

## SİBER SUÇLAR BİLİŞİM SUÇLARI

o "bilgisayar suçları", "bilişim suçları", "internette işlenen suçlar"

şeklinde de ifade edildiği görülmektedir.

o siber uzay denilen bilişim teknolojilerinin oluşturduğu ortamda işlenen suçlara siber suç adı verilmektedir.

o siber suç, bilişim teknolojilerini kullanarak, yine bir bilişim teknolojisine zarar vermek amacıyla siber uzaya yapılan eylemler olarak tanımlanabilir.

## BİLİŞİM SUÇLARINA İLK OLARAK RASTLANILAN ABD DOKTRİNİNDE SUÇLAR 12 BAŞLIK HALİNDE İNCELENMIŞTİR

1. Verilere veya hizmetlere karşı gerçekleştirilen hırsızlıklar
2. Mülkiyete karşı hırsızlıklar
3. Giriş İhlalleri
4. Veri sahtekârlığı
5. Şahıslardan kaynaklanan hatalar (insan hataları neticesi oluşan ihlaller)
6. Gasp
7. Sır aleyhine ihlaller
8. Sabotajlar
9. Maddi kişimlara yönelik hırsızlıklar 1
10. Vakalarda gerçekleştirilen sahtekârlıklar
11. Bankamatik(ATM) kartları konusundaki hırsızlıklar
12. Manyetik kartların şifreleri hususunda gerçekleştirilen eylemler

## BİRLEŞMİŞ MİLLETLER SINIFLANDIRMASI

BM'nin yayınladığı "Uluslararası Suç Politikasının Değerlendirilmesi-Bilgisayarla İlişkili Suçlar Kontrol ve Korunma Rehberi"nde yaygın olarak görülen bilgisayarla ilişkili suçlar 5 kategoriye ayrılmıştır (Birleşmiş Milletler, 1994).

- +**
- Bilgisayar manipülasyonu ile dolandırıcılık
  - Bilgisayar sahteciliği
  - Bilgisayar veri ve/veya programlarının değiştirilmesi ya da hasara uğratılması
  - Bilgisayar sistem ve servislerine yetkisiz erişim
  - Yasal olarak korunan programların izinsiz çoğaltılması  $\Rightarrow$  Patent, telif hakkı

## AVRUPA KONSEYİ SİBER SUÇ SÖZLEMESİ SINIFLANDIRMASI

Avrupa Konseyi Bakanlar Komitesince 8 Kasım 2001 tarihinde onaylanan ve hedefi ortak bir ceza politikasının oluşturulması ile toplumun siber suça karşı korunması, özellikle gerekli mevzuatın kabul edilmesi ve uluslararası işbirliğinin gerçekleştirilmesi olan Avrupa Konseyi Siber Suç Sözleşmesi'nde siber suçlar dört ana kategoride incelenmiştir. Bunlar;

- 4**
- Bilgisayar veri ve sistemlerinin bütünlüğüne, gizliliğine ve erişe bilirliğine ilişkin suçlar
  - Bilgisayarlarla ilgili suçlar
  - İçerikle ilgili suçlar
  - Telif Hakları ile ilgili suçlardır.

243 - 246

## ULUSLARARASI TELEKOMÜNIKASYON BİRLİĞİ SINIFLANDIRMASI

- +**
- o ITU'nun BİT Uygulamaları Ve Siber Güvenlik Birimi tarafından O hazırlanan raporlardan biri olan Siber Suçları Anlamak: Gelişmekte Olan Ülkeler için Rehber (ITU. 2009) de tanımlanan siber suç kategorilerini kapsar.
  - o ITU'nun suç sınıflandırması Avrupa Konseyi Siber Suç Sözleşmesindeki sınıflandırma temel alınıp bunların daha da geliştirilmesiyle oluşturulmuştur.

# ULUSLARARASI TELEKOMÜNIKASYON BİRLİĞİ SINIFLANDIRMASI

## 1. Bilgisayar veri ve sistemlerinin bütünlüğüne, gizliliğine ve erişe bilirliğine ilişkin suçlar.

- Yasadışı erişim (Illegal Access- Hacking, Cracking)
- Veri casusluğu (Data Espionage)  $\Rightarrow$  Bir Şirkette Çalışıyorsunuz o şirkete ait verileri dışarıda paylaşmak yasak ve bu veri casus lugudur.
- Yasadışı müdahale (Illegal Interception)
- Verilere müdahale (Data Interference)
- Sistemlere müdahale (System Interference)

## 2. Bilgisayarlarla ilişkili suçlar

- Bilgisayar yoluyla sahtekârlık fiilleri
- Bilgisayar yoluyla dolandırıcılık fiilleri

Bankkartları, kişisel verileri kaydetme

## 3. İçerikle ilgili suçlar

- Pornografi  $\rightarrow$  kullanımı ve satanması
- Çocuk Pornografisi
- Siber Propaganda  $\Rightarrow$  İstikbaldeki patlame  $\Rightarrow$  İnsanları galyana getirmesi
- Din karşıtı suçlar
- Siber kumar
- Hakaret ve yanlış bilgiler
- İstem dışı elektronik posta (Spam)

## 4. Telif hakları ile ilgili suçlar

### MCCONNELL SİBER SUÇ SINIFLANDIRMASI

- o Uluslararası platformda genel kabul gören McConnell International adlı ABD İnenşeli küresel politika ve teknoloji yönetimi danışmanlık firması tarafından yapılan sınıflandırmaya göre siber suçlar veri suçları, ağ suçları, erişim suçları ve ilgili suçlar şeklinde dört başlık altında incelemiştir (McConnell- International, 2000).  
 $\Rightarrow$  244 TCK
- o Veri suçları
  - Verilere müdahale edilmesi (Data Interception)
  - Verilerin değiştirilmesi (Data Modification)
  - Veri hırsızlığı (Data Theft)
- o Ağ suçları
  - Ağ engellemesi (Network Interference)
  - Ağ sabotajı (Network Sabotage)
- o Erişim suçları
  - Yetkisiz erişim (Unauthorized Access)
  - Virüs yayımı (Virus Dissemination)
- o İlgili Suçlar
  - Bilgisayarla İlgili Sahtekârlıklar
  - Bilgisayarla İlgili Dolandırıcılık



Bir ağıya kişi herin haber olayından gizlice girilmesi ve veriyi yönetmesi

243 Bilişim sisteme girmeye suçu yetkisiz iletisim durumu

### EGM - KAPSAMI

[HTTPS://WWW.EGM.GOV.TR/SİBER/SİBERSUCNEDİR](https://www.egm.gov.tr/siber/sibersucnedit)

#### 1. Siber Suç Nedir?

Her geçen gün teknolojinin ve bu teknolojilere erişilebilirliğin artmasına paralel olarak bilişim sistemlerine yönelik işlenen suçlar da artmaktadır. Siber Suç, bir bilişim sisteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlardır. Siber Suçu diğer suçlardan ayıran özelliği bir bilişim sistemi olmadan işlenememesidir. Bu suç türü bilgisayar ve internete özgü suçlar olarak da adlandırılabilir. Tüm suçların bilişim sistemleri kullanılarak işlenebileceği de bir gerçektir. Ancak böyle olması o eylemi siber suç yapmayacaktır. Siber Suçlar Sözleşmesi ve dairemiz görev alanı perspektifinde bakıldığından, siber suç bir bilişim sistemine izinsiz olarak ve hukuka aykırı olacak şekilde girilmesi ve sonrasında yapılan eylemdir. Bu suçta hedef bir kişi olabileceği gibi kişinin malvarlığı veya bir sistemin kendisi de olabilir. Örneğin, bir sisteme girerek, zarar verme, verileri silme, şifreleme, ele geçirme, veri ekleme, sistemin kullanımını engellemeye, özel hayatın gizliliğine müdahale etme, iletişimini engelleme, iletişimini izinsiz izleme ve kayıt etme gibi eylemler siber suç kategorisinde değerlendirilir.

## 1. Hacking?

Kısaca hacking diye tabir edilen eylem, bilişim sisteme yetkisiz ve izinsiz erişim olarak da adlandırılabilir. Bir bilişim sistemine hukuka aykırı olarak ve sahibinin bilgisi veya rızası dışında erişilmesi suçdur. Bir çok ülkede de olduğu gibi ülkemizde de suç olarak sayılmaktadır. Genelde bu suçla beraber bir çok hak ihlali de yapılmakta, başka suçların işlenmesi için bir kapı açmaktadır.

## 2. Verilere Yönelik Suçlar?

Yetkisiz ve hukuka aykırı erişimden sonra verilerin sistemdeki verilere eklenmesi, verilerin silinmesi, değiştirilmesi, şifrelenmesi, çalınması verilere erişimin engellenmesi, yeni veri eklenmesi, bu kapsamda değerlendirilir.

## 3. Bot-Net / D-Dos Saldırıları

Bir sistemin erişilmesini engellemek amacıyla yapılan saldırıdır. Daha önceden zararlı yazılım yüklenerek ele geçirilmiş ve BOT olarak tabir edilen bilgisayarlara komut vererek istenen web sitesine kısa sürede çok sayıda istek göndererek başka kullanıcıların ulaşmasının engellenmesi eylemdir. Aynı anda 10 kişinin geçebileceği bir market kapısına 10.000 kişinin yiğilması gibi bir benzetme yapılabilir. Genelde ticari amaçla yapılır ama siyasi ve terör amacı ile de yapıldığı görülmektedir. ~~DR → ÖSYM sınav sonucu tıpkı aynı anda sisteme girişmesi~~

## 4. Bilişim Sistemine Girme

Bir bilişim sisteminin bir kısmına veya tamamına girme suçudur. Burada veri silinmesi veya bedel karşılığı hizmet verilen sistemlere karşı yapılsa ayrıca artırıcı sebeptir. Türk Ceza Kanunu Madde 243 de düzenlenmiştir.

## 5. Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme

Bir sistemin her ne surette olursa olsun işleyişini engellemek, sisteme bulunan verileri bozmak, değiştirmek, başka yere göndermek, yok etmek ve benzeri eylemler suçtur.

Bu suç banka sistemleri üzerinde işlenirse cezayı artırıcı sebeptir. Türk Ceza Kanunu Madde 244 de düzenlenmiştir.

## 6. Haberleşmenin Gizliliğini İhlal

Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleştirilirse, bir yıldan üç yıla kadar hapis cezasına hükmün olunur. Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alener ~~ifşa~~ eden kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması halinde, ceza yarı oranda artırılır. Türk Ceza Kanunu Madde 132 de düzenlenmiştir.

## 7. Özel Hayatın Gizliliği

Özel hayatın gizliliğinin ihlal edilmesi suçtur. Bu suç işlenirken özel hayat ile ilgili ses ve görüntü alınması ile bu ses ve görüntülerin dağıtılması artırıcı sebeptir. Türk Ceza Kanunu Madde 134 de düzenlenmiştir.

## 8. Kişisel Verilerin Kaydedilmesi

Kişilerin siyasi, felsefi veya dini görüşlerine, ırkı kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydetmek ayrıca kişilere ait olan verilerin hukuka aykırı olarak ve rızası dışında kaydetmek de bu suç kapsamındadır. Türk Ceza Kanunu Madde 135 de düzenlenmiştir.

## 9. Nitelikli Hırsızlık

Temel olarak bir takım zararlı yazılımlar ile bir sistemdeki veya sistemler arasındaki trafik içinde aktarılan veri veya verilerin sahibinin rızası ve bilgisi dışında ele geçirilmesi suçudur. Örneğin, çevrimiçi online oynanan oyunlarda oyuncularının çalınması, banka hesabındaki mevduatın başka hesaplara EFT / havale edilmesi bu tip suçlardandır. Türk Ceza Kanunu Madde 142/2-e de düzenlenmiştir.

## 10. Nitelikli İnteraktif Dolandırıcılık

Bilişim sistemlerinin, banka ve kredi kurumlarının aracı olarak kullanılması suretiyle yapılan dolandırıcılık suçudur. Sahte e-postalar ile kullanıcıların bilgilerinin istenmesi, sahte sitelerle kullanıcıların bu sitelere bilgilerini girmesi suretiyle kişisel verilerin ele geçirilmesi ve bu verilerin kullanılarak menfaat temin edilmesidir. Türk Ceza Kanunu Madde 159/1-f de düzenlenmiştir.

#### 11. Banka ve Kredi Kartı suçları

Her ne surette olursa olsun bir kişiye ait olan banka veya kredi kartının bilgilerini kişinin bilgisi ve rızası dışında ele geçirmek / elinde bulundurmak, kullanmak / kullandırmak suçtur. Sahte yolla üretilen kartı kullanmak ağırlaştırıcı sebeptir. Şubemizde mail veya bilgilerinin ele geçirilmesi ile yapılan hırsızlıklar ve kart manyetik bilgisinin kopyalanması yolu ile yapılan hırsızlıklara karşı soruşturma yürütülmektedir. Türk Ceza Kanunu Madde 245 de düzenlenmiştir.

#### 12. Çocuk Pornografisi

Çocuk pornografisinden önce cinsel istismar konusuna kısaca değinecek olursak: Cinsel istismar, 15 yaşından küçük veya bu eylemin hukuki sorumluluğunu anlayamayacak akıl yapısında kişiye karşı cinsel yönden yapılan eylemlerdir. Bu suçta çocuğun vücutuna cinsel organ veya başka bir şey sokulması durumunda alt sınırı 8 yıldan başlayan hapis cezası öngörlür. Akrabalar tarafından, cebir ve şiddet ile veya sağlığı bozacak şekilde yapılması yine ağırlaştırıcı sebeplerdir. Türk Ceza Kanunu Madde 103 de düzenlenmiştir. 15 yaşını doldurmamış veya bunun hukuki anlamını anlayamayacak durumda olan kişilere karşı cinsel yönden istismar etmek suç olduğu gibi bunu kaydetmek, yayılmamak, saklamak, depolamak, ülkeye sokmak, satmak, ihraç etmek, başkalarının kullanımına sunmak veya bulundurmak da suçtur. Türk Ceza Kanununda alt sınırı 5 yıl hapis cezası öngörlülmüştür. Yayınlama işi basın yayın organları üzerinde yapıllırsa ağırlaştırıcı sebeptir. Türk Ceza Kanunu Madde 226 da düzenlenmiştir.

#### 13. Online Örgütü Kumar Siber Kumar

Kumar oynamaya yer ve imkan sağlamak suçtur. Burada yer kavramı gerçek yer olabileceği gibi yer sağlayıcılarında alınmış bir alan üzerinde sanal olarak sağlanmış bir yer de olabilir. Çocukların erişim sağlayabileceği şekilde bir yer sağlama faaliyeti ağırlaştırıcı sebeptir. Türk Ceza Kanunu Madde 228 de düzenlenmiştir.

#### SİBER SUÇLARIN İŞLENME ŞEKİLLERİ

- 1) Çöpe Dalma (Scavenging)  $\Rightarrow$  Telefonuz bozulduğu zaman gönderilen tamsıde verileri alınması.
- 2) Gizlice Dinleme (Eavesdropping)  $\Rightarrow$  Ağ dinleme
- 3) Veri Aldatmacası (Data Diddling)  $\Rightarrow$  Truva Atı (Troyan Horse)
- 5) Oltalama (Phishing)  $\Rightarrow$  bilinmeyen reklam ve linklere tıklanma
- 6) Süper Darbe (Super Zapping)
- 7) Salam Tekniği (Salami Techniques)
- 8) Gizli Kapılar (Trap Doors)
- 9) Eşzamansın Saldırıları (Asynchronous Attacks)
- 10) Ağ Solucanları (Network Worms)
- 11) Bilgisayar Virüsleri
- 12) Sırtlama (Piggybacking)
- 13) istem Dışı Alınan Elektronik İletiler (Spam)
- 14) Mantık Bombaları (Logic Bombs)
- 15) Yerine Geçme (Masquerading)  $\Rightarrow$  kurulum yapılmış : )
- 16) Kredi Kartı Sahtekârlıkları
- 17) Diğer : Tavşanlar, Bukalemun, Sahte İleti(Fake Mail), Yazılım Bombaları, Kurtlar, Bug Ware gibi yöntemlerde bilişim suçları işlenme şekilleri arasında sayılmaktadır.

## HACK - HACKER KAVRAMLARI

Bilgisayar

- Hack: bilgisayar sistemlerindeki zayıflıkları yada hataları kullanarak sistemi ele geçirmek
- Hacker: bilişim teknolojilerindeki bilgisini İYİ veya KÖTÜ olmak üzere bir sistemi ele geçirmek üzere kullanan kişi.

## HACKER ÇEŞİTLERİ

- Hacktivist:
  - Bu grupta yer alan Hackerlerin bir amacı ve ideolojisi vardır. Genel anlamda görüşleri "Bilgi herkesindir ve kamusal olmalıdır" içerisinde şekillenir. Kendilerine göre yanlış buldukları bir politik olayı veya toplumsal olayı düzeltmeye çalışırlar. Bu da genelde siteleri Hackleyip site üzerinde mesaj vererek yaparlar.
- Black Hat; (Siyah Şapkalılar) *Cadi, Kötü, zararlı*
  - Hacker türleri arasındaki en zararlı ve aynı zamanda en çok bilgi sahibi olanlardır.
  - Hedefleri her türlü bilgisayarı, sistemi, yazılımı, siteyi Hacklemektir ki bunu da çoğu zaman gerçekleştirirler.
  - Girdikleri sistemi bozabilirler, tüm bilgileri alabilirler ve bilgiler sayesinde maddi kazanç sağlayabilirler.
- White Hat; (Beyaz Şapkalılar) *Siber Güvenlik Uzmanları*
  - Zarar vermemeyi götmekler ama Siyah Şapkalılar kadar bilgilidirler.
  - Bazıları şirketlerde veya devlet kurumlarında çalışırlar. Amaçları Siyah Şapkalıları önlemek, verdikleri zararları gidermektir.
- Grey Hat; (Gri Şapkalılar) *Ortada kalmış, uşakçı* *⇒ Amacı para dir*
  - Bu kişiler arasında hem Beyaz hem de Siyah şapkalılar olabilir, daha doğrusu onların yaptıklarını yapabilirler. Bu yüzden iyi niyetli olup olmadıklarını anlayamayız.
  - Genelde sistem açıklarını bulup içeriye söyle bir bakarlar ancak "genelde" bilgi çalmazlar.
  - Sonrasında ise açığı para karşılığında sistem yöneticisine bildirirler veya bazen açıkları rakip sistemlere bildirirler.
- Cracker; (Yazılım Korsanları) *Sisteme indirilen crack uygulamalar*
  - Korsan oyunlar, yazılımları bunlar hazırlar. iyi görüp verilerini zi ve fotoğraflarını 22 de la birle.
  - Lisanlı yazılımların kodlarını baştan derleyebilirler veya hiç uğraşmadan aktivatör yaparlar.
  - Örneğin Windows 8'i tam sürüm yapma aracı gibi, veya Pes 2013'ün crack'ı gibi.
  - Yaptıkları yazılımların içine virüs veya botnet koyabilirler.
- Phreaker: *Braket suları altında yapılısa hackerlik degildir.*
  - Genelde hedeflerini çok büyük tutmazlar.
  - Telefon ağlarını, Uluslararası Ağları veya VoIP ağları hackerler ve bedava görüşme gibi birkaç iş yaparlar.
  - Veya konuşmalarınızı dinleyebilirler ve bilgileri satabilirler.
- Lamer; *İlgili yapılabilecek eylemler sosyal medya calismasi*
  - Bilişim konusunda çok fazla bilgiye sahip olmayıp internet üzerinden kendilerince e-posta/site hacklemeye çalışırlar. *⇒ Kötü ve iyİ*
- Script Kiddie; *⇒ Dolumsta tazelesin mesajlarını da doması sosyal mühendislik yapmas!*
  - Genellikle e-posta hesapları veya mesajlaşma verilerinin hırsızlığını yaparlar.
  - Çok fazla bilgi sahibi değildirler.
  - Hackerlığa özenen, ilgi duyan kişilerdir ancak kendilerini sürekli geliştirirler.
  - Araştırap bilgi edinirler ve edindikleri bilgileri zararlı amaçlar için kullanırlar.
- Yazılım Korsanları:
  - Bu tip korsanlar genellikle program, film gibi yazılım ve multimedya verilerini kopyalayarak para kazanırlar. *Kızılay korsan dvd, cd satılması*

## • ETİK HACKİNG $\Rightarrow$ 263 - 244 - 245 - 246

- Etik Hacking, bir ağdaki olası veri ihlallerini ve tehditlerini tanımlamak için sistem güvenliğinin izinli olarak kullanılmasıdır.
- Sistem veya ağın sahibi olan şirket sistemin savunmasını test etmek için siber güvenlik uzmanlarına bu tarz faaliyetler için izin verir.
- Bu sebeple, kötü niyetli hacking aksine bu süreç, planlı, onaylı ve çok daha önemlisi yasaldır.
- bilgisini sistem ve ağlarının güvenlik açıklarını ve veri ihlallerini önleyici çözümler geliştirme üzerine kullanan kişi
- etik hackerlar, sistem ya da networkün kötü niyetli hackerlar tarafından istismar edilebilecek zayıf noktalarını bulmaya çalışırlar.
- Sistem, network ve uygulamaların güvenliğini güçlendirecek yolları bulmak için bilgileri toplar ve analiz ederler. Bu çalışmalar ile güvenlik ayak izini geliştirmeyi ve böylelikle saldırılara karşı daha dayanıklı ve onları yönlendirecek kabiliyette olurlar.

## ETİK HACKERLARIN GÖREV VE SORUMLULUKLARI Siber Güvenlik Uzmanı

1. Etik hacker sistemin sahibi olan kuruluşun rızasını gözetmelidir. İzin
2. Herhangi bir güvenlik yoklaması gerçekleştirmeden önce tam bir onay almaları gereklidir. Onay
3. Yoklamaları gerçekleştirmeden önce planlanan işlemin çapından kurumu haberdar ederler. Saat vermedes bu Hafte Tc'de deorbit
4. Tespit ettikleri bütün açıkları ve ihlalleri bildirirler.
5. Elde edilen bilgiler gizli tutulmalıdır. Gizlilik
6. Amaçları, sistemi veya ağı güvence altına almak olduğu için, etik hackerlar gizlilik anlaşmalarını kabul etmeli ve onlara uymalıdır.
7. Herhangi bir güvenlik açığı olup olmadığını kontrol ettikten sonra yapılan hack işleminin tüm izleri silinmelidir. Böylece kötü niyetli hackerların bu ortaya çıkarılmış açıklardan sistem'e girmeleri engellenir.

## Dünya'nın en ünlü 10 Hacker'i

- Kevin Mitnick. Kevin Mitnick.
- Jonathan James. Jonathan James.
- Albert Gonzalez. Albert Gonzalez.
- Kevin Poulsen. Kevin Poulsen.
- Gary McKinnon. Gary McKinnon.
- Robert Tappan Morris. Robert Tappan Morris.
- Loyd Blankenship.
- Julian Assange. Julian Assange.

## Dünya Devlerine zəbā dərsi veren 3 Türk Hacker

- İbrahim Balic: Facebook Google, Google Play, Apple gibi dev şirketleri hackledi, ve birçok güvenlik açığını buldu
- İbrahim Yıldızlı: ABD savunma bakanlığı pentagonun düzenlediği siber yarışmaya katılarak yüzlerce kişiyi geçip, birinci oldu hem de tek başına. Ayrıca Amerikan vatandaşlığını reddetti Türkiye'ye hizmet etmeyi seçti
- İskorpitx: dünya hacker şampiyonu. Dünyada hacklemede birinci sırada. Microsoft gibi şirketleri hackleyerek ünlendi. Dünya birincisi.

## Dünyaca ünlü 8 Türk Hacker Grubu

- Ayyıldız Tim
- RedHack
- Cyber Warrior
- Skorsky
- Börteçine Siber Tim
- Türk Hack Team
- Anonymous Türkiye
- Türk Güvenliği

5237 sayılı TCK'nın 243. maddesinin metni şu şekildedir:

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

(2) Yukarıdaki fıkarda tanımlanan fiillerin bedeli karşılığı yararlanıla- bilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir. ~~Sistemde veriler alındıysa ekstra bir zarar var verilmeli değil, sade~~

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

#### Türk Ceza Kanunu 243

- Madde üç fıkradan oluşmaktadır.
  - Birinci fıkarda suçun temel şekli düzenlenirken; ikinci ve üçüncü fíralarda nitelikli hallerine yer verilmiştir.
  - Bu hallerden ilkinin gerçekleşmesi halinde faile suçun temel şekline nazaran daha az, ikincisinin gerçekleşmesi halinde ise daha fazla ceza verilmesi öngörülmüştür.
- İzinsiz* bilişim sisteme hukuka aykırı olarak girme ve orada kalmaya devam etmeyi suç olarak kabul etmektedir.
- bilişim sistemlerine yasadışı erişimin önlenmesiyle sistemi kullananların farklı türdeki menfaatleri korunmaktadır.
    - kullanıcıların özel hayatlarının gizliliğinin korunması,
    - özel hayatın dokunulmazlığı,
    - bireylerin haberleşme özgürlüklerinin de koruma alına alma,
    - kurumların ihtiyaç duyduğu güvenlik duygusu gibi farklı hukuki yararlardır
  - Bilişim sisteme girme suçu, failin hedef dosya ya da programlara izinsiz giriş yapması halinde ortaya çıkmaktadır.
  - Diğer bir deyle "girmek" kavramından, bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fizikten ya da uzaktan başka bir cihaz yoluyla erişilmesi anlaşılmaktadır.
  - "İzinsiz erişim" Avrupa Komisyonu tarafından da, bilgisayar sistemlerinin bir bölümüne ya da tümüne yapılan izinsiz erişimleri tanımlamak için kullanılmıştır. *Telefonunu ~~izinsiz~~ alıp şifreyi girdip ~~izinsiz~~ kariştırmaya*
  - Sisteme erişim yöntemi önemli değildir.
  - Ağ üzerinden sisteme girmek için birçok yöntem kullanılabilir; bir virus kullanarak 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 tanımlanır.

#### BİLİŞİM SİSTEMİNDE GİRME VE KALMA SUÇUYLA KORUNMAK İSTENEN HUKUKİ DEĞER

1. Toplum düzenini korumak
2. Özel hayatın gizliliği
3. Haberleşmenin gizliliği
4. Kullanıcı ve sistem sahibinin menfaatleri
5. Olası başka suçların işlenmesinin önlenmesi
6. Bilişim sisteminin güvenliği

*Bu hükümler değerleri kapsamıyorrsa suç değiş bir*

#### BİLİŞİM SİSTEMİNDE GİRME SUCUNUN MUHTELİF İSLENME ŞEKİLLERİ

- Konu : BİLİŞİM SİSTEMİNDE GİRME SUCU
- BÜŞRA ÖZÇELİK, YÜKSEK LİSANS TEZİ
- 2019 İSTANBUL ÜNİVERSİTESİ
- SOSYAL BİLİMLER ENSTİTÜSÜ
- KAMU HUKUKU ANABİLİM DALI
- Hedef bilişim sisteme doğrudan hiçbir araç ve yöntem kullanmadan manuel olarak erişilebileceği gibi, çeşitli yazılımlarla veya yöntem ya da tekniklerle işlenebilmesi mümkündür.
- Bu yöntemler mevcut açıklardan yararlanarak gerçekleştirilebileceği gibi, açık yaratarak veya bilinen şifre/parolaların kullanımıyla yetkisiz şekilde hesaplara ulaşarak da yapılabilir.
- Bilişim sisteme erişimde en sık kullanılan yöntemlerden biri "hacking" yani bilişim korsanlığıdır.

- bilişim korsanları, girmeyi amaçladıkları bilişim sisteminin DNS, IP bilgileri, port tarama, işletim sistemini bulma veya sistemdeki kodlama hataları, karmaşık sistemlerin yarattığı açık ve hatalardan faydalananma gibi işlemlerle hedef bilişim sisteminde yer alan eksiklik, açıklık veya zayıflıkları tespit ederek bilişim istemine sızabilir.
  - Bunun dışında bilişim korsanları, sahte e-postalar yoluyla bilişim sistemine ait verilere ulaşarak bilişim sistemlerine girebilir.
  - Sahte e-postada yer alan bağlantıların yönlendirdiği sayfalara girilen kullanıcı adı, şifre gibi önemli bilgilerin girilmesiyle veya üçüncü linklerin bilişim sistemine indirdiği zararlı yazılımlarla bilişim korsanları kolayca hedef bilişim sistemlerine erişebilmektedir.
  - Birtakım zararlı yazılımlarda da hedef bilişim sistemine erişim sağlanabilmektedir. Bunlardan biri hedef bilgisayardaki işlemleri kaydetmeye yarayan "tuş kaydedici (keylogger)" yöntemidir. *Bankamatiklerde*
  - Tuş kaydedici (keylogger) yöntemi donanımsal veya yazılımsal olarak gerçekleştirilebilir.
  - Donanımsal tuş kaydedici (keylogger) yönteminde hedef bilişim sistemine takılan bir cihaz bilişim sistemine girerek işlemleri kaydeder.
  - Yazılımsal tuş kaydedici (keylogger) ise bir trojan veya
  - rootkit'in parçası olarak bilişim sistemine yerlesir.
  - Trojan hedef bilgisayarın kullanıcısının bilişim sistemine yararlı bir yazılım gibi yerleşen, bilişim sisteminde yer alan bilgilere erişim sağlayan kötücul yazılımlardır.
  - Trojan aracılığıyla hedef bilişim sisteminde yer alan ekrana müdahale etme dâhil tüm özellikleri kontrol edebilme yetkisi bilişim korsanı tarafından gerçekleştirilebilir hale gelir. *Sıyah sapaklı korsanların yetkisi*
  - Sisteme erişim sağlayan bilişim korsanı çoğu zaman bilişim sisteminde kendisine kolayca erişim sağlama imkânı veren "backdoor" yani arka kapı kurar. *kendi kapınızı kendiniz açı yosunuz*
  - Böylece bilişim sistemine erişen bilişim korsanı yerini garantiyerek, bilişim sahibinin izni olmaksızın istediği zaman bilişim sistemine erişim sağlayabilir.
  - Backdoor, daha sonra hukuka aykırı olarak erişim sağlamak için bir program veya sisteme gizli şekilde eklenen kodlardır.
  - Bilişim korsanları bazen de bilişim sistemlerinde yer alan kodlama hataları ve dikkatsizliklerden faydalananarak uygulamalara yönelik komut saldıruları yapabilir.
  - Örneğin, "command injection" yani komut enjeksiyonu, bilişim korsanına bilişim sisteminde yer alan zayıflıklardan faydalananma yoluyla komut enjekte etmesini, böylece sizilen bilişim sisteminde bilişim korsanının dilediği komutu çalıştırmasını sağlar.
  - Rootkit ise bilişim sisteminin dosya ve işlemlerini gizleyerek manipüle eden yazılımlar olup, bilişim sistemi sahibinin bilişim sistemine erişildiğini anlamasını zorlaştırmakta ve tespit edilmesini engellemektedir.
  - Hedef sisteme trojan göndermek veya arka kapı bırakmak isteyen bilişim korsanı için rootkitler "can simidi" görevini üstlenmektedir.
  - Örneğin anti-virus programlarındaki basit bir taramayla ortaya çıkabilecek bir trojan türü, rootkitler yardımıyla görünmez hale gelir. *İçerden dışarı dışarı dan tane dosya gönderim yapılmamalı, hersey sistemin içinde olmalıdır*
  - Sosyal mühendislik, bilişim korsanlarının insanların doğal güvenme eğiliminin akılîcî manipüle edilmesi olarak tanımlanmaktadır.
  - Bilişim korsanının bu yolu kullanmadada amacı bilişim sistemine ve sistemde yer alan bilgilere yetkisiz erişim sağlamaktır. Bunun dışında haksız yarar sağlama veya sisteme zarar verme gibi amaçlar da söz konusu olabilir. Böylece bilişim sisteminde güvenlik açılarından faydalananmaksızın kişiler etkilendir, zorlanır veya aldatılır; bu kişilerin bilişim sistemine erişim sağlanır ve bu sayede bu kişilerin gizli bilgileri edinilmeye çalışılır.
  - En çok karşılaşılan sosyal mühendislik teknikleri
    - oltalama (phishing),
    - sahte senaryolar
    - uydurmak (pretexting),
    - tuzak donanım ve yazılımlar kullanmak (baiting),
    - bir menfaat karşılığı bilgilerin paylaşılması veya satılmasını sağlamaktır (quid pro quo)
- TÜK 243 dışarı gitme durumu*

- Verilerin korunması ile ilgili olarak Türk Ceza Hukuku'ndaki ilk düzenleme 765 sayılı TCK'nın ikinci kitabının mal aleyhine cürümler başlıklı onuncu babının on birinci faslında bilişim alanında suçlar başlığı ile (525/a), (525/b), (525/c) ve (525/d) maddelerinin eklenmesi ile yapılmıştır.
- Bu bölümde; "bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirmek" (525/a),
- "bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri kısmen veya tamamen tahrif etmek" (525/b),
- "sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sistemi tahrif etmek" (525/c), "suç konusu eylemleri gerçekleştirenlere ayrıca uygulanacak cezalar" (525/d) düzenlenmiştir.

#### SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME - MADDE 244

##### Sistemi engelleme, bozma, verileri yok etme veya değiştirme

**Madde 244-** (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) 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.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. *Devlet Kurumu*

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlı para cezasına hükmolunur.

#### SUÇUN UNSURLARI - TİPKİLGİN MADDİ UNSURLARI FİİL

- Hareketin şekli bakımından suçlar, icrai ve ihmali olarak ortaya çıkabilir.
  - Hareket bir şeyi yapmak veya yapmamak şeklinde olabilir.
  - Yapılması yasaklandığı halde bir hareket yapılmışsa buna, icrai hareket denir. Suçlar genellikle icrai hareketle işlenir.
  - Emredici hukuk kuralına aykırılık teşkil eden olumsuz davranış, ihmali suçu oluşturur. Ancak, ihmali suçlarda failin sadece hareketsiz kalması yeterli değildir, önemli olan suç tipinde belirlenmiş olan hareketin yapılmamış bulunmasıdır.
- Bilişim Sisteminin İşleyişini Engellemek
- Bilişim Sisteminin İşleyişini Bozma

#### BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİ ENGELLEMЕK

- Sözlükte engelleme, "istek, gereksinim veya bir davranışın belli bir sonuca ulaşmasının önlenmesi" anlamına gelmektedir.
- Yargıtay, sistemin işleyişinin engellenmesini, bilişim sisteminin verimli çalışmasının önlenmesi, icra ettiği faaliyet ve sahip olduğu kapasitesinin müdahale ile sınırlanması, yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesi olarak tanımlamaktadır.
- Sözlüğe göre bozma; "Bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek; Bir yerin, bir şeyin düzenini karıştırmak; Dokunmak, zarar vermek, Geçersiz bir duruma getirmek" anımlarına gelmektedir.
- Yargıtay, bozma eylemini bilişim sisteme dahil olan mekanik parçanın veya bir yazılım programının esasen yapması gereken özgülendiği işlevi yapamayacak hale getirilmesi ile birlikte sistemin engellenmesi halinin en üst noktası olan durma noktasından daha ileri olarak sistemin çökertilmesi, zarara uğratılması, işlemez hale getirilmesi, hatta, fiziki olarak dahi zarar verilmesi olarak tanımlamaktadır.

## SUÇUN NİTELİKLİ UNSURLARI

- Nitelikli unsurlar;
  - fiilin işleniş şekli,
  - zamanı,
  - yeri,
  - failin ve mağdurun vasfi,
  - fail ile mağdur arasındaki ilişki,
  - suçun konusu
  - fiilin işlenmesinde güdülen amaç" başlıklar altında incelenebilir.

Bir suç varsa bu soruların hepsi cevap verilmesi lazımdır.

## (1) SUÇUN BİR BANKA VEYA KREDİ KURUMUNA YA DA BİR KAMU KURUM VEYA KURULUŞUNA AİT BİLİŞİM SİSTEMİ ÜZERİNDE İŞLENMESİ (M. 244/3)

- 5411 sayılı Bankacılık Kanununun 157'nci maddesinde bu Kanuna tabi kuruluşların TCK'nın 244'üncü maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu açısından banka veya kredi kurumu olarak kabul edileceği düzenlenmiştir ancak, Bankacılık Kanununda kredi kurumuna ilişkin bir tanımlama yapılmamıştır.
- Kamu kurum ve kuruluşlarına ait bilişim sistemlerine yönelik suçların cezasının arttırılması, öncelikle genel ceza siyasetinden ve kamuya yönelik suçların daha vahim görülmüşinden kaynaklanmaktadır.
- Örneğin, sınav giriş başvurularının yapıldığı dönemde ÖSYM'ye ait sisteme erişimin engellenmesi ya da nüfus müdürlüklerine ya da vergi dairelerine ait sistemlerin bozulması durumunda kısa bir zaman dilimi içinde dahi çok sayıda kişi bu suçtan dolayı zarar görecektir.
- 3713 sayılı Terörle Mücadele Kanununun 4'üncü maddesinde "Aşağıdaki suçlar linci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır" denilmiş ve sayılı suçlar arasında bilişim alanında işlenen suçlara da yer verilmiştir. Buna göre bilişim sisteminin işlevisini engelleme veya bozma suçunun terör amacıyla işlenmesi halinde terör suçu sayılacaktır.

## BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİ ENGELLEME VEYA BOZMA SUÇU FİİL

- (1) Bilişim Sistemindeki Verileri Bozma
- (2) Bilişim Sistemindeki Verileri Yok Etme
- (3) Bilişim Sistemindeki Verileri Değiştirme
- (4) O Bilişim Sistemindeki Verileri Erişilmez Kılma
- (5) Bilişim Sistemine Veri Yerleştirme
- (6) Bilişim Sisteminde Var Olan Verileri Başka Bir Yere Gönderme

### (1) BİLİŞİM SİSTEMİNDEKİ VERİLERİ BOZMA

- Bozma eylemi sözlükte, "Bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek; Biçimini ve kullanılmasını değiştirmek..." şeklinde tanımlanmış olup
- TCK'nın 244/2'inci maddesi kapsamında, bilişim sisteminde yer alan bir verinin, yok edilmeden, ise yaramayacak ve kendisinden beklenilen faydayı sağlayamayacak duruma getirilmesini, verinin içeriğine veya yapısına müdahale etmek suretiyle verinin kısmen veya tamamen kullanılmaz hale getirilmesini ifade eder.
- Verinin bozulmasıyla yok edilmesi arasındaki fark ise şu şekildedir;
- veriye yönelik müdahale sonucunda verinin bozulması durumunda, bozuk da olsa bir veri bulunmaktadır, Ancak işlevini tamamen ya da kısmen yitirmiştir ve onarılma imkânı bulunmaktadır.
- Yok edilme halinde ise, veri sahibinin veriye ulaşması mümkün olmamaktadır.

## (2) BİLİŞİM SİSTEMİNDEKİ VERİLERİ YOK ETME

- Sözlükte yok etmek; "varlığına son vermek, ortadan kaldırmak" şeklinde tanımlanmıştır. Bilişim sisteminde yer alan verileri siber uzay kapsamında tamamen ortadan kaldırmak ya da varlığına son vermek mümkün değildir. Burada mantıksal bir yok oluş söz konusudur.
- Yok etmek sisteme fiziksel müdahale yoluyla yapılabileceği gibi sisteme bir bilişim ağı vasıtıyla bağlanmak suretiyle de gerçekleştirilebilecektir.

## (3) BİLİŞİM SİSTEMİNDEKİ VERİLERİ DEĞİŞTİRME

- Sözlükte "değiştirmek" kavramı, "Başka bir biçimde sokmak, değişikliğe uğratmak, başka bir duruma, başka bir görünümé getirmek." şeklinde tanımlanmaktadır.
- Akbuluña göre verilerin değiştirilmesi, kaydedilmiş verilerin başka bir bilgi içeriği almasını ifade etmektedir.
- Artuk/Gökçen/Yenidünya, değiştirmek hareketini "verilerin başka biçimlere sokulması, yeni içerik kazandırılması, niteliklerinin değiştirilmesi şeklinde veriler üzerinde yapılan manipülasyon" olarak tanımlamıştır.

## (4) BİLİŞİM SİSTEMİNDEKİ VERİLERİ ERİŞİLMEZ KILMA

- Sözlükte erişmek kavramı; "Varılması zamana, emege bağlı olan veya uzakta bulunan bir amaca varmak, ulaşmak, Bir yere ulaşmak, varmak" şeklinde tanımlanmıştır.
- Doktrinde bilişim sistemindeki verilerin erişilmez kılınması, "verinin içerdigi bilgi ya da enformasyona müdahale edilmeden, veriye olağan şekilde erişimin engellenmesi; verilerin malikinin ya da ilgilisinin istediği zaman istediği verilere ulaşmasının engellenmesi; verinin içerdigi bilgiye ve veriye dokunmadan, veriye ulaşım için gereken işlem bağıının koparılarak bilişim sistemi üzerinde hak sahibi olan kimsenin olağan şekilde veriye istediği zaman ulaşmasının engellenmesi" şeklinde tanımlanmıştır.

## (5) BİLİŞİM SİSTEMİNE VERİ YERLEŞTİRME

- Sözlükte yerleştirmek; "Yerleşmesini sağlamak, Yerine koymak" şeklinde tanımlanmıştır.
- Doktrinde ise bilişim sistemine veri yerleştirmek, "bilişim sistemindeki mevcut verilere dokunmadan, onlara herhangi bir zarar vermeden, değiştirmeden, bozmadan, yok etmeden, onlara erişimi engellemeden, bilişim sistemine ek olmak üzere önceden bulunmayan bazı verileri ilave etmek; sistemde yer alan verilere herhangi bir zarar vermeden, onlara ulaşma imkanını ortadan kaldırımadan sisteme veri eklemek fail tarafından bilişim sistemine ya da veri taşıma aracına dışarıdan ve sistemin maliki ya da ilgisinden izin alınmaksızın çeşitli verilerin sisteme kaydedilmesi, yüklenilmesi ya da eklenmesi" şeklinde tanımlanmıştır.

## (6) BİLİŞİM SİSTEMİNDE VAR OLAN VERİLERİ BAŞKA BİR YERE GÖNDERME

- Göndermek eylemi sözlükte "Bir yere doğru yola çıkarmak, yollamak, ulaşmasını, gitmesini sağlamak, Yetki vererek gitmesini sağlamak, Bir kaynaktan çıkışip gelmek, ulaşmak" şeklinde tanımlanmıştır.
- Bilişim sisteminde var olan verileri başka bir yere gönderme eylemi ise doktrinde; "failin, bilişim sisteminde bulunan bir veriyi, bilişim sistemi içinde bir yere veya başka bir bilişim sisteme göndemesi mağdura ait verilerin gerek mağdurun bilişim sisteminde farklı bir dosyaya gerekse de farklı bir bilişim sistemine gönderilmesi; bilişim sistemi içerisindeki verilerin başka bir bilişim sisteme ya da veri taşıma cihazına aktarılması, kaydedilmesi ya da kopyalanması" şeklinde tanımlanmıştır.

BANKA VEYA KREDİ KARTLARININ KÖTÜYE KULLANILMASI SUÇU ÜÇ FARKLI BİÇİMDE İŞLENEBİLİR:

MADDE 1 - Başkasına ait gerçek bir banka veya kredi kartının kötüye kullanılması (TCK md.245/1),

- Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlı para cezası ile cezalandırılır.<https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf>
- Maddede, bir bilişim sisteme bağlı olarak çalışan ve bilişim temelli bir faaliyetin sonucu olarak fonksiyon gösteren banka ve kredi kartlarıyla işlenen suçlar kastedilmektedir.

↑ internet üzerinden yapılan alışverişte kartın kopyalanması veya bilgilerinin alınması bu maddesi kapsıyor

MADDE 2 - Sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek (TCK md.245/2),

- o Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlı para cezası ile cezalandırılır. <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf>
- o İkinci fikrasında, gerçek bir kart veya kart numarasının sahtecilik yoluyla yeniden üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi eylemleri yaptırırmaya altına alınmıştır.

MADDE 3 Sahte bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak (TCK md.245/3).

- o Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlı para cezası ile cezalandırılır. <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf>
- o Üçüncü fikrasında ise sahte olarak üretilen yanı gerçek olmayan kart ile gerçek olduğu halde birtakım müdahaleler sonucu sahte hale getirilen kartın kullanılması sonucunda yarar sağlanması eylemi yapılmaya bağlanmıştır.

MADDE 4 Birinci fikarda yer alan suçun;

- o Haklarında ayrılık kararı verilmemiş eşlerden birinin,
- o Üstsoy veya altsoyunun veya bu derecede kayın hısimlarından birinin veya evlat edinen veya evlâtlığını,
- o Aynı konutta beraber yaşayan kardeşlerden birinin, zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolenmez. ⇒ Anne baba ketti ihlal oğlu  
Burda ceza huküm değil ihmâl yaptırımı olur

MADDE 5 (Ek: 6/12/2006 – 5560/11 md.) Birinci fikra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır. Pişmanlığı dersinden yaptırımlar Azaaltıyor. <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf>

YASAK CIHAZ VE PROGRAMLAR (TCK M. 245/A) Ekran kaydedici, sistem dinleneme yöntemleri vb.

- o Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adlı para cezası ile cezalandırılır. Bir şifreyi birkaç saatlik erken program çalı satmak, vermek, satmak
- o Madde metninde de anlaşılacığı üzere suç, seçimlik hareketli bir suçtur ve belirtilen hareketlerden birinin yapılması ile suç tamamlanır
- o Bu açıdan suçun oluşması için bir zararın meydana gelmesi beklenmediğinden, soyut tehlke suçudur.

Crack

## INTERNET ÜZERİNDEN HAKARET SUÇU SES VE GÖRÜNTÜNÜN KAYDA ALINMASI SUÇU

- o 5237 SAYILI TÜRK CEZA KANUNU'NDA HAKARET SUÇU

- TCK 125-131 MADDELERİNİ KAPSAR <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf>

### HAKARET SUÇU

- o Hakaret suçunun, 5237 sayılı Ceza Kanunu'ndaki düzenlendiği yere bakıldığında, şeref'e karşı suçlar başlığı altında yer aldığı görüyoruz.
- o Hakaret suçu, TCK'nın 125. maddesinde, 'Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden ya da yakıştırmalarda bulunmak veya söylemek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran.....' şeklinde düzenlenmiştir.

dil, ırk, idari...

Hakaret

Suçun işlenmesi için  
Madde 125- (1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden (...) 45 veya söylemek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Mağdurun guyabında hakarenin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilat ederek işlenmesi gereklidir.

Internet (2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde, yukarıdaki fikrada belirtilen cezaya hükmolunur.

(3) Hakaret suçunun;

- a) Kamu görevlisine karşı görevinden dolayı,
- b) Dini, siyasi, sosyal, felsefi inanç, düşünce ve kanaatlerini açıklamasından, değiştirmesinden, yaymaya çalışmasından, mensup olduğu dinin emir ve yasaklarına uygun davranışlarından dolayı,
- c) Kişinin mensup bulunduğu dine göre kutsal sayılan değerlerden bahisle, İşlenmesi halinde, cezanın alt sınırı bir yıldan az olamaz.

12 ay

(4) (Değişik: 29/6/2005 - 5377/15 md.) Hakarenin alenen işlenmesi halinde ceza altıda biri oranında artırılır.

(5) (Değişik: 29/6/2005 - 5377/15 md.) Kurul hâlinde çalışan kamu görevlilerine görevlerinden dolayı hakaret edilmesi hâlinde suç, kurulu oluşturan üyelere karşı işlenmiş sayılır. Ancak, bu durumda zincirleme suça ilişkin madde hükümleri uygulanır.

### Kişinin hatırlasına hakaret

Madde 130- (1) Bir kimsenin öldükten sonra hatırlasına en az üç kişiyle ihtilat ederek hakaret eden kişi, üç aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Ceza, hakarenin alenen işlenmesi halinde, altıda biri oranında artırılır.

(2) Bir ölünenin kısmen veya tamamen ceset veya kemiklerini alan veya ceset veya kemikler hakkında tahkir edici fiillerde bulunan kişi, üç aydan iki yıla kadar hapis cezası ile cezalandırılır. Mezarde ceset gelme mezar 22 ay verme

### INTERNET ÜZERİNDEN HAKARET SUÇU

- o TCK'nın 125. maddenin 2. fıkrasında, '..Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde..' huzurda işlenmiş sayılacağı düzenlenmiştir
- o Internet; iletişim aracı; ses, yazı ve görüntüyü de içerebilen çok yönlü iletişim aracı olmasından dolayı, internet yoluyla yapılan hakaret suçu, huzurda yapılmış sayılacaktır.
- o Anılan hükmün internet ve sosyal medyayı da kapsadığı ifade edilebilmektedir.

## SOSYAL MEDYA ÜZERİNDEN YAPILAN HAKARET SUÇUNUN UNSURLARI

- Sosyal medya aktörleri 5651 sayılı Kanun ve özel mevzuat kapsamında "icerik sağlayıcı", "yer sağlayıcı" veya "sosyal ağ (ortam) sağlayıcı" olarak, 6698 sayılı Kanun kapsamında "veri işleyen", "veri sahibi", "veri sorumlusu" olarak da tanımlamak mümkündür.
- Bu itibarla, Basın Kanunu'nda süreli yayınlar için ele alınan hususların internet ve sosyal medya için de yorumlanmasıının mümkün olduğu değerlendirilmektedir.

## SOSYAL MEDYA ÜZERİNDEN GERÇEKLEŞTİRİLEN HAKARET SUÇUNA İLİŞKİN DELİLLERİN TOPLANMASI VE DEĞERLENDİRİLMESİ

- Sosyal medya üzerinden icra edilen hakaret suçuna ilişkin deliller,
  - ekran görüntüsü,
  - URL adresi,
  - IP adresi, MAC adresi arka plana degişmez
  - trafik bilgilerinin (log kayıtlarının) tutulması ve saklanması olarak karşımıza çıkmaktadır.
  - Arka plan Kayıtları

## SOSYAL MEDYA ÜZERİNDEN GERÇEKLEŞTİRİLEN HAKARET SUÇUNA İLİŞKİN DELİLLERİN TOPLANMASI VE DEĞERLENDİRİLMESİ

- Elektronik deliller kolay zarar görebilen, değiştirilebilen ve yok edilebilen deliller olmaları nedeniyle yargılama sürecinde anılan delillerin doğruluğu yargılamanın objektif ve tarafsız olması bakımından oldukça önemlidir.
- Delillerin bilgisayar veya ekran çıktısı olarak hazır edilmesi halinde delil özelliği taşıyan şeyin çıktı değil, dijital ortamda verinin kendisi olması gerekmektedir.
- Delilin güvenilirliği oldukça önemli olup, güvenilirlik delilin miteber olup olmadığına, tarihe uygun olmasına ve nesnel olmasına bağlıdır.
- Örneğin, Twitter üzerinden işlenen hakaret içerikli mesajların şikayet dilekçesine siyah beyaz ekran çıktısı olarak eklenmesine ilişkin Yargıtay kararında;

"mesajların paylaşılıp paylaşılmadığının tespit edilmesi, mesajların varlığının tespit edilmesi halinde suça konu paylaşımın yapıldığı Twitter hesabının kime ait olduğunu tespiti için, sosyal paylaşım sitesinin yer sağlayıcısı olan şirketten, tespit edilen mesajın ne zaman ve hangi IP numarasından geldiğinin öğrenilmesi, daha sonra da tespit edilecek IP numarasının kime ait olduğu araştırılarak sonucuna göre sanıkların hukuki durumunun belirlenmesi gerekirken" bunların yapılmadığını ifade ederek, kararı bozma nedeni olarak sayılmıştır.

Karar metninden de çıkarılacağı gibi siyah beyaz ekran çıktısıyla iddianame düzenlenmesi, kamu davası açılması, mahkeme ekran görüntülerinin çıktısının gerçekliğini araştırmadan karar vermesi Yargıtay tarafından eksik olarak değerlendirilmiştir.

URL => link

- Hakaret suçunun konusu olan sosyal medya gönderisinin delillerinden biri de URL adresidir.
- "Uniform Resource Locator" (Tekdüzen Kaynak Bulucu) olarak nitelenen URL adresi, hakaret içeren paylaşımın adres kısmını oluşturmakta ve bir ispat aracı kullanılmaktadır.
- Bu çerçevede, dosyadaki URL adresi tıklandığında paylaşım silinmediyse tespiti mümkün olabilecek ve URL adresi delil niteliği taşıyabilecektir

- Hakaret suçunun ispatında kullanılan bir diğer delil de IP adresidir.
- IP adresi, internete bağlanmak isteyen bilgisayarlarla internet servis sağlayıcıları tarafından atanın kimlik numarasıdır.
- Örneğin, 155.212.56.73. Ancak nüfusun artması, teknolojinin ilerlemesi ve her türlü elektronik eşyanın internete girmesi için olmazsa olmaz olan IP adreslerin adedinde sıkıntısı yaşadığından IPv6 standarı üzerinde çalışılmaktadır.
- Anılan adres sosyal medya paylaşımının oluşturduğu yer, kullanıcının kimlik bilgileri ve adresini ilgili makamlara sağlamaktadır.
- Hakaret suçunu teşkil eden paylaşımın yapıldığı hesabin ait olduğu IP adresinin tespiti mahkemelerin hukuka uygun huküm kararı almalarına imkân vermektedir.
- Örneğin, bu durumun aksının yaşadığı bir karara ilişkin Yargıtay, sanığın Twitter adresinin kendisinin olmadığını ifade etmesi üzerine,
- "mesajın ne zaman ve hangi IP numarasından geldiğinin öğrenilmesi, daha sonra da tespit edilecek IP numarasının kime ait olduğu araştırılarak sonucuna göre sanığın hukuki durumunun belirlenmesi" gerektiği kararını vermiştir,
- Kararda devamlı, IP adresinin delil vasıtasıyla paylaşımın kime ait olduğu hususunun belirlenebileceği, anılan belirleme gerçekleştirilmeden verilen kararın kanuna aykırı olduğu ve kararın bozulması kararının alındığı kaydedilmiştir.

## LOG

- Log kayıtları, internetteki her hareketi kaydeden izler ya da günlük kayıtları olarak nitelenemektedir.
- Internet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik erişim kayıtlarını 3. maddesinin e fıkrasında,
  - "Kendi iç ağlarında dağıtılan IP adres bilgilerini,
  - kullanıma başlama ve bitiş zamanını ve bu IP adreslerini kullanan bilgisayarların tekil ağ cihaz numarasını (MAC adresi) gösteren bilgileri,
  - hedef IP adresi,
  - bir veya birden fazla IP adresinin portlar aracılığı ile kullanıcılara paylaştırılması yöntemi ile sunulan internet erişim hizmetinde kullanıcıya tahsis edilen gerçek IP ve port bilgileri" olarak ele almaktadır.
- Telekomünikasyon Kurumu Tarafından, Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik ise 3. maddesinin (f) fıkrasında, erişim sağlayıcısı trafik bilgi kavramını
  - "Internet ortamına erişime ilişkin olarak abonenin adı, adı ve soyadı, adresi, telefon numarası, abone başlangıç tarihi, abone iptal tarihi, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri" şeklinde nitelmiştir.
- Buna göre tarafların IP adresleri, port bilgileri, verilen hizmetin başlangıç ve bitiş saatleri, kullanılan hizmetin türü, aktarılan veri miktarı ve varsa abonenin kimlik bilgileri trafik bilgisi olarak alınır.
- 5651 Sayılı Kanun'un 5. Maddesine göre, barındırma sağlayıcısı içeriği kontrol etmek veya yasadışı faaliyetleri araştırmak zorunda değildir, ancak verilen hizmetlere ilişkin trafik bilgilerini en az 1 yıl ve en fazla 2 (iki yıl). Bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakta sorumludur.
- Elektronik Posta Aracılığıyla Gönderilen İçeriklerdeki Hakaret Suçları
- Facebook, Twitter ve Instagram Gibi Popüler Sosyal Medya Araclarında İşlenen Hakaret Suçları

7253 SAYILI KANUN Sensor Yasası

- 7253 sayılı "Internet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun", 31.07.2020 tarih ve 31202 sayılı resmi gazetede yayınlanarak yürürlüğe girdi.
- 5651 sayılı, "Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 2 da yapılan ilave düzenlemeleri içermektedir.
- 7253 sayılı sosyal medya düzenlemesi, "Sosyal Ağ Sağlayıcı" kavramını hayatımıza dahil etmiş olup, yürütme ve yürürlük maddesiyle birlikte toplama 9 maddeden oluşmaktadır.

## SOSYAL AĞ SAĞLAYICI KAVRAMI

- Kanun'a göre sosyal ağ sağlayıcı; sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses ve konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek veya tüzel kişileri ifade eder.
- Yani sosyal etkileşim amacı güden ve internet ortamında her türlü içeriğin oluşturulabilmesi, görüntülenebilmesi veya paylaşılabilmesine olanak sağlayan gerçek veya tüzel kişiler sosyal ağ sağlayıcılarıdır.
- Kanun'daki tanımdan yola çıkılarak değerlendirme yapıldığında; "sosyal etkileşim amacı bulunması"nın ve "kullanıcıların içerikleri oluşturmaları, görüntülemeleri veya paylaşması"nın sosyal ağ sağlayıcılığının unsurlarını oluşturduğu görülecektir.

## 7253 SAYILI YASA İLE GETİRİLEN DÜZENLEMELER TEMSİLCİ ATAMA YÜKÜMLÜLÜĞÜ

- 7253 Sayılı Kanun ile Sosyal Ağ Sağlayıcılaraya getirilen en önemli yükümlülüklerden biri "Temsilci Atama Yükümlülüğü 'dür.
- Günlük erişimi bir milyondan fazla olan yurtdışı kaynaklı Sosyal Ağ Sağlayıcı, Türkiye'de en az 1 gerçek veya tüzel kişiyi temsilci olarak atamakla yükümlüdür.
- Temsilcinin gerçek kişi olması hâlinde Türk Vatandası olma zorunluluğu mevcuttur (7253 Sayılı Kanun- md. 4/1)/
- Bu düzenleme sonucunda Türkiye'de günlük erişimi 1 milyondan fazla olan Facebook, Twitter ve Instagram gibi platformların Türkiye'de birer temsilcilerinin olması zorunlu hâle getirilmiştir.
- Aksi takdirde sosyal ağ sağlayıcılar iki aşamalı para cezasi, daha sonra reklam yasağı ve devamında iki aşamalı internet trafiği bant genişliğinin daraltılması olmak üzere toplamda beş aşamalı bir yaptırıım süreci düzenlenmiştir.

## BAŞVURULARA YANIT VERME YÜKÜMLÜLÜĞÜ

- Günlük erişimi bir milyondan fazla olan Sosyal Ağ Sağlayıcılara 5651 Sayılı Kanun'un 9.maddesinde yer alan kişilik haklarına ilişkin ve 9/A maddesinde yer alan özel hayatın gizliliğini ihlale ilişkin saldırısı olduğu gerekçesiyle yapılan başvurulara, 48 saat içinde olumlu yahut olumsuz (gerekçeli olarak) cevap verme yükümlülüğü getirilmiştir.
- Sosyal ağ sağlayıcının yurtdışı kaynaklı olması durumunda bu başvuru sosyal ağ sağlayıcının Türkiye temsilcисine yapılabilir.
- Temsilcinin bu başvuruya 48 saat içerisinde olumlu veya olumsuz cevap vermemesi halinde ise hak ihlaline sebep olan sosyal ağ sağlayıcısına 5 milyon TL idari para cezası verilecektir.
- Hukuka aykırılığı hâkim veya mahkeme karıyla tespit edilen içeriğin Sosyal ağ sağlayıcısına bildirilmesine rağmen 24 saat içerisinde içeriğin çıkarılmaması veya içeriğe erişimin engellenmemesi, halinde buradan doğacak zararın tazmini doğrudan sosyal ağ sağlayıcısından talep edilecektir.

## VERİLERİN TÜRKİYE'DE MUHAFAZA EDİLMESİ YÜKÜMLÜLÜĞÜ

- 7253 Sayılı Kanun'un 4/5 Ek maddesi ile birlikte Türkiye'den günlük erişimi 1 milyondan fazla olan yurt içi ve yurt dışı kaynaklı sosyal ağ sağlayıcılara Türkiye'deki kullanıcıların verilerini Türkiye'de muhafaza etme yükümlülüğü getirilmiştir.
- Bu yükümlülüğün yerine getirilmemesi halinde sosyal ağ sağlayıcıya uygulanacak yaptırıım hakkında ise Kanun'da hüküm bulunmamaktadır.

## RAPOR VERME YÜKÜMLÜLÜĞÜ

- 7253 Sayılı Kanun ile birlikte sosyal ağ sağlayıcı, kendisine bildirilen içeriğin çıkarılması veya erişimin engellenmesi kararlarının uygulanmasına ve kişiler tarafından yapılacak başvurularla ilişkin istatistiksel ve kategorik bilgileri içeren Türkçe hazırlanmış raporları 6 aylık periyotlarla Bilgi Teknolojileri ve İletişim Kurumu'na bildirmekle yükümlü kılınmıştır.
- Bu yükümlülüğünü yerine getirmeyen sosyal ağ sağlayıcıya ise 7253 Sayılı Kanun md.6/6 gereği on milyon Türk lirası idari para cezası Başkan tarafından verilir.

## ERİŞİMİN ENGELLENMESİ VEYA İÇERİĞİN ÇIKARILMASI YÜKÜMLÜLÜĞÜ

- Kanun'da mevcutta bulunan içeriğin engellenmesi tanımına ilave olarak yapılan düzenleme, "iceriğin kaldırılması" tanımını getirdi.
- Bu düzenleme ile Kanun'un 8. Maddesinde düzenlenen suçlar ve 9. Maddesinde belirtilen kişilik haklarını ihlal eden hallerde içeriğin çıkarılması mümkün ise artık erişimin engellenmesi yerine içeriğin çıkarılması yanı silinmesi kararının verilmesi imkânı sağlandı.

## UNUTULMA HAKKI UNUTULMA HAKKI;

- Avrupa Birliği ülkelerinde hukuki temellerde uygulama alanı bulan, Avrupa Birliği uygulamasında Avrupa Birliği Adalet Divanı'nın Google İspanya kararı ile yaygın ka ve ulkemizde de Anayasa Mahkemesi kararlarında ifadesini bulan, ülkemizde yasal düzenlenmesi olmamasına karşın Anayasa Mahkemesi kararlarında karsımıza çıkan bir kavramdır.
- Kisaca unutulma hakkı; kişi ve kurumların internette kendi adlarıyla arama yapıldığında derlenen sonuçlar arasında kendileriyle ilgili bilgi, fotoğraf, belge gibi verilere yer verilmemesini isteme hakkıdır.

## SES VE GÖRÜNTÜNÜN KAYDA ALINMASI SUÇU

243 - 244 - 245 - 246

- TCK 132 - Haberleşmenin gizliliğini ihlal
- TCK 133 - Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması
- TCK 134 - Özel hayatın gizliliğini ihlal
- TCK 135 - Kişisel verilerin kaydedilmesi
- TCK 136 - Verileri hukuka aykırı olarak verme veya ele geçirme
- TCK 226 - Müstehcenlik
- TCK 286 - Ses veya görüntülerin kayda alınması. Gibi bir çok maddeyi kapsar.

Ses veya görüntülerin kayda alınması

Madde 286- (1) Soruşturma ve kovuşturma işlemleri sırasında ses veya görüntüleri yetkisiz olarak kayda alan veya nakleden kişi, altı aya kadar hapis cezası ile cezalandırılır.

Klasik 7 soru geneli bilgi tabanlı 6. ve 7. Soru

Bir suç örneği verilmiş hikaye şeklinde o hikaye üzerinden TCK'da işlenen 10 maddeleri hangi yönyle, hangilerine hitapda bulunuyor.

Sınıflandırma suç şekillerinden 1 adet sorup hangi suç açısından gires ve hangi yönyle gires diye sormur.

