

^H**BİLİŞİM SİSTEMİNE GİRME SUÇU**
-Suçun Kamu Personeline ve Özel Sektör Çalışanlarına
Tahsis Edilen Bilgisayarlarla İşlenmesine İlişkin
Bir Değerlendirme-

Dr. Öğr. Üyesi Meral EKİCİ ŞAHİN*

Arş. Gör. Irmak KORUCULU**

Öz

Bilişim sistemleri, 20. yüzyılın ikinci yarısından itibaren yaşanan hızlı teknolojik gelişmelere bağlı olarak insan hayatına girmiş ve hayatın her alanını etkilemeye başlamıştır. Bugün hem özel hem de iş yaşamına ilişkin pek çok veri, bilişim sistemlerine kaydedilip, saklanmaktadır. Geçmişte çok az insanın erişim imkanına sahip olduğu bilişim sistemlerine, artık özel bir uzmanlığa gerek olmaksızın, herkes kolayca erişebilmekte, yetkisiz kişiler başkalarına ait bilişim sistemlerine hukuka aykırı yollarla girebilmektedir. Bu nedenle, bilişim sistemlerinin ve sistem içinde yer alan verilerin yetkisiz erişimlere karşı korunması önem kazanmıştır.

Bu bağlamda 5237 sayılı TCK'nın 243. maddesinin 1. fıkrasında, bir bilişim sistemine hukuka aykırı olarak girmek suç olarak düzenlenmiştir. Ancak, bilişim sistemi kavramından ne anlaşılması gerektiği tartışmalıdır. Öte yandan Türk ceza hukuku öğretisinde, "bilişim sistemine girme suçu" daha ziyade kişisel bilgisayarlar ve bilişim sistemleri üzerinden incelenmekte; ancak kamu personelleri ve özel sektör çalışanlarına tahsis edilen bilgisayarlar ile bilişim sistemlerine ilişkin problemler ihmal edilmektedir. Kanaatimizce, kamu personelleri ve özel sektör çalışanlarına tahsis edilen bilgisayarlar, bilişim sistemine girme suçu açısından özel olarak değerlendirilmelidir. Zira, kamu kurum ve kuruluşlarında ve özel sektör işyerlerinde

^H Hakem incelemesinden geçmiştir.

* Bursa Uludağ Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Öğretim Üyesi (e-posta: meralekicisahin@yahoo.de) ORCID: <https://orcid.org/0000-0002-5857-5662> (Makalenin Geliş Tarihi: 02.07.2018) (Makalenin Hakemlere Gönderim Tarihleri: 04.07.2018-05.07.2018-14.12.2018/Makale Kabul Tarihleri: 08.11.2018-02.12.2018-15.01.2019)

** Sakarya Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı (e-posta: irmakkoruculu@sakarya.edu.tr) ORCID: <https://orcid.org/0000-0002-2112-5094> (Makalenin Geliş Tarihi: 02.07.2018) (Makalenin Hakemlere Gönderim Tarihleri: 04.07.2018-05.07.2018-14.12.2018/Makale Kabul Tarihleri: 08.11.2018-02.12.2018-15.01.2019)

görev yapan personelin kendilerine tahsis edilmiş olan bilgisayarları ortak kullanmaları istisnai bir durum değildir. Bu nedenle işlerin yürütülmesi sırasında, çalışanların bilişim sistemine girme suçunu işleyebilmeleri için, özel bazı şartların aranıp aranmayacağının belirlenmesi uygulama açısından önemlidir.

Bu çalışma, kişisel bilgisayarlar ile kamu personellerine ve özel sektör çalışanlarına tahsis edilen bilgisayarlar arasında bilişim sistemine girme suçunun unsurları açısından fark olup olmadığı sorusuna bir cevap verebilmek amacıyla yapılmıştır. Çalışmada bilişim sistemine girme suçu incelenmiş, kamu personellerine ve özel sektör çalışanlarına tahsis edilen bilgisayarlara ilişkin özellik arz eden hususlar incelenmiştir. Ancak 24.03.2016 tarih ve 6698 Sayılı Kanunla TCK m. 243'e 4. fıkra olarak eklenen "veri nakillerini teknik araçlarla izleme suçu", bilişim sistemine girme suçuyla aynı maddede düzenlenmiş olmasına rağmen, bağımsız bir suç olduğundan çalışmanın kapsamı dışında bırakılmıştır.

Anahtar Kelimeler

Bilişim sistemi, bilişim sistemine girme suçu, kamu personellerine ve özel sektör çalışanlarına tahsis edilen bilgisayarlar, rıza, kamu hizmeti

UNAUTHORIZED ACCESS TO IT SYSTEMS

-An Evaluation Regarding Computers Assigned to Public And Private Sector Employees In Terms Of The Crime-

Abstract

Information systems has been come into human life, since the second part of twentieth century as a result of rapid technological developments and has begun to affect every area of life. Today; a great many of information related with both private and business life has been recorded and saved in information systems. In the past, very few people has a right of access to information systems. Today without any need for special expertness, everybody can access easily. Even unauthorized people can access to information systems which belong to other people in unlawful ways. For this reason, protection of information systems and information takes part in that system against unauthorized accesses has been gained great importance in terms of criminal law.

In Turkish Criminal Code No. 5237 art. 243/1 accessing information system illegal has been prepared as a crime. On the other hand, what should be understood from information systems notion, what should be considered in this notion should be discussed. Discussion is important in terms of identification of punished and unpunished acts. In Turkish criminal law discipline, "unauthorized access to IT systems" has been considered rather on personal computers and information systems but, problems related with computers assigned to public and private sector

employees and information systems has been neglected. To our knowledge, computers assigned to public and private sector employees should be considered separately in terms of unauthorized access to IT systems. Because, if public and private sector employees use computer which belongs to other personnel constitutes a crime or not is an important question that should be answered. Studies done for answering this question will lead the way to application.

This study has been done for the purpose of if computers assigned to public and private sector employees should be assessed separately or not in terms of unauthorized access to IT systems; giving an answer to a question related with if there is a difference between personal computers and computers which are assigned for the purpose of doing community service or not, in terms of commission of offence and scrutinizing problems related with the subject.

In the study, were examined in detail. But, with the Code No. 6698 dated 24.03.2016, which was added as a fourth paragraph art. 243, is excluded from the scope of the work, because it is an independent offense, even though it is regulated in the same Article.

Keywords

IT system, unauthorized access to IT systems, computers assigned to public and private sector employees, consent, public welfare

I. GENEL AÇIKLAMALAR

Bilişim sistemleri; insan müdahalesi olmadan otomatik işlem yapabilen, veri işleyebilen, saklayabilen, toplayabilen, veri iletebilen ve genel amaçlı kullanılabilme özelliğine sahip olan sistemlerdir¹. Bilişim sistemleri, teknolojiadaki gelişmelere bağlı olarak hem özel hem de iş hayatının vazgeçilmezi haline gelmiştir. Bugün modern insan, ne özel yaşamında ne de kamusal yaşamında bilişim sistemlerinden uzak durabilir. Bireyin, bilişim sistemleriyle olan ilişkisi arttıkça; sistem içinde yer alan verilerin güvenliği ve saklanması önemli bir sorun haline gelmektedir. Zira, teknolojik gelişmelere bağlı olarak, sadece veri işleyebilen ve veri saklayabilen sistemler ortaya çıkmamış; bilişim sistemlerine karşı veya bu sistemler aracı kılınarak² yeni suçlar da işlenmeye başlanmıştır. Bu suçlar arasında en çok işlenen; dışa açık olmayan bir bilişim sistemine haksız erişimdir³. Bilişim sistemine girme suçu olarak adlandırılan bu suç, başka suçların işlenmesine olanak sağladığı için, bilişim alanında işlenen diğer suçlar arasında özel bir yere sahiptir⁴. Diğer bir deyişle bilişim sistemine hukuka aykırı olarak erişim, başka suçların işlenmesi açısından potansiyel bir tehlike yaratır. Bu nedenle, ayrıca bir suç işlenmesini beklemeden, yalnızca bilişim sistemine girme fiilinin cezalandırılabilmesinin olanaklı hale getirilmesi anlamlıdır.

765 sayılı TCK m. 525a/1’de “*verilerin ele geçirilmesi*” suçu düzenlenmişti. Bu düzenlemeyle bilişim sisteminde bulunan verilerin hukuka aykırı olarak ele geçirilmesi cezai yaptırıma bağlanmıştı. Ancak, bir bilişim sistemine karşı en sık gerçekleştirilen ihlal olmasına rağmen, bilişim sisteminin güvenliği aşılarak sisteme girilmesi cezalandırılmıyordu. Bu husus, 765 sayılı TCK’nın yürürlükte olduğu dönemde eleştirilmiştir⁵.

¹ **Koca**, Mahmut/Üzülmez, İlhan: Türk Ceza Hukuku Özel Hükümler, 3. Baskı, Ankara 2016, s. 810; **Tezcan**, Durmuş/**Erdem**, Mustafa Ruhan/**Önok**, Murat R.: Teorik ve Pratik Ceza Özel Hukuku, 14. Baskı, Ankara 2017, s. 977.

² Öğretide “bilişim suçu” kavramı genellikle, bilişim sistemleri aleyhine işlenen suçlarla bilişim sistemleri aracılığıyla işlenen suçları birlikte kapsayacak şekilde kullanılmaktadır. Öğretide bilişim suçu yerine, “siber suç” kavramını kullananlar da vardır. Siber suç kavramının, hakaret, cinsel taciz veya dolandırıcılık gibi klasik suçların bilişim sistemleri aracılığıyla işlenmesini de kapsadığı kabul edilmektedir. Terminoloji konusundaki değerlendirmeler için bkz. **Önok**, Murat: “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”, Prof. Dr. Nur Centel’e Armağan, Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Özel Sayı, Y: 2013, C: 19, S: 2, s. 1231.

³ **Karagülmez**, Ali: Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri, 3. Baskı, Ankara 2011, s. 175. 2015 yılı adalet istatistiklerinde, hangi bilişim suçunun ne sıklıkla işlendiğine dair ayrıntılı bir veri yer almamakla birlikte; TCK m. 243- 246 arasında düzenlenmiş olan bilişim suçlarına ilişkin açılan davalardaki toplam suç sayısı 24314 olarak verilmiştir. Bkz. http://www.adlisicil.adalet.gov.tr/istatistik_2015/CEZA/33.pdf, Tarih: 11.04.2018.

⁴ **Ketizmen**, Muammer: Türk Ceza Hukukunda Bilişim Suçları, Ankara 2008, s. 79.

⁵ **Tezcan/Erdem/Önok**, s. 978; **Dülger**, Murat Volkan: Bilişim Suçları ve İnternet İletişim Hukuku, 4. Baskı, Ankara 2014, s. 321.

Türkiye, 10.11.2010 tarihinde Avrupa Konseyi Siber Suçlar Sözleşmesi'ni imzalamış ve sözleşme 22.04.2014 tarih ve 6533 sayılı “*Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanması ve Uygun Bulunduğuna Dair Kanun*” ile onaylanıp 02.05.2014 tarihli 28988 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Sözleşmenin 2. maddesinde;

“Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezai bir suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, söz konusu suçun, bilgisayar verilerini elde etmek veya başka bir sahtekar niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koşabilir.” şeklindeki düzenlemeyle taraf devletlere, bir bilgisayar sisteminin bütününe veya herhangi bir kısmına haksız erişimin suç olması için gerekli önlemleri alma yükümlülüğü yüklenmiştir.

Türk Ceza Kanunu 2003 hükümet tasarısının⁶ 346. maddesinde bulunan, “*bilişim sistemine giren veya orada kalmaya devam eden*” ibaresi, TBMM Genel Kurulundaki görüşmeler sırasında verilen bir önergeyle “*bir bilişim sistemine giren ve orada kalan*” şeklinde değiştirilmiş ve bilişim sistemine girme suçu bu şekilde yasalaşmıştır⁷. Ancak, bilişim sistemine haksız olarak girmenin münferit bir suç olarak değil, aynı zamanda sistemde haksız şekilde kalınmasıyla birlikte suç olarak düzenlenmesi öğretide eleştirilmiştir⁸. Avrupa Konseyi Siber Suçlar Sözleşmesiyle TCK arasındaki bu çelişkinin giderilmesi için “ve” yerine “veya” bağlacı getirilmesi gerektiği görüşü savunulmuştur⁹. Düzenlemenin bu halinin suçun işlenmesini zorlaştırdığı ve bu şekilde suçla korunan hukuki değer de zedelendiği görüşü öne sürülmüştür¹⁰. Nitekim, 24.03.2016 tarih ve 6698 sayılı kanunla 5237 sayılı TCK m. 243/1’deki “ve” bağlacı “veya” olarak değiştirilmiş; böylece TCK m. 243/1’deki düzenleme, Avrupa Konseyi Siber Suçlar Sözleşmesiyle uyumlu hale gelmiştir.

Yapılan son değişiklikten sonra 5237 sayılı Türk Ceza Kanunu’nun ikinci kitabının “*Topluma Karşı Suçlar*” başlıklı üçüncü kısmının “*Bilişim Alanında Suçlar*” başlıklı onuncu bölümünde m. 243’de yer alan “*bilişim sistemine girme suçu*”;

⁶ Tasarı ve gerekçesi için bkz. <http://www2.tbmm.gov.tr/d22/1/1-0593.pdf>, Tarih: 11. 04. 2018.

⁷ **Özbek**, Veli Özer/**Doğan**, Koray/**Bacaksız**, Pınar/**Tepe**, İlker: Türk Ceza Hukuku Özel Hükümler, 10. Baskı, Ankara 2016, s. 935.

⁸ **Dülger**, s. 321; **Apaydın**, Cengiz: “Bilişim Sistemine Girme Suçu”, TADD, Yıl 2016, S. 24, (s. 245-308), s. 266.

⁹ **Dülger**, s. 321; **Apaydın**, s. 266; **Karagülmez**, s. 203.

¹⁰ **Karagülmez**, s. 178.

(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) 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.”

şeklini almıştır.

II. SUÇ TİPİYLE KORUNAN HUKUKİ DEĞER

Bilişim sistemine girme suç tipiyle korunan hukuki değer ne olduğu konusunda doktrinde farklı görüşler bulunmaktadır. Bu suç tipiyle birden fazla hukuki değer korunduğu görüşü öğretilde yaygın olarak savunulmaktadır. Bazı yazarlar, TCK m. 243 ile bilişim sistemlerinin güvenliği ve güvenilirliğinin korunduğunu¹¹ kabul ederken; başkaları sistemin güvenliğinin yanında ayrıca özel hayatın gizliliği¹², sırların masuniyeti¹³, haberleşmenin gizliliği¹⁴, haber-

¹¹ Özbek/Doğan/Bacaksız/Tepe'ye göre bilişim sistemine girme suçuyla bilişim sistemlerinin güvenliği ve güvenilirliği korunmaktadır. Bkz. **Özbek/Doğan/Bacaksız/Tepe**, s. 933. **Akbulut'a** göre ise; korunan hukuki değer bilişim sisteminin güvenliği ve dokunulmazlığıdır. Bkz. **Akbulut**, Berrin: Bilişim Alanında Suçlar, 2. Baskı, Adalet Yayınevi, Ankara, 2017, s. 118. Benzer şekilde **Dülger'e** göre de bu suçla korunan hukuki değer; bilişim sisteminin güvenliğidir. Bu suç özel hayatının gizliliği, verilerin korunması ve güvenlik duygusu gibi farklı değerleri koruma altına alır. Ne var ki tüm bu değerleri kapsayacak olan üst kavram bilişim sisteminin güvenliğidir. Bkz. **Dülger**, s. 328. **Parlar'a** göre; bu suç tipiyle bilişim sisteminin güvenliğinin yanında, özel hayatın gizliliği de korunmaktadır. Bkz. **Parlar**, Ali: Türk Ceza Hukukunda Bilişim Suçları, 3. Baskı, Ankara 2015, 17.

¹² **Tezcan/Erdem/Önok'a** göre; bu suçla hem sistemin güvenliği hem de kişilerin özel hayatlarının gizliliğinin korunması amaçlanmıştır. Bkz. **Tezcan/Erdem/Önok**, s. 979. **Karakehya**, bu suçla korunan hukuki değer dijital hayattaki özel alan olduğunu savunmaktadır. **Karakehya**, Hakan: “Türk Ceza Kanunu’nda Bilişim Sistemine Girme Suçu”, TBBD Yıl 2009, S. 81 (187-210), s. 198.

¹³ **Kurt'a** göre; bilişim sistemine girme suçuyla özel hayatın gizliliği ve sırların masuniyetinin korunması amaçlanmaktadır. Bkz. **Kurt**, Levent: Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005, s. 148.

¹⁴ **Artuk/Gökçen/Yenidünya'ya** göre; bilişim sistemine girme suçuyla hem bireylerin özel hayatlarının gizliliği ve sırların masuniyeti hem de haberleşmenin gizliliği korunur. Bkz. **Artuk**, M. Emin/**Gökçen**, Ahmet/**Yenidünya**, A. Caner: Ceza Hukuku Özel Hükümler, 15. Baskı, Ankara 2015, s. 860; **Yenidünya**, A. Caner: “Bilişim Sistemine Hukuka Aykırı Erişim Suçu”, Legal Fikri ve Sınai Haklar Dergisi, Yıl: 1, Sayı: 4, İstanbul 2005, (s. 1017-1047), s. 1024.

leşme özgürlüğü¹⁵ ve mülkiyet¹⁶ gibi hukuksal değerlerden bir veya birkaçının birlikte korunduğu görüşünü savunmaktadır. Diğer yandan öğretilde, bilişim sistemine girme suçuyla malvarlığının korunduğunu kabul edenler de bulunmaktadır¹⁷. Suçun işlenebilmesi için bilişim sistemine yetkisiz olarak girildikten sonra sistemde kalmaya devam edilmesi gerektiğini savunan bir görüşe göreyse, suç tipiyle bilişim sistemini kullananların belli bir süreden sonra rahatsız edilmeme hakkı ve sistem kullanıcılarının menfaatleri korunur¹⁸.

Kanaatimizce bilişim sistemine girme suçu, birden fazla hukuki değeri koruyan, karma nitelikli bir suçtur. Bilişim sistemine girme suçuyla korunan hukuki değere ilişkin öğretildeki görüşlere genel anlamda katılmakla birlikte; suç tipiyle bilişim sisteminin güvenliği ve güvenilirliğinin, kişilerin özel hayatlarının gizliliği ve haberleşme özgürlüğünün koruma altına alındığını düşünmekteyiz.

Öncelikle bilişim sistemine girme suçunu düzenleyen TCK m. 243, Türk Ceza Kanunu'nun ikinci kitabının üçüncü kısmının "Bilişim Alanında Suçlar" başlıklı 10. bölümde düzenlenmiştir. Bu nedenle suçla korunan hukuki değer esas itibarıyla, bilişim sisteminin güvenliği ve güvenilirliğidir. Sisteme yetkisiz erişim, sisteme duyulan güveni ve sistemin güvenilirliğini zedeler. Bilişim sistemleri herkesin kullanımına açık olabileceği gibi bazen özellikle de içerdikleri bilgilerden dolayı sadece belirli kişilerin erişimine izin verecek şekilde koruma altına alınmış olabilir. Bu şekilde sınırlı erişime izin veren sistemlere yetkisiz erişimin ceza tehdidiyle karşı karşıya kalması, bilişim sistemlerinin bugünkü önemi dikkate alındığında yerinde bir düzenlemedir.

Bilişim sistemleri kişilerin özel hayatlarına ilişkin resimler, videolar, belgeler, özel bilgiler, başkalarıyla yapılan yazışmalar gibi pek çok veriyi içermektedir. Kişilerin özel hayatlarına ilişkin bu bilgiler genellikle kendilerine ait sistemler aracılığıyla bilişim sisteminin bir parçası haline gelmektedir. Bunun yanında kişilere ait kimlik bilgilerine, sağlık durumlarına, ekonomik durumlarına ilişkin kayıtlar da bilişim sistemlerinde depolanmaktadır. TCK m. 243, insanlara ilişkin kimi zaman onların bilgisi dahilinde, kimi zamansa bilgisi dışında oluşturulmuş pek çok özel bilgi içeren sistemlere usulsüz erişimlerin engellenmesi amacıyla ihdas edilmiştir.

¹⁵ *Erdağ'a* göre; bu suçla öncelikli olarak özel hayatın gizliliği ve *konut dokunulmazlığının ihlalinin elektronik şekli* olarak da nitelendirilebileceğinden, sırların dokunulmazlığı ve haberleşme özgürlüğü korunur. Bkz. **Erdağ**, Ali İhsan: "Bilişim Alanında Suçlar", Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. 14, Yıl 2010, S. 2, (s. 275-303), s. 5-6.

¹⁶ *Yaşar/Gökcan/Artuç'a* göre bu suçla korunan hukuki değer; kişilerin özel hayatlarının gizliliği, sırların masuniyeti ve haberleşme özgürlüğü ve mülkiyet hakkıdır. Bkz. **Yaşar**, Osman/**Gökcan**, Hasan Tahsin/**Artuç**, Mustafa: Yorumlu Uygulamalı Türk Ceza Kanunu, 2. Baskı, C. V, Ankara, 2014, s. 7287.

¹⁷ *Ketizmen'e* göre; bu suçla korunan hukuki değer malvarlığıdır. Bkz. **Ketizmen**, s. 99.

¹⁸ **Karagülmez**, s. 180.

Teknolojik gelişmeler bilişim sistemlerini, haberleşme açısından önemli bir noktaya taşımıştır. Telefonlar, basit iletişim araçları olmaktan çıkmış, küçük bilgisayarlar dönüşmüştür. Akıllı cep telefonlarına yetkisiz erişim sağlandığında, sistem sahibinin başkalarıyla yaptığı haberleşmenin gizliliği de ihlal edilebilmektedir. Haberleşme amacıyla kullanılan bilişim sistemine hukuka aykırı olarak girildiğinde, yalnızca izinsiz girilen bilişim sisteminin ait olduğu kişinin değil, onunla haberleşen kimselerin “haberleşme özgürlükleri” de ihlal edilir. Bu nedenle, bilişim sistemine girme suç tipiyle haberleşme özgürlüğünün korunduğu da söylenebilir¹⁹.

III. BİLİŞİM SİSTEMİNE GİRME SUÇUNUN MADDİ UNSURLARI

A. Suçun Maddi Konusu

Bilişim sistemine girme suçunun maddi konusu “bilişim sistemidir”. Bilişim sistemi dendiğinde aklımıza ilk olarak bilgisayarlar gelir. Ancak bilişim sistemi, bilgisayarı da içine alan bir üst kavramdır²⁰. Bilişim sistemine girme suçunun maddi konusunun doğru tespit edilebilmesi, “bilişim sistemi” kavramının sınırlarının net bir şekilde belirlenmesine bağlıdır. Bilişim sistemi kavramının sınırlarını belirlerken ilk bakılması gereken yer TCK m. 243’ün gerekçesidir. TCK m. 243’ün gerekçesine göre: “*Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir.*” Ancak gerekçede yapılan tanım, bilişim alanındaki gelişmeler göz önünde bulundurulduğunda yetersiz kalmaktadır. Ayrıca verilerin kim tarafından toplanacağı ve nereye yerleştirileceği hususu açık değildir²¹.

Bilişim kavramı, Türkçe sözlükte; “*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik*”²² şeklinde tanımlanmaktadır.

Öğretide yapılan tanımlara göre ise bilişim: içerisinde bilginin, saklanması, organizasyonunun yapılmasını, bu bilginin başka bir yere aktarılmasını ve yeniden kullanımını barındıran kuram ve tekniklerdir²³. Bu açıdan bilişim, özünde “veri işleme sürecini” ifade eder²⁴.

¹⁹ Tezcan/Erdem/Önok, s. 979.

²⁰ Erdağ, s. 279.

²¹ Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 934.

²² Türkçe Büyük Sözlük.

²³ Yıldız, Mehmet Emre: Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, Adalet Yayınevi, Ankara, 2015, s. 10; Baş, Eylem: Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, Yetkin Yayınları, Ankara, 2015, s. 25.

²⁴ Yıldız, s. 10.

Avrupa Konseyi Siber Suçlar Sözleşmesi'nin tanımlar başlığını taşıyan 1. maddesinde ise bilişim sisteminin değil bilgisayar sisteminin tanımı yapılmıştır. Buna göre:

“Bilgisayar sistemi; herhangi bir cihaz ve birbiriyle bağlantılı bir grup veya cihazlar yoluyla bir veya birden fazla program tarafından devam ettirilen verinin otomatik olarak işlenmesi, bu işlemin yerine getirilmesidir”.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 2/1-k maddesinde “veri” kavramı tanımlanmıştır. Buna göre; “*Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri*” ifade etmektedir. Avrupa Siber Suç Sözleşmesinin 1. maddesinde ise; “*Bilgisayar verisi: belirli durumların, bilgilerin kaydı ya da bir bilgisayarın bir işlemi gerçekleştirmesini sağlayacak biçimleri de içeren bilgisayar sisteminde icra edilebilecek bir işlemler bütünüdür*” şeklinde tanımlanmıştır. TCK m. 243'ün gerekçesinde ise, sistem içindeki bütün soyut unsurların “veri” terimini kapsadığı ifade edilmiştir.

Suçun maddi konusuna ilişkin olarak açıklanması gereken diğer bir kavram da “veri işleme” kavramıdır. Veri işleme: veriler üzerinde yapılan her çeşit işlemin genel adıdır²⁵. Kişisel Verilerin Korunması Kanunu m. 3'te kişisel verilerin işlenmesi; “*...kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*” olarak tanımlanmıştır. Bu tanımda yer alan veri işleme kavramı, veriler üzerinde bilgisayar ya da bilgisayara bağlı sistemlerle gerçekleştirilen her türlü işlemi kapsamaktadır²⁶.

Yargıtay kararlarında da “bilişim” ve “bilişim sistemi” kavramlarına ilişkin tanımlara yer verilmiştir²⁷. Yargıtay'a göre bilişim: “*...bilginin otomasyona tabi tutulması sonucunda işlenmesini yani verinin saklanması, organize edilmesi,*

²⁵ Akbulut, s. 13.

²⁶ Akbulut, s. 14.

²⁷ “...Bilişim kelimesi, Fransızca “*İnformatique*” kelimesinden Türkçeye çevrilmiş olup Fransızca ‘bilgi’ ve ‘otomatik’ kelimelerinin birleşiminden türemekte ve bilginin otomasyona tabi tutulması sonucunda işlenmesini yani verinin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılması anlamlarını içermektedir.” Bilişim suçu verilere karşı ve /veya veri işleme bağlantısı olan sistemlere karşı bilişim sistemleri aracılığıyla işlenen suçlar şeklinde tanımlanabilir. Bilişim suçlarının çok geniş ve sürekli ilerleyen bir alan olması sebebiyle 5237 Sayılı TCK’nda öğretide görüş birliğiyle bilgisayara karşılık geldiği belirtilen ‘bilgileri otomatik işleme tabi tutan sistem’ yerine bu tür araçlarla işlenen suçları da kapsayabilmesi ve yeni teknolojik ilerlemelere açık olması amacıyla ‘bilişim sistemi’ terimi kullanılmıştır...”, YCGK, E. 2014/15-288, K. 2016/255, T. 10.05.2016, www.kazanci.com.tr, Erişim Tarihi: 25.05.2018.

değerlendirilmesi, nakledilmesi, çoğaltılması anlamlarını içerir. Bilişim sistemi ise; bilgisayara karşılık gelen bilgileri otomatik işleme tabi tutan sistemlerdir.”

Bu tanımlardan, bilişim sistemlerinin başında bilgisayarların geldiği sonucuna ulaşılmaktadır. Bilgisayarı işlevsel hale getiren unsurlar ise donanım ve yazılımlardır²⁸. Donanım, bilişim sistemini meydana getiren fiziki parçaları ifade etmek için kullanılan bir kavramdır. Yazılım ise; donanımın veri işlem yapmasına yarayan soyut öğeleri ifade eder²⁹. Bilişim sistemi dendiğinde ilk akla gelen bilgisayar olsa da bilişim sistemi kavramı bilgisayarlarla sınırlı değildir³⁰. Nitekim bilişim sistemi, bilgisayar, çevre birimleri, iletişim altyapısı ve programlarından oluşan veri işleme saklama ve iletmeye yönelik sistem şeklinde de tanımlanmaktadır³¹. Bu doğrultuda; akıllı cep telefonları da bilişim sistemine girme suçunun konusunu oluşturmaktadır³².

Suçta konu bilgisayar veya diğer bilişim sistemleri, kişisel bilgisayar veya cep telefonu gibi gerçek kişilere ait olabileceği gibi özel veya kamu hukuku tüzel kişilerine ait de olabilir. Bu açıdan, diğer şartlar yerine getirildiğinde özel veya resmi işyerinde bulunan bilgisayarlar üzerinde de bu suç işlenebilir. Kamu kurum ve kuruluşlarıyla, özel işyerlerinde bulunan bilişim sistemlerine ilişkin ayrıntılı değerlendirme eylem başlığı altında yapıldığından, konu üzerinde tekrara düşmemek adına burada ayrıca durulmamıştır.

B. Fail

Bilişim suçları ilk ortaya çıktığında, bilişim suçlarının bu işi meslek edinen veya gelişmiş bir bilişim sistemine sahip olan kişilerce işlenebileceği kabul

²⁸ Baş, s. 27.

²⁹ Akbulut, s. 125.

³⁰ Tezcan/Erdem/Önok, s. 980.

³¹ Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı m. 2, <http://www.tbd.org.tr>, Tarih: 22.05.2018.

³² “...Somut olayda; katılanın cep telefonundan çekilmediği halde sanığın; “Sen Hacer’i değil, parayı seviyorsun..., kızım seninle görüşmez, bırak kızımın peşini, dolanma peşinde, seni uyandırıyorum, Hacer’in seninle işi olmaz, bir daha bir araya gelmeniz ben hayattayken imkansız...” şeklindeki mesajı oluşturduğu ve telefonuna geldiği iddiasıyla boşanma dava dosyasında delil olarak ibraz ettiği bahisle açılan davada, sanık suçlamayı kabul etmemiş, bilirkişi raporunda ise iletişim detaylarında suçta konu mesajlaşmaya dair kayıt bulunmadığı, ancak cep telefonlarına özel yazılımlar yüklenerek veya internet vasıtasıyla mesaj oluşturulabileceği belirtilerek mesaj çekilen ve mesaj alan cep telefonlarının incelenip, iletişim kayıtlarıyla karşılaştırılması gerektiğinin bildirilmesi karşısında, cep telefonlarında mobil işletim sistemleri bulunduğu ve program yüklenebilmesinin mümkün olduğu gözetilerek, taraflara ait cep telefonları alınıp uzman bilirkişi tarafından incelenip, iletişim kayıtları ile karşılaştırılmak suretiyle program yükleme veya internette gönderme şeklinde suçta konu mesaj gönderilip gönderilmediğinin araştırılması, sonucuna göre sanığın hukuki durumunun tayin ve takdiri gerekirken, cep telefonlarının bilişim sistemine girme ve orada kalma suçunun konusunu oluşturmayacağından bahisle, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması,” Y. 8. CD. E. 2014/30037, K. 2015/14023, T. 18.03.2015, www.kazanci.com.tr, Erişim Tarihi: 25.05.2018.

ediliyordu³³. Ancak, teknolojinin gelişip yaygınlaşması ve kişisel bilgisayarların hemen her eve, hatta akıllı telefonlarla her cebe girmesiyle, bilişim suçları herkes tarafından işlenebilen suçlara dönüşmüştür³⁴. Bu açıdan bilişim sistemine girme suçu herkes tarafından işlenebilen, özel faillik sıfatı gerektirmeyen bir suçtur³⁵. Ancak doğal anlamda iradi hareket etme yetenekleri olmayan tüzel kişilerin³⁶ bilişim sistemine girme suçunun faili olmaları mümkün değildir³⁷.

Bilişim sistemine girme suçu, genellikle sistemin güvenlik duvarı aşıl原因arak, “hacker” ya da “cracker” olarak adlandırılan kişiler tarafından işlenmektedir. Bununla birlikte suç, bilişim ağları kullanılmadan, bir bilişim sisteminin düğmesine basıp oturum açmak suretiyle³⁸, bilişim alanında özel bilgisi olmayan herhangi bir kişi tarafından da işlenebilir. Uygulamada, uzaktan erişim ile bilişim sistemine girilmesi durumunda; IP numarası üzerine kayıtlı olan kişi, fail kabul edilmektedir. Ancak, ceza hukukumuzda objektif sorumluluk esası benimsenmediğinden, üzerine IP numarası kayıtlı olan kişinin otomatik olarak fail kabul edilip cezalandırılması hem Anayasa’ya hem de TCK’nın kusur sorumluluğuna ilişkin ilkelerine aykırıdır³⁹. Bu durumda suçu gerçekleştiren kişinin IP sahibi olup olmadığının araştırılması ve ispatı gerekmektedir.

Suçun aile bireyleri tarafından birbirine karşı işlenebilmesi de mümkündür. TCK m. 243 açısından, TCK m. 245/4’da düzenlenen banka ve kredi kartlarının kötüye kullanılması suçunda olduğu gibi yakın akrabalar açısından şahsi cezasızlık nedeni de öngörülmemiştir. Eşler veya aynı evde birlikte yaşayan aile bireyleri tedip hakkı gibi, eylemi hukuka uygun hale getiren bir neden bulunmadığı sürece bu suçun faili olabilirler.

Bilişim sistemine giren kişinin kamu görevlisi olması, suçun temel şekli açısından önemli olmadığı gibi, bu husus cezanın ağırlaştırılmasını gerektiren bir neden olarak da dikkate alınmamıştır. Bir hukuka uygunluk nedeni olmaksızın bilişim sistemine giren kamu görevlisinin, örneğin CMK m. 134 gereğince hukuka uygun olarak verilmiş bilgisayarda arama izni olmamasına veya CMK m. 135 gereğince iletişimin tespiti dinlenmesi veya kayda alınması kararı olmasına rağmen şüphelinin bilgisayarında arama yapan veya iletişimini sisteme girerek takip eden polis memurunun cezasında, özel sıfatı nedeniyle artırım yapılmaz.

³³ Artuk/Gökçen/Yenidünya, Özel Hükümler, s. 865-866; Akbulut, s. 120.

³⁴ Apaydın, s. 259; Akbulut, s. 120; Karagülmez, s. 183.

³⁵ Dülger, s. 336; Mahmutoglu, Fatih Selami: “Türk Ceza Kanunda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 72, S. 1, 2013, s. 859.

³⁶ Kangal, Zeynel, Tüzel Kişilerin Ceza Sorumluluğu, Ankara 2003, s. 125, 126.

³⁷ Dülger, s. 336.

³⁸ Koca/Üzülmez, Özel Hükümler, s. 812.

³⁹ Apaydın, s. 260.

C. Mağdur

Mağdur, suçun hukuki konusunu oluşturan bireysel, toplumsal veya kamusal nitelikteki varlık veya menfaatin sahibidir⁴⁰. Suç tipiyle korunan ve suçla ihlal edilen hak veya menfaatin sahibidir⁴¹. Öğretide kabul edilen bir görüşe göre; bilişim sistemine girme suçuyla korunan hukuki değer bilişim sisteminin güvenliği olduğundan; suçun mağduru belirli bir kişi olamaz⁴². Buna göre, bilişim sistemine girme suçunun mağduru toplumu oluşturan herkeştir. Bizim de iştirak ettiğimiz ikinci görüşe göre ise; bilişim sistemine girme suçunun mağduru, bilişim sistemi üzerinde hak sahibi olan kişidir⁴³.

Hukuka aykırı olarak kısmen veya tamamen erişilen veya hukuka aykırı olarak kalınmaya devam edilen sistem üzerinde hak sahibi olan kişi, bu suçun mağdurdur⁴⁴. Bir bilişim sistemine girme yetkisine sahip olan ve bu yetkisini doğrudan kullanabilen kişiler o bilişim sistemi üzerinde hak sahibidir⁴⁵.

Tüzel kişilerin bilişim sistemine girme suçunun mağduru olup olamayacağı hususunda öğretide farklı görüşler bulunmaktadır. Bir görüşe göre; bu suçun mağduru hem gerçek hem de tüzel kişiler olabilir⁴⁶. Aksi görüşe göreyse; suçun mağduru yalnızca gerçek kişiler olabilir. Tüzel kişilerse mağdur değil, ancak suçtan zarar gören sıfatına sahip olabilirler⁴⁷. Bu konuda ortaya konan üçüncü bir görüş ise; “hukuka aykırı olarak erişilen bilişim sistemi bir kamu tüzel kişisine veya özel hukuk tüzel tüzel kişisine aitse, mağdur belirli bazı kişiler olabileceği gibi toplumun tamamı da olabilir” şeklindedir⁴⁸. Kanaatimizce gerçek kişiler gibi tüzel kişiler de bir bilişim sistemi üzerinde hak sahibi olabilirler. Bilişim sistemi üzerinde hak sahibi olan bir banka, başka bir özel şirket veya kamu hukuku tüzel kişisi bilişim sistemine girme suçunun mağduru olabilir⁴⁹.

⁴⁰ **Toroslu**, Nevzat/**Toroslu**, Haluk: Ceza Hukuku Genel Kısım, Ankara 2018, 114.

⁴¹ **Demirbaş**, Timur: Ceza Hukuku Genel Hükümler, 12. Baskı, Ankara 2018, s. 556.

⁴² **Tezcan/Erdem/Önok**, s. 979.

⁴³ **Koca/ Üzülmmez**, Özel Hükümler, s. 809; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 934; **Yenidünya**, s. 1027.

⁴⁴ **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s. 867; **Yenidünya**, s. 1027.

⁴⁵ **Koca/Üzülmmez**, Özel Hükümler, s. 809; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 934; **Yenidünya**, s. 1027.

⁴⁶ **Yenidünya**, s. 1027.

⁴⁷ **Dülger**, s. 340; **Mahmutoğlu**, s. 860.

⁴⁸ **Akbulut**, s. 121.

⁴⁹ Ancak **Mahmutoğlu**’na göre; bir bankanın bilişim sistemine girerek müşteri bilgilerinin incelenmesi durumunda, bilgileri incelenen her bir müşteri suçun mağduru, banka tüzel kişiliği ise suçtan zarar görendir. Bkz. **Mahmutoğlu**, s. 859, dp. 18. Bir bankanın bilişim sistemi üzerinde, bankanın müşterileri değil, tüzel kişi olan banka hak sahibidir. Bu nedenle kanaatimizce bankanın müşterileri bilişim sistemine girme suçunun mağduru değildir. Müşteriler suçtan zarar gören olabilirler. Ayrıca bankanın bilişim sistemine yetkisiz olarak girildikten sonra müşterilerin bilgilerinin kaydedilmeksizin ele geçirilmesi TCK m. 136’da düzenlenmiş olan kişisel verileri hukuka aykırı olarak ele geçirme suçunu oluşturur.

Suç mağdur bakımından özellik göstermemektedir. Bilişim sistemi üzerinde hak sahibi olan kişinin sıfatı suçun oluşumu açısından önemsizdir. Bir kamu görevlisinin veya başkasının bilişim sistemine hukuka aykırı olarak girmesi arasında fark bulunmamaktadır.

D. Eylem

1. Genel Olarak

TCK m. 243/1'de düzenlenen bilişim sistemine girme suçunun oluşabilmesi için; fail bir bilişim sistemine hukuka aykırı olarak girmeli veya hukuka aykırı olarak sistemde kalmaya devam etmelidir. 24.03.2016 tarih ve 6698 sayılı Kanunla yapılan değişiklik öncesinde bu suçun oluşabilmesi için bir bilişim sistemine hukuka aykırı olarak girilmesi ve sistemde kalmaya devam edilmesi gerekiyordu. Gerekçeyle çelişen bu durum 6698 sayılı Kanunla düzeltilmiştir. Böylece bilişim sistemine girme suçu; bir bilişim sistemine hukuka aykırı olarak girilmesi veya sistemde kalınmaya devam edilmesiyle tamamlanır hale gelmiştir. Kanunun mevcut haliyle, failin sisteme kasten ve hukuka aykırı olarak girmesi suçun oluşması için yeterlidir⁵⁰. Ayrıca sistemde belirli bir süre kalmaya devam etmesine gerek yoktur.

Karşılaştırmalı hukukta bilişim sistemine haksız erişime ilişkin; “*yetkisiz erişim*”, “*yetkili erişimin aşılması*”, “*zorla erişim*”, “*hileyle erişim*” gibi farklı terimler kullanılmaktadır⁵¹. Türk ceza hukukunda ise bilişim sistemine haksız erişim için 5237 sayılı TCK m. 243'ün başlığında “*Bilişim Sistemine Girme*” terimi kullanılmıştır. Öğretide bu suçun eylem unsurunu açıklamak için kullanılması gereken doğru terminolojinin ne olduğu konusunda farklı görüşler bulunmaktadır. Bir görüşe göre; “*girme*” kelimesinin daha çok fiziksel alanlar için kullanılması ve bilişim sisteminin yapısı birlikte değerlendirildiğinde, fail tarafından gerçekleştirilen fiilin aslında bilişim sistemine “*girme*” değil, “*erişim*” olduğu görülür⁵². Çünkü bir bilişim sistemine “*girme*” tabiriyle kastedilen; bilişim sisteminden oluşan elektronik yapıdaki sanal ortama erişilmesidir. Erişim, ağ üzerinden olabileceği gibi, doğrudan fiziksel temasla sisteme girilerek de gerçekleştirilebilir⁵³. Aksi yöndeki görüşe göre ise; “*girme*” hem bilişim sistemine ağlar vasıtasıyla erişimi hem de bir düğmeye basarak sisteme dahil olmayı karşılar. Kanaatimizce de “*girme*” sözcüğü “*erişim*” terimine göre daha genel

⁵⁰ Gül, Ahmet: Doğrudan/Dolaylı Bilişim Suçları, Ankara, 2016, s. 56; Tezcan/Erdem/Önok, s. 980

⁵¹ Karagülmez, s. 175.

⁵² Karagülmez, s. 182; Apaydın, s. 254; Erdoğan, Yavuz: “Bilişim Sistemine Girme ve Kalma Suçu”, DEÜHFD, C. 12, Prof. Dr. Burhan Ceyhan’a Armağan Özel Sayısı, Yıl 2010, s. 1366 (s. 1363-1433).

⁵³ Parlar, Ali/Hatipoğlu, Muzaffer: Açıklamalı- Yeni İçtihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu, 4. Cilt, Seçkin Yayıncılık, Ankara, 2010, s. 3743.

olduğundan, yerinde ve isabetlidir⁵⁴. Ancak bu kavramlardan birini tercih edip, diğerinden tamamen vazgeçmek mümkün değildir.

Failin hukuka aykırı olarak bilişim sistemine girmesindeki asıl amaç, güvenlik duvarlarını aşarak ya da yeterli koruma olmamasından yararlanarak bir bilişim sistemine veya bilişim ağına erişim sağlamaktır⁵⁵. Kişinin yetkili olmadığı bir bilişim sistemine erişim sağlarken, sistemdeki güvenlik açıklarından yararlanarak sisteme bizzat kendi oluşturduğu güvenlik açıklarını kullanarak girmesi arasında fark yoktur⁵⁶. Bazı durumlarda bir bilişim sistemi herkese açık olabilir, ancak sistem içerisinde bulunan bir veriye erişim sınırlandırılmış olabilir. Böyle bir durumda, bilişim sistemine girme suçu herkesin erişimine açık olmayan, özel olarak erişimi kısıtlanmış veriye yetkisiz olarak erişim sağlandığında işlenir⁵⁷.

Bu suç; erişilmesi amaçlanan sistem açılıp işlem yapılmaya başlanmasıyla işlenebileceği gibi, internet aracılığıyla aynı ağa bağlı diğer bir sisteme hukuka aykırı olarak girilmesi veya orada kalınmasıyla da işlenebilir⁵⁸. Benzer şekilde, bilişim sistemine haksız erişim ağ aracılığıyla bilgisayarlarda oturum açılmak suretiyle sağlanabileceği gibi emanet edilen bilgisayar açılarak içindeki sosyal paylaşım hesabına izinsiz erişilmesiyle de işlenebilir⁵⁹. TCK m. 243'te bilişim sistemine girmenin ne şekilde olması gerektiği konusunda herhangi sınırlama yapılmamıştır⁶⁰. Bu nedenle bilişim sistemine girme suçu hem sisteme girme hem de sistemde kalma hareketleri açısından serbest hareketli bir suçtur⁶¹.

Bilişim sistemine girme suçu, bir bilişim sistemine hukuka aykırı olarak girme veya sistemde kalmaya devam etmek suretiyle işlenebilen seçimlik hareketli bir suçtur⁶². Failin sisteme hukuka aykırı olarak girmesiyle suç tamamlanır. Suçun tamamlanabilmesi için, failin sisteme girdikten sonra, ayrıca orada belli bir süre kalması da gerekmez⁶³. “Sistemde kalma” seçimlik hareketi açısından ise, önceki hareketin yani sisteme girme hareketinin hukuka aykırı olması şart değildir. Fail, bilişim sistemine hukuka uygun yollardan girmiş olsa bile, sistemde kalması veya kalmaya devam etmesi hukuka aykırıysa, suç oluşur. Bu seçimlik hareket açısından belirleyici olan failin hukuka aykırı bir şekilde,

⁵⁴ Akbulut, s. 129.

⁵⁵ Karagülmez, s. 185.

⁵⁶ Ketizmen, s. 103.

⁵⁷ Akbulut, s. 134.

⁵⁸ Dülger, s. 344; Karakehya, s. 201.

⁵⁹ Gül, s. 61.

⁶⁰ Parlar/Hatipoğlu, s. 3743.

⁶¹ Dülger, s. 343.

⁶² Akbulut, s. 126; Gören, Sami: En Son Değişikliklerle Açıklamalı-İçtihatlı 5237 Sayılı Türk Ceza Kanunu, Yetkin Basımevi, Ankara, 2012, s. 1311.

⁶³ Tezcan/Erdem/Önok, s. 980-981.

sistemde kalmaya devam etmesidir⁶⁴. Failin bilişim sistemine hukuka aykırı olarak girdikten sonra, sistemde kalmaya devam etmesi, iki ayrı bilişim sistemine girme suçunun oluşmasına yol açmaz. Bilişim sistemine girmek ve girdikten sonra sistemde kalmaya devam etmek, tek bir bilişim sistemine girme suçunun icra hareketleridir⁶⁵.

Bir bilişim sistemine hukuka aykırı (haksız) erişim⁶⁶; o bilişim sisteminde bulunan verilerin bir kısmına veya tamamına doğrudan (fiziken) veya uzaktan izinsiz erişimi ifade etmektedir⁶⁷. Bilişim sitemine haksız (yetkisiz) erişim, bilişim sisteminin ve bu sistemin kapsadığı verilerin gizlilik, bütünlük, kullanılabilirlik gibi hususları kapsayan güvenliğine yönelik tehdit ve saldırılar biçimindeki hukuka aykırı fiilleri ifade eder. TCK m. 243/1 anlamında bir bilişim sistemine girmek: varsa sistem güvenliğini devre dışı bırakarak⁶⁸ sistemin tamamına veya bir bölümüne haksız olarak erişmek anlamına gelir⁶⁹. Sisteme girilmesi genel olarak sınırlandırılmamış, ancak sistem üzerindeki belirli yerlere erişim sınırlandırılmışsa; sistemin geneline girmek suç olmasa bile girişi sınırlandırılmış olan

⁶⁴ Akbulut, s. 136.

⁶⁵ Akbulut, s. 126.

⁶⁶ Karagülmez, s. 185.

⁶⁷ "... Bilişim sistemine girmek", bir bilişim sisteminde bulunan verilen bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir. 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), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Bilgisayar veri ve sistemlerine yapılan izinsiz giriş, aynı zamanda, "bilgisayara tecavüz", "kod kırma" ya da "bilgisayar korsanlığı" olarak da tanımlanmaktadır. Suçun, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi bir ağ aracılığıyla oturumun açılması yoluyla da işlenebilir. Girmede, iletişimin kablolu veya kablosuz olması ile mesafenin yakın veya uzak olması arasında bir fark da yoktur. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinde bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine (windows, linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır..." Y. 8. CD., E. 2016/12839, K. 2017/11114, T. 11.10.2017, www.kazancı.com, Erişim Tarihi: 06.05.2018.

⁶⁸ "... Sanık ... olay tarihinde annesi ..'nın abonesi gözüktüğü ... numaralı cep telefonu hattıyla müşteki ...'nın e- posta adresine şifresini kırmak suretiyle müştekinin izni ve bilgisi olmaksızın erişim sağladığı ve müştekinin erişimini şifresini değiştirerek engellediği, ardından da kendisini müşteki ... 'nın arkadaşı ... olarak tanıtarak para talep ettiği, müştekinin arkadaşı ... ile telefonla görüşerek söz konusu mailin ... tarafından gönderilmediği ...'ya ait mail adresinin başkalarınca ele geçirildiğini öğrenmesi üzerine para göndermediği, sanığın bu şekilde üzerine atılı suçlu işlediğinin kabul edildiği olayda,... sanığın, müştekinin elektronik posta adresinin şifresini kırarak, hesaba giriş şifresini değiştirerek erişimi engellemesi şeklinde gerçekleşen eyleminin TCK'nın m. 244/2 maddesi kapsamında kaldığı halde aynı Kanun'un 243/1. maddesinden mahkumiyet hükmü kurulması kanuna aykırı olup...". Y. 15. CD., E. 2016/3871, K. 2016/8608, T. 15.12.2016, www.kazancı.com, Erişim Tarihi: 06.05.2018.

⁶⁹ Erdoğan, s. 1375; Tezcan/Erdem/Önok, s. 980.

yere yetkisiz veya izinsiz girilmesi de bu suçu oluşturur⁷⁰. Başkasına ait bilgisayar açılarak içindeki verileri görüntülenmesi şeklinde doğrudan sisteme girilebileceği gibi, başka bir cihaz yardımıyla uzaktan da sisteme girilebilir. Bununla birlikte, suçun oluşması için, failin sistem içerisinde bulunan belirli bir bilgi veya veriyi elde etmesi gerekmez⁷¹.

Bilişim sistemine girme suçu “girme” seçimlik hareketiyle işlendiğinde, icrai bir suçtur. Buna karşın, “sistemde kalma” seçimlik hareketi bakımından, bilişim sistemine girme suçunun ihmali bir suç olup olmadığı tartışmalıdır. Bir görüşe göre; sisteme girme icrai, sistemde kalmaya devam etme ise ihmali hareketle işlenir⁷². Aksi görüşe göre; sistemde kalma her zaman ihmali bir hareket olmak zorunda değildir. Çünkü; sistemdeki güvenlik önlemleri nedeniyle, fail sistemde kalmak için birtakım işlemler yapmak zorunda kalabilir⁷³. Bu nedenle bilişim sistemine girme suçunun “sistemde kalma” seçimlik hareketi hem icrai hem de ihmali nitelikte olabilir.

Bilişim sistemine girme suçunun düzenlendiği TCK m. 243’te ayrı bir neticeden bahsedilmemiştir⁷⁴. Bilişim sistemine girme suçu sırf hareket suçu, diğer bir ifadeyle neticesi harekete bitişik bir suçtur⁷⁵. Suç, kanunda gösterilen hukuka aykırı olarak “sisteme girme” veya “sistemde kalma” hareketlerinin yapılmasıyla tamamlanır⁷⁶. Sistemde bir zarar meydana gelmesine veya sistemin tehlikeye düşmesine gerek yoktur. Bu açıdan bilişim sistemine girme suçu soyut tehlike suçudur⁷⁷. Bununla birlikte bilişim sistemine hukuka aykırı erişim nedeniyle, sistem içinde bulunan veriler zarar görürse, TCK m. 243/3’te düzenlenen bilişim sistemine girme suçunun neticesi sebebiyle ağırlaştırılmış şekli oluşur.

Bu suçun oluşması için, failin kendisine veya bir başkasına menfaat temin etmesi gerekmez⁷⁸ de suç gerçek veya tüzel kişilerin yararına işlenebilir⁷⁹. Suçun bir tüzel kişinin yararına işlenmesi halinde, TCK m. 246 gereğince tüzel kişi hakkında güvenlik tedbirine hükmedilir⁸⁰.

⁷⁰ Tezcan/Erdem/Önok, s. 981; Akbulut, s. 134.

⁷¹ Taşkın, Şaban Cankat: Bilişim Suçları, İstanbul 2008, s. 26.

⁷² Ketizmen, s. 107.

⁷³ Dülger, s. 343.

⁷⁴ Esen, Sinan: Anlatımlı ve İçtihatlı Malvarlığına Karşı Suçlar Belgelerde Sahtecilik ve Bilişim Alanında Suçlar, Ankara 2007, 629.

⁷⁵ Dülger, s. 348, Yenidünya, s. 1035; Artuk/Gökçen/Yenidünya, Özel Hükümler, s. 863; Akbulut, s. 128.

⁷⁶ Karagülmez, s. 183.

⁷⁷ Dülger, s. 343; Kurt, s. 152; Parlar/Hatipoğlu, s. 3743; Yaşar/Gökçen/Artuç, C. V, s. 7294; Mahmutoglu, s. 862.

⁷⁸ Dülger, s. 332; Apaydın, s. 259.

⁷⁹ Mahmutoglu, s. 859.

⁸⁰ Dülger, s. 332; Tezcan/Erdem/Önok, s. 979; Apaydın, s. 259, Karagülmez, s. 184.

Suç, hukuka aykırı olarak “sistemde kalma” seçimlik hareketiyle işlendiğinde, fail sistemde kalmanın hukuka aykırı olduğunu bilmeli ve buna rağmen sistemde kalmaya devam etmelidir⁸¹. Bilişim sistemine girme suçu, sistemde kalma seçimlik hareketi açısından mütemadi bir suçtur⁸². Sistemde kalmanın hukuka aykırı olduğu anda suç tamamlanır⁸³, hukuka aykırı olarak sistemde kalmaya son verildiğinde suç da sonlanmış olur. Bu husus zamanaşımı ve suçun işlendiği yerin tespitinde göz önünde bulundurulmalıdır⁸⁴. Hukuka aykırı olarak bilişim sisteminde kalma seçimlik hareketi açısından, failin ne kadar süreyle sistemde kalması gerektiği kanunda gösterilmemiştir. Bu nedenle bilişim sisteminde kalmanın sürenin uzun veya kısa olmasının önemi yoktur⁸⁵. Bununla birlikte failin sistemde kaldığı süre, fiil sebebiyle ortaya çıkan tehlikenin ağırlığına bağlı olarak, temel cezanın belirlenmesinde göz önünde bulundurulabilir⁸⁶.

Belli tedbirler alınarak erişimin sınırlandırıldığı bilişim sisteminin işleyişine ancak işlem yapma yetkisine sahip kişiler müdahale edebilir⁸⁷. Kanunda açık bir düzenleme bulunmamakla birlikte, herhangi bir koruma veya güvenlik önlemi olmayan ve isteyen herkesin girebileceği bir sisteme erişim, hukuka aykırı değildir⁸⁸. Suçun oluşabilmesi için; sisteme girişi engelleyici şifre veya parola konmuş olması zorunlu değildir. Şifresiz bir sisteme, hukuka aykırı olarak girildiğinde de suç oluşur. Ancak, sisteme girmek için şifre konması, izinsiz veya yetkisiz girişlere rıza gösterilmediğine işaret eder. Hak sahibinin sisteme izinsiz girişlere müsaade etmediği açık veya zımni davranışlarından anlaşılıyorsa, bilişim sistemine girme suçu oluşur. Rıza alınmasına gerek olmadan, herkesin erişebildiği bir sisteme girmek ise suç değildir⁸⁹.

Bir bilişim sistemine erişime olanak sağlayan yetki, hukuka uygun usullerle verilmelidir. Yetkilendirmede hangi usule riayet edileceği, o bilişim sisteminde erişimi sınırlandıran yönetici birim tarafından belirlenir. Bu nedenle usulüne uygun alınmış kullanıcı adı veya şifresinin, bir başka kişi tarafından sahibinin rızası hilafına hukuka aykırı bir şekilde temin edilmesi ve bu suretle erişimin sağlanması bilişim sistemine hukuka aykırı (yetkisiz) erişimdir⁹⁰.

⁸¹ Özbe/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 937.

⁸² Karagülmez, s. 184; Parlar/Hatipoğlu, s. 3744; Gören, s. 1311.

⁸³ Artuk/ Gökçen/Yenidünya, Özel Hükümler, s. 862; Yaşar/Gökcan/Artuç, C. V, s. 7293.

⁸⁴ Dölger, s. 348.

⁸⁵ Tezcan/Erdem/Önok, s. 980, 981; Yenidünya, s. 1034.

⁸⁶ Özbe/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 937.

⁸⁷ Özbe/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 936.

⁸⁸ Şahbaz, İbrahim: Açıklamalı ve İçtihatlı Türk Ceza Kanunu 2. Cilt, Ankara 2016, s. 2739.

⁸⁹ Koca/Üzülmez, Özel Hükümler; s. 813; Özbe/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 936.

⁹⁰ Özbe/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 936.

2. Suçun Kamu Personeline ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarla İşlenmesi

Bilişim sistemine girme suçunun kamu personellerine ve özel sektör çalışanlarına tahsis edilen bilgisayarlarla işlenmesi, önemi nedeniyle burada ayrıca değerlendirilmelidir.

Bilindiği gibi kamu kurum ve kuruluşlarıyla özel sektör işyerlerinde bulunan bilgisayarlar genellikle belli bir personele zimmetlenir ve onun kullanımına tahsis edilir. Ancak bu bilgisayarların zaman zaman aynı kurumda çalışan diğer bir personel tarafından kullanılması istisnai bir durum değildir. Bu şekilde belli bir personele zimmetlenmiş olan bilgisayarın, başka bir personel tarafından açılması ve sisteme girilmesi halinde bilişim sistemine girme suçunun oluşup oluşmayacağı veya suçun hangi şartlar altında oluşacağı uygulama açısından önem arz etmektedir.

Kamu kurum ve kuruluşları, belirli bir ya da birden fazla kamu hizmetinin yürütüldüğü tüzel kişiliği haiz idare teşkilat birimi⁹¹ olup, devletin temel fonksiyonları olan yasama, yürütme ve yargı niteliği taşıyan kamu hizmetlerinin görüldüğü yerlerdir⁹². Diğer bir deyişle, kamu kurum ve kuruluşu, niteliğine bakılmaksızın kamuya ait işlerin görüldüğü her türlü yeri ifade eder⁹³.

Kamu görevlisi denince akla ilk olarak memurlar gelmektedir. Öğretide, memuru devletin mütemmim cüzü olarak gören; onu kamusal faaliyetlerin yürütülmesinde sürekli olarak görev alan kimse şeklinde tanımlayan yazarlar bulunmaktadır⁹⁴. Ancak kamu görevlisi kavramıyla kast edilen sadece memurlar değildir. Kamu görevlisi; idareyi soyut bir mekanizmadan, somut bir organizmaya çeviren; onu haklarla donatan ve yasaklarla sınırlayan işlem ve eylemleri gerçekleştiren; statüleri ve ait oldukları hukuki rejimleri farklı personelleri ifade eden bir üst kavramdır⁹⁵. Geniş anlamda kamu görevlisi tanımı yapılırken kamu tüzel kişiliğinde çalışıyor olma kriteri esas alınmaktadır⁹⁶. Dolayısıyla geniş anlamda kamu görevlisi kavramından devlet ve diğer kamu tüzel kişilerinde görevi bulunan ve hukuki statüleri birbirinden farklı olan tüm kamu personeli anlaşılır⁹⁷.

Türkiye Cumhuriyeti Anayasası m. 128’de; “Devletin, kamu iktisadi teşebbüsleri ve diğer kamu tüzelkişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği asli ve sürekli görevler,

⁹¹ Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 598.

⁹² Koca/Üzülmez, Özel Hükümleri, s. 548.

⁹³ Tezcan/Erdem/Önok, s. 663.

⁹⁴ Özen, Muharrem/Tozman, Önder: “Türk Ceza Kanunu’nda Kamu Görevlisi Kavramı”, Amme İdaresi Dergisi, C. 42, S. 4, Aralık 2009, (s. 25-57), s. 31.

⁹⁵ Özey, İlhan: Günışığında Yönetim, İstanbul, 2004, s. 983.

⁹⁶ Çağlayan, Ramazan: İdare Hukuku Dersleri, 5. Baskı, Ankara 2017, s. 498.

⁹⁷ Kalabalık, Halil: İdare Hukuku Dersleri Cilt: 1, 7. Baskı, Konya 2016, s. 317.

*memurlar ve diğer kamu görevlileri eliyle görülür” hükmü bulunmaktadır. Buna göre kamu görevlisi; kamu kurum ve kuruluşlarının genel idare esaslarına bağlı olarak yürütme yükümlülüğü altında olduğu kamu hizmetlerinin gerektirdiği sürekli işleri yürütmekle görevli olan kimselerdir*⁹⁸.

657 Sayılı Devlet Memurları Kanunu’nun 4. maddesinde⁹⁹ ve 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun’un 2. maddesinde¹⁰⁰ kamu görevlilerine ilişkin tanımlar bulunmaktadır¹⁰¹.

Kamu kurum ve kuruluşuyla kamu görevlisi kavramlarına ilişkin bu açıklamalardan sonra, kamu kurum ve kuruluşlarında bulunan bilgisayarların statüsünün belirlenmesi gerekmektedir. Kamu kurum ve kuruluşlarında bulunan bilgisayarlar bilişim sistemine girme suçu açısından, şahsi bilgisayarlardan farklı değerlendirilmelidir. Zira, kamu kurumlarında bulunan bilgisayarlar kamu görevlilerinin kişisel bilgisayarı değildir. Bu bilgisayarlar kamu görevlileri tarafından, tahsis amaçları dışında, şahsi işlerin görülmesinde kullanılamaz. Söz konusu bilgisayarlar, kamu hizmetinin yürütülmesi amacıyla, çalıştıkları kurum tarafından kamu görevlilerine tahsis edilir. İdare kamu görevlisine tahsis ettiği bilgisayarı, yetkili amirin emriyle her zaman geri alabilir. İdare bilgisayarı geri aldığı anda, bilgisayar içinde kişiye özel bir veri bulunamaz. Aksi halde 657 sayılı Devlet Memurları Kanunu gereğince, kurum araçları özel işlerde kullanıldığı için, kamu görevlisinin disiplin sorumluluğu doğar¹⁰².

Buradan hareketle şahsi bilgisayarlarla kamu kurum ve kuruluşlarında bulunan bilgisayarın iki açıdan birbirinden ayrıştığı söylenebilir. Bunlardan ilki kamu kurum ve kuruluşunda bulunan bilgisayarın tahsis amacıdır. Şahsi bilgisayarlar tamamen bireyin kendi şahsi kullanımına hizmet ederken, kamu kurum

⁹⁸ **Tan**, Turgut: İdare Hukuku, 3. Bası, Ankara 2014, s. 489.

⁹⁹ 657 sayılı Kanun madde 4’e göre; “Memur; Mevcut kuruluş biçimine bakılmaksızın, Devlet ve diğer kamu tüzel kişiliklerince genel idare esaslarına göre yürütülen asli ve sürekli kamu hizmetlerini ifa ile görevlendirilenlerdir,

Sözleşmeli personel; Kalkınma planı, yıllık program ve iş programlarında yer alan önemli projelerin hazırlanması, gerçekleştirilmesi, işletilmesi ve işlerliği için şart olan, zaruri ve istisnai hallere münhasır olmak üzere özel bir meslek bilgisine ve ihtisasına ihtiyaç gösteren geçici işlerde, Bakanlar Kurulunca belirlenen esas ve usuller çerçevesinde kurumun teklifi ve Devlet Personel Başkanlığının görüşü üzerine Maliye Bakanlığınca vizelenen pozisyonlarda, mali yılla sınırlı olarak sözleşmeyle çalıştırılmasına karar verilen ve işçi sayılmayan kamu hizmeti görevlileridir.”

¹⁰⁰ 4483 sayılı Kanun madde 2’ye göre kamu görevlileri; “Devletin ve diğer kamu tüzel kişilerinin genel idare esaslarına göre yürüttükleri kamu hizmetlerinin gerektirdiği asli ve sürekli görevleri ifa eden” kimselerdir.

¹⁰¹ Hakim, savcı, askeri personel, il özel idareleri ve belediyelerde istihdam edilen personel 657 Sayılı Kanunda tanımlanmamıştır. Üniversite öğretim üyeleri ve yardımcıları da yalnızca mali yönlerden 657 Sayılı Kanuna tabidir. **Demren Dönmez**, Burcu: “Türk Ceza Kanunu’nda ‘Kamu Görevlisi’ Kavramı”, TBB Dergisi, S. 94, 2011, s. 102 (s. 95-130).

¹⁰² **Erdoğan**, s. 1410.

ve kuruluşlarında bulunan bilgisayarlar kamu hizmetinin görülmesi, yürütülmesi, hizmetin sunulması amacıyla kamu görevlilerine tahsis edilir.

İkinci olarak, bireysel bilgisayarların kullanımı, tamamen bilgisayar sahibinin tasarrufundadır. Buna karşın kamu kurum ve kuruluşlarında bulunan bilgisayarın mülkiyeti devlete aittir ve kamu görevlisi bu bilgisayarlar üzerinde serbestçe tasarruf edemez, örneğin bilgisayarı evine götüremez veya satamaz. Kamu kurum ve kuruluşlarında bulunan bilgisayarların kullanımı kurum amirlerinin denetimindedir; tahsis ve kullanım amaçları dışına çıkılması kamu görevlisinin cezai sorumluluğunu gerektirir. Bu nedenle şahsi bilgisayarlar açısından, bilgisayar sahibi dışında birinin bilgisayarı açma yetkisi olmadığı için, böyle bir bilgisayarın düğmesine basılıp açılarak sisteme girilmesi, bilişim sistemine girme suçunun oluşması için yeterli iken, kamu kurumlarında kamu hizmetinin görülmesi amacıyla personele tahsis edilmiş bilgisayarlar açısından aynı değerlendirme yapılamaz. Zira yukarıda da bahsedildiği üzere; bilişim sistemine girme suçunun oluşması için, suç tipiyle korunan özel hayat ve haberleşme sisteminin güvenilirliği gibi hukuki değerlerin ihlal edilmesi gerekmektedir.

Kamu kurum ve kuruluşlarında olduğu gibi özel sektör işyerlerinde de çalışanlara bilgisayar tahsis edilmektedir. Bu bilgisayarların tahsis amacı da o işyerinin işlerinin yürütülmesidir. Bu nedenle personelin şahsi işleri için kullanamaz. Kamu kurumlarında olduğu gibi özel sektör işyerlerinde de çalışanlar, işlerin yürütülmesi için başka bir çalışana tahsis edilen bir bilgisayarı kullanabilmektedirler. Tıpkı resmi kurumlardaki bilgisayarlar gibi, özel sektör işyerlerinde çalışanlara tahsis edilmiş olan bilgisayarlar da şahsi bilgisayarlardan farklıdır.

Çalışanlar, kullanımlarına tahsis edilmiş olan bilgisayarlara yetkisiz kişilerin erişimini engellemek amacıyla şifre koyabilirler. Böyle bir güvenlik tedbirinin konulması, yürütülen faaliyetle ilgili bilgi ve belgelerin korunması açısından önemli, kimi zaman da zorunludur. Bununla birlikte kamu kurumlarında ve özel sektör işyerlerinde kaynak yetersizliği nedeniyle her personele bir bilgisayar verilememesi ve sınırlı sayıdaki bilgisayarın birden fazla çalışan tarafından ortak kullanılması da istisnai bir durum değildir. Pek çok işyerinde, bir bilgisayar çalışanlardan birinin zimmetine bırakılmakta, ancak diğer çalışanlar da bu bilgisayardan yararlanmaktadırlar.

Kamu kurumlarında ve özel işyerlerinde bulunan bilgisayarlarda genellikle bilgisayarın zimmetlendiği personele ait şifreli bir hesabın yanında, orada çalışan herkesin gerektiğinde giriş yapabileceği bir genel kullanıcı hesabı oluşturulmaktadır. Böylece, gerektiğinde şifresiz hesap kullanılarak, yürütülen faaliyet aksamadan diğer çalışanlar da işlemlere devam edebilmektedirler. Gerçekten de işyerinde bulunan bilgisayarlardan birinde bir arıza meydana geldiğinde veya başka bir nedenle kullanılmadığında, diğer bilgisayarlar kullanılarak faaliyetin yürütülmesine devam edilmelidir. Bu nedenle bu bilgisayarlara ve bu bilgisayarların şifrelenmemiş kısımlarına aynı yerde çalışan ve aynı faaliyeti yürütmekle

görevli diğer çalışanların da işlerin yürütülmesi amacıyla sınırlı olarak, erişim yetkilerinin olduğu kabul edilmelidir. Bu bilgisayarların erişimin sınırlandırılmadığı bölgelerine giriş yapmaya, aynı işi yapmakla görevli diğer çalışanların da yetkili olduğu kanaatindeyiz. Örneğin, bir mahkeme kaleminde bulunan ve katiplerden biri adına zimmetlenmiş olan kurum bilgisayarına, talep edilen bir evrakın çıktısını almak amacıyla bir diğer katip giriş yapmaya yetkili olmalıdır. Ancak, aynı yetkinin görev tanımı farklı olan mübaşirde bulunmadığı kanaatindeyiz.

Buradan hareketle bir çalışanın, bir başkasının üzerine zimmetli olan bilgisayara, işlerin yürütülmesi amacıyla, o bilgisayarın tahsis edildiği çalışanın şifreli hesabına müdahale etmeden, genel kullanıcı hesabı üzerinden girmesi sisteme yetkisiz erişim değildir. Bu amaç ve yolla erişim, bilişim sisteminin ve sistem içindeki verilerin gizlilik, bütünlük, kullanılabilirlik gibi hususları kapsayan güvenliğine yönelik bir tehdit veya saldırı niteliğinde değildir. Öte yandan böyle bir eylem; aynı bilgisayar üzerinde bulunan şifreli hesap kullanıcılarının özel hayatın gizliliği ve bilişim sistemlerinin güvenliği gibi TCK m. 243 ile koruma altına alınan hukuki değerleri de ihlal etmez.

Bununla birlikte; aynı işyerinde çalışıyor ve aynı işi yapıyor olmak, kişiye başkasına tahsis edilen bilgisayarın, şifre veya başka tedbirlerle erişimi sınırlandırılmış alanlarına girme yetkisi vermez. Bu nedenle sistemin şifre gibi özel koruma duvarlarıyla korunan alanına, sisteme erişim yetkisi olan kişinin rızası ve izni dışında erişim, yetkisiz erişimdir.

Ayrıca, çalışanların işyerinde bulunan diğer bilgisayarlara erişim yetkisi, işlerin yürütülmesi amacıyla sınırlı bir yetkidir. Bu amacın dışındaki erişimler de bilişim sistemine girme suçunu oluşturur. Örneğin, bir çalışanın mesai arkadaşının bilgisayarını açıp, onun sisteme kayıtlı şifresini kullanarak sosyal medya hesaplarına girmesi, sisteme erişim yetkisi olmadığından bilişim sistemine girme suçunun oluşmasına neden olur.

Kamu görevlilerine görevleri gereği tahsis edilen bilgisayarların kamu görevlisinin rızası olmaksızın kurumun yetkili amiri ya da teftişle görevli kişi tarafından incelenmesinin hukuka uygun olup olmadığının da değerlendirilmesi gerekmektedir. Değerlendirme yapılırken öncelikle bu bilgisayarların veriliş amacı tespit edilmelidir. Yukarıda da açıklandığı üzere; bu bilgisayarlar kamu görevlilerine yalnızca kamusal faaliyetin yürütülmesi için verilmektedir. Bu bilgisayarlar yetkili merciin emriyle her zaman geri alınabilir. Bu nedenle de bu bilgisayarların kamu görevlisinin rızası aranmaksızın yetkili amir veya amirin emriyle bir başkası tarafından incelenmesi hukuka aykırı olmayacağından, eylem bilişim sistemine girme suçunu oluşmaz¹⁰³.

¹⁰³ Erdoğan, s. 1410; Apaydın, s. 284-285.

Bu konuda Anayasa Mahkemesi'nin vermiş olduğu 24.03.2016 tarihli B. No 2013/4825 kararıyla AİHM'in konuya ilişkin vermiş olduğu 22.02.2018 tarihli Libert/Fransa (B. No 588/13) kararına değinmek gerekmektedir.

AYM'nin 24.03.2016 tarihli B. No 2013/4825 kararına konu olayda; özel bir şirkette çalışmakta olan başvurucunun kullandığı ve mahremiyetine ilişkin yazışmaların da yer aldığı kurumsal e-posta hesaplarının işveren tarafından incelenmesi ve bu yazışmaların görülmekte olan işe iade davasında dosyaya sunulması nedeniyle özel hayatının ve haberleşmenin gizliliğinin ihlal edildiği iddiasıyla bireysel başvuru yoluna gidilmiştir. AYM bu dosyada özetle; işverenlerin, çalışanlarının özel hayatlarına sınırsız bir müdahale haklarının bulunmadığını, ancak anayasal hak ve özgürlüklerin sağladığı güvencelere, kanunlara ve uluslararası sözleşmelere aykırı olmamak koşuluyla işletmenin ticari gerekliliğine ve iç disiplin anlayışına göre belirlenen kuralların açık bir şekilde yer aldığı düzenlemelerin yapılması ve bu düzenlemeler konusunda çalışanların bilgilendirilmesi koşuluyla, çalışanların özellikle de çalışma saatleri içerisinde birtakım haklarının kısıtlanmasının mümkün olduğu tespitini yapmıştır. Ayrıca kurumsal e-posta adreslerinin iş sözleşmesi ve eki niteliğindeki düzenlemelere uygun olarak kullanılıp kullanılmadığının işveren tarafından incelenmesi makul kabul edilmiştir. Anılan nedenlerle AYM, başvurucunun haklarının ihlal edilmediği sonucuna varmıştır¹⁰⁴.

AİHM'in konuya ilişkin vermiş olduğu 22.02.2018 tarihli Libert/Fransa (B. No 588/13) kararına konu olan olayda ise; Fransız demiryolu şirketinde çalışmakta olan başvuru, hakkında yapılan bir soruşturma nedeniyle bir süre işinden uzaklaştırılmış ve işe tekrar döndüğünde işyerinde kullanmakta olduğu bilgisayarına el konulduğunu görmüştür. Bu hususla ilgili olarak kendisine; bilgisayar incelendiğinde içerisinde oynanmış adres değişikliği formu gibi resmi formların ve pornografik içeriklerin tespit edildiği bildirilmiştir. Bunun üzerine başvuru özel hayatının gizliliğinin ihlal edildiği iddiasıyla hukuki yollara başvurmuş ve uyuşmazlık en nihayetinde AİHM önüne gelmiştir. AİHM bu dosyada Fransız hukukunun bu konudaki kriterlerine uygun olarak başvurucunun özel hayatının ihlal edilmediğine karar vermiştir. AİHM'e göre; eğer iş yönergesinde açıkça belirtilmemiş ise çalışanların "özel" olarak isimlendirmedikleri dosyalarının incelenmesi orantılı bir tedbir olarak değerlendirilmiştir. Ancak AİHM; işverenin, bilgisayarların incelenmesi ve haberleşmelerinin izlenmesi tedbirlerine orantılı bir şekilde başvurmaları gerektiğine dikkat çekmiştir¹⁰⁵.

Hem AYM hem de AİHM yukarıda kısaca değindiğimiz kararlarıyla iş ilişkisi kapsamında mahremiyet hakkı ve kişisel verilerin korunması konularında önemli değerlendirmelerde bulunmuşlardır. Buna göre; işveren iş ilişkisi nedeniyle çalışanına vermiş olduğu bilgisayarı ve kurumsal e-posta adresini inceleme

¹⁰⁴ AYM, 24.03.2016 tarih, B. No 2013/4825 kararı.

¹⁰⁵ AİHM 22.02.2018 tarihli Libert/Fransa (B. No 588/13) kararı.

yetkisini haizdir. Ancak bu yetki kullanılırken çalışanların kanundan, Anayasa-dan veya uluslararası sözleşmelerden kaynaklanan haklarının ortadan kaldırıl-maması, bu husustaki düzenlemelerin açık bir şekilde yapılması ve çalışanın bu düzenlemeler hakkında bilgilendirilmiş olması gerekmektedir. Bu kararlardan hareketle, çalışanlara önceden, örneğin sözleşmeyle açıkça bildirilmiş olması veya konuya ilişkin kurum içi bir düzenlemenin bulunması halinde hem çalışan-ların hem de yöneticilerin bilgisayarları denetlenebilir. Bu durumda bilişim sistemine girme suçu oluşmaz. Kurum uzantılı e-posta hesaplarına girilmesi de bu kapsamda değerlendirilmelidir.

İşverenlerin, çalışanlarına tahsis ettikleri bilgisayarları ve işyeri uzantılı e-mailleri kötü amaçlı kullanımları önlemek için denetleyebilecekleri, Yargıtay 9. Hukuk dairesinin verdiği kararlarda da vurgulanmıştır. Örneğin mahkeme, 13.10.2010 tarihinde verdiği 2010/447 esas ve 2010/37516 karar sayılı içtihadta, “işverenin kendisine ait bilgisayar ve e-mail adresleri ile bu adreslere gelen e-postaları her zaman denetleme yetkisi”nin bulunduğuna işaret etmiştir.

Bununla birlikte amirlerin memurlarının veya işverenlerin çalışanlarının kurum uzantılı olmayan kişisel e-maillerine veya sosyal medya hesaplarına gir-meleri, bilişim sistemine haksız erişim niteliğinde olacağından suç teşkil eder.

IV. SUÇUN MANEVİ UNSURU

Bilişim sistemine girme suçu, kasten işlenebilen bir suçtur¹⁰⁶. TCK m. 21/1’e göre; “Kast, suçun kanuni tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesidir”. Bu düzenleme gereğince; kastın varlığından söz edebil-mek için, failin bilişim sistemine girme suçunun kanuni tanımında yer alan unsurları bilerek ve isteyerek gerçekleştirmesi gerekir. Bu durumda TCK m. 243/1’de düzenlenmiş olan “bilişim sistemine girme” suçunun oluşabilmesi için fail, girdiği yerin bir bilişim sistemi olduğunu bilmenin yanında, bu sisteme girme yetkisinin veya izninin olmadığını da bilmelidir¹⁰⁷. Yani eylemin hukuka aykırı olduğu¹⁰⁸ ve haksızlık teşkil ettiği bilinciyle hareket etmelidir. Öğretide

¹⁰⁶ Dülger, s. 359; Karagülmez, s. 186; Artuk/Gökçen/Yenidünya, Özel Hükümler, s. 875; Akbulut, s. 139; Mahmutoglu, s. 862.

¹⁰⁷ Dülger, s. 362.

¹⁰⁸ “... 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 veya kişilerle paylaştığı ve/veya çoğalttığına dair hakkında bir iddia ileri sürülmeyen sanıkların, devam eden soruşturmada iddialarını ispat-lama amacı taşıyan eylemlerinde gerektiğinde soruşturmayı yürüten makam tarafından da söz konusu kayıtların getirilebileceği göz önüne alındığında hukuka aykırı hareket etme bilinciyle davrandıkları kabul edilemeyeceğinden, atılı suçların oluşmadığından bahisle beraat kararı verildiğine yönelik yerel mahkemenin kabulünde bir isabetsizlik görülme-miştir...” Y. 12. CD., E. 2015/16132, K. 2017/3999, T. 16.5.2017, www.kazancı.com.tr, Tarih: 22.05.2018.

bu suçun olası kastla işlenebileceği görüşü de savunulmaktadır¹⁰⁹. Bizim de katıldığımız diğer bir görüşe göre ise; fail eylemin hukuka aykırı olduğu bilinciyle hareket etmek zorunda olduğundan, bu suç olası kastla işlenemez¹¹⁰, yalnızca doğrudan kastla işlenebilir¹¹¹.

Bilişim sistemine girme suçunun taksirli şekli Türk Ceza Kanunu'nda cezai yaptırıma bağlanmamıştır. Dolayısıyla taksirle bir bilişim sistemine girmek suç değildir¹¹². Ancak dikkatsizlik veya tedbirsizlik nedeniyle yanlışlıkla bir bilişim sistemine girdikten sonra, durumu fark etmesine rağmen sistemde kalmaya devam etmek suçtur¹¹³.

Fail suçu işlerken belirli bir veriyi ele geçirme amacıyla hareket etmek zorunda değildir¹¹⁴. Failin başkalarına zarar vermek ya da kendisine yarar sağlamak gibi bir amacı olsa bile, söz konusu saikler bilişim sistemine girme suçunun oluşması bakımından önemsizdir¹¹⁵. Failin sisteme hukuka aykırı olarak girmesi veya sistemde kalmasıyla suç oluşur¹¹⁶.

V. SUÇUN HUKUKA AYKIRILIK UNSURU

Bilişim sistemine girme suçu bir bilişim sisteminin tümüne veya bir kısmına hukuka aykırı olarak kasten girilmesi veya hukuka uygun yollardan girilmiş olsa bile sistemden çıkmayıp hukuka aykırı olarak kalmaya devam edilmesi suretiyle işlenebilir. TCK m. 243'te suçun kanuni tanımında; sisteme "hukuka aykırı olarak" girilmesi gerektiği açıkça belirtildiği için, failde ayrıca eylemin haksızlık teşkil ettiği bilinci mevcut olmalıdır. Suç tipinde hukuka aykırılığın bu şekilde özel olarak belirtilmesine "hukuka özel aykırılık" denir¹¹⁷. Hukuka özel aykırılığın arandığı durumlarda, failin genel olarak suç işleme kastı dışında, ayrıca özel olarak eylemin hukuka aykırı olduğu bilinciyle hareket edip etmediği de araştırılır¹¹⁸. Bilişim sistemine girme suçunun oluşup oluşmadığı konusunda değerlendirme yapılırken failde hukuka aykırılık bilincinin bulunup bulunmadığı her somut olayda ayrıca araştırılmalıdır¹¹⁹. Bilişim sistemine erişim yetkisi veya izni olmadığını, sisteme girmenin hukuka aykırı olduğunu bilen ve bu bilinçle

¹⁰⁹ Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 941; Tezcan/Erdem/Önok, s. 982, Yaşar/Gökcan/Artuç, C. V, s. 7295; Yenidünya, s. 1037; Mahmutoglu, s. 862.

¹¹⁰ Artuk/Gökcan/Yenidünya, Özel Hükümler, s. 876.

¹¹¹ Koca/Üzülmez, Özel Hükümler, s. 815; Parlar/Hatipoğlu, s. 3744.

¹¹² Dülger, s. 359; Karagülmez, s. 186; Parlar, s. 20; Akbulut, s. 139; Kurt, s. 159.

¹¹³ Akbulut, s. 139; Gül, s. 64.

¹¹⁴ Gül, s. 56; Karagülmez, s. 186.

¹¹⁵ Dülger, s. 332; Apaydın, s. 259; Karagülmez, s. 186.

¹¹⁶ Karakehya, s. 202.

¹¹⁷ Centel, Nur/Zafer, Hamide/Çakmut, Özlem: Türk Ceza Hukukuna Giriş, 10. Bası, İstanbul 2017, s. 301; Yenidünya, s. 1038.

¹¹⁸ Yaşar/Gökcan/Artuç, C. V, s. 7295.

¹¹⁹ Artuk/Gökcan/Yenidünya, Özel Hükümler, s. 876.

hareket eden kişide hukuka aykırılık bilinci vardır. Aynı şekilde bilişim sisteme hukuka aykırı olarak girdiğini fark etmesine rağmen, sistemden çıkmayıp kalmaya devam eden kişinin de aynı bilinçle hareket ettiğinde herhangi bir tereddüt yoktur¹²⁰.

Ancak Yargıtay, kararlarında hukuka aykırılık bilincinin varlığı konusunda farklı kıstasları göz önünde bulundurabilmektedir. Özellikle boşanma davalarında delil elde edilmesi amacıyla eşlerin birbirlerinin bilişim sistemlerine yetkisiz erişimlerinde hukuka aykırılık bilincinin bulunmadığı yönünde kararlar verilmektedir¹²¹. Yargıtay'ın bu yönde verdiği kararlar pek çok açıdan sakıncalıdır. Öncelikle; bu tip kararlarda faile karşı gerçekleşmekte olan şantaj, tehdit, hakaret gibi bir suç söz konusu olmadığından başka türlü delil elde etme imkanının bulunmamasından bahsedilemez. İkinci olarak; Yargıtay her ne kadar delil elde etme amacını meşru kabul ederek failde hukuka aykırılık bilincinin bulunmadığı kanaatinde ise de hukuka aykırılık bilinci faillerin amaçlarının meşru olup olmadığına göre belirlenemez. Kaldı ki; davanın tarafları ispat hakkına sahip iseler de bu hak suç işleyerek delil elde edilmesine cevaz vermez. Bu nedenle de bir hukuka uygunluk nedeni teşkil etmez. Aralarında herhangi bir husumet bulunmayan evli çiftlerin birbirlerinin telefon ya da bilgisayarlarına izinsiz erişim-

¹²⁰ **Yenidünya**, s. 1034.

¹²¹ “Dosya kapsamına göre; resmi nikahlı eşi olan mağdurun sadakatinden kuşkulanan ve aldatıldığını düşünen sanığın, henüz boşanma davası açılmadığı ve mağdurla fiilen birlikte yaşadıkları dönemde, mağdurun rızası dışında cep telefonunu alıp, şifresini kırarak elde ettiği mağdura ait MSN, GSM görüşmelerini ve elektronik iletileri, daha sonra açtığı boşanma davasına delil olarak sunmak suretiyle haberleşmenin gizliliğini ihlal, özel hayatın gizliliğini ihlal ve bilişim sistemine girme suçlarını işlediğinin iddia edildiği olayda,

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 dair 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 dair hakkında bir iddia ileri sürülmeyen 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.

Yapılan yargılama sonunda, yüklenen suçlar açısından sanığın kastının bulunmadığı gerekçeleri gösterilerek mahkemece kabul ve takdir kılınmış olduğundan, katılan vekilinin eksik incelemeye dayalı olarak karar verildiğine dair temyiz itirazlarının reddiyle, beraata dair hükümlerin isteme uygun olarak ONANMASINA 15.06.2015 tarihinde oybirliğiyle karar verildi.” Y. 12. CD. E. 2015/439, K. 2015/10716, T. 15.06.2015, www. kazanci.com.tr, Erişim Tarihi: 25.05.2018.

lerinin suç olmadığı konusunda kaçınılmaz hataya düşmeleri halinde TCK m. 30/4'te düzenlenen haksızlık yanılığının varlığı gündeme gelebilirse de bu eylemlerin boşanma davasında delil elde etmek amacıyla gerçekleşmesi halinde suç oluşur. Çünkü bu durumda mağdurun bilişim sistemine girilmesine rıza göstermeyeceği ve bu nedenle failin hukuka aykırılık bilinciyle hareket edeceği açıktır. Yargıtay'ın kararlarında failin hukuka aykırılık bilincinin bulunmaması nedeniyle kastın yokluğu nedeniyle suçun oluşmadığı yönünde verdiği kararlar isabetsizdir.

Bir bilişim sistemine girilmesi veya orada kalınmasına cevaz veren yasal bir düzenleme bulunması durumunda eylem hukuka uygun hale gelecektir. Bu doğrultuda CMK m. 134'te düzenlenen bilgisayarlarda, bilgisayar kütük ve programlarında yapılan arama¹²² ve CMK m. 135'te düzenlenen iletişimin tespiti amacıyla bilişim sistemine erişilmesi veya sistemde kalınması kanun hükmünün yerine getirilmesi hukuka uygunluk nedeni kapsamında değerlendirilir¹²³. Ayrıca bu suçun kamu kurumları, internet kafeler, üniversiteler, restoranlar ve oteller gibi toplu kullanım alanlarında bulunan bilgisayarlarla işlenmesi delillerin toplanması açısından sıkıntılara yol açabileceğinden yeterli suç şüphesinin varlığı durumunda şüpheli tarafından kullanılan bilişim sistemi üzerinde CMK m. 134 kapsamında araştırma yapılması gerekmektedir¹²⁴.

Bilişim sistemine girme suçu bakımından ortaya çıkabilecek hukuka uygunluk nedenlerinden biri de meşru savunmadır. Örneğin; başkasına ait bir sosyal medya hesabında kendisinin cinsel içerikli fotoğraflarının rızası dışında paylaşıldığını gören kişinin, fotoğrafları paylaşan kişiden bunları kaldırmasını istemesine rağmen, fotoğraflar kaldırılmazsa; şahsına karşı gerçekleşen ve devam etmekte olan bu haksız saldırının defedilmesi zorunluluğu içerisinde bu hesabın şifresini kırıp fotoğrafları silmesi durumunda, meşru savunma hükümlerinin uygulanması gündeme gelebilir. Ancak meşru savunma hükümlerinin uygulanabilmesi için kişinin yalnızca saldırıyı defetme amacıyla hareket etmesi, söz konusu fotoğrafları sildikten sonra sistemdeki verilere zarar vermeden derhal sistemden çıkması gerekir. Fotoğrafların silinmesiyle birlikte haksız saldırı defedilmiş olacağından sistemde kalmaya devam edilmesi halinde, meşru savunmanın sınırı kasten aşılmış olacaktır. Bu durumda her ne kadar sisteme girme hareketi hukuka uygun olsa da hukuka aykırı bir şekilde sistemde kalmaya devam edildiğinden suç oluşacaktır. Böyle bir olayda, saldırıya uğrayan kişinin yargısal yollara başvurma zorunluluğu düşünülebilirse de saldırının niteliği, bilişim sistemleri aracılığıyla yapılan paylaşımların yayılma hızı ve yargısal sürecin uzunluğu göz önünde bulundurulduğunda kişinin yargı yoluna başvurmaması

¹²² Özбек/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 940; Tezcan/Erdem/Önok, s. 983; Akbulut, s. 137; Mahmutoğlu, s. 862.

¹²³ Tezcan/Erdem/Önok, s. 983.

¹²⁴ Gül, s. 62.

nedeniyle hukuka aykırı hareket ettiği düşünülemez. Kaldı ki; zorunluluk halinin (TCK m. 25/2) uygulanmasında aranan “başka suretle korunma olanağı bulunmaması” şartı meşru savunma bakımından aranmamıştır.

Bu suç açısından dikkate alınması gereken bir diğer hukuka uygunluk nedeni de rızadır. Hukuka uygunluk nedeni olan rızanın, hukuki sonuç doğurabilmesi için; öncelikle üzerinde serbestçe tasarruf edilebilecek bir hakkın bulunması, rıza açıklayan kişinin rıza açıklamaya yetkili olması, rıza açıklayan kişinin rıza ehliyetine sahip olması ve rıza açıklamasının cebir, tehdit, hile gibi irade sakatlıklarıyla sakatlanmamış olması gerekir¹²⁵. Rızanın maddi şartlarından ilki, üzerinde serbestçe tasarruf edilebilecek bir hakkın varlığıdır. Kişinin üzerinde mutlak surette tasarruf yetkisine sahip olmadığı haklar bakımından yaptığı rıza açıklaması, eylemi hukuka uygun hale getirmez¹²⁶. Rıza, ayrıca özgür iradeye dayanmalı ve irade sakatlıklarıyla sakatlanmamış olmalıdır¹²⁷.

TCK m. 243 ile bilişim sisteminin güvenliğinin yanında, kişilerin haberleşme özgürlükleri, özel yaşamlarının gizliliği¹²⁸, kişilerin bilişim sisteminin başkalarının müdahalesinden uzak şekilde işlediğine yönelik güvenleri de korunur¹²⁹. Bu hukuksal değerler kişilerin üzerinde serbestçe tasarruf edebileceği haklardandır. Dolayısıyla TCK m. 243 açısından rıza, bilişim sistemine girme veya orada kalma filleri hukuka uygun hale getiren bir nedendir. Bu durumda bilişim sistemine girme veya sistemde kalma, sisteme girme konusunda yetkili olan hak sahibinin rızası (TCK m. 26/2) ile gerçekleşirse, fiil hukuka uygundur ve suç teşkil etmez¹³⁰. Hak sahibinin rızası olmadan sisteme girilmesi veya kalınması ise hukuka aykırıdır ve eylemi hukuka uygun hale getiren başka bir neden de mevcut değilse suç oluşur¹³¹.

¹²⁵ **Özbek**, Veli **Özer/Doğan**, Koray/**Bacaksız**, Pınar/**Tepe**, İlker: Türk Ceza Hukuku Genel Hükümler, 7. Baskı, Ankara 2016, s. 349 vd.

¹²⁶ **Artuk**, M. Emin/**Gökçen**, Ahmet/**Yenidünya**, A. Caner: Ceza Hukuku Genel Hükümler, 10. Baskı, Ankara 2016, s. 456.

¹²⁷ **Ekici Şahin**, Meral: Ceza Hukukunda Rıza, İstanbul 2012, s. 185.

¹²⁸ **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 932-933.

¹²⁹ **Koca/Üzülmez**, Özel Hükümler, s. 808.

¹³⁰ **Erdoğan**, s. 1408; **Koca/Üzülmez**, Özel Hükümler, s. 815; **Akbulut**, s. 137.

¹³¹ “...Katılanın rızası olmadan e-mail hesabına 17.05.2007 tarihinde girip şifrelerini değiştirmek suretiyle bilişim sistemine girmesini engellediğinden bahisle açılan davada; sanığın suçlu kabul etmemesine karşın, katılanın hesabına sanığın 15.05.2007 tarihinde saat 18.57 de giriş yaptığı, saat 20.42 de bağlantıdan çıkış yaptığının ve katılana ait IP numarasıyla aynı gün saat 20.46 da giriş yapıldığı, 16.05.2007 tarihinde saat 17.18 de bağlantıdan çıktığı ve müdürlüğünü yaptığı okulun internet hattından da 17.05.2007 tarihinde giriş yapıldığının tespit edildiğinin anlaşılması ve tüm dosya kapsamı karşısında, sanığa ait internet hattıyla katılanın e-mail hesabına izinsiz girildiği sabitse de şifresini değiştirmek sureti ile erişimi engellediğine dair tespit bulunmaması karşısında eyleminin TCK.nun 243. maddesi kapsamında değerlendirilmesi gerekirken suç vasfında yanılı sonucu yazılı şekilde hüküm kurulması...” Y. 8. CD., E. 2016/10095, K. 2017/13454, T. 29.11.2017, www.kazancı.com, Erişim Tarihi: 25.05.2018.

Bilişim sistemine girme veya orada kalmaya ilişkin olarak verilen rıza, bu sisteme girme yetkisine sahip olan gerçek veya tüzel kişi tarafından verilmeli, bu kişinin iradesi sakatlanmamış olmalı ve rıza açık veya örtülü bir şekilde açıklanmış olmalıdır¹³². Rıza açıklaması yazılı veya sözlü olarak açıkça yapılabileceği gibi, işaret, hareket veya davranışlarla zımni olarak da yapılabilir. Eğer somut koşullardan ve kişinin davranışlarından rıza gösterdiği anlaşılabiliyorsa rızanın zımnen açıklandığı kabul edilir. Kişinin rızasının varlığını ortaya koyan başka belirtiler varsa fiile karşı koymamak ya da sessiz kalmak da rıza beyanı olarak nitelendirilebilir¹³³. Sessiz kalmanın rıza açıklaması olarak değerlendirilebilmesi için, somut olaya bakmak gerekir. Burada, toplumsal ilişkiler, faille mağdur arasındaki ailevi veya kişisel ilişkiler göz önünde bulundurulur¹³⁴. Aralarında hiçbir ilişki bulunmayan iki kişiden birinin diğerine ait bilişim sistemine girmesine rızasının olmayacağı kabul edilmelidir. Ancak kişi, bilişim sistemine giriş şifresini vererek¹³⁵, şifresiz olarak veya şifre girildikten sonra bilişim sistemini bir kimsenin kullanımına sunarak bu husustaki rızasını ortaya koyabilir. İnternet üzerinden, kişinin sosyal medya hesaplarında veya başka mecralarda yer alan herkesin erişimine açık, şifrelenmemiş veya sınırlanmamış bilgilerine ulaşılması da örtülü rıza kapsamında hukuka uygundur¹³⁶.

Rıza, yalnızca kendisine rıza gösterilen kişinin eylemlerini hukuka uygun hale getirir. Sisteme girişine izin verilen kişinin, üçüncü bir kişinin eylemine rıza göstermesi yani zincirleme rıza bilişim sistemine girme suçunu hukuka uygun hale getirmeyecektir. Zira rıza gösterme yetkisi, sistem üzerinde hak sahibi olan gerçek veya tüzel kişiye aittir¹³⁷. Asıl hak sahibinin rızasıyla sisteme giriş yapan kişi, 3. bir kişinin sisteme girmesine rıza göstermeye yetkili değildir. Örneğin; bir banka çalışanına verilmiş olan şifrenin, bu kişi tarafından ilgisiz bir başka kişiye verilerek sisteme girişinin sağlanması durumunda; mağdurun rızası banka çalışanının sisteme girişine ilişkindir ve üçüncü kişinin eylemine rızası yoktur. Rıza bu şekilde ikincil eylemleri hukuka uygun hale getirmez¹³⁸. Banka çalışanının müşterinin kendisine verdiği şifreyi üçüncü şahıslara vermesi, müşterinin başlangıçta açıkladığı rızasının sınırları dışındadır.

İşverenin çalışanlarına tahsis ettiği bilgisayarları veya işletme hizmetlerinin görülmesi için verilen işyeri uzantılı e-postaları denetlemesi, önceden sözleşmeyle çalışana bildirilmiş ve çalışan da bu denetlemeyi kabul etmişse, yapılan denetimler çalışanın rızası kapsamında hukuka uygun olur¹³⁹.

¹³² Dülger, s. 368; Yaşar/Gökcan/Artuç, C. V, s. 7296.

¹³³ Ekici Şahin, s. 177.

¹³⁴ Demirbaş, s. 330.

¹³⁵ Erdoğan, s. 1409.

¹³⁶ Karakehya, s. 16 vd.

¹³⁷ Tezcan/Erdem/Önok, s. 984.

¹³⁸ Dülger, s. 369, 370.

¹³⁹ Tezcan/Erdem/Önok, s. 620-621.

Bir kamu görevlisinin kamuya ait araç, gereç ve benzeri eşyayı özel işleminde kullanması 657 sayılı Kanun'un 125/B- e maddesinde kınama cezası gerektiren eylemlerden biri olarak sayılmıştır. Aynı Kanun'un 10. maddesinde amirlerin kamu hizmetlerinin eksiksiz olarak yerine getirilmesini sağlamak ve maiyetlerindeki memurların hal ve hareketlerini takip ve kontrolden sorumlu oldukları belirtilmiştir. Kanun'un 11. maddesinde devlet memurlarının kanun ve diğer mevzuatla belirtilen esaslara uymakla ve amirler tarafından verilen görevleri yerine getirmekle yükümlü ve görevlerinin en iyi ve doğru yürütülmesinden amirlerine karşı sorumlu oldukları düzenlenmiştir. Ayrıca 657 sayılı Kanun'un 12 maddesinde devlet memurlarının, görevlerini dikkat ve itina ile yerine getirmek ve kendilerine teslim edilen devlet malını korumak ve her an hizmete hazır halde bulundurmamakla yükümlü oldukları da vurgulanmıştır. Bu düzenlemeler birlikte değerlendirildiğinde amirin bir kamu kurumunda bulunan bilgisayara girmesi veya denetimle görevli kişilerin girişine izin vermesi ve bilgisayarın denetlenmesi TCK m. 24/1 gereğince kanun hükmünün icrası kapsamında hukuka uygun kabul edilmelidir. Ancak bu durumda da hukuka uygunluk nedeninin sınırlarının aşılmaması gerekir. Memurun kamu hizmetinin yürütülmesiyle alakası olmayan, amirin denetim yetkisi bulunmayan şahsi hesaplarına veya sosyal medya hesaplarına girilmesi hukuka aykırıdır.

Failin hukuka uygunluk nedenlerinin varlığı konusunda hataya düşebilir. Hata, gerçeğin bilinmemesi veya yeteri derecede bilinmemesi nedeniyle, yanlış bir hüküm verilmesidir¹⁴⁰. Hatanın sonuçları Türk Ceza Kanunu m. 30'da düzenlenmiştir.

Somut olayda bir hukuka uygunluk nedeni bulunmuyor, ancak fail, böyle bir nedenin bulunduğu düşüncesiyle hareket ediyorsa, eyleminin haksızlık teşkil ettiğini bilmiyor demektir. Hukuka uygunluk nedenlerinin maddi şartlarının gerçekleştiğine ilişkin bilgi kasta dahildir¹⁴¹. Bu nedenle işlediği fiil bakımından bir hukuka uygunluk nedeninin maddi şartları esasen gerçekleşmediği halde, bu şartların gerçekleştiği zannıyla hareket eden kişinin, işlediği suç açısından kastının varlığından söz edilemez¹⁴². Nitekim TCK m. 30/1'e göre: "*Fiilin icrası sırasında suçun kanuni tanımındaki unsurları bilmeyen bir kimse, kasten hareket etmiş olmaz. Bu hata dolayısıyla taksirli sorumluluk hali saklıdır.*" Bu durumda TCK m. 243/1'de düzenlenmiş olan "*bilişim sistemine girme*" suçu açısından, rızanın maddi şartlarının var olduğunu zannederek sisteme giren kişi, suç tipinde açıkça aranan "*hukuka aykırı olarak bilişim sistemine girme kastıyla*" hareket etmiş olmaz. TCK m. 243'te düzenlenen suç tipinde açıkça "*bir bilişim siste-*

¹⁴⁰ Demirbaş, s. 420.

¹⁴¹ Koca, Mahmut/Üzülmez, İlhan: Türk Ceza Hukuku Genel Hükümler, 11. Baskı, Ankara 2018, s. 300; Özgenç, İzzet: Türk Ceza Hukuku Genel Hükümler, 11. Baskı, Ankara 2015, s. 455.

¹⁴² Koca/Üzülmez, Genel Hükümler, s. 300; Özgenç, s. 455.

mine hukuka aykırı olarak” girme şartı arandığı için failin kastı, olayda bir hukuka uygunluk nedeninin bulunmadığını da kapsamalıdır. Örneğin; rızanın maddi şartlarının gerçekleştiğine ilişkin olarak yapılan hata, TCK m. 30/1 gereğince failin “*bir bilişim sistemine hukuka aykırı olarak girme*” kastını ortadan kaldırır.

Bununla birlikte fail, hukuka uygunluk nedenlerinin maddi şartlarının gerçekleştiğine ilişkin hataya düşmekte kusurluysa, hatası kendi dikkatsiz ve özensiz davranışından kaynaklanmışsa, taksirle hareket etmiş olur. Ancak “*bilişim sistemine girme*” suçunun taksirli şekli Türk Ceza Kanunda düzenlenmemiştir. Dolayısıyla bir hukuka uygunluk nedeninin, örneğin rızanın maddi şartlarının gerçekleştiği konusunda taksiri bulunan ve rızanın var olduğunu zannederek bilişim sistemine giren fail cezalandırılmaz¹⁴³.

VI. SUÇA ETKİ EDEN NEDENLER

1. Suçun Bedeli Karşılığı Yararlanılan Sistemler Hakkında İşlenmesi (TCK m. 243/2)

TCK m. 243/2’de bilişim sistemine girme suçunun işlenmesi nedeniyle, fail hakkında hükmedilecek cezanın indirilmesini gerektiren bir nitelikli hal düzenlenmiştir. Buna göre; TCK m. 243/1’de temel şekli düzenlenen suçun “*bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi*” halinde, faile verilecek olan ceza yarı oranında indirilecektir.

Bedeli karşılığında yararlanılabilen sistemlerden ne anlaşılması gerektiği tartışmalıdır. Ancak genel olarak bu kavramdan, internet üzerinden ücret karşılığı hizmet veren veya hukuka uygun başka bir bedel karşılığında yararlanılabilecek web sayfalarının veya bilişim sistemlerin anlaşılması gerektiği kabul edilmektedir¹⁴⁴. Öğretide, internet kafe ve benzeri yerlerde verilen hizmetin de bu fıkra anlamında “bedeli karşılığında yararlanılabilen sistemler” olduğuna ilişkin bir görüş savunulmaktadır¹⁴⁵. Ancak bu görüş, TCK m. 243/2’de sistemin kullanıldığı mekanın değil, sistem içerisindeki elektronik yapıda sunulan hizmetlerin bedel karşılığı yararlanılmasının vurgulandığı gerekçeyle haklı olarak reddedilmektedir¹⁴⁶.

Bilişim sistemine girme suçunun bedeli karşılığı yararlanılabilen bir sistem hakkında işlenmesinin hafifletici neden olarak düzenlenmesi de eleştirilmekte ve bu düzenlemenin yerinde olmadığı görüşü savunulmaktadır¹⁴⁷. Bu görüşü savu-

¹⁴³ Koca/Üzülmez, Özel Hükümler, s. 815.

¹⁴⁴ Koca/Üzülmez, Özel Hükümler, s. 816; Karagülmez, s. 174-175.

¹⁴⁵ Dülger, s. 374.

¹⁴⁶ Tezcan/Erdem/Önok, s. 982; Karagülmez, s. 174-175; Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 939; Koca/Üzülmez, Özel Hükümler, s. 816.

¹⁴⁷ Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 939.

nanlara göre; bilişim sistemine girme suçunun bedeli karşılığı yararlanılabilen bir sistem hakkında işlenmesi halinde hem bilişim sisteminin güvenliği hem de yetkilendirilmeyen kişilerin sisteme girişine müsaade edilmediğinden sistem içi veri güvenliği, veri mülkiyeti ve zilyetlik gibi birden fazla hukuksal değer ihlal edilir. Bedelin ödenmesi karşılığı hizmet veren bir sisteme, bedel ödenmeden erişim sağlandığında, sistemi işletenin sistem üzerindeki hakları zarar görür¹⁴⁸. Bu durumda cezayı artırmak gerekirken, indirim yapılması çelişkidir¹⁴⁹.

Başka bir görüşe göre ise; bu suç, 2016 tarihli 6698 sayılı kanunla yapılan değişiklikle sisteme girme veya sistemde kalmaya devam etme hareketlerinden biriyle işlenebilen seçimlik hareketli bir suç haline geldiğinden, 2. fıkra bakımından da bu seçimlik hareketler ayrı ayrı değerlendirilmelidir. Buna göre; sistemde kalmaya devam etme hareketi bakımından kalmaya devam edilen sistemin bedeli karşılığı yararlanılabilen bir sistem olması halinde bu nitelikli hal uygulanarak cezada indirime gidilemez¹⁵⁰.

Bizim de görüşlerine iştirak ettiğimiz yazarlara göre ise, bilişim sistemine girme suçunun, bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesinin indirim nedeni olarak düzenlenmesi isabetlidir¹⁵¹. Bilişim sistemi üzerinde hak sahibi olan kişi, sisteme giriş bedeli ödendiğinde, girişe izin verir. Bu nedenle, bedeli ödendiğinde giriş izni verilen sisteme hukuka aykırı olarak girilmesiyle ortaya çıkan haksızlık, hiçbir şekilde girilmesine müsaade edilmeyen bir sisteme girildiğinde oluşacak haksızlığa göre daha hafiftir¹⁵². Ayrıca, bilişim sistemine girme suçuyla bilişim sistemi sahibinin özel yaşam ve haberleşme özgürlüğü gibi mahremiyetine ilişkin hakları da korunur. Bedeli karşılığında yararlanılabilen sistemler söz konusu olduğunda ise, mahremiyet yerine maddi menfaat öne çıkmaktadır. Bu nedenle kanun koyucu ekonomik değerlerin, mahremiyete oranla daha az cezaya layık olduğuna karar vermiştir¹⁵³.

Bedeli karşılığında yararlanılan sisteme girmek için, bedelin sisteme giriş yapan kişi tarafından bizzat ödenmesi gerekmez. Örneğin, akademik yayınlara veya yargı kararlarına ulaşma imkanı sunan elektronik veri tabanlarına üniversite veya diğer kurumlar abone olmakta, böylece çalışanlar herhangi bir ücret ödmeden sistemden yararlanabilmektedir. Bedeli karşılığı yararlanılabilen sisteme giriş yapan kişiler, giriş bedelini bizzat kendileri ödemeseler de bu tür bir sistem de “bedeli karşılığı yararlanılabilen bir sistemdir”. Bedel kurum tarafından ödendiği için çalışanların sisteme girme hakları vardır. Ancak çalışan işten ayrıldıktan sonra, kurum tarafından kendisine verilen şifreyi kullanarak sisteme

¹⁴⁸ **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 939.

¹⁴⁹ **Tezcan/Erdem/Önok**, s. 982; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 939.

¹⁵⁰ **Akbulut**, s. 143.

¹⁵¹ **Karagülmez**, s. 189; **Mahmutoğlu**, s. 863.

¹⁵² **Koca/Üzülmez**, Özel Hükümler, s. 816.

¹⁵³ **Yenidünya**, s. 1040.

girmişse, artık sisteme giriş yetkisi bulunmadığı için bilişim sistemine girme suçu oluşur. Söz konusu sistem bedeli karşılığı yararlanılan bir sistem olduğundan, fail hakkında TCK m. 243/2 hükmü uygulanmalıdır. Kurum çalışanının şifresini bir başkasına vererek sisteme girme ve sistemden yararlanma yetkisine sahip olmayan 3. bir kişinin sisteme girmesi halinde de bu suç oluşur. Zira sisteme giriş yapmaya rıza göstermeye yetkili olan kişi, kurum çalışanı değil, tüzel kişi olan kamu kurumu (bu örnekte üniversite) veya şirkettir. Yetkisiz kişinin rızasıyla sisteme giren 3. kişinin eylemi hukuka aykırı olmaya devam eder.

Bilişim sistemine girme suçunun bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi durumunda fail hakkında daha az cezaya hükmedilmesi isabetli ise de kanımızca bu fıkranın TCK m. 243 içerisinde değil, karşılıksız yararlanma suçunun düzenlendiği TCK m. 163 kapsamında düzenlenmesi daha isabetli olacaktır.

2. Bilişim Sistemindeki Verilerin Yok Edilmesi veya Değiştirilmesi (TCK m. 243/3)

TCK m. 243/3'ün; *“Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.”* şeklindeki 3. fıkrasının, TCK m. 243/1’de düzenlenen bilişim sistemine girme suçunun nitelikli hali mi, yoksa neticesi sebebiyle ağırlaşmış suç mu olduğu tartışmalıdır.

Bir görüşe göre; TCK m. 243/3’te düzenlenen eylem, yalnızca bilişim sistemine girme veya orda kalma değil, bu hareketler sebebiyle sistemde bulunan verinin yok edilmesi ya da değiştirilmesidir. Bu nedenle de bu fıkranın neticesi sebebiyle ağırlaşmış bir suç olarak kabul edilmesi gerekir¹⁵⁴. Diğer bir görüşe göre ise, bilişim sistemine girme veya orada kalma eylemleri gerçekleştirilirken, sistemin içerdiği veriler yok olur veya değişirse, daha ağır bir ceza verileceğine ilişkin TCK m. 243/3 hükmü, bilişim sistemine girme suçunun nitelikli hali-
dir¹⁵⁵.

TCK m. 244/2’de düzenlenen *“Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.”* hükmüyle de verilerin bozulması, yok edilmesi, değiştirilmesi veya

¹⁵⁴ Koca/Üzülmez, Özel Hükümler, s. 817; Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 937; Yenidünya, s. 1041; Erdoğan, s. 1402; Kurt, s. 152; Akbulut’a göre; nitelikli hallerin kastın kapsamında değerlendirilmesi gerektiğinden taksirli olarak gerçekleşmeleri mümkün değildir. Ancak 3. fıkra düzenlenenen neticenin taksirli olarak gerçekleşmesi gerekmektedir. Ayrıca nitelikli halde temel suç tipinde yer almayan bir netice düzenlenemez. TCK m. 243/1’de düzenlenen bilişim sistemine girme suçu sırf hareket suçudur. 3. fıkra ise neticenin gerçekleşmesi aranmaktadır. Bu nedenlerle TCK m. 243/3 nitelikli hal olarak değerlendirilemez. Bkz. Akbulut, s. 148, 149.

¹⁵⁵ Tezcan/Erdem/Önok, s. 982.

erişilmez kılınması hareketleri suç olarak düzenlenmiştir. Aynı hareketler için iki ayrı düzenlemenin mevcut olması nedeniyle failin hangi madde kapsamında cezalandırılacağı sorusu, tereddütlere yol açmaktadır. Bir görüşe göre; verilerin bozulması veya değiştirilmesi hareketleri bakımından failin kastı belirlenmeli, ona göre TCK m. 243/3 ya da TCK m. 244/2 uygulanmalıdır¹⁵⁶. TCK m. 243/3’de düzenlenen suç gerçek neticesi sebebiyle ağırlaşan suçtur. Bu suçlarda ağır neticeye yalnızca taksirle sebebiyet verilebilir¹⁵⁷. Bu nedenle TCK m. 243/3’ün uygulanabilmesi için, failin verilerin bozulması ya da değiştirilmesine yönelik bir kastı olmamalıdır. Eğer failin kastı verileri yok etmek veya değiştirmekse TCK m. 244/2 uygulanmalıdır¹⁵⁸. Bir görüşe göre ise; neticesi sebebiyle ağırlaşmış suç hem kasten hem de taksirle işlenebileceğinden verilerin yok olması ya da değişmesi durumunda failin kasten ya da taksirle hareket etmesi arasında bir fark yoktur. Bu durumda failin sorumluluğu TCK m. 243/3’e göre belirlenir. Buna karşın fail verileri yok etme veya değiştirme kastıyla hareket ederse, TCK m. 244/2’de tanımlanan suç da oluşur ve bu iki suç arasında fikri içtima kuralları uygulanmalıdır¹⁵⁹.

Öğretide, failin TCK m. 243/3’de yer alan ağırlatıcı sebepten sorumlu tutulması için taksirin varlığının yeterli görülmesini, kast sorumluluğunu esas alan Avrupa Konseyi Siber Suç Sözleşmesi hükümleriyle çelişkili olduğu gerekçesiyle eleştiren yazarlar da bulunmaktadır¹⁶⁰.

TCK m. 243/3’de yer alan düzenlemenin, TCK m. 243/1’de düzenlenmiş olan bilişim sistemine girme suçunun neticesi sebebiyle ağırlaşmış şekli olduğu yönündeki görüşe katılıyoruz. Bu husus TCK m. 243’ün gerekçesinde de belirtilmiş, ayrıca hükmün uygulanabilmesi için failin verileri yok etme veya değiştirme kastıyla hareket etmemesi gerektiğine işaret edilmiştir. Bu durumda kasten bir bilişim sistemine giren veya orada kalmaya devam eden fail, verilerin yok olması veya değiştirilmesi neticeleri açısından taksirli hareket etmişse TCK m. 243/3 hükmü uygulanır. Failin verileri yok etme veya değiştirme kastıyla hareket ettiği hallerde ise, TCK m. 244/2 uygulanmalıdır.

Bilişim sistemine girme veya orada kalmaya devam etme fiili nedeniyle yok olan veya değişen verilerin niteliği önemli değildir. Bu veriler, sistemin

¹⁵⁶ Tezcan/Erdem/Önok, s. 982; Gül, s. 65.

¹⁵⁷ Koca/Üzülmez, ağır netice bakımından failin yalnızca taksirle hareket etmesi gereken neticesi sebebiyle ağırlaşmış suçları “gerçek neticesi sebebiyle ağırlaşmış suçlar”; ağır netice bakımından taksirle de kasten de hareket edilebilecek neticesi sebebiyle ağırlaşmış suçları ise “gerçek olmayan neticesi sebebiyle ağırlaşmış suçlar” olarak adlandırmaktadır. Bkz. Koca/Üzülmez, Genel Hükümler, s. 246; Koca/Üzülmez, Özel Hükümler, s. 817, Karagülmez, s. 191.

¹⁵⁸ Koca/Üzülmez, Özel Hükümler, s. 817; Karagülmez, s. 191; Artuk/Gökçen/Yenidünya, Özel Hükümler, s. 863; Akbulut, s. 149; Ketizmen, s. 111.

¹⁵⁹ Dülger, s. 350.

¹⁶⁰ Yenidünya, s. 1041.

çalışmasına yarayan yazılımlar olabileceği gibi, sistemde kayıtlı herhangi bir bilgiye ilişkin bir veri de olabilir¹⁶¹.

Yok olan veya değiştirilen verilerin bulunduğu sistemin, bedeli karşılığı yararlanılabilen bir sistem olması halinde, TCK m. 243/3 uygulanır. Bu durumda TCK m. 61/4'e göre, faile verilecek cezada önce TCK m. 243/3'e göre artırım, ardından TCK m. 243/2'ye göre indirim yapılır.

VII. TEŞEBBÜS

TCK m. 243/1'de düzenlenen bilişim sistemine girme suçu teşebbüse elverişlilik açısından, her bir seçimlik hareket ayrı ayrı ele alınarak değerlendirilmelidir¹⁶².

Sistemin tamamına ya da bir kısmına hukuka aykırı olarak “girme” seçimlik hareketi açısından, suçun teşebbüs aşamasında kalması kural olarak zor görünmektedir¹⁶³. Bununla birlikte yetkisiz erişim için elverişli bir şekilde icra hareketlerine başlanmasına rağmen erişim sağlanamazsa, suç teşebbüs aşamasında kalır¹⁶⁴. Örneğin; hukuka aykırı olarak erişim sağlanması amaçlanan bilişim sistemine, siber saldırı başlamış olmasına rağmen, bu saldırı bilişim sisteminde bulunan güvenlik programlarınca engellenirse, suç teşebbüs aşamasında kalır¹⁶⁵. Aynı şekilde fail bilgisayarı açmak için düğmeye basmasına rağmen, elektrikler kesik olduğu için veya teknik bir arıza nedeniyle bilgisayar açılmaz veya şifrelenmiş bir sisteme şifreyi kıramadığı için giremezse, suç yine teşebbüs aşamasında kalacaktır.

Sistemde kalma seçimlik hareketi açısından ise suç teşebbüse elverişli değildir¹⁶⁶. Zira bu seçimlik hareket için herhangi bir süre belirlenemeyeceğinden hareketi neticeden ayırmak da mümkün görünmemektedir¹⁶⁷.

Öğretide savunulan bir görüşe göre; TCK m. 243/3'te düzenlenen sistemin içerdiği verilerin yok olması veya değişmesi neticesi açısından da kural olarak teşebbüs mümkün değildir. Bununla beraber netice hareketten ayrılabiliyorsa teşebbüs mümkün olabilir¹⁶⁸. Bizim de katıldığımız diğer bir görüşe göre ise; TCK m. 243/3 yalnızca taksirle gerçekleştirilebileceğinden ve taksirli bir suça da

¹⁶¹ Koca/Üzülmez, Özel Hükümler, s. 817.

¹⁶² Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 941.

¹⁶³ Koca/Üzülmez, Özel Hükümler, s. 817-818.

¹⁶⁴ Akbulut, s. 151; Tezcan/Erdem/Önok, s. 984, Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 941.

¹⁶⁵ Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 941; Koca/Üzülmez, Özel Hükümler, s. 818.

¹⁶⁶ Tezcan/Erdem/Önok, s. 984; Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 941; Akbulut, s. 151.

¹⁶⁷ Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 941

¹⁶⁸ Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 941.

teşebbüs edilmesi mümkün olmadığından bu fıkra bakımından teşebbüs mümkün değildir¹⁶⁹.

VIII. İŞTİRAK

Bilişim sistemine girme suçu iştirak açısından herhangi bir özellik arz etmez. Suç birden fazla kişi tarafından ortaklaşa işlendiğinde, iştirake ilişkin genel hükümler uygulanır¹⁷⁰. TCK m. 243 bakımından tüm faillik ve şeriklik türlerinin oluşması mümkündür¹⁷¹.

IX. SUÇLARIN İÇTİMAI

Bilişim sistemine girme suçu zincirleme şekilde işlenebilir. Bilişim sistemine girme suçunun unsuru olan seçimlik hareketler, başka bir suçun unsuru veya nitelikli hali de olabilir.

Failin aynı suç işleme kararının icrası kapsamında, ancak farklı zamanlarda aynı bilişim sistemine birden fazla girmesi veya orada kalması durumunda, bilişim sistemine girme suçu zincirleme şekilde işlenir. Bu durumda TCK m. 43/1 uygulanır¹⁷².

TCK m. 243'teki suçlar nitelikleri gereği başka bir suçun unsuru ya da nitelikli hali olabilir. Bu durumda bileşik suç hükümleri uygulanacağından, ayrıca TCK m. 243'ten ceza verilmez¹⁷³. Örneğin; bilişim sistemini araç olarak kullanarak hırsızlık suçunu işleyen fail hakkında bileşik suç hükümleri gereğince yalnızca TCK m. 142/2-e hükmü uygulanacaktır¹⁷⁴. Benzer şekilde TCK m. 158/1-f'de dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlenmesi ağırlatıcı neden olarak düzenlenmiştir. Hukuka aykırı olarak bilişim sistemine giren fail, insanları kandırıp kendisine veya başkasına menfaat temin ediyorsa, ceza TCK m. 243'e göre değil, TCK m. 158/1-f'ye göre belirlenir. Bir Yargıtay kararına¹⁷⁵ da konu olan olayda olduğu gibi: Fail, mağdurun "MSN Messenger" adresinin şifresini ele geçirir ve farklı zamanlarda internete girerek MSN listesindeki arkadaşlarına acil kontör ihtiyacı olduğunu söyleyerek, onları aldatır. Fail, kimliği konusunda aldattığı kişilerin kendisine

¹⁶⁹ Akbulut, s. 151.

¹⁷⁰ Dülger, s. 380; Esen, s. 631.

¹⁷¹ Akbulut, s. 152.

¹⁷² "... Saniğin, mağdura ait elektronik posta hesabına, bir suç işleme kararının icrası kapsamında üç kez izinsizce giriş yapması biçiminde sübutu kabul edilen eyleminin, zincirleme şekilde TCK m. 243/1. maddesinde tanımlanan bilişim sistemine girme suçunu oluşturduğu gözetilmeden..." Y 12. CD., E. 2016/5905, K. 2017/ 7072, T. 4.10.2017, www.kazancı.com, Erişim Tarihi: 06.05.2018; Tezcan/Erdem/Önok, s. 984; Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 942; Koca/Üzülmez, Özel Hükümler, s. 818.

¹⁷³ Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 942.

¹⁷⁴ Mahmutoglu, s. 864.

¹⁷⁵ Y. 15. CD., E. 2016/4937, K. 2017/19032, T. 28.09.2017, www.kazancı.com.tr, Erişim Tarihi: 21.05.2018.

gönderdikleri şifrelerle elde ettiği kontörleri, başkalarına daha ucuza satarak maddi menfaat temin eder. Söz konusu olayda fail artık bilişim sistemine girme suçundan değil, dolandırıcılık suçundan cezalandırılmalıdır¹⁷⁶. Failin bilişim sistemine, dolandırıcılık veya özel yaşamın gizliliğini ihlal gibi başka bir suç işlemek amacıyla girmesi halinde TCK m. 243 ile birlikte ilgili suçtan da cezalandırılması gerektiği görüşü de öğretide savunulmaktadır¹⁷⁷. Ancak biz bu görüşe iştirak etmiyoruz.

Bilişim sistemine girme veya orada kalma hareketleriyle aynı zamanda özel hayatın gizliliği ihlal edilir (TCK m. 134) veya kişiler arasındaki haberleşme engellenirse (TCK m. 124) fikri içtima hükümleri uygulanmalıdır¹⁷⁸. Aynı şekilde, kişinin e-maillerine girilerek elektronik postaları okunursa, fikri içtima kuralları gereği fail daha ağır cezayı gerektiren TCK m. 132’de düzenlenmiş olan haberleşmenin gizliliğini ihlal suçundan cezalandırılmalı, ayrıca TCK m. 243’ten cezalandırılmamalıdır¹⁷⁹.

¹⁷⁶ “... Sanık hakkında TCK m. 243/1 maddesi uyarınca kamu davası açılmasına rağmen bu suçla ilgili tartışma ve değerlendirme yapılmadığı gibi,... Sanık, MSN Messenger adreslerinin şifresini ele geçirip farklı zamanlarda internete girerek, MSN adreslerindeki arkadaş listesinde bulunan kişilerden acil olarak kontör istedikleri, ..., şikayetçi ..’nın kontör şifresini bilgisayara yazıp gönderdikleri, gönderilen kontör şifrelerinin sanıklar tarafından piyasada ucuza satıldığı şeklinde gerçekleşen eylemlerinin nitelikli dolandırıcılık suçlarını oluşturduğu anlaşıldığından mahkemenin kabulünde bir isabetsizlik görülmemiştir...” Y. 15. CD., E. 2016/4937, K. 2017/19032, T. 28.09.2017, www.kazanci.com.tr, Tarih: 21.05.2018; “...Sanık ...’ın olay tarihinde annesi ...’ın abonesi gözüktüğü ... numaralı cep telefonu hattıyla müşteki ...’ın e-posta adresine şifresini kırmak suretiyle müştekinin izni ve bilgisi olmaksızın erişim sağladığı ve müştekinin erişimini şifresini değiştirerek engellediği, ardından da kendisine müşteki ...’ın arkadaşı... olarak tanıtılarak para talep ettiği, müştekinin arkadaşı... ile telefonla görüşerek söz konusu mailin ... tarafından gönderilmediği, ...’e ait mail adresinin başkalarınca ele geçirildiğini öğrenmesi üzerine para göndermediği, sanığın bu şekilde üzerine atılı suçu işlediğinin iddia edildiği olayda,
1-) Sanık hakkında nitelikli dolandırıcılık suçundan verilen mahkumiyet hükmüne yönelik temyiz incelemesinde,

Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre; sanığın temyiz itirazlarının reddiyle, hükmün ONANMASINA...” Y. 15. CD., E. 2016/3871, K. 2016/8608, T. 15.11.2016, www. Kazanci.com.tr, Erişim Tarihi: 25.05.2018. “... Sanığın olay tarihinde kendi adına kayıtlı cep telefonu hattı ile giriş yaparak katılan ...’nın email adresini ve bu adrese bağlı facebook hesabının şifresini kararak, hesaba giriş şifresini değiştirip, katılanın arkadaş listesinde olan katılan ...’dan acil olduğunu söyleyerek 280 TL para istediği, katılan ...’un da sanığın vermiş olduğu hesap numarasına 280 TL yatırdığı, aynı gün katılan ...’e de mesaj atarak internet bankacılığı kullanıp kullanmadığını sorduğu, katılan ...’in durumdan şüphelenerek ne yapacağını sorması üzerine sanığın katılan ...’e sinkaflı küfürler ettiği, bu surette sanığın katılan ...’ya bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık,... sanığın atılı suçları işlediği anlaşıldığından mahkemenin kabul ve uygulamasında bir isabetsizlik görülmemiştir...” Y. 15. CD., E. 2017/7493, K. 2018/1371, T. 27.02.2018, www.kazanci.com.tr, Erişim Tarihi: 18.06.2018.

¹⁷⁷ Tezcan/Erdem/Önok, s. 985.

¹⁷⁸ Özbek/Doğan/Bacaksız/Tepe, Özel Hükümler, s. 942.

¹⁷⁹ Koca/Üzülmez’e göre; haberleşmenin gizliliğini ihlal etmek amacıyla bilişim sistemine girildiğinde iki suç oluşur. Failin başkasına ait şifreyi ele geçirerek elektronik posta adresine

Bilişim sistemine hukuka aykırı olarak girme suçuyla TCK m. 136'da düzenlenen verileri ele geçirme suçu arasında da özel bir içtima ilişkisi vardır. Bir görüşe göre¹⁸⁰, bu ilişki tüketen- tüketilen norm şeklinde ortaya çıkan bir görünüşte içtima ilişkisidir. Zira TCK m. 243'te düzenlenen suçun işlenebilmesi için, verilerin ele geçirilmesi gerekmez. Bu nedenle, TCK m. 243 ile TCK m. 136 arasında fikri içtima hükümleri uygulanamaz. Ancak kişisel verilerin hukuka aykırı olarak ele geçirilmesi, bilişim sistemine hukuka aykırı olarak girme suçunun haksızlığını da içerisinde barındırır. Bu iki norm arasında tüketen- tüketilen norm ilişkisi var olduğundan, fail yalnızca TCK m. 136'ya göre cezalandırılmalıdır¹⁸¹. Diğer bir görüşe göre ise; araç- amaç suç ilişkisinin söz konusu olduğu hallerde, bu suçların icra hareketleri arasında örtüşme yoksa her bir suçtan ayrı ayrı ceza verilmelidir. Araç suç ile amaç suçun icra hareketlerinin birbiriyle örtüştüğü durumlarda ise, failin cezai sorumluluğu farklı neviden fikri içtima hükümlerine göre belirlenmelidir¹⁸². Bu durumda, fail TCK m. 243'ten değil, daha ağır cezayı gerektiren TCK m. 136'dan cezalandırılmalıdır.

Suçların içtimai ile ilgili olarak üzerinde durulması gereken bir diğer konu da TCK m. 243 ile TCK m. 244 arasındaki ilişkidir. Bir görüşe göre; TCK m. 244'de düzenlenmiş olan suçlarla TCK m. 243'te düzenlenmiş olan bilişim sistemine girme fiili örtüşmektedir. Bu nedenle bu iki suç arasında fikri içtima hükümleri uygulanmalıdır¹⁸³. Diğer bir görüşe göre ise; failin kastına göre değerlendirme yapılmalı ve m. 244'te yer alan suçun işlenmesi halinde, aynı eylemden dolayı faile TCK m. 243'ten ceza verilmemelidir¹⁸⁴. Failin kastından hareket eden bir başka görüşe göre; fail bilişim sistemine, sistemin işleyişini engellemek veya bozmak amacıyla girmişse TCK m. 243 değil, TCK m. 244/1; verileri bozma, değiştirme, erişilmez kılma, veri yerleştirme, verileri başka yere gönderme amacıyla girmişse TCK m. 244/2¹⁸⁵; haksız bir yarar sağlamak

girip, buradaki yazışmalarını okuması halinde hem TCK m. 243'de düzenlenmiş olan bilişim sistemine girme, hem de TCK m. 132/1'de düzenlenmiş olan haberleşmenin gizliliğini ihlal suçları oluşur. Ancak yazarlar bu durumda fikri içtima kurallarının uygulanıp uygulanamayacağına ilişkin bir görüş beyan etmemişlerdir. Bkz. **Koca/Üzülmez**, Özel Hükümler, s. 484.

¹⁸⁰ **Tezcan/Erdem/Önok**, s. 985.

¹⁸¹ **Tezcan/Erdem/Önok**, s. 985.

¹⁸² **Koca/Üzülmez**, Özel Hükümler, s. 818.

¹⁸³ **Koca/Üzülmez**, Özel Hükümler, s. 819.

¹⁸⁴ **Yenidünya**, s. 1039; **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s. 942.

¹⁸⁵ "... Çukurova Üniversitesi Fen Edebiyat Fakültesi'nde işçi olarak çalışan sanık M.. 'nın, aynı Fakülte'nin Biyoloji Bölümü II. öğretim öğrencisi B.. 'nin bilgisi dahilinde, bu sanığa ait 2000-2002 ve 2003 güz ve bahar dönemlerindeki başarısız olduğu birçok dersin sınav sonuçlarını değiştirip başarılı olmasını sağladığı, aynı şekilde Çukurova Üniversitesi Mühendislik Fakültesi Makina Mühendisliği Bölümü II. Öğretim öğrencisi sanık S.. ile Çukurova Üniversitesi Su Ürünleri Fakültesi II. Öğretim öğrencisi sanık A'nın da kendilerine ait başarısız oldukları birçok dersin sınav sonuçlarını değiştirdiklerinin iddia olunması... iddianamede dava konusu edilen fiil, sanıkların bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri değiştirmelerinden ibaret olup... 5237 sayılı TCY'nın 244/2. Maddesinde de benzer

amacıyla girmişse TCK m. 244/4¹⁸⁶ uygulanmalıdır. TCK m. 243 ile TCK m. 244 arasında tüketen- tüketilen norm ilişkisidir. Bu nedenle TCK m. 244'ün unsurlarının olduğu hallerde faile ayrıca TCK m. 243'den ceza verilmez¹⁸⁷. Başka bir görüşe göre ise; TCK m. 243 ile TCK m. 244 arasında tüketen- tüketilen norm ilişkisi yoktur. Hatta burada failin hareketi de tek değildir. Bu nedenle zamansal değerlendirme yapılmalıdır. Eylemler arasında zamansal yakınlık varsa yalnızca TCK m. 244'den, zamansal yakınlık yoksa her iki suçtan da ayrı ayrı ceza verilmelidir¹⁸⁸.

X. YAPTIRIM VE MUHAKEME

TCK m. 243/1'de bilişim istemine girme suçunu işleyen fail hakkında *bir yıla kadar hapis veya adli para cezasına hükmedileceği* düzenlenmiştir. TCK m. 243/2'de, suçun bedeli karşılığında yararlanılabilen sistemler hakkında işlenmesi halinde faile verilecek cezanın yarı oranında indirileceği; m. 243/3'te, fiil nedeniyle verilerin yok olması ya da değişmesi halinde fail hakkında altı aydan iki yıla kadar hapis cezasına hükmedileceği; m. 243/4'te ise bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen failin bir yıldan üç yıla kadar hapis cezasıyla cezalandırılacağı düzenlenmiştir.

Bilişim sistemine girme suçu re'sen takip edilen bir suçtur. Ancak, suçun haksızlık içeriğinin kamu adına re'sen soruşturma ve kovuşturma yapılmasını gerektirecek kadar önemli olmadığı kanaatindeyiz. Bu nedenle suçun takibi şikayete bağlı hale getirilerek, bilişim sistemine girme suçu CMK m. 253 bağlamında uzlaştırma kapsamına alınabilir.

Yargılama açısından görevli mahkeme, asliye ceza mahkemesidir.

SONUÇ

Yaşanan teknolojik gelişmelere bağlı olarak bilişim sistemleri hayatımızın her alanında yer almakta ve hem kişisel hem de iş hayatımıza dair pek çok bilgiyi içerisinde barındırmaktadır. Bunun sonucunda bilişim sistemlerinin, özel

şekilde düzenlemeye konu edilmiştir...iddianamede açıklanan ve suç oluşturduğu ileri sürülen fiil "bilişim sistemine girmek suretiyle bilgileri değiştirmek"ten ibaret olup...", YCGK, E. 2007/11- 44, K. 2007/200, T. 9.10.2007, www.kazancı.com.tr, Tarih: 22.05.2018.

¹⁸⁶ "...Sanığın, katılanın yetkilisi olduğu Z. T. İmalat Pazarlama Sanayi ve Ticaret Limited şirketinin Türkiye E. Bankası Denizli şubesinde bulunan hesabına 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 aykırıdır...", Y. 11. CD., E. 2008/18190, K. 2009/3058, T. 26.03.2009, www.kazancı.com.tr, Tarih: 22.05.2018.

¹⁸⁷ Tezcan/Erdem/Önok, s. 985.

¹⁸⁸ Dülger, s. 384.

hayatın gizliliğinin ihlali veya maddi menfaat temini gibi farklı saiklerle saldırıya uğrama riski de artmaktadır. Bu nedenle de bilişim sistemlerinin içerdiği verileri korumaya yönelik önlemlerin alınması büyük bir önem arz etmektedir. Bu önemlerin başında ise bilişim sistemlerine yetkisiz erişimin suç olarak düzenlenmesi gelmektedir.

Bilişim sistemine haksız erişim gerek 765 sayılı TCK gerekse yürürlükte bulunan 5237 sayılı TCK'da suç olarak düzenlenmiştir. Ancak bilişim sistemine haksız erişim 765 sayılı Türk Ceza Kanunundan farklı olarak 5237 sayılı TCK'da münferit bir suç olarak düzenlenmiştir. Bilişim sistemine girme suçu 5237 sayılı TCK m. 243'te düzenlenmiş olup bu suç; bilişim sisteminin güvenliği ve güvenilirliğinin, özel hayatın gizliliğinin ve haberleşme özgürlüğünün korunması amacını taşıyan karma nitelikli bir suçtur.

Bilişim sistemine girme suçunun 5237 sayılı TCK'da münferit bir suç olarak düzenlenmesi ve 765 sayılı TCK'dan farklı olarak bu suçun oluşması için "verilerin ele geçirilmesi" neticesinin aranmaması bilişim sistemlerinin korunması bakımından yerinde olmuştur. Ayrıca 24.03.2016 tarih ve 6698 sayılı kanun ile 5237 sayılı TCK m. 243/1'de değişiklik yapılarak "ve" bağlacı "veya" olarak değiştirilmiş; yapılan bu değişiklikle hem Avrupa Konseyi Siber Suçlar Sözleşmesiyle uyum sağlanmış hem de bilişim sistemlerine yönelen saldırılara karşı daha kapsamlı bir koruma mekanizması oluşturulmuştur.

Bilişim sistemine girme suçu açısından, kamu personellerine ve özel sektör çalışanlarına görevleriyle ilgili olarak tahsis edilen bilgisayarların durumunun ayrıca değerlendirilmesi gerekmektedir. Bu bilgisayarlar o işyerine özgü faaliyetlerin yürütülmesi amacıyla çalışanlara teslim edilmektedir. Uygulamada yaygın olarak bu bilgisayarlarda hem şifreli bir hesap hem de şifre gerektirmeyen genel kullanıcı hesabı bulunmaktadır. Genel kullanıcı hesabının açılmasının nedeni ise; işlerin yürütülmesi amacıyla bir başka personelin de bu bilgisayarı kullanabilmesidir. Bir personelin başka bir çalışana zimmetlenen bilgisayara işlerin yürütülmesi amacıyla, bilgisayarın verildiği personelin şifreli hesabına müdahalede bulunmaksızın, genel kullanıcı hesabından girmesi veya sistemde kalması yetkisiz erişim olarak değerlendirilemez. Bu erişim, şifreyle koruma altına alınan hesap kullanıcısının özel hayatına, haberleşme özgürlüğüne ve bilişim sisteminin güvenliğine karşı bir saldırı olarak değerlendirilemeyeceğinden TCK m. 243 ile korunan hukuki değerleri ihlal etmez.

Şayet bir kurumda çalışan personelin ortak kullanımına sunulmuş ve bir kimsenin zimmetine bırakılmamış bir bilgisayar söz konusu ise; burada çalışanların her birinin sisteme girme yetkisi olduğundan bilişim sistemine girme suçu söz konusu olmaz. Bunun yanında, bir personele zimmetlenmiş olan bilgisayara girilmesi, hak sahibinin açıkça rıza göstermediği veya şifrelemek suretiyle başkalarının sisteme girişine izin vermediği hallerde, hukuka aykırı olduğundan bilişim sistemine girme suçu oluşacaktır.

Diğer yandan, birden çok kişinin aynı ortamda mesai yaptığı kamu kurum ve kuruluşlarıyla özel sektör işyerlerinde çalışanların, işlem yapmak yahut çıktı almak gibi sebeplerle birbirlerinin bilgisayarlarını kullanmaları sıklıkla karşılaşılan bir durumdur. Çoğunlukla yargıya taşınmayan bu durumlar, araya başkaca husumetlerin girmesiyle cezai uyuşmazlığa dönüşmekte ve yargının önüne gelebilmektedir. Kanaatimizce bu gibi durumlarda hayatın olağan akışı içerisinde yürütülen faaliyetin gereği olarak gerçekleştirilen bilişim sistemine girme eylemlerinin hukuka aykırılık bilinciyle gerçekleştirildiği kabul edilemez. Esasen buradaki hukuki meselenin rıza, rızanın varlığında hata, hukuka aykırılık bilinci veya kastın bulunup bulunmadığı çerçevesinde değerlendirilmesi gerekmektedir.

KAYNAKÇA

- Akbulut**, Berrin: Bilişim Alanında Suçlar, 2. Baskı, Adalet Yayınevi, Ankara, 2017.
- Apaydın**, Cengiz: Bilişim Sistemine Girme Suçu, TADD, Yıl 2016, S. 24, s. 245-308.
- Artuk**, M. Emin/**Gökçen**, Ahmet/**Yenidünya**, A. Caner: Ceza Hukuku Genel Hükümler, 10. Baskı, Ankara 2016.
- Artuk**, M. Emin/**Gökçen**, Ahmet/**Yenidünya**, A. Caner: Ceza Hukuku Özel Hükümler, 15. Baskı, Ankara, 2015.
- Baş**, Eylem: Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, Yetkin Yayınları, Ankara, 2015.
- Centel**, Nur/**Zafer**, Hamide/**Çakmut**, Özlem: Türk Ceza Hukukuna Giriş, 10. Bası, İstanbul, 2017.
- Çağlayan**, Ramazan: İdare Hukuku Dersleri, 5. Baskı, Ankara, 2017.
- Demirbaş**, Timur: Ceza Hukuku Genel Hükümler, 11. Baskı, Ankara, 2016.
- Demren Dönmez**, Burcu: “Türk Ceza Kanununda ‘Kamu Görevlisi’ Kavramı”, TBB Dergisi, S. 94, 2011, s. 95-130.
- Dülger**, Murat Volkan: Bilişim Suçları ve İnternet İletişim Hukuku, 4. Baskı, Ankara, 2014.
- Ekici Şahin**, Meral: Ceza Hukukunda Rıza, İstanbul, 2012.
- Erdağ**, Ali İhsan: Bilişim Alanında Suçlar, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. 14, Yıl 2010, S. 2, s. 275-303.
- Erdoğan**, Yavuz: Bilişim Sistemine Girme ve Kalma Suçu, DEÜHFD, C. 12, Prof. Dr. Burhan Ceyhan’a Armağan Özel Sayısı, Yıl 2010, s. 1363-1433.
- Esen**, Sinan: Anlatımlı ve İctihatlı Malvarlığına Karşı Suçlar Belgelerde Sahtecilik ve Bilişim Alanında Suçlar, Adalet Yayınevi, Ankara, 2007.
- Gören**, Sami: En Son Değişikliklerle Açıklamalı-İctihatlı 5237 Sayılı Türk Ceza Kanunu, Yetkin Basımevi, Ankara, 2012.
- Gül**, Ahmet: Doğrudan/Dolaylı Bilişim Suçları, Ankara, 2016.
- Kangal**, Zeynel: Tüzel Kişilerin Ceza Sorumluluğu, Ankara 2003
- Kalabalık**, Halil: İdare Hukuku Dersleri Cilt: 1, 7. Baskı, Konya, 2016.
- Karagülmez**, Ali: Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri, 3. Baskı, Ankara 2011.
- Karakehya**, Hakan: Türk Ceza Kanununda Bilişim Sistemine Girme Suçu, TBB Dergisi, Yıl 2009, S. 81, s. 187-210.
- Ketizmen**, Muammer: Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008.
- Koca**, Mahmut/**Üzülmez**, İlhan: Türk Ceza Hukuku Genel Hükümler, 11. Baskı, Ankara 2018.

- Koca**, Mahmut/Üzülmez, İlhan: Türk Ceza Hukuku Özel Hükümler, 3. Baskı, Ankara, 2016.
- Kurt**, Levent: Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005.
- Mahmutoğlu**, Fatih Selami: “Türk Ceza Kanunda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 72, S. 1, 2013, s. 855-889.
- Önok**, Murat: Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, Prof. Dr. Nur Centel’e Armağan, Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Özel Sayı, Y: 2013, C: 19, S: 2, s. 1229-1269.
- Özay**, İlhan: Günışığında Yönetim, Filiz Kitabevi, İstanbul, 2004.
- Özbek**, Veli Özer/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker: Türk Ceza Hukuku Genel Hükümler, 7. Baskı, Seçkin Yayıncılık, Ankara, 2016.
- Özbek**, Veli Özer/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker: Türk Ceza Hukuku Özel Hükümler, 10. Baskı, Seçkin Yayıncılık, Ankara, 2016.
- Özen**, Muharrem/Tozman, Önder: “Türk Ceza Kanununda Kamu Görevlisi Kavramı”, Amme İdaresi Dergisi, C. 42, S. 4, Aralık 2009, s. 25-57.
- Özgenç**, İzzet: Türk Ceza Hukuku Genel Hükümler, 11. Baskı, Ankara 2015.
- Parlar**, Ali: Türk Ceza Hukukunda Bilişim Suçları, Bilge Yayınevi, 3. Baskı, Ankara 2015.
- Parlar**, Ali/Hatipoğlu, Muzaffer: Açıklamalı- Yeni İçtihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu, 4. Cilt, Seçkin Yayıncılık, Ankara, 2010.
- Şahbaz**, İbrahim: Açıklamalı ve İçtihatlı Türk Ceza Kanunu 2. Cilt, Ankara, 2016.
- Tan**, Turgut: İdare Hukuku, 3. Bası, Turhan Kitabevi, Ankara, 2014.
- Taşkın**, Şaban Cankat: Bilişim Suçları, İstanbul, 2008.
- Tezcan**, Durmuş/Erdem, Mustafa Ruhan/Önok, Murat R.: Teorik ve Pratik Ceza Özel Hukuku, 14. Baskı, Ankara, 2017.
- Toroslu**, Nevzat/Toroslu, Haluk: Ceza Hukuku Genel Kısım, Ankara 2018.
- Yaşar**, Osman/Gökcan, Hasan Tahsin/Artuç, Mustafa: Yorumlu Uygulamalı Türk Ceza Kanunu, 2. Baskı, C. V, Ankara, 2014.
- Yenidünya**, A. Caner: Bilişim Sistemine Hukuka Aykırı Erişim Suçu, Legal Fikri ve Sınai Haklar Dergisi, Yıl: 1, Sayı: 4, İstanbul, 2005, s. 1017-1047.
- Yıldız**, Mehmet Emre: Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, Adalet Yayınevi, Ankara, 2015.