DİJİTAL OKURYAZARLIK

DİJİTAL DÜNYADA BİLGİ GÜVENLİĞİ VE MAHREMİYET

GİRİŞ

Günümüzde dijital teknolojiler yaşamın her alanında yoğun olarak kullanılmaktadır.

Dijital dünyadaki küresel iletişim platformları, bilgi kaynaklarına, web sitelerine, sanal alanlara ve sosyal forum ortamlarına erişim için yaygın şekilde kullanılmaktadır.

Bu süreçte bilgiler ağ ortamında yayıldığı için bilgi güvenliği ve mahremiyeti ile ilgili sorunlar ortaya çıkabilir.

Dijital çağda mahremiyet

Mahremiyetin tehdit altında olduğu dijital çağda, bireysel kararların bağımsızlığı ve dijital ortamdaki bilgi akışına ilişkin bireysel kontrol genellikle tehlikeye atılmaktadır.

Bireyler kimlik ve tanımlama sürecini yeni teknolojileri kullanarak gerçekleştirebilmektedir. Kimlik ve kimlik doğrulama kişisel verileri içerdiğinden dolayı bilgi güvenliğini doğrudan etkilemektedir.

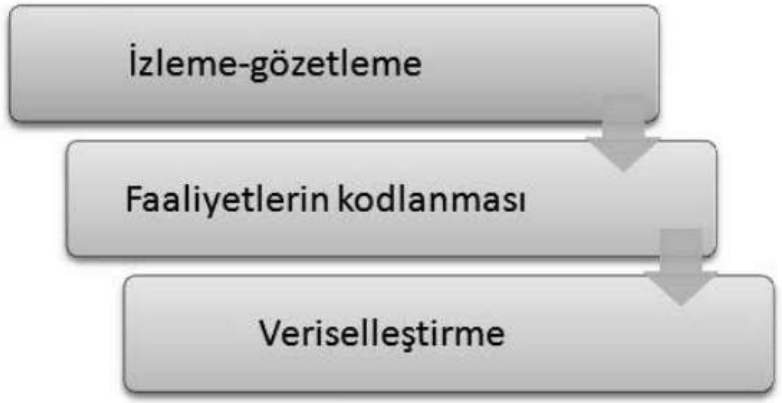
Gelişen teknolojiler ve teknoloji kullanımındaki hatalar bilgi mahremiyeti konusunda endişelere yol açmaktadır.

Bu endişeleri ortadan kaldırmak için bilgi güvenliği ve mahremiyet kavramlarına önem vermek gerekmektedir.

Dijital çağda mahremiyet

Dijital bilgi toplumunda mahremiyeti anlamak için yeni ve geliştirilmiş anlayışlara ihtiyaç duyulmaktadır.

Mahremiyet ihlali üç model altında ele alınabilir.



Mahremiyet İhlailine İlişikin Modeller

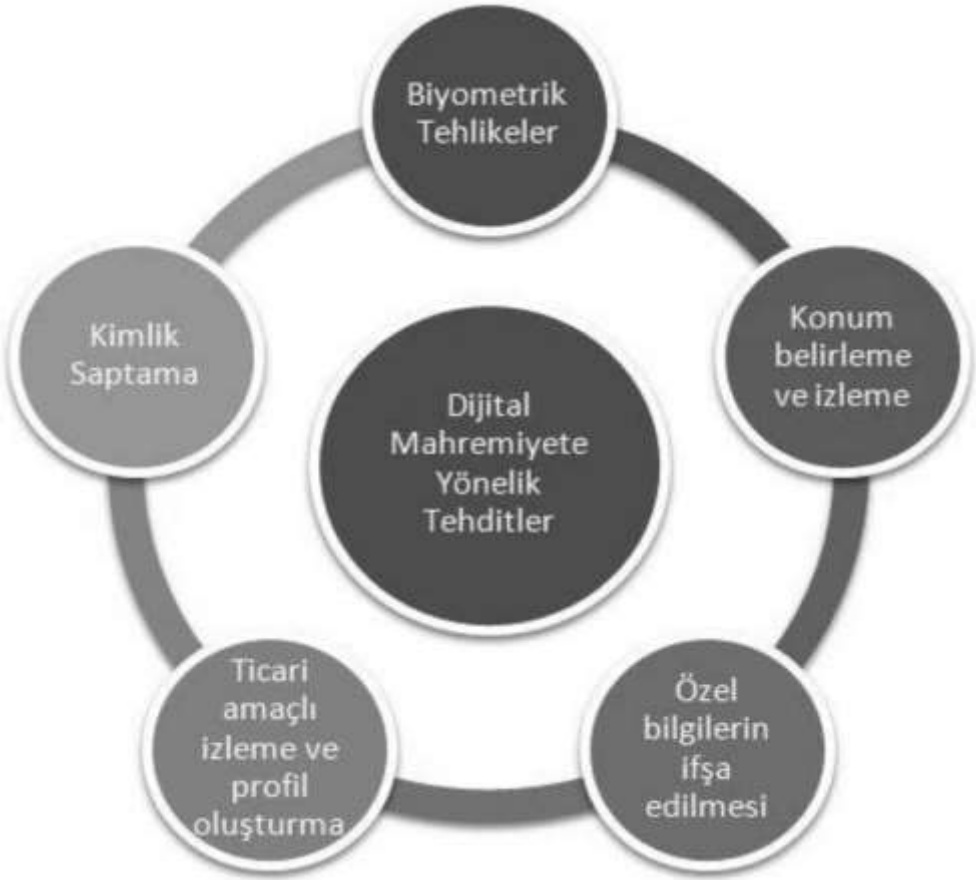
Dijital çağda mahremiyet

Veriler; ticari kuruluşlar, devlet kurumları ve sağlık sektörleri tarafından çeşitli araçlar kullanılarak toplanmaktadır. Bu şekilde toplanan veriler, ortaya çıkması riskli olan hassas kişisel bilgileri de içerebilmektedir.

Çevrim içi ortamda paylaşılan kişisel bilgilerin sınırlandırılması konusundaki hassasiyet, bireylerin kişisel bilgilerini kontrol etme ihtiyacına ve yaşanılan mahremiyet ihlallerine dayanmaktadır.

Veri mahremiyetinin sağlanması için büyük veri ekosistemindeki modern araçların ve teknolojilerin avantajlarından yararlanılması gerektiği söylenebilir

Dijital Dünyada Mahremiyete Yönelik Tehditler ve Mahremiyet İhlalleri



1.Biyometrik tehlikeler

Biyometri, bireyleri yüz, parmak izi, iris, ses, yürüyüş ve imza gibi davranışsal ve biyolojik özelliklerine göre tanıma bilimidir.

Biyometrik tanıma içeren uygulamalar;

- Mantıksal ve fiziksel erişim sistemleri
- Suçlara karşı mücadele operasyonları
- Göç kontrolü ve sınır güvenlik sistemleri
- Ulusal kimlik programları
- Kimlik yönetim sistemleri
- Askeri sistemler gibi

1.Biyometrik Tehlikeler

Bahsedilen biyometrik sistemlerde güvenlik ve mahremiyet çok önemli iki gerekliliktir.,

Biyometrik verilerde mahremiyeti ve güvenliği sağlamaya yönelik olarak şifreleme protokolleri, uygulamalar ve güvenlik analizleri mevcuttur.

Örneğin; kişiye özel uzaktan biyometrik kimlik doğrulaması veya fiziksel erişim kontrolü senaryosuna karşılık gelen bölgesel biyometrik tanımlama sağlanabilmektedir.

1. Biyometrik Tehlikeler

Biyometrik sistemlerin tasarımı için mahremiyet açısından dört ana kapsam önerilmektedir.

Biyometrik Sistemlerin Tasarımı ve Kullanımına İlişkin Konular

2.Tanımlama-Kimlik Saptama

Tanımlama; kimlik saptayıcı aracılığıyla isim, adres veya herhangi bir takma adın kişiyle ve onun hakkındaki verilerle ilişkilendirilmesi tehlikesine işaret etmektedir.

Gelişen teknolojilerin birbirine bağlantılı yapısı ve etkileşim özelliklerinin etkisi tanımlama tehdidini daha da artırmaktadır.

Bireylerin çevrim dışı ve çevrim içi faaliyetlerinin büyük bir kısmı elektronik veritabanlarında dijital ayak izleri bırakmaktadır. Ayrıca büyük veri içeren iş veya bilimsel amaçlı süreçler günümüzde bulut teknolojileri ile yürütülmektedir. Bu durumda özel bilgiler kolayca açığa çıkabilmektedir.

3.Konum Belirleme ve İzleme

Konum belirleme ve izleme, bir kişinin konumunu zaman ve mekân içinde belirleme ve kaydetme tehdidini kapsamaktadır.

Bu işlem küresel konumlandırma sistemi (GPS), internet trafiği veya cep telefonu konumu gibi farklı yollarla mümkün olabilmektedir.

Konum mahremiyetini ihlal eden bu gibi uygulamalarda örneğin kullanılan arabanın dönüş açıları bir haritadaki verilerle eşleştirilerek kullanıcıların yol bilgileri elde edilebilir

4.Ticari Amaçlı İzleme ve Profil Oluşturma

Veri analitiğinin çok büyük veri kümelerine uygulanması işlemi, tüketiciler hakkında kişisel bilgilerin elde edilmesini veya bilinmeyen kişisel bilgilerin keşfedilmesini mümkün kılabilmektedir.

Ayrıca mobil uygulamaların kullanıcılar hakkında değerli bilgiler topladığına, birtakım amaçlar doğrultusunda kullanıcıların profillerini belirlemek için bu bilgilerin kullanıldığına veya bu bilgilerin ticari çıkarlar için satıldığına değinilmektedir.

Ticari süreçlerde tüketicinin durumunun ve mahremiyetinin korunması ile verilerin uygun şekilde kullanılması oldukça önemlidir. Bu bağlamda mahremiyet politikalarının dikkatli okunması ve mahremiyet bilincinin oluşturulması için kullanıcıların teşvik edilmesi, konum izleme gibi uygulamalarda geçerli onayların nasıl alınabileceği konusunda kullanıcıların bilgilendirilmesi gerekmektedir.

5.Özel Bilgilerin İfşa Edilmesi

Teknolojik gelişmelerle birlikte değişen iletişim biçimi tüm dünyada sosyal yönelimleri de etkileyebilmektedir. Kullanıcı sayısı hızla artan sosyal medyanın hayatın merkezine alınması ile sosyal görünürlükle var olunan bu ağlar nedeniyle mahremiyet sorunsalının gündeme geldiği görülmektedir.
Bazı kullanıcılar çevrim içi sosyal ağ ortamlarında başkalarının dikkatini çekebilmek için kişisel bilgilerini açığa vurabilmektedirler.

Akıllı sistemler bilgi ifşası ile ilgili bir diğer tehlikedir. bu teknolojilerdeki veriler, sistemin yapısı gereği halka açık niteliktedir.

Kullanıcılar akıllı teknolojileri hareket etmek, dokunmak ve konuşmak gibi çeşitli amaçlarla kullanmaktadırlar. Akıllı sistem ile kullanıcı arasında özel bilgi alışverişi yapıldığında gizlilik için bir tehdit hâline gelmektedir.

Dijital Dünyada Mahremiyeti Koruma çabaları

Mahremiyet temel bir insan hakkıdır. Bireyler ve ülkeler bazında veri gizliliğinin özel bağlamı ve derecesi değişse de mahremiyetin yasalar, politikalar ve prosedürlerle korunması gerekmektedir. Veri mahremiyeti konusunda ele alınması gereken ilkeler mevcuttur. Bunlar;

Uyarı	Saklama	Uygulama	Katılım
Kullanım Kısıtlaması	Minimizasyon	Erişim	Şeffaflık
Kalite	Güvenlik	İzin	Açıklama

Dijital Dünyada Mahremiyeti Koruma çabaları

Dünya çapında mahremiyet kültürleri arasında farklılıklar olabilir. Ülkelere göre veri mahremiyeti ilkelerinin dağılımı aşağıda sunulmaktadır.

Mahremiyet İlkesi	Avusturalya	Brezilya	Kanada	Çin	Kolombiya	AB Ülkeleri	Gana	Hong Kong	Malezya	Meksika	Yeni Zelanda	Filipinler	Rusya	Güney Afrika
Uyarı	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kullanım Kısıtlaması	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kalite	✓	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Saklama	✓	x	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
Minimizasyon	✓	✓	✓	✓	x	✓	✓	✓	✓	✓	x	✓	✓	✓
Güvenlik	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	x	x	✓
Uygulama	x	✓	✓	✓	✓	✓	✓	✓	x	✓	✓	✓	✓	✓
Erişim	✓	✓	✓	✓	x	x	✓	✓	✓	✓	✓	x	x	✓
İzin	✓	x	✓	✓	✓	x	✓	✓	✓	✓	✓	x	x	✓
Katılım	✓	✓	✓	✓	x	x	✓	✓	✓	✓	✓	x	x	✓
Şeffaflık	✓	✓	✓	✓	x	✓	✓	✓	✓	✓	x	x	x	✓
Açıklama	✓	x	✓	x	x	x	✓	✓	✓	✓	✓	x	x	✓

Türkiye’de Dijital Mahremiyetin Korunması çabaları

Türkiye‘de, 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazete’de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu ile kişisel verilerin korunmasına ilişkin usul ve esaslar düzenlenmiştir.

Bu Kanun’un amacı; kişisel verilerin işlenmesinde temel hak ve özgürlüklerin korunmasını, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlenmesini, kişilerin mahremiyetinin korunmasını ve veri güvenliğini sağlamaktır.

Bilgi ve İletişim Kurumu (BTK) aracılığıyla da güvenli internet kullanımı, kişisel verilerin korunması, dijital mahremiyet gibi konulara yönelik konferans, araştırma, eğitim, atölye gibi çeşitli etkinlikler gerçekleştirilmektedir.

https://www.btk.gov.tr/

Dijital Dünyada Mahremiyetin Korumasına Yönelik Öneriler

Dijital dünyada mahremiyet ihlalleri ve mahremiyetin korunmasına yönelik öneriler aşağıdaki gibidir;

- Sosyal Ağ platformlarının Kullanımına Yönelik Öneriler
- Bulut Teknolojilerinin Kullanımına Yönelik Öneriler
- Mobil Teknolojilerin Kullanımına Yönelik Öneriler

Sosyal Ağ Platformlarının Kullanımına Yönelik Öneriler

Yaygın kullanılan sosyal medya siteleri çoğunlukla iki mekanizma şeklinde mahremiyet desteği sağlar.

Bu özellikler;

- etiketleme/etiketi kaldırma
- uygunsuz içeriği bildirmek

Sosyal Ağ Platformlarının Kullanımına Yönelik Öneriler

Sosyal ağ platformunda mahremiyetin sağlanmasına yönelik teknik çözümlerin uygulanmasının yanı sıra kullanıcıların da dikkate alması gereken aşağıdaki gibi durumlar söz konusudur;

- Paylaşılan mesajların, fotoğrafların ve diğer bilgilerin **gizlilik ayarları** kontrol edilmelidir.
- Paylaşımlarda kullanılan "**etiketleme**" özelliği kontrol edilmelidir.
- Sosyal ağ ortamlarında yapılan paylaşımları **yabancı kişilerin** de görebileceği ve/veya takip edebileceği düşünülerek bu konuda her zaman özenli olunmalıdır.
- Sosyal medya kullanımı sürecinde görünürlüğü artırmaya yönelik gerçekleştirilen eylemlerin sınırları belirlenmelidir. Görünür olma, tanınma, sevilme, beğenilme gibi psikososyal ihtiyaçlar nedeniyle mahremiyet ihlaline sebep olabilecek paylaşımlardan kaçınılmalıdır.

Bulut Teknolojilerinin Kullanımına Yönelik Öneriler

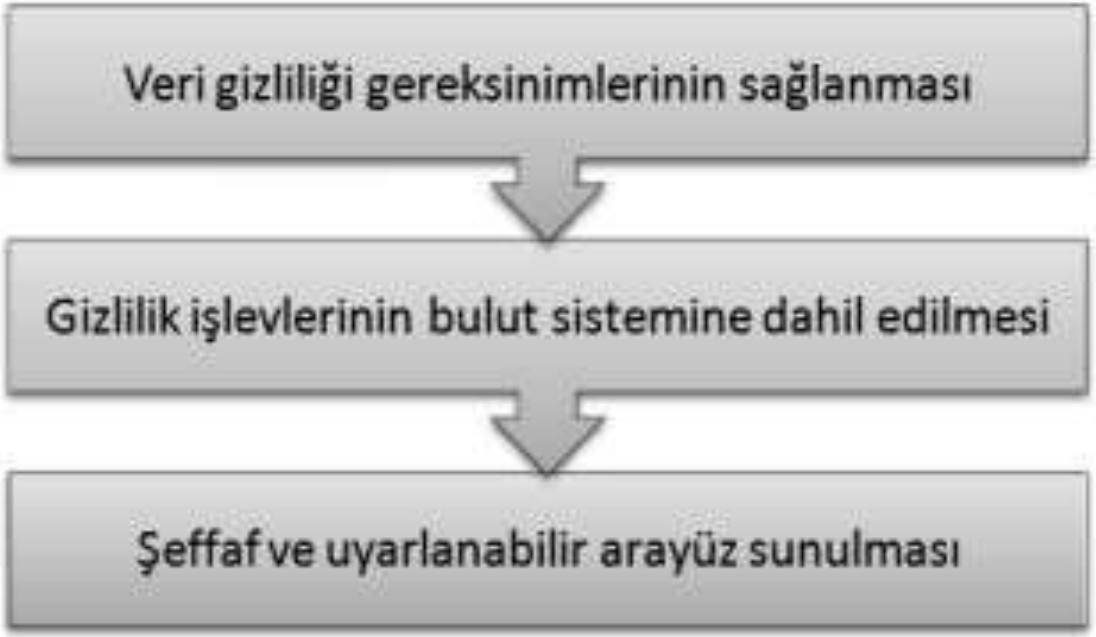
Bulut, kullanıcı gereksinimlerini karşılamak için ağ veya internet üzerinden çeşitli hizmetler sunan veri merkezlerinde donanım ve yazılım kaynaklarının bulunduğu bir ortamdır.

Bulut altyapısına geçiş yaparak sağlanan esneklik ve maliyet tasarrufu, birçok şirketi önemli uygulamaları için bulut bilişim kullanmaya teşvik etmektedir.

Bulut bilişim modelinin özellikleri mahremiyete yönelik yeni tehditleri beraberinde getirmektedir.

Bu nedenle mahremiyet sorunları çözülmedikçe bulut bilişimin; kullanıcıların mahremiyetinin çok önemli olduğu finansal işlemler veya tıbbi kayıtlar gibi hassas uygulamalar için kullanılmaması gerektiği söylenebilir.

Bulut Teknolojilerinin Kullanımına Yönelik Öneriler



Bulut Tabanlı Mahremiyetin Sağlanmasına İlişkin Öneriler

Bulut Teknolojilerinin Kullanımına Yönelik Öneriler

Bulut teknolojileri kapsamında mahremiyetle ilgili olası tehditler ve alınabilecek önlemler aşağıda ayrıntılandırılmaktadır.

- Olası saldırıların önlenmesi
- Hizmetin kötüye kullanımının engellenmesi
- Kimlik yönetiminin sağlanması

Mobil Teknolojilerin Kullanımına Yönelik Öneriler

Mobil sistemler; şebeke operatörleri, uygulama geliştiricileri, kullanıcılar, kanun yapıcılar ile ilgili teknolojiler ve politikaların toplamını içermektedir.

Akıllı telefonlar ve giyilebilir cihazlar gibi sensör bakımından zengin mobil cihazların popülerliği ile mobil kitle kaynak kullanımı veri toplama ve işlemede etkili bir yöntem olarak ortaya çıkmaktadır.

Öte yandan güvenlik ve mahremiyet ile ilgili birçok zorluğu da beraberinde getirmektedir.

Mobil Teknolojilerin Kullanımına Yönelik Öneriler

İnternet kullanıcılarının bu anlamda dikkat etmesi gereken hususlar;

- İnternet tarayıcısının “izlememe” (do not track) seçeneği aktif hâle getirilmelidir.
- İlgili internet sayfalarının kullanım politikası ve gizlilik sözleşmeleri mutlaka okunmalı; “iletişim” ve “hakkımızda” gibi bölümler incelenmelidir.
- Mobil platformlardan indirilen uygulamaların kullanıcıdan ne tür bilgiler topladığı incelenmelidir.
- İndirilen mobil uygulamaların telefondaki hangi uygulamalarla ve bilgilerle eşleştirildiğine dikkat edilmelidir.
- Güvenilir kaynaklar dışındaki mobil uygulamalar yüklenmemelidir.
- Telefonların yazılım güncellemeleri takip edilerek gerekli güncellemeler yapılmalıdır.

Dijital dünyada bilgi güvenliği ve mahremiyet farkındalığı

Çocuklar, gençler ve yetişkinlerin dijital dünyada farkındalığının kazandırılması için;

- **Ortak kullanılan bilgisayar**, tablet gibi cihazlar kullanıldıktan sonra kişisel bilgiler silinmeli, açılan hesap oturumlarından mutlaka çıkış yapılmalıdır. Bu cihazlarda **şifre kaydetme, otomatik form doldurma gibi ayarlar devre dışı bırakılmalıdır.**
- Sosyal ağ ortamlarında paylaşılan bilgilerin bu ortamlardan kaldırılması mümkün olmayabilir. Bu nedenle sosyal medya ortamlarında **adres, okul, telefon, kimlik numarası gibi bilgiler kesinlikle paylaşılmamalıdır.**
- Sosyal ağ ortamlarında her gönderi için gizlilik ayarları kontrol edilmelidir. Aksi takdirde istenmeyen yabancı kişilerce takip edilebilir ve/veya görüntülenebilir.

Dijital dünyada bilgi güvenliği ve mahremiyet farkındalığı

- İnternet ortamında yabancı kişilerle iletişim kurulmamalı, yabancı kişilerden gelen fotoğraf, video gibi içerikler **kabul edilmemelidir**.
- Kaynağı bilinmeyen, güvenilir olmayan kaynaklardan gelen mesajlara dikkat edilmeli, eğer varsa mesajdaki **bağlantılara tıklanmamalıdır**.
- İnternet ortamında **özel fotoğraf** ve **videolar** paylaşılmamalı ya da paylaşırken kimlerle paylaşıldığı **gizlilik ayarları** ile kontrol edilmelidir.
- Telefon, tablet, bilgisayar gibi teknolojik araçlar herkesin erişebileceği yerlerde bırakılmamalı, gerekli durumlarda kullanım izni için **şifre** belirlenmelidir.

Dijital dünyada bilgi güvenliği ve mahremiyet farkındalığı

- **Güvenilmeyen web siteleri ziyaret edilmemeli**, sahte web sitelerine dikkat edilmelidir.
- Akıllı telefonlara **yeni bir uygulama** yüklerken uygulamanın telefondaki hangi bilgilere erişebileceğine dikkat edilmelidir.
- **Kablosuz ağlara bağlanırken** şifreli ve güvenilir olduğu bilinen bağlantılar tercih edilmelidir.
- Bir ortama girişte oluşturulan parolanın güvenli bir yapıda olmasına dikkat edilmelidir.
- İnternet ortamında karşılaşılan **rahatsız edici bir durum aile bireyleri ile paylaşılmalıdır**.