

## BÖLÜM 2

### SOSYAL MEDYA

#### 2.1. ETİK VE BİLİŞİM ETİĞİ

**Etik** kavramı, günümüzde daha çok iş hayatı içinde davranış biçimlerini düzenleyen ve etkileyen bir disiplin olarak yerini almıştır. Bilişim etiği ise özellikle bilgisayar kullanımı için ağ ve internet ortamında uyulması gereken kuralları tanımlayan normlar ve kodlar için kullanılır.

**Bilişim etiği**, bilişim sektöründe çalışanların dünyanın her yerinde aynı davranış normlarına uymasını sağlayarak hareket etmelerini gerektirir. Bilişim sektörünün gelişmesiyle birlikte ortaya çıkan **etik problemlerden** bazıları şunlardır:

- Bilgi doğruluğunun sorgulanması
- Özel yaşama ilişkin sorunlar
- Siber suçların ortaya çıkması
- Fikrî mülkiyet hakları
- İşsizlik sorunları
- Sağlık sorunları
- Sosyal ilişkiler ve aile ilişkileri sorunları
- Sanal ortam ve sanal ilişkilerin varlığı
- Yapay zekâ ile ilgili sıkıntıların yaşanması

**Bilişim temel hak ve özgürlüklerinin ihlal edildiği durumlar:**

- Başkalarının bilgisayarlarına zarar vermek ve bilgisayarlarını bozmak
- Bilgisayarda çalışan insanların çalışmalarına müdahale etmek
- Kişilerin bilgisayar dosyalarını izinsiz almak ve kullanmak
- Bilgisayarda hırsızlık yapmak
- Doğru olmayan bilgileri yaymak için bilgisayar kullanmak
- Korsan yazılım kullanmak
- İzinsiz olarak başkalarının şifrelerini kırmak, kullanmak
- Başkalarının bilgi birikimlerini izinsiz kullanmak
- Kötü amaçlı program yazmak

**Sosyal medyada uyulması gereken etik kurallar:**

- Taraf tutmamak
- Yalan beyanda bulunmamak
- Toplumun değer yargılarıyla çatışmamak
- Başkaları hakkında asılsız beyanlarda bulunmamak
- Kendini farklı göstermemek
- Açık ve anlaşılır dil kullanmak
- Bağlayıcı açıklamalardan kaçınmak (kişinin bağlı bulunduğu kurumu, grubu ya da zümreyi dâhil etmemek)
- Argo ve küfürden kaçınmak
- Başkalarının özeline saygı duymak

## İnternet Etiği

İnternet etiği, gerçek hayatta kişilere gösterilen saygının internet ortamında da devam etmesidir. **İnternet etiği ile ilgili yazılı olmayan kurallar** aşağıda belirtilmiştir.

- İnternet, kişilere zarar verecek şekilde kullanılmamalıdır.
- Kişilerin yaptığı çalışmalar engellenmemelidir.
- Başkalarının özel dosyalarına izinsiz erişim sağlanmamalıdır.
- Doğruluğu kanıtlanmamış bilgiler desteklenmemelidir.
- Yazılımlar lisanslı olarak kullanılmalıdır.
- Kişilere ait elektronik iletişim kaynakları, kişilerin haberi olmadan kullanılmamalıdır.

## Bilgi ve Bilgi Güvenliği

Bilgi, insan aklının idrak edebileceği gerçek olgu ve unsurların hepsine birden verilen isimdir. Bilişim teknolojilerinde ise bilişim araçları ile işlenmekte olan verilerin tümüne bilgi denir.

**Bilgi güvenliği**; bilgi sahibinin rızası olmadan bilginin yetkisiz olarak elde edilmesini, değiştirilmesini, dışarıya sızdırılmasını, çalınmasını, el değiştirmesini ve bilgiye zarar verilmesini engellemek için alınan önlemler bütünü olarak tanımlanır. Bilgi güvenliği; gizlilik, bütünlük ve erişilebilirlik olarak isimlendirilen **üç temel ilkeden** meydana gelir.

**1-Gizlilik:** Erişim izni olmayan kişilerin eline geçmemesi için bilgilerin korunmasıdır. İnternet bankacılığına ait hesap bilgilerinin bir saldırganın [hacker eline geçmesi, gizlilik ihlaline örnek verilebilir.

**2-Bütünlük:** Erişim izni olmayan kişiler tarafından bilgilerin değiştirilmemesidir. Bir web sayfasının içeriğinin değiştirilmesi, bütünlük ilkesinin ihlaline örnek verilebilir.

**3-Erişilebilirlik:** İhtiyaç duyulduğunda bilginin erişilebilir ve kullanılabilir durumda olmasıdır. Bir web sayfasına erişimin bir saldırgan (hacker) tarafından engellenmesi, bu ilkenin ihlaline örnek olarak verilebilir.

Bu üç temel güvenlik ögesinden herhangi biri zarar gördüğünde güvenlik zafiyeti oluşur.

## 2.3. SİBER ZORBALIK

İnternetin ve sosyal medyanın yaygınlaşması ile değişik sosyo-ekonomik ve kültürel sınıfa mensup birbirinden farklı yaş gruplarındaki kişilerin, kimlik gizliliğini de koruyarak iletişime geçmesi mümkün olmuştur. Bu iletişim esnasında bazı riskli durumların yaşanması da kaçınılmazdır. Siber zorbalık, bu riskli durumlardan biridir. Paylaşım yapılan sosyal medya platformlarından, kişinin kendisine ya da kendisine ait değerlere yönelik zorbalık içeren yorum ve paylaşımlar yapılabilir. Bu paylaşımlar kişi ve topluluklara karşı yalan haber, aşağılayıcı ifadeler, kötü sözcükler, tehditler ve utandırıcı görsel paylaşımlar şeklinde olabilir. Bu zorba davranışlar kişilerde ruhsal, fiziksel ve duygusal hasara neden olabilir.

### 2.3.1. Güvenlik Yazılımları

Güvenlik yazılımları, dijital dünyada kişilerin bilgi güvenliğini sağlamak amacıyla hazırlanmış programlardır. Bu programlar, siber zorbalığa maruz kalma riskini azaltmak için internet kullanıcılarına yardımcı olan önemli bir unsurdur.

Bilgisayar, telefon ya da tablette bulunan özel bilgi veya görsel içeriklerin siber hırsızlık ile ele geçirilip kullanılmasını engellemek amacıyla aşağıda belirtilen önlemler alınmalıdır.

- Antivirüs ve güvenlik duvarı program ya da uygulamalar, kullanılan cihaza yüklenmeli ve bu program ya da uygulamalar güncellenmelidir.
- E-posta hesaplarına gelen postaları denetleyen güvenlik eklentileri kullanılmalıdır.
- Lisanslı yazılımlar kullanılmalı ve bu yazılımlar güncel tutulmalıdır.
- Herhangi bir depolama birimini (haricî sabit diskler, USB bellekler vb. ) bir yerdeki dijital cihaza bağlarken tarama yapması amacıyla bu konuyla ilgilenen güvenlik yazılımları kullanılmalıdır.

#### **Siber zorbalığa karşı alınabilecek önlemler aşağıda sıralanmıştır.**

- Çevrimiçi paylaşımlarda siber zorbalığa maruz kalınmasına sebep olabilecek bilgiler, fotoğraf, video gibi görseller, ses içerikleri, adres, telefon ve kimlik bilgileri paylaşılmamalıdır.
- Kullanılan sosyal medya platformunun gizlilik ayarları dikkatlice incelenmeli ve gereken ayarlamalar yapılmalıdır.
- Utandırıcı yorum ya da kişilik haklarına karşı yapılan saldırılar, sosyal medya platformu yetkililerine bildirilmelidir.
- Gerçek hayatta tanımadığınız kişiler, sosyal medyadan eklenmemelidir.
- Gerektiğinde sosyal medya paylaşımları kişilere göre sınırlandırılmalı ya da risk oluşturmada söz konusu kişiler silinmelidir.
- Siber zorbalık yapabilecek olası hesaplar engellenmelidir.

#### **DİJİTAL MARKA YÖNETİMİ VE DİJİTAL DÖNÜŞÜM**

Dijital marka yönetimi, üretilen mal veya hizmetin sanal dünyada vermek istediği imajın oluşturulması ve yönetilmesidir. Dijital marka yönetimi sayesinde pazarlanan markanın tüketici tarafından, marka vizyonu çerçevesinde tanınması sağlanabilir.

Dijital marka yönetiminde, markanın dönüşümünü belirlerken dikkate alınması gereken unsurlar aşağıda belirtilmiştir.

- Olası müşteri profili beklentilerini karşılaması
- Marka vizyonunu doğru yansıtması
- Ürün değerlendirme ve güncelleme basamaklarında müşteri ihtiyaçlarının dikkate alınması
- Sürdürülebilir bir marka pazarlama stratejisinin belirlenmesi

Müşteri beklentilerine cevap verebilmek için önemli strateji basamakları şunlardır:

- Dürüstlük
- Şeffaflık
- Hızlı geri dönüş yapmak
- Soruna çözüm olacak cevaplar vermek

#### **SOSYAL MEDYA ARAÇLARI**

Sosyal medya, standart medya araçlarından (tv, radyo, gazete, dergi, süreli yayın vb.) farklı olarak yayınlanan içeriklerin sadece tek bir kaynaktan değil sosyal medya hesabı açılmış tüm kaynaklardan içerik üretilmesi prensibine dayalı, internet üzerinden anlık paylaşım yapılan yayın organlarıdır.

Sosyal medya platformlarından bazıları şunlardır:

**Sosyal Ağlar:** Günlük hayattaki sosyal yaşantıların, duygu, düşünce, görsel gibi paylaşımların yapılabildiği platformlardır

**Bloglar:** Sosyal medya kullanıcılarının kendi yaşantılarını ya da herhangi bir konuyla ilgili fikirlerini günlük biçimde yazıp paylaşabildiği platformlardır.

**Microbloglar:** Kullanıcıların duygu ve düşüncelerini ya da duyurmak istediği bir olguyu, zamandan bağımsız olarak kısa cümlelerle paylaşabileceği platformlardır.

**Çevrimiçi Ansiklopediler:** Sosyal medya kullanıcılarının çeşitli konularla ilgili bilgi paylaşımlarını derlenmiş şekilde sanal dünyada paylaşan platformdur.

**Forumlar:** Sosyal medyada kullanıcıların çeşitli konularla ilgili fikirlerini paylaşarak tartışabileceği platformlardır.

**İçerik Toplulukları:** Kullanıcıların görsel ve hareketli resim şeklinde paylaşım yapabileceği ve etkileşim alabileceği platformlardır.

**Mobil Sosyal Ağlar:** Kullanıcıların; cep telefonu, tablet vb. araçlar kullanarak içerik paylaşmasını ve mesajlaşmasını sağlayan platformlardır.

## 2.6. SOSYAL MEDYA PLATFORMLARI İÇİN İÇERİK PLANI OLUŞTURMA

Sosyal medya platformunda içerik oluşturulurken ilk yapılması gereken içerik planı oluşturmaktır. Çünkü profesyonel tüm işlerde planlama aşaması, işin doğru yapılması için gereken en önemli adımdır. Planlama yapılırken de düşünülmesi gereken bazı adımlar vardır. Bu adımlar sosyal medyada öne çıkarılmak istenen ürünü en doğru şekilde ifade etmeyi amaçlamalıdır.

### 2.6.1. Hedef Kitlenin Tespiti

Bir sosyal medya platformu içeriği hazırlanırken bu içeriğin hitap etmesi istenen topluluğa **hedef kitle** denir. Hedef kitlenin tespiti ve doğru tanınması ürünün başarılı bir şekilde pazarlanmasını sağlar. Bu sebeple **hedef kitle belirlenirken cevaplanması gereken bazı sorular** vardır.

Hedef kitle belirlenirken şu sorular sorulmalıdır:

- Hedef kitlenin yaş aralığı kaçtır?
- Hedef kitlenin cinsiyet dağılımı nasıldır?
- Hedef kitlenin eğitim durumu nedir?
- Hedef kitlenin yaşadığı yer neresidir?
- Hedef kitlenin alışveriş alışkanlıkları nedir?
- Hedef kitlenin özel zevkleri nelerdir?
- Hedef kitlenin tercihleri nelerdir?
- Hedef kitlenin beklentileri nelerdir?
- Hedef kitle hangi sosyal medya kanallarını kullanmaktadır?

### 2.6.2. Uygun Kategorilerin Oluşturulması

Sosyal medyada paylaşılan içeriklerin çeşitli kategorileri vardır. Sosyal medya içerik planı hazırlanırken dijital marka profiline uygun içerik kategorileri seçilmelidir. Seçilen kategorinin özelliklerine uyan tasarım ve içerik hazırlanıp paylaşılmalıdır. Sosyal medya içerik kategorileri şöyle sıralanabilir:

**Metinsel İçerikler:** Yazım kurallarına uygun, akıcı, çok uzun olmayan ve anahtar kavramlara vurgu yapılmış özelliklere sahip içerikler (liste, açıklama, blog, tanıtım, rehber vb.) olmalıdır.

**Görsel İçerikler:** Hem ilgi çekici hem de tasarım kurallarına uygun, hedef kitleyi kısa sürede yakalayabilen özelliklerde [resim, fotoğraf, video, afiş, infografik (bir bilgiyi grafik ve görsellerle anlatan içerik) vb.] olmalıdır.

**Reklam ve Tanıtım İçerikleri:** Verilmek istenen mesajı yalın ve etkili bir şekilde veren, merak uyandıran özelliklerde (bülten, broşür, e-posta içerikleri vb.) olmalıdır.

**Uzman Yardımı:** Hedef kitlenin faydalanabileceği şekilde ve özellikte içerikler (reklam, planlama, strateji vb.) uzmanlar tarafından hazırlanmalıdır.

**Güncel İçerikler:** Sosyal medya etkileşimini artırmaya yönelik, güncel, doğrulanmış, özet içerikler (haberler, bilim, teknoloji, spor ve sanattaki gelişmeler vb.) olmalıdır.

**Etkileşimli İçerikler:** Sosyal medya hesabı takipçisini artırabilecek, hedef kitlenin memnuniyetini sağlayabilecek, markayı doğru temsil etmeyi sağlayacak içerikler ( soru-cevap, beğeni toplama içerikleri vb.) olmalıdır.

**Özel Gün İçerikleri:** Hedef kitlenin ve toplumun değerlerine uygun kutlama ve anma içerikleri (belirli gün ve haftalar) olmalıdır

### 2.6.3. İçerik Planı Takviminin Hazırlanması

İçerik yayınlama sıklığı ve içerik sayısı belirlenirken şu sorulara cevaplar verilmelidir:

- Yayınlanacak içerik ne kadar iş gücü gerektiriyor?
- Markanın dâhil olduğu sektörün beklediği paylaşım sıklığı ve sayısı nedir?
- Hangi aralıklarla paylaşım yapılırsa hedef kitlenin beklentileri karşılanır?
- Paylaşım sıklığı ve sayısı, dijital marka stratejisinde belirlenen hedeflere uyuyor mu?

### İçerik Konusu ve Konuya Uygun İçerik Türü Belirleme

Dijital marka stratejisi dikkate alınarak yayınlanacak içeriklerin türü ve konu kapsamı belirlenmelidir.

### İçeriğin Uyandıracığı Düşünce ve Duyguları Kararlaştırma ve İçeriği Oluşturma

Yayınlanacak içeriğin eğlendirici bir özelliği mi olmalı yoksa bilgi verici türde mi olmalı?

Bu durum önceden belirlenmeli ve içerik buna göre oluşturulmalıdır.

### İçerik Yayın Zamanı Belirleme

Paylaşılacak içeriğin gün, hafta ve ay bazında yayınlanma tarih ve saatleri belirlenmelidir.

Ayrıca dijital markaya özgü yapılması istenen periyodik paylaşımlar varsa bu paylaşımlar için de bir planlama yapılmalıdır.

### İçeriğin Yayınlanacağı Sosyal Medya Platformu

Bir dijital markanın birçok sosyal platform hesabı olabilir ancak bazı paylaşımların tüm sosyal medya platformlarında paylaşılması gerekmez. Planlanan içeriğin hangi sosyal medya platformlarında paylaşılacağı ihtiyaca göre belirlenmelidir.

### Şifre Güvenliği

İnternet ortamında güvenlik için kullanılacak şifrelerin sahip olması gereken bazı özellikler olmalıdır. Bu özellikler aşağıda belirtilmiştir.

**Kolay tahmin edilebilecek şifre seçenekleri tercih edilmemelidir.**

Kişisel bilgi içermeyen (doğum tarihi, yakınlarının ismi, doğum yeri, telefon numarası vb.), kişiyle ilgili yapılan basit bir araştırma sonucunda tahmin edilemeyecek bir şifre seçilmelidir.

Çok bilinen tekrar eden sayıların, sıralanmış rakamların, klavyede yan yana duran harflerin bulunduğu şifreler kolayca kırılabilir.

**Karmaşık bir şifre oluşturulmalıdır.**

En az sekiz karakterden oluşan, küçük ve büyük harfler ile birkaç rakam da içeren, en az bir noktalama işaretinin bulunduğu şifreleri kullanmak daha güvenlidir. Şifre tercih edilirken tek bir sözcük yerine birkaç sözcüğün oluşturduğu birleşik sözcükler kullanmak, daha da güvenlisi rastgele harf, rakam ve sembollerden oluşmuş şifreler seçmek en doğrusudur.

**İki aşamalı güvenlik kullanılmalıdır.**

Birçok internet platformu kimlik doğrulaması için birden fazla güvenlik aşaması sunar. İlgili platformun ayarlarından söz konusu güvenlik seçenekleri ayarlanarak internet hesapları daha güvenli hâle getirilebilir.

**Şifreler belirli aralıklarla değiştirilmelidir.**

Farkında olunmadan şifrelerin ele geçirilmesi ve bilgilerin çalınması riskine karşılık kişisel hesap şifreleri sıklıkla değiştirilmelidir.

**Tüm hesaplar için farklı şifreler seçilmelidir.**

Herhangi bir internet platformu hesabının ele geçirilmesi olasılığı, diğer hesapların da ele geçirilebilmesine neden olabilir. Bu sebeple her internet platformu için ayrı şifre kullanmak daha güvenlidir.