını, Cilt:49, No:3-4, 1994 s. 151.

¹⁸ Akbulut, **a.g.e.** s. 13-17.

¹⁹ YCGK. E. 2007/6-136 K. 2007/150 T. 19.6.2007 www.lexpera.com.tr (E. T. 19.10.2021)

²⁰ Yenidünya/Değirmenci, **a.g.e.** s. 30-31., Berrin Bozdoğan Akbulut, “*Bilişim Suçları*”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, C. 8, S.1-2, 2000 s. 546.

²¹ Dülger, **a.g.e.** s. 67.

İlk olarak 1989 tarihli TCK ön tasarısında rastladığımız bilişim kavramı 14 Haziran 1991 tarihli ve 3756 sayılı kanunla²², “*Bilişim Alanındaki Suçlar*” bölümünün 765 sayılı TCK’ya eklenmesiyle mevzuatımıza girmiştir. 5237 sayılı TCK’da ise bilişim kavramı kullanılmasına rağmen önceki tasarıların aksine kanun ve gerekçesinde kavramın tanımına yer verilmemiştir. Gerek 765 gerekse 5237 sayılı TCK’da kullanılan “*bilişim alanı*” kavramı doktrinde yerinde ve doğru bir kullanım olarak görülmüştür. Zira “*bilişim alanı*” kavramı hem düzenlenen suçların konusunu ve işlendikleri ortamı hem de öngörülemez bir şekilde gelişen teknolojinin ortaya çıkaracağı yeni araç ve sistemleri kapsayacaktır²³.

B. Bilişim Sistemi ve Bilgisayar

1. Bilgisayar

TCK’da düzenlenmiş olan bilişim alanındaki suçları iki şekilde işlenmektedir. Bir suç, bilişim sistemine karşı işlenebileceği gibi; bilişim sistemi kullanılarak bir suçun işlenmesi de mümkün olabilmektedir. Bu iki durumda da uygulamada en çok karşılaşılan araç ve mecra kuşkusuz ki bilgisayarlardır²⁴. Bu nedenle öncelikle bilgisayar kavramının ve özelliklerinin incelenmesi yerinde olacaktır.

Türk Dil Kurumuna göre “*Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin*²⁵” olarak tanımlanan bilgisayar için doktrinde çeşitli tanımlar²⁶ yapıldığı görülmektedir. Bu tanımlar içerisinde “*Dış ortamdan aldığı verileri, üzerine yüklenen programlar aracılığıyla depolayan, işleyen, yeni sonuçlar üreten, ürettiği sonuçları kullanıcıya sunan, veri iletişimini sağlayan makine*²⁷” tanımı gerek ilgili kavramı daha kapsayıcı bir bakış açısıyla ele alması gerekse incelemekte olduğumuz

²² Resmi Gazete, 3756 Sayılı 765 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun, T. 14.06.2021 <https://www.resmigazete.gov.tr/arsiv/20901.pdf> (E.T. 19.10.2021)

²³ Dülger, a.g.e. s. 66-67.

²⁴ Akbulut, a.g.e. s. 5. Yavuz Erdoğan, *Türk Ceza Kanunu’nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları ile)*, Legal Yayıncılık, 2012 s. 8.

²⁵ <https://sozluk.gov.tr> (E.T. 19.10.2021)

²⁶ Yazıcıoğlu, *Bilgisayar Suçları* s. 24-26. Akbulut, a.g.e. s. 10-12. Sulhi Dönmezer, *Kişilere ve Mala Karşı Cürümler*, 17. Baskı, İstanbul: Beta Basım A.Ş., 2004, s. 617. Kurt, a.g.e. s. 31 Özgür Eralp, *Hukukçular İçin Bilişim Terimleri Sözlüğü*, Ankara: Avbil Yayınları, 2007 s. 26.

²⁷ Yenidünya/Değirmenci, a.g.e. s. 19

suçun işlenebilmesi için olmazsa olmaz olan “*veri depolama*” niteliğini içermesi bakımından yapılan tanımlar içerisinde en yerinde olanıdır²⁸.

Burada değinilmesi gereken önemli bir husus ise söz konusu tanımlardaki unsurları taşıyan tüm cihazların bilgisayar sayılamayacağıdır. Örneğin Charles Babbage tarafından geliştirilen çözümleyici makine ya da İkinci Dünya Savaşı’nda kullanılan Harvard Mark I ve ENIAC gibi makineler de sayılan unsurları bulundurmasına rağmen günümüzdeki kullanım biçimiyle bilgisayar sayılamayacaklardır²⁹. Bilgisayar, tek bir amaca özgülenmiş hesap makineleri gibi araçların aksine genel olarak programlanabilmekte, önceden tanımlanmış olması kaydıyla her türlü işlemi yapabilmektedir³⁰. Ayrıca tek bir amaca özgülenmiş makinelerin aksine bilgisayarda kullanım amacına göre yüklü bulunan yazılımların yanına yenileri eklenebilmekte yahut bu yazılımlar silinebilmektedir³¹.

Hukuki metinlere bakıldığında ise Avrupa Konseyi Siber Suç Sözleşmesi Açıklayıcı Raporu’nun 23. maddesinde bilgisayar “*dijital verilerin otomatik olarak işlenmesi için geliştirilmiş donanım ve yazılımdan oluşan bir cihaz*” olarak tanımlanmıştır. Maddeye göre “*otomatik*” ifadesi ile kastedilen verilerin işlenmesi sırasında insan müdahalesinin olmamasıdır. Yine aynı maddede bilgisayarın giriş, çıkış ve depolama birimleri ile merkezi ve çevre birimlerine sahip olabileceği ve tek başına çalışabileceği gibi başka makinelerle yahut ortak bir ağa bağlanarak da çalışabileceği ifade edilmiştir³². Adalet Bakanlığı tarafından hazırlanmış olan 2006 tarihli Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı’nda ise “*Belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçlar...*”³³ olarak tanımlanmıştır.

Bilgisayarları oluşturan unsurlar yazılım(software) ve donanım(hardware) olarak ikiye ayrılmaktadır. Bu unsurlardan donanım, bilgisayarın fiziksel olarak algılanabilen parçalarını ifade etmekte olup çeşitli türleri bulunmaktadır. Klavye, fare,

²⁸ Dülger, **a.g.e.** s. 59.

²⁹ Ifrah, **a.g.e.** s. 31-32.

³⁰ Bozdoğan Akbulut **a.g.m.** s. 545.

³¹ Dülger, **a.g.e.** s.63-64.

³² Conseil of Europe, **Explanatory Report to the Convention on Cybercrime**, 23.11.2001 <https://rm.coe.int/16800cce5b> (E. T. 01.03.2021)

³³ Türkiye Cumhuriyeti Adalet Bakanlığı **Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı**, , 2006 <https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/> (E.T. 09.03.202)

tarayıcı, kamera ve mikrofon gibi dış ortamdaki verileri bilgisayara aktarmak için kullanılan araçlar giriş birimleri; bilgisayarda işlenen verileri, işlenmesinin ardından okunabileceği ve saklanabileceği manyetik bir ortama, bir ekrana ya da bir tür kâğıt üzerine aktarmaya yarayan monitör, yazıcı ve hoparlör gibi parçalara ise çıkış birimleri denir. Ana kart ve işlemci gibi bilgisayara dışarıdan alınan veriler üzerinde çeşitli işlemlerde bulunan parçalar ana işlem birimi olarak adlandırılmaktadır. İşlem birimleri tarafından işlenmiş yahut işlenmemiş verilerin saklanması maksadıyla kullanılan Hard Disk(HDD ya da SSD), RAM, USB bellek ya da CD-DVD Rom gibi birimlere depolama; bu verilerin farklı bilgisayarlar arasında iletilmesini sağlayan data ve ağ kablosu, modem gibi birimlere ise iletişim birimleri adı verilmektedir. Yazılım ise bilgisayarın; fiziki olarak var olmayan, soyut olarak çalıştırılabilen parçalarıdır. Bilgisayar her açıldığında çalışmaya başlayan ve tüm işlemlerin üzerinde yapıldığı Windows, Mac, Linux gibi işletim sistemlerine sistem yazılımı; uyumlu olduğu işletim sistemi üzerinden çalıştırılarak belli amaçların ifa edilmesine özgülünen programlara ise uygulama yazılımı denir. Microsoft Word ve Excel gibi ofis yazılımları, Mozilla Firefox ve Google Chrome gibi tarayıcılar, Winrar, anti-virüs programları ya da video oyunları gibi çeşitli amaçlar için kullanılan yazılımlar bu kapsamdadır. Genel olarak sistem yazılımları dışında kalan tüm program ve uygulamalar uygulama yazılımıdır³⁴.

2. Bilişim Sistemi

Bilişim alanındaki suçlar, söz konusu olduğunda en çok karşılaşılan araç ve suç mecrası bilgisayar olsa da Yargıtayın da kararlarında ifade ettiği gibi “*bilişim sistemi*” kavramı bilgisayarlarla sınırlı değildir³⁵. Yukarıda verilen bilişim ve bilgisayar tanımları incelendiğinde görülebilecektir ki her bilgisayar yapısı gereği bir bilişim sistemi ya da bilişim sisteminin bir parçası olmak zorunda olsa da bilgisayar dışında da bilişim sistemi özelliklerini bünyesinde barındıran cihazlar bulunmaktadır³⁶.

³⁴ Akbulut, **a.g.e.** s. 12. Dülger, **a.g.e.** s. 60-63. Tunç Demircan, **Bilişim Alanında Suçlar**, İstanbul: Legal Yayıncılık, 2016 s. 12-15. Kurt, **a.g.e.** s. 31-17. Erdoğan, **Türk Ceza Kanunu’nda Bilişim Suçları** s. 24. Hüseyin Akarslan, **Bilişim Suçları, 2. Baskı**, İstanbul: Seçkin, 2015 s. 31.

³⁵ YCGK., E. 2014/288 K. 2016/255 T. 10.5.2016 www.lexpera.com.tr (E. T. 08.12.2021)

³⁶ Dülger, **a.g.e.** s. 8. Yenidünya/Değirmenci, **a.g.e.** s. 27. Ersoy, **a.g.e.** s. 151. Şaban Cankat Taşkın, **Bilişim Suçları**, İstanbul: Beta Yayınevi, 2008 s. 2.

Bilişim sistemi için doktrinde yapılan tanımlar³⁷ ve açıklamalar³⁸ incelendiğinde verilerin sisteme yüklenerek işlenip çıktı haline getirilmesini ifade eden “*veri işleme*” ile bu verilerin bilişim sistemleri arasında çeşitli ağlar vasıtasıyla aktarılması anlamına gelen “*veri iletişimi*” unsurlarının bilişim sisteminin temelini oluşturduğu görülecektir³⁹. Şu hâlde bilişim sistemi kısaca üzerine veri yüklenebilen, bu verileri otomatik bir şekilde işleme tabi tutabilen ve bu işlemler sonucu ortaya çıkan verileri diğer bilişim sistemlerine aktarabilen elektronik- manyetik sistemler olarak tanımlanabilir⁴⁰.

5237 sayılı TCK ile birlikte eski kanundaki “*bilgileri otomatik işleme tabi tutan sistem*” ifadesi terkedilerek yerine “*bilişim sistemi*” terimi tercih edilmiştir. Bu değişiklik kavramın kapsamını genişletmekte, gelişmekte olan ve ileride gelişen teknolojilere karşı işlenen suçların da kanun kapsamına alınmasını kolaylaştırmaktadır⁴¹. Kanun gerekçesinde ise bilişim sistemi “*Verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemler.*”⁴² olarak tanımlanmıştır. Yargıtay da kararların istikrarlı olarak bu tanıma kullanmıştır⁴³. Bu tanım hem bilişim sistemini sadece manyetik cihazlara indirgemesi⁴⁴ nedeniyle hem de bilişim sisteminin veri işleme yönünü kapsamasına rağmen veri iletim işlevini barındırmaması nedeniyle doktrinde eleştirilmiş, kanun koyucunun burada bilgisayarın tanımını yaptığı öne sürülmüştür⁴⁵. Yine doktrinde

³⁷ Tanımlar için bkz. Ahmet Caner Yenidünya, “*Bilişim Sistemine Hukuka Aykırı Erişim Suçu*”, **Legal Fikri ve Sınai Haklar Dergisi**, C. 1, S. 4, 2005 s. 1029. Kubilay Taşdemir, **Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları**, Ankara: Cantekin Matbaacılık, 2009 s. 243. İsmail Malkoç, **Açıklamalı İctihatlı Yeni Türk Ceza Kanunu**, C. 2, Ankara: Malkoç Kitabevi, 2007 s. 1665. Nurullah Aydın, **Türk Suç ve Ceza Hukuku Genel ve Özel Hükümler**, 2. Baskı, Ankara: Adalet Yayınevi, 2009 s. 380. Akarslan, **a.g.e.** s. 30. Özçelik, **a.g.e.** s. 52. Veli Özer Özbek/ Koray Doğan/ Pınar Bacaksız, **Türk Ceza Hukuku Özel Hükümler, Genişletilmiş ve Güncellenmiş 16. Baskı**, Ankara: Seçkin, 2021 s. 957.

³⁸ Kimi yazarlar bir tanım yapmaktan kaçınmış, sadece bir sistemin bilişim sistemi olabilmek için taşınması gereken özellikleri saymakla yetinmiştir: Kurt, **a.g.e.** s. 140. Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara: Adalet Yayınevi, 2008 s. 19. Şaban Cankat Taşkın, “*Bilişim Hukuku Uluslararası Uyuşmazlıklar*”, **Türkiye Barolar Birliği Dergisi**, S. 85, Aralık 2009 s. 333-334. Erdoğan, **a.g.e.** s. 16. Mahmut Koca/İlhan Üzülmmez, **Türk Ceza Hukuku Özel Hükümler**, 7. Baskı, Ankara: Adalet Yayınevi, 2020 s. 898.

³⁹ Akbulut, **a.g.e.** s. 13-17.

⁴⁰ Özbek/Doğan/Bacaksız, **a.g.e.** s. 957. Koca/Üzülmmez, **a.g.e.** s. 898. Akarslan, **a.g.e.** s. 30. Taşkın, **a.g.m.** s. 333-334. Özçelik, **a.g.e.** s. 52.

⁴¹ Yazıcıoğlu, **Bilgisayar Suçları** s. 215. Kurt, **a.g.e.** s. 139.

⁴² **Türk Ceza Kanunu Madde Gerekçeleri** www.lexpera.com.tr (E. T. 12.04.2021)

⁴³ YCGK. E. 2007/6-136 K. 2007/150 T. 19.6.2007, YCGK., E. 2014/288 K. 2016/255 T. 10.5.2016 www.lexpera.com.tr (E. T. 08.12.2021)

⁴⁴ Erdoğan, **a.g.e.** s. 10-11. Ketizmen, **a.g.e.** s. 17-18.

⁴⁵ Ali İhsan Erdağ, “*Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)*”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C.XIV, Sayı:2, 2010 s. 277-278. R. Yılmaz Yazıcıoğlu, “*Yeni Türk Ceza*

gerekçedeki bu tanımın; uygulamada esas alınması halinde yanlış uygulamalara sebebiyet verebilecek düzeyde hatalı olduğu dile getirilmiştir⁴⁶. Karşıt bir görüş ise; “*bilgileri otomatik işleme tabi tutmuş sistem*” kavramı ile ifade edilmek istenenin “*Mantıklı bir düzene uygun suretle verileri otomatik olarak işleme tabi tutan sistem*.”⁴⁷ olduğunu savunmuştur; yapılan bu tanım kavramın kapsamını genişletmesi nedeniyle doktrinde desteklenmiştir⁴⁸.

2006 yılında Adalet Bakanlığı tarafından hazırlanan fakat kanunlaştırılmayan “*Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı*” bünyesinde, bilişim sistemi “*bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem*” olarak tanımlanmıştır. Her ne kadar söz konusu tasarı yasalaşmamış olsa da 20 Eylül 2011’de Resmî Gazete’de yayımlanarak yürürlüğe giren Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik⁴⁹ madde 3’te de aynı tanımın tekrar edildiği görülmektedir. Bu tanım gerek bilişim sisteminin unsurlarını eksiksiz olarak barındırması gerekse TCK gerekçesinde yapılan tanımda kapsam dışı bırakılan bilişim sisteminin veri iletim ve saklama özelliğini barındırması açısından TCK gerekçesindeki tanıma göre daha yerinde bulunmuştur⁵⁰.

AKSSS’deki tanımdan önce kavramın çevirisinde mevcut olan bir ikilikten bahsetmek yerinde olacaktır. Sözleşmenin İngilizce, Almanca ve Rusça nüshalarında “*bilgisayar sistemi*” olarak tercüme edilebilecek terimler kullanılmışken⁵¹; Fransızca, İspanyolca ve İtalyanca nüshalarında “*bilişim sistemi*” olarak Türkçeleştirebileceğimiz kavramlar tercih edilmiştir⁵². 2 Mayıs 2014 günü Resmi Gazete’de Sanal Ortamda İşlenen Suçlar Sözleşmesi olarak yayınlanan Türkçe nüshada ise “*bilgisayar sistemi*” ifadesi tercih edilmesine rağmen kanaatimizce tanımlanmak istenen terim “*bilişim*

Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi” Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.2, S. 2, İstanbul, 2005 s. 404 Koca/Üzülmez, a.g.e. s. 898.

⁴⁶ Özbek/Doğan/Bacaksız a.g.e. s. 958.

⁴⁷ Dönmezer, a.g.e. s. 617.

⁴⁸ Taşkın, Bilişim Suçları s. 7.

⁴⁹ Resmi Gazete, Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik, 20.11.2011 <https://www.resmigazete.gov.tr/eskiler/2011/09/20110920-4.htm> (E.T. 08.12.2021).

⁵⁰ Oğuzhan Emre Parlak, Türk Ceza Muhakemesinde Bilişim Sistemlerinde Arama, Kopyalama ve Elkoyma, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, 2019 s. 5-6.

⁵¹ Sözleşmenin İngilizce Nüshasında “*computer system*”, Almanca nüshasında “*Computersystem*”, Rusça nüshasında ise yine aynı anlama gelen “*компьютерная система*” terimleri kullanılmıştır.

⁵² Sözleşmenin Fransızca Nüshasında “*système informatique*”, İspanyolca nüshasında “*sistema informatico*”, İtalyanca nüshasında ise “*sistema informatico*” terimleri kullanılmıştır.

sistemi” terimidir. Sonuç olarak ilgili sözleşmede bilişim sistemi: “*Bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı.*” olarak tanımlanmıştır. İşbu tanım incelendiğinde bilişim sistemlerinin sadece veri işleme yönüne değinildiği, veri iletimi kısmının kapsam dışında bırakıldığı görülmektedir.

Günümüze gelindiğinde ise bilişim sistemlerinde sayısız işlemin yapıyor olması, bu işlemlerin denetiminde yeterli kontrol mekanizmalarının kurulamamış olması ve bu süreçlerdeki anonimlik; bilişim sistemlerini suç işlenmesi için uygun bir ortam haline getirmektedir⁵³.

C. Bilişim Suçu

1. Terim Sorunu

Temel olarak bilişim sisteminin işleyişine, verilerin bütünlüğüne ve gizliliğine yönelmiş olan⁵⁴ bilişim suçları adlandırılırken gerek uluslararası literatür gerekse ülkemiz doktrininde farklı kavramların kullanıldığı görülmektedir. Bilişim suçları ilk olarak bilgisayarın da keşfedildiği yer olan Amerika Birleşik Devletleri’nde tartışılmaya başlanmış ve Amerikan doktrini tarafından isimlendirilmiştir⁵⁵. İlk gözlemlenen bilişim suçlarının bilgisayarla karşı ya da bilgisayar kullanılarak işlenmesinin de etkisiyle Amerikan doktrininde esas olarak “*computer crime*”⁵⁶(*bilgisayar suçu*)” kavramı kullanılmıştır. Bunun yanında “*computer related crime*”⁵⁷(*bilgisayarla bağlantılı suç*), “*computer-assisted crime*(*bilgisayar destekli suç*)” ve “*crime against computer*(*bilgisayara karşı suç*)” terimleri de çalışmalarda tercih edilmiştir⁵⁸.

⁵³ Emin D. Aydın “*Bilişim Sistemlerinde Güvenlik, Güvenilirlik, Mahremiyet ve Bilişim Suçları*”, **Marmara İletişim Dergisi**, İstanbul, S.1, Aralık 1992 s. 113-116.

⁵⁴ Ulrich Sieber, “*Bilişim Suçları*”, **Bilişim Teknolojileri ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku (Yazarın Seçilmiş Makaleleri)**, Editörler: Prof. Dr. Feridun YENİSEY, Av. Dr. Salih OKTAR, DR. Öğrt. Üyesi Zehra BAŞER DOĞAN, Ankara: Seçkin, 2021 s. 260.

⁵⁵ Dülger, **a.g.e.** s.70.

⁵⁶ Ian Walden, “*Harmonising Computer Crime Laws in Europe*”, **European Journal of Crime, Criminal Law and Criminal Justice**, Vol. 12, Issue 4, 2004, s. 321 vd.

⁵⁷ Ulrich Sieber, “*Legal Aspects of Computer-Related Crime in Information Society-A Comcrime Study*”, **European Commission Information Society**, 1 Ocak 1998 s. 18 <https://www.law.tuwien.ac.at/sieber.pdf> (E.T. 15.12.2021)

⁵⁸ Dülger, **a.g.e.** s. 70. Erdoğan, **a.g.e.** s. 44.

Her ne kadar bu suçlar hukuk literatürüne bilgisayar sayesinde girmiş olsa da son yıllarda “*cybercrime*⁵⁹(siber suç)” terimi de bilimsel çalışmalarda yaygın bir şekilde kullanılmaya başlanmış, neredeyse “*computer crime*” kavramının önüne geçmiştir. Öte yandan meydana gelen teknolojik gelişmelerin ceza hukukuna olan etkisinin artmasına paralel olarak “*e-crime*⁶⁰(e-suç)”, “*techno crime*⁶¹(teknoloji suçu)”, “*hi-tech crime*⁶²(yüksek teknoloji suçu)” ve “*technology-enabled crime*⁶³(teknoloji destekli suç)” gibi ifadeler de akademik çalışmalarda yer almıştır. Bunun yanında Almanya’da “*computerkriminalität*(bilgisayar suçu)”, Fransa’da ise “*la fraude informatique*(bilgişim suçu)” kavramlarının tercih edildiği görülmektedir⁶⁴.

Dünyaya paralel olarak ülkemizde de kavramın isimlendirilmesi konusunda fikir birliği olmadığı görülmektedir. Yazarlar tarafından “*sanal suç*”, “*siber suç*⁶⁵”, “*elektronik suç*”, “*dijital suç*⁶⁶”, “*sınırşan suç*⁶⁷”, “*çok yargısal suç*”, “*internet suçu*⁶⁸”, “*bilgisayar suçu*⁶⁹”, “*bilgisayar ile ilgili suç*⁷⁰”, “*bilgişim suç hukuku*⁷¹”,

⁵⁹ Orin S. Kerr, “Cybercrime’s Scope: Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes”, *New York University Law Review*, Vol. 78, 2003, s. 1596 vd. <https://heinonline.org/> (E.T. 11.12.2021)

⁶⁰ Majid Yar, “E-Crime 2.0: The Criminological Landscape of New Social Media”, *Information & Communications Technology Law*, Volume 21, Issue 3, 2012 s. 207 vd. <https://heinonline.org/> (E.T. 11.12.2021)

⁶¹ James M. Byrne/ Kathryn A. Kimball, “Inside The Darknet: Techno-Crime And Criminal Opportunity”, *Criminal Justice Technology In The 21st Century: Third Edition*, Ed. Laura J. Moriarty, Springfield, 2017 s. 206 vd.

⁶² Paul Norman, “Policing ‘Hi-Tech’ Crime Within The Global Context: The Role Of Transnational Policy Networks”, *Crime and The Internet*, Ed. David Wall, London: Routledge, 2001 s. 184 vd. <https://www.taylorfrancis.com/> (E.T. 11.12.2021)

⁶³ Sam McQuade, “Technology-enabled Crime, Policing and Security”, *Journal of Technology Studies*, 2006 <http://scholar.lib.vt.edu/ejournals/JOTS/v32/v32n1/pdf/mcquade.pdf> (E.T. 11.12.2021) s. 32 vd.

⁶⁴ Dülger, *a.g.e.* s.70-71.

⁶⁵ Hasan Sınar, *İnternet ve Ceza Hukuku*, İstanbul: BETA, 2001 s.69-70. Ergün, *a.g.e.* s. 13-14. Sacit Yılmaz, *Türk Ceza Hukuku Sisteminde Siber Suçlar*, Ankara, Adalet Yayınevi, 2016

⁶⁶ Emre Cihan Ateş “Suç 4.0: Dijital Suç ve Güvenlik”, *Dijital Dönüşüm Trendleri*, İstanbul: Filiz Kitabevi, Mayıs 2019 s. 258 vd.

⁶⁷ Ersoy, “*a.g.e.*”, s. 173 dipnot.

⁶⁸ Feridun Yenisey, “İnternet Suçlarının Yeni İşleniş Biçimleri”, *Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001*, İzmir: Dokuz Eylül Üniversitesi Yayınları, 2002 Sevil Yıldız, *Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi*, Ankara: Nobel Yayın Dağıtım, 2007 s.38-39., Veli Özer Özbek, “İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları” *DÜHFD*, C. 4, S. 1, İzmir, 2002 s. 106-107. Mehmet Niyazi Tanılır, *İnternet Suçları ve Bireysel Mahremiyet*, Ankara: Liberte Yayınları, 2002 s. 13 vd.

⁶⁹ Yazıcıoğlu, *Bilgisayar Suçları* s. 53vd. Faruk Erem, “Bilgisayar Suçları ve Türk Ceza Kanunu”, *Yargıtay Dergisi*, C. 17, S. 4, Ekim 1991 s. 436vd. Erol Çetin, İsmail Malkoç, *Uygulamada Sahtekarlık Suçları, Bilgisayar Suçları, Tebligat Suçları ve İlgili Mevzuat*, Ankara: Adalet Yayınevi, 1995 s.543vd.

⁷⁰ Hasan Dursun, “Bilgisayar ile İlgili Suçlar”, *Yargıtay Dergisi*, C. XXIV, S. 3, Ankara, 1998 s. 334vd.

⁷¹ İnancı bilgişim hukukunu “*bilgişim telif hukuku*” ve “*bilgişim suç hukuku*” olarak ikiye ayırmıştır. Halil İnancı, “*Bilgişim ve Yazılım Hukuku Uygulama İçinden Görünüşü*”, *İstanbul Barosu Dergisi*, C. LLX, S. 7-8-9, İstanbul 1998 s. 512-513.

“*bilişim sistemi aracılığıyla işlenen suç*⁷²” terimleri kullanılmış, “*bilişim suçu*⁷³” ve 5237 sayılı TCK’nın tercih ettiği “*bilişim alanındaki suç*⁷⁴” ise bunlar içerisinde en sık tercih edilenler olmuştur. Gerçekten de “*bilişim suçu*” ve “*bilişim alanındaki suç*” dışındaki kavramların kastettiğimiz suç gurubunu nitelendirme konusunda yetersiz olduğu görülmektedir.

İncelemekte olduğumuz suçların işlenmesi için zemin oluşturan ağlardan en yaygın kullanılanı internet olsa da yukarıda açıklanan “*bilişim alanı*” kavramı internet ile sınırlı değildir. Bilişim suçları internet ağlarının yanı sıra intranet, extranet gibi benzer ağ modelleri üzerinde de işlenebileceği⁷⁵ gibi herhangi bir ağ kullanılmadan doğrudan bilgisayarlar üzerinde de işlenebilmektedir⁷⁶. Bu nedenle internet üzerinden işlenen suçlarla ilgili spesifik çalışmalar⁷⁷ haricinde “*internet suçu*” teriminin kullanılması doğru değildir. Kaldı ki bu kapsamda yapılan bir çalışmada incelenecek suçların da salt internet üzerinden işlenebiliyor olması yani internete özgü suçlar⁷⁸ olması gerekmektedir. Aksi halde “*internet suçu*” terimini kullanımı anlatılan suçu tanımlamakta yetersiz olacaktır.

Çeşitli yazarlarca benimsenen “*bilgisayar suçu*”, “*bilgisayara karşı suç*”, “*bilgisayar destekli suç*” gibi terimler ise özellikle kapsayıcılık yönünden eleştirilmiştir. Zira incelemekte olduğumuz suçlar yalnızca bilgisayarlara karşı ya da bilgisayarlar aracılığıyla değil; örneğin bilgisayarlar sayılamayacak mobil cihazlar, banka ATM’leri ya da bilgisayarları birbirine bağlayan ağ protokollerine karşı ya da bunlar kullanılarak da işlenebilir. Bu nedenle daha geniş çaplı bir alanı ifade eden

⁷² Yener Ünver, “*Türk Ceza Kanunu’nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi*”, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası İnternet Özel Bölümü*, Cilt. LIX, Sayı.1-2, İstanbul, 2001 s. 78-79.

⁷³ Köksal Bayraktar, “*Banka ve Kredi Kartları ile Ortaya Çıkan Ceza Hukuku Sorunları*”, **Prof. Dr. M. Kemal Oğuzman’ın Anısına Armağan**, İstanbul: Beta Yayınları, Ocak 2000 s. 202. Durmuş Tezcan/ Mustafa Ruhan Erdem/ Murat Önok, **Teorik ve Pratik Ceza Özel Hukuku, Güncellenmiş 19. Basım**, Ankara: Seçkin, 2021 s. 1147. Yenidünya/Değirmenci, **a.g.e.** s. 27. Akbulut, **a.g.e.** s. 549. Koray Doğan, “*Bilişim Suçları ve Türk Ceza Kanunu*”, **Hukuk ve Adalet Eleştirel Hukuk Dergisi**, Y.2 S.6, 2005 s. 294.

Ersoy kanundaki “*bilişim suçu*” terimini benimsemiş olsa da yer yer “*bilgisayar suçu*” terimini de geniş anlamda kullanmıştır. Ersoy, **a.g.e.** s. 151-152.

⁷⁴ Akbulut, **a.g.e.** s. 58 vd.

⁷⁵ Sınar, **a.g.e.** s. 69. Yenidünya/Değirmenci, **a.g.e.** s. 31-32. Taşkın, **a.g.e.** s. 11.

⁷⁶ Akbulut, **a.g.e.** s. 59.

⁷⁷ Bkz. Özbek **a.g.e.** s. 107.

⁷⁸ Yıldız internet suçlarını “*internet aracılığıyla gerçekleştirilen eylemler*” ve “*internete özgü eylemler*” şeklinde iki gruba ayırmakta; internete özgü eylemleri ise “*internet yoluyla yine internetin içinde bulunduğu bilgisayar sisteminin çeşitli unsurlarına yönelik müdahaleler*” olarak tanımlamaktadır. Yıldız, **a.g.e.** s. 38-39..

“*bilişim suçu*” kavramının tercih edilmesi yerinde olacaktır⁷⁹. Öte yandan nasıl ki kasten öldürme veya yaralama suçlarının işlendikleri mekâna göre adlandırılması söz konusu değilse; bilişim suçlarının da kullanılan cihaza göre “*bilgisayar suçu*” olarak adlandırılması da söz konusu olmamalıdır⁸⁰.

İnternet ağına göre daha geniş kapsamlı olan “*siber uzay*” kavramından yola çıkılarak “*siber suç*” ve “*sanal suç*” kavramları da doktrinde bazı yazarlarca kullanılmaktadır. Bu yazarlara göre bu kavramların tercih edilmesinin nedeni internet suçuna göre daha geniş kapsamlı olmalarıdır. Nihayetinde her siber suç internet suçu olmasa da her internet suçu aynı zamanda bir siber suçtur⁸¹. “*Siber suç*” ve “*sanal suç*” kavramları daha kapsayıcı olmasına rağmen işlenen suçların sadece sanal ağlar üzerinden işlenebileceği ve bu suçların fiziki karşılıklarının bulunmadığı izlenimini uyandırması nedeniyle eleştirilmiştir⁸². Ayrıca özellikle kolluk tarafından benimsenen “*siber suç*” kullanımı sözcüğün kökeninin Türkçe olmaması nedeniyle eleştirilmiş, halihazırda hem Türkçe hem de anlam olarak daha kapsayıcı olan “*bilişim suçu*” teriminin kullanımının daha yerinde olacağı ifade edilmiştir⁸³.

“*Bilişim sistemi/bilgisayar aracılığıyla işlenen suç*” ve “*bilişim sistemine/bilgisayara karşı işlenen suç*” gibi terimlerin ise suç tiplerinin incelenirken yapılacak sınıflandırmalarda kullanılması kabul edilebilir olsa da bu terimler bilişim suçları gibi çok boyutlu bir olguyu ele almak için yetersiz kalacaktır. Zira bu kavramlar incelemekte oldukları suçları ve fiilleri tek yönlü olarak ele almakta, teknolojinin gelişmesiyle de bağlantılı olarak gelişen ve değişen bir yapısı olan “*bilişim suçlarını*” kapsamak konusunda yetersiz kalmaktadır⁸⁴.

Kimi yazarlarca kullanılan “*elektronik suç*” ve “*dijital suç*” kavramları ise elektronik ve dijital cihazların sadece bilgisayar ve bilişim sistemi ile sınırlı olmadığı gerekçesiyle eleştirilmiş ve tercih edilmemiştir⁸⁵.

⁷⁹ Yenidünya/Değirmenci, **a.g.e.** s. 30-31.

⁸⁰ **a.g.e.** s. 32.

⁸¹ Sınar, **a.g.e.** s. 69. Yılmaz, **a.g.e.** s. 5.

⁸² Ünver, **a.g.e.** s. 78-79. Tezcan/Erdem/Önok, **a.g.e.** s. 1147.

⁸³ Dülger, **a.g.e.** s. 72. Yenidünya, **a.g.e.** s. 1020-1021.

⁸⁴ Dülger, **a.g.e.** s. 72-73.

⁸⁵ Akbulut, **a.g.e.** s. 59. Ö. Umut Eker, “*Türk Ceza Hukuku’nda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 s. Yeni Türk Ceza Kanunu’nun İlgili Hükümlerinin Yorumu*”, **TBB Dergisi**, Yıl:19, Sayı: 62, Ocak-Şubat 2006 s. 103.

Bilişim suçlarının ortaya çıktığı ve ülkemizde tanınmaya başladığı yıllarda kimi yazarlarca yukarıda örnekleri verilen farklı adlandırmalar tercih edilmişse de günümüzde “*bilişim suçu*” kavramı üzerinde doktrinde görüş birliğine varılmış; bu çalışmada da hem Türkçe olması hem de genel ve kapsayıcı bir kavram olması sebebiyle “*bilişim suçu*” teriminin kullanımı tercih edilmiştir.

2. Bilişim Suçlarının Tanımlanması ve Sınıflandırılması

Gerek ülkemiz gerekse karşılaştırmalı hukuk mevzuatı incelendiğinde; bilişim suçları kavramının tanımlanmasından kaçınıldığı, bu suçlara sebebiyet veren fiillerin tek tek sayılması yoluyla düzenlemeler yapıldığı görülmektedir⁸⁶. Bu kapsamda AKSSS’de de düzenleme konusu suçlar tanımlanmamış, imzacı devletlerin engellemekle yükümlü oldukları fiillerin tek tek sayılması yoluna gidilmiştir. Doktrinde de her ne kadar yazarlar tarafından çeşitli tanımlamalar yapılmış olsa da üzerinde uzlaşılan bir tanımın mevcut olmadığı görülmektedir⁸⁷.

Kimi yazarlar bilişim suçlarını tanımlarken temel kriter olarak suçun bilişim sistemi ile ilgisi olmasını; suçun bu sistemler kullanılarak ya da bu sistemlere karşı işlenmesini aramıştır⁸⁸. Bu yaklaşım bilişim sistemlerine özgü olmayan klasik suçların da bilişim suçu olarak değerlendirilmesine yol açabilecek olması nedeniyle sakıncalıdır. Bilişim suçları tanımlanırken, bilişim sistemlerinin fiziksel varlığının suçun hedefi değil daima aracı olduğu unutulmamalıdır. Zira suçu işleyen failin hedefi bilişim sistemi gibi görünse de suçla hedeflenen söz konusu sistemdeki veriler yahut bu sistemin işleyişidir. Bilişim sisteminin içerdiği verilere ya da sistemin işleyişine zarar verilme kastı olmaksızın yerinin değiştirilmesi ya da bu sistemin fiziki varlığına

⁸⁶ Carlo Sarzana, “*Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması İtalya’daki Durum*”, Çev. Vesile Sonay Daragenli, **İstanbul Hukuk Fakültesi Dergisi**, Prof. Dr. Türkan Rado’ya Armağan Sayısı, C.LV, S.3 İstanbul 1997s. 393-394.

⁸⁷ Akbulut, **a.g.e.** s. 55. Olgun Değirmenci, **Bilişim Suçları**, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul, 2002 s. 56.

⁸⁸ “*Bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suç*” Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 5. Bası**, Ankara: Seçkin Yayınevi, 2014 s.57. “*Verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi, ve iletilmesi ile ilgili ve bilişim alanı içinde işlenen, bir bilgisayar ya da ağına yönelik olarak ya da onları kullanarak icra edilen her türlü yasadışı eylem*” Kurt, **a.g.e.** s. 53. “*Bilişim sistemlerine yetkisiz olarak erişimde bulunarak, bilişim sistemleri aracılığıyla bu sistemde yer alan veri ya da verileri yetkisiz bir şekilde çeşitli saiklerle kendisinin ya da başkasının yararına kullanma, erişilmez kılma, silme, değiştirme veya bozma suretiyle işlenen suçlar*” Cengiz Apaydın, “*Bilişim Sistemine Girme Suçu*”, **Türkiye Adalet Akademisi Dergisi**, Y. 7, S. 24, Ocak 2016, s. 251.

zarar verilmesi bilişim suçu olarak değerlendirilmeyip TCK'nın -hırsızlık ya da mala zarar verme suçu gibi- ilgili hükümlerine tabi olacaktır⁸⁹.

Kimi yazarlar ise bilişim suçlarını sadece malvarlığı ihlalleriyle sınırlamış, tanımlarını da bu kapsamda yapmıştır⁹⁰. Bu yaklaşım maddi değer taşımayan bilişim verilerini hedef alan fillerin ve bilişim sistemlerine yönelik maddi kazanç elde etme amacı taşımayan sabotaj ve saldırılarını bilişim suçu sayılmamasına neden olduğu için eleştirilmiş ve doktrinde benimsenmemiştir⁹¹.

Bilişim suçlarına ilişkin şimdiye kadar yapılan tanımlar incelendiğinde görülecektir ki yapılan tanımlar zaman içinde güncelliğini kaybetmiş, teknolojinin gelişimi ile birlikte ortaya çıkan yeni fiiller de yapılan tanımlarda yer bulmaya başlamıştır. Yine suçların tanımlanmasında malvarlığını esas alan yahut failde özel nitelikler arayan yaklaşımlar da zaman içinde terk edilmiştir⁹². Buradan yola çıkan kimi yazarlar ise tüm bilişim suçlarını kapsayan genel geçer bir tanım yapmak yerine bilişim suçlarını gruplandırma yoluna gitmiştir. Örneğin Dülger bilişim suçlarını eylemlerin suç tiplerini baz alarak üç gruba ayırmıştır. Bu ayrıma göre ilk grupta incelemekte olduğumuz bilişim sistemine girme suçu gibi *“bilişim sistemlerinin ve/veya içerdiği verilerin işleyişine, bütünlüğüne, güvenliğine karşı işlenen suçlar”*; ikinci grupta kumar oynanması için yer ve mekan sağlama ya da hırsızlık suçlarının bilişim sistemleri kullanılarak işlenmesinin nitelikli hal sayılması örneklerindeki gibi *“bilişim sistemlerinin kullanılmasının suçun nitelikli unsuru olarak tanımlandığı suçlar”*; üçüncü grupta ise hakaret, tehdit gibi suçlarda olabileceği gibi *“bilişim sistemlerinin yalnızca bir araç olarak kullanıldığı ancak suçun unsuru olarak ayrıca tanımlanmadığı suçlar”* bulunmaktadır⁹³.

Amerika Birleşik Devletleri Adalet Bakanlığı'nın da benimsediği bir görüş ise bilişim suçlarını yine üç gruba ayırmıştır. İlk grupta bilgisayarın konusu olduğu suçlar bulunmaktadır. Fiziki olarak bir bilgisayarın donanımının ya da yazılımının çalınması ya da tahrip edilmesi bu gruptaki suçlar için verilebilecek en tipik örneklerdir. İkinci

⁸⁹ Akbulut, **a.g.e.** s. 61. Dülger, **a.g.e.** s. 75.

⁹⁰ “Bilgisayar kullanılarak başkalarının malvarlığına yönelik yapılan her türlü kasti saldırı, tecaviüz” Öykü Didem Aydın, “Bilişim Suçları”, **Bilişim !93 bildiriler: Türkiye Bilişim Derneği Bilişim 93 Etkinlikleri 28 Eylül – 1 Ekim 1993**, İstanbul: İnterpro Yayıncılık, 1993 s. 75.

⁹¹ Akbulut, **a.g.e.** s. 62-63.

⁹² **a.g.e.** s. 69-70.

⁹³ Dülger, **a.g.e.** s. 75. Fatih Selami Mahmutoglu, “Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, **İÜHFİM**, C. LXXI, S.1, 2013, s. 856.

gruptaki suçlarda ise bilgisayar konu olmaktan çıkıp suçun süjesi olmaktadır. Virüs, trojen ya da solucan gibi zararlı yazılımlar kullanılarak işlenen suçlar bu gruba örnek gösterilebilir. Son grupta ise bilgisayarın araç olarak kullanıldığı suçlar bulunmaktadır. Dolandırıcılık ve müstehcenlik suçlarında bilgisayarın kullanıldığı durumlar bu grubun en bilinen örnekleridir⁹⁴.

Bir görüş ise bilişim suçlarını ikili bir sınıflandırma çerçevesinde incelemiştir. İlk grupta bilgisayar sistemine karşı suçlara yer verirken; ikinci grubun ise bilgisayar sistemine yönelik suçlardan oluşacağını ifade etmiştir⁹⁵. Bir başka yazar ise bilişim suçlarını; bilgisayarın maddi konusunu teşkil ettiği suçlar, bilgisayar aracılığıyla işlenen suçlar ve bilgisayar ortamında işlenen suçlar olmak üzere üç grupta incelemiştir⁹⁶. Bilişim suçlarında esas olanın bilişim sisteminin hedef olması olduğunu savunan bir görüş ise suçları üç kategoride incelemiştir. Buna göre bilişim sisteminin fiziki yapısının, sistemin işleyişinin ya da bilişim ağlarının hedef olduğu üç çeşit bilişim suçu vardır⁹⁷.

Bilişim suçlarının tanımlanması sırasında en çok başvurulmuş ve bizim de esas aldığımız sınıflandırma ise dar ve geniş anlamda bilişim suçu ayrımıdır. Bilişim teknolojilerinde yaşanan gelişmelerle birlikte ortaya çıkan fillerin söz konusu olduğu; verilerle veya bu verilerin işlenmesiyle bağlantısı olan ve bilişim sistemleri aracılığıyla ya da bu sistemlere karşı işlenen suçlar dar anlamda bilişim suçlarıdır. Bilişim sistemine girme, sisteme ve verilere yetkisiz müdahale, cihazların kötüye kullanılması gibi klasik bilişim suçları bu kapsama girmektedir⁹⁸. Geniş anlamda bilişim suçları terimiyle ise her türlü bilişim sistemine yahut sistemin içerdiği veriler aracılığıyla yahut bunlara karşı işlenen tüm suçlar ifade edilmektedir. Hırsızlık, dolandırıcılık, hakaret, tehdit gibi klasik suçların bilişim sistemleri kullanılarak yahut bu sistemlere karşı işlenmesi bu kapsama girmektedir⁹⁹. Doktrinde bu ayrımı benimseyen kimi yazarlarca, dar anlamda bilişim suçları için “*bilişim sistemine özgü suçlar*” ve

⁹⁴ Özçelik, **a.g.e.** s. 16. Brain Craig, **Cyberlaw, The Law of the Internet and Information Technology**, New Jersey, Pearson Education, s. 112.

⁹⁵ Dönmezer, **a.g.e.** s. 616.

⁹⁶ Ersoy, **a.g.e.** s. 160.

⁹⁷ Karagülmez, **a.g.e.** s. 71.

⁹⁸ Akbulut, **a.g.e.** s. 69.

⁹⁹ İlker Tepe, “*İnternet (Bilişim) Ceza Hukuku Örneğinde Türk Ceza Hukuku’ndaki Yeni Gelişmeler*” **Alman Türk Karşılaştırmalı Ceza Hukuku**, Yayına Hazırlayanlar Prof. Dr. Eric Hilgendorf, Prof. Dr. Yener Ünver, İstanbul, Yeditepe Üniversitesi Hukuk Fakültesi Yayın No: 17, 2010. S. 274. Ergün, **a.g.e.** s. 32 vd. Dülger, **a.g.e.** s. 75-76.

“doğrudan-gerçek bilişim suçları”; geniş anlamda bilişim suçları için ise “*bilişim sistemleri aracılığıyla işlenebilen suçlar*” ve “*dolayısıyla bilişim suçları - bilişim bağlantılı suçlar*” terimlerini de kullanılmıştır¹⁰⁰.

Geniş anlamda bilişim suçları tanımının esas alınmasına doktrinde şiddetle karşı çıkmıştır. Zira her suçun içerisine araç yahut amaç olarak bilişim sistemlerinin dahil olabilmesi mümkündür. Bu şekilde geniş kapsamlı bir tanım kabul edildiği takdirde içeriği çok geniş ve sınırları belirsiz bir suç türü ortaya çıkacaktır¹⁰¹.

Yargıtay ise verdiği kararlarda dar anlamda bilişim suçları için yapılan tanıma paralel bir şekilde bilişim suçlarını “*verilere ve/veya veri işlemle bağlantısı olan sistemlere karşı bilişim sistemleri aracılığıyla işlenen suçlar*”¹⁰² olarak tanımlamaktadır.

D. Veri

İngilizce “*data*” sözcüğünün dilimizdeki karşılığı olan veri, bilgi sözcüğü ile eş anlamlı olmayıp¹⁰³ bilişim sistemlerinde işlenmek ve depolanmak için biçimlendirilerek yazılım diline çevrilmiş olan bilgilerdir¹⁰⁴. Başka bir deyişle bilişim sistemleri tarafından okunabilen, işlenebilen ve bu sistemler tarafından depolanabilen her şey veri olarak ifade edilebilir¹⁰⁵.

AKSSS’nin 1. maddesinde bilgisayar verisi “*bilgisayar sistemlerinin işlevlerini yerine getirmesinde yardımcı olan programlar dâhil, olguların, bilgilerin veya kavramların bir bilgisayar sisteminde işlenebilir haldeki temsiller*” olarak tanımlanmıştır¹⁰⁶. Sözleşmede kavramın tanımlanırken “*bilgisayar verisi*” olarak adlandırılması kapsamını daralttığı gerekçesiyle eleştirilmektedir. Zira bu haliyle sadece bir bilişim sistemi olan bilgisayarlar üzerinde bulunan veriler tanım kapsamına girmekte; CD ya da taşınabilir bellek gibi fiziksel depolama aygıtları yahut bulut

¹⁰⁰ Nebahat Kayaer, “*Türk Hukukunda Bilişim Sistemine Girme Suçu(TCK m.243.)*”, **Ceza Hukuku Dergisi**, S. 39, Nisan 2019 s. 84-86.

¹⁰¹ Eda Taştumur, **Türk Ceza Hukukunda Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu** s. 19-20.

¹⁰² YCGK. E. 2007/6-136 K. 2007/150 T. 19.6.2007 www.lexpera.com.tr (E. T. 10.04.2021)

¹⁰³ Aydın, **Bilişim Suçları ve Hukukuna Giriş**, s. 3.

¹⁰⁴ Yazıcıoğlu, **Bilgisayar Suçları** s. 29. Dülger, **a.g.e.** s. 76.

¹⁰⁵ Yenidünya/Değirmenci, **a.g.e.** s. 47-48.

¹⁰⁶ Conseil of Europe, **Convention on Cybercrime**, 23.11.2001 <https://rm.coe.int/1680081561> (E.T. 29.09.2021 00:07)

sunucuları gibi üzerine yalnızca veri yüklenebilen sanal bilgi depolarındaki veriler kapsam dışı kalmaktadır¹⁰⁷. Buradan yola çıkarak Özbek, “*elektronik olarak işlenmiş ve saklanmış veri*” teriminin kullanılmasının daha doğru olacağını ifade etmiştir¹⁰⁸.

Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı ile İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun’da ise veri “*Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer*¹⁰⁹” olarak tanımlanmıştır. TCK m. 243’ün gerekçesine bakıldığında ise net bir tanım yapılmamış olsa da “*Sistem içindeki bütün soyut unsurlar, fıkra da geçen ‘veri’ teriminin kapsamındadır.*” denilerek veri kavramının çerçevesi çizilmiştir. Tüm bu düzenlemeler dikkate alındığında kanun koyucunun bilişim sisteminde işlenebilen her değeri veri olarak kabul ederek oldukça geniş bir tanım yaptığı göze çarpmaktadır¹¹⁰.

Bu başlık altında kişisel veri kavramına da değinilmesi yerinde olacaktır. Kişisel veri kavramı, 6698 Kişisel Verilerin Korunması Hakkındaki Kanun¹¹¹ m. 3/d’de “*kimliği belirli veya belirlenebilir gerçek kişiye dair her türlü bilgi*” olarak tanımlanmıştır. Kişisel verileri, kişisel olmayan verilerden ayıran temel farkları; bu verilerin bir kişiye ait olması ve bu kişinin belirli ya da belirlenebilir olmasıdır¹¹². Bir kişiyi blirlemeye yarayan akla gelebilecek her tür objektif ve sübjektif nitelikteki bilgi kişisel veri olarak kabul edilmektedir¹¹³. Bireyin kimliğini saptamaya yarayacak ölçüde onu diğer insanlardan ayıran ve karakterize eden adı, soyadı, doğum tarihi ve taabiyeti gibi özelliklerinin yanı sıra kişinin ailevi, ekonomik, sosyal, siyasal ve kültürel durumuna ilişkin bilgiler de kişisel veri olarak kabul edilmektedir¹¹⁴. Yine kişinin boyu, kilosu, göz rengi gibi fiziksel özellikleri, sağlık ve DNA verileri; parmak

¹⁰⁷ Dülger, **a.g.e.** s. 77.

¹⁰⁸ Veli Özer Özbek, “*Elektronik Ortamda Saklı Bulunan Verilerin Delil Olarak Niteliği*”, İÜFHM, C. LIX. S. 1-2. İstanbul, 2001 s. 183.

¹⁰⁹ **Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı** m. 2/1-n. Resmi Gazete, **İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun** m.2/1-k <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf> (E. T. 03.10.2021 00:35)

¹¹⁰ Özçelik, **a.g.e.** s. 63.

¹¹¹ Resmî Gazete, **6698 Sayılı Kişisel Verilerin Korunması Kanunu**, 07.04.2016 <https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf> (E.T. 15.12.2021)

¹¹² Elif Küzeci, **Kişisel Verilerin Korunması, 4. Baskı**, İstanbul: On İki Levha Yayıncılık, Mayıs 2020 s. 10. Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, Hukuk Akademisi Yayınları, 2019 s. 6-12. Zeynel T. Kangal, **Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması**, İstanbul: On İki Levha Yayınları, Eylül 2019 s. 28-31.

¹¹³ Dülger, **a.g.e.** s. 1. Kangal, **a.g.e.** s. 22. Mehmet Maden, **Ceza Hukukunda Kişisel Verilerin Korunması**, Ankara: Adalet Yayınevi, 2021 s.40-41.

¹¹⁴ Dülger, **a.g.e.** s. 5.

izi ve biyometrik verileri de kişisel veri olarak kabul edilmektedir¹¹⁵. Bilişim suçları ile bağlantılı olabilecek kişinin telefon rehberi ve mesajları, sosyal medya hesaplarından yaptığı yazılı, sesli ya da görüntülü paylaşımlar¹¹⁶ ile kişinin çevrimiçi kimliği ile internette ziyaret ettiği sitelere ait bilgiler¹¹⁷ de yine kişisel veri kapsamında değerlendirilmektedir

Bilişim sistemine girme fiilinin suç olarak düzenlenmesi ile kişisel verilerin dolaylı olarak korunduğu doktrinde ifade edilmiştir. Buna göre bilişim suçlarının ihdas edilmesi ile veri güvenliğinin sağlanmasına katkıda bulunmaktadır¹¹⁸. Bilişim sistemine girme suçunun özellikle kişisel bilgisayar ve bilişim sistemlerine karşı işlenmesi çoğunlukla şifreler ve kullanıcı adları gibi kişisel nitelikteki verilerin elde edilmesi ile mümkün olabilmektedir. Öte yandan bilişim sistemine girme suçunun işlenmesi ile de kişisel alanlar ihlal edilebilmekte; aynı zamanda kişisel verilerin elde edilmesi ya da kaydedilmesi gibi suçlar da meydana gelebilmektedir¹¹⁹. Bilişim sistemine girme suçunun işlenmesi sırasında kişisel verilere yönelik ihlallerinde gerçekleşmesi halinde ne şekilde ceza verileceğine bu çalışmanın “*Suçların Birleşmesi*” bölümünde değinilecektir.

E. İnternet

Bilişim sistemleri ve teknolojilerinin gelişmesiyle bu sistemlerdeki verilerin birbirleri arasında iletilmesi ihtiyacı ortaya çıkmış; bunun sonucu olarak da ağ(network) kavramının gelişimi kendini göstermiştir¹²⁰. Bilgisayarların birbirleriyle bağlanmaları sonucu oluşan ağların birbirleriyle tekrar bağlantı sağlamaları ile meydana gelen ve bu şekilde büyüyerek tüm dünyada yaygınlığa ulaşan iletişim sistemine ise “*internet*” denir¹²¹. Yargıtay da kararlarında¹²² benzer bir tutum

¹¹⁵ Kangal, **a.g.e.** s. 22.

¹¹⁶ YHGK, E. 2017/4-1340, K. 2018/1622, T. 06.11.2018 www.kazanci.com Erişim (E.T.15.12.2021).

¹¹⁷ Kangal, **a.g.e.** s. 22.

¹¹⁸ Küzeci, **a.g.e.** s. 492.

¹¹⁹ Maden, **a.g.e.** s. 191. İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Güncellenmiş 2. Baskı**, Ankara: Seçkin Yayınları, Nisan 2019 s. 283.

¹²⁰ Yenidünya **a.g.e.** s.1030.

¹²¹ Kayıhan İçel, **Kitle İletişim Hukuku**, 13. Baskı, İstanbul: Beta, 2018 s. 491.

¹²² YCGK, E. 2013/239, K. 2013/289, T. 11.6.2013; YCGK, E. 2014/288, K. 2016/255, T. 10.5.2016; YCGK, E. 2015/12-11, K. 2019/148 T. 05.03.2019; YCGK, E. 2016/23-1033 K. 2020/2 T. 14.01.2020 www.lexpera.com.tr (E. T. 04.10.2021)

gözetmekte ve kavramı "dünya üzerindeki milyonlarca bilgisayarın birbirlerine bağlanmaları ile oluşan global bir bilgisayar ağı sistemi" olarak tanımlamaktadır.

Soğuk savaş döneminin bir sonucu olarak 1969 yılında geliştirilen ARPANET ile askeri amaçla kullanılmaya başlanan internet¹²³; 1990'lı yılların ortalarından itibaren geniş halk kitlelerinin erişimine açılarak çok hızlı bir şekilde yayılmış¹²⁴ ve günümüze gelindiğinde ise ticaretten eğitime, sağlıktan hukuk sistemine neredeyse her alanda her türlü bilgiyi bünyesinde barındırır hale gelmiştir¹²⁵. Gerek içerdiği bilgiler ve yaygın kullanımı gerekse aklımıza gelebilecek neredeyse her türlü bilişim sistemini birbirine bağlaması nedeniyle internet, bilişim sistemleri ve bilişim hukukun vazgeçilmez ve önemli bir parçasıdır.

İnternetin gün geçtikçe hem içerik hem de kullanıcı sayısı açısından büyümesi, onu hata ve saldırılara karşı açık hedef haline getirmektedir¹²⁶. Bunun yanında internet kullanımı ve bu yolla yapılan iletişimin artması ile internet üzerinde yeterli bir denetim mekanizması kurulamaması; mücadele edilmesi zor bir suçluluk biçiminin ortaya çıkmasına neden olmuştur¹²⁷. Bu haliyle internet hem klasik suçların işlenmesi için yeni bir mecra hem de kendine özgü suçlara¹²⁸ kaynaklık edebilen bir ortam haline gelmiştir¹²⁹. Buna paralel olarak, bilişim suçlarının en kolay ve yaygın olarak işlendiği ortam olarak karşımıza çıkan internetin ¹³⁰ denetlenme ve bu alandaki suçlarla mücadele edilebilmesini amaçlayan 5651 Sayılı İnternet Ortamında Yapılan

¹²³ İnternetin tarihçesi hakkında ayrıntılı bilgi için bkz. Mehmet Bedii Kaya, **İnternet Hukuku**, İstanbul: On İki Levha Yayıncılık, Ocak 2021 s. 7-11. Sınar, **a.g.e.** s. 21-23

¹²⁴ Andrew Odlyzko, **The History of Communications and its Implications for the Internet** s. 118-119. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=235284 (E.T.: 03.10.2021)

¹²⁵ İçel, **a.g.e.** s. 492-493.

¹²⁶ Fatih Selami Mahmutoğlu, "Karşılaştırmalı Hukuk Bakımından İnternet Sijilerinin Ceza Sorumluluğu", **İÜHFİM, İnternet Özel Bölümü**, C. 59, S. 1-2, 2001, s.39.

¹²⁷ E. Eylem Aksoy Retornaz, "5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun Kapsamında İçerik Sağlayıcının Yükümlülükleri ve Ceza Sorumluluğu", **Ceza Hukuku Dergisi**, Y. 16, S. 45, Nisan 2021 s. 10.

¹²⁸ "İnternetteki bir web sitesini kırmak veya tahrif etmek(crackking), interneti kullanmak suretiyle başkalarının bilgisayar sitelerine izinsiz girmek(hacking), başkalarına ait elektronik posta kutularına sürekli elektronik posta göndermek suretiyle kişileri rahatsız etmek, posta kutularını doldurarak işlevsiz hale getirmek(spamming), elektronik posta vb yollarla sisteme bağlı başkalarına ait bilgisayarlara virüs bulaştırmak." Özbek, **İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları** s. 108-109.

¹²⁹ Selman Dursun, "İnternette Kaynaklanan Ceza Sorumluluğundaki Gelişmeler", **Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni- Prof. Dr. Gülören Tekinalp'e Armağan**, C. 23, S. 1-2, İstanbul, 2003, s.252. Hasan Sınar, "İnternet'in Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı", **Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni ılmaz Altuğ'a Armağan**, C. 17, S.1-2, İstanbul 2000 s. 356-357.

¹³⁰ Dülger, **Bilişim Suçları** s. 80.

Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun 04.05.2007 tarihinde yürürlüğe girmiştir¹³¹.

II. TARİHİ GELİŞİM

A. Uluslararası Hukukta Bilişim Suçlarının Tarihi Gelişimi

1. Bilgisayar ve Bilişim Suçlarının Tarihi Gelişimi

Bilişim suçları, 1960'lı yıllarda bilgisayarların ortaya çıkması ile kamuoyunda duyulmaya başlanmış; 1990'lı yıllarda internetin halkın kullanımına açılması ve yaygınlaşması ise işlenen bu suçların sayısının artmasına neden olarak caza kanunlarında düzenleme yapılması ihtiyacını doğurmuştur¹³². Literatürde bilinen ilk bilişim suçu Minneapolis Tribune gazetesinin 18 Ekim 1966 tarihli baskısında yer alan “*Bilgisayar Uzmanı Banka Hesabında Tahrifat Yapmakla Suçlanıyor*” başlıklı haberle Amerika’da görülmüştür¹³³. Bilgisayarın ve internetin anavatanı olan Amerika Birleşik Devletleri bilişim suçlarına ilişkin ilk düzenlemelerin de yapıldığı ülke olmuştur¹³⁴. Yetmişli yılların ikinci yarısından itibaren bilişim suçları konusunda ABD’de çalışmalar yapılmaya başlanmış ve birçok eyalette bilişim suçlarına ilişkin özel düzenlemeleri yürürlüğe girmiştir. Avrupa’da ise seksenli yılların başında İsveç, Hollanda gibi ülkelerde bilişim suçlarının incelenmesi ve araştırılması için çalışmalar yapılmaya başlanmıştır. Avrupa Topluluğu, Suç Problemleri Avrupa Komitesi bünyesinde bir komisyon kurulmuş; uzmanlardan oluşan bu komisyon bilişim suçları hakkında araştırmalar yaparak bu suçlarla mücadelede başarılı olunması için çalışmalar yapmıştır. Bu çalışmalar sırasında bilişim suçlarının ilk resmi tanımı

¹³¹ Aksoy Retornaz, **a.g.e.** s. 10. Timur Demirbaş, **Ceza Hukuku Genel Hükümler, Güncellenmiş 16. Baskı**, Ankara: Seçkin Yayıncılık, 2021 s. 437.

¹³² Dülger, **a.g.e.** s. 93-94.

¹³³ Aydın, **Bilişim Suçları ve Hukukuna Giriş**, s. 25.

¹³⁴ Mahmutoglu, **a.g.e.** s. 41.

yapılmıştır¹³⁵. 1985 yılında ise Milano’da düzenlenen Birleşmiş Milletler toplantısında ise bilişim suçları ve sonuçları tartışılmıştır¹³⁶.

Önceleri işlenen bilişim suçları ekonomik kazanç sağlamaya yönelik olsa da 1980’li yıllara gelinliğinde kişisel bilgisayarların yaygınlaşması ve bilgisayarın kullanım alanlarının artması suçların malvarlığı dışındaki değerlere yönelmeye başlamasına sebep olmuştur. Bu kapsamda hastane bilgisayarlarının manipüle edilmesi, çeşitli yöntemlerle kişilik haklarının ihlal edilmesi ya da ülkelere ait gizli bilgilerin deşifre edilmesi gibi çeşitli suçlar kamuoyunun dikkatini çekmiştir¹³⁷. 1980 yılında Fransa’da yürürlüğe giren “*Bilgisayar-Yönetmelik Fişler ve Özgürlükler Yasası*” ile bilgisayarların kişi özgürlükleri, hakları ve özel yaşamları ile kamu özgürlüklerine zarar vermemesi amaçlanmıştır¹³⁸.

Doksanlı yıllara gelindiğinde ise internetin yaygınlaşmasıyla dünyanın her yeriyle eş zamanlı olarak bağlantı kurabilme olanağının doğması bilişim suçları için oldukça elverişli bir ortam yaratmış; buna bağlı olarak da yıldan yıla bilişim suçlarının sayısında artış meydana gelmiştir¹³⁹. Bilhassa devlet kurumlarının ve şirketler gibi büyük kuruluşların veri tabanlarındaki verilerin truva atı adı verilen küçük yazılımlarla erişilebilir ya da değiştirilebilir hale gelmesi ve virüs yazılımlarıyla bu veri tabanlarının çökertilebilmesi bilişim sistemlerine duyulan güvenin azalmasına ve bu sistemlerin güvenliğinin sağlanması amacıyla çözümler aranmasına neden olmuştur. Bu arayış ise ceza kanunlarında bilişim sistemlerine yönelik fiillerin suç olarak düzenlenmesini gerekli kılmış ve birçok ülke bu minvalde düzenlemeler yaparak uygulamaya koymuştur¹⁴⁰.

İnsanlığın ikinci milenyuma erişmesiyle birlikte bilgisayar ve internet kullanımı yaygınlaşmaya ve artmaya devam etmiş; buna paralel olarak bilişim suçlarının da yeni

¹³⁵ “Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde, gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış bilişim suçudur.” İnci Biçkin, “Siber Suç Sözleşmesi ve 5237 s. Türk Ceza Kanununda Bilişim Suçları”, *Yargıtay Dergisi*, Cilt:32, Ocak-Nisan 2006, S.1-2. s. 150.

¹³⁶ Yazıcıoğlu, *Bilgisayar Suçları* s. 52-56. Olgun Değirmenci, “Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukuktaki Düzenlenişi”, *Legal Hukuk Dergisi*, C. 1, S. 11, 2003 s. 2753.

¹³⁷ Bozdoğan Akbulut, *a.g.m.* s. 546.

¹³⁸ Günay Dinç, “Bilgisayar Çağında Özel Yaşamın Korunması”, *Ankara Barosu Dergisi* S. 1987/2 s. 203-204.

¹³⁹ Akbulut, *a.g.e.* s. 53.

¹⁴⁰ Dülger, *a.g.e.* s. 97. Kurt, *a.g.e.* s. 115.

işleniş biçimleri ortaya çıkmıştır¹⁴¹. Günümüze gelindiğinde ise bilişim sistemleri aracılığıyla hukuka aykırı yarar elde etmeyi amaçlayan suçlar, kişisel verilere yönelik suçlar, siber terörizmin ve bilişim korsanlığının bilişim sistemlerinin en zorlu ve problemleri alanları olduğu görülmektedir¹⁴².

Bilişim teknolojileri doğaları gereği değiştikçe ve geliştikçe yeni suç işleme yöntemlerinin de ortaya çıkması kaçınılmaz olacaktır. Ceza kanunlarının da ortaya çıkabilecek yeni suçlara uyumlu hale getirilmesi gerekmektedir. Bu kapsamda büyük veri, blokzincir, nesnelerin interneti gibi teknolojiler ve yapay zekâ kullanan araçlar veya sistemlerin gelecekte yeni bilişim suçlarının ortaya çıkmasına yol açacağı su götürmez bir gerçektir. Bu yönüyle bilişim ceza hukuku sürekli gelişim ve değişime açık bir alan olacaktır¹⁴³.

2. Avrupa Konseyi Siber Suç Sözleşmesi

Avrupa Konseyi Bakanlar Komitesine bağlı olarak siber suçlarla mücadele konusunda bağlayıcı bir hukuki metin hazırlanması amacıyla 1997 yılında uzmanlardan oluşan bir komisyon tarafından sözleşmenin hazırlık çalışmalarına başlanmış; hazırlanan taslak Nisan 2000’de internette yayınlanarak kamuoyunun bilgisine sunulmuştur. Yapılan eleştiri ve değerlendirmeler sonucunda Haziran 2001’de nihai halini alan AKSSS 23 Kasım 2001 tarihinde Budapeşte’de imzaya açılmıştır. Alanındaki ilk uluslararası belge olan sözleşme 1 Temmuz 2004 tarihinde yürürlüğe girmiştir¹⁴⁴. 2021 yılının sonu itibariyle aralarında ABD, Kanada ve Japonya gibi Avrupa Konseyi üyesi olmayan ülkelerin de bulunduğu 66 devlet tarafından imzalanmıştır¹⁴⁵.

Sözleşme ile internet ortamındaki ve dijital ortamdaki telif hakkı ihlalleri, bilgisayarla ilişkili sahtecilik eylemleri, çocuk pornografisi, internet ortamındaki ağ ve sistem güvenliği ihlalleri ile siber suçlara karşı yürütülecek mücadelede kullanılacak yetki ve prosedürler düzenlenmiştir. Bu suçlardan toplumun korunması amacıyla ülkelerin ceza mevzuatlarının uyumlu hale getirilmesi, ortak bir ceza politikasının

¹⁴¹ Akbulut, **a.g.e.** s. 53-54.

¹⁴² Dülger, **a.g.e.** s. 99.

¹⁴³ Akbulut, **a.g.e.** s. 54. Dülger, **a.g.e.**101.

¹⁴⁴ Önok **a.g.e.** s. 1241.

¹⁴⁵ Council of Europe, **Chart of signatures and ratifications of Treaty 185**, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=185> (E.T. 15.11.2021)

oluşturulması ve uluslararası alanda iş birliğinin artırılması amaçlanmıştır¹⁴⁶. Bu amaçta da başarılı olunmuş, sözleşmenin imzalanmasının ardından birçok imzacı devletin mevzuatını AKSSS'ye uyumlu hale getirmeye yönelik çalışmalar yaptığı görülmüştür¹⁴⁷.

Türkiye ise söz konusu sözleşmeyi 10 Kasım 2010'da imzalayarak taraf devletlerden biri olmuştur. 22 Nisan 2014 tarihinde ise sözleşmenin onaylanması Türkiye Büyük Millet Meclisi tarafından görüşülerek uygun bulunmuş¹⁴⁸ 9 Ağustos 2014'te ise "*Sanal Ortamda İşlenen Suçlar Sözleşmesi*" Türkiye Cumhuriyeti'nin şerh ve beyanları ile birlikte Resmî Gazete'de yayınlanarak¹⁴⁹ ulusal hukukumuzun parçası haline gelmiştir. Türkiye, sözleşmenin 2. ve 7. maddelerine ilişkin beyanda bulunmuş 14., 22. ve 29. maddelerine ise çekince koymuştur.

Sözleşmenin "*terimler*" başlıklı ilk kısmında sözleşmede kullanılan internet ve bilişimle ilgili kavramların tanımı yapılmıştır. Sözleşmenin 2. ile 22. maddeleri arasında düzenlenen "*ulusal düzeyde alınacak önlemler*" başlıklı ikinci bölümünde ise imzacı devletlerin sorumlu oldukları maddi ceza hukuku, usul hukuku ve yetkiye ilişkin hükümlere yer verilmiştir. 23. ve 35. maddeler arasında düzenlenen "*uluslararası iş birliği*" başlıklı üçüncü bölümde ise imzacı devletler amacıyla bilişim suçlarını önlemeye yönelik uluslararası adli yardımlaşmaya ilişkin düzenlemeler yer almıştır. Sözleşmenin "*diğer hükümler*" başlıklı son kısmında ise sözleşmenin imzalanması ve uygulanmasına ilişkin usuli ve teknik hükümler düzenlenmiştir¹⁵⁰.

Sözleşmenin "*Yasadışı Erişim*" başlıklı ikinci maddesi ile bilişim sistemlerine hukuka aykırı bir şekilde erişim sağlanması düzenlenmiştir. Bu madde ile imzacı devletlere "*bir bilgisayar sisteminin tamamına veya bir kısmına haksız bir şekilde erişim fiilinin*" ceza hukuku anlamında suç olarak düzenleme yükümlülüğü getirilmiştir. Bu düzenleme ile her şeyden önce "*hacking*" olarak adlandırılan bilişim

¹⁴⁶ Kayıhan İçel, "*Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında 'Avrupa Siber Suç Politikasının Ana İlkeleri'*", **İÜHFİM, İnternet Özel Bölümü**, C. 59, S. 1-2, 2001 s. 6. Aslı Deniz Helvacıoğlu; "*Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerinin İncelenmesi*", **İnternet ve Hukuk**, Derleyen: Yeşim M. Atamer, Bilgi Üniversitesi Yayınları, 1.Baskı, İstanbul, Ocak 2004 s. 279.

¹⁴⁷ Biçkin, **a.g.e.** s. 147.

¹⁴⁸ Resmi Gazete, **6533 Sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun**, S. 28988, T. 02.05.2014 <https://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm> (E.T. 15.11.2021)

¹⁴⁹ Resmi Gazete, **Sanal Ortamda İşlenen Suçlar Sözleşmesi**, S. 29083, T. 09.08.2014 <https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5-1.pdf> (E.T. 15.11.2021)

¹⁵⁰ Önok, **a.g.e.** s. 1242-1244. Helvacıoğlu, **a.g.e.** s. 279-280.

sistemlerine rıza dışı girişlerin önüne geçilmek istenmiştir. Bu yolla sistemdeki gizli ve hassas bilgilerin ele geçirilmesi, sistemin ücretsiz kullanılması ile bilişim sistemleri aracılığıyla işlenen sahtecilik ve dolandırıcılık fiillerinin önüne geçilmek istenmiştir¹⁵¹.

Maddenin devamında ise imzacı devletlerin ulusal mevzuatlarında yetkisiz erişim suçunu belli bir amaç ya da konuyla sınırlı olacak şekilde düzenleyebilecekleri ifade edilmiştir. Bu kapsamda devletler suçun sadece “bilgisayar verilerinin elde edilmesi amacıyla veya sahtekarlığa yönelik başka bir amaçla güvenlik sisteminin ihlal edilmesi” amaçları ya da “başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini esas alarak” işlenmesini şart koşabileceklerdir. Türkiye de AKSSS’nin 40. maddesine göre beyanda bulunmuş ve suçun işlenmiş sayılması için ikinci maddede sayılan hallerin gerçekleşmesini şart koştuğunu ifade etmiştir¹⁵².

5237 sayılı TCK’nın ilk kanunlaşan halinde TCK m. 243’te “*bilişim sistemine giren ve kalmaya devam eden*” kimsenin suçu işlemiş olacağı düzenlenmekteydi. Her ne kadar kimi yazarlar kanun koyucunun AKSSS’ye koyduğu şerh kapsamında suçu düzenlerken sistemde kalınması şartını da arayabileceğini belirtse de¹⁵³ ilgili madde Sözleşmeye aykırı olduğu gerekçesiyle eleştirilmekteydi. Zira 2. madde ile bir bilişim sistemine yasadışı erişimin suç olacağı öngörülmüş olmasına rağmen TCK’ya göre sisteme girilmesinin yanında sistemde bir süre kalınması da gerekmekteydi¹⁵⁴. 24.03.2016 tarihli ve 6698 sayılı kanunun 30. maddesi yapılan değişiklik ile “ve” ibaresi “veya” ile değiştirilerek bu eksiklik giderilmiş; TCK m. 243 Sözleşme ile uyumlu bir hale gelmiştir.

Sözleşmenin hazırlandığı tarihten bugüne değin teknoloji oldukça hızlı bir şekilde gelişmiş olsa da Sözleşme içerdiği suç tipleri ve uygulama açısından

¹⁵¹ Füsün Sokullu Akıncı, “Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi”, **İÜHFM, İnternet Özel Bölümü**, C. 59, S. 1-2, 2001 s. 14-15.

¹⁵² “40. ve 2. maddeye istinaden, Türkiye cumhuriyeti Devleti, “suçun, bilgisayar verilerini elde etmek veya başka bir sahtekâr niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koştuğunu beyan eder.” **Sanal Ortamda İşlenen Suçlar Sözleşmesi**, Şerhler ve Beyanlar

¹⁵³ Aysun Dalkılıç, “Avrupa Birliği’ne Uyum Sürecinde Bilişim Suçları”, **Avrupa Birliği’ne Uyum Sürecinde Türk Ceza ve Ceza Muhakemesi Hukuku**, Proje Yöneticisi Fatih Selami Mahmutoğlu İstanbul: İstanbul Barosu Yayınları Ekim 2008 s. 207. Erdoğan, **a.g.e.** s. 119-120.

¹⁵⁴ Dülger, **a.g.e.** s. 238-239.

güncelliğini korumaktadır¹⁵⁵. Gerek sözleşmenin içeriğinin güncelliğini koruması ve kapsayıcılığı gerekse bilişim suçları ile mücadele konusunda bağlayıcı ilk uluslararası düzenleme olması bu konudaki en önemli uluslararası belge olarak nitelendirilmesine neden olmuştur¹⁵⁶..

B. Türkiye’de Bilişim Suçlarının Tarihi Gelişimi

1. 765 Sayılı Türk Ceza Kanunu Dönemindeki Durum

765 sayılı TCK döneminde bilgisayar ve bilişim sistemlerinin fiziki varlığına karşı işlenen hırsızlık veya mala zarar verme gibi fillerin TCK’nın ilgili hükümleri uyarınca cezalandırılması mümkün olsa da¹⁵⁷ bilişim sistemleri ve bunların ihtiva ettiği veri, program veya diğer unsurlara yönelik suçları düzenleyen hükümler kanunda yer almamaktaydı¹⁵⁸. Hukukumuzda bilişim suçlarına ilişkin ilk düzenlemelere “Dönmezer Tasarısı” olarak da adlandırılan¹⁵⁹ 1989 tarihli TCK Ön Tasarısı’nda rastlanmaktadır. 1988 tarihinde yasalaşan ve 1994 tarihli Fransız Ceza Kanunu’nun da temeli olan Fransız Ceza Kanunu Projesi’nden esinlenerek¹⁶⁰ hazırlanan tasarıda “bilgileri otomatik işleme tabi tutan sistem” kavramı etrafında hukukumuzda ilk defa bilişim suçları düzenlenmiştir¹⁶¹.

1989 tarihli TCK Ön Tasarısı her ne kadar tamamı itibariyle yasalaşmamış olsa da bilişim suçlarına ilişkin düzenlemeler 06.06.1991 tarihli ve 3756 sayılı Kanunla TCK’ya ilave edilmiştir. Anılan kanunun 20. maddesi ile “Bilişim Alanındaki Suçlar” başlıklı 11. bap 765 sayılı TCK’ya eklenmiş, yine aynı kanunda bu bap altında 4 madde halinde bilişim suçları düzenlenmiştir. Anılan maddelerde, mehzaz İtalyan Ceza

¹⁵⁵ Jonathan Clough, “The Council Of Europe Convention On Cybercrime: Defining ‘Crime’ In A Digital World”, **Criminal Law Forum**, Springer, (2012)-23 s. 390.

¹⁵⁶ Micheal Vatis, “The Council of Europe 's Convention on Cybercrime”, **Berkeley Technology Law Journal**, S. 18, 2014 s. 212.

¹⁵⁷ “Bilişim teknolojilerinde ortaya çıkan her gelişme ve kullanıcı sayısındaki artış, çok yönlü bir şekilde kötüye kullanım olanaklarını da birlikte getirmektedir. Bunun sonucu olarak hırsızlık, dolandırıcılık, mala zarar verme, hakaret, belgede sahtecilik gibi klasik suç tiplerinin bilişim alanında işlenen ihlallerini önlemekte yetersiz kalmaktadır. Gerçekten, ceza hukukuna egemen olan yasallık ilkesi nedeniyle klasik suç tiplerinin bilişim alanında gerçekleşen ihlalleri de kapsayacak biçimde geniş yorumlanması her zaman mümkün olamamaktadır.” Tezcan/Erdem/Önok, **a.g.e.** s. 146.

¹⁵⁸ Hakan Karakehya, “Türk Ceza Kanunu’nda Bilişim Sistemine Girme Suçu”, **TBB Dergisi** S. 81, 2009 s 4. Kurt, **a.g.e.** s. 115.

¹⁵⁹ Devrim Aydın, “Yeni Türk Ceza Kanunu’nun Hazırlanış Süreci”, **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, C. 59, S. 4, Nisan 2004 s. 249.

¹⁶⁰ Dönmezer, **a.g.e.** s.613. Yazıcıoğlu, **Bilgisayar Suçları** s. 207-208., Erem **a.g.e.** s. 441.

¹⁶¹ Tasarının gelişim süreci ve madde ayrıntıları için bkz. Kurt, **a.g.e.** s. 118-121.

Kanunu'nda olduğu gibi bilişim kavramları ve özellikleri tanımlanmamış; genel kapsamlı olarak “*bilgileri otomatik olarak işleme tabi tutmuş sistem*” deyiminin kullanılmasıyla yetinilmiştir¹⁶².

TCK'ya eklenen 525a maddesinin; ilk fıkrasında bilişim sisteminde bulunan verilerin ele geçirilmesi, ikinci fıkrasında ise bu verilerin başkalarına zarar vermek maksadıyla kullanılması, nakledilmesi ve çoğaltılması suç olarak düzenlenmiştir. Yine mezkûr kanunla TCK'ya eklenen 525b maddesinin birinci fıkrasında bilişim sistemine, içerdiği verilere yahut diğer herhangi bir unsuruna zarar verilmesi, aynı maddenin ikinci fıkrasında ise bilişim sistemlerinin kullanılması yoluyla hukuka aykırı olarak menfaat temini suçları düzenlenmiştir. 525c maddesinde bilişim sistemleri üzerinde işlenen veri sahteciliğine yönelik fiiller suç olarak düzenlenirken; 11. bap ile 765 sayılı TCK'ya eklenen son madde olan 525d maddesi ile ise 525a ve 525b'de düzenlenen suçların cezalarını ağırlaştırıcı haller düzenlenmiştir¹⁶³.

3756 sayılı kanun ile eklenen maddelerde bu çalışmanın konusu olan bilişim sistemine girme ve bu sırada sisteme ve sistemde bulunan verilere zarar verme fiili suç olarak düzenlenmemiş; bu durum doktrinde eleştirilmiştir¹⁶⁴. Bununla birlikte kimi yazarlar bilişim sistemine girme suçunun düzenlendiği 5237 sayılı TCK'nın 243. maddesinin 765 sayılı TCK'nın 525a maddesinin yeniden düzenlenmiş hali olduğunu savunmaktadır¹⁶⁵. Doktrinde çoğunluğun savunduğu görüşe göre ise anılan iki madde arasında, maddi unsurlar bakımından kısmen benzerlik olsa da¹⁶⁶, devamlılık ilişkisi bulunmamakta olup bilişim sistemine- verileri ele geçirme ya da sisteme zarar verme kastı olmaksızın- girilmesi münhasıran ilk defa 5237 sayılı TCK'da suç olarak düzenlenmiştir¹⁶⁷. Zira 765 sayılı TCK'nın 525a maddesindeki suçun işlenebilmesi

¹⁶² Yazıcıoğlu, **Bilgisayar Suçları** s. 27.

¹⁶³ Maddelerle ilgili detaylı inceleme için bkz. Hatice Akıncı/A. Emre Alıç/Cüneyd Er, “*Türk Ceza Kanunu ve Bilişim Suçları*”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ocak 2004 s. 218-263. Ö. Umut Eker, **a.g.e.** s. 111-119.

¹⁶⁴ “*Gerçekten, örneğin bir bilgisayar sistemine izinsiz girilmesi fiili Ceza Kanununda suç olarak öngörülmemiştir. Böyle bir sisteme izinsiz girip programın ‘tahribine’ yol açan kişi de, şayet ‘başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak. Maksadıyla’ hareket etmemişse yine bu maddelere göre cezalandırılmayacaktır. Fiillerin taksirli şekilde işlenmesi öngörülmediği için, özellikle fail programa girmek istemekle beraber programları istemeden zarara uğratmış ise bu mı dahi cezalandırma kapsamı dışında kalacaktır.*” Ersoy, **a.g.e.** s. 166.

¹⁶⁵ Ketizmen, **a.g.e.** s. 80. Dipnot 52. Tezcan/Erdem/Önok, **a.g.e.** s. 1147.

¹⁶⁶ Erdağ, **a.g.e.** s.282. Osman Yaşar/Hasan Tahsin Gökcan/Mustafa Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu, C. V. Madde 197-251, 2. Baskı**, Ankara: Adalet Yayınevi, 2014 s. 7286.

¹⁶⁷ Ali Kemal Yıldız, “*Bilişim Sistemine Girme*”, **Özel Ceza Hukuku C. VIII: Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ile Bilişim Alanındaki Suçlar**, İstanbul: On İki Levha Yayıncılık 2020. S. 233.

için bilişim sistemine girilmesi yahut sistemde kalınması yeterli olmayıp sistemde bulunan program, veri ya da başka herhangi bir unsurun hukuka aykırı şekilde ele geçirilmesi gerekmektedir¹⁶⁸. Yürürlükte olduğu dönemde eksikliği¹⁶⁹ vurgulanan bu düzenlemenin 5237 sayılı TCK ile yapılmış olması özellikle bilişim korsanlarının eylemlerine karşı önlem alması nedeniyle doktrinde olumlu karşılanmıştır¹⁷⁰.

5237 Sayılı TCK m. 243'ün gerekçesinde ise iki düzenleme arasında geçen süre içerisinde meydana gelen gelişmelerden dolayı eski kanundaki maddeler üzerinden düzenleme yapılmadığı; bilişim suçlarına ilişkin maddelerin bütünüyle yeniden ele alınarak kaleme alındığı ifade edilmiştir¹⁷¹. Kimi yazarlara göre ise 765 sayılı TCK'nın 525a maddesinin birinci fıkrasında tanımlanan suç 5237 sayılı TCK'nın 135. ve 136. maddelerinde düzenlenmiştir¹⁷².

2. 5237 Sayılı Türk Ceza Kanunu Hazırlık Süreci

765 sayılı TCK'nın yürürlükte olduğu süreçte yeni bir ceza kanunu hazırlamaya yönelik çalışmalar ve tasarıların hazırlanmasına devam edilmiş; bu kapsamda Adalet Bakanlığınca kurulan bir komisyon tarafından 1989 tasarısı gözden geçirilerek 1997 tarihinde yeni bir tasarı hazırlanmıştır¹⁷³. Bilişim sistemine ya da içerdiği verilere herhangi bir zarar verme ve verileri ele geçirme şartı olmaksızın yalnızca bilişim sistemine girilmesi veya orada kalınması fiili ise ilk defa 1997 Ön Tasarısı'nın 347.

Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu". **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Prof. Dr. Burhan CEYHAN'a Armağan**, C. 12, Özel S. 2010, s. 1366, Eker, **a.g.e.** s.120-122, Kurt, **a.g.e.** s. 136. Ali Parlar, **Türk Ceza Hukukunda Bilişim Suçları**, 3. Basım, Ankara: Bilge Yayınevi 2015 Cengiz Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, İstanbul: Acar Matbaacılık, 2017 s. 4

¹⁶⁸ Akbulut, **a.g.e.** s.112. Olgun Değirmenci, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", **TBB Dergisi**, S. 58., 2005 s. 203-204.

¹⁶⁹ Ünver, **a.g.e.** s.118-119. Yazıcıoğlu, **Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi** s. 403. Dilek Güler, "Bilişim Sistemine Girme Suçu", **KTO Karatay Üniversitesi Hukuk Fakültesi Dergisi**, C. 3, S. 2, Temmuz 2018 s. 15.

¹⁷⁰ Apaydın, **Bilişim Sistemine Girme Suçu** s. 252. Murat Volkan Dülger, "Türk Ceza Kanunu'nda Yer Alan Bilişim Suçları ve Eleştirisi", **Bilişim Hukuku**, Der. Mete Tevetoğlu, İstanbul: Kadir Has Üniversitesi, 2006 s. 416. Ali Parlar/Muzaffer Hatipoğlu, **Açıklamalı-Yeni İçtihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu**, 4. Cilt (230-245. Maddeler), Ankara: Seçkin Yayıncılık, 2011 s. 3741.

¹⁷¹ "1/3/1926 tarihli ve 765 sayılı Kanunun 525 a ilâ 525 d maddelerinde yer alan bilişim suçları, 1989 Tasarısından çok küçük değişikliklerle alınıp 6/6/1991 tarihli ve 3756 sayılı Kanunla kanunlaştırılmış ve 765 sayılı Kanuna sokulmuştu. Aradan geçen süre içinde bu suçlar konusunda Batı hukukunda değişiklikler olduğu gibi bizde de metinler ve suçların oluşması yönünden bazı duraksamalar meydana geldi. Bu nedenle Tasarıdaki maddelerin bütünüyle yeniden ele alınması uygun sayılmıştır" **Türk Ceza Kanunu Madde Gerekçeleri** www.lexpera.com.tr (E. T. 19.10.2021)

¹⁷² Dülger, **a.g.m.** s. 400. Esra Yayıcı, **Bilişim Suçları**, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Ankara 2007 s. 66.

¹⁷³ M. Emin Artuk / Ahmet Gökçen / M. Emin Alşahin/ Kerim Çakır, **Ceza Hukuku Genel Hükümler**, 14. Baskı, Ankara: Adalet Yayınevi, 2020 s. 138-139.

maddesinin birinci fıkrasında düzenlenmiştir. Bu düzenleme ile bilişim sistemlerindeki kişisel alanların ihlali ilk defa yaptırım altına alınmak istenmiştir¹⁷⁴. Ayrıca yine bu tasarıda “*bilgileri otomatik olarak işleme tabi tutmuş sistem*” teriminin kullanımı terk edilerek “*bilişim sistemi*” terimi kullanılmıştır. Tasarının madde gerekçesinde iki kavramın aynı anlama geldiği ifade edilmiş¹⁷⁵; bu değişiklik gerek kanunun bilişim diline uygun hale gelmesi¹⁷⁶ gerekse daha basit ve anlaşılır bir ifade olması nedeniyle doktrinde olumlu karşılanmıştır¹⁷⁷. Kimi yazarlar ise anlamda farklılığa sebebiyet vermeyen bu terim değişikliğinin kanuna bir katkısı olmadığını savunmuş ve bu değişimi eleştirmiştir¹⁷⁸.

1997 tarihli tasarı kanunlaşmamış ve bu tasarının yeniden ele alınmasıyla 2000 yılında yeni bir TCK ön tasarısı¹⁷⁹ oluşturulmuştur. 1997 tasarısındaki bilişim suçlarına ilişkin hükümler, gerekçeleriyle birlikte, ufak kelime farklılıkları haricinde 2000 TCK Ön Tasarısı’nda da yer almıştır. Yenilik olarak ise yalnızca tasarının 350. maddesi ile “*Banka ve Kredi Kartlarının Kötüye Kullanımı*” suçu düzenlenmiştir.

2000 yılında hazırlanan tasarı da aradan geçen sürede yasalaşmamış; 2003 yılında ise son bir tasarı¹⁸⁰ hazırlanarak Bakanlar Kurulu tarafından TBMM’ye 14.04.2003 tarihinde sunulmuştur¹⁸¹. Sunulan bu tasarının bilişim suçları ile ilgili maddeleri para cezalarının güncel rakamlara göre tekrar belirlenmiş olması dışında gerek madde metinleri gerekse gerekçeleri olarak 2000 yılında hazırlanan tasarının tamamen aynısıdır. 2003 yılında hazırlanan tasarı yeni bir ceza kamu yapılması amacıyla hazırlanan tasarıların sonuncusu olmuştur.

2003 TCK tasarısı ilk olarak adalet alt komisyonu ardından ise meclis genel kurulunda görüşülmüş; bilişim sistemine girme suçunu düzenleyen 346. madde çeşitli değişikliklere uğramıştır. Öncelikle madde numarası ve başlığı değişmiş; 346 olan madde numarası 243; “*bilişim sistemine girme, verileri tahrip ve bozma*” olan madde

¹⁷⁴ Değirmenci, **a.g.m.** s. 197-198.

¹⁷⁵ Kurt, **a.g.e.** s. 124-125.

¹⁷⁶ Doktrinde “Bilgileri otomatik işleme tabi tutmuş sistem” kavramı ile sadece bilgisayarların kastedildiği öne sürülmekteydi. Değirmenci, **a.g.m.** s. 199.

¹⁷⁷ Eker, **a.g.e.** s. 120. Akıncı/Alıç/Er, **a.g.e.** s. 266-267. Dönmezer, **a.g.e.s.** 529-532.

¹⁷⁸ Ünver, **a.g.e.** s.119-120.

¹⁷⁹ 2000 Tarihli TCK Tasarısı’ndaki bilişim suçları hakkında ayrıntılı bir değerlendirme için bkz. Ünver, **a.g.e.** s. 114 vd.

¹⁸⁰ Tasarı hakkında detaylı bir inceleme için bkz. Cevat Özel, “*Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı*”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ocak 2004 s. 341-361.

¹⁸¹ **2003 TCK Tasarısı** <https://www2.tbmm.gov.tr/d22/1/1-0593.pdf> (E.T. 25.10.2021)

başlığı “*bilişim sistemine girme*” olarak değişmiştir. Bunun yanında da bilişim sistemine girme suçunun cezadan indirim sebebi olan suçun “*bedeli karşılığında yararlanılabilen sistemler hakkında işlenmesini*” düzenleyen ikinci fıkra kanuna eklenmiştir. Son olarak ise teşebbüs halindeki suçun da işlenmiş gibi cezalandırılacağına ilişkin fıkra madde metninden çıkarılmıştır. Yapılan bu iki değişiklik de olası, telafisi güç zarar ve mağduriyetleri önlemiş olması sebebiyle yerinde bulunmuştur¹⁸².

Kuşkusuz ki görüşmeler sırasında yapılmış olan en önemli değişiklik ise birinci fıkradaki “*bilişim sistemine giren veya orada kalmaya devam eden*” ifadesinin “*bilişim sistemine giren ve orada kalmaya devam eden*” olarak değiştirilmesidir. Bu değişikliğin bir sonucu olarak yalnızca bilişim sistemine girme eylemi suçun işlenmesi için yeterli olmayacak; failin cezalandırılabilmesi için sisteme girildikten sonra bir süre sistemde kalınması gerekecektir. TBMM genel kurul tutanaklarına¹⁸³ göre bu değişiklik, yanlışlıkla bilişim sistemine giren kişilerin cezalandırılmasının önüne geçilmek amaçlanmıştır¹⁸⁴.

Tüm bu değişikliklerin yanında 243. maddenin gerekçesinde bilişim sistemlerini tanımına yer verilmiş; bu durum ise doktrinde şiddetle eleştirilmiştir. Bu görüşe göre; en doğru olan tutum tanım verilmeyerek boşluğun doldurulmasının doktrin ve mahkemelere bırakılmasıdır. Fakat kanun koyucu bunu tercih etmemiş; bunun yanında doktrinde yapılan daha kapsamlı ve daha doğru tanımlar yerine yetersiz bir tanım tercih etmiştir¹⁸⁵.

5237 sayılı TCK ile yapılan ve değinilmesi gereken bir diğer değişiklik ise 765 sayılı TCK’nın aksine bilişim suçlarına ayrı bir bölüm ayrılmayarak “*Topluma Karşı Suçlar*” başlıklı üçüncü kısmında düzenlenmiş olmasıdır¹⁸⁶. Bu değişikliklerle birlikte tasarı 26.09.2004 tarihinde TBMM Genel Kurulunda kabul edilmiş, 1 Haziran 2005 tarihi itibarıyla ise yürürlüğe girmiştir.

¹⁸² Yazıcıoğlu, *Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi* s. 406-407.

¹⁸³ İlgili Genel Kurul tutanakları için bkz. <https://mevzuat.tbmm.gov.tr/mevzuat/faces/maddedetaylari?psira=18779&psorgukriteri=> (E.T. 25.10.2021).

¹⁸⁴ Özçelik, *a.g.e.* s. 24-26.

¹⁸⁵ Dülger, *a.g.m.* s. 401.

¹⁸⁶ Yazıcıoğlu, *Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi* s. 403.

3. 5237 Sayılı TCK'da Bilişim Sistemine Girme Suçu

Bilişim sistemine girme suçu 5237 sayılı TCK'nın “Özel Hükümler” başlıklı ikinci kitabının “Topluma Karşı Suçlar” başlıklı üçüncü kısmının “Bilişim alanındaki Suçlar” başlıklı onuncu ve son bölümünde, 243. maddede düzenlenmiştir. “Bilişim Sistemine Girme Suçu” başlıklı maddenin; ilk fıkrasında bilişim sistemine hukuka aykırı olarak girme veya sistemde kalmaya devam etme fiillerinin cezalandırılacağı, ikinci fıkrasında fiilin bedeli karşılığı yararlanılabilen sistemlere yönelik olarak icra edilmesi durumunda verilecek cezada indirimle gidileceği, üçüncü fıkrasında ise suçun netice sebebiyle ağırlaştırılmış hali düzenlenmiştir. Maddeye 2016 yılında 6698 sayılı kanun ile eklenen dördüncü fıkra ise bilişim sistemine girmeksizin veri nakillerinin izlenmesi fiili suç olarak düzenlenmiştir.

Ülkemizin tarafı olması nedeniyle iç hukukumuzun bir parçası olan AKSSS'nin 2. maddesi imzacı devletlere bilişim sistemine yasa dışı erişim fiilini suç olarak düzenleme yükümlülüğü getirmektedir. Bu nedenle; bilişim sistemine girme suçunu düzenleyen 243. maddenin genel kurulda yapılan görüşmeler sonucunda değiştirilerek “bilişim sistemine girme ve orada kalmaya devam etmeyi” suç olarak düzenlemesi anılan sözleşmeye aykırı olduğu gerekçesiyle doktrinde eleştirilmiştir. Zira suçun unsurlarının ve niteliğinin değişmesine yol açan¹⁸⁷ bu değişiklik son halini alan 243. madde sözleşmenin öngördüğü şekilde bilişim sistemine yetkisiz erişim fiilini cezalandırmamakta, bu yönüyle hem sözleşmeye hem de bilişim sisteminin bütünlüğünün korunması ilkesine ters düşmekteydi¹⁸⁸. Rızaen bilişim sisteminde girildiği durumlarda rızanın ortadan kalkmasına rağmen sistemde kalmaya devam edilmesi fiilinin kanunun bu halinde suç olmaktan çıkması da ayrıca eleştirilmiştir¹⁸⁹. Bazı yazarlar ise sözleşmenin hukuka aykırı erişim fiilini suç olarak düzenleme yükümlülüğü getirdiğini fakat ulusal mevzuatlarda yapılan düzenlemelerde ek unsur ve koşulların getirilebileceğini savunmuştur. Bu yazarlara göre sisteme girdikten sonra

¹⁸⁷ Ketizmen, **a.g.e.** s. 81-82.

¹⁸⁸ Yılmaz Yazıcıoğlu, “Hackerler Ve Bilişim Sistemine Girme Suçu (TCK. Md. 243)” **Ord. Prof. Dr. Sulhi Dönmezer Armağanı**, C. II., Ankara: Türk Ceza Hukuku Derneği Atatürk Araştırma Merkezi Başkanlığı Yayını, 2008 1255-1256. Apaydın, **a.g.m.** s. 266-267. Karagülmez **a.g.e.** s. 169. Akbulut, **a.g.e.** s. 115. Özge Apiş, “Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama El koyma Koruma Tedbiri” **Yasama Dergisi Kamu Yönetiminde Teknoloji Özel Sayısı II**, C.12, S.37, Haziran 2018, s. s. 52.

¹⁸⁹ Dülger, **Bilişim Suçları** s. 238-239.

bir süre kalma fiili de bu unsurlar kapsamındaydı. Bu yazarlara göre söz konusu düzenleme AKSSS'nin 2. maddesine aykırılık oluşturmamaktaydı¹⁹⁰.

Yine yukarıdaki paragrafta değinilen konuyla bağlantılı olarak 243. maddenin başlığının “*bilişim sistemine girme*” olmasının da kimi yazarlarca eleştirildiği görülmektedir. Bu yazarlara göre; madde metnine göre suçun işlenebilmesi için bilişim sistemine girilmiş olması yetmemekte, ayrıca sistemde bir süre kalınması gerekmektedir. Bu haliyle incelemekte olduğumuz maddede başlıkta belirtilen bilişim sistemine girme fiili tek başına suç olarak düzenlenmemiştir. Suç olarak düzenlenen fiil “*bilişim sistemine girme ve kalma*” fiilidir. Bu haliyle yanıltıcı olan madde başlığının da buna göre belirlenmesinin daha uygun olacağı ifade edilmiştir¹⁹¹.

5237 sayılı TCK'nın yürürlüğe girmesinin ardından çeşitli maddelerinde değişiklikler yapılmış olsa da incelemekte olduğumuz 243. maddede yapılan tek değişiklik 24.03.2016 tarihli ve 6698 sayılı kanunla yapılmıştır. Anılan kanunun 30. maddesi ile m. 243/1'deki “ve” bağlacı “veya” bağlacı ile değiştirilerek madde metni “*bilişim sisteminin bütününe... giren veya orada kalmaya devam eden...*” şeklindeki güncel halini almıştır. Bu haliyle bilişim sistemine girme suçu “*bağlı hareketli suç*” olmaktan çıkıp “*seçimlik hareketli suç*” halini almış¹⁹² ve doktrinde eleştirilen AKSSS m. 2'ye olan aykırılık hali de ortadan kalkmıştır¹⁹³ Bu değişiklikte birlikte tek başına bilişim sisteminde kalma fiili de suç olarak düzenlenmiştir. AKSSS' deki düzenlemeye ek olarak rızaen bilişim sistemine girilmesi halinde rızanın ortadan kalmasına rağmen sistemde kalmaya devam edilmesi hali de suç olarak düzenlenmiştir¹⁹⁴.

Birinci fıkrada yapılan ve yukarıda değindiğimiz değişikliklerin yanı sıra; 6698 sayılı kanunun 30. maddesi ile 243. maddeye 4. fıkra eklenerek “*bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleme*” fiili de suç olarak düzenlenmiştir. TCK'ya eklenen bu suçun kanuna yeni bir madde eklenerek¹⁹⁵ düzenlenmesinin daha doğru olacağı ifade edilmiştir¹⁹⁶. Her ne kadar 243. madde

¹⁹⁰ Dalkılıç, **a.g.e.** s. 207. Erdoğan, **a.g.m.** s. 1368-1369. Taşdemir, **a.g.e.** s. 332 vd.

¹⁹¹ Erdoğan, **a.g.m.** s. 1368. Akbulut, **a.g.e.** s. 127-128. Karagülmez, **a.g.e.** s. 169.

¹⁹² Dülger, **a.g.e.** s. 238.

¹⁹³ Akbulut, **a.g.e.** s. 114-115. Koca, Üzülmüş, **a.g.e.** s. 892. Karagülmez **a.g.e.** s. 203.

¹⁹⁴ Dülger, **a.g.e.** s. 238. Akbulut, **a.g.e.** s. 115.

¹⁹⁵ Yine 6698 Sayılı Kanun'un 30. maddesi ile “*Yasak Cihaz ve Programların Üretilmesi ve Ticareti Suçu*” TCK'ya eklenmiş; bu sırada var olan bir maddeye fıkra eklenmesi tercih edilmeyerek kanuna eklenen 245A maddesinde bu yeni suç düzenlenmiştir.

¹⁹⁶ Akbulut, **a.g.e.** s. 158-159. Dülger, **a.g.e.** 237,310. Gül, **a.g.e.** s. 91.

içerisinde düzenlenmiş olsa da doktrindeki çoğu yazara göre dördüncü fıkra düzenlenen suç bilişim sistemine girme suçundan farklı bir suçtur¹⁹⁷. Kimi yazarlar¹⁹⁸ iki ayrı suçun varlığını kabul etmekle birlikte dördüncü fıkrayı da “*Bilişim Sistemine Girme Suçu*” başlığı altında incelenmiş olsa da çalışmamızda çoğunluk görüşü benimsenmiş ve “*Veri Nakillerinin Teknik araçlarla İzleme Suçu*” çalışmanın kapsamı dışında bırakılmıştır.

Türk Ceza Kanunu’nun yanında bilişim suçlarını düzenlemek için 2006 yılında Adalet Bakanlığınca Bilişim Ağı Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun Tasarısı hazırlanmış fakat aradan geçen 15 yılı aşkın sürede yayımlanmamıştır. İncelemekte olduğumuz suç bu tasarının 15. Maddesinde “*Bilişim Sistemine Girme ve Veri Elde Etme*” başlığıyla düzenlenmiştir. Bu maddede sisteme girilmeksizin verilerin izlenmesi fiili ile bilişim sistemine girme fiili hem aynı fıkra düzenlenmiş hem de aynı şekilde cezalandırılacakları hükme bağlanmıştır.

¹⁹⁷ Akbulut, **a.g.e.** 158-159. Koca/Üzülmez, **a.g.e.** s. 907-908. Dülger, **a.g.e.** s. 310.

¹⁹⁸ “243. maddede iki ayrı suç tipine yer verilmiş olmakla birlikte aşağıda yapılacak incelemede bu suç tipleri ayrı başlıklar halinde değil, aynı başlık altında ele alınacak ancak farklı özellikler gösterdikleri durumlarda bunlara ilişkin açıklamalar yapılacaktır.” Yıldız, **Bilişim Sistemine Girme** s. 232. Özbek/Doğan/Bacaksız, **a.g.e.** s. 962.

III. KORUNAN HUKUKİ DEĞER

Ceza hukukunda bir eylemin hukuka aykırı olup olmadığını saptamak için ölçüt olarak suçla korunun hukuki değer kavramı kullanılmaktadır¹⁹⁹. Suç teşkil eden her fiil aynı zamanda bir hukuki değeri de ihlal etmektedir²⁰⁰. Suçun hukuki konusu olarak da isimlendirilen²⁰¹ korunması amaçlanan hukuki değer, belirli bir fiilin kanunda suç olarak düzenlenmesindeki amaç olarak ifade edilmektedir. Bu amaç toplumsal düzenin korunması gibi toplumsal bir nitelik göstermekle beraber kişilerin menfaatlerinin korunmasını da içermektedir²⁰².

İncelemekte olduğumuz bilişim sistemine girme suçunun koruduğu hukuki menfaatin ne olduğuna ilişkin doktrinde çeşitli görüşler mevcuttur. Kimi yazarlar suçla korunan birden fazla hukuki değer olduğunu ve suçla korunan hukuki değer karma nitelikte olduğunu savunurken²⁰³; kimi yazarlar ise suçla tek bir hukuki değer korunmaya çalışıldığını savunmuştur²⁰⁴.

TCK m. 243 ile korunması amaçlanan hukuki değer karma nitelikte olduğunu savunan yazarlar arasında da fikir birliğine varılamadığı görülmektedir. Kimi yazarlara göre: öncelikle korunmak istenen değer bilişim sisteminin güvenliği, ikincil olarak sisteme girme ve kalma fillerinin engellenmesi sebebiyle özel yaşamın gizliliği, özel olarak ise haberleşme özgürlüğüdür²⁰⁵. Bazı yazarlar ise bilişim sistemine duyulan güvenin korunmasının tali olarak amaçlandığını öne sürmüş; asıl korunmak istenenin özel hayatın gizliliği, sırların mahremiyeti ve haberleşme özgürlüğü olduğunu

¹⁹⁹ Murat Volkan Dülger, **Türk Ceza Hukuku Genel Hükümler**, İstanbul: Hukuk Akademisi, 2021 s. 123.

²⁰⁰ Yener Ünver, **Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer**, Ankara: Seçkin Yayıncılık, 2003. s. 147. İzzet Özgenç, **Türk Ceza Hukuku Genel Hükümler, Gözden Geçirilmiş ve Güncellenmiş 17. Baskı**, Ankara: Seçkin Yayıncılık, 2021 s. 176.

²⁰¹ Zeki Hafızoğulları/Muharrem Özen, **Türk Ceza Hukuku Genel Hükümler, 12. Baskı**, Ankara: U-SA Yayıncılık, Eylül 2019 s. 199. Demirbaş, **a.g.e.** s. 589. Doğan Soyaslan, **Ceza Hukuku Genel Hükümler, Güncellenmiş 9. Baskı**, Ankara: Yetkin Yayınları, 2020 s. 250.

²⁰² Sulhi Dönmezer/Sahir Erman, **Nazari ve Tatbiki Ceza Hukuku, C. II, 15. Tıpkı Basım**, İstanbul: Der Yayınları, 2021 s. 35.

²⁰³ Tezcan/Erdem/Önok, **a.g.e.** s. 1149. Özbek/Doğan/Bacaksız, **a.g.e.** s. 957.

²⁰⁴ Akbulut, **a.g.e.** s. 118. Koca/Üzülmez, **a.g.e.** s. 895. Özçelik, **a.g.e.** s. 45. Zeki Hafızoğulları/Muharrem Özen, **Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, 3. Baskı**, Ankara: U-SA Yayıncılık, Eylül 2017 s. 445.

²⁰⁵ Tezcan/Erdem/Önok, **a.g.e.** s. 1149. Gül, **a.g.e.** s. 92. Meral Ekici Şahin/Irmak Koruculu, “*Bilişim Sistemine Girme Suçu - Suçun Kamu Personeline ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarla İşlenmesine İlişkin Bir Değerlendirme*”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Prof. Dr. Durmuş TEZCAN’a Armağan**, C. 21, Özel S. 2019, s. 590-592. Parlar, **a.g.e.** s. 15.

savunmuştur²⁰⁶. Kimi yazarlar ise hem özel hayatın gizliliği, kişisel verilerin korunması gibi bireysel hak ve özgürlüklerin hem de bilişim sistemlerinin güvenliğinin ve kamu düzeninin korunmak istendiğini savunmuş; bunlar arasında herhangi bir öncelik sıralaması yapmamıştır²⁰⁷. Bu görüşü savunan yazarlara göre TCK m. 243'te düzenlenen bilişim sistemine girme suçunun diğer bilişim suçlarının işlenebilmesi için araç (geçit) suç olduğu göz önüne alındığında farklı türden birçok hukuki değer bu suçla korunmaktadır²⁰⁸. Bir görüş ise korunmak istenen asıl menfaatin bilişim sistemlerinin güvenliği olduğunu; sistemin güvenliğinin sağlanması ve sisteme yasa dışı erişimin engellenmesiyle kullanıcıların kişisel verileri ve özel hayatlarının gizliliği gibi çeşitli menfaatlerinin de güvence altına alındığını öne sürmüştür²⁰⁹.

Suçla korunmak istenen hukuki değerın karma nitelikte olduğunu savunan bir diğer görüş ise bilişim sisteminin güvenliği ve toplumda bu sistemlere karşı duyulan güvenin, bir başka ifadeyle bilişim sisteminin güvenilirliğinin korunmasının amaçlandığını ifade etmiştir²¹⁰. Farklı bir görüş ise incelemekte olduğumuz suçla toplumsal düzen, özel hayat ve haberleşmenin gizliliği, kullanıcı ve sistem sahiplerinin hakları ile sistemin güvenliğinin korunması ve olası başka suçların işlenmesinin engellenmesinin hedeflendiğini belirterek tüm bu değerlerin sistemin güvenilirliğini oluşturduğunu ifade etmektedir²¹¹.

Bilişim sistemine girme suçunun “*Topluma Karşı Suçlar*” başlığı altında düzenlenmesinden yola çıkan bir görüşe göre ise korunmak istenen hukuki menfaat: - her ne kadar bireylerin menfaatleri zarara uğrasa da- sağlıklı bir bilişim ortamının oluşturulmasına, geliştirilmesine ve sağlıklı, güvenli ve güvenilir bir şekilde işlenmesinin sağlanmasına ilişkin ferdi-kamusal yarardır²¹². Buna rağmen TCK'nın

²⁰⁶ M. Emin Artuk/Ahmet Gökçen/Caner Yenidünya, **Ceza Hukuku Özel Hükümler**, 15. Baskı, Ankara: Adalet Yayınevi, 2015 s. 860. Yenidünya/Değirmenci, **a.g.e.** s. Yenidünya, **a.g.e.** s. 1014-1025. Erdağ **a.g.e.** s. 279-280. Taşdemir **a.g.e.** s. 255-256. Akarslan, **a.g.e.** s. 44.

²⁰⁷ Apaydın, **a.g.m.** s. 258. Taşkın, **a.g.e.** s. 23. Doğan Soyaslan, **Ceza Hukuku Özel Hükümler**, 13. Baskı, Ankara: Yetkin Yayınları, 2020., s. 661. Mahmutoglu, **Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar** s. 859-860. Yazıcıoğlu, **Hackerler Ve Bilişim Sistemine Girme Suçu(TCK Md. 243)** s.1254. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7286-7287. İbrahim Şahbaz, **Açıklamalı ve İctihath Türk Ceza Kanunu**, 3. Cilt (Madde 197-345), 5. Baskı, Ankara: Yetkin Yayınları, 2020 s. 3127.

²⁰⁸ Kayaer, **a.g.e.** s.88. Koca/Üzülmez, **a.g.e.** s. 896.

²⁰⁹ Dülger, **Bilişim Suçları** s. 246 Ali. Parlar/Mustafa Öztürk, **Doğrudan ve Dolaylı Bilişim Suçları ve Bilişim Sistemleri Aracılığıyla İşlenen Suçlar**, İstanbul: Aristo Yayınları, Mart 2020 s. 25. Sami Kabadayı, **Bilişim Sistemine Girme Suçu(TCK m. 243)**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Ankara, 2021 s. 68-69.

²¹⁰ Özbek/Doğan/Bacaksız, **a.g.e.** s. 957.

²¹¹ Erdoğan, **Türk Ceza Kanunu'nda Bilişim** s. 120-123.

²¹² Hafızogulları/Özen, **Topluma Karşı Suçlar** s. 445.

genel gerekçe ve madde gerekçeleri incelendiğinde “*Bilişim Alanındaki Suçlar*” bölümünde düzenlenen suçların topluma karşı zarar verecek nitelikte olup olmadığına dair herhangi bir açıklama yapılmadığı; kanun koyucunun hukuki bir değerlendirme yapmaksızın uygulamada kolaylık sağlamak amacıyla bu suçları ayrı bir başlık altında topladığı görülmektedir²¹³.

Doktrindeki diğer görüşlere bakıldığında ise TCK m. 243'teki düzenleme ile; kişilerin sanal ortamdaki özel alanının²¹⁴, özel hayatın gizliliğinin²¹⁵, sistemin muhteviyatının²¹⁶, malvarlığının²¹⁷, kişilerin ya da kurumların güvenlik duygusunun korunmak istendiğinin ifade edildiği görülmektedir²¹⁸. Bir görüş ise bu suçun düzenlenmesi ile bilişim sistemleri aracılığıyla işlenebilecek diğer suçların engellenmek istediğini savunmuştur²¹⁹. Maddenin 2016 yılında yapılan değişiklik öncesindeki halini temel alan bir görüş ise maddeye göre bilişim sistemine girilmesinin tek başına suçun oluşumu için yeterli olmaması ve sistemde kalınmaya devam edilmesi gerektiğini ifade ederek; kanun koyucunun anlık yetkisiz erişimleri suç olarak düzenlemediğini ve suçla korunmak istenen hukuki değer sistemin güvenliği olmasının mümkün olmadığını savunmuştur. Buna göre suçla bilişim sistemi kullanıcılarının rahatsız edilmemesi amaçlanmış, sistem kullanıcılarının menfaatleri korunmak istenilmiştir²²⁰. 2016 yılında yapılan değişiklikle birlikte sistemde bir süre kalmaksızın icra edilen anlık yetkisiz erişimler de suç olarak tanımlanmış ve bu görüşün geçerliliği kalmamıştır²²¹.

Bizim de katılmakta olduğumuz görüşe göre ise incelemekte olduğumuz suçla korunmak istenen hukuki değer bilişim sistemlerinin güvenliğidir. Zira, kanun koyucu sadece bilişim sistemlerine girilmesini suçun oluşması için yeterli kabul etmiş; ayrıca verilerin ele geçirilmesi, sisteme zarar verilmesi gibi bir gereklilik öngörmemiştir. Bu durumda halihazırda TCK'nın farklı maddelerinde düzenlenmiş olan suçların konusu

²¹³ Dalkılıç, **a.g.e.** s. 216-217.

²¹⁴ Karakehya, **a.g.e.** s. 12. Uğur İhtiyaroğlu, “*Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi*”, **Hacettepe Üniversitesi Hukuk Fakültesi Dergisi**, C. 10, S. 2, 2020 s.411-412.

²¹⁵ Kurt, **a.g.e.** s. 148.

²¹⁶ Muhammed Sefa Çetin, “*Yargıtay Kararları Işığında Bilişim Sistemine Girme ve Kalma Suçu (TCK m. 243.)*” **Türkiye Adalet Akademisi Dergisi**, Y. 12, S. 45, Ocak, 2021, s. 5.

²¹⁷ Ketizmen, **a.g.e.** s. 92.

²¹⁸ Tepe, **a.g.e.** s. 278.

²¹⁹ BAYINDIR Aslı, “*Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları*”, **Suç ve Ceza Dergisi**, Y. 2010, S. 2 s. 61.

²²⁰ Karagülmez, **a.g.e.** s. 201-202.

²²¹ Dülger, **Bilişim Suçları** s. 247.

olan özel hayatın gizliliği, kişisel veriler ya da malvarlığının korunmak istendiğini söylemek mümkün değildir²²².

Son olarak belirtmekte fayda görüyoruz ki yukarıda yapılan açıklamalar 243. maddenin üçüncü fıkrasında düzenlenen suçun neticesi sebebiyle ağırlaştırılmış hali olan “*sistemin içerdiği verilerin yok olması veya değişmesi*” fiili için geçerli değildir. Kanun koyucu bu fıkrayı düzenlemekle sistemdeki verilerin dışarıdan gelen saldırılara karşı korunmasını amaçlamıştır²²³.

IV. SUÇUN UNSURLARI

A. Maddi Unsur

1. Fail

Fail, suçun kanunu tanımındaki eylemi ve haksızlığı gerçekleştiren kişi olarak tanımlanmaktadır²²⁴. Her suçta mutlaka suçu oluşturan fiili işleyen bir kişi bulunmakta; bu kişi fail olarak adlandırılmaktadır²²⁵. Bir suçun kanunu tanımında sadece belli bir nitelik taşıyan yahut yükümlülük altında bulunan kişilerce işlenebileceği düzenlenmiş ise bu suçlara “*özgü suç*” denilmektedir²²⁶.

Bilişim sistemlerinin kullanımının yaygın olmadığı dönemlerde; bu suçları işleyen kişilerin bilgisayarla ilgili işlerde çalışmaları ve bilişim konusunda teknik ve özel bir bilgi seviyesine sahip olmaları nedeniyle bu suçlar doktrinde “*beyaz yaka suçları*” olarak adlandırılmaktaydı²²⁷. Günümüze gelindiğinde ise bilişim sistemleri ve internetin kullanımının giderek artması bu suçun işlenmesinin basitleşmesini de beraberinde getirmiş; eskiden bilişim korsanlarının yaptığı karmaşık işlemlerin basitçe

²²² Akbulut, **a.g.e.** s. 118. Özçelik, **a.g.e.** s. 45. Necati Meran, **Sahtecilik, Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar**, 2. Baskı, Ankara: Seçkin Yayınları, 2008 s. 563. Ergün, **a.g.e.** s. 87-88.

²²³ Koca/Üzülmez, **a.g.e.** s. 896.

²²⁴ Dönmezer/Erman, **a.g.e.**, s. 724. Berrin Akbulut, **Ceza Hukuku, Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 7. Baskı**, Ankara: Adalet Yayınevi, 2020 s.411. Eylem Baş Bayraktaroğlu, **Ceza Hukukunda Fail ve Mağdur**, Ankara: Seçkin Yayıncılık, 2021 s. 114.

²²⁵ Mahmut Koca/İlhan Üzülmez, **Türk Ceza Hukuku Genel Hükümler, Gözden Geçirilmiş ve Güncellenmiş 14. Baskı**, Ankara: Seçkin Yayınevi, 2021 s. 114.

²²⁶ Dönmezer/Erman, **a.g.e.**, s. 725. Baş Bayraktaroğlu, **a.g.e.** s. 119-120. Veli Özer Özbek/Koray Doğan/Pınar Bacaksız, **Türk Ceza Hukuku Genel Hükümler, Genişletilmiş ve Güncellenmiş 12. Baskı**, Ankara: Seçkin, 2021 s. 213. Kayıhan İçel, **Ceza Hukuku Genel Hükümler, 18. Baskı**, İstanbul: Beta, 2018 s. 305.

²²⁷ Ersoy, **a.g.e.** s. 167. Aydın, **Bilişim Suçları ve Hukukuna Giriş**, s. 30.

yapılabildiği programlar²²⁸ kullanılarak sistemlere hukuksuz olarak erişim sağlanması mümkün hale gelmiştir. Gerek bu programlara gerekse bunlarla ilgili açıklayıcı rehber ve dokümanlara internet ortamında kolayca ulaşılabilmektedir²²⁹. Sonuç olarak bilişim suçlarının işlenebilmesi için bir meslek mensubu ya da uzman olunmasına gerek olmadığı, bu suçların basit düzeyde bilgisayar kullanabilen kişilerce de işlenebildiği görülmektedir²³⁰. Öyle ki yapılan çalışmalar ilköğretim öğrencilerinin dahi bilişim suçlarının faili olabildiklerini göstermiştir²³¹.

Kanuni düzenlemeye bakıldığında TCK m. 243'te "*bilişim sistemine giren ve orada kalmaya devam eden kimsenin*" suç işlemiş olacağı düzenlenmiş; bunun dışında failin sahip olması gereken özel bir nitelikten bahsedilmemiştir. Günümüzde üzerinde fikir birliğine varılmış olan görüşe göre incelemekte olduğumuz suçun işlenebilmesi için kanunda bir özellik aranmamış olup herkes bu suçu işleyebilmektedir²³². Burada failin suçu kimin için yahut neden işlediğinin herhangi bir önemi yoktur²³³. Bununla birlikte suçu işleyecek kişilerin bilişim sistemleri ve bunların kullanımı hakkında temel seviyede bilgi sahibi olması gerekmektedir²³⁴. Unutulmaması gereken nokta ise bu gerekliliğin failin suçu işleyebilmesi için söz konusu olan fiili bir gereklilik olduğu ve kanunun böyle bir şartı aramadığıdır²³⁵.

Bilişim sistemine girme suçunun failini yalnızca bilişim ağlarını kullanarak bir başka bilişim sistemine yetkisiz olarak erişen kimse oluşturmaz. Doğrudan bir bilişim sistemine erişen kişi de bu suçu işlemiş sayılacaktır²³⁶. Bununla birlikte girilmek istenen bilişim sisteminin güvenlik seviyesi arttıkça sisteme erişim zorlaşmakta; normalin üstünde bir bilgi ve beceri gerektirmektedir²³⁷. Bu nedenle incelemekte

²²⁸ Program örnekleri için bkz. Mojid Yor/ Kevin F. Steinmetz, **Cybercrime and Society. Third Edition**, London: Sage Publications, 2019 s. 66-67.

²²⁹ Dülger, **Bilişim Suçları** s. 249.

²³⁰ Akbulut, **Bilişim Alanında Suçlar** s. 120. Gül, **a.g.e.** s. 94-95. Bayındır, **a.g.e.** s. 62.

²³¹ Emre Cihan Ateş/Ahmet Saluk, "*Bilişim Suçları Kapsamında Suça Sürüklenen Çocukların İncelenmesi*", **HUMANITAS - Uluslararası Sosyal Bilimler Dergisi**, C. 6, S. 12, 2018 s. 163-164.

²³² Dülger, **Bilişim Suçları** s. 249. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 958. Hafızoğulları/Özen, **Topluma Karşı Suçlar** s. 445. Şahbaz, **a.g.e.**, s. 3130. Özçelik **a.g.e.** s. 47.

²³³ Yaşar/Gökcan/Artuç, **a.g.e.** s. 7287. Apaydın, **a.g.m.** s. 258.

²³⁴ Koca/Üzülmez, **Özel Hükümler** s. 896. Akarslan, **a.g.e.** s. 44. Çetin, **a.g.e.** s. 6.

²³⁵ Kurt, **a.g.e.** s. 241.

²³⁶ Koca/Üzülmez, **Özel Hükümler** s. 896.

²³⁷ Dülger, **Bilişim Suçları** s. 249.

olduğumuz suç çoğunlukla “*hacker*”²³⁸ ya da “*cracker*” gibi isimlerle anılan bilgisayar korsanları tarafından işlenmektedir²³⁹.

Bilişim sistemine girme suçunun başka bir bilişim sistemi ve bir ağ vasıtasıyla uzaktan işlendiği durumlarda faili belirlemenin en kolay ve kısa yolu ihlali yapan bilişim sisteminin IP bilgilerini takip etmektir. IP bilgilerinin takibi ile suç konusu eylemin icrasında kullanılan cihazın abone ve konum bilgilerine ulaşılabilir²⁴⁰. Bununla birlikte suçun işlendiği IP adresinin üzerine kayıtlı olduğu kimsenin doğrudan suçlu olarak kabul edilmesi objektif ceza sorumluluğunun benimsendiği sonucunu doğuracağından hukuka aykırı olacaktır. Böyle bir durumda IP’nin sahibi görünen kişinin gerçekten söz konusu suçu işleyip işlemediğinin araştırılması ve ispatlanması gerekmektedir²⁴¹. Yargıtay da verdiği bir kararda IP numarasını birden fazla cihazın sürekli ya da geçici olarak kullanmasının mümkün olduğunu; suçun işlendiği IP adresinin ve suç işlendiği sırada sanığın kullandığı telefon ve bilgisayarların incelenerek suç işlenen IP’ye bağlanıp bağlanmadığının ayrıca araştırılması gerektiğini ifade etmiştir²⁴². Yine yüksek mahkeme kararlarına²⁴³ bakıldığında

²³⁸ İlk ortaya çıktığı 1960’lı yıllarda bilgisayar problemlerine yaratıcı, zarif ve etkili çözümler geliştirme konusunda yetenekli kişileri tanımlamak için kullanılan hacker kavramı günümüzde üç gruba ayrılmaktadır. 1. Sistemdeki açıkları bularak suç işlemeyi ve bunun sonucunda kişisel çıkar elde etmeyi amaçlayan siyah şapkalı hackerlar. 2. Bilgisayar korsanlarına karşı sistemi daha güvenli hale getirmek için sistemin açıklarını arayan ve bunu sistem sahipleri ile otoritelerle paylaşan beyaz şapkalı hackerlar. 3. İki gruba da dahil olmayarak menfaati doğrultusunda hareket eden gri şapkalı hackerlar. Yor/Steinmetz, **a.g.e.** s. 53-54.

²³⁹ Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 958.

²⁴⁰ Doğan Gedik, “*Bilişim Suçlarında Ip Tespiti İle Ekran Görüntüleri Çıktılarının İspat Değeri*”, **Bilişim Hukuku Dergisi**, C. 1, S. 1, 2009 s. 55-56.

²⁴¹ Tezcan/Erdem/Önok, **a.g.e.** s. 1149 Apaydın, **a.g.m.** s.260. Ekici Şahin/Koruculu, **a.g.e.** s. 595.

²⁴² “... Tutulmasında yasal zorunluluk bulunmayan PORT bilgisine ulaşıldığında, birden fazla kişiye verilen IP’nin, suçun işlendiği saatte kim tarafından kullanıldığının belirlenmesi mümkün olmaktadır. Microsoft Corporation’dan de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde e-mail adresinin aktif olup olmadığı, bu adrese giriş yapılıp yapılmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise değişikliğin ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili Telekom Müdür- lüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli ve loglar üzerinde inceleme yapılmalı, ayrıca IP adresini kullanan bilgisayarların MAC numaraları araştırılmalıdır.” Yar. 8. CD, E. 2013/4668, K. 2014/9860, T. 16.04.2014 <https://lexpera.com.tr> (E.T. 04.12.2021) Aynı yönde bkz. Yar. 8. CD, E. 2019/19020, K. 2020/10577, T. 27.02.2020 <https://legalbank.net> (E.T. 04.12.2021) Aynı yönde bkz. Yar. 12. CD, E. 2014/11923, K. 2015/14, T. 12.01.2015 (Kararı aktaran: Ümit Erdem/Çağrı Şükrü Uluslu/Gökberk Dumanlı, **Yargıtay (2014-2016) Kararlarında Sosyal Medya**, İstanbul: Legal Yayıncılık, 2016 s. 300-311.)

²⁴³ “Sanık ...’ın tüm aşamalarda, adına kayıtlı bulunan IP numarasının başkası tarafından kullanılarak suça konu havale işlemlerinin yapılmış olabileceğini, atılı suçu işlemediğini savunması karşısında, suç tarihi itibariyle sanığın kullandığı modemin kablosuz olup olmadığı, şifre ile kullanıp kullanılmadığı, aynı IP numarası üzerinden sanığın bilgisayarı dışında başka bilgisayarlardan internete girilip girilmediği, IP numarasının dinamik olup olmadığı sorularak, gerekirse bilirkişi incelemesi de yaptırılarak IP numarasının sahte oluşturulup oluşturulamayacağı, sanığa ait modemden başkasının

özellikle birden fazla kişinin ortak bir internet bağlantısını kullandığı ortamlarda internet sağlayıcısından bilgi istenilmesi ve log kayıtlarının incelenerek suçun hangi cihazla işlendiğinin tespit edilmesi gerektiği vurgulanmıştır.

Bu başlık altında değinilmesi gereken son nokta ise tüzel kişilerin bilişim sistemine girme suçunun faili olup olamayacağıdır. Tüzel kişilerin ceza hukuku anlamında fail olup olamayacağına ilişkin doktrinde farklı görüşler²⁴⁴ olsa da TCK m. 20’de cezai sorumluluğun şahsi olduğu ve tüzel kişilere cezai yaptırım uygulanamayacağı düzenlenmiştir. Ancak tüzel kişilerin yararına ya da bunların faaliyetleri çerçevesinde suç işlendiği takdirde kanunda öngörülen güvenlik tedbirleri uygulanabilecektir²⁴⁵. TCK m. 246 ile de bu duruma ilişkin bir düzenleme yapılarak “*Bilişim Alanında Suçlar*” bölümde düzenlenen suçların işlenmesi sonucunda yararına menfaat temin edilmiş olan tüzel kişiler hakkında TCK m. 60’ta düzenlenen güvenlik tedbirlerinin uygulanacağı ifade edilmiştir²⁴⁶.

2. Mağdur

Mağdur, doktrinde suçun işlenmesi sonucunda zarara uğratılan yahut tehlikeye maruz bırakılan hak ve menfaatin sahibi olan kişi olarak tanımlanmaktadır²⁴⁷. Bir başka ifadeyle mağdur, suçun konusunun ait olduğu kişidir²⁴⁸.

TCK m. 243 incelendiğinde, kanun metninde suçun mağduru için özel bir nitelik ve gereklilik öngörülmediği görülmektedir. Bizim de katıldığımız yazarlara göre incelemekte olduğumuz suçun mağduru suça konu sisteme doğrudan erişim ve kullanım yetkisi olan ve bu sistem üzerinde hak sahibi olan şahıstır²⁴⁹. Bu şahıs

giriş yapıp yapamayacağı da belirlenerek sanığın hukuki durumunun takdir ve tayini gerekirken eksik inceleme ve soruşturma ile yazılı şekilde hüküm kurulması bozmayı gerektirmiş...” Yar. 8. CD, E. 2014/28153, K. 2016/7842, T. 19.04.2016 Aynı yönde bkz. Yar. 8. CD, E. 2019/19020, K. 2020/10577, T. 27.02.2020, Yar. 8. CD,, E. 2016/12634 K. 2017/4967, T. 03.05.2017, Yar. 8. CD,, 2015/13416 K. 2015/2470, T. 18.11.2015 <https://legalbank.net> (E.T. 04.12.2021)

²⁴⁴ Ayrıntılar için bkz. Baş Bayraktaroğlu, **a.g.e.** s. 131 vd. Devrim Aydın, “*Tüzel Kişilerin Ceza Sorumluluğu Tartışmaları*”, **Uyuşmazlık Mahkemesi Dergisi**, S. 10, 2017 s. 100-103.

²⁴⁵ Dönmezer/Erman, **a.g.e.**, s. 714. Baş Bayraktaroğlu, **a.g.e.** s. 365. Kerim Çakır, “*Tüzel Kişiler Hakkında Güvenlik Tedbirleri*”, **Beykent Üniversitesi Hukuk Fakültesi Dergisi**, C. 4, S. 8, Aralık 2018 s. 132-133. Soyaslan, **Genel Hükümler**, s. 530.

²⁴⁶ Dülger, **Bilişim Suçları** s. 257. Yaşar/Gökcan/Artaç, **a.g.e.** s. 7287. Çetin, **a.g.e.** s. 6.

²⁴⁷ Dönmezer/Erman, **a.g.e.**, s. 726. Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 213. Akbulut, **Genel Hükümler** s. 423.

²⁴⁸ Koca/Üzülmez, **Genel Hükümler** s. 116.

²⁴⁹ Koca/Üzülmez, **Özel Hükümler** s. 897. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 958-959. Artuk /Gökçen/Yenidünya, **a.g.e.** s. 867. Çetin, **a.g.e.** s. 6.

sistemin sahibi olabileceği gibi sistemin sahibi tarafından sisteme giriş ve kullanım yetkileriyle donatılmış bir kişi de olabilir²⁵⁰.

Tüzel kişilerin suçun mağduru olup olamayacağı hususunda doktrinde görüş ayrılığı bulunmaktadır. Kimi yazarlara göre TCK sistematığına göre suçun mağduru ancak gerçek kişiler olabilmekte; suç nedeniyle menfaatleri ihlal edilen tüzel kişiler ve tüzel kişiliği haiz olmayan kişi toplulukları ise suçtan zarar gören olarak adlandırılmaktadır²⁵¹. Bu görüşü savunan yazarlara göre suç konusu bilişim sistemini sahibi dahi olsa tüzel kişiler mağdur olarak değil, suçtan zarar gören olarak yargılama süreçlerine katılabileceklerdir²⁵². Bizim de desteklediğimiz yazarlara göre ise TCK’da tüzel kişilerin mağdur olmalarını engelleyici bir düzenleme bulunmadığından suçun niteliği elverdiği ölçüde tüzel kişiler de suçun mağduru olabilmektedir²⁵³. Sistemin sahibi olan yahut sistem üzerinde -kira, ariyet ya da finansal kiralama gibi sözleşmelerle- hak sahibi olmuş tüzel kişiler de tıpkı gerçek kişiler gibi suçun mağduru olarak kabul edilmelidir²⁵⁴.

Bilişim sistemine girme suçunun mağduru kimi yazarlarca bilişim sistemine girilmesi veya sistemde kalınması sonucunda hak ve menfaatleri zarar gören kişi olarak tanımlanmış²⁵⁵ olsa da kanaatimizce bu yaklaşım doğru değildir. Zira bilişim sistemine girme suçu bir tehlike suçudur ve suçun işlenmiş olması için zararın meydana gelmesi gerekmemektedir. Bu sebeple suçun mağduru sisteme girilmesi ve orada kalınması nedeniyle menfaatleri tehlikeye girmiş olan kişidir²⁵⁶.

Hak ve menfaatleri ihlal edilen kişilerin birden fazla olması durumunda ise bu kişilerin tamamı mağdur olarak kabul edilmelidir²⁵⁷. Buradan yola çıkan kimi yazarlar ise yasadışı erişilen sistemde bulunan verilerin ilgili olduğu üçüncü kişilerin de bilişim sistemine girme suçunun mağduru olduğunu öne sürmektedir. Sözgelimi bir bankanın

²⁵⁰ Akbulut, **Bilişim Alanında Suçlar** s. 121. Mahmutoglu, **a.g.e.** s. 859.

²⁵¹ Koca/Üzülmmez, **Genel Hükümler** s. 117. Dülger, **Genel Hükümler** s. 378-279.

²⁵² Dülger, **Bilişim Suçları** s. 258. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7288. Apaydın, **a.g.m.** s. 260. Mahmutoglu, **a.g.e.** s. 860. Özçelik, **a.g.e.** s. 51.

²⁵³ Tuğrul Katoğlu, “*Ceza Hukukunda Suçun Mağduru Kavramının Sınırları*”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C. 61, S. 2, 2012 s.672-673. Dönmezer/Erman, **a.g.e.**, s. 727-728. Demirbaş, **a.g.e.** s. 592. Baş Bayraktaroğlu, **a.g.e.** s. 742.

²⁵⁴ Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu** s. 1394. Soyaslan, **Özel Hükümler**, s. 662. Doğan **Bilişim Suçları ve Türk Ceza Kanunu**. s.295. İhtiyaroğlu, **a.g.e.** s.415. Ekici Şahin/Koruculu, **a.g.e.** s. 596. Kurt, **a.g.e.** s. 163. Gül, **a.g.e.** s.95. Kabadayı, **a.g.e.** s. 72-73.

²⁵⁵ Yılmaz, **a.g.e.** 182. Soyaslan, **Özel Hükümler**, s. 662. Parlar, **a.g.e.** s. 25

²⁵⁶ Mahmutoglu, **a.g.e. Suçlar** s. 862. Özçelik, **a.g.e.** s. 50. dipnot 16.

²⁵⁷ Taşkın, **a.g.e.** s. 24. Kurt, **a.g.e.** s. 242. Kabadayı, **a.g.e.** s. 72.

sistemine hukuka aykırı olarak girildiği takdirde sistemdeki verilerinin gizliliği ihlal edilen müşteriler de bu suçun mağduru olacaklardır²⁵⁸. Bizim de desteklediğimiz görüşe göre ise bu tip bir durumda TCK m. 243 özelinde suçun mağduru sadece sistemin sahibi veya sistem üzerinde hak sahibi olan kişi veya kişiler olacaktır. Bilişim sistemine girme suçu sistemdeki verilerin değil doğrudan sistem üzerinde işlenmektedir²⁵⁹. Burada sistemin içerisindeki bulunan verilerin korunmasına yönelik bir düzenleme olmadığı için kendileri ile ilgili veriler ele geçirilen kişiler TCK m. 136'da yer alan verilerin hukuka aykırı şekilde ele geçirilmesi suçunun mağduru olacaklardır²⁶⁰. Bunun yanında 243. maddenin üçüncü fıkrasında düzenlenen suçun netice itibarıyla ağırlaşmış halinin meydana gelmesi; bir başka ifadeyle “*sistemin içerdiği verilerin yok olması veya değişmesi*” durumunda zarar gören veriler kime ilişkin ise o kişiler de suçun mağduru olacaktır.

Bilişim sistemine girme suçu ile korunması amaçlanan değer bu sistemlerin güvenliği olduğunu savunan bazı yazarlara göre belirli bir grubun ya da kişilerin bu suçun mağduru olduğu söylenemez²⁶¹. Yine benzer şekilde incelemekte olduğumuz suçun “*Kişilere Karşı Suçlar*” başlığı altında düzenlenmemiş olmasından yola çıkan bir görüş ise suçun failinin bir kişi ya da kişiler değil kamu idaresi olduğunu savunmaktadır. Zira güvenlik bir bilişim sistemini sağlamak kamu düzeninin gereği olduğu için; bu güvenin ihlal edilmesi durumunda da kamu idaresi mağdur edilmiş olacaktır. Bu yazarlara göre kişiler ancak suçtan zarar gören olabilecektir²⁶². Bir görüş ise yasadışı erişim sağlanan sistemin bir tüzel kişiye ait olması durumunda birden fazla kişinin bu suçun mağduru olabilmesinin mümkün olabileceğini ifade etmiştir. Burada tüzel kişinin niteliği göz önünde bulundurulduğunda tüm toplumun mağdur olması da mümkündür²⁶³.

3. Suçun Konusu

Ceza hukuku anlamında bir suçu meydana getiren her hareketin muhakkak bir konusu vardır²⁶⁴. Maddi anlamda suçun konusunu yasada tarif edilen fiilin üzerinde

²⁵⁸ Artuk/Gökçen/Yenidünya, **a.g.e.** s. 867. Yenidünya, **a.g.e.** s. 1027. Doğan **Bilişim Suçları ve Türk Ceza Kanunu**, s.295. Apaydın, **a.g.m.** s. 260. Erdoğan, **a.g.m.** s. 1394-1395. Kayaer, **a.g.e.** s. 97.

²⁵⁹ İhtiyaroğlu, **a.g.e.** s.415.

²⁶⁰ Akbulut, **Bilişim Alanında Suçlar** s. 122. Güler, **a.g.e.** s. 22.

²⁶¹ Tezcan/Erdem/Önok, **a.g.e.** s. 1150.

²⁶² Hafızoğulları/Özen, **Topluma Karşı Suçlar** s. 445.

²⁶³ Akbulut, **Bilişim Alanında Suçlar** s. 121.

²⁶⁴ Koca/Üzülmez, **Genel Hükümler** s. 117.

işlendiği insan, insana ait maddi veya manevi bir değer, eşya veya araçlar oluşturmaktadır²⁶⁵.

Öncelikle bilişim sistemine girme suçunun konusunun incelenmesi hususunda doktrinde meydana gelen maddenin ikinci ve üçüncü fıkraları kaynaklı fikir ayrılığından söz etmek yerinde olacaktır. Kimi yazarlar incelemekte olduğumuz suçun konusunu “*bilişim sistemi*” olduğunu kabul ederek incelemelerini buna göre yapmaktadır²⁶⁶. Bir kısım yazar ise maddenin fıkraları temelinde bir ayırım yapmakta ve ilk fıkranın konusunun “*bilişim sistemi*” olduğunu kabul etmekle birlikte ikinci ve üçüncü fıkralar için ayrı konu belirleme yoluna tercih etmektedir. Bu yazarlar suçun bedeli karşılığı yararlanabilen sistemlere karşı işlenmesi halinde cezanın azaltılacağını düzenleyen ikinci fıkranın konusunun “*bedeli karşılığı yararlanılabilen sistemler*”; suçun neticesi sebebiyle ağırlaşmış hali olan bilişim sistemine girilmesi sırasında sistemdeki verilerin yok edilmesi veya değiştirilmesi halini düzenleyen üçüncü fıkranın konusunun ise “*sistemin içerdiği veriler*” olarak kabul etmektedir²⁶⁷. Bu çalışmada ise ilk görüş benimsenecek ve anlam bütünlüğünün korunması açısından ikinci ve üçüncü fıkralara özgü hususlara kendi alt başlıkları altında değinilecektir.

Türk Ceza Kanunu m. 243’te düzenlenen bilişim sistemine girme suçunun konusunu tamamına veya bir kısmına hukuka aykırı şekilde girilen veya orada kalmaya devam edilen bilişim sistemi oluşturur²⁶⁸. Daha önce de belirtildiği üzere; bilişim sistemi kısaca üzerine veri yüklenebilen, bu verileri otomatik bir şekilde işleme tabi tutabilen ve bu işlemler sonucu ortaya çıkan verileri diğer bilişim sistemlerine aktarabilen elektronik- manyetik sistemler olarak tanımlanabilir²⁶⁹. Yargıtay ise kanun gerekçesinde yer alan “*verileri toplayıp yerleştirdikten sonra bunları otomatik*

²⁶⁵ Dönmezer/Erman, **a.g.e.**, s. 33. Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 214. Dülger, **Genel Hükümler** s. 382. Akbulut, **Genel Hükümler** s. 425.

²⁶⁶ Akbulut, **Bilişim Alanında Suçlar** s. 122. Koca/Üzülmez, **Özel Hükümler** s. 897-899. Tezcan/Erdem/Önok, **a.g.e.** s. 1150-1151. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 959-960. Yıldız, **Bilişim Sistemine Girme** s. 235.

²⁶⁷ Özçelik, **a.g.e.** s. 52. Dülger, **Bilişim Suçları** s. 259. İhtiyaroğlu, **a.g.e.** s. 415 vd. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7288.

²⁶⁸ Dülger, **Bilişim Suçları** s. 259. Soyaslan, **Özel Hükümler**, s. 662. Şahbaz, **a.g.e.** s. 3128.

²⁶⁹ Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 957. Koca/Üzülmez, **Özel Hükümler** s. 898. Akarslan, **a.g.e.** s. 30. Taşkın, **Bilişim Hukuku Uluslararası Uyuşmazlıklar** s. 333-334. Özçelik, **a.g.e.** s. 52.

*işlemlere tâbi tutma olanağını veren manyetik sistemler*²⁷⁰” şeklindeki tanımları kararlarında²⁷¹ istikrarlı bir şekilde kullanmaktadır²⁷².

Bir sistemin bilişim sistemi sayılabilmesi ve suçun konusunu oluşturabilmesi için doktrinde vurgulanmakta olan temel gereklilik sistemin hem veri-işleme hem de veri-iletişim işlevlerini bünyesinde barındırıyor olmasıdır²⁷³. Öte yandan sistemin genel amaçlı olarak verileri işleyebilir ve kullanılabilir olması da bazı yazarlarca aranmaktadır. Bir başka ifadeyle sadece belirli işlemleri otomatik bir şekilde yerine getirebilen ve belli bir amacı ifaya özgülenmiş, veri işleme ve iletim özelliği olmayan -örneğin barkod okuyucular, hesap makineleri, bina girişlerinde kullanılan manyetik kartlar, kahve otomatları ve klasik anlamda beyaz eşyalar- elektronik ve manyetik cihazlar bilişim sistemi olmayıp suçun konusunu oluşturamazlar²⁷⁴. Yargıtay da kararlarında genel amaçlı olarak kullanılabilirlik özelliğini vurgulayarak önceden belirlenmiş bir amaca özgülenip bundan başka bir fonksiyon eda edemeyen araçların bilişim sistemi sayılamayacaklarını ifade etmiştir²⁷⁵. Günümüzde artık para çekme işlevinin dışında birçok bankacılık faaliyetinin de yapılabildiği; ATM’ler ise her ne kadar kimi yazarlarca²⁷⁶ bilişim sistemi olarak değerlendirilmese de kanaatimizce bilişim sistemi özelliklerini taşımaktadır. Yargıtayın da kararlarında²⁷⁷ belirttiği gibi bu cihazlar tek başlarına bilgisayar özelliği göstermeseler de banka bilişim sistemiyle bağlantılı olarak çalışan ve günümüzde bilişim sistemi özelliğine sahip cihazlardır²⁷⁸. Yine gerçek ya da tüzel kişilerin sahip oldukları banka hesaplarına internet bankacılığı

²⁷⁰ **Türk Ceza Kanunu Madde Gereklileri** www.lexpera.com.tr (E. T. 08.12.2021)

²⁷¹ YCGK E. 2013/448, K. 2014/524, T. 25.11.2014; Yar. 15. CD, E. 2013/13869, K. 2015/28709, T. 15.09.2015; Yar. 12. CD, E. 2015/10388, K. 2017/1556, T. 01.03.2017; Yar. 8. CD, E. 2019/9478, K. 2020/15892, T. 23.09.2020 <https://legalbank.net> (E.T. 08.12.2021)

²⁷² Bilişim sistemi kavramı için doktrinde yapılan tanımlar, tartışmalar ve kanun gerekçesindeki tanıma dair eleştirilere bu çalışmanın “*Temel Kavramlar*” bölümünde ayrıntılı bir şekilde değinilmiştir.

²⁷³ Akbulut, **Bilişim Alanında Suçlar** s. 13-17. Yenidünya, **a.g.e.** s. 1029.

²⁷⁴ Koca/Üzülmüş, **Özel Hükümler** s. 898-899. Karakehya **a.g.e.** s. 8. Taşkın, **a.g.m.** s. 334.

²⁷⁵ “*Bilişim sisteminin, bilgileri otomatik olarak işleme tabi tutması ve manyetik olması dışında en önemli özelliği, genel amaçlı kullanım özelliğidir. Yani belli bir işin yapılmasına özgülenip başka bir fonksiyon eda edemeyen bir sistem bilişim sistemi değildir.*” YCGK, E. 2009/11-193, K. 2009/268, T. 17.11.2009 Aynı yönde bkz. Yar. 8. CD, E. 2018/1810, K. 2019/6992, T. 16.05.2019 <https://legalbank.net> (E.T. 08.12.2021)

²⁷⁶ Tezcan/Erdem/Önok, **a.g.e.** s. 1150. Kayaer, **a.g.e.** s. 94.

²⁷⁷ Yar. 10. CD, E. 2004/14311 K. 2004/10906 T. 02.11.2004; Yar. 11. CD, E. 2014/7245, K. 2014/5492, T. 24.03.2014; Yar. 8. CD, E. 2016/2859, K. 2016/7187, T. 01.06.2016 <https://legalbank.net> (E.T. 08.12.2021)

²⁷⁸ Kurt, **a.g.e.** s. 156. Taşkın, **a.g.m.** s. 333. Taştırmur, **a.g.e.** s. 12.

aracılığıyla hukuka aykırı olarak girilmesi halinde bilişim sistemine girme suçu oluşacaktır²⁷⁹.

Kuşkusuz ki bu çalışmanın konusu olan suçun üzerinde işlendiği başlıca sistemler bilgisayarlardır²⁸⁰. Bununla birlikte uygulamada en sık karşılaşılan bilişim sistemi bilgisayar da olsa; bilişim sistemleri bilgisayardan ibaret olmayıp bilgisayarı da kapsayan daha geniş bir kavramdır²⁸¹. Yargıtay Ceza Genel Kurulu da bir kararında bilişim sisteminin bilgisayarı da kapsayan bir üst kavram olduğunu ifade etmiştir²⁸². Bu anlamda bilgisayar dışında; veri-işleme ve veri-iletme yeteneğine sahip GPRS uyumlu cep telefonları ve akıllı telefonlar da incelmekte olduğumuz suçun konusunu oluşturabilmektedir²⁸³. Yargıtay da verdiği kararlarda bu cihazların bilişim sistemi olarak kabul edilmesi gerektiğini ifade etmiştir²⁸⁴.

Bilişim sistemine girme suçunu düzenleyen 243. maddede “*bir bilişim sisteminin tamamına veya bir kısmına*” ifadesinin kullanıldığı göz önüne alındığında sistemin donanımı, bileşenleri, yazılımı içerisindeki dizinler gibi belli bir parçasına hukuka aykırı şekilde girilmesi durumunda da anılan suçun oluşacağı söylenebilir²⁸⁵. Bu durumda bir bilişim sistemi ile arasındaki bağlantısı devam ettiği²⁸⁶ sürece bu sistemin

²⁷⁹ “Sanığın ... internet üzerinden izinsiz giriş yaptığı, ancak şirkete ait hesaba girdikten sonra bu hesapta oynama yaparak başka bir hesaba havale yapmadığının iddia ve kabul olunması karşısında sanığın eyleminin 5237 sayılı TCK'nun 243/1.maddesinde düzenlenen suçu oluşturduğu gözetilmeden yazılı şekilde (5237 sayılı TCK. nun 244/4, 35/2. maddeleri gereğince) hüküm tesisi, yasaya aykırı ” Yar. 11. CD, E. 2008/18190, K. 2009/3058, T. 26.03.2009 <https://legalbank.net> (E.T. 08.12.2021)

²⁸⁰ Bilgisayar kavramının tanımı, bileşenleri ve türleri bu çalışmanın “Temel Kavramlar” bölümünde açıklanmıştır.

²⁸¹ Erdağ, **a.g.e.** s. 279.

²⁸² “Görüldüğü gibi, “bilişim sistemi”, “bilgisayara” göre daha geniş bir alanı kapsayıp bu haliyle bir üst kavramdır. Bilgisayar verilerin depo edilmesi, saklanması, işlenmesi ve yeniden değerlendirilmesi faaliyetini gerçekleştirmesine karşın “bilişim sistemi” hem verilerin işlenmesi hem de verilerin aktarılmasını kapsar.” YCGK. E. 2007/6-136 K. 2007/150 T. 19.6.2007 www.lexpera.com.tr (E. T. 08.12.2021)

²⁸³ Tezcan/Erdem/Önok, **a.g.e.** s. 1150. Ekici Şahin/Koruculu, **a.g.e.** s. 594. Kayaer, **a.g.e.** s. 94.

²⁸⁴ “ ...Cep telefonlarında mobil işletim sistemleri bulunduğu ve program yüklenebilmesinin mümkün olduğu ... Cep telefonlarının bilişim sistemine girme ve orada kalma suçunun konusunu oluşturmayacağından bahisle, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması yasaya aykırı ... görülmüş olduğundan” Yar. 8. CD, E. 2014/30037, K. 2015/14023 T. 18.03.2015; Aynı yönde bkz. Yar. 8. CD, E. 2014/29566, K. 2015/13421, T. 11.03.2015; Yar. 8. CD, E. 2018/10307, K. 2019/10751, T. 17.9.2019 <https://legalbank.net> (E.T. 08.12.2021)

²⁸⁵ Karakehya, **a.g.e.** s. 14-15. Erdağ, **a.g.e.** s. 282.

²⁸⁶ “Faili mağdura ait USB, taşınabilir bellek gibi donanımları kendi bilişim sistemine takarak çalıştırması ve içindeki verilere ulaşılması halinde 5237 sayılı TCK kapsamında özel hayatın gizliliğini ihlal, verileri hukuka aykırı olarak verme veya ele geçirme suçu gibi somut olaya göre farklı suçlar gündeme gelebilecektir.” Özçelik, **a.g.e.** s. 51. dipnot

bir parçası olarak kabul edilen disket, CD, USB Bellek gibi araçlara hukuka aykırı olarak erişim sağlanarak da suç işlenebilecektir²⁸⁷.

Herhangi bir donanıma bağlı olmaksızın uzaktan erişilebilme özelliğine sahip sistemler de bilişim sistemine girme suçunun konusunu oluşturabilmektedir. Özellikle başkalarına ait online oyun profillerine²⁸⁸, sosyal medya hesaplarına²⁸⁹ ve e-posta adreslerine²⁹⁰ hukuka aykırı bir şekilde erişim sağlanarak bu suçun işlenmesi sıkça yargı kararlarına konu olmaktadır. Yine gerek bireysel gerekse ticari amaçla kullanılan web sitesi sunucuları²⁹¹ ve bulut bilişim²⁹² sistemleri de incelemekte olduğumuz suçun konusu olabilmektedir.

Son yıllarda ortaya çıkan ve günlük hayatımızda gittikçe daha fazla yer tutmaya başlayan akıllı sistemler ile “Nesnelerin İnterneti (*Internet of Things*)” kavramlarına da bu başlık altında değinilmesi yerinde olacaktır. Nesnelerin interneti, algılayıcısı/sensörü olan nesnelerin internet bağlantısını kullanarak birbiriyle haberleşmesini ifade etmektedir²⁹³. Akıllı telefonlar ve kişisel bilgisayarlara bağlanabilen evlerdeki akıllı sistemler ve giyilebilir teknoloji ürünleri nesnelerin

²⁸⁷ Akbulut, **Bilişim Alanında Suçlar** s. 126. Karakehya, **a.g.e.** s. 14-15. Kurt, **a.g.e.** s. 156.

²⁸⁸ Murat Semiz, **Bilişim Suçları ve Soruşturma Yöntemleri**, Ankara: Adalet Yayınevi, Ocak 2020 s. 64-65.

²⁸⁹ “Şikayetçinin rızası olmadan e-mail ve Facebook hesabına girip şifrelerini değiştirmek suretiyle ... sanığın eyleminin TCK’nın 243/1. maddesi kapsamındaki suçu oluşturacağı gözetilmeden suç vasfında yanılığa düşülerek yazılı şekilde hüküm kurulması, yasaya aykırı...” Yar. 8. CD, E. 2018/10824, K. 2019/15723, T. 25.12.2019 Aynı yönde bkz. Yar. 8. CD, E. 2016/8243 K. 2017/4158 T. 13.4.2017; Yar. 8. CD, E. 2015/3445 K. 2015/22717 T. 14.10.2015 YCGK. E. 2007/6-136 K. 2007/150 T. 19.6.2007 www.lexpera.com.tr (E. T. 10.12.2021) Yine aynı yönde bkz. Yar. 12. CD, E. 2013/27327, K. 2014/14176, T. 09.06.2014 (Kararı aktaran: Erdem/ Uluslu/Dumanlı, **a.g.e.**, s. 350-352.)

²⁹⁰ “Sanığın, katılana ait iki farklı mail adreslerine izinsiz olarak girme eyleminin sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu değil, TCK’nın 243/1.maddesinde düzenlenen bilişim sistemine girme suçunu oluşturduğu” Yar. 12. CD, E. 2015/9555 K. 2016/10731 T. 22.6.2016 Aynı yönde bkz. Yar. 8. CD, E. 2015/3445, K. 2015/22717, T. 14.10.2015; Yar. 8. CD, E. 2015/6218, K. 2015/23910, T. 04.11.2015 Yar. 8. CD, E. 2016/11236, K. 2017/10500, T. 27.09.2017 https://legalbank.net (E.T. 08.12.2021)

²⁹¹ “Dosyanın bir bütün halinde incelenmesinde, sanığın birden fazla kez aynı kast altında katılanın yetkilisi olduğu ve F2 Bilişim Sistemleri Ltd. Şti’nin internet sitesine girerek ... sanığın eyleminin TCK’nın 244/2 maddesinde belirtilen bilişim sistemine izinsiz girerek veri yerleştirme ve bozma suçunu değil, sadece bilişim sistemine hukuka aykırı olarak girme suçunu oluşturduğu” Ankara BAM 8. CD, E. 2017/207, K. 2018/439, T. 17.4.2018 www.lexpera.com.tr (E. T. 10.12.2021)

²⁹² Bilgisayar tabanlı kaynakların internet ağ yapısı üzerinden sanallaştırılarak paylaşılması ve kullanılması temelli bir modeldir. İnternet üzerinden istenilen her yerden bu sisteme bağlanılarak sistemin/sunucuların içerisindeki veri ve uygulamalara erişilebilmektedir. Ayrıntılı bilgi için bkz. Murat Topaloğlu/Harun Özkişi/Egemen Tekkanat, **Bulut Bilişim**, Ankara: Seçkin Yayıncılık, 2017 s. 19 vd. Metin Turan, **Bulut Bilişim, 2. Baskı**, Ankara: Seçkin Yayıncılık, 2017 s. 69 vd.

²⁹³ Zeynel T. Kangal, **Yapay Zeka ve Ceza Hukuku**, İstanbul: On İki Levha Yayınları, Mayıs 2021 s. 35.

internetinin en yaygın örnekleridir²⁹⁴.. Birbirine bağlanan cihazların oluşturduğu sistemler; veri işleme, iletme ve saklama yeteneğine sahip olduklarından bilişim sistemi olarak kabul edilmelidir. Bu sistemlere veya sistemi oluşturan cihazlara hukuka aykırı bir şekilde giren veya sistemde kalmaya devam eden kişi incelemekte olduğumuz suç işlemiştir²⁹⁵.

Suç konu bilişim sistemleri kişisel bilgisayar ve cep telefonları gibi gerçek kişilere ait araçlar olabileceği gibi özel²⁹⁶ ve kamu tüzel kişilerine ait sistemler de olabilir²⁹⁷. Madde metni incelendiğinde sistem sahibinin kimliğinin suçun oluşumu ya da ceza miktarını etkilemeyeceği anlaşılmaktadır. Ayrıca TCK m. 243'e göre suçun oluşması için suç konusu bilişim sisteminin herhangi bir güvenlik önlemiyle koruma altında olmasına da gerek yoktur²⁹⁸. Kimi yazarlar ise bu durumu bir eksiklik olarak değerlendirmekte; suçun, özel programlar ve güvenlik tedbirleriyle korunan sistemler²⁹⁹ ile kamu kurumlarına ait bilişim sistemlerine³⁰⁰ karşı işlenmesi hallerinin cezayı ağırlaştırıcı nedenler olarak düzenlenmesi gerektiğini savunmaktadırlar.

4. Hareket

Bir suçun varlığında söz edilebilmesi için maddedeki tanıma uygun şekilde dış dünyada bir değişiklik meydana getirmeyi hedefleyen ve insan iradesine dayanan müspet ya da menfi bir hareket mevcut olmalıdır³⁰¹. Dış dünyada gerçekleştirilen hareketin kanundaki tanımla örtüşmesi durumunda cezalandırılması söz konusu olacaktır³⁰².

Çalışmamıza konu suçun düzenlendiği TCK m. 243'ün ilk kanunlaşan halinde suçun işlenebilmesi için bilişim sistemine tamamına ya da bir kısmına hukuka aykırı

²⁹⁴ Kavram hakkında ayrıntılı bilgi için bkz. Armağan Ebru Bozkurt Yüksel, “Nesnelerin İnternetinin Hukuki Yönden İncelenmesi”, **DEÜHFD**, C. 17, S. 2, Aralık 2015 s. 115.

²⁹⁵ Kangal, **a.g.e.** s. 36. Bozkurt Yüksel, **a.g.e.** s. 131

²⁹⁶ “...sanığın kendi ikrarı ile sabit olan şifreyle girilebilen şirket bilgisayarına ele geçirdiği şifre ile yetkisiz olarak hukuka aykırı girmesi eyleminin TCK'nın 243/1. maddesine uyan bilişim sistemine girme suçunu oluşturacağı gözetilerek, bu suçtan mahkumiyetine hükmedilmesi gerekirken, delillerin takdirinde ve suç vasfında yanılğıya düşülerek, dosya kapsamına uygun düşmeyen yetersiz gerekçelerle beraatine karar verilmesi, kanuna aykırı olup...” Yar. 12. CD, E. 2014/2525, K. 2014/17259, T. 08.09.2014 <https://legalbank.net> (E.T. 08.12.2021)

²⁹⁷ Tezcan/Erdem/Önok, **a.g.e.** s. 1150. Erdoğan, **a.g.m.** s. 1396. Apaydın, **a.g.m.** s. 261. Ekici Şahin/Koruculu, **a.g.e.** s. 594.

²⁹⁸ Özçelik, **a.g.e.** s. 57. Karşı görüş için bkz. Şahbaz, **a.g.e.** s. 3128.

²⁹⁹ Dülger, **Bilişim Suçları** s. 275. Ketizmen, **a.g.e.** s. 110. Erdoğan, **a.g.m.** s. 1400.

³⁰⁰ Karagülmez, **a.g.e.** 206. Özçelik, **a.g.e.** s. 58.

³⁰¹ Dönmezer/Erman, **a.g.e.**, s. 77. Dülger, **Genel Hükümler** s. 246.

³⁰² Koca/Üzülmüş, **Genel Hükümler** s. 122. Akbulut, **Genel Hükümler** s. 280.

olarak girmek ve orada kalmaya devam etmek şartı aranmakta ve bu nedenle doktrinde “çok hareketli suç³⁰³” ya da “bileşik hareketli suç³⁰⁴” olarak nitelendirilmekteydi. 6698 sayılı kanunla 2016 yılındaki değişikliklerle kanundaki “ve” ibaresi “veya” ile değiştirilmiştir. Bu değişiklik sonrası seçimlik hareketli bir suç haline gelmiş olan bilişim sistemine girme suçu “sisteme hukuka aykırı olarak girilmesi” fiiliyle işlenebileceği gibi, “sistemde kalınmaya devam etmek” şeklinde de işlenebilmektedir³⁰⁵. Suçun oluşabilmesi için bu iki fiilden birinin gerçekleşmesi yeterli olmakla birlikte aynı anda bu iki fiilin birlikte gerçekleşmesi halinde de tek bir suç işlenmiş olacaktır.³⁰⁶

Sisteme girme ve kalmaya devam etme eylemleriyle ilgili açıklamalara başlanmadan doktrindeki madde başlığına ilişkin eleştirilere değinmek yerinde olacaktır. Öncelikle madde metninde suçun bilişim sistemine girilmesi veya orada kalınması suretiyle işlenebileceği düzenlenmiş olmasına rağmen madde başlığının “Bilişim Sistemine Girme” şeklinde olmasının suçun sadece bilişim sistemine girilmek suretiyle işlenebileceği izlenimini uyandırması nedeniyle yanıltıcı olduğu ifade edilmiş³⁰⁷; madde metninde seçimlik hareket olarak öngörülen iki fiilden birini kapsamayan madde başlığı doktrinde yetersiz bulunmuştur. Bu eleştirilere paralel olarak 2016 yılında yapılan değişiklikten önce yazılan kimi eserlerde anılan suçun “bilişim sistemine girme ve kalmaya devam etme suçu³⁰⁸” ya da “bilişim sistemine girme ve kalma suçu³⁰⁹” şeklinde isimlendirildiği görülmektedir. Kimi yazarlar ise 2016 yılında sisteme girmeksizin veri nakillerini izlemeyi suç olarak düzenleyen dördüncü fıkranın eklenmesiyle bu eleştirilerin daha da önem kazandığını belirtmiştir. Zira dördüncü fıkradaki suç “bilişim sistemine girmeksizin” işlenmekte iken madde başlığı sisteme girmeyi ifade etmektedir³¹⁰.

Kanun metnindeki “girme” ifadesini fiziki olarak bir yere girmeyi çağrıştırdığı için eleştiren kimi yazarlar, bilişim sistemlerine fiziksel olarak girilemeyeceğini ifade

³⁰³ Özçelik, **a.g.e.** s. 67-68. Akbulut, **Bilişim Alanında Suçlar** s. 126. İhtiyaroğlu, **a.g.e.** s. 425.

³⁰⁴ Dülger, **Bilişim Suçları** s. 260-261. Yenidünya, **a.g.e.** s. 1034. Karagülmez, **a.g.e.** s. 202. Erdoğan, **a.g.m.** s. 1373-1374.

³⁰⁵ Akbulut, **Bilişim Alanında Suçlar** s. 126. Tezcan/Erdem/Önok, **a.g.e.** s. 1151. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 959-960. Koca/Üzülmez, **Özel Hükümler** s. 899. Soyaslan, **Özel Hükümler**, s. 662. Hafizoğulları/Özen, **Topluma Karşı Suçlar** s. 446.

³⁰⁶ Akbulut, **Bilişim Alanında Suçlar** s. 126. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 961.

³⁰⁷ Erdoğan, **a.g.m.** s. 1374. Tepe, **a.g.e.** s. 278.

³⁰⁸ Karagülmez, **a.g.e.** s. 199 vd.

³⁰⁹ Erdoğan, **a.g.m.** s. 1363 vd.

³¹⁰ Akbulut, **Bilişim Alanında Suçlar** s. 128. Güler, **a.g.e.** s. 18.

etmiş; İngiliz “access” kelimesinin Türkçe karşılığı olan “erişim” kelimesinin kullanılmasının daha doğru olacağını savunmuştur³¹¹. Bu fikre karşı çıkan yazarlara göre ise başka bir sistem üzerinden ağ yoluyla bir bilişim sistemine bağlanma anlamına gelen³¹² ve sistemin içerisindeki dosyalar, veriler gibi soyut unsurlara yönelik olan³¹³ erişim fiili ancak internet ya da benzer bir bilişim ağı ile uzaktan gerçekleştirilebilecektir. Girme eylemi ise Yargıtayın da kararlarında³¹⁴ belirttiği gibi hedef bilişim sisteminin düğmesine basılarak fiziki olarak gerçekleştirilebileceği gibi başka bir bilişim sistemi ve bilişim ağları yoluyla da icra edilebilecektir. Bu yönüyle erişim kavramını da kapsayan “girme” terimini tercih eden kanun koyucunun kararı isabetlidir³¹⁵.

Ceza hukuku anlamında kanunda öngörülen sonucun bir şeyi yapmak suretiyle doğması durumunda “icrai hareket”, yapılması beklenen hareketi yapmaktan imtina etmek suretiyle doğması halinde ise “ihmali hareket” söz konusu olacaktır³¹⁶. Bilişim sistemine girme fiilinin ancak icrai bir hareketle işlenebileceğine ilişkin doktrinde görüş birliği olsa da aynı durum kalma fiili için geçerli değildir. Kimi yazarlar sistemde kalmaya devam etmenin ancak ihmali hareketle gerçekleştirilebileceğini ifade etmektedir³¹⁷. Örneğin hukuka aykırı şekilde elde edilen şifre ile başkasına ait bir bilişim sistemine girilmesi halinde icrai hareketle işlenen girme eylemi söz konusu olacaktır. Girme yetkisi bulunmayan bir sisteme hata sonucu girmiş olduğunu fark eden failin sistemde kalmaya devam etmesi halinde ise ihmali hareketle sistemde kalmaya devam etme şeklinde suç işlenmiş olacaktır³¹⁸. Sisteme girmiş olan failin sistemde kalabilmesi için icrai bir hareket yapmak zorunda olabileceğini ifade eden bir

³¹¹ Dülger, **Bilişim Suçları** s. 261-262. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 960. Artuk/Gökçen/Yenidünya, **a.g.e.** s. 861. Karagülmez, **a.g.e.** s. 16. Ketizmen **a.g.e.** s. 100. Bayındır, **a.g.e.** s. 62. Kabadayı, **a.g.e.** s.76-77.

³¹² **Madde 3/1-e:** “Erişim: Herhangi bir vasıta ile internet ortamına bağlanarak kullanım olanağı kazanılmasını” Resmi Gazete, **İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik** <https://www.resmigazete.gov.tr/eskiler/2007/11/20071130-6.htm> (E.T. 11.12.2021)

³¹³ Akbulut, **Bilişim Alanında Suçlar** s. 128-129.

³¹⁴ “Bilişim sistemine girmek, bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir.” Yar. 8. CD, E. 2018/1078, K. 2018/2485, T. 08.03.2018 Aynı yönde: Yar. 8. CD, E. 2014/19342, K. 2015/2322, T. 03.02.2015; Yar. 8. CD, E. 2013/15110, K. 2014/11220, T. 30.04.2014 <https://legalbank.net> (E.T. 11.12.2021)

³¹⁵ Akbulut, **Bilişim Alanında Suçlar** s. 129. Koca/Üzülmüş, **Özel Hükümler** s. 900. Özçelik, **a.g.e.** s. 71-72.

³¹⁶ Dönmezer/Erman, **a.g.e.**, s. 82-83. Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 214. Hafizoğulları/Özen, **Ceza Hukuku Genel Hükümler** s. 170.

³¹⁷ Koca/Üzülmüş, **Özel Hükümler** s. 899-900. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7292. Erdoğan, **a.g.m.** s. 1373. Taşkın, **Bilişim Suçları** s. 26. Ketizmen, **a.g.e.** s. 106. Çetin, **a.g.e.** s. 10.

³¹⁸ Kayaer, **a.g.e.** s. 104-105.

diğer görüş ise kalma fiilinin ihmali hareketin yanında icrai hareketle de işlenebileceğini ifade etmektedir³¹⁹. Örneğin güvenlik yazılımları tarafından sistemden atılmamak için belli bir yazılımı çalıştıran fail icrai bir harekette bulunarak sistemde kalmaya devam etmiş olacaktır³²⁰. Her iki görüşün kabulü halinde de bilişim sistemine girme suçunun hem icrai hem de ihmali hareketle işlenebilmesinin mümkün olduğu söylenebilecektir.

Her ne kadar kimi yazarlar girme fiilinin gerçekleştirilebilmesi için girilmek istenen bilişim sistemine çeşitli tedbir ve uygulamalarla sınırlandırılmış ve korunuyor olması gerektiğini ifade etse³²¹ de biz bu görüşe katılmamaktayız. Sisteme girme fiilinin suç olarak kabul edilebilmesi için hukuki sınırların bulunması; bir başka ifadeyle sistem sahibince sisteme giriş için açık ya da zımni bir şekilde izin verilmemiş olması yeterlidir³²². Nihayetinde hak sahibinin açık ve zımni davranışları ile sisteme izinsiz ve yetkisiz girişlere izin verilmediği anlaşılabiliyorsa suç oluşacaktır³²³. Yargıtay da verdiği kararlarda “*Mağdurun kişisel bilgisayarına ait işletim sistemine bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi*³²⁴” durumda suçun oluşacağını ifade etmiştir. Herkesin erişimine açık ve hukuki olarak dahi sınırlandırılmamış bir sisteme girilmesi suç oluşturmayacaktır³²⁵. AKSSS Açıklayıcı Raporu’nun 47. maddesinde de bu konuya dikkat çekilmiş; sistem sahibi tarafından yetkilendirilen kişilerin sisteme girişleri ile kamuoyunun ücretsiz ve açık erişimine sunulan sistemlere girişlerin haklı giriş olacağı ve suç sayılmayacağı ifade edilmiştir³²⁶.

Herkes açık bir sisteme girilmesi bilişim sistemine girme suçunu oluşturmuyor olsa da bu sistemler içerisindeki belli bölüm ya da verilere erişimin kısıtlanması söz konusu olabilir. Bu halde de her ne kadar sisteme giriş eylemi suç oluşturmayacak

³¹⁹ Tezcan/Erdem/Önok, **a.g.e.** s. 1152. Ekici Şahin/Koruculu, **a.g.e.** s. 600.

³²⁰ Dülger, **Bilişim Suçları** s. 261.

³²¹ “*Her şeyden önce söz konusu bilişim sistemine erişimin bir takım tedbir veya uygulamalarla sınırlandırılmış olması gerekmektedir. Burada sınırlandırmadan kastedilen şey, bilişim sisteminin işleyişinin, ancak işlem yapma yetkisine sahip kişilerce gerçekleştirilmesidir. Böyle bir yetkilendirmeye en bariz örnek, şifrelendirilmiş bilişim sistemleri olarak gösterilebilir ... Erişimi uygun kılacak yetkinin usulüne uygun olarak alınmış olması gerekmektedir.*” Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 960.

³²² Koca/Üzülmöz, **Özel Hükümler** s. 900-901. Akbulut, **Bilişim Alanına Suçlar** s. 132-134.

³²³ Ekici Şahin/Koruculu, **a.g.e.** s. 601. Güler, **a.g.e.** s. 17-18.

³²⁴ Yar. 8. CD, E. 2014/21961, K. 2015/12125, T. 18.02.2015; Yar. 8. CD, E. 2014/29566, K. 2015/13421, T. 11.03.2015 www.lexpera.com.tr (E. T. 12.12.2021)

³²⁵ Tezcan/Erdem/Önok, **a.g.e.** s. 1151. Ekici Şahin/Koruculu, **a.g.e.** s. 601.

³²⁶ Conseil of Europe, **Explanatory Report to the Convention on Cybercrime**, 23.11.2001 <https://rm.coe.int/16800cce5b> (E. T. 15.12.2021)

olsa da sınırlandırılmış bölümlere girildiği takdirde bu suç oluşacaktır³²⁷. Yargılama sırasında kullanıcıların yetkileri araştırılmalı; erişimi yasaklanan sistem bölümüne yahut veriye erişme ihtimalleri değerlendirilerek sonuca varılmalıdır³²⁸. Ayrıca failin bilişim sistemine kendi adına veya başka bir kimse için girmesi arasında suçun oluşması açısından bir fark yoktur³²⁹.

Öncelikle belirtmelidir ki girme eylemi bilişim sistemine fiziki olarak girilmesi değil³³⁰; çalışan sistemin sanal/dijital alanına girilmesi anlamına gelmektedir³³¹. Zaten bilişim sisteminin fiziki yapısına zarar verilmesi durumunda TCK m. 151’de düzenlenen mala zarar verme suçu söz konusu olacaktır³³². Bilişim sistemine nasıl girileceğine yönelik kanunda bir sınırlama öngörülmemiş olup sisteme girilmesi sonucunu doğuran her türlü hareketle bu suç işlenebilmektedir. Fiziki olarak temas edilen sistemi koruyan güvenlik önlemleri çeşitli yazılımlarla devre dışı bırakılarak veya öncesinde öğrenilmiş olan şifreler kullanılarak sisteme doğrudan giriş yapılarak suç işlenebilecektir. Öte yandan uzakta bulunan bir sisteme kablolar yardımıyla veya ağ bağlantılarıyla kablosuz bir şekilde erişilerek suçun işlenebilmesi de mümkündür³³³. Buradan yola çıkılarak doktrinde bu suç “*serbest hareketli suç*”³³⁴ olarak nitelendirilmektedir³³⁵.

Bilişim sistemine girme suçuna ilişkin kanunda bir belirleme ve sınırlama yapılmamış olsa da belli yöntemlerin bilişim korsanlarınca sıkça tercih edildiği görülmektedir. Özellikle maddi çıkarı hedefleyen bilişim korsanlarının diğer suçları işleyebilmeleri için sisteme girmeleri gerektiğinden bilişim sistemine girme suçu ile

³²⁷ Akbulut, **Bilişim Alanında Suçlar** s. 134. Tezcan/Erdem/Önok, **a.g.e.** s. 1153. Ketizmen, **a.g.e.** s. 104.

³²⁸ Kayaer, **a.g.e.** 102. Ketizmen, **a.g.e.** s. 104.

³²⁹ Taşkın, **Bilişim Hukuku Uluslararası Uyuşmazlıklar** s. 336.

³³⁰ Akbulut, **Bilişim Alanında Suçlar** s. 130. Artuk/Gökçen/Yenidünya, **a.g.e.** s. 861. Parlar/Hatipoğlu, **a.g.e.** s. 3743. Gül, **a.g.e.** s. s. 99.

³³¹ Dülger, **Bilişim Suçları** s. 262. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7291. Soyaslan, **Özel Hükümler**, s. 662-663. Parlar/Öztürk, **a.g.e.** s. 27.

³³² Taşkın, **Bilişim Suçları** s. 25. Kayaer, **a.g.e.** s. 102. Apış, **a.g.e.** s. 62. Şahbaz, **a.g.e.** s. 3130.

³³³ Dülger, **Bilişim Suçları** s. 261. Artuk/Gökçen/Yenidünya, **a.g.e.** s. 861. Akbulut, **Bilişim Alanında Suçlar** s. 130. Kurt, **a.g.e.** s. 156. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7292-7293. Ketizmen, **a.g.e.** s. 101. Erdoğan, **a.g.m.** s. 1375. Taşkın, **a.g.e.** s. 26. Gül, **a.g.e.** s. 98. Apış, **a.g.e.** s. 62.

³³⁴ Dülger, **Bilişim Suçları** s. 261. Yaşar/Artuç/Gökcan, **a.g.e.** s. 7294. Özçelik, **a.g.e.** s. 73. Erdoğan, **a.g.m.** s. 1378. Ekici Şahin/Koruculu, **a.g.e.** s. 598.

³³⁵ Koca/Üzülmez’e göre suçun işlenmesi sırasında kullanılacak araçlar hususunda bir sınırlama olmaması suçu serbest hareketli suç yapmamaktadır. Serbest hareketli suçlar, kanunda neticenin gösterildiği fakat fiillerin belirtilmediği suçlardır. Yazarlara göre, bilişim sistemine girme suçunu serbest hareketli suç olarak nitelendiren yazarlar suç konusu fiilin işleniş şekillerini ve fiilin işlenişinde kullanılan araçları birbirine karıştırmaktadır. Koca/Üzülmez, **Özel Hükümler** s. 901-902. Aynı yönde bkz. Çetin, **a.g.e.** s. 9-10.

uygulamada sıkça karşılaşılmaktadır³³⁶. “*Hacking*” olarak isimlendirilen bu eylemler tamamen teknik yöntemler ve virüsler, solucanlar ya da truva atları gibi programlar yardımıyla gerçekleştirilebileceği³³⁷ gibi kullanıcıları yanıltmaya yönelik psikolojik ve manipülatif yöntemlerle de gerçekleştirilebilir³³⁸. Bu kapsamda ilk olarak bilişim korsanlarınca kullanılan zararlı yazılımdan bahsetmek yerinde olacaktır.

Bilişim korsanlarınca en sık kullanılan zararlı yazılımlardan ilki sisteme çeşitli yöntemlerle ardından kendini çoğaltarak bilişim sistemine ve sistemdeki programlara zarar vererek sistemi ve işleyişini bozan virüslerdir. Virüslere göre daha hızlı ve otomatik olarak harekete geçen, sistem üzerinde çok hızlı bir şekilde yayılan, ağ üzerinden sistemdeki verileri başka sistemlere aktaran ve kendi izlerini yok edebilen solucanlar da yine bilişim korsanlarınca sıkça kullanılmaktadır³³⁹. Bunun yanında adını tarihteki Truva Atı Efsanesinden alan³⁴⁰, zararsız bir programın içinde sisteme sızan, kullanıcıdan habersiz olarak arka planda çalışarak başka sistemlere veri aktarabilen ve sistemde yeni ihlaller için arka kapılar açabilen “*truva atı (trojan horse)*” yazılımları da sıkça kullanılmaktadır³⁴¹. Bilişim sistemine girme suçu ve veri güvenliği açısından en büyük tehlikeyi oluşturan yazılımlar ise sisteme sızdıktan sonra sistemdeki donanım ve yazılımların aktivitelerini kaydeden casus yazılımlardır. Bu konuda en sık karşılaşılan örnek ise kullanıcıların klavye aktivitelerini izleyerek kaydeden ve başka bir bilişim sistemine aktaran “*tuş kaydedici (keylogger)*” yazılımlarıdır³⁴². Bunların yanı sıra “*tavşanlar (rabbits)*”, “*bukalemunlar (chamelons)*”, “*mantık bombaları (magic bombs)*”, “*rootkit*” ve “*gizli dinleme (sniffing)*” yazılımları gibi programlar da bilişim korsanları tarafından sıkça kullanılmaktadır³⁴³. Bu tür yazılımları kullanan bilişim koşanları sistemdeki gevşek

³³⁶ Kerr, a.g.e. s. 1606-1607.

³³⁷ Sieber, **Bilişim Suçları**, s. 160.

³³⁸ Jessica Bregant/Robert Bregant, “Cybercrime and Computer Crime”, **The Encyclopedia of Criminology and Criminal Justice**, First Edition, Edited by Jay S. Albanese, John Wiley & Sons Inc., 2014 <https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118517383.wbecj244> (E. T. 15.12.2021) s. 1-2

³³⁹ Elkin Girgenti, “Computer Crimes”, **American Criminal Law Review**, Annual Survey of White Collar Crime, Vol. 55, Issue 4, Fall 2018 s. 922-923. <https://heinonline.org> (E.T. 08.12.2021) s. 917.

³⁴⁰ Aydın, **Bilişim Suçları ve Hukukuna Giriş**, s. 48.

³⁴¹ Basil Cupa, “Trojan Horse Resurrected - On The Legality Of The Use Of Government Spyware”, **Living in Surveillance Societies: The State of Surveillance**, Edit. Webster, C William R. Living, Zurich Open Repository and Archive, University of Zurich, 2013, s. 419-420. https://www.zora.uzh.ch/id/eprint/81157/1/Cupa_Living_in_Surveillance_Societies_2012.pdf (E. T. 04.12.2021)

³⁴² Girgenti, a.g.e. s. 916.

³⁴³ Elbahadır, a.g.e. s. 108 vd.

güvenlik önlemlerinden faydalanarak sisteme girebilecekleri gibi çeşitli vasıtalarla sistemi tarayarak hedef sistemin teknik açıklarını bulup bu açıklardan da sisteme sızabilirler³⁴⁴. “*Tarama(scanning)*” olarak adlandırılan bu eylem, bir ağa bağlı bilişim sistemlerinin ve bunların IP adreslerinin tespiti şeklinde olabileceği gibi şifrelenmiş bir sistemdeki hata ve açıkların tespitine ya da şifrelerin çözülmesine yönelik de olabilir³⁴⁵. Yargıtay kararlarında da bu tür yazılımlar kullanılarak bilişim sistemine girme suçunun işlenebileceği sıklıkla ifade edilmektedir³⁴⁶.

Çeşitli zararlı yazılımlar yoluyla bilişim sistemlerine erişen bilgisayar korsanları sonradan tekrar sisteme erişebilmek için de çalışmalar yapmaktadır. Bu kapsamda Truva atları, virüs ya da solucan gibi yazılımlarla sistemde bırakılan “*arka kapılar (backdoors)*” ve “*gizli kapılar (trap doors)*” aracılığıyla bilişim korsanları istedikleri zaman tekrar sisteme erişebilmektedir³⁴⁷. Bilişim sistemine girme suçunun bırakılan bu arka kapılar sayesinde birden çok kez işlenmesi halinde ise zincirleme suç söz konusu olacaktır³⁴⁸. Failin yararlandığı güvenlik açıklarının anlatılan şekillerde kendisi tarafından oluşturulması ile kendiliğinden var olması arasında suçun oluşması bakımından fark yoktur³⁴⁹.

Bu bölümde bahsedilen yazılımların çalıştırılabilmesi için öncelikle hedef sisteme yüklenebilmesi gerekmektedir. Bu yazılımlar zaman zaman sistemlerin açıklarından faydalanılarak sisteme sızdırılırsalar da bu sızmaların çoğunlukla kullanıcıların manipüle edilerek gerçekleştiği görülmektedir. Bilişim korsanlarının kullanıcıların içlerinde bulunan güvenme eğilimlerini çeşitli hile ve tekniklerle manipüle ederek sisteme ve sistemde bulunan verilere erişmeleri “*sosyal mühendislik yöntemleri*” olarak adlandırılır³⁵⁰. Bu kapsamda bilişim korsanları kendilerini olmadıkları kişiler (müşteri hizmetleri yetkilileri, banka görevlileri gibi) olarak

³⁴⁴ Hamza Elbahadır, **Hacking Interface**, 17. Baskı, İstanbul: Kodlab, 2018 s. 73.

³⁴⁵ Akbulut, **Bilişim Alanında Suçlar** s. 130. Jonathan Clough, **Principles of Cybercrime, Second Edition**, Cambridge: Cambridge University Press, 2015 s. 29.

³⁴⁶ “Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), kötü niyetli yazılımlar, truva atı (trojan horse), macro virüsü, solucanlar vs. kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir.” Yar. 8. CD, E. 2018/1078, K. 2018/2485, T. 08.03.2018 Aynı yönde bkz. Yar. 8. CD, E. 2013/4668, K. 2014/9860, T. 16.04.2014; Yar. 8. CD, E. 2014/29566, K. 2015/13421, T. 11.03.2015; Yar. 8. CD, E. 2016/12839, K. 2017/11114, T. 11.10.2017 www.lexpera.com.tr (E. T. 12.12.2021)

³⁴⁷ Elbahadır, **a.g.e.** s. 228-229.

³⁴⁸ Özçelik, **a.g.e.** s. 66.

³⁴⁹ Ketizmen, **a.g.e.** s. 103. Ekici Şahin/Koruculu, **a.g.e.** s. 598.

³⁵⁰ Katharina Krombholz/Heidelinde Hobel/Markus Huber/Edgar Weippl, “Advanced Social Engineering Attacks”, **Journal Of Information Security And Applications**, Vol. 22, 2015 s. 114.

tanıtılarak kullanıcıların kullandıkları sistemlere dair erişim bilgilerini ve şifrelerini elde etmeye çalışırlar. Bunun yanında özellikle “*oltalama (phishing)*”³⁵¹ tekniğinde olduğu gibi teknik yöntemlerin yardımıyla da sosyal mühendislik yapılabilmektedir³⁵². Burada kişi rutin olarak kullandığı web sitelerinin görünümünün taklit edildiği kötü amaçlı web sitelerine yönlendirilmekte; bu sitelere girerken kullandığı kullanıcı adı ve şifreler ise bilişim korsanlarınca ele geçirilerek söz konusu hesaplara hukuka aykırı olarak erişilmek amacıyla kullanılmaktadır. Burada kimi zaman kullanıcılar kendi ulaştıkları sahte web sitelerinin kurbanı olmakta; kimi zaman ise bilgisayar korsanlarınca “*İstem Dış Alınan E-Postalar (SPAM)*” yoluyla kullanıcılara ulaşılmaktadır³⁵³. Bunun dışında son yıllarda medyada da sıkça görünür olan “*Pegasus*” gibi yazılımlarla hedef sisteme bir bağlantı gönderilerek -sistem sahibinin bağlantıyı görmesine ya da tıklamasına gerek olmaksızın- sisteme ve içerisindeki bilgilere erişilebilmektedir³⁵⁴. Aslında bir bilişim sistemine elektronik posta ya da bir dosya gönderilmesi ve oltalama eylemleri tek başlarına bilişim sistemine girme suçunu değil; TCK m. 244’teki veri gönderme³⁵⁵ suçunu oluşturmaktadır. Bununla birlikte bu yöntemler aracılığıyla gönderilen dosyalar ve kullanıcıyı yanlış yönlendiren bağlantı ve programlar vasıtasıyla bilişim sistemine girme suçunun işlenebilmesi mümkündür³⁵⁶.

Sisteme hukuka aykırı girilmesiyle birlikte suç konusu fiil gerçekleşmiş olacaktır. Bunun dışında sistemde bulunan verilere ulaşılarak bu verilerin okunması ya da görülmesi bu suçun fiil unsurunu oluşturmaz³⁵⁷. Sisteme girildikten sonra şifrenin değiştirilerek sistemin ulaşılmaz kılınması veya sistemdeki verilere zarar verilmesi ya da kopyalanması halinde ise TCK’nın 243/3. ve 244. maddelerinde düzenlenen suçların oluşup oluşmadığı değerlendirilmelidir³⁵⁸. Şayet fail sistemdeki

³⁵¹ Girgenti, **a.g.e.** s. 920.

³⁵² Bregant/Bregant, **a.g.e.** s. 2

³⁵³ Girgenti, **a.g.e.** s. 920.

³⁵⁴ Ajav Chawla, “*Pegasus Spyware—’A Privacy Killer’*”, **Available at SSRN**, 2021, <https://ssrn.com/abstract=3890657> or <http://dx.doi.org/10.2139/ssrn.3890657> (E.T. 12.12.2021)

³⁵⁵ “*Sanıkların ... bir yazılım ile müşterki şirketin bilişim sistemine veri gönderip, seri şekilde milyonlarca sorgu yapıp sistemde var olan verileri aldıkları anlaşıldığından sanıkların eyleminin 5237 sayılı TCK’nun 244/2-4 maddelerinde düzenlenen suçu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde bilişim sistemine girme suçundan mahkumiyetlerine karar verilmesi...*” Yar. 15. CD, E. 2017/14178, K. 2020/4067, T. 01.06.2020 www.lexpera.com.tr (E. T. 12.12.2021)

³⁵⁶ Akbulut, **Bilişim Alanına Suçlar** s. 130-132. Tezcan/Erdem/Önok, **a.g.e.** s. 1153. Mahmutoğlu, **a.g.e.** s. 861. Artuk /Gökçen/Yenidünya, **a.g.e.** s. 861. Yenidünya, **a.g.e.** s. 1033.

³⁵⁷ Akbulut, **Bilişim Alanında Suçlar** s. 129. Dülger, **Bilişim Suçları** s. 264-265. Yıldız, **Bilişim Sistemine Girme** s. 238.

³⁵⁸ Yıldız, **Bilişim Sistemine Girme** s. 240.

verilere zarar verme konusunda taksirle hareket etmişse TCK m. 243/3, kasten hareket etmişse TCK m. 244 uygulanacaktır. Yargıtay da verdiği bir kararda³⁵⁹ bu yönde bir değerlendirme yapılması gerektiğini ifade etmiştir.

Failin bilişim sistemine girdikten sonra sistemde kalmaya devam etmesi iki ayrı suç oluşmasına neden olmayacak; böyle bir durumda tek bir suç oluşacaktır³⁶⁰. Bilişim sistemine girilmesiyle halihazırda suç işlenmiş olduğundan; sistemde kalınmaya devam edilmesinin suçun oluşumu bakımından bir önemi yoktur³⁶¹. Özellikle bilişim korsanlarının sistemlerin güvenlik önlemlerini saf dışı bırakabildiklerini göstermek maksadıyla sisteme girdikten sonra kalmaksızın sistemi terk ettikleri görülmektedir³⁶².

Sistemde kalmaya devam etmek suretiyle suçun işlenmesi ise tamamına veya bir kısmına giren kişinin sistemin soyut alanındaki varlığını sürdürmesi şeklinde meydana gelmektedir³⁶³. Kalma eylemi, hukuka aykırı şekilde girilen sistemde kalmaya devam etmek şeklinde gerçekleşebileceği gibi hukuka aykırı olarak girildiği fark edilmeksizin girilen sistemde durumu fark ettikten sonra sistemden çıkmamak şeklinde de gerçekleşebilmektedir³⁶⁴. Hukuka uygun olarak sisteme giren failin girişini meşru kılacak sebep ortadan kalkmasına veya sistemde kalmasına izin verilen süre dolmasına rağmen sistemi terk etmemesi halinde de yine kalma fiili gerçekleşmiş olacaktır³⁶⁵. Bunun yanı sıra başkası tarafından sisteme sokulan bir kişinin sistemde kalmaya devam etmesi de bu suçun oluşabilmesi için yeterli olacaktır³⁶⁶. Sistemde kalınmasının hukuku aykırı bir nitelik kazandığı anda suç işlenmiştir³⁶⁷. Fail, sistemde kalmaya devam ederek sistemdeki verilere ulaşma ve müdahale etme imkanına sahip olmaktadır³⁶⁸.

³⁵⁹ “*sanığın, katılana ait mail adreslerine girdiğinin tespit edildiği, ancak üçüncü kişilerle yazışma yaptığına dair kayıtlara rastlanmadığının bildirildiği dikkate alındığında, sanığın aksi kanıtlanamayan savunmaları ve tüm dosya kapsamı birlikte değerlendirildiğinde, sanığın, katılana ait iki farklı mail adreslerine izinsiz olarak girme eyleminin sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu değil, TCK’nın 243/1.maddesinde düzenlenen bilişim sistemine girme suçunu oluşturduğu gözetilmeden suçun vasfında yanlışlığa düşülerek yazılı şekilde hüküm kurulması,*” Yar. 12. CD, E. 2015/9555, K. 2016/19731, T. 22.06.2016 www.lexpera.com.tr (E. T. 16.12.2021)

³⁶⁰ Akbulut, **Bilişim Alanında Suçlar** s. 126. Yıldız, **Bilişim Sistemine Girme** s. 238. Bayındır, **a.g.e.** s. 64.

³⁶¹ Koca/Üzülmez, **Özel Hükümler** s. 902.

³⁶² Dülger, **Bilişim Suçları** s. 262.

³⁶³ Akbulut, **Bilişim Alanında Suçlar** s. 136.

³⁶⁴ Koca/Üzülmez, **Özel Hükümler** s. 902. Ergün, **a.g.e.** s. 89.

³⁶⁵ Yıldız, **Bilişim Sistemine Girme** s. 239. Şahbaz, **a.g.e.** s. 3124. Erdağ, **a.g.e.** s. 283. Yılmaz, **a.g.e.** s. 239.

³⁶⁶ Tezcan/Erdem/Önok, **a.g.e.** s. 1153. Kayaer, **a.g.e.** s. 103. Kabadayı, **a.g.e.** s. 82.

³⁶⁷ Artuk/Gökçen/Yenidünya, **a.g.e.** s. 862. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7292.

³⁶⁸ Yıldız, **Bilişim Sistemine Girme** s. 239.

Sistemde kalmaya devam etme fiili, failin sistemden tamamen çıkış yaptığı ana kadar işlenmeye devam edecek olup bu yönüyle kesintisiz (mütemadi³⁶⁹) bir suçtur³⁷⁰. Suça ilişkin zamanaşımı ve suçun işlendiği yer gibi hususların belirlenmesi sırasında da fiilin bu özelliğinin göz önünde bulundurulması gerekmektedir³⁷¹. Bunun yanında failin sistemde kaldığı saptandıktan sonra kalma eyleminin ne kadar sürdüğünün suçun varlığı açısından bir önemi yoktur. Ancak girişin ardından daha uzun süre kalınması daha fazla zarar meydana getireceği için verilecek cezanın belirlenmesi sırasında TCK'nın 61. maddesi kapsamında dikkate alınacaktır³⁷².

5. Netice

Hukuk düzenini bozan ve suçun oluşmasına sebep olan hareket kimi zaman dış dünyada görülebilecek bir değişikliğe sebep olmakta; bu değişiklik ise netice olarak ifade edilmektedir. Bir başka ifadeyle netice ilgili ceza normları açısından önem arz eden ve fiil sonucu meydana getirilen ya da engel olunmayarak sebep olunan dış dünyadaki değişimdir³⁷³. Bazı durumlarda ise fiil dış dünyada gözlenebilecek bir değişiklik ve zarara sebep olmamaktadır. Bu nedenle ceza kanunları kimi zaman failin cezalandırılabilmesi için dış dünyada bir zararın ya da değişikliğin meydana gelmesini aramaksızın sadece fiilin gerçekleşmesini yeterli görmektedir. Bu şekilde düzenlenen suçlar doktrinde neticesiz suç, şekli suç³⁷⁴, neticesi harekete bitişik suç³⁷⁵ ya da sırf hareket suçu³⁷⁶ olarak adlandırılmaktadır³⁷⁷.

TCK m. 243'teki suçun işlenmiş olması için sistemin bir bölümüne ya da tamamına hukuka aykırı şekilde girmek ya da kalmak yeterli olup bundan başka bir zararın veya neticenin meydana gelmesi aranmamaktadır. Suçu işleyen failin kanunda

³⁶⁹ Kesintisiz(mütemadi) suçlar ve bunların hüküm ve sonuçlarıyla ilgili ayrıntılı bilgi için bkz. Tuğrul Katoğlu, **Kesintisiz Suç (Mütemadi Suç)**, Ankara: Seçkin Yayınları, 2022

³⁷⁰ Yaşar/Artuç/Gökcan, **a.g.e.** s. 7292. Yıldız, **Bilişim Sistemine Girme** s. 239. Kabadayı, **a.g.e.** s. 81.

³⁷¹ Dülger, **Bilişim Suçları** s. 265. Tezcan/Erdem/Önok, **a.g.e.** s. 1150. Ekici Şahin/Koruculu, **a.g.e.** s. 601. Karagülmez, **a.g.e.** s. 206.

³⁷² Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 961. Soyaslan, **Özel Hükümler**, s. 662. Kayaer, **a.g.e.** s. 104.

³⁷³ Dönmezer/Erman, **a.g.e.**, s. 97. Koca/Üzülmez, **Genel Hükümler** s. 115. 129. Dülger, **Genel Hükümler** s. 307.

³⁷⁴ Demirbaş, **a.g.e.** s. 257. Yaprak Öntan, **Ceza Hukukunda Davranış ve Netice**, Ankara: Seçkin Yayıncılık, 2021 s. 290.

³⁷⁵ “104-Kanaatimizce her suçta bir netice vardır, bu netice bazen hareketten ayrıdır, bazen ise harekete bitişiktir. Esasen suçun hukuki konusunu teşkil eden hak ve menfaatin ihlali başlı başına bir neticedir ve böyle bir ihlal bulunmadıkça suçun varlığından söz edilemez.” Dönmezer/Erman, **a.g.e.**, s. 101.

³⁷⁶ Koca/Üzülmez, **Genel Hükümler** s. 129. Akbulut, **Genel Hükümler** s. 354.

³⁷⁷ Dönmezer/Erman, **a.g.e.**, s. 99. Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 228.

verilen seçimlik hareketlerden en az birini yapması suçun oluşumu için yeterli olacaktır³⁷⁸. Bu yönüyle bilişim sistemine girme suçu doktrinde “*sırf hareket suçu*³⁷⁹” ve “*neticesi harekete bitişik suç*³⁸⁰” olarak nitelendirilmiştir. TCK 243. maddenin gerekçesinde de bu durum “*Sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir.*” şeklinde ifade edilerek suçun oluşması için ayrıca bir neticeye gerek olmadığı vurgulanmıştır.

Suçun konusunun zarar görmesi veya tehlikeye düşmesi bakımından doktrinde ikili bir ayrım yapılmaktadır. Haksızlık oluşturan eylem sonucunda suçun konusunun zarar görmesi halinde “*zarar suçu*”; suçun konusunu tehdit eden bir tehlikenin ortaya çıkması halinde ise “*tehlike suçu*” söz konusu olacaktır. Şayet suç konusu eylem suçun konusu üzerinde somut ve gerçek bir tehlike oluşturuyorsa “*somut tehlike suçu*”; kanunda hareketin icra edilmesiyle tehlikenin oluşacağı öngörülüyor ise “*soyut tehlike suçu*” oluşacaktır³⁸¹.

Bilişim sistemine girme suçunun işlenmiş olması için bir zararın ortaya çıkması ya da somut ve gerçek bir tehlikenin gerçekleşmesi aranmamıştır. Halihazırda suça konu eylemlerin en az birinin gerçekleşmesi ile birlikte, suçla korunmak istenen menfaat olan bilişim sistemlerinin güvenliği tehlikeye düşecektir. Bu durum da bilişim sistemine girme suçunun bir “*soyut tehlike suçu*” olduğunu göstermektedir³⁸².

İncelemekte olduğumuz suçun işlenebilmesi için ayrıca failin kendisine ya da bir başka kişiye herhangi bir yarar sağlamış olması zorunluluğu yoktur³⁸³. Buna rağmen suçun işlenmesiyle gerçek ve tüzel kişilere çeşitli menfaatler temin edilmesi de mümkündür³⁸⁴. Suçtan lehine menfaat temin edilen bir tüzel kişi söz konusu olduğunda

³⁷⁸ Dülger, **Bilişim Suçları** s. 265. Yıldız, **Bilişim Sistemine Girme** s. 241. İhtiyaroğlu, **a.g.e.** s. 422. Taşdemir, **a.g.e.** s. 23. Sinan Esen, **Anlatımlı ve İçtihatlı Malvarlığına Karşı Suçlar, Belgede Sahtecilik ve Bilişim Alanında Suçlar**, Ankara: Adalet Yayınevi, 2007 s. 629.

³⁷⁹ Akbulut, **Bilişim Alanında Suçlar** s. 128. Dülger, **Bilişim Suçları** s. 265. Koca/Üzülmüş, **Özel Hükümler** s. 901-902. Tezcan/Erdem/Önok, **a.g.e.** s. 1153. Karagülmez, **a.g.e.** s. 205-206.

³⁸⁰ Soyaslan, **Özel Hükümler**, s. 663. Kayaer, **a.g.e.** s. 103. Taşkın, **a.g.e.** s. 26. Yenidünya, **a.g.e.** s.1035. Demircan, **a.g.e.** s. 89.

³⁸¹ Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 130-131. Özgenç, **a.g.e.** s. 221. Dülger, **Genel Hükümler** s. 309-311.

³⁸² Dülger, **Bilişim Suçları** s. 266. Koca/Üzülmüş, **Özel Hükümler** s. 901. Tezcan/Erdem/Önok, **a.g.e.** s. 1153.-1154. Taşkın, **a.g.e.** s. 26. Karakehya, **a.g.e.** s. 13. Kurt, **a.g.e.** s. 153. Doğan **Bilişim Suçları ve Türk Ceza Kanunu**. s.295. Tepe, **a.g.e.** s. 279-280. Güler, **a.g.e.** s. 20. Parlar/Öztürk, **a.g.e.** s. 27-28.

³⁸³ Ekici Şahin/Koruculu, **a.g.e.** s. 600.

³⁸⁴ Soyaslan, **Özel Hükümler**, s. 663. Mahmutoglu, **a.g.e.** s. 859.

TCK m. 246. gereğince bu tüzel kişiler hakkında kanunda öngörülen güvenlik tedbirlerine hükmedilebilecektir³⁸⁵.

Bu başlık altında belirtilmesi gereken son nokta ise yukarıda yapılan açıklamaların 243. maddenin üçüncü fıkrası için geçerli olmadığıdır. Zira anılan maddede suçun işlenmesi sırasında sistemdeki verilerin değişmesi ya da yok olması halinde suçun basit halinde göre daha ağır bir ceza verileceği düzenlenmiştir³⁸⁶. Burada sadece kanun koyucunun üçüncü fıkra özelinde bir netice aradığına değinilmekle yetinilecek olup gerekli açıklamalar konu bütünlüğünün korunması amacıyla ilgili bölümde yapılacaktır.

6. Teşebbüs

TCK'nın 35. maddesine göre suç işleme kastıyla hareket eden failin elverişli hareketlerle suçun icrasına başlamasına rağmen elinde olmayan nedenlerle suçu tamamlayamadığı durumlarda teşebbüs nedeniyle sorumluluğu söz konusu olacaktır³⁸⁷.

Doktrinde teşebbüs değerlendirilirken seçimlik hareketlere göre ayırım yapılmakta ve bilişim sistemine girme fiili bakımından teşebbüsün mümkün olduğu ifade edilmektedir. Failin bir başkasına ait sisteme hukuka aykırı olarak ve kasten girmeye çalışmasına rağmen elinde olmayan sebeplerle hareketini tamamlayamadığı durumlarda teşebbüs söz konusu olacaktır³⁸⁸. Örneğin bir sisteme girmeye çalışan failin sistemdeki güvenlik yazılımları nedeniyle bu eyleminde başarısız olması durumunda suç teşebbüs aşamasında kalacaktır³⁸⁹. Yargıtay da verdiği bir kararda katılanın sosyal medya hesabının şifresini ele geçirmeye çalışan sanık hakkında teşebbüs hükümlerinin uygulanıp uygulanmayacağına tartışılmamasını bozma nedeni olarak kabul etmiştir³⁹⁰. Teşebbüs maddenin birinci fıkrasında düzenlenen suçun basit

³⁸⁵ Kayaer, **a.g.e.** s. 106. Karagülmez, **a.g.e.** s. 184.

³⁸⁶ Dülger, **Bilişim Suçları** s. 266.

³⁸⁷ Koca/Üzülmez, **Genel Hükümler** s. 414. Demirbaş, **a.g.e.** s. 488. Akbulut, **Genel Hükümler** s. 702. Dülger, **Genel Hükümler** s. 651. Artuk/Gökçen/Alşahin/Çakır, **a.g.e.** s. 673-675.

³⁸⁸ Dülger, **Bilişim Suçları** s. 300. Koca/Üzülmez, **Özel Hükümler** s. 905-906. Tezcan/Erdem/Önok, **a.g.e.** s. 1160. Soyaslan, **Özel Hükümler**, s. 664. Güler, **a.g.e.** s. 31-32. Çetin, **a.g.e.** s.19.

³⁸⁹ Akbulut, **Bilişim Alanında Suçlar**, s. 150. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 965. Yıldız, **Bilişim Sistemine Girme** s. 242. Ekici Şahin/Koruculu, **a.g.e.** s. 618. Esen, **a.g.e.** s. 631. Kayaer, **a.g.e.** s. 117.

³⁹⁰ "...bilirkişi raporu içeriğinden, her ne kadar katılanın hesabına erişimi bir süre engellenmiş ise de henüz şifreyi tespit edemediğinden hesaba giremediği, katılanın müdahalesi sonucu girişiminin

hali açısından mümkün olduğu gibi, ikinci fıkradaki daha az cezayı gerektiren hal bakımından da mümkündür³⁹¹.

Özellikle bilişim sistemlerine uzaktan zararlı yazılım gönderilmesi durumunda teşebbüsün oluşup oluşmayacağı konusunda doktrindeki tartışmaya da değinmek gerekmektedir. Bilişim sisteminin sahibinin dikkati sayesinde yahut sistemdeki güvenlik yazılımları marifetiyle e-posta ya da başka bir yolla sisteme gönderilen zararlı yazılımlar daha çalışmaya başlamadan tespit edilerek etkisiz hale getirilebilmektedir. Bu durumda kimi yazarlar teşebbüsün mümkün olamayacağını ifade etmektedir³⁹². Bazı yazarlar ise zararlı yazılımın gönderilmesi ile birlikte halihazırda suçun icrasına başlanmış olduğunu ifade ederek; failin elinde olmayan sebeplerle zararlı yazılımın etkisiz hale getirilmesinden dolayı bu halde teşebbüsün olabileceğini savunmuşlardır³⁹³.

Hukuka aykırı bir şekilde sisteme giren failin sistemde kalma eyleminin yarıda kalması halinde ise teşebbüs hükümleri uygulanmayacaktır. Zira halihazırda girme seçimlik hareketi başarılı bir şekilde icra edildiğinden suç oluşmuştur³⁹⁴.

İncelemekte olduğumuz suçun ikinci seçimlik hareketi olan kalmaya devam etme fiili açısından ise teşebbüsün mümkün olmadığı ifade edilmektedir³⁹⁵. Suçun kanuni tanımında kalma eyleminin süresine ilişkin bir alt sınır getirmediği için birkaç saniyeliğine sistemde kalınması halinde dahi fiil gerçekleşmiş olacaktır³⁹⁶. Yine ihmali hareketle sistemde kalınması halinde de suç oluşmuş olacaktır. Örneğin sistem sahibinin rızası ile sisteme giren fail, sistemden çıkması istenilmesine rağmen sistemde kalmaya devam ediyorsa bu durumda halihazırda suç tamamlandığından teşebbüsten söz edilemeyecektir³⁹⁷.

sonuçlanamaması ve bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kalma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme eylemlerinin gerçekleşmediğinin anlaşılması karşısında, sanığın eyleminin bilişim sistemine girmeye teşebbüs suçunu oluşturup oluşturmayacağını karar yerinde tartışılmaması” Yar. 8. CD, E. 2016/11922, K. 2017/6655, T. 07.06.2017 www.lexpera.com.tr (E. T. 19.12.2021)

³⁹¹ Akbulut, **Bilişim Alanında Suçlar**, s. 151.

³⁹² Mahmutoglu, **a.g.e.** s. 861.

³⁹³ Erdoğan, **a.g.m.** s. 1415. Özçelik, **a.g.e.** s. 120.

³⁹⁴ Dülger, **Bilişim Suçları** s. 300.

³⁹⁵ Tezcan/Erdem/Önok, **a.g.e.** s. 1160. Ekici Şahin/Koruculu, **a.g.e.** s. 618. Kayaer, **a.g.e.** s. 118. Güler, **a.g.e.** s. 32. Kabadayı, **a.g.e.** s. 99. Aksi yöndeki görüş için bkz. Gül, **a.g.e.** s. 111.

³⁹⁶ Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 965.

³⁹⁷ Akbulut, **Bilişim Alanında Suçlar**, s. 151.. Koca/Üzülmöz, **Özel Hükümler** s. 906. Dülger, **Bilişim Suçları** s. 300-301.

Suçun neticesi sebebiyle ağırlaşan hali için de teşebbüsün mümkün olmadığı doktrinde ifade edilmiştir³⁹⁸. Zira maddenin üçüncü fıkrasında netice girme eyleminin sonucu olarak öngörülmüştür. Şu hâlde girme eyleminin teşebbüs halinde kalması durumunda neticenin gerçekleşmeyeceği açıktır. TCK m. 243/3'te düzenlenen suçta netice bakımından taksirle hareket etmek gerekmektedir. Taksirli suça teşebbüsün de mümkün olmayacağı göz önüne alındığında bilişim sistemine girme suçunun neticesi sebebiyle ağırlaşmış haline teşebbüs mümkün değildir³⁹⁹.

Kimi yazarlar ise incelemekte olduğumuz suçun bir tehlike suçu olmasından yola çıkarak girme ve kalma fiillerinin gerçekleşmesi ile suçun halihazırda oluşacağını ve bu suça teşebbüsün mümkün olmadığını ifade etmişlerdir⁴⁰⁰. Doktrinde destek bulmayan bu görüşe biz de katılmamaktayız.

Teşebbüsün mümkün olduğu hallerde icra hareketlerine başlamış failin bu hareketler tamamlanmadan suçu işlenmekten vazgeçmesi halinde ise gönüllü vazgeçmeye ilişkin TCK m. 36 hükümleri uygulanacaktır. Bu halde fail teşebbüs ettiği suçtan dolayı cezalandırılmayacak, sadece o zamana kadar işlediği fiilden dolayı cezalandırılacaktır⁴⁰¹. Bu kapsamda örneğin mağdura ait bilişim sistemine giriş bilgilerini elde etmesine rağmen sisteme girme eylemini icradan kaçınan fail hakkında da bilişim sistemine girme suçuna teşebbüsten dolayı ceza verilmeyecektir⁴⁰². Bunun yanında mağdurun sosyal medya hesabı ya da e-posta adresinin şifresini öğrenmiş olmasına rağmen bilişim sistemine girme suçunun icrasına başlamamış faile TCK m. 136'da düzenlenen kişisel verilerin ele geçirilmesi suçu gereğince ceza verilmesi gerekmektedir⁴⁰³.

B. Manevi Unsur

Bir hareketin ceza hukuku kapsamında cezalandırılabilmesi için hukuka aykırı fiilin bazı manevi nitelikleri de bünyesinde barındırması gerekmektedir⁴⁰⁴. Bu kapsamda fail ile işlediği fiil arasında bir manevi bağın bulunması gerekmekte; bu bağ

³⁹⁸ /Doğan/Bacaksız, **Özel Hükümler** s. 965. Ekici Şahin/Koruculu, **a.g.e.** s. 618. Güler, **a.g.e.** s. 32.

³⁹⁹ Akbulut, **Bilişim Alanında Suçlar**, s. 151. Kayaer, **a.g.e.** s. 118.

⁴⁰⁰ Yılmaz, **a.g.e.** s. 190.

⁴⁰¹ Koca/Üzülmez, **Genel Hükümler** s. 437-438. Dülger, **Genel Hükümler** s. 680-681. Yıldız, **Bilişim Sistemine Girme** s. 243. Kayaer, **a.g.e.** s. 117-118. İhtiyaroğlu, **a.g.e.** s. 430.

⁴⁰² Taşkın, **a.g.e.** s. 30.

⁴⁰³ Özçelik, **a.g.e.** s. 119.

⁴⁰⁴ Dönmezer/Erman, **a.g.e.**, s. 444.

ise suçun manevi unsurunu oluşturmaktadır. Bu manevi bağın bulunmaması halinde suçun varlığında söz edilemeyecektir⁴⁰⁵. Fail ile işlediği fiil arasında manevi bağ kast, olası kast ya da taksir olarak ortaya çıkmaktadır⁴⁰⁶.

TCK m. 21'e göre suçun kasten işlenebilmesi için failin suç konusu fiili ve yasal tanımındaki unsurlarını bilerek ve isteyerek gerçekleştirmesi gerekmektedir⁴⁰⁷. Kanundaki bilme ifadesi kastın “*düşünme ve öğrenme*” unsurunu, isteme ifadesi ise “*irade*” unsurunu oluşturmaktadır⁴⁰⁸. Failin suça konu fiilin sonuçlarını öngörmesine rağmen eylemi gerçekleştirmesi durumunda ise “*olası kast*” söz konusu olacaktır⁴⁰⁹. Olası kast söz konusu olduğunda failin neticenin gerçekleşmesinin istemesinin bir önemi yoktur çünkü bu durum fail tarafından görmezden gelinmektedir⁴¹⁰. “*Doğrudan kast*” söz konusu olduğunda ise kastın bilme unsuru ağırlık kazanmakta; fail neticenin gerçekleşeceğini kesin olarak bilmekte veya öngörmektedir⁴¹¹.

Bilişim sistemine girme suçu kasten işlenebilmektedir. Fail, suç konusu bilişim sistemine hukuka aykırı olarak girdiğini veya kalmaya devam ettiğini bilmeli⁴¹² ve bu eylemlerini sürdürmek istemelidir⁴¹³. Madde metninde failin amacına işaret eden bir ifade bulunmadığından suçun ortaya çıkması için genel kast yeterlidir⁴¹⁴. Kanunda suçun taksirle işlenebileceğine yönelik bir düzenleme olmadığından suçun taksirle işlenebilmesi mümkün değildir⁴¹⁵. Eğer ki fail yeterli dikkat ve özeni göstermemesi sonucunda istemeden sisteme girmişse burada suç oluşmayacaktır⁴¹⁶. Yalnızca taksirli bir hareketle sisteme istemeden girilmesi ile suç oluşmayacak; failin sistemde olduğunu fark ettikten sonra da bilerek sistemde kalmaya devam etmesi halinde ise suç oluşacaktır⁴¹⁷. Kimi yazarlara göre hataen sisteme giren failin sistemde olduğunu

⁴⁰⁵ Artuk/Gökçen/Alşahin/Çakır, **a.g.e.** s. 384. Akbulut, **Genel Hükümler** s. 433. Dülger, **Genel Hükümler** s. 388.

⁴⁰⁶ Koca/Üzülmez, **Genel Hükümler** s. 146. Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 255.

⁴⁰⁷ Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 156.

⁴⁰⁸ Dönmezer/Erman, **a.g.e.**, s. 464. Demirbaş, **a.g.e.** s. 389.

⁴⁰⁹ Dülger, **Genel Hükümler** s. 413. Özgeç, **a.g.e.** s. 244.

⁴¹⁰ Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 262.

⁴¹¹ Koca/Üzülmez, **Genel Hükümler** s. 170.

⁴¹² Koca/Üzülmez, **Özel Hükümler** s. 902 Tezcan/Erdem/Önok, **a.g.e.** s. 1155. Güler, **a.g.e.** s. 26.

⁴¹³ Dülger, **Bilişim Suçları** s. 280. Yıldız, **Bilişim Sistemine Girme** s. 243. Artuk/Gökçen/Yenidünya, **a.g.e.** s. 875. Erdoğan, **a.g.m.** s. 1405. Gül, **a.g.e.** s.104. Çetin, **a.g.e.** s. 11.

⁴¹⁴ Tezcan/Erdem/Önok, **a.g.e.** s. 1155. Apaydın, **a.g.m.** s. 276. Yenidünya, **a.g.e.** s. 1037. Parlar/Öztürk, **a.g.e.** s. 28.

⁴¹⁵ Dülger, **Bilişim Suçları** s. 277. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 965 Apaydın, **a.g.m.** s. 276. Karagülmez, **a.g.e.** s. 208. Karakehya, **a.g.e.** s. 15.

⁴¹⁶ Yıldız, **Bilişim Sistemine Girme** s. 245.

⁴¹⁷ Akbulut, **Bilişim Alanında Suçlar** s. 139. Koca/Üzülmez, **Özel Hükümler** s. 902. Ekici Şahin/Koruculu, **a.g.e.** s. 608. Taşdemir, **a.g.e.** s. 260.

fark etmesine rağmen teknik zorluklar sebebiyle sistemden çıkamayıp kalmaya devam etmesi halinde söz konusu fiil taksirle işlenmiş olacağından TCK m. 243 gereği cezalandırılmayacaktır⁴¹⁸.

TCK m. 30/1’de suçun icrası sırasında suçun kanuni tanımındaki maddi unsurları bilmeyen failin kasten hareket etmiş sayılamayacağı düzenlenmiştir. Fiili ya da hukuki bir hata sonucu suç işleyen failin kasten hareket ettiği söylenemeyecektir⁴¹⁹. Bilişim sistemine girme fiilinin hata sonucu gerçekleşmesi halinde de TCK m. 30’da düzenlenen hataya ilişkin hükümler uygulanacaktır⁴²⁰. Örneğin aynı renk ve moldeldeki kendi bilgisayarını zannederek bir başkasına ait bilgisayarını açan fail fiili hataya düşmüş olacaktır. İnsanların ortak kullanımına ait bir bilgisayarda kayıtlı bir şifre ile fark etmeden bir başkasının e-posta hesabına giren fail için de yine hata söz konusu olacaktır. Bu durumlarda failde kastın varlığından söz edilemeyeceğinden TCK m. 243’te düzenlenen bilişim sistemine girme suçu oluşmayacaktır⁴²¹.

Aynı maddenin ikinci fıkrasında ise suçun nitelikli hallerinin gerçekleştiği hususunda hataya düşen failin hatasından yararlanacağı düzenlenmiştir⁴²². Somut olayda cezada indirim yapılmasını gerektiren nitelikli hal bulunmamasına rağmen, bu halin varlığı zannıyla hareket eden faile ceza verilirken nitelikli halin gerektirdiği indirim uygulanacaktır⁴²³. Örneğin girdiği bilişim sisteminin bedeli karşılığı yararlanılabilen bir sistem olduğunu düşünerek suç işleyen faile verilecek ceza TCK m. 30/2. ve m. 243/2 gereğince yarı oranında indirilecektir. Mevcut olan hafifletici nedenin varlığını bilmeyen fail de hatasından yararlanacaktır⁴²⁴. Bir başkasına ait özel bir sisteme girdiğini düşünmesine rağmen bedeli karşılığı yararlanılabilen bir sisteme girmiş olan faile verilecek cezaya da indirim uygulanacaktır.

AKSSS’nin yetkisiz erişim suçu düzenleyen ikinci maddesi ile imzacı devletlere suçu verilerin elde edilmesi veya başka sahtekâr bir amaçla işlenmesi şartına

⁴¹⁸ Bıçkın, **a.g.e.** s. 153. Demircan, **a.g.e.** s. 76-77.

⁴¹⁹ Veli Özer Özbek, “*Türk Ceza Hukukunda Hata(m.30)*”, **Ceza Hukuku Dergisi**, C. 3, S. 7, Ağustos 2008 s. 86. Ahu Karakurt, “*Türk Ceza Kanunu’nda Hata*”, **Ceza Hukuku Dergisi**, C. 4, S. 10, Ağustos 2009 s. 115. Koca/Üzülmez, **Genel Hükümler** s. 255.

⁴²⁰ Akbulut, **Bilişim Alanında Suçlar** s. 139.

⁴²¹ Hafızoğulları/Özen, **Topluma Karşı Suçlar** s. 448. Ekici Şahin/Koruculu, **a.g.e.** s. 613-614. Kabadayı, **a.g.e.** s. 90.

⁴²² Karakurt, **a.g.e.** s.122. Koca/Üzülmez, **Genel Hükümler** s. 263.

⁴²³ Dönmezer/Erman, **a.g.e.** s. 565. Özbek, **a.g.e.** s. 88.

⁴²⁴ Dönmezer/Erman, **a.g.e.** s. 565. Özbek, **a.g.e.** s. 88. Koca/Üzülmez, **Genel Hükümler** s. 264.

bağlı tutabilecekleri düzenlenmiştir. Kimi ülke mevzuatlarında bu tarz sınırlayıcı düzenlemeler yapılmış olmasına rağmen⁴²⁵ TCK'nın 243. maddesi incelendiğinde kanun koyucunun böyle bir sınırlama getirmeyi tercih etmeyerek failin amacına yönelik bir kriter getirmediği görülecektir⁴²⁶. Fail sisteme e lenmek i in ya da kendi becerisini sınamak amacıyla girebilece i gibi hukuka aykırı menfaatler ya da sistemde bulunan verileri temin etmek maksadıyla da girebilecektir. Failin amacının su un olu umu a ısından bir  nemi bulunmamaktadır⁴²⁷.

Failin su  konusu eylemi  zel bir ama la icra etmesine gerek olmadı ından yola  ıkan kimi yazarlar incelemekte oldu umuz su un olası kast ile de i lenebilece ini ifade etmi lerdir⁴²⁸. Bu yazarlara g re madde metninde do rudan kasta g nderme yapan bir ifade bulunmadı ından su un olası kastla i lenmesi  n nde de bir engel yoktur⁴²⁹. Bizim de katıldı ımız g r  e g re ise bu su  sadece do rudan kast ile i lenebilmektedir⁴³⁰. Zira kanun koyucu madde metninde a ık a fiilin “*hukuka aykırı olarak*” icra edilmesini aramı  olup failin sisteme girdi i veya kalmaya devam etti i sırada bu bilince sahip olması gerekmektedir⁴³¹. Ayrıca yine madde metninde ge en ve su un se imlik hareketlerinden biri olan “*sistemde kalmaya devam etme*” eyleminin kanuna eklenme gerek esinden de su un ancak do rudan kastla i lenebilece i anlaşılmaktadır⁴³².

Failin kusurlulu unu ortadan kaldıran hallerden birinin mevcut olması halinde ise failin kınanabilirli i ve kusuru s z konusu olmadı ı i in su  i lenmi  olsa da faile ceza verilmeyecektir⁴³³.  rne in tehdit altındayken su  konusu fiili i leyen ve sisteme hukuka aykırı olarak giren bir bili im uzmanının cezalandırılması s z konusu olmayacaktır⁴³⁴. Yine kusurlulu u etkileyen hallerin de bili im sistemine girme su u

⁴²⁵ Yenid nya, **a.g.e.** s. 1038. Erdo an, **a.g.m.** s. 1407.

⁴²⁶ Akbulut, **Bili im Alanında Su lar** s. 139.

⁴²⁷ Yenid nya/De irmenci, **a.g.e.** s. 75-76. Erdo an, **a.g.m.** s. 1405. Akarslan, **a.g.e.** s. 44-45. O uzhan  mer Demir/Mehmet Arı /Halil Polat, **Bili im Su ları ve Bili im Yoluyla I lenen Su lar Soru turma ve Kovu turma Y ntemleri**, Ankara: Adalet Yayınevi, 2015 s. 5.

⁴²⁸  zbek/Do an/Bacaksız, ** zel H k mler** s. 964-965. Apaydın, **a.g.m.** s. 276. Mahmutog lu, **a.g.e.** s. 862. Do an, **a.g.e.** s. 297.

⁴²⁹ Yenid nya, **a.g.e.** s. 1037.

⁴³⁰ Akbulut, **Bili im Alanında Su lar** s. 139. Yıldız, **Bili im Sistemine Girme** s. 244. Artuk/G k en/Yenid nya, **a.g.e.** s. 867.  z elik, **a.g.e.** s. 77. Erdo an, **a.g.m.** s. 1405-1406. Ekici  ahin/Koruculu, **a.g.e.** s. 608.

⁴³¹ Akbulut, **Bili im Alanında Su lar** s. 139. Kayaer, **a.g.e.** s. 116. Mehmet Burak Kızıltan, **5237 Sayılı T rk Ceza Kanununda Bili im Sistemine Girme, Sistemi Engelleme ve Bozma Su ları**, İstanbul  niversitesi Sosyal Bilimler Enstit s , Y ksek Lisans Tezi, 2007 s. 68.

⁴³² Koca/ z lmez, ** zel H k mler** s. 903. Erdo an, **a.g.m.** s. 1405-1406.

⁴³³ Karakehya'ya g re ise bu durumda su  olu mayacaktır. Karakehya, **a.g.e.** s. 15.

⁴³⁴ Apaydın, **a.g.m.** s. 278. G ler, **a.g.e.** s. 26.

bakımından söz konusu olması mümkündür. Burada kusurluluğu etkileyen hallerden haksız tahrik ve zorunluluk haline ayrıca değinilmesi yerinde olacaktır.

Haksız tahrik, kendisine karşı gerçekleştirilen haksız fiilin doğurduğu öfke ve elemle hareket eden bir kimsenin kendisine karşı haksız fiili icra eden kimseye karşı suç işlemesidir. TCK m. 29'a göre haksız tahrik altında suç işleyen faile verilecek cezada indirimle gidilecektir⁴³⁵. Kendisine karşı icra edilen haksız fiil nedeniyle öfke ve üzüntü etkisinde kalan failin işlediği suç ile bu duygular arasında bir illiyet bağı olmalıdır⁴³⁶. Bir başka ifadeyle failin tahrik edilmemiş olması durumunda bu suçun işlemeyecek olması gerekecektir⁴³⁷. Bilişim sistemine girme suçu bakımından haksız tahrik indirimi uygulanmasının önünde bir engel bulunmamaktadır⁴³⁸. Örneğin kendisine ya da bir yakınına ait özel nitelikte görüntü veya yazışmaların yayınlandığı bir sosyal medya hesabının şifresini kırarak bu hesaba hukuka aykırı olarak giren fail bakımından haksız tahrikin varlığından söz edilebilecektir. Zira fail yayınlanan görüntüler sebebiyle duyduğu üzüntü ve öfkenin etkisiyle bir başkasına ait bilişim sistemine girme eylemini icra etmiştir.

Kendisine yahut bir üçüncü kişiye yönelik kendisinin sebep olmadığı ağır ve muhakkak bir tehlikeyi ancak kanunun suç olarak kabul ettiği ve tehlikenin ağırlığı ile orantılı bir fiil ile bertaraf edebilen fail bakımından zorunluluk hali söz konusu olacaktır⁴³⁹. TCK m. 25/2'ye göre zorunluluk hali çerçevesinde suç işleyen fail bu fiili sebebiyle cezalandırılmayacaktır. Bununla birlikte tehlikeden bir başka kimsenin hakkına zarar verilmeden de korunmak mümkün ise zorunluluk halinden söz edilemeyecektir⁴⁴⁰. Bilişim sistemine girme suçu bakımından da bu zorunluluk hali ile ilgili ayrı bir durum bulunmamaktadır. Mevcut tehlikeyi engellemenin başka bir yolu bulunmaması halinde fail işlediği bilişim sistemine girme suçu için cezalandırılmayacaktır. Örneğin yangın çıkan bir binada başkasına ait akıllı telefonu yardım çağırmak için kullanan failin eylemi zorunluluk hali kapsamında

⁴³⁵ Dönmezer/Erman, **a.g.e.** s. 591. Timur Demirbaş, **Haksız Tahrik, Güncellenmiş ve Genişletilmiş 3. Baskı**, Ankara: Seçkin Yayınları, 2021 s. 22. Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 418.

⁴³⁶ Dönmezer/Erman, **a.g.e.** s. 616-618. Zeynel T. Kangal, "Türk Ceza Hukukunda Haksız Tahrik", **Erzincan Üniversitesi Hukuk Fakültesi Dergisi**, C. XIV, S. 3-4, 2010 s. 47.

⁴³⁷ Demirbaş, **a.g.e.** s.87.

⁴³⁸ Özçelik, **a.g.e.** s. 115.

⁴³⁹ Dönmezer/Erman, **a.g.e.** s. 359. Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 391. Hakan Hakeri, **Ceza Hukuku Genel Hükümler, 22. Baskı**, Ankara: Adalet Yayınevi, 2019 s. 405.

⁴⁴⁰ Dönmezer/Erman, **a.g.e.** s. 374-375. Selahattin Samet Bilge, "Türk Ceza Hukukunda Zorunluluk Hali", **Başkent Üniversitesi Hukuk Fakültesi Dergisi**, C. 7, S. 2, 2017 s. 380.

değerlendirileceğinden faile ceza verilmeyecektir⁴⁴¹. Kendine ya da bir yakınına ait özel nitelikteki fotoğrafların istekleri dışında yayınlandığı sosyal medya hesabına erişerek bu fotoğrafları silen fail bakımından zorunluluk halinin uygulanıp uygulanmayacağı sorusu ortaya çıkacaktır. 5651 sayılı kanunun 9. maddesi ile kişilik hakları ihlal edilen kişi ve kurumlara içerik sağlayıcı, yer sağlayıcı ya da sulh ceza hakimliklerine başvurarak bu içeriklerin yayından kaldırılması veya bu içeriklere erişimin engellenmesini isteme hakkı verilmiştir⁴⁴². Ayrıca sosyal medya platformları⁴⁴³ ile arama motorlarının⁴⁴⁴ da kişilik haklarını ihlal eden içeriklerin engellenmesine dair şikâyet mekanizmaları bulunmaktadır. İçerik sağlayıcılar yahut arama motorları tarafından içeriğin kaldırılmasına yönelik talepleri kabul edilmeyen yahut cevapsız bırakılan kimselerin Kişisel Verilerin Korunması Kuruluna başvurması da mümkündür⁴⁴⁵. Kanaatimizce bu mekanizmalara başvurulmaksızın doğrudan TCK m. 243'teki suçun işlenerek tehlikenin bertaraf edilmesi halinde, TCK m. 25/2'de düzenlenen “*başka suretle korunmak olanağı bulunmama*” şartı yerine getirilmemiş olacağından, zorunluluk hali söz konusu olmayacaktır.

C. Hukuka Aykırılık Unsuru

1. Genel Olarak

Hukuka aykırılık denilince fail ile hukuk düzeni arasındaki zıtlık ve çatışma ilişkisi anlaşılmaktadır⁴⁴⁶. Kanunda sınırları çizilen tipe uygun eylemin hukuka uygunluğuna dair bir olgu mevcut değilse eylem hukuka aykırı olarak kabul edilecek ve ilgili madde gereğince cezalandırılacaktır. Hukuka uygunluk sağlayacak sebepler ise TCK'nın 24. ve 26. maddeleri arasında sayılmıştır. Şayet bu sebeplerden birisi mevcutsa suç konusu hukuka aykırılık unsuru ortadan kalkacak ve fiil ceza hukuku

⁴⁴¹ Özçelik, **a.g.e.** s. 117.

⁴⁴² Aksoy Retornaz, **a.g.e.** s. 15-16.

⁴⁴³ Twitter, **Kaldırma Talepleri - Twitter Şeffaflık Merkezi**, <https://transparency.twitter.com/tr/reports/removal-requests.html#2021-jan-jun> (E.T. 27.06.2022)

⁴⁴⁴ Google, **İçeriği Google'dan Kaldırma - Yasal Yardım**, <https://support.google.com/legal/troubleshooter/1114905?hl=tr> (E.T. 27.06.2022)

⁴⁴⁵ Kişisel Verilerin Korunması Kurulu, **Karar No: 2020/481, T. 23.06.2020**, <https://www.kvkk.gov.tr/Icerik/6776/2020-481> (E.T. 27.06.2022)

⁴⁴⁶ Dönmezer/Erman, **a.g.e.**, s. 241. Koca/Üzülmez, **Genel Hükümler** s. 264. Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 278. Hafizoğulları/Özen, **Ceza Hukuku Genel Hükümler** s. 193.

kuralına aykırı hale gelmeyeceği için suç oluşmayacaktır⁴⁴⁷. TCK'nın 27. maddesinde ise hukuka aykırılık nedenlerinde sınırın aşılması hali düzenlenmiştir.

Hukuka aykırılık tipikliğin dışında suçun yapısal bir unsuru kabul edilmekte olup madde metninde özellikle belirtilmesine gerek yoktur. Buna rağmen kanun koyucunun kimi suç tiplerini düzenlerken “*hukuka aykırı olarak*” veya “*haksız olarak*” gibi ifadeler kullanarak hukuka aykırılığı madde içerisine eklediği görülmektedir. Bu durum hukuka aykırılığın tipikliğe dahil olup olmadığı konusunda bir tartışmayı beraberinde getirmiş olup özellikle suçta hatanın tespiti yönünde belirsizliğe yol açmıştır⁴⁴⁸. Suçun yasal tanımında “*hukuka aykırılık*” ifadesine yer verilmesinin ne anlama geldiği konusunda doktrinde çeşitli görüşler mevcuttur⁴⁴⁹.

Bizim de görüşlerine katıldığımız ve bu durumu “*hukuka özel aykırılık*”⁴⁵⁰ olarak adlandıran yazarlara göre manevi unsurun bir parçası olan hukuka aykırılık tipikliğin bir unsuru haline gelmiştir. Söz konusu suçun unsurlarının tamamlanabilmesi için failin hukuka aykırı hareket ettiğinin bilincinde olması gerektiğinden suç sadece doğrudan kast ile işlenebilmektedir⁴⁵¹. Burada hukuka aykırılık karinesi artık ortadan kalkmakta; suçun oluşabilmesi için hukuka aykırılığın ayrıca tespit edilmesi gerekmektedir^{452,453}. Bu durumda failin suç işleme kastı ile hareket etmesi yeterli olmayıp ayrıca eylemin hukuka aykırı olduğu bilinciyle hareket etmesi de aranacaktır⁴⁵⁴. Fiilin hukuka aykırılığı konusunda hataya düşmesi durumunda ise TCK m.30/1’de düzenlenen hataya ilişkin hükümler uygulanır⁴⁵⁵. Bu görüşe göre bilişim sistemine girme suçunda da hukuka özel aykırılık hali mevcut olup failde hukuka

⁴⁴⁷ Dönmezer/Erman, **a.g.e.**, s. 249. Koca/Üzülmüş, **Genel Hükümler** s. 265.

⁴⁴⁸ Neslihan Göktürk, “*Suçun Yasal Tanımında Yer Alan “Hukuka Aykırılık” İfadesinin İcra Ettiği Fonksiyon*”, **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, C. 7, S. 1, 2016 s. 408-409.

⁴⁴⁹ Bu konudaki görüşler ve tartışmalar hakkında detaylı bilgi için bkz. Göktürk, **a.g.e.** s. 424-436. Tuğrul Katoğlu, **Ceza Hukukunda Hukuka Aykırılık**, Ankara: Seçkin Yayınları, 2003 s. 131 vd.

⁴⁵⁰ Dönmezer/Erman, **a.g.e.**, s. 249. Demirbaş, **a.g.e.** s. 295., Soyaslan, **Genel Hükümler**, s. 440.

⁴⁵¹ Dönmezer/Erman, **a.g.e.**, s. 253. Artuk/Gökçen Özgenç, **a.g.e.** s. 310311. Yenidünya/Değirmenci, **a.g.e.** s. 73-74. Dülger, **Bilişim Suçları** s. 284-285. Mahmut Koca, “*YTCK’da Hukuka Uygunluk Sebepleri*”, **Ceza Hukuku Dergisi**, C. 1, S. 1, Eylül 2016 s. 118-119.

⁴⁵² İçel, **Ceza Hukuku Genel Hükümler** s. 320-321. Akbulut, **Bilişim Alanında Suçlar** s. 136. Demirbaş, **a.g.e.** s. 296.

⁴⁵³ Kurt’a göre halihazırda bilişim sistemine hukuka aykırı olarak girebilecek teknik bilgi ve beceriye sahip bir kişinin eyleminin hukuka aykırılığının bilincinde olamayacağı düşünülemeyecektir. Kurt, **a.g.e.** s. 158.

⁴⁵⁴ Akbulut, **Genel Hükümler** s. 258. Artuk/Gökçen/Alşahin/Çakır, **a.g.e.** s. 480.. Yaşar/Gökcan/Artuk, **a.g.e.** s. 7295. Apaydın, **a.g.m.** s. 279.

⁴⁵⁵ Akbulut, **Bilişim Alanında Suçlar** s. 136. Apaydın, **a.g.m.** s. 279.

aykırılık bilincinin mevcut olup olmadığı her somut olay özelinde araştırılmalıdır⁴⁵⁶. Failde hukuka aykırılık bilincinin tespit edilememesi durumunda ise hukuka aykırılık unsuru ve suç oluşmayacaktır⁴⁵⁷.

Doktrindeki diğer görüş ise hukuka aykırılığın suçun bir unsuru olup olmadığının tespiti sırasında kanun koyucunun aykırılığa işaret eden ifadeyi ne şekilde kullandığının üzerinde durmakta ve bu konuda ikili bir ayrıma gitmektedir. Örneğin TCK m. 244/4'te kullanılan "*haksız bir çıkar*" ve TCK m. 91/5'te yer verilen "*hukuka aykırı yollarla elde edilmiş organ*" ifadelerinde olduğu gibi hukuka aykırılık ifadesinin suçun maddi unsurlarından birini nitelediği kanısına varılırsa burada hukuka özel aykırılık görüşü uygulanabilecektir. Bu hallerde hukuka aykırılık tipikliğin bir unsuru olacağından failin kastının hukuka aykırılığı da kapsamı gerekmektedir⁴⁵⁸. Maddedeki hukuka aykırılık ifadesinin suçun unsurlarını değil de genel olarak suç konusu eylemi nitelemesi halinde ise hukuka özel aykırılık görüşünün uygulanması söz konusu olmayacaktır. Zira bu durumda kanun koyucunun amacı suçtaki hukuka aykırılık unsuru ve haksızlık bilincinin vurgulamaktır. TCK m. 243'ün de örnek olarak gösterilebileceği bu suçlarda hukuka aykırılığa işaret eden ifade kanun metninden çıkarılsa bile failin hareketinin hukuka aykırı olma niteliği değişmeyecektir⁴⁵⁹. Burada kanun koyucunun amacı sıklıkla hukuka aykırılık nedenlerinin ortaya çıkabileceği suçlarda uygulayıcıların dikkatini çekmek ve hukuka uygunluk sebeplerinin varlığının daha dikkatli bir şekilde araştırılmasını sağlamaktır⁴⁶⁰.

Yargıtay kararlarına bakıldığında ise çoğunlukla hukuka özel aykırılık görüşünün benimsendiği ve failde özel olarak hukuka aykırılık bilincinin bulunmadığına kanaat getirilen olaylarda kastın ve suçun oluşmayacağına hükmedildiği görülmektedir. Bu kapsamda Yargıtay, bir kararında, eşine ait telefon ve sosyal medya uygulamalarına eşinin rızası hilafına erişim sağlayarak buradaki yazışmaları açacağı boşanma davasında eşinin aleyhine delil olarak kullanan sanığın, hukuka aykırı davranma bilinciyle hareket etmediğinden, bilişim sistemine girme

⁴⁵⁶ Mahmutoglu, **a.g.e.** s. 862. Ekici Şahin/Koruculu, **a.g.e.** s.608. Yenidünya, **a.g.e.** s. 1038. Kayaer, **a.g.e.** s. 112.

⁴⁵⁷ Koca/Üzülmez, **Özel Hükümler** s. 903. Erdoğan, **a.g.m.** s. 1407. Doğan, **a.g.e.** s. 296. Güler, **a.g.e.** s. 24.

⁴⁵⁸ Göktürk, **a.g.e.** s. 426-427. Koca/Üzülmez, **Genel Hükümler** s. 268. Dülger, **Bilişim Suçları** s. 285.

⁴⁵⁹ Koca/Üzülmez, **Genel Hükümler** s. 268-269. Dülger, **Genel Hükümler** s. 485-486. Hakeri, **a.g.e.** s. 226-227. Apış, **a.g.e.** s. 67.

⁴⁶⁰ Göktürk, **a.g.e.** s. 432-433. Dülger, **Bilişim Suçları** s. 286. Özçelik, **a.g.e.** s. 79. Katoğlu, **Ceza Hukukunda Hukuka Aykırılık** s. 125. Çetin, **a.g.e.** s. 13.

suçunu işlemediğine hükmetmiştir. Yargıtay, elde ettiği ve boşanma davasında delil olarak sunduğu verileri üçüncü şahıslarla paylaşmamış olan failin hukuka aykırı olarak hareket ettiği bilinciyle davranmadığına hükmetmiştir⁴⁶¹.

Yargıtayın farklı olaylarda da benzer bir tutum sergilediği ve özel olarak hukuka aykırı hareket etme bilincini tipikliğin bir unsuru olarak kabul ettiği görülmektedir. Örneğin yargılama sürecindeki tanık beyanlarının doğru olmadığını ortaya çıkarabilmek için Sosyal Güvenlik Kurumu'nun sistemine giriş yaparak sistemden elde ettiği bilgi ve belgeleri mahkemeye sunan sanık hakkında da hukuka aykırılık bilinciyle hareket etmediğinden yola çıkarak beraat kararı verilmiştir⁴⁶². Bir başka kararda ise üçüncü bir kişinin bilgisayarına uzaktan bağlanarak bu kişinin kullanıcı adı ve şifresiyle ücreti karşılığı faydalanabilen bir web sitesine erişim sağlayan failin web sitesine yasal olmayan yollarla giriş yapmadığı gerekçesiyle suçun oluşmadığına hükmedilmiştir⁴⁶³. Tüm bu kararların ortak noktası ise faillerin hak sahibi olmadıkları bilişim sistemlerine hak sahiplerinin rızaları hilafına girmiş olmalarına rağmen

⁴⁶¹ “Kişinin, bir daha kanıt elde etme olanağının bulunmadığı ve yetkili makamlara başvurma imkanının olmadığı ani gelişen durumlarda, örneğin; kendisine karşı işlenmekte olan (cinsel saldırı, hakaret, tehdit, iftira veya şantaj gibi) bir suç söz konusu olduğunda ya da kendisine veya aile birliğine yönelen, onurunu zedeleyen, haksız bir saldırıyı önlemek için, kaybolma olasılığı bulunan kanıtların kaybolmasını engelleyip, yetkili makamlara sunarak güvence altına almak amacıyla, saldırıyı gerçekleştiren tarafın bilgisi ve rızası dışında, özel hayata ait bilgileri okuma, konuşma ve haberleşme içeriklerini veya özel hayata ilişkin ses ve görüntüleri dinleme, izleme ya da kaydetme, kişisel verileri kaydetme, ele geçirme ve yayma eylemlerinin hukuka aykırı olduğunu kabul etmek mümkün olmadığı gibi, esasen bu hallerde, kişinin hukuka aykırı hareket ettiği bilinciyle davrandığından da söz edilemeyeceği nazara alındığında,

Şikayete konu belge örneklerini, üçüncü kişi ya da kişilerle paylaştığı ve/veya çoğaltarak dağıttığına ilişkin hakkında bir iddia ileri sürülmeleyen sanığın, boşanma davasındaki iddiasını ispatlama amacını taşıyan eylemlerinde, hukuka aykırı hareket ettiği bilinciyle davranmadığı anlaşılmakla, sanık hakkında atılı suçlardan beraat kararı verilmesinde bir isabetsizlik görülmemiştir.” Yar. 12. CD, E. 2015/439, K. 2015/10716, T. 15.06.2015 www.lexpera.com.tr (E. T. 15.12.2021)

⁴⁶² “Eş olan sanıkların şikayeti üzerine devam eden bir soruşturmada fikir ve eylem birliği içinde katılanın tanık olarak verdiği beyanlarının doğru olmadığını ortaya çıkarmak için katılanın rızası dışında Sosyal Güvenlik Kurumunun hizmet dökümü sistemine giriş yaparak katılanın hizmet bilgilerinin alınıp devam eden soruşturma dosyasına delil olarak sundukları olayda, söz konusu içerikleri üçüncü kişi ya da kişilerle paylaştığı ve/veya çoğaltarak dağıttığına ilişkin hakkında bir iddia ileri sürülmeleyen sanıkların, devam eden soruşturmada iddialarını ispatlama amacını taşıyan eylemlerinde gerektiğinde soruşturmayı yürüten makam tarafından da söz konu kayıtların getirilebileceği göz önüne alındığında hukuka aykırı hareket etme bilinciyle davrandıkları kabul edilemeyeceğinden, atılı suçların unsurlarının oluşmadığından bahisle beraat kararı verildiğine yönelik yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir.” Yar. 12. CD, E. 2015/16132, K. 2017/3999, T. 16.05.2017 www.lexpera.com.tr (E. T. 15.12.2021)

⁴⁶³ “...sanığın tanıktan aldığı kullanıcı adı ve şifre bilgileri ile, tanığın bilgisayarından doğrudan ve TeamViewer isimli program aracılığıyla uzaktan bağlantı yoluyla katılan şirkete ait web sitesine yasal yollardan giriş yaparak, site içeriğindeki bazı bilgileri kopyaladığı, kopyalanan bu bilgilerin sanığın çalıştığı şirkete ait internet sitesine konulduğuna dair bilgi olmadığı, dolayısıyla katılan şirkete ait siteye yasal olmayan yollardan giriş yapılmadığı, olayın hukuki nitelikte bulunduğu, TCK.nun 243. maddesinde tanımlanan suçun yasal unsurlarının oluşmadığı...” Yar. 8. CD, E. 2014/35223 K. 2015/19051 T. 15.06.2015 www.lexpera.com.tr (E. T. 15.12.2021)

amaçlarının hukuka aykırı olmamasıdır. Bu kararlar doktrinde eleştirilmiş; hukuka aykırılık bilincinin faillerinin amaçlarının meşruluğu ile ölçülemeyeceği ifade edilmiştir. Zira bilişim sistemi üzerinde hak sahibi olan mağdurun sisteme girmesine rıza göstermediğini bilen failin hukuka aykırılık bilinciyle hareket ettiği tartışmasızdır⁴⁶⁴.

Anayasa Mahkemesi ise Yargıtay kararlarındaki tutumu benimsememiş; cep telefonuna eşi tarafından casus yazılım ile erişilen ve özel yazışmaları boşanma davasına delil olarak sunulan başvurucunun başvurusunu kabul ederek somut olayda hak ihlali olduğuna hükmetmiştir. Yüksek mahkemeye göre sanığın verileri üçüncü kişilere ifşa etmemiş olması hukuka aykırı davranma bilinciyle hareket etmediğini tek başına göstermemektedir. Zira verileri paylaşma fiili yargılama konusu suçun unsuru dahi değildir. Burada mahkemece suç konusu fiilin işleniş biçimi ve kapsamı ile sanığın amacının meşru olup olmadığı birlikte değerlendirilerek sanığın suç işleme kastının bulunup bulunmadığı araştırılmalıdır⁴⁶⁵.

Kimi yazarlar ise gelişen bilişim teknolojileri ve karmaşık ağ yapıları nedeniyle failin hukuka aykırılık bilincinin tespitinin çok zor olduğunu ifade etmektedir. Bu görüşe göre Alman Ceza Kanununda olduğu gibi sistemin güvenlik önlemleriyle korunuyor olması şartının aranması gerekmektedir⁴⁶⁶. Bir başka görüş ise TCK m. 243 açısından suçun işlenmemiş olmasının tek yolunun sisteme girmeye yetkili kişi olmak

⁴⁶⁴ YILDIZ, **Bilişim Sistemine Girme** s. 244. Tezcan/Erdem/Önok, **a.g.e.** s. 1156. Ekici Şahin/Koruculu, **a.g.e.** s. 609-610.

⁴⁶⁵ “44- Başvurucunun özel yaşamının gizli alanına dahil önemli bir unsur olan telefonuna yazılım programı yüklenerek ulaşılan kişisel verilerin elde ediliş şekline, kapsamına ve kişisel verilere ulaşma amacının meşru olup olmadığına yönelik olarak derece mahkemelerince bir değerlendirme yapılmamıştır. Ayrıca başvurucunun eşinin, başvurucunun telefonuna program yüklediğine, kişisel verilerine ulaştığına ve bunları kullandığına ilişkin açık ikrarının olduğu gözetildiğinde verilerin hukuka aykırı şekilde ele geçirilmesine ilişkin suç kastının bulunup bulunmadığının başvurucunun süreç içinde ileri sürdüğü tüm iddiaları karşılanarak ve gösterilen deliller araştırılarak ortaya konulması gerekirken, ele geçirme fiilinin unsuru olmadığı hâlde verilerin ifşa edilmediği gerekçesine dayanılmıştır. Derece mahkemelerinin eşlerin birbirlerine karşı özel hayat alanlarının bulunmadığı sonucunu doğuracak mahiyetteki yaklaşımının anayasal güvencelere aykırı olduğu açıktır. Bu hususlar dikkate alındığında derece mahkemelerince açıklanan gerekçelerin başvurucunun kişisel verilerinin korunması hakkının güvencelerini gözeterek şekilde ilgili ve yeterli olduğunun söylenmesi mümkün görünmemektedir.” AYM Birinci Bölüm, **B.Y. Kararı, Başvuru No: 2018/30296, T. 07.09.2021**, Resmi Gazete S. 31628 T. 14.10.2021 <https://www.resmigazete.gov.tr/eskiler/2021/10/20211014-4.pdf> Benzer bir karar için bkz. AYM Birinci Bölüm, **H. Ö. Kararı, Başvuru No: 2019/20473, T. 03.02.2022**, Resmi Gazete S. 31782, T. 18.03.2021, <https://www.resmigazete.gov.tr/eskiler/2022/03/20220318-18.pdf> (E.T. 06.05.2022)

⁴⁶⁶ Soyaslan, **Özel Hükümler**, s. 664.

olduğunu ifade ederek hukuka uygunluk sebeplerinin bu suç için söz konusu olamayacağını savunmuştur⁴⁶⁷.

Hukuka aykırılığı ortadan kaldıran hukuka uygunluk sebepleri TCK'nın 24. ile 26. maddeleri arasında yer almaktadır. Bu haller; kanunun hükmünün (24/1) ve amirin emrinin (24/2) yerine getirilmesi, meşru savunma (25/1) hali, hakkın kullanılması (26/1) ve ilgilinin rızası (26/2) olarak sayılmıştır. Bilişim sistemine girme suçu bakımından görevin ve amirin emrinin ifası maksadıyla hareket edilen hallerde tipiklik ve suç oluşmayacağından⁴⁶⁸ bu çalışmada değinilmeyecektir.

Hukuka uygunluk nedenlerine değinilmeden önce unutulmamalıdır ki bu haller ancak kendi sınırları içerisinde gerçekleşmeleri halinde bir fiili suç olmaktan çıkaracaktır⁴⁶⁹. TCK m. 27'de hukuka uygunluk sebeplerinde sınırın taksirle aşılması halinde ceza verilebilmesi için suçun taksirle işlenebilmesi şart koşulmuştur. Buna göre taksirle işlenen bir suçta hukuka uygunluk nedenini sınırı taksirle aşılmışsa, suçun taksirli hali için belirlenen ceza üzerinden indirim yapılacaktır⁴⁷⁰. Bilişim sistemine girme suçu taksirle işlenebilen bir suç olmadığı için hukuk uygunluk nedenlerinde sınırın taksirle açılması halinde suç oluşmayacaktır⁴⁷¹. Sınırın kasten aşılmış olması halinde ise kanunda özel bir düzenleme yapılmadığı için genel hükümler uygulanacaktır. Buna göre fail sınırı aşmışsa hukuka uygunluk nedeni ortadan kalkacak, eylem hukuka aykırı hale gelecektir. Bu halde cezadan herhangi bir indirim yapılması söz konusu olmayacaktır⁴⁷².

2. Kanun Hükmünün Yerine Getirilmesi

TCK m. 24/2'ye göre kanunun hükmünü yerine getiren kimseye işlediği fiil nedeniyle ceza verilemeyecektir⁴⁷³. Burada kanundan kasıt yalnızca ceza kanunu değildir. Diğer kanunlar ya da yönetmelikler gibi farklı türde mevzuattan kaynaklanan görevlerin ifası da bu madde kapsamında olacaktır.⁴⁷⁴ Bilişim sistemine girme veya

⁴⁶⁷ Hafizoğulları/Özen, **Topluma Karşı Suçlar** s. 448.

⁴⁶⁸ Akbulut, **Bilişim Alanında Suçlar** s.137.

⁴⁶⁹ Koca/Üzülmüş, **Genel Hükümler** s. 305. Demirbaş, **a.g.e.** s. 356.

⁴⁷⁰ Dönmezer/Erman, **a.g.e.**, s. 379. Artuk/Gökçen/Alşahin/Çakır, **a.g.e.** s. 552-553.

⁴⁷¹ Dülger, **Bilişim Suçları** s. 294. Ekici Şahin/Koruculu, **a.g.e.** s. 113-114.

⁴⁷² Dülger, **Bilişim Suçları** s. 294. Ekici Şahin/Koruculu, **a.g.e.** s. 114.

⁴⁷³ Hafizoğulları/Özen, **Ceza Hukuku Genel Hükümler** s. 213-214. Artuk/Gökçen/Alşahin/Çakır, **a.g.e.** s. 483.

⁴⁷⁴ Dönmezer/Erman, **a.g.e.**, s. 319.

sistemde kalmaya devam etme fiili, kanuni bir düzenlemeye dayanılarak icra ediliyorsa hukuka uygundur⁴⁷⁵.

Ceza yargılamaları sırasında şartlarının oluşması halinde “bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma” tedbirinin uygulanacağı CMK⁴⁷⁶ m. 134’te düzenlenmiştir. Aynı konuyu düzenleyen ve geneli itibariyle CMK’daki düzenlemeye paralel olan Adli ve Önleme Aramaları Yönetmeliği’nin 13. Maddesinde ise bu tedbirlerin “bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımlar” için de uygulanacağı ifade edilmiştir. Bu kapsamda bilgisayar, bilgisayar programı ve kütüklerinin yanı sıra CD, USB bellek, harici disk gibi veri depolama araçları ile bilgisayar ağları ve uzak bilgisayar kütükleri hakkında da arama, kopyalama ve elkoyma tedbirleri uygulanabilecektir. Kişilerin bilişim sistemleri üzerinden çeşitli program ve sosyal medya uygulamaları aracılığıyla yaptıkları konuşmaların kayıtları⁴⁷⁷ ile bilgisayarlarda kayıtlı e-postaların⁴⁷⁸ incelenmesi de yine bu madde kapsamındadır. Kimi yazarlarca⁴⁷⁹ yanlış bulunduğu ifade edilse de akıllı cep telefonları da Yargıtay⁴⁸⁰ ve bir kısım yazar

⁴⁷⁵ Ekici Şahin/Koruculu, **a.g.e.** s. 610.

⁴⁷⁶ Resmi Gazete, **5271 Sayılı Ceza Muhakemeleri Kanunu** <https://www.resmigazete.gov.tr/eskiler/2004/12/20041217.htm#1> (E.T. 16.12.2021)

⁴⁷⁷ “Şüpheli veya sanığın internet ortamında çeşitli programlar ya da sosyal iletişim siteleri (Msn Messenger, Facebook, Twitter vb.) vasıtasıyla gerçekleştirdiği iletişime ilişkin kayıtların aranması, CMK’nun 135. maddesinin birinci fıkrasına göre değil, aynı Kanunun 134. maddesinin birinci fıkrasına göre yapılabilir. Zira CMK’nun 135. maddesinin birinci fıkrasında düzenlenen telekomünikasyon yoluyla iletişimin denetlenmesi koruma tedbiri, teknik araçlarla iletişimin dinlenmesini ve kayda alınmasını kapsamaktadır.” YCGK, E. 2017/956, K. 2017/370, T. 26.09.2017 www.lexpera.com.tr (E. T. 16.12.2021)

⁴⁷⁸ Olgun Değirmenci, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, Ankara: Seçkin, Mart 2014 s. 333.

⁴⁷⁹ Özen/Özocak’a göre akıllı cep telefonları üzerinde yapılacak arama, kopyalama ve elkoyma faaliyetleri bakımından ikili bir ayrıma gidilmeli; söz konusu arama, kopyalama ya da elkoyma faaliyeti cihazın telefon özelliği ile ilgili ise genel arama hükümleri uygulanmalıdır. Yapılacak işlem cihazın işletim sistemi üzerindeki uygulamalarla ve cihazın bilgisayar özellikleri ile ilgili ise söz konusu tedbirin uygulanması CMK m. 134 kapsamında olacaktır. Muharrem Özen/Gürkan Özocak, “**Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)**”, **Ankara Barosu Dergisi**, S. 2015/1 s. 69-70. Parlak’a göre cep telefonları bilgisayar kapsamına girmemekte; Yargıtay bu uygulaması ile kanunun lafzını genişletici bir şekilde yorumlamaktadır. Yapılması gereken kanun metninin cep telefonlarını da kapsayacak şekilde “**bilişim sistemlerinde arama kopyalama ve el koyma**” şeklinde değiştirilmesidir. Parlak, **Türk Ceza Muhakemesinde Bilişim Sistemlerinde Arama, Kopyalama ve Elkoyma**, s. 50-51. Taşkın da benzer yönde görüş belirterek madde başlığındaki bilgisayar ifadesinin dar yorumlanması gerektiğini, cep telefonunun CMK m. 134 kapsamında incelenmesinin Anayasa m. 38/2 ve CMK m. 230/1-b’ye aykırı olacağını ifade etmiştir. Yazar CMK 134. maddenin başlığının “**verileri otomatik işleme tabi tutan araçlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma**” şeklinde değiştirilmesini önermiştir. Taşkın, **a.g.e.** s. 173-174.

⁴⁸⁰ “Genel olarak 134. maddesinin uygulamada; bilgisayar, akıllı telefonlar, GPS cihazları, donanım ve yan donanımlar, verileri dijital olarak kaydetme ve işleme yeteneğinde olan her türlü dijital cihazları kapsadığı kabul edilmektedir.” YCGK, E. 2016/544, K. 2020/127, T. 25.2.2020 Aynı yönde bkz.

tarafından madde kapsamında değerlendirilmektedir⁴⁸¹. CMK m. 134'teki şartlar oluşmuş ve hâkim kararı alınmışsa; bahsedilen cihazlarda yapılan arama, kopyalama ve elkoyma faaliyetleri sırasında icra edilen bilişim sistemine girme ve sistemde kalma eylemleri suç oluşturmayacaktır⁴⁸². Özellikle bilgisayarların birden fazla kişinin kullanımına tahsis edildiği; internet kafeler, kamu kurumları ve okullar gibi yerlerde bulunan bilişim sistemleriyle suç işlenmiş olması halinde bu maddeler gereğince yapılacak inceleme ve araştırmanın önemi artmaktadır⁴⁸³. Ceza soruşturmaları haricinde yapılacak idari soruşturmalarda ise bu tedbire başvurulması mümkün olmayacaktır⁴⁸⁴.

CMK'nın 135. maddesine göre ise belli şartların gerçekleşmesi halinde sanık hakkında “*telekomünikasyon yoluyla iletişimin tespiti, dinlenmesi ve kayda alınması*” tedbirinin uygulanması söz konusu olabilecektir. Kanunun bu bölümündeki tedbirlerin uygulanmasına ilişkin yönetmeliğin 4. maddesinin ilk fıkrasının j bendinde ise telekomünikasyon kavramı “*işaret, sembol, ses ve görüntü ile elektrik sinyallerine dönüştürülebilen her türlü verinin; kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektro kimyasal, elektro mekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması*” olarak tanımlanmıştır. Söz konusu tanım incelendiğinde iletişim faaliyetinin yürütülebildiği her türlü bilişim ağı, bilişim sistemi ve bu sistemler aracılığıyla kullanılan uygulamalar üzerinden yapılan iletişim bu tedbirin konusu olabilecektir⁴⁸⁵. Burada dikkat edilmesi gereken nokta iletişim faaliyetlerinin yürütülmesi sırasında bu tedbirin uygulanacağıdır. İletişim sonrasında sistemde oluşan kayıtlar ise CMK m. 134'ün konusunu oluşturacaktır⁴⁸⁶. Bu

YCGK, E. 2017/961, K. 2019/622, T. 22.10.2019; Yar. 16. CD, E. 2015/4672, K. 2016/2330, T. 21.4.2016 www.lexpera.com.tr (E. T. 16.12.2021)

⁴⁸¹ Apiş, **a.g.e.** s. 78-79. Murat Volkan Dülger/Gözde Mодоğlu, **Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet İletişim Hukuku Uygulama Rehberi**, Ankara: Avrupa Birliği ve Konseyi Ortak Yayını, 2014, s. 112

⁴⁸² Akbulut, **Bilişim Alanında Suçlar** s. 137-138. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 964. Yıldız, **Bilişim Sistemine Girme** s. 245. Soyaslan, **Özel Hükümler**, s. 663-664. Mahmutoglu, **a.g.e.** s. 862. Taşkın, **a.g.e.** s. 28. Güler, **a.g.e.** s. 25. Kayaer, **a.g.e.** s. 113-114. Hasan Tahsin Gökcan/Mustafa Artuç, **Türk Ceza Kanunu Şerhi, 5. Cilt (Md. 197-254)**, Ankara: Adalet Yayınevi, 2021 s.8134-8135.

⁴⁸³ Ekici Şahin/Koruculu, **a.g.e.** s. 610.

⁴⁸⁴ Muharrem Özen/İhsan Baştürk, **Temel Hak ve hürriyetler Bağlamında İlişim-İnternet ve Ceza Hukuku**, Ankara: Adalet Yayınevi, 2011 s. 144.

⁴⁸⁵ Nur Centel, “5271 Sayılı Ceza Muhakemesi Kanunu’na Göre Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi”, **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Köksal BAYRAKTAR’a Armağan S.** 2020/1, C. 1. s. 175. Özçelik, **a.g.e.** s. 96-97.

⁴⁸⁶ Parlak, **a.g.e.** s. 53.

tedbirlerin uygulanması sırasında sisteme girildiği takdirde bilişim sistemine girme suçu oluşmayacaktır⁴⁸⁷.

Kimi yazarlarca CMK m. 140'ta düzenlenen “*teknik araçlarla izleme*” tedbirinin uygulanmasının da incelemekte olduğumuz suç bakımından hukuka uygunluk sebepleri arasında olacağı ifade edilmiştir⁴⁸⁸. Fakat uygulama yönetmeliğinin 17. maddesi incelendiğinde bu tedbirin “*kişilerin işyeri veya kamuya açık yerlerdeki tüm faaliyetlerinin izlenmesi, görüntülenmesi ve kayda alınması*” şeklinde icra edilebileceği ifade edilmiştir. Bu tedbirin uygulanması sırasında bilişim sistemine girilmesi söz konusu olmayacağından TCK m. 243. açısından bir hukuka uygunluk sebebinin varlığından da söz edilemeyecektir⁴⁸⁹.

2559 sayılı PVSK bünyesinde de bilişim sistemine girilmesi ve sistemde kalınmasını gerektiren eylemler düzenlenmiş olup bu eylemlerin icrası da suçu oluşturmayacaktır. Anılan kanunun 13A maddesine göre polis, kaybolan çocukların bulunması maksadıyla iletişimin denetlenmesi faaliyetini icra edebilecektir⁴⁹⁰. Yine aynı kanunun Ek. 7. maddesi ile içerisinde bilişim suçlarının da bulunduğu bir grup suçu önlemek amacıyla polise “*telekomünikasyon yoluyla yapılan iletişim veya internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen veriler tespit etme, dinleme, sinyal bilgileri değerlendirme, kayda alma*” yetkisi verilmiştir. Benzer şekilde jandarmaya da Jandarma Teşkilat, Görev ve Yetkileri Kanunu ek madde 5 ile görev alanı içerisindeki belli suçların önlenmesi maksadıyla “*telekomünikasyon yoluyla yapılan iletişimi tespit etme, dinleme, sinyal bilgilerini değerlendirme, kayda alma*” yetkisi verilmiştir. Devlet İstihbarat Hizmetleri Ve Milli İstihbarat Teşkilatı Kanunu’nun 6. maddesinde ise Milli İstihbarat Teşkilatına “*Anayasanın 2nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesi*” amacıyla iletişimin denetlenmesi yetkisi verilmiştir. Bu maddeler kapsamında yapılacak önleme araması ve iletişimin denetlenmesi faaliyetleri

⁴⁸⁷ Mahmutoglu, **a.g.e.** s. 862. Taşkın, **a.g.e.** s. 28. Kayaer, **a.g.e.** s. 114.

⁴⁸⁸ Apaydın, **a.g.m.** s. 281. Doğan, **a.g.e.** s.297. İhtiyaroğlu, **a.g.e.** s. 427.

⁴⁸⁹ Apiş, **a.g.e.** s. 80. Özçelik, **a.g.e.** s. 99-100.

⁴⁹⁰ Özçelik, **a.g.e.** s. 96.

de -ilgili mevzuat hükümlerine uygun bir şekilde icra edildikleri takdirde- bilişim sistemine girme suçunu oluşturmayacaktır⁴⁹¹.

Tekrarlamakta fayda görüyoruz ki; ilgili kanunlarda verilen emirlerin hangi şartlarda ve kimler tarafından uygulanacağı hususu önem arz etmektedir. Bu maddelerde gösterilen eylemlerin şartları oluşmadan yahut maddede gösterilmeyen kişiler tarafından icra edilmesi halinde hukuka uygunluk sebebinden söz edilemeyecektir⁴⁹².

3. Meşru Savunma

Meşru savunma ağır ve haksız bir saldırıya maruz kalan kimsenin bu saldırıyı kendisinden uzaklaştırmak amacıyla gösterdiği zorunlu bir tepkidir⁴⁹³. Hukuk düzeninin korumak istediği bir değere yapılan saldırının engellenmesi amacıyla, bu saldırıyı defetmek amacı taşıyan kişinin fiili hukuk düzeni tarafından mazur görülmektedir⁴⁹⁴. Meşru savunmanın incelemekte olduğumuz suç açısından bir hukuka uygunluk nedeni olup olmadığı konusunda doktrinde farklı görüşler öne sürülmektedir.

Bilişim sistemine girme suçunda meşru savunmanın hukuka uygunluk nedeni olamayacağını savunan yazarlar bu durum için iki önemli gerekçe sunmuşlardır. Öncelikle meşru savunmayı düzenleyen TCK'nın 25. maddesinde “*o anda hal ve koşullara göre saldırı ile orantılı biçimde defetmek zorunluluğu*” aranmakta; sisteme yapılan ihlalin o anda belirlenmesi teknik olarak mümkün görünmemektedir. Saldırıya bir karşılık verildiğinde ise meşru savunma iddiasıyla gerçekleştirilen fiilin saldırıyı defetmesi ve bunun yargılama sırasında ispat edilmesi oldukça güçtür. Yazarlar, bu çekincelerin görmezden gelinerek meşru savunmanın mümkün görülmesi halinde ise adeta bilişim suçlarının işlenmesinin teşvik edilmiş olacağını ifade etmişlerdir. Meşru savunmaya ilişkin ölçüyü belirlemek ve sınırları çizmek oldukça zor olduğundan

⁴⁹¹ Akbulut, **Bilişim Alanında Suçlar** s. 138. Kayaer, **a.g.e.** s. 114.

⁴⁹² Dönmezer/Erman, **a.g.e.**, s. 320.

⁴⁹³ Dönmezer/Erman, **a.g.e.**, s. 333. Artuk/Gökçen/Alşahin/Çakır, **a.g.e.** s. 490.

⁴⁹⁴ Koca/Üzülmez, **Genel Hükümler** s. 278. Özgen., **a.g.e.** s. 367.

cezalandırılması gereken birçok bilişim suçunun da meşru savunma kapsamında değerlendirilmesi mümkün olacaktır⁴⁹⁵.

Bir görüşe göre ise çalışma konusu suç bakımından meşru savunmanın bir hukuka uygunluk nedeni olup olmadığı tartışılırken saldırının niteliğinin belirlenmesi önem arz etmektedir. Bir ağ aracılığıyla uzaktan yapılan sisteme girme yahut sistemde kalma eylemi söz konusu ve bu saldırı sistem sahibi tarafından fark edilmiş ise burada meşru savunmadan söz edilemeyecektir. Zira kullanıcı tarafından sistem kapatılarak ya da sistemin saldırıda kullanılan ağ ile bağlantısı kesilerek suç sonlandırılabilir. Bu durumda karşı tarafa saldırı yapılması gibi bir gereklilik mevcut olmadığından meşru savunmadan da söz edilemeyecektir. Buna rağmen bilişim sistemine yönelik saldırının sisteme fiziki bir temasla gerçekleştiriliyor olması halinde meşru savunmadan bahsedilebilecektir⁴⁹⁶.

Genel hatlarıyla yukarıdaki görüşe paralellik gösteren bir başka görüş ise suç konusu bilişim sistemine uzaktan erişilerek suçun işlendiği hallerde bağlantının kesilmesi ya da sistemin kapatılması yoluyla suçun engellenmesinin her zaman mümkün olmadığına dikkat çekmiştir. Özellikle ticari amaçlı işletilen servislerin kısa süreliğine kapatılması halinde dahi ciddi zararların meydana çıkabileceği dikkate alındığında sistem sahiplerince karşı bir saldırı yapılması meşru savunma kapsamında değerlendirilebilecektir. Bunun yanında büyük şirketler ve kamu kurumları sahip oldukları sistemlerin saldırılardan korunması maksadıyla ciddi yatırımlar yapmakta ve bu işlerde uzman beyaz şapkalı hacker olarak adlandırılan kişileri istihdam etmektedirler. Teknik bilgi ve becerisi yüksek bu kişiler tarafından saldırının sonlandırılması ya da saldırganların kimliğini tespit edilmesi için saldırganların sistemlerine girilmesi mümkün olabilmektedir⁴⁹⁷. Bir görüş ise burada gerçekleştirilen karşı saldırı eylemi hukuka uygun olsa da meşru savunmanın şartları oluşmadığını savunmaktadır. Bu görüşe göre karşı saldırıyı icra edende bu fiile ilişkin hukuka aykırılık bilincinin bulunmadığı kabul edilmeli ve ceza verilmemelidir⁴⁹⁸.

⁴⁹⁵ Dülger, **Bilişim Suçları** s. 293. Karagülmez, **a.g.e.** s. 75. Pelin Topçuoğlu, **Türk Ceza Kanunu Kapsamında Bilişim Sistemine Girme Suçu**, İstanbul: Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, 2022 s. 61.

⁴⁹⁶ Erdoğan, **a.g.m.** s. 1410-1411.

⁴⁹⁷ Özçelik, **a.g.e.** s. 94.

⁴⁹⁸ Apaydın, **a.g.m.** s. 284-285.

Kimi yazarlar ise fiili icra edecek kişinin teknik bilgi ve beceri sahibi olması gibi herhangi bir ön koşul öne sürmeksizin bilişim sistemine girme suçunun bir suçun önlenmesi için meşru savunma eylemi olarak da işlenebileceğini savunmaktadır. Örneğin herkes tarafından görülmesini istemediği görüntülerinin bir sosyal medya hesabında yayınlandığını fark eden kimse, bu fotoğrafları kaldırmak amacıyla söz konusu sosyal medya hesabının şifresini kırarak bu hesaba erişim sağlayabilir. Bu durumda mevcut saldırı engellendikten sonra vakit kaybedilmeden herhangi bir veriye zarar vermeksizin sistemde çıkılması halinde eylem meşru savunma sınırları içinde kalacağından suç oluşmayacaktır⁴⁹⁹. Bu görüşteki yazarlar meşru savunma halinin söz konusu olabilmesi için zorunluluk halinde olduğu gibi “*başka suretle korunma olasılığı olmaması*” şartının aranmayacağını ifade etmişlerdir. Bu nedenle içerik ve yer sağlayıcıları ile adli makamlara yönelik şikâyet mekanizmalarının mevcut olması meşru savunma halinin varlığını etkilemeyecektir⁵⁰⁰.

Burada meşru savunma halinin savunmaya ilişkin koşullarından olan “*savunmada zorunluluk bulunması hali*” üzerinde durmak gerekecektir. Savunma, saldırıyı sona erdirmek için daha yumuşak ancak aynı şekilde etkili bir başka yolun bulunmaması halinde zorunludur⁵⁰¹. Bilişim sistemleri ve internet yoluyla kişilik haklarına saldırıda bulunulması halinde bu saldırıları önlemek için öngörülen şikâyet mekanizmalarının buradaki zorunluluğu ortadan kaldırabileceği düşünülebilir. Somut uyuşmazlıkta “*savunmada zorunluluk bulunması*” şartının mevcut olup olmadığının belirlenmesi sırasında failin içerisinde bulunduğu durum göz önüne alınmalıdır⁵⁰². Doktrinde kanunun kimseyi korkak ve alçak bir şekilde davranmaya zorlayamayacağı ifade edilmiştir⁵⁰³. Failin içerisinde bulunduğu ruh hali değerlendirilmeli ve fail şerefine leke sürecek ya da onur kırıcı şekilde davranmak zorunda bırakılmamalıdır⁵⁰⁴. Buradan yola çıkılarak şikâyet mekanizmalarına başvurulması halinde geçecek süreçte failin uğrayacağı maddi ve manevi zarar dikkate alınarak somut olay özelinde değerlendirme yapılması gerektiği kanaatindeyiz.

⁴⁹⁹ Ekici Şahin/Koruculu, **a.g.e.** s. 610. Tezcan/Erdem/Önok, **a.g.e.** s. 1159.

⁵⁰⁰ Ekici Şahin/Koruculu, **a.g.e.** s. 611.

⁵⁰¹ Koca/Üzülmez, **Genel Hükümler** s. 282-283. Hakaeri, **a.g.e.** s.334.

⁵⁰² Dönmezer/Erman, **a.g.e.** s. 353. Hakeri, **a.g.e.** s. 335.

⁵⁰³ Dönmezer/Erman, **a.g.e.** s. 355.

⁵⁰⁴ Özbek/Doğan/Bacaksız, **Genel Hükümler**, s.311.

4. Hakkın Kullanılması

TCK m. 26/1’de hakkını kullanan kimseye ceza verilmeyeceği düzenlenmiştir. Buradaki hak kavramının kapsamı bakımından bir sınır bulunmamaktadır. Söz konusu hak özel hukuk ya da kamu hukukundan kaynaklanabileceği gibi örf ve âdet hukuku kaynaklı da olabilir⁵⁰⁵. Bir mesleğin, sanatın ya da sporun icrası ile basın özgürlüğünün sağladığı haklar da hukuka uygunluk sebebi olarak kabul edilmektedir⁵⁰⁶.

Bilişim sistemine girme suçu açısından ilk olarak özel hukuk sözleşmelerine değinmek yerinde olacaktır. Kişiler abonelik, lisanslama, kiralama gibi sözleşmelerle kendilerine ait olmayan bilişim sistemlerine girme ve kalma hakkı elde edebilirler. Bu durumda kişilerin özel hukuk sözleşmeleri ile elde etmiş oldukları hakları kullanarak başkalarına ait bilişim sistemine girmesi da kalmaya devam etmesi halinde suç oluşmayacaktır⁵⁰⁷. Bununla birlikte failin bilişim sistemine erişim sağlarken sözleşmedeki şartlara uymaması veya sözleşmede aksi kararlaştırılmış olmasına rağmen kendisine tahsis edilen sisteme giriş bilgilerini üçüncü kişilere vermesi halinde burada hakkın kullanılmasından söz edilemeyecektir. Sonuç olarak sisteme yetkisiz erişim sağlayan üçüncü kişiler fail, sözleşme ile sisteme girme ve kalma yetkisine sahip olan kişi ise azmettiren ya da yardım eden durumunda olacaktır⁵⁰⁸.

Genel hükümler açısından gazetecilik ve haber verme hakkının da hukuka uygunluk nedeni bağlamında hakkın kullanılması kapsamına girdiği belirtilmektedir⁵⁰⁹. Her ne kadar ülkemiz uygulamasında rastlanmamış olsa da kamusal bir hak olan haber verme hakkının incelemekte olduğumuz özelinde hukuka uygunluk sebebi olup olmayacağı hususu doktrinimizde tartışılmaktadır⁵¹⁰. Bir görüş haber yapmak amacıyla doğrudan bilişim sistemine girme suçunun işlenmesi halinde suçun oluşacağı ve cezalandırılması gerektiğini savunmaktadır⁵¹¹. Karşıt görüşe göre

⁵⁰⁵ Faruk Erem, “*Ceza Hukukunda ‘Hakkın Kullanılması’*”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C. 41, S. 1, Ocak 1990 s. 8. Esra Türkoğlu Arslan, “*Hukuka Uygunluk Sebebi Olarak Hakkın Kullanılması*”, **Konya Barosu Dergisi**, C. 2, S. 1, 2018 s. 176. Demirbaş, **a.g.e.** s. 333. Özgenç, **a.g.e.** s. 313-314.

⁵⁰⁶ Koca/Üzülmöz, **Genel Hükümler** s. 286-287. Özbek/Doğan/Bacaksız, **Genel Hükümler** s.318. Türkoğlu Aslan, **a.g.e.** s. 175.

⁵⁰⁷ Karakehya, **a.g.e.** s. 16.

⁵⁰⁸ Özçelik, **a.g.e.** s. 90-92.

⁵⁰⁹ Dönmezer/Erman, **a.g.e.**, s. 277. Hafızoğulları/Özen, **Ceza Hukuku Genel Hükümler** s.229-230. Demirbaş, **a.g.e.** s. 337.

⁵¹⁰ Tartışmalar ve diğer ülkelerdeki örnek kararlar için bkz. Dülger, **Bilişim Suçları** s. 292-294. Özçelik, **a.g.e.** s. 88-90.

⁵¹¹ Dülger, **Bilişim Suçları** s. 294.

ise gerçek ve güncelliğini yitirmemiş bir olayın toplumun faydası için haber yapılması için işlenen bilişim sistemine girme suçu hakkın kullanılması kapsamında değerlendirilmeli ve suçun oluşmadığı kabul edilmelidir⁵¹². Doktrinde haber verme hakkının bir hukuka uygunluk nedeni sayılabilmesi için; haberin gerçek ve güncel olması, haberin yayınlanmasında kamu yararı olması ve ölçülülük ilkesine uyulması gerektiği ifade edilmiştir⁵¹³. Kanaatimizce bu şartları sağlayan bir haber yapmak maksadıyla bilişim sistemine girme fiilinin işlenmesi halinde hukuka uygunluk hali söz konusu olacak ve faile ceza verilmeyecektir.

Kimi yazarlar sistem sahibi ile sistemdeki güvenlik açıklarının bulunması ve giderilmesi için çalışmak üzere sözleşme yapan beyaz şapkalı hackerlar için de hakkın kullanılması halinin söz konusu olduğunu ifade etmektedir. Bu görüşü savunan yazarlara göre bu kişiler güvenlik açıklarını test etmek amacıyla sisteme girmeyi ve orada kalmayı deneyecek, kimi zaman da başarılı olacaktır. Sonuç olarak tüm bu faaliyetlerin yapılabileceği sistem sahibi ile yapılan sözleşmede kararlaştırıldığından burada da hakkın kullanılması söz konusudur⁵¹⁴. Kanaatimizce bu görüşe katılmak mümkün değildir. Sızma testi olarak da adlandırılan sistem açıklarını tespit etmek maksadıyla gerçekleştirilen sisteme girme fiillerinin hakkın kullanılması kapsamına girmeyeceği açıktır. Bir sonraki bölümde ayrıntılı biçimde açıklanacağı üzere burada TCK m. 26/2'de yer alan ilgilinin rızası söz konusu olacaktır.

5. İlgilinin Rızası

Üzerinde mutlak olarak tasarrufta bulunulabilen haklara ilişkin hak sahibinin rızasına uygun olarak icra edilen fiiller suçun unsurlarını taşıyor olsa bile hukuka uygun kabul edilecek ve cezalandırılmayacaklardır⁵¹⁵.

Bir bilişim sistemine sistem sahibi ya da yetkilisinin rızası dahilinde girilmesi veya sistemde kalınması halinde fiil hukuka uygun hale geleceğinden suç oluşmayacaktır⁵¹⁶. Rıza açık bir irade beyanıyla açıklanmış olabileceği gibi zımnen

⁵¹² Özçelik, **a.g.e.** s. 89-90.

⁵¹³ Ayvaz Cebre, “*Hukuka Uygunluk Sebebi Olarak Haber Verme Hakkı*”, **Uyuşmazlık Mahkemesi Dergisi**, C. 4, S. 7, Haziran 2016 s. 304-309.

⁵¹⁴ Kurt, **a.g.e.** s. 148,157. Apaydın, **a.g.m.** s. 279.

⁵¹⁵ Dönmezer/Erman, **a.g.e.**, s. 305-318. Koca/Üzülmez, **Genel Hükümler** s. 294-297. Hafizoğulları /Özen, **Ceza Hukuku Genel Hükümler** s. 227-228.

⁵¹⁶ Yıldız, **Bilişim Sistemine Girme** s. 244. Soyaslan, **Özel Hükümler**, s. 663. Apaydın, **a.g.m.** s. 281. Mahmutoglu, **a.g.e.** s. 862.

verilmiş bir rıza da olabilir⁵¹⁷. Örneğin arkadaşından açık olan bilgisayarındaki bir problemle ilgilenmesini isteyen kişi, kendine ait bilişim sistemine girmesi ve orada kalması için arkadaşına rıza vermiş olacak; bu rızaya uygun olarak sisteme girilmesi halinde suç oluşmayacaktır⁵¹⁸.

Öncelikle rızanın sadece sistem üzerinde hak sahibi olan kişiler tarafından verilebileceğini belirtmek gerekmektedir. Bu yetki mülkiyet hakkına dayanabileceği gibi farklı hukuki ilişkilere de dayanabilmektedir. Bu kapsamda sisteme giriş için sistem sahibinin rızasını almış bir kişinin üçüncü bir kişiye sisteme giriş için rıza vermesi hukuka uygunluk sebebi sayılmayacaktır⁵¹⁹. Örneğin üniversitelerin satın aldığı ücretli veri tabanlarını verdiği kullanıcı adı ve şifrelerle öğrenci ve çalışanlarına ücretsiz olarak tahsis etmesi de rıza kapsamındadır. Bir öğrencinin üniversite tarafından kendisine verilen şifreyi üçüncü bir kişiyle paylaşması halinde ise rızanın varlığından söz edilemeyecektir. Sisteme giren üçüncü kişi TCK m. 243'te düzenlenen suçun faili olacak; şifreyi faille paylaşan kişi ise iştirak hükümlerine göre cezalandırılacaktır⁵²⁰.

Hak sahibinin rızayı bir olayın gerçekleşmesi ya da belli bir sürenin geçmesi gibi bir şarta bağlaması da mümkündür. Rızanın içerdiği şartlara aykırı olarak icra edilen eylem hukuka aykırı olduğundan suç oluşacaktır⁵²¹.

Bilişim sistemine girme ve kalma için verilecek rıza sistemin belli bir bölümüne yönelik olarak verilebileceği gibi⁵²² sadece belli bir amacın ifa edilmesine yönelik olarak da verilebilir. Kimi yazarlar bir amacı ifa etmek üzere yetkilendirilmiş kişinin yetkisini bu amaç dışındaki eylemler için kullanması halinde TCK m. 243 kapsamında suç oluşmayacağını savunmaktadır⁵²³. Bir başka görüşe göre ise sistem sahibi burada belli bir amacın ifa edilmesini şart koşan bir rıza vermiştir. Söz konusu amaç dışında sisteme girilmesi halinde rızanın geçerliliğinden söz edilemeyecek, suç oluşacaktır⁵²⁴.

⁵¹⁷ Yaşar/Gökcan/Artuç, **a.g.e.** s. 7295. Erdoğan, **a.g.m.** s. 1408. Güler **a.g.e.** s. 24.

⁵¹⁸ Dülger, **Bilişim Suçları** s. 290.

⁵¹⁹ Kurt, **a.g.e.** s. 157. Erdoğan, **a.g.m.** s. 1408-1409. Ekici Şahin/Koruculu, **a.g.e.** s.612. Güler, **a.g.e.** s. 25. Taşdemir, **a.g.e.** s. 259. Bayındır, **a.g.e.** s. 65-66.

⁵²⁰ Tezcan/Erdem/Önok, **a.g.e.** s. 1155.

⁵²¹ Akbulut, **Bilişim Alanında Suçlar** s. 137. Özçelik, **a.g.e.** s. 84-85.

⁵²² Erdoğan, **a.g.m.** s. 1408.

⁵²³ Akbulut, **Bilişim Alanında Suçlar** s. 137.

⁵²⁴ İhtiyaroğlu, **a.g.e.** s. 428. Özçelik, **a.g.e.** s. 85.

Her ne kadar kimi yazarlar bilişim sistemine girmek için verilen rızanın kalma eylemini de kapsadığını savunsa⁵²⁵ da kanaatimizce suçun iki seçimlik hareketi için de ayrı ayrı rıza aranmalıdır. Rıza sadece bilişim sistemine girilmesi için verilmiş olmasına rağmen fail girdiği sistemde kalmaya devam ediyorsa burada hukuka uygunluk sebebinin varlığından söz edilemeyecektir⁵²⁶. Örneğin kişisel bilgisayarının açılması için arkadaşına şifresini söyleyen ve özellikle sadece bilgisayarı açması gerektiğini, sistemde yapılacak işlemleri kendisinin bizzat yapacağını ifade eden kişi sadece sisteme girilmesi için rıza vermiştir. Rızanın sisteme girme ya da kalma fiillerinden birisine yönelik olduğu belirtilmediğinde ise iki eylem için de rıza verilmiş olarak kabul edilmelidir⁵²⁷.

Özellikle kurumlara ait bilişim sistemlerinin dışarıdan gelecek saldırılara karşı korunabilmesi için yetkilendirilmiş kişilerce sisteme sızma testleri yapılmaktadır⁵²⁸. Sızma testinin yapılması amacıyla bilişim uzmanları veya beyaz şapkalı hackerlar tarafından bilişim sistemine girilmesi halinde sistem sahibinin rızası söz konusu olacağından suç oluşmayacaktır⁵²⁹. Bir kamu kurumu⁵³⁰ ya da işyerinde çalışan kişilerin o işyerindeki bilgisayar ve diğer bilişim sistemlerine girmelerin halinde de rızanın varlığı söz konusudur. Bu kişilerin çalıştıkları yerlerdeki bilişim sistemlerine erişimleri halinde suç oluşmayacaktır⁵³¹.

Bir kurum ya da şirketteki çalışanlara tahsis edilen bilgisayarların belirlenen kurallara göre kullanılıp kullanılmadığının denetlenmesi amacıyla; bu sistemlere girilmesinin suç oluşturup oluşturmayacağı hususu doktrinde tartışmalıdır. Kurumlar tarafından çalışanlara verilen bilgisayarların bir amacın ifası uğruna tahsis edildiğine ve bu amaç dahilinde kullanılması gerektiğine dikkat çeken yazarlara göre bu

⁵²⁵ Aslında bu görüşlerin gerekçesi maddenin 2016 yılından önceki haline dayanmaktadır. Değişiklikten önce suçun işlenmiş olması için sisteme girildikten sonra kalınmaya devam edilmesi aranmaktaydı. Bu durumda suçun mütemadi suç olduğunu savunan yazarlar sisteme girilmesi ile suçun tamamlanmadığını, rızanın ise suç tamamlanana kadar verilebileceğini savunmaktadır. Yaşar/Artuç/Gökcan, **a.g.e.** s. 7296. Erdoğan, **a.g.m.** s. 1409-1410. Apaydın, **a.g.m.** s. 283.

⁵²⁶ Dülger, **Bilişim Suçları** s. 291. Özçelik, **a.g.e.** s. 82-83.

⁵²⁷ Dülger, **Bilişim Suçları** s. 291.

⁵²⁸ Ahu Karakurt Eren, “Sızma Testleri ile Türk Ceza Kanunu’nun 243, 244 ve 245/A Maddelerinde Düzenlenen Suçlar Arasındaki İlişkinin Değerlendirilmesi”, **Terazi Hukuk Dergisi**, C. 15, S. 164, Nisan 2020, s. 748.

⁵²⁹ Karakurt Eren, **a.g.e.** s. 752.

⁵³⁰ Kimi yazarlara göre bir kamu kurumunda çalışan kişinin memur olmaya hak kazanması nedeniyle verilen şifreyi kullanması durumunda rıza değil kanundan aldığı hakkın/yetkinin kullanılması söz konusudur. Kurt, **a.g.e.** s. 157. Apaydın, **a.g.m.** s. 281.

⁵³¹ Akbulut, **Bilişim Alanında Suçlar** s. 137. Kayaer, **a.g.e.** s. 115-116.

bilgisayarlar üzerinde yapılan denetimler suç oluşturmayacaktır⁵³². Bizim de desteklediğimiz görüşteki yazarlar ise sistemlerin tahsis edildiği kişilere karşı böyle bir denetimin yapılabileceğini kabul etseler de çalışanların bu hususta önceden bilgilendirilmemiş olması halinde rızanın yokluğu nedeniyle suçun oluşacağını ifade etmiştir⁵³³. 657 sayılı Devlet Memurları Kanunu’nun 125/B-e maddesi ile “*Devlete ait resmi araç, gereç ve benzeri eşyayı özel işlerinde kullanmak*” kınama cezasını gerektiren bir disiplin suçu olarak düzenlenmiş; aynı kanunun 10. maddesi amirler, maiyetlerindeki memurların “*hal ve hareketlerini takip ve kontrol etmekle*” görevlendirmiştir⁵³⁴. Buna rağmen memurun rızası olmadan, kamu hizmetinin yürütülmesi ile ilgili olmayan özel yazışmalarını içeren mail adreslerine ya da sosyal medya hesaplarına girilmesi bilişim sistemine girme suçunu oluşturacaktır⁵³⁵.

AIHM de verdiği kararlarda işyerinde kendisine tahsis edilen bilgisayar ve telefonları şahsi yazışmaları için kullandığı gerekçesiyle iletişimi izlenen ve bu gerekçeyle işten çıkarılan başvurucunun AIHS m. 8⁵³⁶ ile güvence altına alınan “*özel yaşamın gizliliği*” hakkının ihlal edildiğine hükmetmiştir⁵³⁷. Mahkemeye göre çalışanın kullandığı telefon ve bilgisayarlara yönelik yapılacak denetim faaliyetlerinin ne şekilde ve neleri kapsayacak biçimde yapılacağının çalışanlara bildirilmesi zorunludur; gizli dinleme ve denetleme yapılmamalıdır⁵³⁸. AYM ise verdiği bir kararda işverenin önceden bildirmesi halinde kurumsal e-postalar üzerinde denetim yapabileceğine hükmetmiştir⁵³⁹.

⁵³² Yaşar/Artuç/Gökcan, **a.g.e.** s. 7297. Apaydın, **a.g.m.** s. 283-284 Doğan, **a.g.e.** s. 297. Güler, **a.g.e.** s. 25.

⁵³³ Akbulut, **Bilişim Alanında Suçlar** s. 139. Tezcan/Erdem/Önok, **a.g.e.** s. 1156-1158. Ekici Şahin/Koruculu, **a.g.e.** s.612. Karakurt Eren, **a.g.e.** s. 753. Özçelik, **a.g.e.** s. 87.

⁵³⁴ Apaydın, **a.g.m.** s. 283-284.

⁵³⁵ Ekici Şahin/Koruculu, **a.g.e.** s.613.

⁵³⁶ **Madde 8/1:** “*Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*” Avrupa Konseyi, **Avrupa İnsan Hakları Sözleşmesi**, https://www.echr.coe.int/documents/convention_tur.pdf (E.T. 16.12.2021)

⁵³⁷ AIHM Büyük Daire, **Bărbulescu v. Romanya**, **Başvuru No: 61496/08**, T. 05.09.2017; AIHM 4. Daire, **Copland v. Birleşik Krallık**, **Başvuru No: 62617/00**, T. 03.04.2017 <https://hudoc.echr.coe.int/> (E.T. 16.12.2021)

⁵³⁸ Hasan Burak Gemalmaz, **Çalışanların İnternet İletişiminin İşverence İzlenmesi Özel Yaşam Hakkına Aykırı mıdır?: AIHM Büyük Dairenin Eylül 2017 Tarihli Barbulescu Kararı**, Lexpera Blog, 0.9.2017, <http://blog.lexpera.com.tr/calisanlarin-internet-iletisiminin-isverence-izlenmesi-ozel-yasam-hakkina-aykiri-midir-aihm-buyuk-dairenin-05-eylul-2017-tarihli-barbulescu-karari/> , E. T. (16.12.2021)

⁵³⁹ “70. İş sözleşmelerinin parçası olan düzenlemeler ile şirket kaynaklarının, bilgisayarların, kurumsal e-posta hesaplarının kişisel amaçlar doğrultusunda kullanımı kesin şekilde yasaklanmış; gerektiğinde yazışmaların ve iletişim kayıtlarının takip edilebileceği ve incelenebileceği hususunda başvurularda gerekli uyarılar ve bilgilendirmeler yapılmıştır. Bunun yanında, kurumsal olmadığı sürece kişisel

Bir bilişim sisteminin açık bırakılması ya da şifre gibi güvenlik önlemleri ile korunmuyor olması o sisteme girme eylemleri için rıza verildiği anlamına gelmemektedir⁵⁴⁰. Örneğin sadece saklaması ve muhafaza etmesi için kişisel bilgisayarını bir komşusuna veren mağdurun bilgisayara giriş için bir şifre belirlemediği gerekçesiyle sisteme girişe rıza verdiği söylenemez⁵⁴¹. Bununla birlikte internet üzerinden kişisel bilgilerin herkese açık bir şekilde yayınlandığı sosyal medya profilleri ve benzeri sayfalara girilmesi durumunda sayfa sahibinin bu bilgileri yayınlanmasına zımnen rıza gösterdiği söylenebilecektir. Rıza mevcut olduğundan bu sayfalara girilmesi TCK m. 243 bağlamında suç oluşmasına sebebiyet vermeyecektir⁵⁴².

Bir kişinin başka bir kişiye sisteme girme ve kalma için verdiği rıza bu kişiler arasındaki şahsi ya da hukuki bir ilişkiye dayanıyor olabilir. Söz konusu şahsi ya da hukuki ilişkinin ortadan kalkması durumunda rızanın dayanağı da ortadan kalkmış olacak ve hukuka uygunluğu sebebinin varlığı da son bulacaktır⁵⁴³. Yargıtay da verdiği kararlarda eşile evli olduğu sırada öğrendiği şifre ile boşandıktan sonra eşinin sosyal medya hesaplarına giren fail⁵⁴⁴ ile çalıştığı iş yerinden ayrıldıktan sonra çalışırken edindiği şifre ile işyerinin bilişim sistemlerine giren fail⁵⁴⁵ açısından rızanın söz konusu olmadığına ve suçun oluşacağına hükmetmiştir.

hesapların ve kişisel iletişim vasıtalarının mesai saatleri içerisinde kullanılma imkânı olmasına ve buna ilişkin bir engel bulunmamasına rağmen, yapılan işin gerekleriyle ilgisi olmayan yazışmaların iş sözleşmelerine aykırı biçimde mesai saatleri içerisinde kurumsal hesaplar üzerinden gerçekleştirildiği anlaşılmaktadır. Bu nedenlerle başvuru sahiplerinin kurumsal e-posta hesapları üzerinden gerçekleştirdikleri kişisel yazışmaların korunması konusunda makul bir beklenti içinde oldukları sonucuna ulaşamaz.” AYM İkinci Bölüm, **Ömür Kara ve Onursal Özbek Kararı, Başvuru No: 2013/4825, T. 24.03.2016** Resmi Gazete S. 29708, T. 10.05.2016, <https://www.resmigazete.gov.tr/eskiler/2016/05/20160510-6.pdf> (E.T. 16.12.2021)

⁵⁴⁰ Yaşar/Artuç/Gökcan, **a.g.e.** s. 7296. Güler, **a.g.e.** s. 24. Ergün, **a.g.e.** s. 90. Gül, **a.g.e.** s. 106.

⁵⁴¹ Apaydın, **a.g.m.** s. 282. Ergün, **a.g.e.** s. 60. İhtiyaroğlu, **a.g.e.** s. 428.

⁵⁴² Kayaer, **a.g.e.** s. 115. Ekici Şahin/Koruculu, **a.g.e.** s.612. Karakehya, **a.g.e.** s. 16.

⁵⁴³ Özçelik, **a.g.e.** s. 83-84.

⁵⁴⁴ “...Sanığın, eski eşi olan mağdura ait facebook şifresini bildiğini ve şifre kırma gibi bir eyleminin olmadığını beyan etmesi, mağdurun, şifresinin kırılarak facebook hesabına giriş yapıldığına dair iddialarını doğrulayan herhangi bir delil bulunmaması karşısında, sanığın sübut bulan bilişim sistemindeki mağdura özel kısma girip, hakkı olmadığı halde sistemde kalmaya devam etme eyleminin TCK'nın 243/1. madde ve fıkrasındaki bilişim sistemine girme ve mağdura ait içeriği özel mesajları okuyup, tarafı olmadığı haberleşme içeriklerini kaydetmesi eyleminin TCK'nın 132/1. madde ve fıkrasındaki haberleşmenin gizliliğini ihlal suçlarını oluşturacağı.” Yar. 12. CD, E. 2019/577, K. 2019/12248, T. 25.12.2019 Aynı yönde bkz. Yar.. 12. CD, E. 2015/2309, K. 2015/15364, T. 14.10.2015 www.lexpera.com.tr (E. T. 16.12.2021)

⁵⁴⁵ “İşten çıkarılmasından önce, ele geçirdiği şifre ile yetkisiz olarak şirket bilgisayarına girerek ... sanığın kendi ikrarı ile sabit olan şifreyle girilebilen şirket bilgisayarına ele geçirdiği şifre ile yetkisiz olarak hukuka aykırı girmesi eyleminin TCK'nın 243/1. maddesine uyan bilişim sistemine girme suçunu

Burada varsayılan rıza kavramına değinilmesi de yerinde olacaktır. Rızasını açıklayamayacak durumda olan ilgilinin, somut olaydaki fiile rıza göstereceğinin varsayılması doktrinde varsayılan rıza olarak adlandırılmaktadır^{546,547}. Rızanın varlığına dair varsayıma somut olayın objektif bir biçimde değerlendirilmesi ile ulaşılmaktadır. Mağdur sonradan failin yapmış olduğu eyleme rıza göstermediğini beyan etmiş olsa dahi failin yerine geçilerek yapılan objektif değerlendirme sonucu rızanın verileceği sonucuna ulaşılıyorsa rızanın var olduğu kabul edilecektir⁵⁴⁸. Bilişim sistemine girme suçu bakımından da varsayılan rızanın uygulanması söz konusu olabilecektir. Örneğin eşine kişisel bilgisayarının ya da sosyal medya hesaplarının şifresini veren mağdurun bundan sonra yapılacak mükerrer girişler için de rıza gösterdiği varsayılabilir. Varsayılan rızaya güvenerek sisteme giriş yapan failin eylemleri hukuka uygun hale geleceğinden faile ceza verilmeyecektir. Bununla birlikte tek seferlik bir işlem yapılması amacıyla bir bilgisayar ya da sosyal medya hesabının şifresinin bir kere söylenmiş olması durumunda sonradan yapılacak mükerrer girişler için rıza verildiği söylenemeyecektir⁵⁴⁹.

Verilen rızaya uygun bir şekilde bilişim sistemine girilmekle birlikte rıza ortadan kalkmasına rağmen sistemde kalınmaya devam edilmesi durumunda da yine suç işlenmiş olacaktır. Zira suç tanımında sadece sistemde kalınması da suç olarak öngörüldüğünden sistem sahibinin iradesinin aksine sistemde kalmaya devam etmek bilişim sistemine girme suçunu oluşturacaktır⁵⁵⁰.

Failin eyleminin hukuka aykırı olup olmadığı fiilin işlendiği anda belirleneceğinden⁵⁵¹; bilişim sistemlerine girilmesi veya kalınması için verilecek rızanın suçun işlendiği anda mevcut olması gerekmektedir. Buradan hareketle, açık veya zımni bir rıza ortada yokken sisteme girilmesi halinde sonradan sistemde kalmak

oluşturacağı” Yar. 12. CD, E. 2014/2525, K. 2014/17259, T. 08.09.2014 <https://legalbank.net> (E.T. 16.12.2021) Aynı yönde bkz. Yar. 11. CD, E. 2009/22385, K. 2012/3683, T. 11.03.2012 kararı aktaran Yaşar/Gökcan/Artuç, **a.g.e.** s. 7303.

⁵⁴⁶ Meral Ekici Şahin, **Ceza Hukukunda Rıza**, İstanbul: On İki Levha Yayınları, 2011 s. 295.

⁵⁴⁷ Koca/Üzülmez’e göre “varsayılan rıza” özel hukuktan ceza hukukuna uyarlanmış “uydurma” bir kavramdır. Bu kavram ile hukuka uygun hale getirilen eylemler çoğunlukla görevin ifası veya hakkın kullanılması çerçevesinde hukuka uygun hale gelmektedir. Koca/Üzülmez, **Genel Hükümler** s. 297-298.

⁵⁴⁸ Zeynel T. Kangal, “*Ceza Hukukunda Varsayılan Rıza*”, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, C. 15, S. 4, Ekim 2011 s. 224-225.

⁵⁴⁹ Tezcan/Erdem/Önok, **a.g.e.** s. 1159.

⁵⁵⁰ Dülger, **Bilişim Suçları** s. 290-291. Güler, **a.g.e.** s. 25. Çetin, **a.g.e.** s.14.

⁵⁵¹ Akbulut, **Bilişim Alanında Suçlar** s. 137.

için rıza alınmış olsa dahi sisteme girme eylemi hukuka aykırı olacağından suç oluşacaktır.⁵⁵².

Ceza yargılaması sırasında rızanın varlığı değerlendirilirken rıza sahibinin iradesini sakatlayan bir nedenin olup olmadığı dikkatle araştırılmalıdır. Zira iradeyi sakatlayan bir durumun mevcudiyeti halinde verilen rıza geçerliliğini kaybedeceğinden suç konusu eylem hukuka aykırı hale gelecektir⁵⁵³. Örneğin tanıtım amacıyla bedava verilen bir uygulama arka planda sisteme erişilmesi için açıklar oluşturuyorsa burada rızadan söz edilemeyecektir⁵⁵⁴.

Bu bölümde üzerinde durulması gereken bir başka konu ise rızanın ispatıdır. Aralarında hukuki ya da şahsi herhangi bir ilişki bulunmayan iki kişi arasında uyumsuzluk var ise bilişim sistemine girme veya orada kalmaya ilişkin rızanın söz konusu olmadığı kabul edilmelidir⁵⁵⁵. Bir bilişim sistemine giren veya sistemde kalmaya devam eden fail eylemlerinin sistem sahibinin rızasına dayandığını iddia ediyorsa bu iddiasını ispatlamalıdır. İspat yükü failin üzerinde olduğundan mağdurdan rıza vermediğini ispatlaması beklenemeyecektir⁵⁵⁶.

D. Suçu Etkileyen Nedenler

Suçun nitelikli unsuru, suçun basit halindeki tipiklik unsuruna eklenerek suçun daha hafif veya ağır sayılmasına ve bu ağırlığa göre cezalandırılmasına yol açan unsurdur. Bu unsurların bulunmaması halinde suçun oluşumu etkilenmeyecek, basit hale göre ceza verilecektir. Söz konusu unsurların suçun basit haline eklenmesi ile suçun nitelikli halleri ortaya çıkmaktadır⁵⁵⁷. Nitelikli hallerin belirlenmesinde eylemin işleniş kriteri olarak alınabileceği gibi; fail ve mağdura göre ya da suçun konusuna göre bir belirleme de yapılabilecektir⁵⁵⁸.

⁵⁵² Dülger, **Bilişim Suçları** s. 291. Apaydın, **a.g.m.** s. 281-82. Hafızoğulları/Özen, **Topluma Karşı Suçlar** s. 448.

⁵⁵³ Dülger, **Bilişim Suçları** s. 291. Erdoğan, **a.g.m.** s. 1408.

⁵⁵⁴ Kurt, **a.g.e.** s. 157.

⁵⁵⁵ Güler, **a.g.e.** s. 24. Parlar/Öztürk, **a.g.e.** s. 29.

⁵⁵⁶ Dülger, **Bilişim Suçları** s. 290. Erdoğan, **a.g.m.** s. 1408. Kurt, **a.g.e.** s. 156-157.

⁵⁵⁷ Dülger, **Genel Hükümler** s. 383. Akbulut, **Genel Hükümler** s. 429-430. Mustafa Özen, **Ceza Hukuku Genel Hükümler Dersleri**, Ankara: Adalet Yayınevi, 2019 s. 542-543.

⁵⁵⁸ Artuk/Gökçen/Alşahin/Çakır, **a.g.e.** s. 381. Dülger, **Genel Hükümler** s. 384.

1. Hafifletici Nedenler

Bilişim sistemine girme suçunu düzenleyen TCK m. 243'ün ikinci fıkrasında “*yukarıdaki fıkra da tanımlanan fiillerin⁵⁵⁹ bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi*” cezada indirim gerektiren nitelikli hal olarak düzenlenmiştir. Bu durumda hâkim tarafından takdir edilecek ceza yarı oranına kadar azaltılacaktır⁵⁶⁰.

Doktrinde kimi yazarlar suçun bu halinin bilişim sistemlerinin güvenliğinin yanı sıra sistem sahibi ve diğer ilgililerin malvarlığını da tehdit ediyor olması sebebiyle basit haline göre daha tehlikeli olduğunu ifade etmiştir. Bu yazarlara göre sistem sahibinin menfaatinin de korunabilmesi için bu fıkra da düzenlenen hal cezayı azaltan değil artıran bir sebep olarak öngörülmelidir⁵⁶¹. Zira bu haliyle madde insanları suç işlemeye teşvik etmektedir⁵⁶².

Bir görüş ise bedeli karşılığı yararlanılabilen sistemlerin değil kamuya açık bilişim sistemlerine girilmesinin cezayı azaltan hal olarak düzenlenmesi gerektiğini savunmuştur⁵⁶³. Kimi yazarlar ise bedeli karşılığı yararlanabilen sistemler söz konusu olduğunda bilişim sisteminin güvenliğini yanı sıra sistemi işletenin sistem üzerindeki haklarının da ihlal edileceğinin ifade ederek cezayı azaltan bir nedene ihtiyaç duyulmadığını savunmuşlardır⁵⁶⁴.

Bir görüş ise nitelikli halin değerlendirilmesi sırasında kanundaki seçimlik eylemlere dayalı ikili bir ayırım yapmaktadır. Tıpkı TCK'nın konut dokunulmazlığının ihlali suçunu düzenleyen 116. maddesinin ikinci fıkrasında olduğu gibi belli sistemlere girilmesi durumunda cezanın azaltılması yönünde bir düzenleme yapılmasında bir sakınca yoktur. Fakat konut dokunulmazlığı suçundan farklı olarak bedeli karşılığı yararlanılabilen bir bilişim sistemde kalınmaya devam edilmesi durumunda ekonomik bir yarar da sağlanmaktadır. Bu görüşe göre kanun koyucu suçun seçimlik hareketleri

⁵⁵⁹ 2016 değişikliği öncesinde suçun sadece “*girme ve kalma*” bileşik hareketi ile işlenebiliyor olması nedeniyle bu fıkra da “*fiillerin*” şeklinde çoğul bir ifade kullanılması doktrinde eleştirilmekteydi. Karagülmez, **a.g.e.** s. 208.

⁵⁶⁰ Akbulut, **Bilişim Alanında Suçlar** s. 140. Yıldız, **Bilişim Sistemine Girme** s. 245. Soyaslan, **Özel Hükümler**, s. 665.

⁵⁶¹ Tezcan/Erdem/Önok, **a.g.e.** s. 1155. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 963. Erdoğan, **a.g.m.** s. 1400. Kayaer, **a.g.e.** s. 111-112.

⁵⁶² İhtiyaroğlu, **a.g.e.** s. 422. Bayındır, **a.g.e.** s. 68-69.

⁵⁶³ Karagülmez, **a.g.e.** s. 210-211.

⁵⁶⁴ Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 963-964.

arasındaki ayrımı gözden kaçırmıştır. Yapılması gereken karşılıksız yararlanma suçu kapsamında bilişim suçları ile ilgili ayrı bir düzenleme yapılmasıdır⁵⁶⁵.

Bizim de görüşlerine katıldığımız ve kanun koyucunun tercihini yerinde bulan yazarlar ise halihazırda sistem sahibinin belli bir bedel karşılığında sistemin güvenliğinde feragat ettiğine dikkat çekmiştir. Bu tür sistemlere girilmesi ile ortaya çıkan haksızlık ve tehlike hiçbir şekilde girilmesi istenmeyen sistemlerde ortaya çıkana nazaran daha azdır⁵⁶⁶. Bazı yazarlara göre ise incelemekte olduğumuz suçun basit halinde bilişim sisteminin güvenliği ile birlikte kişilerin mahremiyeti korunurken; ikinci fıkradaki düzenlemede mahremiyetin yerini ekonomik yarar almış, bu halin cezayı azaltan bir sebep olarak öngörülmesi de yerinde olmuştur⁵⁶⁷.

Kimi yazarlar ise bu düzenlemenin yapılmaması halinde uygulamada bilişim sistemlerine girme suçunun çok geniş bir şekilde görüleceğinden dolayı yaşanabilecek problemlerin önüne geçildiğini ifade etmiştir⁵⁶⁸. Bazı yazarlar ise kanun koyucunun bu fıkradaki suçun cezasını TCK m. 163'te düzenlenen “*karşılıksız yararlanma suçunun*” cezasına yaklaştırmak amacıyla cezanın indirilmesini düzenlediğini öne sürmüşlerdir⁵⁶⁹.

Madde metninde geçen “*bedeli karşılığı yararlanılabilen sistem*” ifadesinin tanımına ve bu halin neden cezayı azalttığına kanunda ya da madde gerekçesinde yer verilmemiş; bu durum kimi yazarlarca eleştirilmiştir⁵⁷⁰. Doktrinde hangi sistemlerin bu kapsama gireceğine ilişkin çeşitli ölçütler çerçevesinde belirlemeler ve örneklendirmeler yapılmıştır. Bununla birlikte bilişim teknolojilerinde yaşanan gelişmelerin hızı dikkate alınarak aşağıda bahsedilecek örneklerle yenilerinin de eklenebileceği unutulmamalıdır⁵⁷¹.

Doktrinde; fıkarda kastedilenin bilişim sistemlerinin bulunduğu mekanlar değil, sistemin içerdiği elektronik yapı üzerinden sunulan hizmetler olduğu ifade

⁵⁶⁵ Akbulut, **Bilişim Alanında Suçlar** s. 142-143. Güler, **a.g.e.** s. 27-28. Benzer görüş için bkz. Özçelik, **a.g.e.** s. 110.

⁵⁶⁶ Koca/Üzülmez, **Özel Hükümler** s. 904. Karakehya, **a.g.e.** s. 17. Kabadayı, **a.g.e.** s.95.

⁵⁶⁷ Artuk/Gökçen/Yenidünya, **a.g.e.** s. 874. Kurt, **a.g.e.** s. 147.

⁵⁶⁸ Yazıcıoğlu, **Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi** s. 407.

⁵⁶⁹ Ketizmen, **a.g.e.** s. 110-111.

⁵⁷⁰ Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 963. Hafızogulları/Özen, **a.g.e.** s. 448-449.

⁵⁷¹ Dülger, **Bilişim Suçları** s. 271

edilmiştir⁵⁷². Buna göre bedeli karşılığı yararlanılan sistem ifadesinden anlaşılması gereken internet kafelerde⁵⁷³ olduğu gibi bir bilişim sisteminin kiralanması değil; belli bir ücret karşılığı bir bilişim sistemi aracılığıyla sunulan hizmetlerden yararlanılmasıdır⁵⁷⁴. Kimi yazarlar ise bu görüşe katılmamakta; fiziki olarak ulaşılabilen ve manuel olarak girilebilen bilişim sistemlerinin de bu fıkra kapsamına girdiğini ve internet kafelerdeki bilgisayarların kullanılması durumunda da TCK m. 243/2'nin uygulanacağını savunmaktadır⁵⁷⁵.

İnternet üzerinden abonelerine ücret karşılığı hizmet sunan tüm web siteleri bu kapsamdadır⁵⁷⁶. Alışveriş siteleri⁵⁷⁷, farklı tür ve konuda dokümanları elektronik arşiv formatında abonelerine sunan web siteleri⁵⁷⁸, ücret karşılığı video oyunlarına erişim imkânı sağlayan platformlar⁵⁷⁹ bu web sitelerine örnek gösterilebilir. Bu tür bir bilişim sistemine ücretini ödeyerek giriş hakkı elde eden kimsenin giriş için gerekli kullanıcı adı ve şifreyi üçüncü kişilerle paylaşması ve üçüncü kişilerin sisteme giriş yapması halinde suç işlenmiş olacaktır⁵⁸⁰.

Bir kuruluş tarafından farklı amaçlarla abonelerin hizmetine sunulan bilişim sistemlerinin de bedeli karşılığı yararlanılan sistemler içerisinde olduğu doktrinde ifade edilmiştir. Örneğin 3. kişilerin akıllı telefonlarına ya da e-posta adreslerine reklam içerikli mesajlar gönderilmesine yarayan sistemler bu kapsamda değerlendirilebilecektir⁵⁸¹. Kullanıcılara belli bir bedel karşılığı sunulan ya da içerdikleri “*kullandığın kadar öde (pay for use)*” özelliği ile abonelerin sadece

⁵⁷² Akbulut, **Bilişim Alanında Suçlar** s. 144. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 963. Parlar, **a.g.e.** s. 22. Şahbaz, **a.g.e.** s. 3133. Fazıl Gürler, **Yargıtay Kararları Işığında Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar**, Ankara: Yetkin, 2015 s. 129.

⁵⁷³ **Madde 2/1-i: “Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan” İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**

⁵⁷⁴ Tezcan/Erdem/Önok, **a.g.e.** s. 1154-1155. Erdoğan, **a.g.m.** s. 1398. Ekici Şahin/Koruculu, **a.g.e.** s. 614. Yazıcıoğlu, **Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi** s. 407. Ketizmen, **a.g.e.** s. 110. Doğan, **a.g.e.** s. 229. Parlar/Öztürk, **a.g.e.** s. 30-31. Kayaer, **a.g.e.** s. 111. Kabadayı, **a.g.e.** s. 92-93.

⁵⁷⁵ Dülger, **Bilişim Suçları** s. 271. Artuk/Gökçen/Yenidünya, **a.g.e.** s. 875. Apaydın, **a.g.m.** s. 270. Mahmutoglu, **a.g.e.** s. 863. Ketizmen, **a.g.e.** s. 111. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7299.

⁵⁷⁶ Dülger, **Bilişim Suçları** s. 270.

⁵⁷⁷ Koca/Üzülmez, **Özel Hükümler** s. 904

⁵⁷⁸ Karagülmez, **a.g.e.** s. 174.

⁵⁷⁹ Karakehya, **a.g.e.** s. 17.

⁵⁸⁰ Tezcan/Erdem/Önok, **a.g.e.** s. 1155.

⁵⁸¹ Dülger, **Bilişim Suçları** s. 270-271.

kullandıkları hizmetlerin bedelini ödediği bulut bilişim sistemleri ve sunucuları da bedeli karşılığında yararlanılabilen sistemler olarak değerlendirilebilecektir⁵⁸².

Ağlar aracılığıyla gerçekleştirilen internet hizmetlerinde yararlanılmasının bu fıkranın uygulama alanında olup olmadığı konusunda da doktrinde görüş ayrılığı vardır. Kimi yazarlar bir ağ üzerinden faydalanılabilen internet hizmetine yetkisiz kişilerce hukuka aykırı olarak erişim sağlanması halinde TCK m. 163/2⁵⁸³'deki karşılıksız yararlanma suçunun oluşacağını savunmaktadır⁵⁸⁴. Bizim de görüşlerine katıldığımız yazarlar ise bedeli karşılığı kullanılabilecek internet ağlarına hukuka aykırı olarak girilmesinin TCK m. 243/2'de düzenlenen bilişim sistemlerine girme suçunun daha az cezayı gerektiren halini oluşturacağını ifade etmişlerdir⁵⁸⁵.

Şifreli yayın yapan kuruluşların sağladıkları yayınların aboneleri tarafından izlenebilmesini sağlayan “şifre çözücü (decoder)” cihazların bilişim sistemi olup olmadığı konusu 765 sayılı TCK döneminde tartışılmış⁵⁸⁶; bu cihazlar bilişim sistemi olarak kabul edilmemiştir⁵⁸⁷. Buna rağmen son yıllarda bilişim ve internet teknolojilerinde yaşanan gelişmelerle birlikte bu durum değişmiştir. Zira günümüzde çoğunlukla şifreli yayınlar internet ağları ve IP üzerinden yapılmakta; IPTV ve Web TV gibi farklı türde sunucular ile bilgisayarlar, tabletler ve akıllı cep telefonları gibi farklı cihazlar üzerinden abonelere hizmet sunulmaktadır. Bu gelişmelerle birlikte televizyonlar telekomünikasyon şebekesi üzerinden aldığı yayını kullanıcılara aktaran cihazlar olmaktan çıkmış; internete bağlanabilen ve bilişim sistemlerinin birçok özelliğini bünyesinde barındıran cihazlar haline gelmiştir. Dolayısıyla şifreli yayınların bilişim sistemleri ve ağları yoluyla yapıldığı hallerde⁵⁸⁸ bu şifrelerin kırıları olarak yayınların izlenmesi durumunda TCK m. 243/2'de yer alan düzenleme

⁵⁸² Turan, **Bulut Bilişim** s. 262.

⁵⁸³ **Madde 163:** “(2) Telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan sahibinin veya zilyedinin rızası olmadan yararlanan kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.”

⁵⁸⁴ Artuk/Gökçen/Yenidünya, **a.g.e.** s. 875. Doğan, **a.g.e.** s. 298. Kayaer, **a.g.e.** s. 111. Zahit Yılmaz/Özge Apış, “Karşılıksız Yararlanma Suçu (TCK m. 163.)”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Prof. Dr. Nur Centel’e Armağan, C. 19, S. 2, 2013 s. 1761,1776.

⁵⁸⁵ Dülger, **Bilişim Suçları** s. 270. Soyaslan, **Özel Hükümler**, s. 666.

⁵⁸⁶ Tartışmalar hakkında ayrıntılı bilgi için bkz. Yazıcıoğlu, **Bilgisayar Suçları** s. 217-219.

⁵⁸⁷ Murat Aydın, “Şifreli Yayınların İzinsiz Toplu Gösterimi Suç Mudur?”, **Yargıtay Dergisi**, C. 22, S. 4, Ekim 1996, s. 500-503. R. Yılmaz Yazıcıoğlu, “Şifreli Yayınların Bilişim Suçları Karşısındaki Konumu”, **Yargıtay Dergisi**, C. 25, S. 1-2, Ocak-Nisan 1999, s. 63-63.

⁵⁸⁸ Kimi yazarlar ise internet yoluyla yapılan yayınların bedeli ödenmeksizin izlenmesi halinde de TCK m. 163/1'de düzenlenen karşılıksız yararlanma suçunun oluşacağını savunmuştur. Tezcan/Erdem/Önok, **a.g.e.** s. 1155. Yılmaz/Apış, **a.g.e.** s. 1760, 1776.

uygulanacaktır. Bununla birlikte şifreli yayın hizmetinin telefon hatları veya frekansları ile elektromanyetik dalgalar kullanılmak suretiyle sağlandığı durumlarda ise TCK m. 163/2’te düzenlenen karşılıksız yararlanma suçu oluşacaktır⁵⁸⁹. Yargıtay da benzer bir tutum sergileyerek verdiği kararlarda telefon frekansları veya elektromanyetik dalgalar aracılığıyla yapılan şifreli yayınların hukuka aykırı olarak izlenmesi halinde bilişim sistemine müdahale edilmediğini, karşılıksız yararlanma suçunun oluşacağını ifade ederken⁵⁹⁰; şifre çözücü cihazın internet üzerinden çalıştığı durumlarda karşılıksız yararlanma suçunun yanında TCK’nın 243. ve 244. maddelerindeki suçların varlığının da tartışılması gerektiğini ifade etmiştir⁵⁹¹.

Otomatlar tarafından sunulan hizmetlerden bedel ödenmeksizin yararlanılması ise incelemekte olduğumuz suçun değil TCK m. 163’teki karşılıksız yararlanma suçunun oluşmasına neden olacaktır⁵⁹². Bir görüş ise halihazırda bilişim sistemlerinin otomatların teknik özelliklerini de bünyelerinde barındırdıklarını ifade etmektedir. Bu görüşe göre bedeli karşılığı kullanılabilen oyun konsolları gibi sistemlerinin hukuka aykırı olarak kullanılması durumunda hem bilişim sistemine girme suçu hem de karşılıksız yararlanma suçu oluşacaktır⁵⁹³.

⁵⁸⁹ Akbulut, **Bilişim Alanında Suçlar** s. 146-147. Güler, **a.g.e.** s. 29. Özçelik, **a.g.e.** s. 60-61.

⁵⁹⁰ “Katılanın tek yönlü olarak frekanslarla veya elektromanyetik dalgalar aracılığıyla yaptığı şifreli yayının sanığa ait uydu alıcısına (decoder) ulaşması üzerine gerekli donanım ve yazılım kullanılarak kartın şifre çözme kabiliyetinin internet ortamından paylaşılması suretiyle şifreli yayınların sanık aracılığıyla başkaları tarafından şifresiz olarak izlenmesinin sağlandığı olayda, katılan tarafından kullanılan bilişim sistemine herhangi bir müdahalede bulunulmadığı anlaşıldığından eylemin 5237 sayılı TCK’nın 163/2. maddesinde düzenlenen karşılıksız yararlanma suçunu oluşturduğu gözetilmeden yazılı şekilde hüküm kurulması, Bozmayı gerektirmiş, “ Yar. 2. CD. E. 2014/17258, K. 2015/22546, T. 07.12.2015 Aynı yönde bkz. Yar. 8. CD, E. 2013/16698, K. 2014/17652, T. 07.07.2014 www.lexpera.com.tr (E. T. 18.12.2021)

⁵⁹¹ “...(D.) sistemine üye olanlara verilen akıllı kartlar, Card Sharing sistemi içerisinde kullanılmadan ve devre dışı bırakılarak yayınlar izlenebilmektedir. Akıllı kartların kontrolü yapmasını sağlayan şifreleme sistemini devre dışı bırakmak için, sistem internete bağlanmakta ve akıllı kartın sağladığı doğrulamayı (...org) internet sitesini kullanarak aşmaktadır. Bu sistemde akıllı kartların yapması gereken kontroller, internet üzerinden sağlanan bilgiler sayesinde aşılmaktadır. Bahsolunan siteye belli kullanıcı adı/şifreler ile bağlanılarak bu bilgiler alınabilmektedir... Bedeli karşılığında izlenmesi gereken şifreli televizyon yayınlarının, sahibinin rızasına aykırı olarak bedelsiz şekilde izlenmesini sağlamak eyleminde TCK’nun 163/2. maddesinde düzenlenen “karşılıksız yararlanma” suçunun unsurlarının oluştuğu, ancak TCK’nun 44. maddesinde yazılı işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır hükmü gereğince, sanığın eyleminin TCK’nun 243 veya 244. maddelerinde gösterilen suçu oluşturduğunun belirlenmesi durumunda, eylemin tek olduğu ancak iki farklı suçun oluştuğu da gözetilip, eyleminin uyduğu maddedeki cezalar ile TCK’nun 163/2. maddesinde yazılı cezanın karşılaştırılması suretiyle TCK’nun 44. maddesi de gözetilerek sonucuna göre sanığın hukuki durumunun belirlenmesi gerektiğinin gözetilmemesi” Yar. 11. CD, E. 2012/439, K. 2013/16403, T. 11.11.2013 https://legalbank.net (E.T. 18.12.2021)

⁵⁹² Dülger, **Bilişim Suçları** s. 271. Soyaslan, **Özel Hükümler**, s. 666. Karagülmez, **a.g.e.** s. 204. Yenidünya, **a.g.e.** s. 1040. Erdoğan, **a.g.m.** s.1398. Demircan, **a.g.e.** s. 79. Çetin, **a.g.e.** s. 8,16.

⁵⁹³ Özçelik, **a.g.e.** s. 59.

Bilişim sisteminden yararlanmanın bedeli çoğunlukla para olsa da başka türlü bir bedelin belirlenmiş olması da söz konusu olabilmektedir. Burada önemli olan nokta sisteme giriş yetkisi verilmesi için bir karşılık isteniyor olmasıdır⁵⁹⁴. Örneğin bir internet sitesi kullanıcılarından ücret almayıp sistemin kullanımı karşılığında belli sayıda abone getirmelerini isteyebilmektedir. Online yayın hizmeti sunan bir yayınevi de kitaplarını ya da makalelerini yayınladığı yazarlara bu yayınlar karşılığı sistemini açabilmektedir⁵⁹⁵. Bedel hizmet alınmadan önce ödenebileceği gibi hizmet sırasında ya da sonradan da ödenebilmektedir. Bu durum suçun oluşumu açısından bir fark teşkil etmemektedir⁵⁹⁶.

TCK m. 243/2'deki hükmün uygulanması için bedeli karşılığı faydalanılabilen bir sisteme girilmesi veya sistemde kalınması gerekmektedir. Bunun dışında sisteme ya da verilere müdahale edilmesi halinde TCK m. 244'te düzenlenen suçlar da işlenmiş olacaktır. Kimi yazarlar bu durumda iki farklı suç oluşacağını savunsa⁵⁹⁷ da Yargıtay, kararlarında sadece TCK m. 244'teki suçun oluştuğuna hükmetmektedir.

2. Ağırlaştırıcı Nedenler

Çalışmamıza konu suçun daha fazla cezayı gerektiren haline ilişkin TCK'da bir düzenleme bulunmamaktadır. Bununla birlikte Terörle Mücadele Kanunu'nun "*terör amacı ile işlenen suçlar*" başlıklı 4. maddesinde bilişim sistemine girme suçunun terör örgütü faaliyeti çerçevesinde işlenmesi durumunda terör suçu olarak sayılacağı düzenlenmiştir. Yine aynı kanunun 5. maddesinde "*3 ve 4'üncü maddelerde yazılı suçları işleyenler hakkında ilgili kanunlara göre tayin edilecek hapis cezaları veya adlî para cezaları yarı oranında artırılarak hükmolunur.*" denilerek; terör amacı ile işlenen bilişim sistemine girme suçunun cezasının artırılacağı düzenlenmiştir. Yine aynı maddede bu şekilde cezanın artırılması halinde belirlenen cezanın suç için maddede öngörülen ceza üst sınırını aşabileceği belirtilmiştir.

Terörle Mücadele Kanunu'nun 5. maddesine 2010 yılında eklenen⁵⁹⁸ fıkrada ise maddeye sınırlama getirilerek cezanın artırılmasına ilişkin hükümlerin çocuklar

⁵⁹⁴ Kayaer, **a.g.e.** s. 112. Şahbaz, **a.g.e.** s. 3133. Özçelik, **a.g.e.** s. 62. Parlar/Öztürk, **a.g.e.** s. 31.

⁵⁹⁵ Dülger, **Bilişim Suçları** s. 271-272. Akbulut, **Bilişim Alanında Suçlar** s. 144. Apaydın, **a.g.m.** s. 272. Erdoğan, **a.g.m.** s. 1397. Karagülmez, **a.g.e.** s. 210. Apiş, **a.g.e.** s. 60.

⁵⁹⁶ Karagülmez, **a.g.e.** s. 101. Kayaer, **a.g.e.** s. 112.

⁵⁹⁷ Yıldız, **Bilişim Sistemine Girme** s. 246.

⁵⁹⁸ Resmî Gazete, **Terörle Mücadele Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun** <https://www.resmigazete.gov.tr/eskiler/2010/07/20100725-1.htm> (E.T. 18.12.2021)

hakkında uygulanmayacağı düzenlenmiştir. Özetle bilişim sistemine girme suçunun 18 yaşını doldurmuş kimseler tarafından terör amacıyla işlenmesi halinde verilecek olan ceza artırılabilecektir⁵⁹⁹.

Terörle Mücadele Kanunu'nda yer alan anılan düzenlemeler haricinde bilişim sistemine girme suçunun cezasını artıran hallere ilişkin ne TCK ne de diğer kanunlarda bir düzenleme bulunmaktadır. Buna rağmen doktrinde suçun konusuna göre cezanın artırılabilmesi ifade edilerek kamu kurumlarına ait sistemler ile özel kişilere ait bilişim sistemleri arasında farklı cezaları öngören bir düzenleme getirilmesi gerektiği savunulmuştur⁶⁰⁰. Buna göre kamu kurumlarına ait ya da devletin güvenliği ile ilgili sistemler gibi bazı sistemlerine karşı suçun işlenmesi durumunda cezanın artırılmasına yönelik bir kanuni düzenleme yapılmalıdır⁶⁰¹. Güvenlik önemleri ile özel olarak koruma altına alınmış bilişim sistemlerine girilmesinin de ağırlaştırıcı sebep olarak düzenlenmesini savunan yazarlar bulunmaktadır⁶⁰². Bunun yanında ikinci fıkraya ilişkin açıklamalarımızı yaparken de değindiğimiz gibi; kimi yazarlar da suçun bedeli karşılığı yararlanılabilen sistemlere karşı işlenmesinin cezayı ağırlaştıran haller arasında düzenlenmesinin yerinde olacağını savunmuştur⁶⁰³.

E. Suçun Netice Sebebiyle Ağırlaşmış Hali

Belli bir suçun icrası kapsamında gerçekleştirilen fiilin kastedilen neticeden daha ağır ve farklı bir neticeyi meydana getirmesi halinde netice sebebiyle ağırlaşmış suç söz konusu olacaktır. Kanun koyucu burada icra edilmek istenen suç bakımından kast, ortaya çıkan netice bakımından ise taksirli hareketi aramaktadır⁶⁰⁴.

İncelemekte olduğumuz suç düzenleyen TCK m. 243'ün üçüncü fıkrasında maddedeki fiilin işlenmesi nedeniyle sistemdeki verilerin yok edilmesi veya değiştirilmesi durumunda fail hakkında altı aydan iki yıla kadar hapis cezası verileceği

⁵⁹⁹ Dülger, **Bilişim Suçları** s. 277.

⁶⁰⁰ Erdoğan, **a.g.m.**, s.1400. Ketizmen, **a.g.e.**, s.110.

⁶⁰¹ Akbulut, **Bilişim Alanında Suçlar** s. 143. Dülger, **Bilişim Suçları** s. 275.

⁶⁰² Dülger, **Bilişim Suçları** s. 275. Ketizmen, **a.g.e.** s. 110. Erdoğan, **a.g.m.** s. 1400.

⁶⁰³ Dülger, **Bilişim Suçları** s. 275. Tezcan/Erdem/Önok, **a.g.e.** s. 1155. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 963. Erdoğan, **a.g.m.** s. 1400. İhtiyaroğlu, **a.g.e.** s. 422.

⁶⁰⁴ Koca/Üzülmez, **Genel Hükümler** s. 242-244. Özen, **a.g.e.** s. 361-364.

düzenlenmiştir. Bu düzenlemeyi suçun nitelikli hali⁶⁰⁵ ya da münferit bir suç⁶⁰⁶ olarak nitelendiren yazarlar bulunmaktadır. Fakat kanun koyucunun madde gerekçesinde⁶⁰⁷ vurguladığı ve doktrinde çoğunluğun da iştirak ettiği üzere bu hal suçun neticesi sebebiyle ağırlaştırılmış halidir⁶⁰⁸. Kanun koyucu bu fıkra ile suçun basit halinden farklı olarak sistemdeki verilerin tehlikeye girmesini ayrıca cezalandırmayı tercih etmiştir. Bu fıkra ile korunmak istenen değer sistemdeki verilerin güvenliğidir⁶⁰⁹.

Bilişim sistemine girme fiili ile verilerin yok olması arasında nedensellik bağı olması yeterli olup failin neticeyi ayrıca istemesine gerek yoktur⁶¹⁰. Kanun gerekçesinde de değinildiği üzere fail, taksirli hareketiyle sistemdeki verilerin değişmesine ya da yok olmasına yol açarsa bu fıkra düzenlenen suç oluşacaktır⁶¹¹. Bu fıkra düzenlenen halin meydana gelebilmesi için fail sisteme girme veya kalma fiillerini kasten icra etmeli, verileri yok etme veya değişmesi neticeleri açısından taksirle hareket etmelidir⁶¹². Bir başka ifadeyle fail kasten bilişim sistemine girmeli ardından ise taksirli hareketleriyle sistemin içerisindeki verilerin değişmesine ya da yok olmasına yol açmalıdır⁶¹³. Bu yönüyle TCK m. 243/3'ün “*gerçek netice sebebiyle ağırlaşan suç*”⁶¹⁴ olduğu söylenebilir⁶¹⁵.

⁶⁰⁵ Karakehya, **a.g.e.** s. 18. Esen, **a.g.e.** s. 630. Kurt, **a.g.e.** s. 153. Soyaslan hem “*ağırlatıcı sebep*” hem de “*neticesi sebebiyle ağırlaştırılmış hal*” ifadelerini kullanmıştır. Soyaslan, **Özel Hükümler**, s. 666.

Erdağ, **a.g.e.** s.282. “*TCK m. 243/3 münferit bir suç olarak daha özelbir ifadeyle neticesi sebebiyle ağırlaştırılmış bir suç olarak kabul etmek gerekmektedir. Çünkü cezai müeyyide altına alınan hareket tek başına tek başına bilişim sistemine girme ve orda kalma değil, bu hareket dolayısıyla sistemde yer alan bir verinin yok edilmesi ve değiştirilmesidir.*” Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 961.

⁶⁰⁷ “*Üçüncü fıkra, bu suçun neticesi sebebiyle ağırlaştırılmış hâli düzenlenmiştir. Birinci fıkra tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi hâlinde failin, suçun temel şekline nazaran daha ağır ceza ile cezalandırılması öngörülmüştür. Dikkat edilmelidir ki, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir.*” **Türk Ceza Kanunu Madde Gerekçeleri** www.lexpera.com.tr (E. T. 19.12.2021)

⁶⁰⁸ Akbulut, **Bilişim Alanında Suçlar**, s. 148-149. Dülger, **Bilişim Suçları** s. 276. Tezcan/Erdem/Önok, **a.g.e.** s. 1154. Artuk/Gökçen/Yenidünya, **a.g.e.** s. 877. Soyaslan, **Özel Hükümler**, s. 666. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7297. Özçelik, **a.g.e.** s. 111-112. Doğan, **a.g.e.** s. 298. Güler, **a.g.e.** s. 30. Kurt, **a.g.e.** s. 152. Erdoğan, **a.g.m.** s. 1402. Meran, **a.g.e.** s. 566. Şahbaz, **a.g.e.** s. 3133.

⁶⁰⁹ Koca/Üzülmez, **Özel Hükümler** s. 896.

⁶¹⁰ Akbulut, **Bilişim Alanında Suçlar**, s. 149. Yıldız, **Bilişim Sistemine Girme** s. 247. Hafizoğulları/Özen, **Topluma Karşı Suçlar** s. 449.

⁶¹¹ Koca/Üzülmez, **Özel Hükümler** s. 905.

⁶¹² Dülger, **Bilişim Suçları** s. 268. Apış, **a.g.e.** s. 65. Özçelik, **a.g.e.** s. 112. Şahbaz, **a.g.e.** s. 3133.

⁶¹³ Dülger, **Bilişim Suçları** s. 291. Özçelik, **a.g.e.** s. 77. A Apaydın, **a.g.m.** s. 277-278.

⁶¹⁴ Failin kastedilenden daha ağır bir neticeye sebep olması halinde gerçek; failin istediği neticenin yanında başka bir neticeye sebep olması halinde ise gerçek olmayan neticesi sebebiyle ağırlaştırılmış suç söz konusu olacaktır. Veli Özer Özbek, “*Neticesi Sebebiyle Ağırlaştırılmış Suçlar*”, **Ceza Hukuku Dergisi**, C. 2, S. 4, Ağustos 2007 s. 228.

⁶¹⁵ Koca/Üzülmez, **Özel Hükümler** s. 905. Kayaer, **a.g.e.** s. 116. Kurt, **a.g.e.** s. 159.

Failin sistemdeki verileri değiştirmek ya da yok etmek kastıyla hareket etmesi halinde ise TCK m. 244/2⁶¹⁶’de düzenlenen “*verilerin yok edilmesi veya değiştirilmesi suçu*” oluşacaktır⁶¹⁷. Bununla birlikte kimi yazarlar iki düzenlemeye birden kanunda yer verilmesinin uygulamada karışıklıklara yol açabileceğini ifade etmişlerdir. Bu yazarlara göre muhtemel karışıklıkların önüne geçilebilmesi için TCK’nın 243. ve 244. maddeleri tek madde olarak düzenlenmeli; bilişim sistemine girme fiili suçun basit hali, diğer fiiller ise suçun nitelikli halleri olarak düzenlenmelidir⁶¹⁸.

Birinci fıkradaki hareketlerin seçimlik olmasına paralel olarak; suçun neticesi sebebiyle ağırlaşan halinin ortaya çıkabilmesi için de neticeler seçimlik olarak düzenlemiştir. Failin icra edeceği fiil sebebiyle verilerin “*yok edilmesi*” veya “*değişmesi*” neticelerinden birinin ortaya çıkması suçun oluşumu için yeterli olacaktır⁶¹⁹.

Madde metninde geçen ve bu fıkradaki halin konusu olan veri ifadesinin kanunda bir tanımı yapılmamış olsa da kanun gerekçesinde⁶²⁰ sistemde bulunan soyut ve sayısal tüm bileşenlerin kavramın kapsamı içerisinde bulunduğu ifade edilmektedir. Buradan yola çıkılarak kanun koyucunun veri kavramını teknik anlamının ötesinde oldukça geniş yorumlandığı söylenebilecektir⁶²¹.

Suç sebebiyle değişen ya da yok olan veriler sistemin temel işleyişinde önemli bir yer tutan yazılıma ilişkin veriler olabileceği gibi sistem işleyişini etkilemeyen, ikincil önemde de olabilirler⁶²². Bu durum kimi yazarlarca eleştirilmiş; sistem ve kullanıcılar için daha fazla önem arz eden verilerle diğer veriler arasında bir ayırım yapılması gerektiği belirtilmiştir⁶²³. Bir görüş ise verilerin önemine ilişkin bir ayırımın

⁶¹⁶ **Madde 244:** “(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kalan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.” **Türk Ceza Kanunu**

⁶¹⁷ Akbulut, **Bilişim Alanında Suçlar**, s. 149. Yıldız, **Bilişim Sistemine Girme** s. 247. Hafızoğulları/Özen, **Topluma Karşı Suçlar** s. 449. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7302. Yenidünya, **a.g.e.** s. 1035. Erdağ **a.g.e.** s. 284. Ekici Şahin/Koruculu, **a.g.e.** s. 617. Güler, **a.g.e.** s. 30. Ketizmen, **a.g.e.** s. 111. Taşdemir, **a.g.e.** s. 262. Erdağ, **a.g.e.** s. 284.

⁶¹⁸ Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 962.

⁶¹⁹ Dülger, **Bilişim Suçları** s. 267. Yıldız, **Bilişim Sistemine Girme** s. 246. Gül, **a.g.e.** s. s.109. Parlar/Öztürk, **a.g.e.** s. 32.

⁶²⁰ “Sistem içindeki bütün soyut unsurlar, fıkra da geçen ‘veri’ teriminin kapsamındadır” **Türk Ceza Kanunu Madde Gerekçeleri** www.lexpera.com.tr (E. T. 19.12.2021)

⁶²¹ Özçelik, **a.g.e.** s. 63.

⁶²² Koca/Üzülmüş, **Özel Hükümler** s. 905. Tezcan/Erdem/Önok, **a.g.e.** s. 1154. Yıldız, **Bilişim Sistemine Girme** s. 246-247. Ekici Şahin/Koruculu, **a.g.e.** s. 617-618.

⁶²³ Karagülmez, **a.g.e.** s. 232.

normatif olarak yapılmasının mümkün olmadığını; hâkimin TCK m. 61'in uygulaması sırasında bu durumu dikkate almasının daha yerinde olacağını ifade etmiştir⁶²⁴.

TCK m. 243/3 ile adeta TCK m. 244/2'de düzenlenen “*verilerin yok edilmesi veya değiştirilmesi*” suçunun taksirli halinin düzenlendiği öne sürülmüştür. Bunun yanında TCK m. 244/1'de düzenlenen “*bilişim sisteminin işleyişinin engelleme veya bozma*” suçunun taksirle işlenmesi hali için herhangi bir düzenleme yapılmamıştır. Buradan yola çıkan bir görüşe göre kanunun mevcut halinde ancak bilişim sisteminin işleyişini etkilemeyecek veri ve yazılımların zarar görmesi veya değişmesi halinde TCK m. 243/3 uygulanabilecektir⁶²⁵.

Bedeli karşılığı yararlanılabilen bir bilişim sistemine girilmesi sonucu sistemdeki verilerin zarar görmesi ya da değişmesi halinde de yine üçüncü fıkra hükmü uygulanacaktır. Zira kanun netice sebebiyle ağırlaşmış halin uygulanmasında ikinci fıkra bir istisna tanımamıştır⁶²⁶.

V. SUÇLARIN BİRLEŞMESİ VE İŞTİRAK

A. Suçların Birleşmesi

Ceza hukukunda kural işlenen suç sayısının ceza verilmesi sonucunu doğuran gerçek içtima kurallarının uygulanmasıdır. Bu durumun istisnaları ise kanunla belirlenen hallerde ortaya çıkan ve birden fazla suç karşılığında tek bir ceza verilmesi sonucunu doğuran bileşik suç, zincirleme suç ve fıkri içtima halleridir⁶²⁷.

Seçimlik hareketli suçlarda kanunda gösterilen hareketlerden birinin yapılmış olması suçun oluşması için yeterli olup diğer hareketlerin yapılmasına ihtiyaç duyulmamaktadır. Bununla birlikte seçimlik hareketlerin tamamının veya birkaçının beraber yapılması halinde de yine tek bir suç oluşacak ve içtima kuralları uygulanmayacaktır⁶²⁸. O halde bir bilişim sistemine girilmesi ve sistemde kalınmaya devam edilmesi halinde tek bir suçun oluşması söz konusu olacak; faile yalnızca bir

⁶²⁴ Dülger, **Bilişim Suçları** s. 268-269.

⁶²⁵ Özçelik, **a.g.e.** s. 63-64.

⁶²⁶ Akbulut, **Bilişim Alanında Suçlar**, s. 149. Koca/Üzülmez, **Özel Hükümler** s. 905. Tezcan/Erdem/Önok, **a.g.e.** s. 1154. Hafizoğulları/Özen, **Topluma Karşı Suçlar** s. 449. Özçelik, **a.g.e.** s. 124-125.

⁶²⁷ Koca/Üzülmez, **Genel Hükümler** s. 505-506. Demirbaş, **a.g.e.** s. 566.

⁶²⁸ Dönmezer/Erman, **a.g.e.**, s. 86. Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 225.

ceza verilecektir. 243. maddenin üçüncü fıkrasında düzenlenen netice sebebiyle ağırlaşan halin gerçekleşmesi durumunda da iki ayrı ceza verilmesi söz konusu olmayıp sadece üçüncü fıkrada belirtilen ceza verilecektir⁶²⁹.

Hedef sisteme ait bir şekilde girildikten sonra sistemin içerisindeki yine bilişim sistemi vasfı taşıyan bölümlere girilmesi halinde de tek bir suç oluşacaktır. Her ne kadar ayırık fillerin konusunun farklı olduğu düşünülebilecek olsa da burada tek bir suç işleme kararı ve fiil mevcuttur. Örneğin bir kimsenin kişisel bilgisayarına rızası dışında giren fail, bu bilgisayarda bulunan e-posta hesabına ya da farklı klasörlere girdiği takdirde tek bir bilişim sistemine girme suçu işlenmiş olacaktır⁶³⁰.

Bir suçun bir başka suçun ağırlaştırıcı nedeni ya da unsuru olarak düzenlenmesi durumunda bileşik suç meydana gelecektir. TCK m. 42'ye göre bu durumda tek bir suç meydana geleceğinden içtima hükümleri uygulanmayacaktır⁶³¹. Bilişim sisteminin kullanılması yoluyla hırsızlık (TCK m. 142/2-e) ve bilişim sisteminin araç olarak kullanılması yoluyla dolandırıcılık (TCK m. 158/1-f) suçlarında bilişim sisteminin kullanımı nitelikli hal olarak düzenlenmiştir. Bu suçların işleme kararı kapsamında bilişim sistemine hukuka aykırı şekilde girilmesi halinde bileşik suçun varlığı söz konusu olacağından TCK m. 243 gereğince ceza verilmeyecektir⁶³². Yargıtay da verdiği kararlarda bir bütün halinde bilişim sisteminin araç olarak kullanılması yoluyla hırsızlık ya da dolandırıcılık suçlarının oluşması durumunda ayrıca TCK m. 243'ten dolayı ceza verilmemesi gerektiğine hükmetmiştir⁶³³.

Bir suç işleme kararının icrası kapsamında bir kişiye karşı farklı zamanlarda aynı suçun işlenmesi durumunda zincirleme suç meydana gelecektir. Aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi⁶³⁴ halinde de yine zincirleme suç

⁶²⁹ Yıldız, **Bilişim Sistemine Girme** s. 247-248.

⁶³⁰ Özçelik, **a.g.e.** s. 125.

⁶³¹ Koca/Üzülmez, **Genel Hükümler** s. 553. Demirbaş, **a.g.e.** s. 570.

⁶³² Tezcan/Erdem/Önok, **a.g.e.** s. 1160-1161. Mahmutoglu, **a.g.e.** s. 864. Ekici Şahin/Koruculu, **a.g.e.** s. 619. Kayaer, **a.g.e.** s. 121-122. Gül, **a.g.e.** s.113. Semiz, **a.g.e.** s. 74. İhtiyaroğlu, **a.g.e.** s. 432.

⁶³³ “Sanığın, müştekiye ait banka hesabından internet bankacılığı yolu ile tanık ... adına kayıtlı hesaba 1.000,00 TL EFT işlemi gerçekleştirip akabinde bankamatikten kart ile, transfer ettiği parayı çekme biçiminde gerçekleşen eyleminin bir bütün halinde hırsızlık suçunu oluşturduğu gözetilmeden, sanığın cezalandırılma olanağı bulunmayan 5237 sayılı TCK'nın 243/1. maddesi uyarınca yazılı şekilde mahkûmiyetine karar verilmesi...bozmayı gerektirmiş...” Yar. 17. CD, E. 2016/10724, K. 2018/12290, T. 10.10.2018 Aynı yönde bkz. Yar. 13. CD, E. 2012/13503, K. 2014/16411, T. 06.05.2014; Yar. 13. CD, E. 2014/2924, K. 2014/36282, T. 18.12.2014; Yar. 13. CD, E. 2014/23539, K. 2015/8515, T. 06.05.2015 <https://legalbank.net> (E.T. 21.12.2021)

⁶³⁴ Tek bir fiille aynı suçun birden fazla kişiye karşı işlenmesi doktrinde “aynı neviden fikri içtima” olarak da adlandırılmaktadır. Demirbaş, **a.g.e.** s. 589-590. Akbulut, **Genel Hükümler** s. 898. Dülger, **Genel Hükümler** s. 777. Özçelik, **a.g.e.** s. 127.

oluşacaktır⁶³⁵. Bu durumda işlenen suç sayısına bakılmaksızın tek bir ceza öngörülecek; bu ceza ise suç için TCK'da belirlenen cezanın dörtte birinden dörtte üçüne kadar artırılmış hali olacaktır⁶³⁶.

Bilişim sistemine girme suçu bakımından da TCK m. 43'teki şartların oluşması halinde zincirleme suça ilişkin hükümler uygulanacaktır. Bir bilişim korsanının belli aralıklarla aynı sisteme defalarca girmesi durumu zincirleme suça örnek olarak gösterilebilir⁶³⁷. Failin aynı suç işleme kararının kapsamına giremeyecek derecede uzun aralıklarla bir sisteme girmesi halinde ise zincirleme suça ilişkin hükümlerin uygulanmasının mümkün olmayacağı yazarlarca ifade edilmiştir⁶³⁸. Bir görüş ise süre konusunda net bir kriter getirmenin sağlıklı olmadığını ifade ederek failin sisteme tekrar girebilmek oluşturduğu arka kapıları kullanarak farklı zamanlarda sisteme girdiği hallerde de zincirleme suçun söz konusu olabileceğini savunmuştur⁶³⁹.

Neticenin taksirle gerçekleşmiş olması durumunda incelemekte olduğumuz suçun netice sebebiyle ağırlaşmış haline de zincirleme suç hükümleri uygulanacaktır⁶⁴⁰. Her ne kadar biz bu görüşe katılmasak da kimi yazarlar tek bir fiille birden fazla bilişim sistemine girmenin mümkün olamayacağı gerekçesiyle TCK m. 43/2'nin bu suç için uygulanmasının mümkün olmadığını ifade etmektedir⁶⁴¹.

Farklı neviden fikri içtimanın düzenlendiği TCK m. 44'e göre tek bir fiille birden çok suçun işlenmiş olması durumunda faile yalnızca kanunda daha ağır ceza öngörülen suçtan dolayı ceza verilecektir⁶⁴². Farklı suçlar ifadesinden TCK'nın farklı maddeleri kastedilmemekte; aynı maddede düzenlenen farklı suçların beraber işlenmesi halinde de fikri içtima mümkün olmaktadır⁶⁴³.

Bilişim suçu olarak sınıflandırılan suçların işlenebilmesi için çoğunlukla ilk olarak suç konusu bilişim sistemine girilmesi gerekmektedir⁶⁴⁴. Bu durumda

⁶³⁵ Dönmezer/Erman, **a.g.e.**, s. 658-659. Koca/Üzülmez, **Genel Hükümler** s. 517-518. İçel, **Ceza Hukuku Genel Hükümler**, s. 596-597. Akbulut, **Genel Hükümler** s.874.

⁶³⁶ Demirbaş, **a.g.e.** s. 572.

⁶³⁷ Yıldız, **Bilişim Sistemine Girme** s. 248. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 966. Soyaslan, **Özel Hükümler**, s. 665. Kayaer, **a.g.e.** s. 119.

⁶³⁸ Dülger, **Bilişim Suçları** s. 302 Erdoğan, **a.g.m.** s.1417. Güler, **a.g.e.** s. 32-33.

⁶³⁹ Özçelik, **a.g.e.** s. 126.

⁶⁴⁰ Akbulut, **Bilişim Alanında Suçlar**, s. 152.

⁶⁴¹ Yaşar/Gökcan/Artuç, **a.g.e.** s. 7301.

⁶⁴² Dönmezer/Erman, **a.g.e.**, s. 681-687. Koca/Üzülmez, **Genel Hükümler** s. 532. İçel, **Ceza Hukuku Genel Hükümler**, s. 579.

⁶⁴³ Dülger, **Genel Hükümler** s. 782-783.

⁶⁴⁴ Dülger, **Bilişim Suçları** s. 302. Soyaslan, **Özel Hükümler**, s. 665.

incelemekte olduğumuz suç diğer bilişim suçlarının işlenebilmesi amacıyla bir araç (geçit⁶⁴⁵) suç olarak karşımıza çıkmakta ve bu suçlar arasındaki içtima ilişkisinin nasıl olacağı sorusu akıllara gelmektedir.

Kimi yazarlar amaç suç-arac suç ilişkisini bulunduğu durumlarda suçların icra hareketler örtüşüyorsa fikri içtima; suçlara sebebiyet veren fiiller farklı ise gerçek içtima kurallarının uygulanacağını ifade etmiştir⁶⁴⁶. Bu kapsamda bir başkasının bilişim sistemine giren failin sistemde kalmaya devam ederek mağdurun özel yazışmalarını ya da fotoğraflarını görmesi durumunda fikri içtima hükümleri uygulanacaktır. Bir başka ifadeyle bilişim sistemine girme suçundan değil sadece haberleşmenin gizliliğini ihlal (TCK m. 132) ve özel hayatın gizliliğini ihlal (TCK m. 134) suçlarından ceza verilecektir. Öte yandan fail sisteme girdikten sonra sistem sahibine ait verileri kendisine ait bir harici depolama aygıtına kaydediyorsa burada gerçek içtima hükümleri uygulanacak; bilişim sistemine girme ve kişisel verilerin ele geçirilmesi (TCK m. 136) suçları için ayrı ayrı ceza verilecektir⁶⁴⁷. Kimi yazarlar ise ikinci durumda her ne kadar bu iki suçu oluşturan fiiller örtüşmese de verileri ele geçirme suçunun bilişim sistemine girme suçundaki haksızlık içeriğini de kapsadığını ifade ederek; yalnızca verileri ele geçirme suçundan dolayı ceza verilmesi gerektiğini ifade etmişlerdir⁶⁴⁸. Bir görüş ise bilişim sistemine girme suçunun başka bir suçun araç suçu olarak işlenmesi halinde; bilişim sistemine girme suçunun diğer ve daha ağır suçun içerisinde eridiğini ve sadece amaç suç için ceza verilmesi gerektiğini savunmaktadır⁶⁴⁹. Kimi yazarlar ise bilişim sistemine girme suçuyla birlikte kişisel verilerin ele geçirilmesi ve kaydedilmesinin yanı sıra haberleşmenin ya da özel hayatın gizliliğinin ihlal edilmesi durumlarında da iki ayrı fiilin söz konusu olduğunu ifade etmektedir⁶⁵⁰. Bu yazarlara göre gerçek içtima kuralları uygulanmalı ve fail her suç bakımından ayrıca cezalandırılmalıdır⁶⁵¹.

⁶⁴⁵ Dönmezer/Erman'a göre fail ve mağdurun aynı olması, failin hareketinin hafiften ağıra doğru giden bir süreç izlemesi, hareketlerin aynı hukuki menfaate yönelik olması, iki suçun neticesinin aynı harekete nedensellik bağı ile bağlanması ve failin hareketi kasten yapmış olması halinde geçitli suç oluşacaktır. Bu durumda fail sadece daha ağır cezayı gerektiren suçtan sorumlu tutulacaktır. Dönmezer/Erman, **a.g.e.**, s. 649-650.

⁶⁴⁶ Koca/Üzülmez, **Özel Hükümler** s. 906. Özçelik, **a.g.e.** s. 134,140.

⁶⁴⁷ Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 966. Kayaer, **a.g.e.** s. 119-120.

⁶⁴⁸ Tezcan/Erdem/Önok, **a.g.e.** s. 1161.

⁶⁴⁹ Artuk/Gökçen/Yenidünya, **a.g.e.** s. 878. Yenidünya, **a.g.e.** s.1039. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7301. Taşkın, **a.g.e.** s. 34. Taşdemir, **a.g.e.** s. 261. Şahbaz, **a.g.e.** s. 3131. Parlar, **a.g.e.** s. 21.

⁶⁵⁰ Tezcan/Erdem/Önok, **a.g.e.** s. 1161.

⁶⁵¹ Yıldız, **Bilişim Sistemine Girme** s. 249. Soyaslan, **Özel Hükümler**, s. 665.

Yargıtay ise verdiği kararlarda failin bilişim sistemine girmenin yanında farklı suçların icrasına yönelik filleri de icra etmesi halinde kanuni şartları oluşturan tüm suçlar bakımından ayrı ayrı cezalandırılması gerektiğine hükmederek geçit suç ya da fikri içtimaya dayalı yaklaşımları benimsemediğini göstermiştir⁶⁵². Özellikle bir kimsenin bilişim sistemine girilerek bu sistem üzerinden başka kişilere karşı dolandırıcılık suçunun işlenmesi durumunda yüksek mahkemenin faili hem bilişim sistemine girme hem de bilişim sisteminin araç olarak kullanılması suretiyle dolandırıcılık suçlarından dolayı cezalandırdığı görülmektedir⁶⁵³.

Biz de Yargıtayca da benimsenen ilk görüşe katılmakta ve çalışmamıza konu suçun bir başka suçun işlenmesi için araç suç olarak icra edilmesi halinde fillerin örtüşüp örtüşmediğinin değerlendirilmesi gerektiğini savunmaktayız. Şayet iki suçun işlendiği fiiller birbiriyle örtüşüyorsa TCK m. 44 uygulanmalı ve yalnızca amaç suç için faile ceza verilmelidir. Failin araç ve amaç suçu farklı filleri icra etmesi durumunda ise gerçek içtima uygulanarak iki suç için de ayrıca ceza verilmelidir.

Suçların birleşmesi başlığı altında TCK m. 244'te düzenlenen “*sistemi engelleme, bozma, verileri yok etme veya değiştirme*” suçlarına özellikle değinilmesi

⁶⁵² “Sanık hakkında düzenlenen iddianamede; sanığın, mağdura ait facebook ve telefon hesaplarına rızası dışında girerek bilişim sistemine girme, mağdurun orijinal fotoğrafları ile birlikte çıplaklık içeren fotoğrafları mağdura aitmiş gibi internette paylaşarak görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçlarını işlediği iddia edilmiş olup, sanığa yüklenen farklı eylemlerden dolayı ayrı ayrı hüküm kurulması gerektiği, TCK’nın 44/1. madde ve fıkrasındaki fikri içtima koşullarının bulunmadığı gözetilmeden, ‘bilişim sistemlerine girme ve özel hayatın gizliliğini ihlal suçlarının sabit olmakla birlikte tek bir eylem ile icra edildiğinden TCK’nın 44. maddesinin bu suçlar yönünden tatbik edilmesine’ biçimindeki yasal ve yeterli olmayan gerekçelerle yazılı şekilde görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçundan mahkumiyet hükmü kurulması,” Yar. 12. CD, E. 2018/8261, K. 2019/6852, T. 29.05.2019 Aynı yönde bkz. Yar. 4. CD, E. 2014/2222, K. 2015/24755, T. 18.03.2015; Yar. 12. CD, E. 2014/15082, K. 2015/1624, T. 02.02.2015 <https://legalbank.net> (E.T. 21.12.2021)

⁶⁵³ “Sanığın kendisine başka bir hesaptan para geleceğini söyleyerek şikayetçi A.. T..’den akrabası A.. T..’e ait olan ve emaneten kullanmakta olduğu bankamatik kartını aldığı, daha sonra 15.03.2007 tarihinde şikayetçi S.. K..’a ait MSN hesabına hukuka aykırı olarak girerek bu kişiye ait arkadaş listesinde bulunan şikayetçi S.. H.. ile yazışma yaptığı, bu yazışmada kendisini asıl hesap sahibi olan S.. K.. gibi takdim ederek para istediği, şikayetçi S..’ın da bir arkadaşı vasıtasıyla, sanığın belirtmiş olduğu A.. T..’e ait bankamatik kartına 250 TL para gönderdiği, sanığın bu suretle şikayetçi S..’ı yanıltarak haksız menfaat temin ettiği, Aynı şekilde 21.03.2007 tarihinde bu defa şikayetçi L.. K..’nın MSN hesabına hukuka aykırı şekilde girerek birlikte iş yaptığı mağdur A.. Ş..’dan 10.000 TL para talep ettiği, mağdur A..’ın para temin etme cihetine gittiği, ancak sanığın yazışmalardaki üslubu ve ısrarı üzerine şüphelenen mağdur A..’ın şikayetçi L..’i araması üzerine durumun anlaşıldığı ve eylemin teşebbüs aşamasında kaldığı, bu suretle sanığın mağdur A..’ı yanıltarak haksız menfaat temin etmeye teşebbüs ettiği kabul olunan olayda; Sanığın mağdurlar S.. ve A..’a yönelik eylemlerinin nitelikli dolandırıcılık, mağdurlar L.. ve S..’a yönelik eylemlerinin ise bilişim sistemine girme suçlarını oluşturduğuna yönelik kabulde bir isabetsizlik görülmemiştir. ” Yar. 23. CD, E. 2015/3995, K. 2015/6595, T. 16.11.2015 Aynı yönde bkz. Yar. 15. CD, E. 2013/74, K. 2014/14216, T. 09.09.2014; Yar. 15. CE, E. 2015/11595, K. 2015/28323, T. 09.09.2015; Yar. 15. CD, E. 2016/2793, K. 2016/7012, T. 22.09.2016 <https://legalbank.net> (E.T. 21.12.2021)

yerinde olacaktır. Her ne kadar bu suçların bilişim sistemine girilmeksizin işlenmesi mümkün olsa da çoğunlukla bilişim sistemine girilerek işlendikleri görülmektedir. TCK m. 244'te düzenlenmiş olan suçlar ile bilişim sistemine girme suçu söz konusu olduğunda fikri içtima uygulanıp uygulanmayacağı konusunda doktrinde fikir ayrılıkları bulunmaktadır.

Kimi yazarlar bilişim sistemine girme ve sistemde kalma eyleminin TCK m. 244'teki suçların unsuru haline geldiğini ifade ederek sadece TCK m. 244 gereğince ceza verilmesini gerektiğini savunmuştur⁶⁵⁴. Bilişim sistemine girme suçunun işlenmesinde icra edilen fiil ile TCK'nın 244. maddesindeki suçların fiillerinin örtüştüğünü savunan görüşe göre ise bu iki madde arasında fikri içtima ilişkisi bulunmaktadır. O halde failin sadece sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarından cezalandırılması gerekmektedir⁶⁵⁵. Bir görüş ise failin kastının esas alınması gerektiğini ifade etmiş; TCK m. 244'te düzenlenen eylemler bakımından kastla hareket eden failin bilişim sistemine girse dahi bu eyleminden dolayı TCK m. 243'ten dolayı cezalandırılmaması gerektiğini savunmuştur⁶⁵⁶. Kimi yazarlar ise suçlara sebep olan fiiller farklı olmasına rağmen korunan hukuki menfaatin ortak olmasının iki düzenleme arasında asli norm-tali norm ilişkisi kurduğunu ifade etmişlerdir. Bu durumda yapılması gereken TCK m. 44 gereğince fikri içtima uygulanarak failin TCK m. 244 gereğince cezalandırılmasıdır⁶⁵⁷. Bir başka görüş ise bu durumda iki ayrı suçun bulunduğu ifade ederek gerçek içtima uygulanarak faile iki suçtan dolayı iki farklı ceza verilmesi gerektiğini ifade etmiştir⁶⁵⁸.

Kimi yazarlar ise TCK m. 244'teki eylemlerin işlenmesi için bilişim sistemine girilmesinin bir zorunluluk olması durumunda fikri içtima, böyle bir zorunluluğun bulunmaması halinde ise gerçek içtima uygulanması gerektiğini savunmuştur⁶⁵⁹. Bizce de bu görüş isabetlidir. Somut olaya bakıldığında failin TCK m. 244'teki suçları işlemesi için bilişim sistemine girme suçunu da işlemesi gerekiyorsa fikri içtima uygulanmalı ve faile yalnızca TCK m. 244'teki ilgili hükümden ceza verilmelidir. Bununla birlikte fail, TCK m. 244'teki suçu işlemesi için bilişim sistemine girmesi

⁶⁵⁴ Doğan, **a.g.e.** s. 300. Karagülmez, **a.g.e.** s. 241.

⁶⁵⁵ Koca/Üzülmez, **Özel Hükümler** s. 906. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7301. Güler, **a.g.e.** s. 33-34.

⁶⁵⁶ Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 966. Tezcan/Erdem/Önok, **a.g.e.** s. 1160. Gül, **a.g.e.** s. 112-113.

⁶⁵⁷ Yıldız, **Bilişim Sistemine Girme** s. 248.

⁶⁵⁸ Meran, **a.g.e.** s. 588.

⁶⁵⁹ Özçelik, **a.g.e.** s. 138-139. Kayaer, **a.g.e.** s. 120-121.

gerekeceği halde ayrıca sisteme girme ve kalma fiillerini de icra ediyorsa gerçek içtima söz konusu olacaktır. Bu halde faile TCK m. 243 m. 244 gereğince iki ayrı ceza verilecektir.

Yargıtayın ise bu konudaki kararları arasında farklılık olduğu görülmektedir. Yüksek mahkeme kimi kararlarında TCK m. 244'teki suçların işlenmesi halinde bilişim sistemine girilmiş olsa bile sadece anılan madde gereğince ceza verilmesine hükmederken⁶⁶⁰ kimi kararlarında ise faile ayrıca TCK m. 243 gereğince de ceza verilmesine karar vermiştir⁶⁶¹.

TCK m. 243 ile TCK m. 244 arasındaki uygulamada ortaya çıkan karışıklığın giderilmesi için doktrinde bu suçların tek madde olarak düzenlenmesi gerektiği ifade edilmiştir. Bu görüşteki yazarlara göre bilişim sistemine girme eylemi suçun temel şekli, diğer haller ise nitelikli hal olarak düzenlenirse uygulamada ortaya çıkan karışıklığın da önüne geçilecektir⁶⁶².

Bu başlık altında son olarak 2016 yılında TCK'ya eklenen 245A maddesi ile düzenlenen “yasak cihaz veya programlar” suçuna değinilmesi yerinde olacaktır. Kanun koyucu bu madde ile bilişim suçları ile bilişim sistemlerinin kullanılması yoluyla işlenen suçların icra edilebilmesi için oluşturulan cihazlar, bilgisayar programları, şifreler ve benzeri güvenlik kodlarının yapılması veya oluşturulmasının önüne geçmek istemiş; bunları bulunduran, başka kişilere veren, satın alan, satan, satışa arz eden, kabul eden, nakil veya sevk eden, ithal eden veya üreten kişilerin cezalandırılacağını düzenlemiştir.

⁶⁶⁰ “Mağdura ait elektronik postaya bağlı facebook hesabının şifresini ele geçirerek bu adrese giren, yazışmalar yapan ve şifreyi değiştirmek suretiyle mağdurun amlan hesaba erişimini engelleyen sanığın eyleminin, TCK'nun 244/2. maddesinde düzenlenen suçu oluşturacağı gözetilmeden eksik ceza tayini,” Yar. 8. CD, E. 2015/9713, K. 2016/1868, T. 18.02.2016 Aynı yönde bkz. Yar. 4. CD, E. 2013/19106, K. 2014/14018, T. 28.04.2014; Yar. 8. CE, E. 018/11204, K. 2020/9307, T. 10.02.2020; Yar. 12. CD, E. 2016/10818, K. 2017/7390, T. 11.10.2017; Yar. 15. CD, E. 2017/31912, K. 2018/2652, T. 17.04.2018 <https://legalbank.net> (E.T. 21.12.2021)

⁶⁶¹ “Sanığın katılan ...'in hesaplarının şifresini ele geçirip, ardından şifreleri değiştirmesi şeklindeki eylemi ile şikayetçi ...'dan para istemesi eyleminin iki ayrı suçu oluşturması karşısında; TCK'nın 44. maddesinin uygulanma imkanının bulunmadığı, ... tebliğnamedeki TCK'nın 243/1 maddesi gereğince bozma isteyen düşünceye iştirik edilmemiş olup, sanığın katılan ...'in e posta adresinin ve facebook hesabının şifresini kırması, ardından da şifreyi değiştirmesi şeklindeki eyleminden dolayı TCK'nın 244/2 maddesinde düzenlenen bilişim sistemindeki verileri bozma yoketme, erişilmez kılma, sisteme veri yerleştirme suçundan da mahkumiyet kararı verilmesi gerekirken yazılı şekilde hüküm kurulması” Yar. 15. CD, E. 2017/31912, K. 2018/2652, T. 17.04.2018 Aynı yönde bkz. Yar. 4. CD, E. 2013/19106, K. 2014/14018, T. 28.04.2014; Yar. 8. CD, E. 2016/104, K. 2016/7753, T. 13.06.2016 www.lexpera.com.tr (E. T. 21.12.2021)

⁶⁶² Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 966.

TCK m. 245A’da düzenlenen suç, bilişim sistemlerine girme suçu başta olmak üzere bilişim suçlarının işlenmesine zemin hazırlamak amacıyla icra edilmektedir. Bilişim sistemine girme suçunu işlemek için yasak cihaz veya programlar üreten ya da satın alan failin bu cihaz ya da programlama bilişim sistemine girme suçunu işlemesi halinde gerçek içtima uygulanacaktır. Yani faile TCK m. 243 ve TK m. 245A gereğince iki ayrı ceza verilecektir⁶⁶³. Benzer şekilde FSEK’in “*teknolojik önlemleri etkisiz kılma*” başlıklı 72. maddesi ile de TCK m. 245A benzeri bir düzenleme yapılmıştır. Buradaki suçun bilişim sistemine girme suçunun hazırlık hareketi olarak işlenmesi durumunda da gerçek içtima uygulanacak ve her iki suç yönünden de faile ceza verilecektir⁶⁶⁴.

B. İştirak

Tek bir kimsenin işleyebileceği bir suçun birden fazla kişi tarafından önceden iş birliği yapılmak suretiyle birlikte suç işleme kararı kapsamında işlenmesi halinde iştirak söz konusu olmakta; bu şekilde işlenen suçlara ise “*iştirak halinde suçlar*” denilmektedir⁶⁶⁵. TCK’da suça iştirak kavramı faillik ve şerikliği kapsayan bir üst kavram olarak kabul edilmektedir⁶⁶⁶.

Suçun birden fazla fail tarafından beraber işlenmesi; faillerin suçun kanuni tanımında bulunan fiil üzerinde ortaklaşa hakimiyet kurmaları durumunda bu kişilere müşterek fail denmektedir⁶⁶⁷. Bir suçun işlenmesinde başka bir kimsenin araç olarak kullanılması halinde ise dolaylı faillik söz konusu olacaktır⁶⁶⁸. Failin suç işlemeye azmettirilmesi yahut faile suç işleme kararında ve kararın icrasında yardım edilmesi ise şeriklik kapsamında değerlendirilmektedir. Bu durumda azmettiren ve yardım edenler fail olarak kabul edilmeseler de cezalandırılacaklardır⁶⁶⁹.

⁶⁶³ Akbulut, **Bilişim Alanında Suçlar**, s. 153. Eylem Aksoy Retornaz, “Yasak Cihaz veya Programlar”, **Özel Ceza Hukuku C. VIII: Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ile Bilişim Alanındaki Suçlar**, İstanbul: On İki Levha Yayıncılık 2020 s. 322. İbrahim Korkmaz, “Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu”, **Terazi Hukuk Dergisi**, C. 13, S. 142, Haziran 2018, s. 53. Özçelik, **a.g.e.** s. 135.

⁶⁶⁴ Özçelik, **a.g.e.** s. 135.

⁶⁶⁵ Dönmezer/Erman, **a.g.e.**, s. 746. Demirbaş, **a.g.e.** s. 526. Akbulut, **Genel Hükümler** s.751.

⁶⁶⁶ Koca/Üzülmez, **Genel Hükümler** s. 449. Demirbaş, **a.g.e.** s. 530. Artuk/Gökçen/Alşahin/Çakır, **a.g.e.** s. 723.

⁶⁶⁷ Koca/Üzülmez, **Genel Hükümler** s. 452-453. Baş Bayraktaroğlu, **a.g.e.** s. 119.

⁶⁶⁸ Baş Bayraktaroğlu, **a.g.e.** s. 113-114.

⁶⁶⁹ Koca/Üzülmez, **Genel Hükümler** s. 473. Akbulut, **Genel Hükümler** s. 793.

Bilişim sistemine girme veya kalma suçunun, iştirak yönünden özel ve ayrık bir yönü yoktur. Suça iştirak konusundaki genel hükümler bu suç için de uygulanacaktır⁶⁷⁰. Yani bilişim sistemine girme suçunun işlenmesi sırasında azmettirme, asıl/dolaylı faillik, müşterek faillik ve suça yardım etme mümkündür⁶⁷¹.

Özellikle bilişim teknolojileri ve sistemleri hakkında yeterli bilgi ve deneyime sahip olmayan kişilerin bu konuların uzmanlarınca bilişim sistemine girmeye veya sistemde kalmaya teşvik edilmeleri halinde azmettirme söz konusu olacaktır⁶⁷². Hakkın kullanılması veya ilgilinin rızası nedeniyle sahip olduğu bilişim sistemine girme yetkisini sistem sahibinin rızasına aykırı olarak bir başkasına veren kişinin de azmettiren veya yardım eden olarak sorumluluğu doğacaktır⁶⁷³.

Sistemde kalmaya devam etme açısından da azmettirme dışındaki iştirak şekillerinin meydana gelmesi mümkündür. Zira fail bilişim sisteminden çıktığı ama kadar suç temadi edecek ve tamamlanmayacaktır. Bu süre zarfında başka kimselerin de fail ya da şerik sıfatıyla suça dahil olması mümkündür⁶⁷⁴.

Bir bilişim sistemine üçüncü kişilerin girebilmeleri amacıyla sistemde açık oluşturan failin de sonradan işlenecek suçlarla iştirak hükümlerince sorumlu olup olmayacağına değinmek gerekmektedir. Sistemde açık meydana getiren kimsenin sonradan işlenen suçlar bakımından iştiraken sorumlu olacağı söylenebilse dahi failliğin şerikliğe asaleti nedeniyle TCK m. 244 ve TCK m. 245A gereğince fail olarak sorumluluğu söz konusu olacaktır⁶⁷⁵.

VI. YAPTIRIM VE YARGILAMA

A. Yaptırım

Ceza kanununda suç olarak düzenlenen fiili icra eden faile uygulanan yaptırıma ceza denir. Bu yaptırım devlet tarafından belirlenen özel infaz şekillerine göre

⁶⁷⁰ Koca/Üzülmmez, **Özel Hükümler** s. 906. Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 966. Dülger, **Bilişim Suçları** s. 301. Yıldız, **Bilişim Sistemine Girme** s. 249. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7300. Şahbaz, **a.g.e.** s. 3130.

⁶⁷¹ Akbulut, **Bilişim Alanında Suçlar**, s. 151-152. Soyaslan, **Özel Hükümler**, s. 665. Apaydın, **a.g.m.** s. 288. Parlar/Öztürk, **a.g.e.** s. 29.

⁶⁷² Karakehya, **a.g.e.** s. 19.

⁶⁷³ Özçelik, **a.g.e.** s. 121.

⁶⁷⁴ Dülger, **Bilişim Suçları** s. 2301-302. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7300. Çetin, **a.g.e.** s. 20.

⁶⁷⁵ Özçelik, **a.g.e.** s. 122.

uygulanır⁶⁷⁶. Suçun oluşması halinde faile verilecek cezaları düzenleyen TCK'nın 45. maddesinde hapis cezası ve adli para cezası olarak iki tür ceza öngörülmüştür⁶⁷⁷.

İncelemekte olduğumuz suçun düzenlendiği TCK'nın 243. maddesinde suç işlediği sabit olan faile “*bir yıla kadar hapis ya da adli para cezası*” verileceği düzenlenmiştir. Maddede hapis ve adli para cezası seçimlik ceza şeklinde öngörüldüğünden faile bu iki cezadan ancak birisi verilebilecektir⁶⁷⁸. Yargıtay da verdiği bir kararda bu durumu vurgulamış ve faile hapis cezası ile adli para cezasının beraber verilmesini kanun yararına bozma nedeni olarak görmüştür⁶⁷⁹. TCK m. 49 gereğince hapis cezasının alt sınırı bir ay; TCK m. 49 ve m. 61/9 gereğince adli para cezasının alt sınırı ise otuz gün olarak belirlenmiştir. Bu durumda hâkim TCK'nın 61. maddesine göre değerlendirmesini yapacak ve verilecek cezanın türü ile miktarını belirleyecektir⁶⁸⁰. Verilecek hapis cezası iki yılın altında olduğu takdirde CMK m. 231 gereğince hükmün açıklanmasının geri bırakılmasına karar verilebilecektir⁶⁸¹.

TCK'nın 50. maddesinin ikinci fıkrasına göre hükmedilen hapis cezasının adli para cezasına çevrilmesi mümkün olmayacaktır. TCK m. 58/3'e göre yargılama konusu suç tekerrür kapsamında sonraki (tekrar eden) suç olarak işlenmişse sadece hapis cezası verilebilecektir⁶⁸².

Bilişim sistemine girme suçunun bedeli karşılığı faydalanılabilen sistemlere karşı işlenmesi durumunu düzenleyen TCK m. 243/2 “*ceza yarı oranına kadar indirilir*” düzenlenmiştir. Burada kanun koyucu hâkime indirim oranı konusunda bir takdir yetkisi tanımamıştır⁶⁸³. İlk olarak birinci fıkraya göre bir ceza belirlenmeli, ardından bu ceza yarı oranına indirilmelidir⁶⁸⁴.

⁶⁷⁶ Özbek/Doğan/Bacaksız, **Genel Hükümler** s. 583. Akbulut, **Genel Hükümler** s.925.

⁶⁷⁷ Demirbaş, **a.g.e.** s. 609. Artuk/Gökçen/Alşahin/Çakır, **a.g.e.** s. 833.

⁶⁷⁸ Koca/Üzülmez, **Özel Hükümler** s. 907. Dülger, **Bilişim Suçları** s. 307.

⁶⁷⁹ “*incelenen dosya içeriğine göre, 5237 sayılı Türk Ceza Kanunu'nun 243/1. maddesinde; hapis ve para cezalarının seçimlik olarak öngörüldüğü gözetilmeden, her ikisine de hükmolunması isabetsiz olup, kanun yararına bozma istemine atfen düzenlenen ihbarnamede yer alan düşünce yerinde görüldüğünden, Balıkesir 1. Sulh Ceza Mahkemesinin 07.05.2010 gün ve 2009/1431 esas, 2010/338 sayılı kararının CMK'nun 309. maddesi uyarınca bozulmasına*” Yar. 11. CD, E. 2011/3398, K. 2012/4441, T. 29.03.2012 www.lexpera.com.tr (E. T. 22.12.2021)

⁶⁸⁰ Akbulut, **Bilişim Alanında Suçlar**, s. 153-154. Yıldız, **Bilişim Sistemine Girme** s. 250. Hafizoğulları/Özen, **Topluma Karşı Suçlar** s. 448.

⁶⁸¹ Güler, **a.g.e.** s. 35.

⁶⁸² Koca/Üzülmez, **Özel Hükümler** s. 907. Şahbaz, **a.g.e.** s. 3124.

⁶⁸³ Aksi görüş için bkz. Akbulut, **Bilişim Alanında Suçlar**, s. 154.

⁶⁸⁴ Koca/Üzülmez, **Özel Hükümler** s. 907. Yaşar/Gökcan/Artuç, **a.g.e.** s. 7302.

Terörle Mücadele Kanunu’nun 4. ve 5. maddelerine göre bilişim sistemine girme suçu bir terör örgütünün faaliyetleri çerçevesinde işlendiği takdirde verilecek hapis ya da adli para cezası yarı oranında artırılacaktır. Yine aynı kanunun 5. maddesine göre verilecek ceza TCK m. 243’te üst sınır olarak düzenlenen bir yılı aşabilecektir. Bu durumda hâkim öncelikle TCK 243’e göre temel cezayı belirleyecek; ardından ise hapis veya adli para cezasına esas aldığı gün sayısı üzerinden cezayı yarı oranında artıracaktır⁶⁸⁵.

TCK m. 243/3 gereğince bilişim sistemine girme suçunun işlenmesi nedeniyle sistemdeki verilerin yok olması veya değişmesi halinde ise faile “*altı aydan iki yıla kadar hapis cezası*” verilecektir. Burada kanun koyucu TCK m. 244/2’ye paralel bir düzenleme yapmış ve sadece hapis cezası verilebileceğini hükme bağlamıştır. Suçun neticesi sebebiyle ağırlaşmış hali bakımından adli para cezası verilmesi mümkün değildir⁶⁸⁶.

TCK m. 246’ya göre bilişim suçlarının bir tüzel kişi yararına işlenmiş olması halinde tüzel kişilere özgü güvenlik tedbirleri uygulanabilecektir. Çalışma konusu suçun işlenmesi ile menfaat temin ettiği tespit edilen tüzel kişi hakkında TCK’nın 60. maddesinde düzenlenen güvenlik tedbirlerine hükmedilebilecektir⁶⁸⁷.

B. Yargılama

İncelemekte olduğumuz suç şikâyeteye bağlı bir suç olarak düzenlenmemiştir. Bilişim sistemine girme suçu; mağdurun, suçtan zarar görenin ya da üçüncü kişilerin şikâyeti aranmaksızın re’sen soruşturulur ve kovuşturulur⁶⁸⁸. Kimi yazarlar suçun işlenmesi halinde faile verilmesi gereken ceza miktarı göz önüne alındığında suçun şikâyeteye bağlı olarak düzenlenmesinin daha uygun olacağını ifade etmiştir⁶⁸⁹. Bizim de katıldığımız görüşe göre ise suçla bilişim sisteminin güvenliğinin ve buradan yola çıkarak tüm toplumu korunmak istendiği dikkate alındığında re’sen soruşturulan bir suç olarak düzenlenmesi yerinde olmuştur⁶⁹⁰.

⁶⁸⁵ Akbulut, **Bilişim Alanında Suçlar**, s. 154. Gül, **a.g.e.** s. 115.

⁶⁸⁶ Akbulut, **Bilişim Alanında Suçlar**, s. 154-155. Dülger, **Bilişim Suçları** s. 307. Özçelik, **a.g.e.** s. 144.

⁶⁸⁷ Yıldız, **Bilişim Sistemine Girme** s. 250.

⁶⁸⁸ Özbek/Doğan/Bacaksız, **Özel Hükümler** s. 967. Dülger, **Bilişim Suçları** s. 307.

⁶⁸⁹ Koca/Üzülmez, **Özel Hükümler** s. 907.

⁶⁹⁰ İhtiyaroğlu, **a.g.e.** s. 434. Özçelik, **a.g.e.** s. 145.

Bilişim sistemine girme suçunun sırf hareket suçu olması nedeniyle suçun işlendiği yer hareketin meydana geldiği yer olarak belirlenecektir⁶⁹¹. Bir bilişim sistemine fiziki olarak ulaşılarak girilmesi durumunda yetkili yargı mercii suçun işlendiği yerdeki yargı merciidir. İnternet gibi kablolu bir ağ üzerinden bağlanılarak fiilin icra edilmesi halinde ise failin yerini tespit etmek her zaman mümkün olmayabilir. Bu durumda suçun işlendiği yerin tespit edilebiliyorsa yetkili yargı yerleri de bu yerde mahkemeler ve savcılıklar olacaktır. Şayet tespit edilmezse suçun konusu olan sistemin bulunduğu yerdeki yargı mercii yetkili olacaktır⁶⁹². Uygulamada genellikle sistemin bulunduğu yer savcılık ve mahkemelerinin yargı yetkilerini kullandıkları görülmektedir. Bununla birlikte özellikle sosyal medya platformları ve web sitelerinde hesaplara yönelik işlenen suçlarda bu platformların yurtdışı merkezli olduğu düşünüldüğünde fiilin işlendiği ülkelerdeki savcılık ve mahkemelerin yetkiye ilişkin kurallarının önemi de artmaktadır⁶⁹³.

Bilişim sistemine girme suçunun basit, daha az cezayı gerektiren ve neticesi sebebiyle ağırlaşmış hali bakımından görevli mahkeme Adli Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev Ve Yetkileri Hakkında Kanun m. 11. ve m. 12. gereğince asliye ceza mahkemeleri olarak belirlenmiştir. Yine aynı kanunun 9. maddesi ile özel kanunlarda aksine bir hüküm olmadığı takdirde Hakimler ve Savcılar Kuruluna ihtisaslaşmanın sağlanması amacıyla birden fazla ceza mahkemesinin olduğu yerlerde daireler arası iş bölümünü belirleme yetkisi verilmiştir. Hakimler ve Savcılar Kurulu ise 30.11.2021 tarihinde Resmî Gazete’de yayınlanan kararı ile bu yetkisini kullanmış; iki veya daha fazla ağır ceza mahkemesi ve asliye ceza mahkemesi bulunan yerlerde belli daireleri bilişim suçları bakımından ihtisas dairesi olarak belirlemiştir. Anılan kararın I-4. maddesinde bilişim suçları da ihtisas mahkemelerinin görev alanına giren suçlar arasında sayılmıştır. Sonuç olarak bilişim sistemine girme suçu açısından 15.12.2021 tarihinden itibaren açılacak davalarda anılan kararda belirtilen asliye ceza mahkemeleri görevli olacaktır.

Kanaatimizce bilişim suçları için ihtisas mahkemelerinin kurulması yerinde olmuştur. Anlaşılması için belli bir düzeyde teknik bilgi ve birikim gerektiren, aynı

⁶⁹¹ Akbulut, **Bilişim Alanında Suçlar**, s. 156.

⁶⁹² Yaşar/Gökcan/Artuç, **a.g.e.** s. 7303. Güler, **a.g.e.** s. 36.

⁶⁹³ Dülger, **Bilişim Suçları** s. 308.

zamanda kendine özgü farklılıkları olan bilişim suçlarının yargılama süreçlerinin alanında ihtisaslaşmış hakimlerce sürdürülmesi olumlu bir değişikliktir.

17.10.2019 tarihli ve 7188 sayılı kanunun⁶⁹⁴ 24. maddesi ile yeniden düzenlenen CMK m. 251'e göre "*asliye ceza mahkemesince, iddianamenin kabulünden sonra adli para cezasını ve/veya üst sınırı iki yıl veya daha az süreli hapis cezasını gerektiren suçlarda*" basit yargılama usulünün uygulanmasına karar verilebilecektir. Bu kapsamda çalışma konusu suçu düzenleyen TCK m. 243'ün üç fıkrası da anılan düzenleme kapsamına girmektedir. Anılan maddedeki diğer koşulların da sağlanıyor olması halinde bilişim sistemine girme suçunun yargılama süreci CMK'daki basit yargılama usulüne ilişkin kurallar kapsamında yürüyebilecektir⁶⁹⁵. Bu usulde mahkeme, iddianameyi kabul ettikten sonra 15 gün içinde sanık, şikayetçi ve mağdura tebliğ edecek; iddianameyi tebliğ alan taraflar ise beyanlarını 15 gün içinde mahkemeye yazılı olacak sunacaktır. Akabinde mahkeme, cumhuriyet savcısının görüşü alınmaksızın dosya üzerinden karar verecektir. Bu halde TCK m. 61'e göre tayin edilecek ceza dörtte bir oranında indirilecektir. Mahkemece verilen hükme süresi içinde itiraz edilmediği takdirde hüküm kesinleşecektir. İtiraz edilmesi halinde ise kararı veren mahkemece duruşma açılacak ve genel hükümler dahilinde yargılamaya devam edilecektir⁶⁹⁶.

Bu başlık altında son olarak uzlaştırma konusuna değinmek yerinde olacaktır. Uzlaştırma kurumunun düzenlendiği CMK m. 253/1-c'ye göre mağdurun tüzel kişi sanığın ise suça sürüklenen çocuk olması halinde hapis cezasının üst sınırı üç yılı geçmeyen suçlar da uzlaştırma kapsamına girmektedir. Yani suça sürüklenen çocuklar tarafından işlenen bilişim sistemine girme suçunun yargılamasına başlanmadan önce taraflar uzlaştırma yoluna sevk edilmelidir⁶⁹⁷.

⁶⁹⁴ Resmi Gazete, **7188 Sayılı Ceza Muhakemesi Kanunu Ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun**, S. 30928, T. 24.10.2019 <https://www.resmigazete.gov.tr/eskiler/2019/10/20191024-25.htm> (E.T. 22.12.2021)

⁶⁹⁵ Gül, **a.g.e.** s. 116.

⁶⁹⁶ Basit yargılama usulü ile ilgili ayrıntılı bilgi için bkz. Mahmut KOCA, "*Ceza Muhakemesinde Basit Yargılama Usulü*", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, C. 7, S. 2, Aralık 2020 s. 182-186. Zahit Yılmaz/Özge Apiş, "*Seri Muhakeme ve Basit Yargılama Düzenlemelerinin Değerlendirilmesi*", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 26, S. 1, 2020 s. 89-101.

⁶⁹⁷ Gül, **a.g.e.** s. 116.

SONUÇ

Bu çalışmada 5237 sayılı Türk Ceza Kanunu'nun 243. maddesinde düzenlenen “*Bilişim Sistemine Girme Suçu*” incelenmiştir. İlgili maddenin; ilk fıkrasında bilişim sistemine hukuka aykırı olarak girme veya orada kalmaya devam etme fiillerinin cezalandırılacağı, ikinci fıkrasında fiilin bedeli karşılığı yararlanılabilen sistemlere karşı işlenmesi durumunda verilecek cezada indirimle gidileceği, üçüncü fıkrasında suçun işlenmesi sırasında sistemdeki verilere zarar verilmesi halinde suçun netice sebebiyle ağırlaştırılmış halinin meydana geleceği düzenlenmiştir. Suç incelenirken öncelikle madde metninde geçen suçla ilişkili olan kavramların tanımlarına ve bu kavramlar hakkında doktrinde yapılan tartışmalara değinilmiştir. Ardından genel olarak bilişim ve bilişim suçları ile bu konudaki uluslararası ve ulusal mevzuatın gelişim süreçleri anlatılmıştır. Akabinde ise suçla korunmak istenen hukuki değer doktrindeki tartışmalar eşliğinde incelenmiştir. Çalışmanın devamında suçun unsurları; maddi unsurlar, manevi unsur ve hukuka aykırılık unsuru başlıkları altında incelenmiştir. Yine bu bölümde suçu etkileyen nedenler ile suçun neticesi sebebiyle ağırlaştırılmış haline değinilmiştir. İlerleyen bölümlerde ise suçların birleşmesi, iştirak, yaptırım ve muhakeme kuralları yargı kararları ve doktrindeki görüşlerle birlikte incelenmiştir.

Bilişim sistemine girme suçunun koruduğu hukuki değerle ilgili doktrinde farklı görüşler ileri sürülmüştür. Yazarlarca; sistemin güvenliği ile güvenilirliği, özel hayatın gizliliği, kişilerin sanal alandaki mahremiyeti, haberleşme özgürlüğü, kişisel veriler, malvarlığı ve kullanıcıların güvenlik duyguları gibi değerlerin korunmak istendiği ifade edilmiştir. Kimi yazarlar tek bir değer korunmak istendiğini savunurken; kimi yazarlar birden fazla değer birlikte korunmak istendiğini öne sürmüştür. Bize göre ise kanun koyucu suçun işlenmesi için maddi bir zararın oluşması, verilerin ele geçirilmesi ya da sisteme zarar verilmesi gibi bir şart aramadığından malvarlığının, özel hayatın gizliliğinin ya da sistemdeki verilerin korunmak istendiği söylenemeyecektir. Bu nedenle TCK m. 243'teki suçun düzenlenmesi ile korunmak istenen menfaat yalnızca bilişim sistemlerinin güvenliğidir. Suçun netice sebebiyle ağırlaştırılmış hali olan TCK m. 243/3'te ise kanun koyucu verilerin değiştirilmesi ya da yok edilmesi durumunda faile daha ağır bir ceza verilmesini öngörmüştür. Bu fıkra ile korunmak istenen hukuki değer ise sistemdeki verilerin güvenliğidir.

TCK m. 243'te düzenlenen suçu işleyecek fail için kanunda özel bir nitelik belirtilmediğinden her gerçek kişi bu suçun faili olabilecektir. Tüzel kişiler ise fail olarak cezalandırılmayacak; suçun işlenmesi sonucu lehine menfaat sağlanan tüzel kişiler için TCK m. 60'ta düzenlenen güvenlik tedbirleri uygulanabilecektir. Doktrinde, bu suçun failinin en azından temel düzeyde bilişim sistemlerini kullanabilecek bilgi ve birikime sahip olması gerektiği ifade edilmiştir. Gerçekten de bilişim sistemine girme suçunun çoğunlukla “*hacker*” olarak adlandırılan bilişim sistemleri konusunda uzman olan bilişim korsanlarınca işlendiği görülmektedir. Fakat unutulmamalıdır ki bu şart suçun tanımından çıkarılan kanuni bir şart değil, pratik bir gerekliliktir. Bilgisayar, akıllı telefonlar ve internetin yaygınlaşması ve kullanımının basitleşmesi ile birlikte ilköğretim çağındaki çocukların dahi bu suçları işleyebilmeleri mümkün hale gelmiştir. Ayrıca herhangi bir program veya yazılım kullanmaksızın doğrudan basit bir şifre girilerek de suçun işlenebilmesi mümkündür.

Bilişim sistemine girme suçunun mağduru, sistem üzerinde hak sahibi olan ve sisteme doğrudan erişim ve kullanım yetkisine sahip kişidir. Suçun işlenmesi ile hak ve menfaatleri tehlikeye düşen mağdur, sistemin sahibi olabileceği gibi sistem sahibi tarafından sisteme erişim ile yetkilendirilmiş de olabilir. Bir başka ifadeyle mağdurun sistem üzerindeki hakkı mülkiyet hakkına dayanabileceği gibi; kira gibi bir sözleşmeye ya da rızaya da dayanabilecektir. Kimi yazarlar yalnızca gerçek kişilerin mağdur olabileceğini; tüzel kişilerin ise suçtan zarar gören olarak yargılama süreçlerinde yer alması gerektiğini savunmaktadır. Bize göre ise TCK'da tüzel kişilerin mağdur olmalarına engel bir düzenleme bulunmadığından suçun niteliği el verdiği ölçüde tüzel kişiler de mağdur olabilecektir. Örneğin bir tüzel kişiye ait bilişim sistemine girilerek müşterilerin bilgilerine erişilmesi halinde TCK m. 243 anlamında yalnızca tüzel kişi mağdur olacaktır. Verileri görüntülenen gerçek kişiler ise TCK m. 136'da düzenlenen kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçunun mağduru olacaktır. Bu suç işlenirken sistemdeki verilere taksirle zarar verilmesi halinde ise hem tüzel kişi hem de sistemdeki verileri zarar gören gerçek kişiler TCK m. 243/3'ün mağduru olacaklardır.

TCK m. 243'te düzenlenen suçun konusu tamamına ya da bir kısmına hukuka aykırı şekilde girilmiş olan bilişim sistemidir. Bilişim sistemi temel olarak verileri işleyebilen, aktarabilen ve saklayabilen elektronik ve manyetik sistemler olarak tanımlanabilir. Bu özelliklerin yanı sıra söz konusu sistemin genel amaçlı olarak

kullanılabilmesi ve verileri işleyebilmesi gerekmektedir. Bir başka ifadeyle veri işleme ve aktarma özelliklerine sahip olsalar bile barkod okuyucuları, kahve otomatları ve beyaz eşyalar gibi belli bir amacı ifaya özgülenmiş cihazlar bilişim sistemi olarak kabul edilmemektedir. Bilgisayarlar, bilgisayar özelliği gösteren akıllı telefonlar ve tabletler yargı kararlarında en sık karşılaşılan bilişim sistemleri olarak öne çıkmaktadır. Günümüzde artık banka sistemleri ile bağlantı kurulabilen ve birçok bankacılık işleminin gerçekleştirilebildiği ATM'ler de bilişim sistemi olarak kabul edilmektedir. Belli bir donanımına sahip olmaksızın uzaktan erişilebilen sistemler de bu suçun konusunu oluşturabilmekte; sosyal medya ve e-posta hesapları, web siteleri, online oyun profilleri, kurumsal veri tabanları, internet bankacılığı uygulamaları sıkça yargı kararlarına konu olmaktadır. Henüz yargı kararlarına yansımamış olsa da yakın zamanda geliştirilen ve günlük hayatımızda yaygınlaşmaya başlayan bulut bilişim sunucuları ile nesnelerin internetiyle çalışan akıllı sistemler de yine TCK m. 243'ün konusu olabileceklerdir. Ayrıca madde metninde suçun bilişim sisteminin belli bir kısmına yönelik olarak işlenebileceği ifade edildiğinden; sistemle bağı devam eden belli bir yazılım ya da donanım birimine yönelik olarak da suç işlenebilecektir. Örneğin sistemdeki belli bir klasör yahut sistemle bağlantısı devam eden bir harici belleğe hukuka aykırı olarak erişen fail de cezalandırılacaktır. Suçun hafifletici nedenin düzenlendiği ikinci fıkrasının konusu yalnızca bedeli karşılığı yararlanılabilen bilişim sistemleri; suçun netice sebebiyle ağırlaşmış halini düzenleyen üçüncü fıkrasının konusu ise sistemin içerdiği verilerdir.

5237 sayılı TCK'nın ilk halinde bilişim sistemine girme suçu bileşik hareketli suç olarak düzenlendiğinden; suçun işlenmiş olması bilişim sistemine girme ve sistemde kalmaya devam etme fiillerinin birlikte icra edilmesi gerekmektedir. 2016 yılında yapılan değişiklikle birlikte kanundaki "ve" ibaresi "veya" olarak değiştirilmiş ve suç seçimlik hareketli suç halini almıştır. Failin sisteme girme veya kalmaya devam etme fiillerinden birini gerçekleştirmesi suçun oluşması için yeterli olacaktır. Suça konusu sisteme yönelen girme eyleminin sadece icrai bir hareketle gerçekleştirilebileceği konusunda doktrinde görüş birliği olsa da aynı durum kalma eylemi için geçerli değildir. Bir görüşe göre sistemde kalmaya devam etme fiili sadece ihmali suretle işlenebilecektir. Başka bir görüş ise sistemde kalma eyleminin ihmali şekilde işlenebileceğini kabul etmekle birlikte; sistemde bulunan failin kendisini sistemden atmaya çalışan güvenlik protokollerini devre dışı bırakmak amacıyla, örneğin bir yazılımı çalıştırarak, icrai hareketler yapabileceğini ifade etmiştir. Her

halükârda bir bütün olarak bakıldığında TCK m. 243'te düzenlenen suç hem icrai hem de ihmali hareketle işlenebilmektedir.

. Kimi yazarlar “*girme*” fiilinin fiziksel olarak bir yere girmeyi çağrıştırdığı gerekçesiyle kanunda “*erişim*” kelimesinin kullanımının daha isabetli olacağını öne sürmektedir. Biz ise bu görüşe katılmamakta ve kanunun kullandığı ifadeyi doğru bulmaktayız. Zira Yargıtay kararlarında da değinildiği üzere “*erişim*” kelimesinin internet veya benzeri bir ağ yoluyla sistemin soyut unsurlarına uzaktan bağlanmayı ifade etmekte; suç konusu sisteme temas edilerek yapılan ihlalleri kapsamamaktadır. “*Girme*” eylemi ise fiziki olarak sistemin düğmesine basılarak icra edilebileceği gibi başka sistemler ya da ağlar aracılığıyla uzaktan da gerçekleştirilebilecektir. *Girme* eyleminin suç olarak değerlendirilmesi için, sistemin herhangi bir tedbir ya da uygulama ile korunması gerekmemekte, sisteme girişin hukuki olarak sınırlandırılmış olması yeterlidir. Bir başka ifadeyle sistem sahibince sisteme *girme* veya *kalma* için açık ya da zımni bir rıza belirtilmediyse *girme* eylemi TCK m. 243'te düzenlenen suçu oluşturacaktır. Örneğin bir kimsenin kişisel bilgisayarını şifrelememiş olması, o bilgisayar sahibinin izni olmaksızın açan failin eylemini suç olmaktan çıkarmayacaktır. Herkesin erişimine açık bilişim sistemlerine girilmesi halinde ise hukuki bir sınırlama söz konusu olmadığından suç oluşmayacaktır. Bununla birlikte herkesin erişimine açık sistemlerde de belli bölümlere yahut verilere erişimin kısıtlanması söz konusu olabilmektedir. Sisteme erişimine izin verilen failin kısıtlanan bölümlere girmesi halinde de cezalandırılması gerekmektedir. Bu tip bir durumda failin giriş yetkilerinin sınırlarının belirlenmesi somut olay bazında adaletin sağlanması açısından önemlidir. Ayrıca failin sisteme *girme* eyleminin motivasyonunun da suçun oluşması bakımından önemi yoktur. Failin sisteme yeteneklerini denemek için, eğlenmek amacıyla ya da başkası adına girmesi arasında bir farklılık bulunmamaktadır.

Bilişim sistemine *girme* kavramı sistemin fiziksel yapısının içerisine değil, çalışan sanal/dijital alanına girilmesini ifade etmektedir. Sistemin fiziki yapısına zarar verilmesi halinde TCK m. 151'de düzenlenmiş olan mala zarar verme suçu oluşacaktır. Suç serbest hareketli olarak düzenlendiği için sisteme girilmesi sonucunu doğuran her türlü hareketle suçun işlenebilmesi mümkündür. Fail bilişim sistemine fiziki olarak temas ettiği sistemin düğmesine basarak ya da yasal olmayan yollarla elde ettiği sistem şifresini girerek sisteme girebileceği gibi; kablolu ya da kablosuz bir bağlantı ile başka

bir bilişim sistemi kullanarak da bu suçu işleyebilecektir. Bilişim suçlarını maddi çıkar amaçlı işleyen ve bu konuda uzmanlaşmış bilişim korsanlarınca bilişim sistemine girme suçunun sıklıkla işlendiği görülmektedir. Zira çalışmamıza konu olan suç diğer bilişim suçlarının işlenebilmesi amacıyla bir geçit suç olma özelliğini taşımaktadır. Bilişim korsanları tarafından virüsler, solucanlar ve Truva atları gibi zararlı yazılımlar kullanılarak sistem sahiplerinin bilgi ve iradesi dışında bilişim sistemlerine girildiği görülmektedir. Bu ve benzeri yazılımlar ile sistemlere sızan bilişim korsanları ileriki zamanlarda sistemlere girişlerini kolaylaştıracak arka kapılar bırakmakta ve bu sayede TCK m. 243'teki suçun ve diğer bilişim suçlarının işlenmesi kolaylaştırılmaktadır. Kimi zaman bilişim korsanlarınca tarama yöntemi ile hedef sistemin açıkları bulunmakta ve bu açıklar kullanılarak söz konusu zararlı yazılımlar sisteme sızdırılmaktadır. Kimi zaman ise sosyal mühendislik olarak adlandırılan psikolojik manipülasyon teknikleri de kullanılarak sistem sahibi yanıltılmakta ve sistem sahibinin yanıltılma sonucu verdiği giriş bilgileri kullanılarak hedef sistemlere erişilmektedir. Bazı durumlarda ise kişilere SPAM (İstem Dışı Elektronik Posta) yoluyla sahte web sayfaları gönderilmekte; bu sayfalara bilgilerini giren kullanıcıların bilgilerini ele geçiren bilişim korsanlarınca TCK m. 243'teki suç işlenebilmektedir. Son yıllarda ise geliştirilen Pegasus yazılımı gibi programlar kullanılarak sadece bir kısa mesaj ya da e-posta gönderilerek -kullanıcının gönderilen mesajı okumasına dahi gerek olmaksızın- bilişim sistemlerine girilebildiği medyaya yansımıştır.

Sistemde kalmaya devam etme fiili ile tamamına ya da belli bir kısmına girilmiş olan bilişim sisteminin soyut alanında kalmaya devam etmek suretiyle işlenmektedir. Fail, kalmaya devam edeceği sisteme kasten veya hata sonucunda hukuka aykırı olarak girmiş olabileceği gibi; sisteme girişe izin veren hukuka uygun halin ortadan kalkması sonucu sistemde kalmış da olabilir. Hataen sisteme girilmesi ya da hukuka uygun halin ortadan kalkması söz konusu olduğunda durumu fark etmesine rağmen sistemde kalmaya devam eden fail TCK m. 243'te düzenlenen suçu işlemiş olacaktır. Failin sistemde kalması hukuka aykırı bir nitelik arz ettiği anda suç işlenmeye başlanacak; sistemden çıkış yaptığı ana kadar işlenmeye devam edecektir. Bu yönüyle kalma eyleminin kesintisiz bir suç olduğu söylenebilecek; zamanaşımı ve suçun işlendiği yer gibi hususlar incelenirken bu durum göz önünde bulundurulacaktır. Failin sistemde kalma süresi ise TCK m. 61 gereğince cezanın belirlenmesinde dikkate alınabilecek olsa da suçun varlığı açısından önem arz etmemektedir.

TCK m. 243 incelendiğinde incelemekte olduğumuz suçun işlenmesi için sisteme girme veya kalmaya devam etme fiillerinden birinin gerçekleştirilmesinin yeterli olduğu; bunun dışında bir neticenin aranmadığı anlaşılmaktadır. Suç konusu fiilin işlenmesi ile birlikte bir zarar meydana gelmesine gerek olmadığı gibi; fail ya da üçüncü bir kişi lehine menfaat temin edilmesine de gerek yoktur. Bu nedenle incelemekte olduğumuz suç doktrinde “*sırf hareket suçu*” ve “*neticesi harekete bitişik suç*” olarak adlandırılmaktadır. Kanun koyucunun sisteme girme fiilini bir zararın yahut somut bir tehlikenin gerçekleşmesine gerek olmaksızın cezalandırması ise TCK m. 243’te düzenlenen suçun doktrinde “*soyut tehlike suçu*” olarak nitelendirilmesine neden olmuştur. Bilişim sistemine girme suçunun neticesi itibariyle ağırlaşmış halinde ise kanun koyucu suçun oluşması için sistemdeki verilerin zarar görmesi neticesini şart koşturmuştur. Bu yönüyle TCK m. 243/3’ün suçun basit halinden ayrılarak “*zarar suçu*” olarak düzenlendiği söylenebilir.

Bilişim sistemine girme eylemi bakımından teşebbüs mümkün olduğundan; sisteme girmek için icrai hareketlere başlayan fail, elinde olmayan sebeplerle sisteme girememesi halinde teşebbüs nedeniyle sorumlu olacaktır. Sistemde kalmaya devam etme fiili bakımından ise teşebbüs mümkün değildir. Kanun koyucu sistemde kalma eylemi için bir süre sınırı koymadığından sistemde bir an bile kalınmış olması suçun oluşması için yeterlidir. Taksirli suçlar bakımından teşebbüsün mümkün olmadığı göz önüne alındığında TCK m. 243/3’te düzenlenen suçun neticesi sebebiyle ağırlaşmış haline teşebbüs söz konusu olmayacaktır. Sisteme girmek için icrai hareketlere başlayan fail ancak 243. maddenin birinci ve ikinci maddelerine teşebbüsten sorumlu olabilecektir. Teşebbüsün mümkün olduğu hallerde TCK m. 36’da düzenlenen gönüllü vazgeçmeye ilişkin hükümlerin uygulanması da mümkün olacaktır. Bilişim sistemine girme suçunu işlemeye yönelik icra hareketlerine başlamış olan failin icra hareketleri tamamlanmadan suçu işlemekten vazgeçmesi halinde teşebbüsten dolayı ceza verilmeyecek; yalnızca vazgeçme anına kadar işlenen ve tamamlanan suç veya suçlardan dolayı ceza verilecektir.

TCK m. 243’ün ilk fıkrasında düzenlenen suçun basit hali ile ikinci fıkrasında düzenlenen daha az cezayı gerektiren hali ancak kasten işlenebilmektedir. Failin bilişim sistemine girdiğini bilmesi ve girmeyi istemesi gerekmektedir. Taksirle ya da hata sonucu bir bilişim sistemine giren fail kastla hareket etmediği için suç oluşmayacaktır. Failin amacının ise suçun oluşumu bakımından önemi yoktur. Failin

maddi çıkar sağlamak, eğlenmek ya da kendi yeteneklerini sınamak amacıyla sisteme girmesi arasında suçun oluşumu bakımından bir fark bulunmamaktadır. Failin kusurluluğunu ortadan kaldıran hallerin mevcut olması halinde de kastın varlığından söz edilemeyeceğinden suç oluşmayacaktır. Suçun neticesi sebebiyle ağırlaşmış hali ise manevi unsur yönünden suçun basit halinden farklılık arz etmektedir. Bu fıkrada kanun koyucu failin sisteme girme fiili bakımından kasten, verilere zarar verme fiili bakımından ise taksirle hareket etmesini aramaktadır.

Bilişim sistemine girme suçunu düzenleyen TCK m. 243'te geçen “*hukuka aykırı olarak*” ifadesinin ne anlama geldiği doktrinde tartışma konusu olmuştur. Bu durumu “*hukuka özel aykırılık*” olarak adlandıran yazarlar kanun koyucunun hukuka aykırılık bilincini tipikliğin bir unsuru olarak aradığını öne sürmektedir. Yargıtayın da kararlarında benimsediği bu görüşe göre failde hukuka aykırı hareket ettiğine dair bilinç yoksa suçun oluştuğundan da söz edilemeyecektir. Bizim de katıldığımız görüşe göre ise kanun koyucunun hukuka aykırılığa gönderme yapan ifadeyi kullanım şekli incelenmelidir. TCK m. 243 incelendiğinde kanun koyucunun amacının hukuka aykırılık bilincini suçun bir unsuru olarak düzenlemek değil; genel olarak suçun ihtiva ettiği haksızlık ve hukuka aykırılığı vurgulamak olduğu görülecektir. Burada kanun koyucunun amacı uygulamada ortaya çıkabilecek hukuka uygunluk hallerinin varlığının araştırılması için uygulayıcıların dikkatini çekmektir. Gerçekten de “*hukuka aykırı olarak*” ifadesi maddeden çıkarılsa dahi eylemin suç olma niteliğinde bir değişim olmayacaktır. Hâkim somut olayı dikkatlice inceleyerek aşağıda değineceğimiz hukuka uygunluk sebeplerinin varlığını araştırmalıdır.

Bir kanun hükmünün icrası kapsamına, kanundaki şartlar ve usul kurallarına riayet etmek şartıyla, bilişim sistemine girme eylemini gerçekleştiren kişiye ceza verilmeyecektir. Örneğin CMK’da düzenlenen bilgisayarlarda bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirini icra eden kolluk personeline ceza verilmeyecektir. Yine CMK ve PYSK ile polisler, jandarma ve istihbarat personeline ise kendi meslek kanunları ile telekomünikasyon yoluyla iletişimin denetlenmesi icra etme yetkisi verilmiştir. İlgili kanunlara uygun olarak bu faaliyetleri yürüten personelin davranışı da hukuka uygun olacağından bu kişilere ceza verilmeyecektir. Doktrinde muhalif görüşler bulunsa da biz bilişim sistemine girme suçunun meşru müdafaa kapsamında işlenebileceği kanaatindeyiz. Örneğin kendi özel fotoğraflarının bir sosyal medya hesabında yayınlandığını gören failin kendisine

yönelik saldırıyı sonlandırmak amacıyla bu sisteme girmesi halinde meşru müdafaa söz konusu olacaktır. Özel ve kamusal nitelikli bir hakkın kullanılması da TCK m. 243 açısından hukuka uygunluk sebebi olarak kabul edilmektedir. Abonelik ya da kiralama gibi bir sözleşmeden aldığı yetkiyle başkasına ait bilişim sistemine giren fail özel hukuk sözleşmeleri kaynaklı bir hakkını kullandığından hukuka aykırı davranmış olmayacaktır. Yaptığı haber gerektirdiği için TCK m. 243'teki suçu işlemiş olan gazetecinin eylemi ise kamusal bir hak olan haber verme hakkını kullanacağı için hukuka uygun olacaktır.

Sistem sahibi veya yetkilisinin rızası ile sisteme giren veya sistemde kalmaya devam eden failin bu rızaya uygun olarak icra edeceği eylem de suç oluşturmayacaktır. Söz konusu rıza açık bir şekilde verilebileceği gibi zımnen de verilmiş olabilir. Örneğin kişisel bir bilgisayarını tamir için bir başka kimseye veren sistem sahibi, bu kimsenin sisteme girmesine zımni olarak rıza göstermiş olacaktır. Aralarında hiçbir hukuki ya da şahsi bağlantı olmayan fail ve mağdur arasında rızanın mevcut olmadığı kabul edilecektir. Diğer hukuka uygunluk sebeplerinde olduğu gibi burada da rızanın varlığını ispat yükü de failin üzerindedir. Sadece sistem sahibinin vereceği rıza hukuka uygunluk sebebi olacaktır. Sistem sahibinden aldığı rızayla sisteme erişim hakkına sahip olan kimsenin üçüncü kişilere vereceği rıza geçerli olmayacaktır. Örneğin kendisine okuduğu üniversite tarafından verilen ücretli akademik veri tabanının şifresini üçüncü bir kişiye veren öğrencinin verdiği rıza geçerli olmayacaktır. Burada öğrenci yardım eden, sisteme giren kişi ise fail olarak sorumlu olacaktır. Rıza bir olayın gerçekleşmesi ya da belli bir sürenin geçmesi gibi bir şarta bağlı olarak verilebileceği gibi; belli bir amacın ifasına yönelik olarak da verilebilecektir. Örneğin sistem sahibi tarafından istihdam edilen ve sistem güvenliğini test etmek için sızma testleri yapan bilişim uzmanlarının eylemleri rızaya dayalı olduğu için hukuka uygundur. Verilen rızanın kapsamı dışına çıkıldığı veya rıza sona ermesine rağmen sistemde kalmaya devam edildiği anda hukuka uygunluk sebebi ortadan kalkacağından TCK m. 243'te düzenlenen suç oluşacaktır. Sistemin yalnızca belli bir kısmına girilmesi için verilen rıza ise failin sistemde girmesi için rıza verilmeyen kısımlara yönelik eylemlerini hukuka uygun hale getirmeyecektir. Rızanın sadece sisteme girmeye yönelik olarak verildiği durumda bu rıza kalma eylemini kapsamayacak; rızanın girme veya kalma eylemlerinin hangisinin hangisini kapsadığının belirtilmediği durumlarda ise iki seçimlik hareket için de rızanın verilmiş olduğu kabul edilecektir. Çalışanlarına kullanmaları için bilgisayar tahsis eden kamu kurumları veya

şirketler de bu sistemlere girmeleri ve sistemde kalmaları için çalışanlarına rıza göstermektedir. Kurumlarca denetim maksadıyla çalışanlara ait bilişim sistemine girilerek bu sistemlerde yapılan işlerin ve yazışmaların denetlenmesinin TCK m. 243'te yer alan suç oluşturup oluşturmayacağı ise doktrinde tartışmalıdır. Kimi yazarlar belli bir amaç için çalışanlara tahsis edilen bilişim sistemlerinin bu amaca uygun olarak kullanılıp kullanılmadığını denetlemeye yönelik eylemler suç oluşturmayacaktır. Bizim de görüşlerine katıldığımız yazarlar ise ancak çalışanların önceden bilgilendirildiği durumlarda bu tür bir denetimin yapılabileceğini kabul etmektedirler. AİHM ve AYM de verdikleri kararlarda çalışanların önceden bilgilendirilmesi ve uyarılması halinde tahsis edilen bilişim sistemlerinin işverenlerce denetlenebileceğine hükmetmiştir. Çalışanların bilgisi olmadan sistemlere girilmesi ve yazışmaların okunması halinde ise rızanın varlığından söz edilemeyeceğinden suç işlenmiş olacaktır.

TCK m. 243/2'ye göre incelemekte olduğumuz suçun “*bedeli karşılığı yararlanılabilen*” sistemlere yönelik olarak işlendiği takdirde fiilin cezası yarı oranına kadar indirilecektir. Bu fıkra göre işlenecek suçun sistem sahibinin sistem üzerindeki yetkisi ile malvarlığı değerlerini de tehdit etmesi nedeniyle da ağır cezalandırılması gerektiğini savunarak; bu halin hafifletici sebep olarak düzenlenmesini eleştirmiştir. Kimi yazarlar ise bedeli karşılığı işlenebilen sistemlere girilmesinin hafifletici sebep olarak düzenlenmesine karşı çıkmamakla birlikte; sistemde kalmaya devam eden failin maddi çıkar sağlıyor olmasının daha ağır bir cezayı gerektirdiğini savunmaktadır. Biz ise suçla korunan hukuki değer sistem güvenliği olduğunu kabul ettiğimizden dolayı TCK m. 243/2'deki düzenlemenin yerinde olduğunu savunmaktayız. Zira halihazırda belli bir bedel karşılığında güvenliğinden feragat edilmiş sistemlere girilmesi, hiçbir suretle dışarıdan erişilmesi istenmeyen sistemlere girilmesi kadar tehlike barındırmamaktadır. Sistemin kullanımı için belirlenecek bedelin para olmasına ilişkin bir zorunluluk bulunmamaktadır. Uygulamada da belli sayıda yeni abonenin sisteme kazandırılması karşılığında ücretli hizmetlerin ücretsiz sunulabildiği görülmektedir. Bedelin hizmet alınmadan önce, hizmet sırasında yahut sonradan ödeniyor olmasının da incelemekte olduğumuz suçta bir etkisi bulunmamaktadır.

Bedeli karşılığında yararlanılabilen sistemlerin tanımının ve örneklerine kanun gerekçesinde yer verilmemesi doktrinde eleştiri konusu olmuştur. Yapılan

alışmalarda fıkrada kastedilenin biliřim sistemlerinin bulunduęu mekanlar deęil, sistemin sanal yapısı üzerinden sunulan hizmetler olduęu ifade edilmiřtir. Muhalif grüşler olsa da doktrindeki baskın grüş bilgisayarların saatlik olarak kiralandığı internet kafeler gibi mekanların bu fıkra kapsamına girmeyeceęi yönündedir. Biliřim sistemi tabanlı olarak hizmet veren tüm sistemler bu fıkra kapsamında deęerlendirilebilecektir. Ücret karřılıęında abonelerine çeřitli hizmetler sunan web siteleri ve uygulamalar bedeli karřılıęı yararlanılabilen biliřim sistemi olarak kabul edilmektedir. Alıřveriř siteleri, video oyunu oynanabilen platformlar ile elektronik veri tabanları bunlara verilebilecek örneklerdendir. Son yıllarda geliřtirilen ve kullanıcıların “*kullandığın kadar öde (pay for use)*” prensibi ile yararlandıkları hizmet ölçüsünde ödeme yaptıęı bulut biliřim yahut nesnelerin interneti teknolojisi tabanlı sistemler de yine bu fıkranın kapsamındadır. Her ne kadar kimi yazarlar bir aę üzerinden faydalanılabilen internet hizmetinin yetkisiz kiřilerce kullanılmasını karřılıksız yararlanma suçu kapsamında deęerlendirse de kanaatimizce bu halde de TCK m. 243/2’nin ihlali söz konusu olacaktır. řifreli yayınların yapıldığı platformların řifrelerinin kınılarak bu oyunların izlenmesi halinde ise ikili bir ayırım yapmak yerinde olacaktır. řifreli yayın hizmetinin telefon hatları ve frekansları ile elektromanyetik dalgalar kullanılarak saęlanması halinde TCK m. 163/2’de düzenlenen karřılıksız yararlanma suçu oluşacaktır. Öte yandan IPTV veya WEB TV gibi sunucular üzerinden bilgisayarlar, tabletler, akıllı telefonlar veya akıllı televizyonlar üzerinden abonelere hizmet sunulan hallerde suç konusu cihazlar biliřim sistemi nitelięi haiz olduęu için TCK m. 243/2 uygulanmalıdır. Otomatlar tarafından sunulan hizmetlerden bedeli ödenmeksizin yararlanması halinde ise TCK m. 163’te düzenlenen karřılıksız yararlanma suçu oluşacaktır.

Doktrinde kamu kurumlarına ait ya da devletin güvenlięiyle ilgili biliřim sistemleri ile özel güvenlik önlemleri ile korunan sistemlere yönelik eylemlere daha ağır cezalar verilmesinin gerektięine dair grüşler olsa da; TCK’da incelemekte olduęumuz suçun daha fazla cezayı gerektiren hallerine iliřkin bir düzenleme bulunmamaktadır. Terörle Mücadele Kanunu’nda ise incelemekte olduęumuz suçun bir terör örgütünün faaliyetleri dahilinde iřlenmesi durumunda terör suçu olarak kabul edileceęi ve TCK m. 243’e göre verilecek cezanın yarı oranında artırılacaęı düzenlenmiřtir. Bu kapsamında artırılacak ceza TCK’da belirlenmiř olan ceza üst limitini aşabilecektir. İncelemekte olduęumuz suçun çocuklar tarafından iřlenmesi

halinde ise Terörle Mücadele Kanunu'nda düzenlenen cezanın artırılmasına yönelik hükümler uygulanmayacaktır.

İncelemekte olduğumuz suçun neticesi sebebiyle ağırlaşmış hali TCK m. 243/3'te düzenlenmiştir. Bu suçu işlediği sırada sistemde bulunan verilerin değişmesine yahut yok olmasına yol açan faile altı aydan iki yıla kadar hapis cezası verilecektir. Bu fıkra düzenlenirken halin oluşabilmesi için sisteme girme ile verilere zarar verilmesi arasında nedensellik bağı bulunması yeterli görülmüş; failin kastının varlığı aranmamıştır. Zaten failin verilere zarar verme kastıyla hareket etmesi halinde TCK m. 244/2'de düzenlenmiş olan “*verilerin yok edilmesi veya değiştirilmesi suçu*” oluşacaktır. Bir başka ifadeyle TCK m. 243/3'teki suçun işlenebilmesi için failin sisteme girme veya kalma eylemi bakımından kast, sistemdeki verilere zarar verme neticesi bakımından ise taksirle hareket etmesi gerekmektedir. Gerçekleşmesi gereken neticeler seçimlik olarak düzenlendiğinden; verilerin “*yok edilmesi*” ya da “*değiştirilmesi*” hallerinden birinin varlığı suçun oluşması için yeterli olacaktır. Madde gerekçesinde veri kavramı teknik anlamından daha geniş bir şekilde ele alınmış, sistemdeki tüm soyut bileşenlerin veri kapsamına girdiği ifade edilmiştir. Zarar gören verilerin sistemin temel işleyişini etkileyen yazılımlara ilişkin veriler olabileceği gibi tali önemdeki uygulamalara ait veriler de olabilecektir.

TCK m. 42 gereğince bilişim sistemine girme suçunun bir başka suçun ağırlaştırıcı nedeni ya da unsuru olarak işlenmesi halinde bileşik suç oluşacak ve faile TCK m. 243 gereğince ceza verilmeyecektir. Bu kapsamda bilişim sisteminin kullanılması yoluyla hırsızlık (TCK m. 142/2-e) ve bilişim sisteminin araç olarak kullanılması yoluyla dolandırıcılık (TCK m. 158/1-f) suçlarını işlemiş olan faile bu suçları işlediği sırada icra ettiği bilişim sistemine girme ya da kalma eylemleri nedeniyle ceza verilmeyecektir. Bilişim sistemine girme suçunun bir suç işleme kararının icrası tarafında aynı kişiye karşı farklı zamanlarda birden fazla kez veya birden fazla kişiye karşı tek bir fiille işlenmesi halinde zincirleme suç söz konusu olacak; faile TCK m. 43 gereğince ağırlaştırılmış tek bir ceza verilecektir. Hedef sisteme girmelerinin ardından sonraki girişleri kolaylaştırmak amacıyla sistemde açık kapılar oluşturan bilişim korsanlarının, bu açık kapıları kullanarak farklı zamanlarda sisteme girmeleri halinde bu kişilere zincirleme hükümleri gereğince ceza verilecektir.

TCK m. 44'e göre tek bir fiil ile birden fazla suçun işlenmesi halinde fail yalnızca en ağır cezayı gerektiren suç için cezalandırılacaktır. Uygulamada

haberleşmenin gizliliğini ihlal (TCK m. 132), özel hayatın gizliliğini ihlal (TCK m. 134) ve kişisel verilerin ele geçirilmesi (TCK m. 136) gibi suçlarla incelemekte olduğumuz suçun sıklıkla birlikte işlendiği görülmektedir. Özellikle TCK m. 243'te düzenlenen suçun bu suçların işlenebilmesi için araç suç olarak işlendiği hallerde TCK m. 44'teki fikri içtima hükmünün uygulanıp uygulanmayacağı sorunu ortaya çıkmaktadır. Kimi yazarlar sayılan bu suçlar ile bilişim sistemine girme suçlarının farklı fiiller ihtiva etmelerinden hareketle gerçek içtima hükümlerinin uygulanarak faile hem araç suç hem de araç suç için iki ayrı ceza verilmesi gerektiğini savunmaktadır. Bazı yazarlar ise bu durumda araç suçun ve amaç suçun fiilleri örtüşmese bile amaç suçun ihtiva ettiği haksızlığın bilişim sistemine girme suçunu da kapsadığını öne sürmektedir. Bu görüşe göre; bilişim sistemine girme suçu daha ağır olan amaç suç içerisinde eriyecek ve TCK m. 44 uygulanarak faile sadece amaç suç için kanunda öngörülen ceza verilecektir. Bizim de katıldığımız yazarlara göre ise araç suç-amaç suç ilişkisinin olduğu hallerde suçun icra hareketleri incelenmeli; şayet iki suçun icra hareketleri örtüşüyorsa TCK m. 44, örtüşmüyorsa gerçek içtima hükümleri uygulanmalıdır. Örneğin failin bilişim sistemine girmeye yönelik eylemi aynı zamanda haberleşme gizliliğini ihlal etmesini de sağlıyorsa TCK m. 44 uygulanmalı ve sadece haberleşmenin gizliliğini ihlal suçundan dolayı ceza verilmelidir. Öte yandan bilişim sistemine girmiş olan fail sistemdeki verileri bir harici belleğe kaydediyorsa; iki farklı fiil söz konusu olacak ve faile her iki suç için ayrıca ceza verilecektir. Yargıtay da kararlarında fiillerin ayırımına dayanan görüşü benimsemektedir.

TCK m. 244'te düzenlenmiş olan “*sistemi engelleme, bozma, verileri yok etme veya değiştirme*” suçlarının bilişim sistemine girilerek işlendiği durumlarda TCK m. 44 hangi gerekçe ile uygulanmayacağı hususu doktrinde tartışma konusu olmuştur. Kimi yazarlara göre bilişim sistemine girme eylemi TCK m. 244'te düzenlenen suçların unsuru haline geldiğinden faile yalnızca TCK m. 244 gereğince ceza verilmelidir. Bazı yazarlar ise failin kastını ön plana çıkarmakta ve TCK m. 244'teki suçları işleme kastıyla hareket eden failin bilişim sistemine girme fiilinden dolayı cezalandırılmaması gerektiğini savunmaktadır. Bir görüş ise iki maddenin de koruduğu hukuki menfaatin aynı olduğuna dikkat çekerek asli norm-tali norm ilişkisi nedeniyle yalnızca TCK m. 244 uyarınca ceza verilmesi gerektiğini ifade etmektedir. Anılan iki maddenin fiillerinin örtüştüğünü ifade eden yazarlar ile TCK m. 44'ün uygulanarak faile yalnızca ağır olan suç için ceza verilmesini dile getirmektedir. Bizim katıldığımız görüşe göre ise somut olaydaki fiiller incelenerek karar verilmesi yerinde

olacaktır. Şayet failin TCK m. 244'te öngörülen neticeleri gerçekleştirmek için bilişim sistemine girmesi kaçınılmaz ise fikri içtima uygulanmalı ve faile sadece TCK m. 244 gereğince ceza verilmelidir. Öte yandan fail sisteme yahut verilere bilişim sistemine girmeksizin zarar verebileceği halde TCK m. 243'teki suçu işlemişse gerçek içtima uygulanarak iki ayrı ceza verilmelidir. Yargıtayın ise benzer nitelikteki olaylara dair kimi kararlarında TCK m. 44'ü uyguladığı; kimi kararlarında ise iki suç için ayrı ayrı ceza verilmesini tercih ettiği görülmektedir.

TCK'ya 2016 yılında eklenen 245A maddesi ile bilişim suçlarını işlemeye yönelik olarak yasal olmayan cihaz ve programların üretimi, ticareti ve bulundurulması suç olarak düzenlenmiştir. Bu madde gereğince temin edilen cihaz yahut programlarla TCK m. 243'te düzenlenmiş olan suçun işlenmesi mümkündür. Bu durumda suçların icra hareketleri örtüşmediği için gerçek içtima uygulanacak ve fail hem TCK m. 243 hem de TCK m. 245A gereğince ayrı ayrı cezalandırılacaktır.

Bilişim sistemine girme suçunun birden fazla fail tarafından işlenmesi mümkündür. Böyle bir durumda müşterek faillik söz konusu olacak ve iki faile de ceza verilecektir. Bir kimsenin başka bir kimseyi TCK m. 243'teki suçu işlemek maksadıyla araç olarak kullanması halinde ise dolaylı faillik söz konusu olacak; asıl faili kullanan kişi de fail olarak cezalandırılacaktır. Bir kimseyi bilişim sistemine girme suçunu azmettiren kişi TCK m. 38 gereğince suçun cezası ile cezalandırılacaktır. Faili suç işlemeye teşvik eden, onun suç işleme kararını kuvvetlendiren; faile suçun icrasından sonra yardım edeceğini vaat eden, suçun icrası için yol gösteren yahut araç temin eden veya suçun icrasından önce yahut suç işlenirken faile yardımda bulunan kişi ise TCK m. 39 uyarınca yardım eden sıfatıyla cezalandırılacaktır.

TCK m. 243'te düzenlenen suçun basit halinin işlenmesi halinde fail bir yıla kadar hapis veya adli para cezası ile cezalandırılacaktır. Maddede hapis ile adli para cezaları seçimlik olarak düzenlendiğinden; hâkimin iki yaptırımdan birini seçmesi gerekecektir. Verilecek hapis cezasının alt sınırı bir ay, adli para cezasının alt sınırı ise otuz gündür. Hâkim TCK m. 61'e göre bir değerlendirme yapmalı ve faile verilecek cezayı belirlemelidir. İncelemekte olduğumuz suçun bedeli karşılığı yararlanılan sistemlere karşı işlenmesi halinde ise hâkimin ilk fıkraya göre belirleyeceği ceza yarı oranında indirilecektir. Anılan suçun bir terör örgütünün faaliyetleri kapsamında işlenmesi durumunda ise yine TCK m. 243 gereğince bir ceza belirlenecek; ardından belirlenen ceza yarı oranında artırılabilecektir. TCK m. 243/3'te düzenlenen suçun neticesi

sebebiyle ağırlaştırılmış halinin işlenmesi durumunda ise TCK m. 61 uyarınca bir değerlendirme yapılarak faile altı aydan iki yıla kadar hapis cezası verilecektir. Bu fıkra gereğince adli para cezası verilmesi mümkün değildir. Tüm bu hallerde verilecek cezanın iki yılın altında olması halinde CMK m. 231'e göre hükmün açıklanmasının geri bırakılması mümkündür. Bilişim sistemine girme suçuyla bir tüzel kişi lehine menfaat temin edilmesi halinde ise bu kişiler hakkında TCK m. 60'ta düzenlenen güvenlik tedbirlerine hükmedilebilecektir.

Bilişim sistemine girme suçu şikayete bağlı olarak düzenlenmemiş olup mağdurun, suçtan zarar görenin yahut üçüncü kişilerin şikayetine gerek olmaksızın re'sen soruşturulmalıdır. TCK m. 243'ün üç fıkrası itibarıyla de görevli mahkeme asliye ceza mahkemesi olacaktır. 15 Ağustos 2021 tarihinde yayımlanan Hakimler ve Savcılar Kurulu kararı ile birlikte iki veya daha fazla ağır ceza mahkemesi ve asliye ceza mahkemesi bulunan yerlerde belli mahkemeler bilişim suçları bakımından ihtisas mahkemesi olarak belirlenmiştir. Bu değişiklikle birlikte belli bir teknik bilgi ve uzmanlık gerektiren bilişim suçlarının alanında ihtisaslaşmış hakimlerce karara bağlanması amaçlanmıştır. İncelemekte olduğumuz suç maddedeki diğer şartlar da karşılandığı takdirde CMK m. 251 ile düzenlenen basit yargılama usulüne tabi olacaktır. Failin suça sürüklenen çocuk olması durumunda ise CMK m. 253/3-c gereğince taraflar yargılamadan önce uzlaştırmaya sevk edilmelidir.

KAYNAKÇA

- AKARSLAN Hüseyin, **Bilişim Suçları, 2. Baskı**, İstanbul: Seçkin, 2015
- AKBULUT Berrin, **Bilişim Alanında Suçlar, 2. Baskı**, Ankara: Adalet Yayınevi, 2017
- AKBULUT Berrin, **Ceza Hukuku, Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 7. Baskı**, Ankara: Adalet Yayınevi, 2020
- AKINCI Hatice/ALİÇ A. Emre/ER Cüneyd, “*Türk Ceza Kanunu ve Bilişim Suçları*”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ocak 2004 s. 158-275..
- AKSOY RETORNAZ E. Eylem, “*5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun Kapsamında İçerik Sağlayıcının Yükümlülükleri ve Ceza Sorumluluğu*”, **Ceza Hukuku Dergisi**, Y. 16, S. 45, Nisan 2021 s. 9-32.
- AKSOY RETORNAZ Eylem, “*Yasak Cihaz veya Programlar*”, **Özel Ceza Hukuku C. VIII: Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ile Bilişim Alanındaki Suçlar**, İstanbul: On İki Levha Yayıncılık 2020. s. 311-324.
- APAYDIN Cengiz, “*Bilişim Sistemine Girme Suçu*”, **Türkiye Adalet Akademisi Dergisi**, Y. 7, S. 24, Ocak, 2016, s. 245-309
- APAYDIN Cengiz, **Bilişim Suçları ve Bilişim Ceza Hukuku**, İstanbul: Acar Matbaacılık, 2017
- APIŞ Özge, “*Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama El koyma Koruma Tedbiri*” **Yasama Dergisi Kamu Yönetiminde Teknoloji Özel Sayısı II**, C.12, S.37, Haziran 2018, s. 49-86.
- ARTUK M. Emin/ GÖKÇEN Ahmet/ ALŞAHİN M. Emin/ ÇAKIR Kerim, **Ceza Hukuku Genel Hükümler, 14. Baskı**, Ankara: Adalet Yayınevi, 2020
- ARTUK M. Emin/ GÖKÇEN Ahmet/ YENİDÜNYA Caner, **Ceza Hukuku Özel Hükümler, 15. Baskı**, Ankara: Adalet Yayınevi, 2015
- ATEŞ Emre Cihan / SALUK Ahmet, “*Bilişim Suçları Kapsamında Suça Sürüklenen Çocukların İncelenmesi*”, **HUMANITAS - Uluslararası Sosyal Bilimler Dergisi**, C. 6, S. 12, 2018 s. 154-176.
- ATEŞ Emre Cihan, “*Suç 4.0: Dijital Suç ve Güvenlik*”, **Dijital Dönüşüm Trendleri, İstanbul: Filiz Kitabevi**, Mayıs 2019 s. 258-284
- AYDIN Devrim, “*Yeni Türk Ceza Kanunu'nun Hazırlanış Süreci*”, **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, C. 59, S. 4, Nisan 2004 s. 249-263.
- AYDIN Devrim, “*Tüzel Kişilerin Ceza Sorumluluğu Tartışmaları*”, **Uyuşmazlık Mahkemesi Dergisi**, S. 10, 2017 s. 97-110.

AYDIN Emin D. “*Bilişim Sistemlerinde Güvenlik, Güvenilirlik, Mahremiyet ve Bilişim Suçları*”, **Marmara İletişim Dergisi**, İstanbul, S.1, Aralık 1992 s. 109-137.

AYDIN Emin Doğan, **Bilişim Suçları ve Hukukuna Giriş**, Ankara: Doruk Yayınları, 1992

AYDIN, Murat, “*Şifreli Yayınların İzinsiz Toplu Gösterimi Suç Mudur?*”, **Yargıtay Dergisi**, C.22, S.4, Ekim 1996, s. 491-505

AYDIN Nurullah, **Türk Suç ve Ceza Hukuku Genel ve Özel Hükümler**, 2. Baskı, Ankara: Adalet Yayınevi,

AYDIN Öykü Didem, “*Bilişim Suçları*”, **Bilişim '93 bildiriler: Türkiye Bilişim Derneği Bilişim 93 Etkinlikleri 28 Eylül – 1 Ekim 1993**, İstanbul: İnterpro Yayıncılık, 1993 s. 73-81.

BAŞ BAYRAKTAROĞLU Eylem, **Ceza Hukukunda Fail ve Mağdur**, Ankara: Seçkin Yayıncılık, 2021

BAYINDIR Aslı, “*Türk Ceza Kanunu’nda Düzenlenen Bilişim Suçları*”, **Suç ve Ceza Dergisi**, Y. 2010, S. 2 s. 55-106.

BAYRAKTAR Köksal, “*Banka ve Kredi Kartları ile Ortaya Çıkan Ceza Hukuku Sorunları*”, **Prof. Dr. M. Kemal Oğuzman’ın Anısına Armağan**, İstanbul: Beta Yayınları, Ocak 2000

BİÇKİN İnci, “*Siber Suç Sözleşmesi ve 5237 s. Türk Ceza Kanununda Bilişim Suçları*”, **Yargıtay Dergisi**, Cilt:32, Ocak-Nisan 2006, S.1-2. s. 145-168.

BİLGE Selahattin Samet, “*Türk Ceza Hukukunda Zorunluluk Hali*”, **Başkent Üniversitesi Hukuk Fakültesi Dergisi**, C. 7, S. 2, 2017 s. 365-389.

BOZDOĞAN AKBULUT, Berrin, “*Bilişim Suçları*”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, C. 8, S.1-2, 2000 ss. 545-555.

BOZKURT YÜKSEL Armağan Ebru, “*Nesnelerin İnternetinin Hukuki Yönden İncelenmesi*”, **DEÜHFD**, C. 17, S. 2, Aralık 2015 s. 113-140.

BREGANT Jessica/BREGANT Robert, “*Cybercrime and Computer Crime*”, **The Encyclopedia of Criminology and Criminal Justice**, First Edition, Edited by Jay S. Albanese, John Wiley & Sons Inc., 2014 <https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118517383.wbeccj244> (E. T. 15.12.2021)

BYRNE James M./KIMBALL Kathryn A., “*Inside The Darknet: Techno-Crime And Criminal Opportunity*”, **Criminal Justice Technology In The 21st Century: Third Edition**, Ed. Laura J. Moriarty, Springfield, 2017 s. 206-233.

CEBRE Ayvaz, “*Hukuka Uygunluk Sebebi Olarak Haber Verme Hakkı*”, **Uyuşmazlık Mahkemesi Dergisi**, C. 4, S. 7, Haziran 2016 s. 287-319.

CENTEL Nur, “5271 Sayılı Ceza Muhakemesi Kanunu’na Göre Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi”, **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Köksal BAYRAKTAR’a Armağan S.** 2020/1, C. 1. s.161-192.

CHAWLA Ajay, “Pegasus Spyware—A Privacy Killer”, **Available at SSRN**, 2021, <https://ssrn.com/abstract=3890657> or <http://dx.doi.org/10.2139/ssrn.3890657> (E.T. 12.12.2021)

CLOUGH Jonathan, “*The Council Of Europe Convention On Cybercrime: Defining ‘Crime’ In A Digital World*”, **Criminal Law Forum**, Springer, (2012)-23 s. -363. 391.

CLOUGH Jonathan, **Principles of Cybercrime, Second Edition**, Cambridge, Cambridge University Press, 2015

CRAIG Brain, **Cyberlaw, The Law of the Internet and Information Technology**, New Jersey, Pearson Education,

CUPA Basil, “*Trojan Horse Resurrected - On The Legality Of The Use Of Government Spyware*”, **Living in Surveillance Societies: ‘The State of Surveillance**, Edit. Webster, C William R. Living, Zurich Open Repository and Archive, University of Zurich, 2013, s.419-428. https://www.zora.uzh.ch/id/eprint/81157/1/Cupa_Living_in_Surveillance_Societies_2012.pdf (E. T. 04.12.2021)

ÇAKIR Kerim, “*Tüzel Kişiler Hakkında Güvenlik Tedbirleri*”, **Beykent Üniversitesi Hukuk Fakültesi Dergisi**, C. 4, S. 8, Aralık 2018 s. 131-146.

ÇETİN Erol, MALKOÇ İsmail, **Uygulamada Sahtekarlık Suçları, Bilgisayar Suçları, Tebligat Suçları ve İlgili Mevzuat**, Ankara: Adalet Yayınevi, 1995

ÇETİN Muhammed Sefa, “*Yargıtay Kararları Işığında Bilişim Sistemine Girme ve Kalma Suçu (TCK m. 243.)*” **Türkiye Adalet Akademisi Dergisi**, Y. 12, S. 45, Ocak, 2021, s. 1-28.

DALKILIÇ Aysun, “*Avrupa Birliği’ne Uyum Sürecinde Bilişim Suçları*”, **Avrupa Birliği’ne Uyum Sürecinde Türk Ceza ve Ceza Muhakemesi Hukuku**, Proje Yöneticisi Fatih Selami Mahmutoglu İstanbul: İstanbul Barosu Yayınları Ekim 2008 s.201-229.

DEĞİRMENCİ Olgun, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, Ankara: Seçkin, Mart 2014

DEĞİRMENCİ Olgun, **Bilişim Suçları**, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul, 2002

DEĞİRMENCİ, Olgun: “*Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukuktaki Düzenlenişi*”, **Legal Hukuk Dergisi**, C. 1, S. 11, 2003 ss. 2750-2758.

DEĞİRMENCİ, Olgun “*2004 Türk Ceza Kanunu’nun Bilişim Suçları Bakımından Değerlendirilmesi*”, **TBB Dergisi**, S. 58., 2005 s. 195-208.

DEMİR Oğuzhan Ömer/ARIÇ Mehmet/POLAT Halil, **Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar Soruşturma ve Kovuşturma Yöntemleri**, Ankara: Adalet Yayınevi, 2015

DEMİRBAŞ Timur, **Ceza Hukuku Genel Hükümler, Güncellenmiş 16. Baskı**, Ankara: Seçkin Yayıncılık, 2021

DEMİRBAŞ Timur, **Haksız Tahrik, Güncellenmiş ve Genişletilmiş 3. Baskı**, Ankara: Seçkin Yayınları, 2021

DEMİRCAN Tunç, **Bilişim Alanında Suçlar**, İstanbul: Legal Yayıncılık, 2016

DİNÇ Günay, “*Bilgisayar Çağında Özel Yaşamın Korunması*”, **Ankara Barosu Dergisi** S. 1987/2, s. 195-204.

DOĞAN Koray, “*Bilişim Suçları ve Türk Ceza Kanunu*”, **Hukuk ve Adalet Eleştirel Hukuk Dergisi**, Y.2 S.6, 2005 s. 290-319.

DÖNMEZER Sulhi, **Kişilere ve Mala Karşı Cürümler**, 17. Baskı, İstanbul; Beta Basım A.Ş., 2004

DÖNMEZER Sulhi/ERMAN Sahir, **Nazari ve Tatbiki Ceza Hukuku, C. II, 15. Tıpkı Basım**, İstanbul: Der Yayınları, 2021

DURSUN Hasan, “*Bilgisayar ile İlgili Suçlar*”, **Yargıtay Dergisi**, C. XXIV, S. 3, Ankara, 1998 s. 334-339.

DURSUN Selman, “*İnternette Kaynaklanan Ceza Sorumluluğundaki Gelişmeler*”, **Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni- Prof. Dr. Gülören Tekinalp’e Armağan**, C. 23, S. 1-2, İstanbul, 2003, s.251-294.

DÜLGER Murat Volkan, **Bilişim Suçları ve İnternet İletişim Hukuku, 8. Baskı**, Ankara: Seçkin Yayıncılık, 2020

DÜLGER Murat Volkan, **Kişisel Verilerin Korunması Hukuku**, Hukuk Akademisi Yayınları, 2019

DÜLGER Murat Volkan, **Türk Ceza Hukuku Genel Hükümler**, İstanbul: Hukuk Akademisi, 2021

DÜLGER Murat Volkan, “*Türk Ceza Kanunu’nda Yer Alan Bilişim Suçları ve Eleştirisi*”, **Bilişim Hukuku**, Der. Mete TEVETOĞLU, İstanbul: Kadir Has Üniversitesi, 2006

EKER Ö. Umut, “*Türk Ceza Hukuku’nda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 s. Yeni Türk Ceza Kanunu’nun İlgili Hükümlerinin Yorumu*”, **TBB Dergisi**, Yıl:19, Sayı: 62, Ocak-Şubat 2006 s. 101-131.

EKİCİ ŞAHİN Meral, **Ceza Hukukunda Rıza**, İstanbul: On İki Levha Yayınları, 2011

EKİCİ ŞAHİN Meral / KORUCULU Irmak, “*Bilişim Sistemine Girme Suçu - Suçun Kamu Personeline ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarla İşlenmesine İlişkin Bir Değerlendirme*”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Prof. Dr. Durmuş TEZCAN’a Armağan**, C. 21, Özel S. 2019, s. 585-626.

ELBAHADIR Hamza, **Hacking Interface**, 17. Baskı, İstanbul: Kodlab, 2018

ERALP Özgür, **Hukukçular İçin Bilişim Terimleri Sözlüğü**, Ankara: Avbil Yayınları, 2007

ERDAĞ Ali İhsan, “*Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)*”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C.XIV, Sayı:2, 2010 s. 265-303.

ERDEM Ümit/ULUSLU Çağrı Şükrü/DUMANLI Gökberk, **Yargıtay (2014-2016) Kararlarında Sosyal Medya**, İstanbul: Legal Yayıncılık, 2016

ERDOĞAN Yavuz, “*Bilişim Sistemine Girme ve Kalma Suçu*”. **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Prof. Dr. Burhan CEYHAN’a Armağan**, C. 12, Özel S. 2010, s. 1363-1433.

ERDOĞAN Yavuz, **Türk Ceza Kanunu’nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları ile)**, Legal Yayıncılık, 2012

EREM Faruk, “*Ceza Hukukunda ‘Hakkın Kullanılması’*”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C. 41, S. 1, Ocak 1990 s. 5-17.

EREM Faruk, “*Bilgisayar Suçları ve Türk Ceza Kanunu*”, **Yargıtay Dergisi**, C. 17, S. 4, Ekim 1991 s. 436-444.

ERGÜN İsmail, **Siber Suçların Cezalandırılması ve Türkiye’de Durum**, Ankara: Adalet Yayınları, 2008

ERSOY Yüksel, “*Genel Hukuki Koruma Çerçevesinde Bilişim Suçları*”, **Prof. Dr. Yılmaz Günel’a Armağan**, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayını, Cilt:49, No:3-4, 1994. s. 149-183.

ESEN Sinan, **Anlatımlı ve İçtihatlı Malvarlığına Karşı Suçlar, Belgede Sahtecilik ve Bilişim Alanında Suçlar**, Ankara: Adalet Yayınevi, 2007

GEDİK Doğan, “*Bilişim Suçlarında İp Tespiti İle Ekran Görüntüleri Çıktılarının İspat Değeri*”, **Bilişim Hukuku Dergisi**, C. 1, S. 1, 2009 s. 51-84.

GIRGENTI Elkin, “*Computer Crimes*”, **American Criminal Law Review**, Annual Survey of White Collar Crime, Vol. 55, Issue 4, Fall 2018 s. 911-960.

GÖKCAN Hasan Tahsin/ARTUÇ Mustafa, **Türk Ceza Kanunu Şerhi, 5. Cilt (Md. 197-254)**, Ankara: Adalet Yayınevi, 2021

GÖKTÜRK Neslihan, “*Suçun Yasal Tanımında Yer Alan ‘Hukuka Aykırılık’ İfadesinin İcra Ettiği Fonksiyon*”, **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, C. 7, S. 1, 2016 s.

GÜL Ahmet, **Doğrudan-Dolaylı Bilişim Suçları, 3. Baskı**, Ankara: Seçkin Yayıncılık, 2021

GÜLER Dilek, “*Bilişim Sistemine Girme Suçu*”, **KTO Karatay Üniversitesi Hukuk Fakültesi Dergisi**, C. 3, S. 2, Temmuz 2018 s. 11-38.

GÜRLER Fazıl, **Yargıtay Kararları Işığında Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar**, Ankara: Yetkin, 2015

HAFIZOĞULLARI Zeki/ÖZEN Muharrem, **Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, 3. Baskı**, Ankara: U-SA Yayıncılık, Eylül 2017

HAFIZOĞULLARI Zeki/ÖZEN Muharrem, **Türk Ceza Hukuku Genel Hükümler, 12. Baskı**, Ankara: U-SA Yayıncılık, Eylül 2019

HAKEİRİ Hakan, **Ceza Hukuku Genel Hükümler, 22. Baskı**, Ankara: Adalet Yayınevi, 2019.

HELVACIOĞLU Aslı Deniz; “Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerinin İncelenmesi”, **İnternet ve Hukuk**, Derleyen: Yeşim M. Atamer, Bilgi Üniversitesi Yayınları, 1.Baskı, İstanbul, Ocak 2004 s. 277- 301.

İÇEL Kayıhan, “Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında ‘Avrupa Siber Suç Politikasının Ana İlkeleri’”, **İÜHFM, İnternet Özel Bölümü**, C. 59, S. 1-2, 2001 s. 3-10.

İÇEL Kayıhan, **Ceza Hukuku Genel Hükümler, 18. Baskı**, İstanbul: Beta, 2018

İÇEL Kayıhan, **Kitle İletişim Hukuku, 13. Baskı**, İstanbul: Beta, 2018

IFRAH Georges **Bilgisayar Ne Sayar: Rakamların Evrensel Tarihi XI**, (Çev. Kurtuluş Dinçer), Ankara: Tübitak Popüler Bilim Kitapları, 2002

İHTİYAROĞLU Uğur, “Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi”, **Hacettepe Üniversitesi Hukuk Fakültesi Dergisi**, C. 10, S. 2, 2020 s. 406-440.

İNANCI Halil, “Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü”, **İstanbul Barosu Dergisi**, C. LLX, S. 7-8-9, İstanbul 1998 s. 510-531.

KABADAYI Sami, **Bilişim Sistemine Girme Suçu(TCK m. 243)**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Ankara, 2021

KANGAL Zeynel T., “Ceza Hukukunda Varsayılan Rıza”, **Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi**, C. 15, S. 4, Ekim 2011 s. 223-251.

KANGAL Zeynel T., **Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması**, İstanbul: On İki Levha Yayınları, Eylül 2019

KANGAL Zeynel T., “Türk Ceza Hukukunda Haksız Tahrik”, **Erzincan Üniversitesi Hukuk Fakültesi Dergisi**, C. XIV, S. 3-4, 2010 s. 19-68.

KARAGÜLMEZ Ali, **Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri, 5. Bası**, Ankara: Seçkin Yayınevi, 2014

KARAKEHYA Hakan, “Türk Ceza Kanunu’nda Bilişim Sistemine Girme Suçu”, **TBB Dergisi** S. 81, 2009 s 1-24

KARAKURT Ahu, “Türk Ceza Kanunu’nda Hata”, **Ceza Hukuku Dergisi**, C. 4, S. 10, Ağustos 2009 s. 109-155.

KARAKURT EREN Ahu, “Sızma Testleri ile Türk Ceza Kanunu’nun 243, 244 ve 245/A Maddelerinde Düzenlenen Suçlar Arasındaki İlişkinin Değerlendirilmesi”, **Terazi Hukuk Dergisi**, C. 15, S. 164, Nisan 2020, s. 747-764.

KATOĞLU Tuğrul, **Ceza Hukukunda Hukuka Aykırılık**, Ankara: Seçkin Yayıncıları, 2003

KATOĞLU Tuğrul, “Ceza Hukukunda Suçun Mağduru Kavramının Sınırları”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C. 61, S. 2, 2012 s.657-694.

KATOĞLU Tuğrul, **Kesintisiz Suç (Mütemadi Suç)**, Ankara: Seçkin Yayınları, 2022

KAYA Mehmet Bedii, **İnternet Hukuku**, İstanbul: On İki Levha Yayıncılık, Ocak 2021

KAYAER Nebahat, “Türk Hukukunda Bilişim Sistemine Girme Suçu(TCK m.243.)”, **Ceza Hukuku Dergisi**, S. 39, Nisan 2019 s. 83-128.

KETİZMEN Muammer, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara: Adalet Yayınevi, 2008

KERR Orin S., “Cybercrime’s Scope: Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes”, **New York University Law Review**, Vol. 78, 2003, s. 1596-1668. <https://heinonline.org> (E.T. 11.12.2021)

KIZILTAN Mehmet Burak, **5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 2007

KOCA Mahmut, “Ceza Muhakemesinde Basit Yargılama Usulü”, **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, C. 7, S. 2, Aralık 2020 s. 173-195.

KOCA Mahmut, “YTCK’da Hukuka Uygunluk Sebepleri”, **Ceza Hukuku Dergisi**, C. 1, S. 1, Eylül 2016 s. 111-143.

KOCA Mahmut/ ÜZÜLMEZ İlhan, **Türk Ceza Hukuku Özel Hükümler**, 7. Baskı, Ankara: Adalet Yayınevi, 2020

KOCA Mahmut/ÜZÜLMEZ İlhan, **Türk Ceza Hukuku genel hükümler**, Gözden Geçirilmiş ve Güncellenmiş 14. Baskı, Ankara: Seçkin Yayınevi, 2021

KORKMAZ İbrahim, “Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu”, **Terazi Hukuk Dergisi**, C. 13, S. 142, Haziran 2018, s. 45-55.

KORKMAZ İbrahim, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Güncellenmiş 2. Baskı, Ankara: Seçkin Yayınları, Nisan 2019

KROMBHOLZ Katharina/HOBEL Heidelinde/HUBER Markus/WEIPPL Edgar, “Advanced Social Engineering Attacks”, **Journal Of Information Security And Applications**, Vol. 22, 2015 s. 113-122.

KURT Levent, **Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara: Seçkin Yayınevi, 2005

KÜZECİ Elif, **Kişisel Verilerin Korunması, 4. Baskı**, İstanbul: On İki Levha Yayıncılık, Mayıs 2020

MADEN Mehmet, **Ceza Hukukunda Kişisel Verilerin Korunması**, Ankara: Adalet Yayınevi, 2021

MAHMUTOĞLU Fatih Selami, “*Karşılaştırmalı Hukuk Bakımından İnternet Sijelerinin Ceza Sorumluluğu*”, **İÜHFİM, İnternet Özel Bölümü**, C. 59, S. 1-2, 2001, s.39-49.

MAHMUTOĞLU Fatih Selami, “*Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi*”, **İÜHFİM**, C. LXXI., S.1, 2013, s. 855-889.

MALKOÇ İsmail, **Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu**, C. 2, Ankara: Malkoç Kitabevi, 2007

MCQUADE Sam, “*Technology- enabled Crime, Policing and Security*”, **Journal of Technology Studies**, 2006
<http://scholar.lib.vt.edu/ejournals/JOTS/v32/v32n1/pdf/mcquade.pdf>, s. 32-42.

MERAN Necati, **Sahtecilik, Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar**, 2. Baskı, Ankara: Seçkin Yayınları, 2008

MİLLARD Christopher/HON Wk., “*Defining ‘Personal Data’ in e-Social Science*”, **Information, Communication & Society**, C. 15, S. 1, 2012,

MODOĞLU Gözde/DÜLGER Murat Volkan, **Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet İletişim Hukuku Uygulama Rehberi**, Ankara: Avrupa Birliği ve Konseyi Ortak Yayını, 2014

NORMAN Paul, “*Policing “Hi-Tech” Crime Within The Global Context: The Role Of Transnational Policy Networks*”, **Crime and The Internet**, Ed. David Wall, London: Routledge, 2001 s. 184-195. <https://www.taylorfrancis.com> (E.T. 11.12.2021)

ODLYZKO Andrew, **The History of Communications and its Implications for the Internet** s. 118-119. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=235284 (E.T.: 03.10.2021)

ÖNOK Murat, “*Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği*”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Prof. Dr. Nur Centel’e Armağan**, C.9, S. 2, 2013 s.1229-1269

ÖNTAN Yaprak, **Ceza Hukukunda Davranış ve Netice**, Ankara: Seçkin Yayıncılık, 2021

ÖZBEK Veli Özer, “*Elektronik Ortamda Saklı Bulunan Verilerin Delil Olarak Niteliği*”, **İÜHFİM: İnternet Özel Bölümü**, C. LIX. S. 1-2. İstanbul, 2001 s. 181-202.

ÖZBEK Veli Özer, “*İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları*” **DÜHFD**, C. 4, S. 1, İzmir, 2002 s. 101-158.

ÖZBEK Veli Özer, “*Neticesi Sebebiyle Ağırlaşmış Suçlar*”, **Ceza Hukuku Dergisi**, C. 2, S. 4, Ağustos 2007 s. 223-246.

ÖZBEK Veli Özer, “*Türk Ceza Hukukunda Hata(m.30)*”, **Ceza Hukuku Dergisi**, C. 3, S. 7, Ağustos 2008 s. 83-99.

ÖZBEK Veli Özer/ DOĞAN Koray/ BACAKSIZ Pınar, **Türk Ceza Hukuku Genel Hükümler, Genişletilmiş ve Güncellenmiş 12. Baskı**, Ankara: Seçkin, 2021

ÖZBEK Veli Özer/ DOĞAN Koray/ BACAKSIZ Pınar, **Türk Ceza Hukuku Özel Hükümler, Genişletilmiş ve Güncellenmiş 16. Baskı**, Ankara: Seçkin, 2021

ÖZGENÇ İzzet, **Türk Ceza Hukuku Genel Hükümler, Gözden Geçirilmiş ve Güncellenmiş 17. Baskı**, Ankara: Seçkin Yayıncılık, 2021

ÖZÇELİK Büşra, **Bilişim Sistemine Girme Suçu**, İstanbul: On İki Levha Yayınları: İstanbul Ceza Hukuku ve Kriminoloji Arşivi, 2021

ÖZEL Cevat, “*Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı*”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ocak 2004 s. 341-361.

ÖZEN Muharrem/BAŞTÜRK İhsan, **Temel Hak ve hürriyetler Bağlamında İlişim-İnternet ve Ceza Hukuku**, Ankara: Adalet Yayınevi, 2011

ÖZEN Muharrem/ÖZCAK Gürkan, “*Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)*”, **Ankara Barosu Dergisi**, S. 2015/1 s. 69-70.

ÖZEN Mustafa, **Ceza Hukuku Genel Hükümler Dersleri**, Ankara: Adalet Yayınevi, 2019

PARLAK Oğuzhan Emre, **Türk Ceza Muhakemesinde Bilişim Sistemlerinde Arama, Kopyalama ve Elkoyma**, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2019

PARLAR Ali, **Türk Ceza Hukukunda Bilişim Suçları, 3. Basım**, Ankara: Bilge Yayınevi 2015

PARLAR Ali/HATİPOĞLU Muzaffer, **Açıklamalı-Yeni İçtihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu, 4. Cilt (230-245. Maddeler)**, Ankara: Seçkin Yayıncılık, 2011

PARLAR Ali/ÖZTÜRK Mustafa, **Doğrudan ve Dolaylı Bilişim Suçları ve Bilişim Sistemleri Aracılığıyla İşlenen Suçlar**, İstanbul: Aristo Yayınları, Mart 2020

SARZANA Carlo, “*Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması İtalya’daki Durum*”, Çev. Vesile Sonay Daragenli, **İstanbul Hukuk Fakültesi Dergisi**, Prof. Dr. Türkan Rado’ya Armağan Sayısı, , C.LV, S.3 İstanbul 1997s. 389-405.

SEMİZ Murat, **Bilişim Suçları ve Soruşturma Yöntemleri**, Ankara: Adalet Yayınevi, Ocak 2020

SINAR Hasan, **İnternet ve Ceza Hukuku**, İstanbul: BETA, 2001

SINAR Hasan, “İnternet’in Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı”, **Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni Yılmaz Altuğ’a Armağan**, C. 17, S.1-2, İstanbul 2000 s. 355-372.

SIEBER Ulrich, “*Legal Aspects of Computer-Related Crime in Information Society-A Comcrime Study*”, **European Commission Information Society**, 1 Ocak 1998 s. 18 <https://www.law.tuwien.ac.at/sieber.pdf> (E.T. 15.12.2021)

SİEBER Ulrich, “*Bilişim Suçları*”, **Bilişim Teknolojileri ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku (Yazarın Seçilmiş Makaleleri)**, Editörler: Prof. Dr. Feridun YENİSEY, Av. Dr. Salih OKTAR, DR. Öğrt. Üyesi Zehra BAŞER DOĞAN, Ankara: Seçkin, 2021

SOKULLU AKINCI Fusun, “*Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi*”, **İÜHFM, İnternet Özel Bölümü**, C. 59, S. 1-2, 2001 s. 12-38.

SOYASLAN Doğan, **Ceza Hukuku Genel Hükümler, Güncellenmiş 9. Baskı**, Ankara: Yetkin Yayınları, 2020

SOYASLAN Doğan, **Ceza Hukuku Özel Hükümler, 13. Baskı**, Ankara: Yetkin Yayınları, 2020

ŞAHBAZ İbrahim, **Açıklamalı ve İçtihatlı Türk Ceza Kanunu, 3. Cilt (Madde 197-345), 5. Baskı**, Ankara: Yetkin Yayınları, 2020

TANILIR Mehmet Niyazi, **İnternet Suçları ve Bireysel Mahremiyet**, Ankara: Liberte Yayınları, 2002

TAŞDEMİR Kubilay, **Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları**, Ankara: Cantekin Matbaacılık, 2009

TAŞKIN Şaban Cankat, **Bilişim Suçları**, İstanbul: Beta Yayınevi, 2008

TAŞKIN Şaban Cankat, “*Bilişim Hukuku Uluslararası Uyuşmazlıklar*”, **Türkiye Barolar Birliği Dergisi**, S. 85, Aralık 2009 s. 332-372.

TAŞTEMUR Eda, **Türk Ceza Hukukunda Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu**, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, 2021

TEPE İlker, “*İnternet (Bilişim) Ceza Hukuku Örneğinde Türk Ceza Hukuku’ndaki Yeni Gelişmeler*” **Alman Türk Karşılaştırmalı Ceza Hukuku**, Yayına Hazırlayanlar Prof. Dr. Eric Hilgendorf, Prof. Dr. Yener Ünver, İstanbul, Yeditepe Üniversitesi Hukuk Fakültesi Yayın No: 17, 2010. S. 267—288.

TEZCAN Durmuş/ ERDEM Mustafa Ruhan/ ÖNOK Murat, **Teorik ve Pratik Ceza Özel Hukuku, Güncellenmiş 19. Basım**, Ankara: Seçkin, 2021

TOPALOĞLU Murat / ÖZKİŞİ Harun / TEKKANAT Egemen, **Bulut Bilişim**, Ankara: Seçkin Yayıncılık, 2017

TOPÇUOĞLU Pelin, **Türk Ceza Kanunu Kapsamında Bilişim Sistemine Girme Suçu**, İstanbul: Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, 2022

TURAN Metin, **Bulut Bilişim, 2. Baskı**, Ankara: Seçkin Yayıncılık, 2017

TURAN Metin, **Bilişim Hukuku, 5. Baskı**, Ankara: Seçkin, 2021

TÜRKOĞLU ARSLAN Esra, “*Hukuka Uygunluk Sebebi Olarak Hakkın Kullanılması*”, **Konya Barosu Dergisi**, C. 2, S. 1, 2018 s. 176.

ÜNVER Yener, “*Türk Ceza Kanunu’nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi*”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası İnternet Özel Bölümü**, Cilt. LIX, Sayı.1-2, İstanbul, 2001 s. 51-153

ÜNVER Yener, **Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer**, Ankara: Seçkin Yayıncılık, 2003.

VATİS Micheal, “*The Council of Europe 's Convention on Cybercrime*”, **Berkeley Technology Law Journal**, S. 18, 2014 s. 207-223.

WALDEN Ian, “*Harmonising Computer Crime Laws in Europe*”, **European Journal of Crime, Criminal Law and Criminal Justice**, Vol. 12”, Issue 4 (April 2004) s. 321-336.

YAR Majid, “*E-Crime 2.0: The Criminological Landscape of New Social Media*”, **Information & Communications Technology Law**, Volume 21, Issue 3, 2012 s. 207-219.

YAŞAR Osman/GÖKCAN Hasan Tahsin/ARTUÇ Mustafa, **Yorumlu Uygulamalı Türk Ceza Kanunu, C. V. Madde 197-251, 2. Baskı**, Ankara: Adalet Yayınevi, 2014

YAYCI Esra, **Bilişim Suçları**, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Ankara, 2007

YAZICIOĞLU Recep Yılmaz, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile**, İstanbul: Alfa Yayınevi, 1997

YAZICIOĞLU R. Yılmaz, “*Şifreli Yayınların Bilişim Suçları Karşısındaki Konumu*”, **Yargıtay Dergisi**, C. 25, S. 1-2, Ocak-Nisan 1999, s. 47-69.

YAZICIOĞLU R. Yılmaz, “*Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi*” **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, C.2, S. 2, İstanbul, 2005 s. 393-412.

YAZICIOĞLU R. Yılmaz, “*Hackerler Ve Bilişim Sistemine Girme Suçu (TCK. Md. 243)*” **Ord. Prof. Dr. Sulhi Dönmezer Armağanı**, C. II., Ankara: Türk Ceza Hukuku Derneği Atatürk Araştırma Merkezi Başkanlığı Yayını, 2008 s. 1236-1263.

YENİDÜNYA Ahmet Caner, “*Bilişim Sistemine Hukuka Aykırı Erişim Suçu*”, **Legal Fikri ve Sınai Haklar Dergisi**, C.1 S.4, 2005 s.1018-1042.

YENİDÜNYA Ahmet Caner, DEĞİRMENCİ Olgun, **Bilişim Suçları**, İstanbul: Legal Yayıncılık, 2003

YENİSEY Feridun, “*İnternet Suçlarının Yeni İşleniş Biçimleri*”, **Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001**, İzmir: Dokuz Eylül Üniversitesi Yayınları, 2002

YILDIZ Ali Kemal, “*Bilişim Sistemine Girme*”, **Özel Ceza Hukuku C. VIII: Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ile Bilişim Alanındaki Suçlar**, İstanbul: On İki Levha Yayıncılık 2020. S. 229-250.

YILDIZ Sevil, **Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi**, Ankara: Nobel Yayın Dağıtım, 2007

YILMAZ Sacit, **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Ankara, Adalet Yayınevi, 2016

YILMAZ Zahit/ APİŞ Özge, “*Karşılıksız Yararlanma Suçu (TCK m. 163.)*”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Prof. Dr. Nur Centel’e Armağan, C. 19, S. 2, 2013 s. 1749-1780.

YILMAZ Zahit/ APİŞ Özge, “*Seri Muhakeme ve Basit Yargılama Düzenlemelerinin Değerlendirilmesi*”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 26, S. 1, 2020 s. 62-106.

YOR Mojid / STEINMETZ Kevin F., **Cybercrime and Society. Third Edition**, London: Sage Publications, 2019

İnternet Kaynakları

2003 TCK Tasarısı <https://www2.tbmm.gov.tr/d22/1/1-0593.pdf>

Avrupa Konseyi, **Avrupa İnsan Hakları Sözleşmesi**, https://www.echr.coe.int/documents/convention_tur.pdf (E.T. 16.12.2021)

Conseil of Europe, **Convention on Cybercrime**, 23.11.2001 <https://rm.coe.int/1680081561>

Council of Europe, **Chart of Signatures and Ratifications of Treaty 185**, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=185> (E.T. 15.11.2021)

Conseil of Europe, **Explanatory Report to the Convention on Cybercrime**, 23.11.2001 <https://rm.coe.int/16800cce5b>

TÜİK, **2021 Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması** [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanım-Arastirmasi-2021-37437](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanım-Arastirmasi-2021-37437) (E.T. 11.04.2022)

Resmi Gazete, **3756 Sayılı 765 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun**, T. 14.06.201991 <https://www.resmigazete.gov.tr/arsiv/20901.pdf> (E.T. 19.10.2021 14:05)

Resmi Gazete, **5271 Sayılı Ceza Muhakemeleri Kanunu** <https://www.resmigazete.gov.tr/eskiler/2004/12/20041217.htm#1> (E.T. 16.12.2021)

Resmî Gazete, **6098 Sayılı Kişisel Verilerin Korunması Kanunu**, 07.04.2016
<https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf> (E.T. 31.10.2021)

Resmi Gazete, **6533 Sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun**, S. 28988, T. 22.04.2014
<https://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm> (E.T. 15.11.2021)

Resmi Gazete, **7188 Sayılı Ceza Muhakemesi Kanunu Ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun**, S. 30928, T. 24.10.2019
<https://www.resmigazete.gov.tr/eskiler/2019/10/20191024-25.htm> (E.T. 22.12.2021)

Resmi Gazete, **Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik**, 20.11.2011
<https://www.resmigazete.gov.tr/eskiler/2011/09/20110920-4.htm> (E.T. 08.12.2021).

Resmi Gazete, **İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**
<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf> (E. T. 03.10.2021 00:35)

Resmi Gazete, **İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik**
<https://www.resmigazete.gov.tr/eskiler/2007/11/20071130-6.htm>

Resmi Gazete, **Sanal Ortamda İşlenen Suçlar Sözleşmesi**, S. 29083, T. 09.08.2014
<https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5-1.pdf> (E.T. 15.11.2021)

Türk Ceza Kanunu Madde Gerekçeleri www.lexpera.com.tr (E. T. 12.04.2021)

Türkiye Cumhuriyeti Adalet Bakanlığı, **Bilişim Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı**, 2006 <https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/>

Google, **İçeriği Google'dan Kaldırma - Yasal Yardım**,
<https://support.google.com/legal/troubleshooter/1114905?hl=tr> (E.T. 27.06.2022)

Twitter, **Kaldırma Talepleri - Twitter Şeffaflık Merkezi**,
<https://transparency.twitter.com/tr/reports/removal-requests.html#2021-jan-jun> (E.T. 27.06.2022)

<https://heinonline.org>

www.kazanci.com

www.lexpera.com.tr

<https://sozluk.gov.tr>

<https://www.taylorfrancis.com>

Yargı Kararları

AIHM Büyük Daire, Bărbulescu v. Romanya, Başvuru No: 61496/08, T. 05.09.2017
<https://hudoc.echr.coe.int/> (E.T. 16.12.2021)

AIHM 4. Daire, Copland v. Birleşik Krallık, Başvuru No: 62617/00, T. 03.04.2017
<https://hudoc.echr.coe.int/> (E.T. 16.12.2021)

AYM Birinci Bölüm, B.Y. Kararı, Başvuru No: 2018/30296, T. 07.09.2021, RG S. 31628 T. 14.10.2021 <https://www.resmigazete.gov.tr/eskiler/2021/10/20211014-4.pdf> (E.T. 06.05.2022)

AYM Birinci Bölüm, H. Ö. Kararı, Başvuru No: 2019/20473, T. 03.02.2022, Resmi Gazete S. 31782 T. 18.03.2021 <https://www.resmigazete.gov.tr/eskiler/2022/03/20220318-18.pdf> (E.T. 06.05.2022)

AYM İkinci Bölüm, Ömür Kara ve Onursal Özbek Kararı, Başvuru No: 2013/4825, T. 24.03.2016 Resmi Gazete S. 29708, T. 10.05.2016, <https://www.resmigazete.gov.tr/eskiler/2016/05/20160510-6.pdf> (E.T. 16.12.2021)

YCGK, E. 2007/6-136 K. 2007/150 T. 19.6.2007 www.lexpera.com.tr (E. T. 19.10.2021)

YCGK, E. 2009/11-193, K. 2009/268, T. 17.11.2009 <https://legalbank.net> (E.T. 08.12.2021)

YCGK, E. 2013/239, K. 2013/289, T. 11.6.2013 www.lexpera.com.tr (E. T. 04.10.2021)

YCGK, E. 2013/448, K. 2014/524, T. 25.11.2014 <https://legalbank.net> (E.T. 08.12.2021)

YCGK, E. 2014/288, K. 2016/255, T. 10.5.2016 www.lexpera.com.tr (E. T. 04.10.2021)

YCGK, E. 2015/12-11, K. 2019/148 T. 05.03.2019 www.lexpera.com.tr (E. T. 04.10.2021)

YCGK, E. 2016/544, K. 2020/127, T. 25.2.2020 www.lexpera.com.tr (E. T. 16.12.2021)

YCGK, E. 2016/23-1033, K. 2020/2, T. 14.01.2020 www.lexpera.com.tr (E. T. 04.10.2021)

YCGK, E. 2017/956, K. 2017/370, T. 26.09.2017 www.lexpera.com.tr (E. T. 16.12.2021)

YCGK, E. 2017/961, K. 2019/622, T. 22.10.2019 www.lexpera.com.tr (E. T. 16.12.2021)

YHGK, E. 2017/4-1340, K. 2018/1622, T. 06.11.2018 www.kazanci.com (E.T.15.12.2021)

Yar. 2. CD, E. 2014/17258, K. 2015/22546, T. 07.12.2015 www.lexpera.com.tr (E. T. 18.12.2021)

Yar. 4. CD, E. 2013/19106, K. 2014/14018, T. 28.04.2014 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 4. CD, E. 2014/2222, K. 2015/24755, T. 18.03.2015 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 8. CD, E. 2013/4668, K. 2014/9860, T. 16.04.2014 <https://lexpera.com.tr> (E.T. 04.12.2021)

Yar. 8. CD, E. 2013/15110, K. 2014/11220, T. 30.04.2014 <https://legalbank.net> (E.T. 11.12.2021)

Yar. 8. CD, E. 2013/16698, K. 2014/17652, T. 07.07.2014 www.lexpera.com.tr (E. T. 18.12.2021)

Yar. 8. CD, E. 2014/19342, K. 2015/2322, T. 03.02.2015 <https://legalbank.net> (E.T. 11.12.2021)

Yar. 8. CD, E. 2014/21961, K. 2015/12125, T. 18.02.2015 www.lexpera.com.tr (E. T. 12.12.2021)

Yar. 8. CD, E. 2014/28153, K. 2016/7842, T. 19.04.2016 <https://legalbank.net> (E.T. 04.12.2021)

Yar. 8. CD, E. 2014/29566, K. 2015/13421, T. 11.03.2015 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 8. CD, E. 2014/30037, K. 2015/14023 T. 18.03.2015 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 8. CD, E. 2014/35223 K. 2015/19051 T. 15.06.2015 www.lexpera.com.tr (E. T. 15.12.2021)

Yar. 8. CD, E. 2015/3445, K. 2015/22717, T. 14.10.2015 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 8. CD, E. 2015/6218, K. 2015/23910, T. 04.11.2015 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 8. CD, E. 2015/9713, K. 2016/1868, T. 18.02.2016 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 8. CD, E. 2015/13416, K. 2015/2470, T. 18.11.2015 <https://legalbank.net> (E.T. 04.12.2021)

Yar. 8. CD, E. 2016/2859, K. 2016/7187, T. 01.06.2016 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 8. CD, E. 2016/8243, K. 2017/4158, T. 13.4.2017 www.lexpera.com.tr (E. T. 10.12.2021)

Yar. 8. CD, E. 2016/104, K. 2016/7753, T. 13.06.2016 www.lexpera.com.tr (E. T. 21.12.2021)

Yar. 8. CD, E. 2016/11236, K. 2017/10500, T. 27.09.2017 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 8. CD, E. 2016/11922, K. 2017/6655, T. 07.06.2017 www.lexpera.com.tr (E. T. 19.12.2021)

Yar. 8. CD, E. 2016/12634, K. 2017/4967, T. 03.05.2017 <https://legalbank.net> (E.T. 04.12.2021)

Yar. 8. CD, E. 2016/12839, K. 2017/11114, T. 11.10.2017 www.lexpera.com.tr (E. T. 12.12.2021)

Yar. 8. CD, E. 2018/1078, K. 2018/2485, T. 08.03.2018 <https://legalbank.net> (E.T. 11.12.2021)

Yar. 8. CD, E. 2018/1810, K. 2019/6992, T. 16.05.2019 <https://legalbank.net> (E.T. 08.12.2021)

Yar 8. CD, E. 2018/10307, K. 2019/10751, T. 17.9.2019 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 8. CD, E. 2018/10824, K. 2019/15723, T. 25.12.2019 www.lexpera.com.tr (E. T. 10.12.2021)

Yar. 8. CE, E. 2018/11204, K. 2020/9307, T. 10.02.2020 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 8. CD, E. 2019/9478, K. 2020/15892, T. 23.09.2020 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 8. CD, E. 2019/19020, K. 2020/10577, T. 27.02.2020 <https://legalbank.net> (E.T. 04.12.2021)

Yar. 10. CD, E. 2004/14311 K. 2004/10906 T. 02.11.2004 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 11. CD, E. 2008/18190, K. 2009/3058, T. 26.03.2009 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 11. CD, E. 2009/22385, K. 2012/3683, T. 11.03.2012 kararı aktaran Osman Yaşar/Hasan Tahsin Gökcan/Mustafa Artuç, Yorumlu Uygulamalı Türk Ceza Kanunu, C. V. Madde 197-251, 2. Baskı, Ankara: Adalet Yayınevi, 2014 s. 7303.

Yar. 11. CD, E. 2011/3398, K. 2012/4441, T. 29.03.2012 www.lexpera.com.tr (E. T. 22.12.2021)

Yar. 11. CD, E. 2012/439, K. 2013/16403, T. 11.11.2013 <https://legalbank.net> (E.T. 18.12.2021)

Yar. 11. CD, E. 2014/7245, K. 2014/5492, T. 24.03.2014 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 12. CD, E. 2014/15082, K. 2015/1624, T. 02.02.2015 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 12. CD, E. 2013/27327, K. 2014/14176, T. 09.06.2014 (Kararı aktaran: Ümit Erdem/Çağrı Şükrü Uluslu/Gökberk Dumanlı, Yargıtay (2014-2016) Kararlarında Sosyal Medya, İstanbul: Legal Yayıncılık, 2016 s. 300-311.)

Yar. 12. CD, E. 2014/2525, K. 2014/17259, T. 08.09.2014 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 12. CD, E. 2014/11923, K. 2015/14, T. 12.01.2015 (Kararı aktaran: Ümit Erdem/Çağrı Şükrü Uluslu/Gökberk Dumanlı, Yargıtay (2014-2016) Kararlarında Sosyal Medya, İstanbul: Legal Yayıncılık, 2016 s. 300-311.

Yar. 12. CD, E. 2015/439, K. 2015/10716, T. 15.06.2015 www.lexpera.com.tr (E. T. 15.12.2021)

Yar. 12. CD, E. 2015/2309, K. 2015/15364, T. 14.10.2015 www.lexpera.com.tr (E. T. 16.12.2021)

Yar. 12. CD, E. 2015/9555, K. 2016/10731 T. 22.6.2016 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 12. CD, E. 2015/10388, K. 2017/1556, T. 01.03.2017 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 12. CD, E. 2015/16132, K. 2017/3999, T. 16.05.2017 www.lexpera.com.tr (E. T. 15.12.2021)

Yar. 12. CD, E. 2016/10818, K. 2017/7390, T. 11.10.2017 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 12. CD, E. 2018/8261, K. 2019/6852, T. 29.05.2019 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 12. CD, E. 2019/577, K. 2019/12248, T. 25.12.2019 www.lexpera.com.tr (E. T. 16.12.2021)

Yar. 13. CD, E. 2012/13503, K. 2014/16411, T. 06.05.2014 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 13. CD, E. 2014/2924, K. 2014/36282, T. 18.12.2014 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 13. CD, E. 2014/23539, K. 2015/8515, T. 06.05.2015 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 15. CD, E. 2013/74, K. 2014/14216, T. 09.09.2014 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 15. CD, E. 2013/13869, K. 2015/28709, T. 15.09.2015 <https://legalbank.net> (E.T. 08.12.2021)

Yar. 15. CE, E. 2015/11595, K. 2015/28323, T. 09.09.2015 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 15. CD, E. 2016/2793, K. 2016/7012, T. 22.09.2016 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 15. CD, E. 2017/14178, K. 2020/4067, T. 01.06.2020 www.lexpera.com.tr (E. T. 12.12.2021)

Yar. 15. CD, E. 2017/31912, K. 2018/2652, T. 17.04.2018 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 16. CD, E. 2015/4672, K. 2016/2330, T. 21.4.2016 www.lexpera.com.tr (E. T. 16.12.2021)

Yar. 17. CD, E. 2016/10724, K. 2018/12290, T. 10.10.2018 <https://legalbank.net> (E.T. 21.12.2021)

Yar. 23. CD, E. 2015/3995, K. 2015/6595, T. 16.11.2015 <https://legalbank.net> (E.T. 21.12.2021)



TEZ ONAY SAYFASI

Üniversite : T.C. GALATASARAY ÜNİVERSİTESİ
Enstitü : SOSYAL BİLİMLER ENSTİTÜSÜ
Hazırlayanın Adı Soyadı : Ahmet Alper AYDIN
Tez Başlığı : Türk Ceza Hukukunda Bilişim Sistemine Girme Suçu
Savunma Tarihi : 20 / 06 / 2022
Danışman : Doç. Dr. E. Eylem AKSOY RETORNAZ

JÜRİ ÜYELERİ:

Unvan, Ad-Soyadı

İmza

Prof. Dr. Pınar MEMİŞ KARTAL

Doç. Dr. E. Eylem AKSOY RETORNAZ

Dr. Öğr. Üyesi Osman Gazi GÜÇLÜTÜRK

Prof. Dr. M. Yaman ÖZTEK

Enstitü Müdürü