BLM5102 Bilgisayar Sistemleri ve Ağ Güvenliği

Prof. Dr. Hasan Hüseyin BALIK

(7. Hafta)

İçerik

- 2.Yönetim Sorunları
  - 2.1. BT Güvenlik Yönetimi ve Risk Değerlendirmesi
  - 2.2.BT Güvenlik Kontrolleri, Planları ve Prosedürleri
  - 2.3.Fiziksel ve Altyapı Güvenliği
  - 2.4. İnsan Kaynakları Güvenliği
  - 2.5. Güvenlik Denetimi
  - 2.6. Bilişim Güvenliğinde Yasal ve Etik Hususlar

2.6. Bilişim Güvenliğinde Yasal ve Etik Hususlar

2.6.İçerik

- Siber Suçlar ve Bilgisayar Suçları
- Fikri mülkiyet Hakları
- Mahremiyet
- Etik konular

Bilgisayar Suçu Türleri

- ABD Adalet Bakanlığı, bilgisayar suçlarını, bilgisayarın suç faaliyetlerinde oynadığı role göre sınıflandırır:

Hedef olarak bilgisayarlar

Veri bütünlüğüne, sistem bütünlüğüne, veri gizliliğine, mahremiyete veya kullanılabilirliğine yönelik bir saldırı içerir

Depolama aygıtı olarak bilgisayarlar

Çalınan parola listelerini, kredi kartı veya arama kartı numaralarını, özel şirket bilgilerini, pornografik görüntü dosyalarını veya korsan ticari yazılımları depolamak için bilgisayarı kullanma

İletişim araçları olarak bilgisayarlar

Dolandırıcılık, kumar, çocuk pornografisi ve reçeteli ilaçların, kontrollü maddelerin, alkolün veya silahların yasa dışı satışı gibi çevrimiçi işlenen suçlar

Bilgisayar Suçu Türleri

- Türk Ceza Kanunu açısından Siber Suçlar:
  - Bilişim sistemine girme suçu (TCK m.243)
  - Sistemi Engelleme, Bozma, Erişilmez Kılma, Verileri Yok Etme veya Değiştirme Suçu (TCK m.244)
  - Banka veya kredi kartının kötüye kullanılması suçu (TCK m.245)
  - Yasak cihaz veya porgram kullanma suçu (TCK m.245/a)
  - Müstehcenlik Suçu (TCK m.226)

Siber Suçlar Sözleşmesi*'nde Bahsedilen Siber Suçlar (1/2)

Madde 2: Yasadışı erişim	Bir bilgisayar sisteminin tamamına veya herhangi bir kısmına hak olmaksızın erişimdir.
Madde 3: Yasadışı durdurma	Bu tür bilgisayar verilerini taşıyan bir bilgisayar sisteminden elektromanyetik emisyonlar da dahil olmak üzere, bilgisayar verilerinin bir bilgisayar sistemine, sistemden veya bilgisayar sistemi içinde kamuya açık olmayan aktarımlarının teknik yollarla haksız olarak kesilmesidir.
Madde 4: Veriye müdahale	Bilgisayar verilerinin haksız yere zarar görmesi, silinmesi, bozulması, değiştirilmesi veya gizlenmesidir.
Madde 5: Sisteme müdahale	Bilgisayar verilerini girerek, ileterek, zarar vererek, silerek, bozarak, değiştirerek veya gizleyerek bir bilgisayar sisteminin işleyişinin hak olmaksızın ciddi şekilde engellenmesidir.
Madde 7: Bilgisayarla ilgili sahtecilik	Bilgisayar verilerinin girilmesi, değiştirilmesi, silinmesi veya gizlenmesi, verilerin doğrudan okunabilir ve anlaşılır olup olmadığına bakılmaksızın, yasal amaçlar doğrultusunda gerçekmiş gibi değerlendirilmesi veya üzerinde işlem yapılması amacıyla gerçek olmayan verilerle sonuçlanmasıdır

*Avrupa Konseyi tarafından geliştirilmiş ve Amerika Birleşik Devletleri dahil 43 ülke tarafından onaylanmıştır.

Siber Suçlar Sözleşmesi*'nde Bahsedilen Siber Suçlar (2/2)

Madde 6: Cihazların kötüye kullanımı	a. Aşağıdakilerin üretimi, satışı, kullanım için tedariki, ithalatı, dağıtımı veya başka bir şekilde kullanıma sunulması: i. Öncelikle yukarıdaki 2 ila 5. Maddeler uyarınca belirlenen suçlardan herhangi birini işlemek amacıyla tasarlanmış veya uyarlanmış bir bilgisayar programı da dahil olmak üzere bir cihaz; ii. Yukarıdaki 2 ila 5. maddelerde düzenlenen suçlardan herhangi birinin işlenmesi amacıyla kullanılmak üzere bir bilgisayar sisteminin tamamına veya herhangi bir kısmına erişilebilen bir bilgisayar şifresi, erişim kodu veya benzeri veriler; ve b. Yukarıdaki a.i veya ii paragraflarında atıfta bulunulan bir eşyanın, yukarıdaki 2 ila 5. Maddelerde belirlenen suçlardan herhangi birinin işlenmesi amacıyla kullanılması niyetiyle bulundurulması. Taraflardan biri, yasa gereği, cezai sorumluluk yüklenmeden önce bu türden bir dizi eşyanın bulundurulmasını talep edebilir.
Madde 8: Bilgisayarla ilgili dolandırıcılık	Başka bir kişinin malını aşağıdaki nedenlerle kaybetmesine neden olmak: a. Bilgisayar verilerinin herhangi bir girişi, değiştirilmesi, silinmesi veya gizlenmesi; b. Bir bilgisayar sisteminin işleyişine, hileli veya dürüst olmayan bir şekilde, kendisi veya bir başkası için ekonomik bir fayda sağlamak amacıyla herhangi bir müdahale.
Madde 9: Çocuk pornografisi ile ilgili suçlar	a. Bir bilgisayar sistemi aracılığıyla dağıtmak amacıyla çocuk pornografisi üretmek; b. Bir bilgisayar sistemi aracılığıyla çocuk pornografisi sunmak veya sağlamak; c. Çocuk pornografisini bir bilgisayar sistemi aracılığıyla dağıtmak veya iletmek; d. Kendisi veya başkası adına bilgisayar sistemi aracılığıyla çocuk pornografisi temin etmek; ve e. Bir bilgisayar sisteminde veya bilgisayar veri depolama ortamında çocuk pornografisi bulundurmak.
Madde 11: Teşebbüs ve yardım veya yataklık	Bu Sözleşmenin yukarıdaki 2 ila 10. Maddeleri uyarınca belirlenen suçlardan herhangi birinin işlenmesine, bu tür bir suçun işlenmesi niyetiyle yardım veya yataklık etmek. Bu Sözleşmenin 3 ila 5, 7, 8 ve 9.1.a ve c maddelerinde belirtilen suçlardan herhangi birini işlemeye teşebbüs.

CERT 2007 E-Suç İzleme Anketi Sonuçları

	İşlenen (net) %	İçeriden %	Dışarıdan %	Belirsiz %
Virüs, solucanlar veya diğer kötü amaçlı kodlar	74	18	46	26
Bilgilere, sistemlere veya ağlara yetkisiz erişim/kullanım	55	25	30	10
Yasadışı spam e-posta üretimi	53	6	38	17
Casus yazılım (reklam yazılımı hariç)	52	13	33	18
Hizmet reddi saldırıları	49	9	32	14
Dolandırıcılık (kredi kartı dolandırıcılığı vb.)	46	19	28	5
Oltalama-Kimlik avı (abonelerinizden veya çalışanlarınızdan kişisel veriler elde etmek amacıyla çevrimiçi şirketiniz gibi davranan biri)	46	5	35	12
Müşteri kayıtları, mali kayıtlar vb. dahil olmak üzere diğer (özel) bilgilerin çalınması	40	23	16	6
Fikri mülkiyet hırsızlığı	35	24	12	6
Özel veya hassas bilgilerin kasıtlı olarak ifşa edilmesi	35	17	12	9
Müşterinin kimlik hırsızlığı	33	13	19	6
Sabotaj: bilgi, sistem veya ağların kasıtlı olarak bozulması, silinmesi veya yok edilmesi	30	14	14	6
Kuruluşun ağındaki zombi makineler/botlar/ağın BotNets tarafından kullanımı	30	6	19	10
Web sitesi tahrifatı	24	4	14	7
Gasp	16	5	9	4
Diğer	17	6	8	7

Yasa Uygulama Zorlukları

- Kolluk kuvvetlerinin bilgisayar ve ağ saldırıları üzerindeki caydırıcı etkisi, cezai tutuklama ve kovuşturmanın başarı oranıyla ilişkilidir.
- Kolluk kuvvetlerinin zorlukları:
  - Bu tür suçlarla mücadele konusunda bilgili ve deneyimli personelin eksikliği
  - Yeterli teknoloji bütçelerinin eksikliği
  - Siber suçun küresel doğası
  - Uzak kolluk kuvvetleriyle işbirliği ve eşgüdüm eksikliği
- Siber Suçlar Sözleşmesi, suçlar için ortak bir terminoloji ve yasaların küresel olarak uyumlu hale getirilmesi için bir çerçeve sunmaktadır.

Siber suçlular

Adalete teslim etmedeki başarısızlık, sayılarının, cesaretlerinin ve operasyonlarının küresel ölçeğinin artmasına yol açtı.

Profil oluşturmak zordur

Genç ve çok bilgisayar meraklısı olma eğilimindedir

Davranışsal özelliklerin aralığı geniştir

Muhtemel şüphelilere işaret edebilecek hiçbir siber suçlu veri tabanı mevcut değildir

Siber Suç Kurbanları

Siber suçluların başarısından ve kolluk kuvvetlerinin başarısızlığından etkilenirler

Bu kuruluşların çoğu, saldırıları önlemek için teknik, fiziksel ve insan faktörü kaynaklarına yeterince yatırım yapmamıştır

Kolluk kuvvetlerine güven eksikliği, kurumsal itibarla ilgili endişeler ve hukuki sorumlulukla ilgili endişeler nedeniyle ihbar oranları düşük olma eğilimindedir

Kolluk Kuvvetleri ile Çalışma

- Üst düzey yönetim ve güvenlik yöneticileri, yasa uygulamalarını bir kaynak ve araç olarak görmelidir.
- Yönetim şunları yapmalıdır:
  - Adli soruşturma sürecini anlamalı
  - Araştırmacıların ihtiyaç duyduğu girdileri anlamalı
  - Mağdurun soruşturmaya nasıl olumlu katkı sağlayabileceğini anlamalıdır.

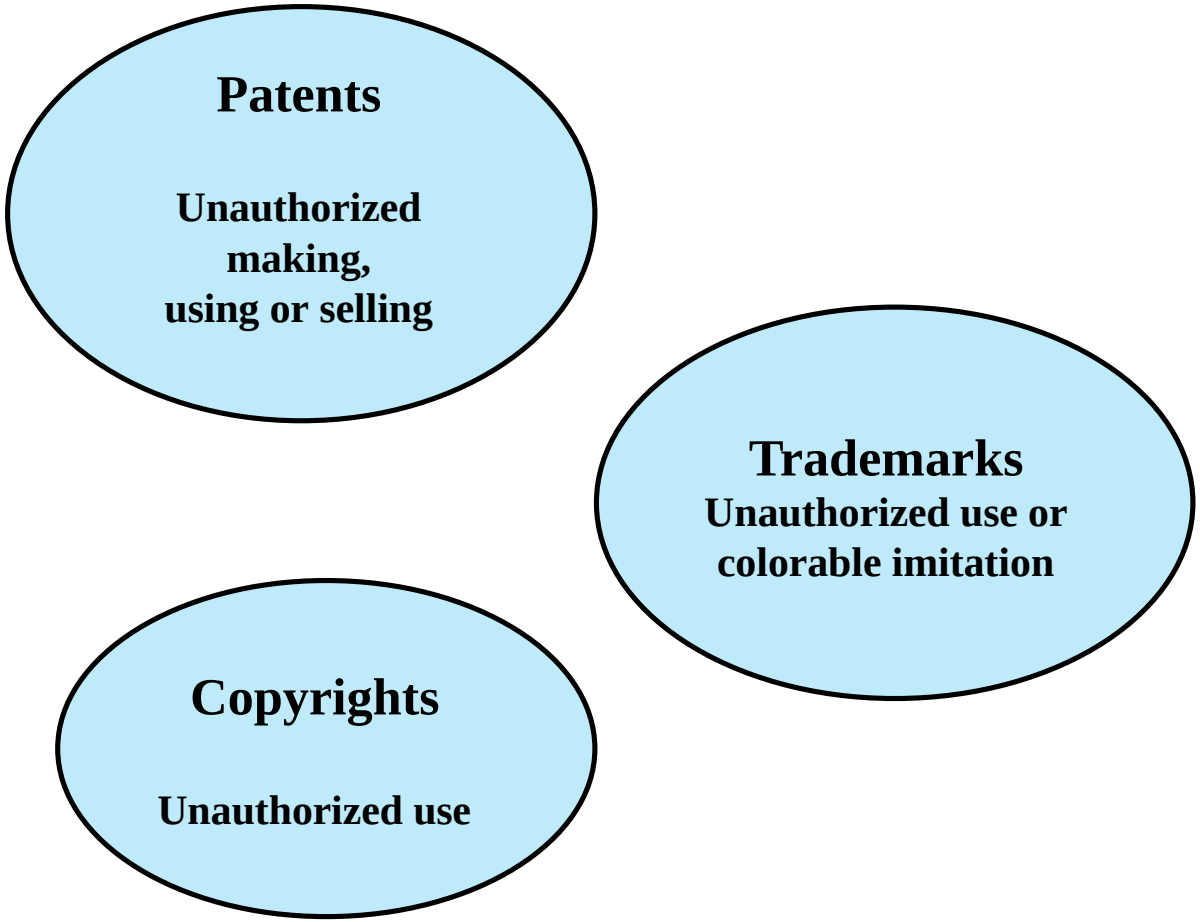


Figure 19.1 Intellectual Property Infringement

Telif hakkı (Copyright)

- Bir fikrin somut veya sabit ifadesini korur ancak fikrin kendisini korumaz
- Yaratıcı, aşağıdaki durumlarda telif hakkını talep edebilir ve ulusal bir devlet telif hakkı ofisinde dosyalayabilir:
  - Önerilen çalışma orijinaldir
  - Yaratıcı, orijinal fikri somut bir forma sokmuştr

Copyright Hakları

- Telif hakkı sahibi, ihlale karşı korunan bu münhasır haklara sahiptir:
  - Çoğaltma hakkı
  - Değişiklik hakkı
  - Dağıtım hakkı
  - Herkese açık gösteri hakkı
  - Herkese açık görüntüleme hakkı
- Örnekler şunları içerir:
  - Edebi çalışmalar
  - Müzikal eserler
  - Dramatik eserler
  - Pandomimler ve koreografik eserler
  - Resim, grafik ve heykel çalışmaları
  - Hareketli resimler ve diğer görsel-işitsel eserler
  - Ses kayıtları
  - Mimari işler
  - Yazılımla ilgili işler

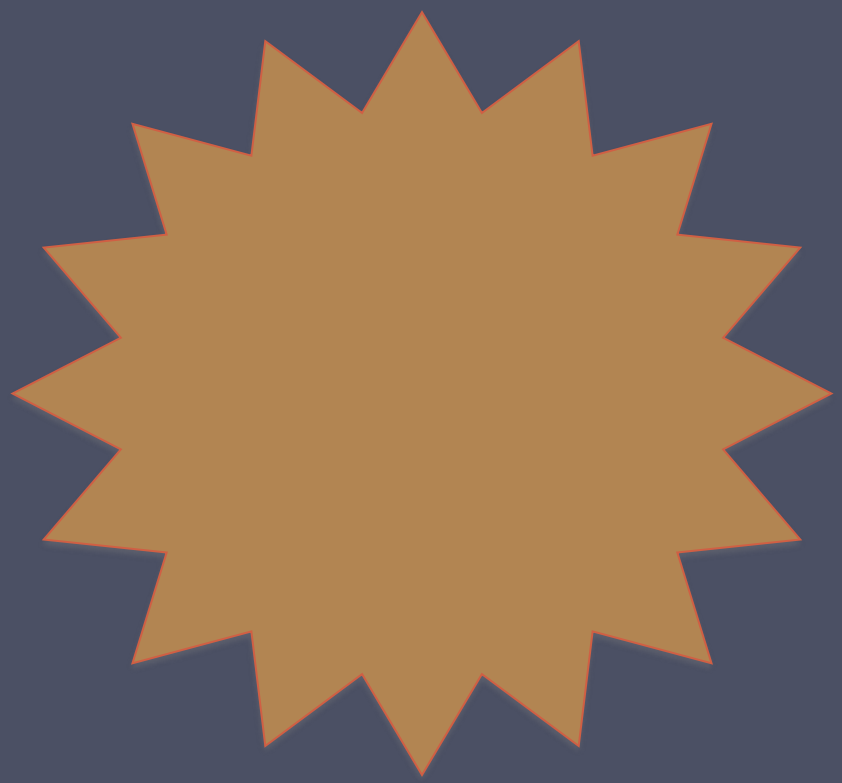
Patent

- Mucide bir mülkiyet hakkı verir
- "Başkalarının buluşu Amerika Birleşik Devletleri'nde yapmasını, kullanmasını, satışa sunmasını veya satmasını" veya buluşu Amerika Birleşik Devletleri'ne "ithal etmesini" engelleme hakkı
- Türler:

Fayda	Tasarım	Bitki
• Herhangi bir yeni ve kullanışlı süreç, makine, imalat ürünü veya madde bileşimi	• Bir üretim ürünü için yeni, orijinal ve süslü tasarım	• Herhangi bir farklı ve yeni bitki çeşidini keşfeder ve eşeysiz olarak yeniden üretme

Marka

- Bir kelime, isim, sembol veya cihaz
- Mal ticaretinde kullanılır
- Malların kaynağını gösterir
- Onları başkalarının mallarından ayırır
- Ticari marka (Trademark) hakları şu amaçlarla kullanılabilir:
  - Başkalarının kafa karıştıracak kadar benzer bir işaret kullanmasını önler
  - Ancak başkalarının aynı malları üretmesini veya aynı mal veya hizmetleri açıkça farklı bir marka altında satmasını engellemez



Ağ ve Bilgisayar Güvenliği ile İlgili Fikri Mülkiyet

- Ağ ve bilgisayar güvenliği bağlamında ilgili bir dizi fikri mülkiyet biçimi vardır.
- En öne çıkanlardan bazılarına örnekler:

Yazılım	Veritabanı	Dijital içerik	Algoritmalar
• Ticari yazılım satıcıları tarafından üretilen programlar • Paylaşılan yazılım • Dahili kullanım için bir kuruluş tarafından oluşturulan tescilli yazılım • Kişiler tarafından üretilen yazılımlar	• Potansiyel ticari değere sahip olacak şekilde toplanan ve düzenlenen veriler	• Ses ve video dosyalarını, multimedya eğitim yazılımını, Web sitesi içeriğini ve diğer tüm orijinal dijital çalışmaları içerir	• Patentlenebilir bir algoritma örneği, RSA açık anahtarlı şifreleme sistemidir

ABD Dijital Milenyum Telif Hakkı Yasası (DMCA)

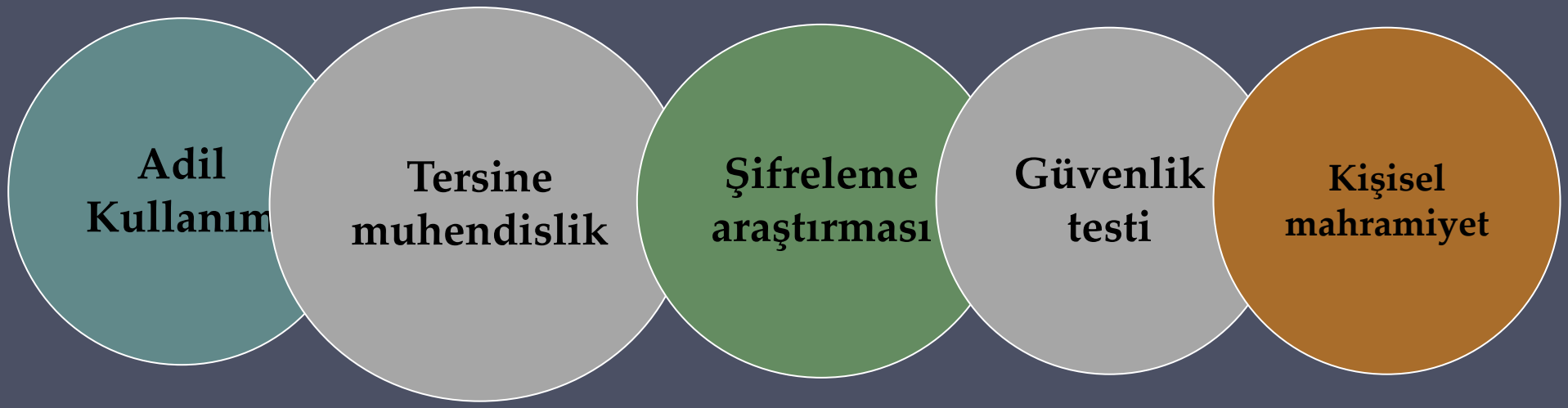
- 1998'de kanunlaştı
- Dijital telif hakkıyla korunan materyallerin korumasını güçlendirmek için WIPO (Dünya Fikri Mülkiyet Örgütü) anlaşmalarını uygular
- Telif hakkı sahiplerini, telif hakkıyla korunan eserlerini korumak için teknolojik önlemler almaya teşvik eder
  - Esere erişimi engelleyen tedbirler
  - Eserin kopyalanmasını önleyici tedbirler
- Önlemleri atlama girişimlerini yasaklar
  - Engelleme girişimlerine hem cezai hem de hukuki yaptırımlar uygulanır.

Dijital Ortamda Telif Haklarını Korumak İçin Başvurulabilecek Yöntemler

- Hukuk Davaları
  - Tecavüzün Kaldırılması (Ref'i) Davası
  - Tecavüzün Durdurulması (Men'i) Davası
  - Maddi ve Manevi Tazminat Davaları
- Ceza Davaları:
  - Bir eseri hak sahibi kişilerin yazılı izni olmaksızın işleyen, değiştiren, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan kişi hakkında bir yıldan beş yıla kadar hapis ve adli para cezasına hükmolunur.

DMCA Muafiyetleri

- Belirli eylemler, DMCA hükümlerinden ve aşağıdakiler dahil diğer telif hakkı yasalarından muaftır:



- DMCA'nın meşru güvenlik ve şifreleme araştırmalarını engellediğine dair önemli endişeler mevcuttur.
  - İnovasyonun ve akademik özgürlüğün bastırıldığını ve açık kaynaklı yazılım geliştirmenin tehdit altında olduğunu hissettirir

Dijital Haklar Yönetimi (DRM)

- Dijital hak sahiplerinin açıkça tanımlanmasını ve çalışmaları için öngörülen ödemeyi almasını sağlayan sistem ve prosedürlerdir.
  - Baskıyı engellemek veya daha fazla dağıtımı yasaklamak gibi başka kısıtlamalar getirebilir
- Tek bir DRM standardı veya mimarisi yok
- Amaç, eksiksiz içerik yönetimi yaşam döngüsü için mekanizmalar sağlamaktır
- Çeşitli dijital içerik türleri/platformları/ortamları için kalıcı içerik koruması sağlar

Mahremiyet

- Bilgisayar güvenliği ile örtüşür
- Toplanan ve saklanan bilgi ölçeğinde çarpıcı artış
  - Kolluk kuvvetleri, ulusal güvenlik, ekonomik teşvikler tarafından motive edilmiştir
- Bireyler, kişisel bilgilere ve yaşamlarıyla ilgili özel ayrıntılara erişim ve bunların kullanımı konusunda giderek daha fazla bilinçlenmeye başlamıştır.
- Mahremiyetten taviz vermenin boyutuyla ilgili endişeler, mahremiyet haklarının güçlendirilmesine yönelik çeşitli yasal ve teknik yaklaşımlara yol açmıştır.

Avrupa Birliği (AB) Veri Koruma Direktifi

- 1998'de kabul edildi:
  - Kişisel bilgileri işlerken üye devletlerin temel gizlilik haklarını koruduğundan emin olunmasını sağlar
  - Üye devletlerin kişisel bilgilerin AB içinde serbest akışını kısıtlamasını önler
- Aşağıdaki ilkeler etrafında örgütlenmiştir:

Fark etme	Razı olma	Tutarlılık	Erişim
Güvenlik	İleri transfer	Uygulama	

Amerika Birleşik Devletleri Gizlilik Girişimleri

1974 Gizlilik Yasası

- Federal kurumlar tarafından toplanan ve kullanılan kişisel bilgilerle ilgili işlemler
- Bireylerin tutulan kayıtları belirlemesine izin verir
- Bireylerin kayıtların başka amaçlar için kullanılmasını yasaklamasına izin verir
- Bireylerin kayıtlara erişmesine ve kayıtları uygun şekilde düzeltmesine ve değiştirmesine izin verir
- Ajansların kişisel bilgileri uygun şekilde toplamasını, muhafaza etmesini ve kullanmasını sağlar
- Bireyler için özel bir dava hakkı oluşturur

Türkiye'de Gizlilik Girişimleri

2016 tarihli 6698 KVKK

- Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenler
- Özel ve Genel Kişisel verilerin işlenme şartları belirler
- Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi ile ilgili hususları belirler
- Kişisel verilerin aktarılması veya yurt dışına aktarılması belirler
- Veri sorumlusunun aydınlatma yükümlülüğünü tanımlar
- Veri sahibinin haklarını belirler
- Veri güvenliğine ilişkin yükümlülükleri tanımlar
- Başvuru, Şikâyet ve Veri Sorumluları ile alakalı hususları belirler

ISO 27002 belirtir. . .

“Bir kuruluşun kişisel olarak tanımlanabilir bilgilerin gizliliği ve korunmasına yönelik veri politikası geliştirilmeli ve uygulanmalıdır. Bu politika, kişisel olarak tanımlanabilir bilgilerin işlenmesine dahil olan tüm kişilere iletilmelidir. Kişilerin mahremiyetinin ve kişisel olarak tanımlanabilir bilgilerin korunmasına ilişkin bu politikaya ve ilgili tüm mevzuat ve düzenlemelere uyum, uygun yönetim yapısı ve kontrolü gerektirir. Genellikle bu en iyi şekilde, yöneticilere, kullanıcılara ve hizmet sağlayıcılara bireysel sorumlulukları ve izlenmesi gereken özel prosedürler konusunda rehberlik etmesi gereken bir gizlilik görevlisi gibi bir sorumlu kişinin atanmasıyla elde edilir. Kişisel olarak tanımlanabilir bilgilerin işlenmesi ve gizlilik ilkeleri konusunda farkındalığın sağlanması sorumluluğu ilgili mevzuat ve düzenlemelere uygun olarak ele alınmalıdır. Kişisel olarak tanımlanabilir bilgileri korumak için uygun teknik ve organizasyonel önlemler uygulanmalıdır.”

Gizlilik ve Veri Gözetimi

- Büyük şirketlerin, hükümetin ve kolluk kuvvetlerinin talepleri, kişisel mahremiyete yönelik yeni tehditler yaratmıştır.
  - Analiz için bilimsel ve tıbbi araştırma verilerinin toplanması
  - Kolluk kuvvetleri veri gözetimi
  - Özel kuruluşlar profil oluşturma
  - Bu, bilimsel araştırma, halk sağlığı, ulusal güvenlik, kolluk kuvvetleri ve kaynakların verimli kullanımı gibi alanlarda faydalı sonuçlara olanak sağlarken, bireyin mahremiyet hakkına saygı duymaya devam etme arasında gerilim yaratır.
- Özellikle endişe duyulan bir diğer alan da, halka açık sosyal medya sitelerinin kullanımındaki hızlı artıştır.
  - Bu siteler, bireyler ve onların diğer bireyler ve kuruluşlarla etkileşimleri hakkında büyük miktarda veri toplar, analiz eder ve paylaşır.
  - Birçok kişi, fotoğraflar ve durum güncellemeleri de dahil olmak üzere büyük miktarda kişisel bilgiyi isteyerek yükler.
  - Bu veriler potansiyel olarak mevcut ve gelecekteki işverenler, sigorta şirketleri, özel dedektifler ve diğerleri tarafından bireyle olan etkileşimlerinde kullanılabilir.

Gizliliğin koruması

- Gizliliği korumak için hem politika hem de teknik yaklaşımlar gereklidir
- Teknik yaklaşımlar açısından, veri tabanı güvenliği için geliştirilen teknik mekanizmalar kullanılarak bilgi sistemlerinde depolanan verilerin gizliliğinin korunması gereklilikleri kısmen ele alınabilir.
- Sosyal medya siteleriyle ilgili olarak teknik kontroller şunları içerir:
    - Bireylere ilişkin verileri kimlerin görüntüleyebileceğini yönetmek için uygun gizlilik ayarlarının sağlanması
    - Bir kişiye referans verildiğinde veya başka bir kişinin içeriğinde etiketlendiğinde bildirim
    - Sosyal medya siteleri bu kontrollerin bir kısmını içerse de sürekli değişiyor ve bu mekanizmalara ayak uydurmaya çalışan kullanıcılar için hayal kırıklığı yaratıyor.
- Büyük veri analizinde mahremiyet endişelerini yönetmek için başka bir yaklaşım, analiz için araştırmacılara veya diğer kuruluşlara verilmeden önce verileri anonimleştirmek, kişisel olarak tanımlayıcı bilgileri kaldırmaktır.

Veri gizliliği

- Politika açısından, gizliliği korumak için uygun kısıtlamaların uygulanmasını sağlayarak büyük verilerin kullanımını ve yeniden kullanımını yönetmek için yönergelere ihtiyaç vardır.
    - Razı olmak
        - Katılımcıların araştırmaya katılımları hakkında bilinçli kararlar alabilmelerini sağlamak
    - Gizlilik ve Mahremiyet
        - Mahremiyet, bireylerin kişisel bilgilerine kimlerin erişebileceği üzerinde sahip olduğu kontroldür.
        - Gizlilik, bilgiye yalnızca yetkili kişilerin erişebilmesi ilkesidir.
    - Mülkiyet ve yazarlık
        - Verilerden kimin sorumlu olduğunu ve bir bireyin hangi noktada kişisel verilerini kontrol etme hakkından vazgeçtiğini ele alır
    - Bilgi paylaşımı–Araştırmanın sosyal faydalarının değerlendirilmesi
        - Veri eşleştirme ve bir kaynaktan veya araştırma projesinden alınan verilerin başka bir kaynakta yeniden kullanılmasından kaynaklanan sosyal faydalar
    - Yönetişim ve gözetim
        - Dijital verilerin yönetimi, organizasyonu, erişimi ve korunmasının gözetimi ve uygulanması

Etik konular

- Etik:

"Belirli eylemlerin yararları ve zararları ile bu eylemlerin amaçlarının ve hedeflerinin doğruluğu ve yanlışlığı ile ilgili bir ahlaki ilkeler sistemi."

- Gizlilik ve güvenlik sorunları yaratan bilgi ve elektronik iletişimin birçok olası kötü kullanımı ve kötüye kullanımı
- Medeniyetler tarafından geliştirilen temel etik ilkeler geçerlidir.
  - Bilgisayarları ve bilgi sistemlerini çevreleyen benzersiz hususlar
  - Daha önce mümkün olmayan faaliyetlerin ölçeği
  - Daha önce üzerinde anlaşmaya varılmış hiçbir etik kuralın oluşturulmadığı yeni türde kuruluşların oluşturulması

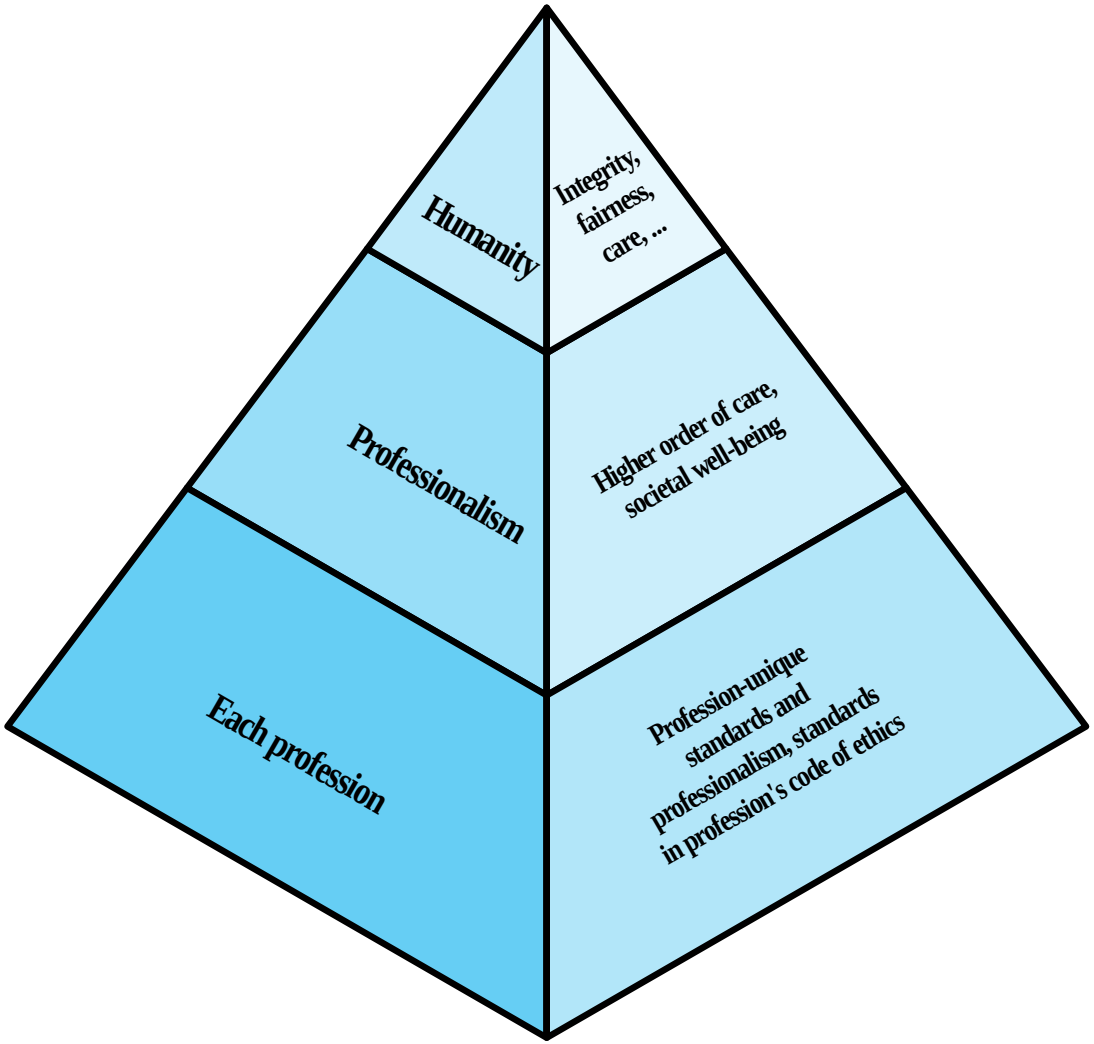


Figure 19.5 The Ethical Hierarchy

Bilgisayarlar ve Bilgi Sistemleri ile İlgili Etik Hususlar

- Bilgisayar kullanımından kaynaklanan bazı etik sorunlar:
  - Bilgi depoları ve işlemcileri
  - Yeni form ve varlık türlerinin üreticileri
  - eylem araçları
  - Yıldırma ve aldatma sembolleri
- Teknolojiyi anlayan, kullanan ve erişim iznine sahip olanların bunlar üzerinde gücü vardır.

Mesleki/Etik Sorumluluklar

- Mesleki sorumlulukları etik veya ahlaki sorumluluklarla dengeleme endişesi
- Bir bilgi işlem veya BT uzmanının karşılaşabileceği etik alan türleri:
  - Bir profesyonel olarak etik görev, işverene sadakatle çatışabilir
  - "Islık çalmak"
  - Halka veya bir şirkete zarar verebilecek bir durumu ifşa etmek'müşterileri
  - Potansiyel çıkar çatışması
- Kuruluşların, çalışanlar için alternatif, daha az aşırı fırsatlar sağlama görevi vardır.
  - Kurum içi ombudsman ve sorunları açığa çıkaran çalışanları cezalandırmama taahhüdü
- Profesyonel dernekler, toplum üyelerinin nasıl ilerleyecekleri konusunda tavsiye alabileceği bir mekanizma sağlamalıdır.

Davranış kuralları

- Etik, kesin yasalar veya gerçekler dizisi değildir
- Birçok alan etik belirsizlik sunabilir
- Birçok profesyonel topluluk, aşağıdakileri yapabilen etik davranış kurallarını benimsemiştir:

1. Olumlu bir uyarıcı olun ve güven aşılar
2. Eğitici olur
3. Bir destek ölçüsü sağlar
4. Caydırıcılık ve disiplin aracı olur
5. Mesleğin kamusal imajını geliştirir

KURALLAR:

1) Bir bilgi işlem ürünü tasarlayan, geliştiren veya dağıtan kişiler, bu yapıdan ve bu yapının öngörülebilir etkilerinden ahlaki olarak sorumludur. Bu sorumluluk, eseri sosyoteknik bir sistemin parçası olarak tasarlayan, geliştiren, dağıtan veya bilerek kullanan diğer kişilerle paylaşılır.

2) Bilgi işlem yapılarının ortak sorumluluğu, sıfır toplamlı bir oyun değildir. Bir bireyin sorumluluğu, yapıtı tasarlamaya, geliştirmeye, dağıtmaya veya kullanmaya daha fazla insan dahil olduğu için azaltılmaz. Bunun yerine, bir kişinin sorumluluğu, yapının davranışlarından ve konuşlandırma sonrasındaki etkilerinden, bu etkilerin o kişi tarafından makul ölçüde öngörülebilir olduğu ölçüde sorumlu olmayı içerir.

3) Belirli bir bilgi işlem yapısını bilerek kullanan kişiler, bu kullanımdan ahlaki olarak sorumludur.

4) Bir bilgi işlem yapıtını bilerek tasarlayan, geliştiren, dağıtan veya kullanan kişiler, bunu yalnızca yapının gömülü olduğu sosyoteknik sistemleri hesaba katmak için makul bir çaba sarf ettiklerinde sorumlu bir şekilde yapabilirler.

5) Bir bilgi işlem ürünü tasarlayan, geliştiren, dağıtan, teşvik eden veya değerlendiren kişiler, yapı veya onun öngörülebilir etkileri veya yapının gömülü olduğu sosyoteknik sistemler hakkında kullanıcıları açık veya dolaylı olarak aldatmamalıdır.