YAPAY ZEKÂ ÇAĞINDA DİJİTAL KİMLİĞİN GÜVENLİĞİ

Sosyal Medya Fotoğraf Akımları, Yapay Zekâ ile Fotoğraf/Video İşleme, Deepfake, Suç Amaçlı Kötüye Kullanım Riskleri ve 6698 Sayılı Kanun Açısından Bir İnceleme

Akademik İnceleme Çalışması

Selçuk DİKİCİ

Endüstri Mühendisi

(Bilişim Teknolojileri ve Siber Güvenlik Uzmanı)

Bursa, 2026

ÖZET

Üretken yapay zekâ teknolojilerinin gündelik yaşama yayılması, fotoğraf ve video üretimini sıradan kullanıcıların birkaç saniye içinde gerçekleştirebildiği bir faaliyete dönüştürmüştür. Sosyal medya platformlarında yayılan "yaşlandırma", "gençleştirme", "çocukluk fotoğrafını canlandırma", "farklı meslekte veya tarihsel dönemde kendini gösterme", "sinema karakterine dönüşme", "aile fotoğrafını hareketlendirme" ve benzeri akımlar, eğlence ve yaratıcılık boyutunun yanında önemli bir dijital güvenlik problemi doğurmaktadır. Kullanıcıların yüksek çözünürlüklü yüz görüntülerini, farklı açılardan çekilmiş fotoğraflarını, aile ilişkilerini ve zaman zaman ses örneklerini üçüncü taraf sistemlere aktarması; kimlik taklidi, sentetik medya üretimi, sosyal mühendislik, dolandırıcılık, şantaj, itibar zedeleme ve hedef profilleme gibi kötüye kullanım senaryolarının veri tabanını genişletebilmektedir.

Bu çalışma, yapay zekâ destekli fotoğraf ve video akımlarını teknik, toplumsal, güvenlik ve hukuk boyutlarıyla birlikte incelemektedir. Çalışmanın merkezinde, bir görüntünün yalnızca "fotoğraf" olarak değil; yüz geometrisi, yaş, mimik, bağlamsal ilişki, mekân, sosyal çevre ve davranışsal ipuçları taşıyan çok katmanlı bir veri nesnesi olarak değerlendirilmesi gerektiği savunulmaktadır. Bununla birlikte her fotoğrafın kendiliğinden biyometrik veri olmadığı; görüntünün kişiyi benzersiz biçimde tanımlama veya doğrulama amacıyla belirli teknik işlemlere tabi tutulması hâlinde biyometrik veri tartışmasının güçlendiği hukuki ayrım özellikle korunmaktadır.

Çalışmada ayrıca deepfake, yüz değiştirme, görüntüden görüntüye üretim, kimlik gömme vektörleri, yüz eşleştirme, dudak senkronizasyonu, ses klonlama ve sentetik avatar teknolojilerinin çalışma mantığı savunma odaklı bir yaklaşımla açıklanmakta; bu teknolojilerin suç veya suç örgütleri tarafından kullanılmasının oluşturabileceği riskler analiz edilmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu bakımından açık rıza, aydınlatma, amaçla sınırlılık, ölçülülük, veri minimizasyonu, saklama, aktarım ve veri güvenliği meseleleri tartışılmaktadır. Sonuçta sosyal medya güvenliğinin yalnızca parola ve hesap güvenliğiyle sınırlı olmadığı; kişinin yüzünün, sesinin ve dijital temsilinin de korunması gereken bir "dijital kimlik varlığı" hâline geldiği ileri sürülmektedir.

Anahtar Kelimeler: Yapay zekâ, üretken yapay zekâ, deepfake, sosyal medya, fotoğraf akımları, dijital kimlik, biyometrik veri, kişisel veri, KVKK, 6698 sayılı Kanun, kimlik taklidi, sentetik medya, sosyal mühendislik, dijital güvenlik.

ABSTRACT

The widespread adoption of generative artificial intelligence has transformed image and video production into an everyday activity. Viral social-media trends that invite users to upload portraits, childhood photographs, family images or voice samples may appear harmless and creative, yet they also create a new class of digital-security risks. High-quality facial imagery, contextual information and repeated representations of the same person can contribute to identity impersonation, synthetic-media fraud, social engineering, reputational attacks, extortion and targeted profiling when misused.

This study examines AI-driven photo and video trends from technical, social, security and legal perspectives, with particular emphasis on Türkiye's personal-data protection framework. It argues that social-media security can no longer be reduced to passwords and account access: the face, voice and synthetic representation of an individual increasingly function as components of a persistent digital identity. The study distinguishes ordinary photographs from biometric processing, discusses deepfakes, face embeddings, image-to-image generation, lip synchronization and voice cloning at a defensive conceptual level, and proposes a layered governance model based on data minimization, transparency, provenance, platform responsibility, user awareness and institutional safeguards.

İÇİNDEKİLER

1. Giriş

2. Araştırmanın Problemi, Amacı ve Kapsamı

3. Kavramsal Çerçeve: Dijital Kimlik ve Sentetik Medya

4. Yapay Zekâ ile Fotoğraf İşleme Teknikleri

5. Yapay Zekâ ile Video İşleme ve Deepfake Teknolojileri

6. Yüz, Ses ve Biyometrik Kimlik Katmanı

7. Sosyal Medya Fotoğraf Akımlarının Veri Ekonomisi

8. Fotoğraf Akımlarının Bireysel Güvenlik Riskleri

9. Suç ve Suç Örgütleri Açısından Kötüye Kullanım Senaryoları

10. Sosyal Mühendislik, Dolandırıcılık ve Kimlik Taklidi

11. Deepfake Şantajı, İtibar Saldırıları ve Mağduriyet

12. Çocuklar, Aile Fotoğrafları ve Kuşaklararası Dijital İz

13. Sosyal Medyada Güven ve Gerçeklik Krizi

14. 6698 Sayılı Kanun Açısından Hukuki Değerlendirme

15. Açık Rıza, Aydınlatma ve Amaçla Sınırlılık

16. Biyometrik Veri ve Yüz Görüntülerinin Hukuki Niteliği

17. Platformların ve Yapay Zekâ Hizmet Sağlayıcılarının Sorumluluğu

18. Kurumsal Riskler ve Kamu Kurumları Açısından Değerlendirme

19. Teknik ve İdari Güvenlik Önlemleri

20. Türkiye İçin Yapay Zekâ Görsel Güvenliği Modeli

21. Tartışma

22. Sonuç ve Öneriler

Ek A. Risk Değerlendirme Matrisi

Ek B. Bireysel Dijital Kimlik Güvenliği Kontrol Listesi

1. GİRİŞ

Dijitalleşmenin ilk dönemlerinde çevrimiçi güvenlik denildiğinde temel olarak kullanıcı adı, parola, kötü amaçlı yazılım ve hesap ele geçirme riskleri anlaşılmaktaydı. Üretken yapay zekânın yaygınlaşmasıyla bu çerçeve genişlemiştir. Günümüzde kişinin hesabı ele geçirilmeden de kimliği taklit edilebilir; gerçek hesabına erişilmeden de yüzü, sesi veya konuşma biçimi kullanılarak inandırıcı sentetik içerikler üretilebilir. Böylece güvenlik nesnesi "hesap" olmaktan çıkıp insanın dijital temsilinin tamamına doğru genişlemektedir.

Sosyal medya fotoğraf akımları bu dönüşümün görünür örneklerinden biridir. Kullanıcı bir akıma katılırken çoğu zaman işlem sonucuna odaklanır: daha genç görünmek, farklı bir çağda kendisini görmek, fotoğrafını hareketlendirmek veya sinematik bir portre elde etmek. Oysa teknik açıdan süreç, kişinin yüzünü ve bağlamsal özelliklerini taşıyan verilerin bir sisteme aktarılmasını gerektirir. Verinin nerede işlendiği, ne kadar süre saklandığı, hangi alt hizmet sağlayıcılarla paylaşıldığı, model geliştirmede kullanılıp kullanılmadığı veya sonradan silinip silinmediği kullanıcı tarafından her zaman kolayca anlaşılamaz.

Bu çalışmanın hareket noktası teknoloji karşıtlığı değildir. Üretken yapay zekâ yaratıcı üretim, erişilebilirlik, eğitim, iletişim ve görsel tasarım bakımından önemli fırsatlar sunmaktadır. Sorun, teknolojinin kapasitesi ile toplumsal farkındalık ve hukuki/teknik koruma mekanizmaları arasındaki hız farkıdır. Bir fotoğrafın eğlence amacıyla yüklenmesi ile o fotoğraftan çıkarılabilecek kimliksel özelliklerin gelecekteki kullanım ihtimalleri arasında önemli bir asimetri vardır.

Bu nedenle çalışma, fotoğraf ve video akımlarının güvenlik boyutunu bireysel mahremiyetin ötesine taşımaktadır. Risk; kişinin yalnızca görüntüsünün ifşa edilmesi değil, görüntünün yeniden üretilebilir, değiştirilebilir, başka bağlamlara yerleştirilebilir ve gerçekmiş gibi sunulabilir olmasıdır. Sentetik medyanın ölçeklenebilirliği, aynı saldırının binlerce kişi üzerinde düşük maliyetle denenebilmesine imkân tanımaktadır.

1.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Dijitalleşmenin ilk dönemlerinde çevrimiçi güvenlik denildiğinde temel olarak kullanıcı adı, parola, kötü amaçlı yazılım ve hesap ele geçirme riskleri anlaşılmaktaydı. Üretken yapay zekânın yaygınlaşmasıyla bu çerçeve genişlemiştir. Günümüzde kişinin hesabı

ele geçirilmeden de kimliği taklit edilebilir; gerçek hesabına erişilmeden de yüzü, sesi veya konuşma biçimi kullanılarak inandırıcı sentetik içerikler üretilebilir. Böylece güvenlik nesnesi "hesap" olmaktan çıkıp insanın dijital temsilinin tamamına doğru genişlemektedir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

1.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Sosyal medya fotoğraf akımları bu dönüşümün görünür örneklerinden biridir. Kullanıcı bir akıma katılırken çoğu zaman işlem sonucuna odaklanır: daha genç görünmek, farklı bir çağda kendisini görmek, fotoğrafını hareketlendirmek veya sinematik bir portre elde etmek. Oysa teknik açıdan süreç, kişinin yüzünü ve bağlamsal özelliklerini taşıyan verilerin bir sisteme aktarılmasını gerektirir. Verinin nerede işlendiği, ne kadar süre saklandığı, hangi alt hizmet sağlayıcılarla paylaşıldığı, model geliştirmede kullanılıp kullanılmadığı veya sonradan silinip silinmediği kullanıcı tarafından her zaman kolayca anlaşılamaz.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi

yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

1.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Bu çalışmanın hareket noktası teknoloji karşıtlığı değildir. Üretken yapay zekâ yaratıcı üretim, erişilebilirlik, eğitim, iletişim ve görsel tasarım bakımından önemli fırsatlar sunmaktadır. Sorun, teknolojinin kapasitesi ile toplumsal farkındalık ve hukuki/teknik koruma mekanizmaları arasındaki hız farkıdır. Bir fotoğrafın eğlence amacıyla yüklenmesi ile o fotoğraftan çıkarılabilecek kimliksel özelliklerin gelecekteki kullanım ihtimalleri arasında önemli bir asimetri vardır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

2. ARAŞTIRMANIN PROBLEMİ, AMACI VE KAPSAMI

Araştırmanın temel problemi, sosyal medyada yaygınlaşan yapay zekâ tabanlı görsel akımların kullanıcıların dijital kimlik güvenliğini nasıl etkilediğidir. Bu problem üç alt soruya ayrılabilir: Birincisi, fotoğraf ve video işleme teknolojileri hangi kimliksel bilgileri kullanmakta veya türetebilmektedir? İkincisi, bu teknik kapasite kötü niyetli aktörlerin elinde hangi mağduriyet biçimlerine dönüşebilir? Üçüncüsü, mevcut kişisel veri koruma yaklaşımı bu yeni risk alanını hangi ölçüde karşılamaktadır?

Çalışmanın amacı belirli bir yapay zekâ ürününü suçlamak veya her görsel işleme hizmetini hukuka aykırı ilan etmek değildir. Amaç, veri yaşam döngüsünün tamamını görünür kılmaktır: toplama, yükleme, ön işleme, özellik çıkarımı, üretim, saklama, paylaşım, silme ve ikincil kullanım. Bu yaşam döngüsünün her aşaması farklı riskler doğurabilir ve her risk aynı hukuki nitelikte değildir.

Yöntem olarak kavramsal ve normatif inceleme benimsenmiştir. Teknik kavramlar saldırı talimatı vermeyecek düzeyde açıklanmakta; kötüye kullanım örnekleri risk modelleme amacıyla ele alınmaktadır. Hukuki değerlendirmelerde 6698 sayılı Kanunun temel ilkeleri merkeze alınmış, ancak çalışma bir somut uyuşmazlık hakkında hukuki görüş verme iddiasında değildir.

Kapsam sosyal medya, üretken yapay zekâ uygulamaları, yüz ve video işleme, ses sentezi, sentetik kimlik, platform güvenliği ve kişisel veri koruma kesişimiyle sınırlandırılmıştır. Ulusal güvenlik, askeri istihbarat veya ileri seviye saldırı teknikleri kapsam dışındadır. Böylece çalışma birey, kurum ve platform seviyesinde önleyici güvenlik yaklaşımına odaklanmaktadır.

2.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Araştırmanın temel problemi, sosyal medyada yaygınlaşan yapay zekâ tabanlı görsel akımların kullanıcıların dijital kimlik güvenliğini nasıl etkilediğidir. Bu problem üç alt soruya ayrılabilir: Birincisi, fotoğraf ve video işleme teknolojileri hangi kimliksel bilgileri

kullanmakta veya türetebilmektedir? İkincisi, bu teknik kapasite kötü niyetli aktörlerin elinde hangi mağduriyet biçimlerine dönüşebilir? Üçüncüsü, mevcut kişisel veri koruma yaklaşımı bu yeni risk alanını hangi ölçüde karşılamaktadır?

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

2.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Çalışmanın amacı belirli bir yapay zekâ ürününü suçlamak veya her görsel işleme hizmetini hukuka aykırı ilan etmek değildir. Amaç, veri yaşam döngüsünün tamamını görünür kılmaktır: toplama, yükleme, ön işleme, özellik çıkarımı, üretim, saklama, paylaşım, silme ve ikincil kullanım. Bu yaşam döngüsünün her aşaması farklı riskler doğurabilir ve her risk aynı hukuki nitelikte değildir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

2.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Yöntem olarak kavramsal ve normatif inceleme benimsenmiştir. Teknik kavramlar saldırı talimatı vermeyecek düzeyde açıklanmakta; kötüye kullanım örnekleri risk modelleme amacıyla ele alınmaktadır. Hukuki değerlendirmelerde 6698 sayılı Kanunun temel ilkeleri merkeze alınmış, ancak çalışma bir somut uyuşmazlık hakkında hukuki görüş verme iddiasında değildir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

3. KAVRAMSAL ÇERÇEVE: DİJİTAL KİMLİK VE SENTETİK MEDYA

Dijital kimlik, bir kişinin çevrimiçi ortamda tanınmasını veya onunla ilişki kurulmasını sağlayan veri parçalarının bütünüdür. Ad-soyad ve kullanıcı adı bunun yalnızca en görünür katmanıdır. Yüz görüntüsü, ses, konuşma üslubu, sosyal çevre, konum ipuçları, mesleki bilgiler, aile ilişkileri, ilgi alanları ve zaman içinde paylaşılan davranış örüntüleri de dijital kimlik mozaiğinin parçalarıdır.

Sentetik medya, tamamı veya bir bölümü algoritmik yöntemlerle üretilen ya da anlamlı biçimde değiştirilen görsel, ses veya video içeriklerini kapsar. Sentetik olması tek başına zararlı olduğu anlamına gelmez. Film prodüksiyonu, erişilebilirlik, eğitim ve sanat gibi meşru kullanım alanları vardır. Risk, sentetik içeriğin kaynağı ve niteliği gizlenerek gerçek bir kişinin sözü, davranışı veya görüntüsüymüş gibi sunulmasıyla yükselir.

Dijital kimliğin yeni özelliği kopyalanabilirliktir. Fiziksel dünyada yüz, bedene bağlıdır; dijital dünyada yüz görüntüsü dosya hâline geldiği anda çoğaltılabilir. Üretken modeller bu kopyayı statik olmaktan çıkararak farklı ışık, açı, ifade ve bağlamlarda yeniden üretebilir. Bu durum kimliğin temsil katmanını kişinin fiilî kontrolünden uzaklaştırabilir.

“Kimlik bütünlüğü” kavramı bu nedenle önemlidir. Mahremiyet, veriye kimin eriştiğiyle; kimlik bütünlüğü ise kişi hakkında hangi temsilin gerçek kabul edildiğiyle ilgilidir. Deepfake çağında bir birey, gizli bilgisi ifşa edilmese bile sahte bir görüntü nedeniyle zarar görebilir. Dolayısıyla veri koruma ile içerik doğrulama güvenliği giderek birbirine yaklaşmaktadır.

3.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Dijital kimlik, bir kişinin çevrimiçi ortamda tanınmasını veya onunla ilişki kurulmasını sağlayan veri parçalarının bütünüdür. Ad-soyad ve kullanıcı adı bunun yalnızca en görünür katmanıdır. Yüz görüntüsü, ses, konuşma üslubu, sosyal çevre, konum ipuçları, mesleki bilgiler, aile ilişkileri, ilgi alanları ve zaman içinde paylaşılan davranış örüntüleri de dijital kimlik mozaiğinin parçalarıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi

yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

3.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Sentetik medya, tamamı veya bir bölümü algoritmik yöntemlerle üretilen ya da anlamlı biçimde değiştirilen görsel, ses veya video içeriklerini kapsar. Sentetik olması tek başına zararlı olduğu anlamına gelmez. Film prodüksiyonu, erişilebilirlik, eğitim ve sanat gibi meşru kullanım alanları vardır. Risk, sentetik içeriğin kaynağı ve niteliği gizlenerek gerçek bir kişinin sözü, davranışı veya görüntüsüymüş gibi sunulmasıyla yükselir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık,

anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

3.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Dijital kimliğin yeni özelliği kopyalanabilirliktir. Fiziksel dünyada yüz, bedene bağlıdır; dijital dünyada yüz görüntüsü dosya hâline geldiği anda çoğaltılabilir. Üretken modeller bu kopyayı statik olmaktan çıkararak farklı ışık, açı, ifade ve bağlamlarda yeniden üretebilir. Bu durum kimliğin temsil katmanını kişinin fiilî kontrolünden uzaklaştırabilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

4. YAPAY ZEKÂ İLE FOTOĞRAF İŞLEME TEKNİKLERİ

Modern görüntü işleme sistemleri klasik filtrelerden farklı olarak görüntünün semantik yapısını analiz edebilir. Yüzün yaklaşık konumu, ifade, aydınlatma, saç, arka plan ve nesneler gibi unsurlar ayrıştırılarak yeni bir görsel üretim sürecinde kullanılabilir. Üretken modeller, metinsel komutlarla veya referans görüntülerle yeni görüntüler oluşturabilir; bir kişinin görünümünü belirli ölçüde korurken bağlamı değiştirebilir.

Görüntüden görüntüye üretimde başlangıç görüntüsü, üretilecek sonucun yapısal veya kimliksel referansı olabilir. Kimlik koruma mekanizmaları, aynı kişiye benzer yüz özelliklerinin farklı sahnelerde sürdürülmesine çalışır. Bu teknikler yaratıcı kullanım açısından değerlidir; ancak gerçek kişiye ait referans görüntüler rıza dışı kullanıldığında kimlik taklidi riskini artırır.

Yüz eşleştirme ve özellik temsilinde sistemler bir görüntüyü sayısal bir temsil uzayına dönüştürebilir. Bu tür temsiller çoğu zaman "embedding" olarak adlandırılır. Embedding, fotoğrafın kendisi değildir; ancak yüzler arasındaki benzerliğin matematiksel olarak karşılaştırılmasına yarayabilir. Bir görüntünün bu şekilde benzersiz tanıma veya doğrulama amacıyla işlenmesi, kişisel veri ve biyometrik veri tartışmasını daha hassas bir düzeye taşır.

Yaşlandırma, gençleştirme, yüz restorasyonu ve süper çözünürlük gibi teknikler de güvenlik bakımından çift kullanımlıdır. Düşük kaliteli eski bir fotoğrafın iyileştirilmesi aile arşivi için faydalı olabilir. Aynı kapasite, daha önce tanımlanması zor bir yüzü daha kullanılabilir hâle getirebilir. Bu nedenle risk değerlendirmesi teknolojinin adına değil; veri kaynağına, işleme amacına, saklama politikasına ve sonuçların kullanımına göre yapılmalıdır.

4.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Modern görüntü işleme sistemleri klasik filtrelerden farklı olarak görüntünün semantik yapısını analiz edebilir. Yüzün yaklaşık konumu, ifade, aydınlatma, saç, arka plan ve nesneler gibi unsurlar ayrıştırılarak yeni bir görsel üretim sürecinde kullanılabilir. Üretken modeller, metinsel komutlarla veya referans görüntülerle yeni görüntüler oluşturabilir; bir kişinin görünümünü belirli ölçüde korurken bağlamı değiştirebilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin

belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

4.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Görüntüden görüntüye üretimde başlangıç görüntüsü, üretilecek sonucun yapısal veya kimliksel referansı olabilir. Kimlik koruma mekanizmaları, aynı kişiye benzer yüz özelliklerinin farklı sahnelerde sürdürülmesine çalışır. Bu teknikler yaratıcı kullanım açısından değerlidir; ancak gerçek kişiye ait referans görüntüler rıza dışı kullanıldığında kimlik taklidi riskini artırır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

4.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Yüz eşleştirme ve özellik temsilinde sistemler bir görüntüyü sayısal bir temsil uzayına dönüştürebilir. Bu tür temsiller çoğu zaman "embedding" olarak adlandırılır. Embedding, fotoğrafın kendisi değildir; ancak yüzler arasındaki benzerliğin matematiksel olarak karşılaştırılmasına yarayabilir. Bir görüntünün bu şekilde benzersiz tanıma veya doğrulama amacıyla işlenmesi, kişisel veri ve biyometrik veri tartışmasını daha hassas bir düzeye taşır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

5. YAPAY ZEKÂ İLE VİDEO İŞLEME VE DEEPFAKE TEKNOLOJİLERİ

Video, tek bir fotoğraftan daha fazla zamansal bilgi içerir. Yüz hareketleri, göz kırpma, baş pozisyonu, konuşma ritmi ve mimikler kareler boyunca devam eder. Yapay zekâ tabanlı video üretiminde bu sürekliliğin inandırıcı biçimde korunması temel teknik zorluklardan biridir. Teknolojik ilerleme, geçmişte uzmanlık gerektiren bazı işlemleri son kullanıcı seviyesine indirmiştir.

Deepfake terimi genel kullanımda gerçek bir kişinin yüzünün veya performansının yapay yollarla başka bir içerikte gerçekçi biçimde taklit edilmesini ifade eder. Teknik yöntemler zaman içinde değişse de güvenlik açısından belirleyici unsur aynıdır: izleyicinin içeriği gerçek sanma olasılığı. Kalite yükseldikçe yalnızca görsel incelemeye dayalı "çıplak gözle tespit" yaklaşımı zayıflamaktadır.

Dudak senkronizasyonu ve konuşan avatar teknolojileri, ses ile ağız hareketlerini eşleştirebilir. Meşru kullanımda dublaj, eğitim ve erişilebilirlik için yararlıdır. Kötüye kullanımda ise gerçek bir kişinin söylemediği bir cümleyi söylüyormuş gibi gösterme potansiyeli taşır. Ses klonlama da bu riski artırarak çok modlu kimlik taklidine yol açabilir.

Video güvenliğinde savunma yaklaşımı tek bir "deepfake dedektörü"ne güvenmemelidir. Kaynak doğrulama, içerik kökeni kayıtları, platform işaretlemeleri, bağlamsal kontrol, tersine arama, hesap geçmişi ve gerektiğinde adli inceleme birlikte düşünülmelidir. Çünkü üretim teknikleri geliştikçe belirli tespit modellerinin başarı oranı değişebilir.

5.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Video, tek bir fotoğraftan daha fazla zamansal bilgi içerir. Yüz hareketleri, göz kırpma, baş pozisyonu, konuşma ritmi ve mimikler kareler boyunca devam eder. Yapay zekâ tabanlı video üretiminde bu sürekliliğin inandırıcı biçimde korunması temel teknik zorluklardan biridir. Teknolojik ilerleme, geçmişte uzmanlık gerektiren bazı işlemleri son kullanıcı seviyesine indirmiştir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

5.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Deepfake terimi genel kullanımda gerçek bir kişinin yüzünün veya performansının yapay yollarla başka bir içerikte gerçekçi biçimde taklit edilmesini ifade eder. Teknik yöntemler zaman içinde değişse de güvenlik açısından belirleyici unsur aynıdır: izleyicinin içeriği gerçek sanma olasılığı. Kalite yükseldikçe yalnızca görsel incelemeye dayalı "çıplak gözle tespit" yaklaşımı zayıflamaktadır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

5.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Dudak senkronizasyonu ve konuşan avatar teknolojileri, ses ile ağız hareketlerini eşleştirebilir. Meşru kullanımda dublaj, eğitim ve erişilebilirlik için yararlıdır.

Kötüye kullanımda ise gerçek bir kişinin söylemediği bir cümleyi söylüyormuş gibi gösterme potansiyeli taşır. Ses klonlama da bu riski artırarak çok modlu kimlik taklidine yol açabilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

6. YÜZ, SES VE BİYOMETRİK KİMLİK KATMANI

Yüz ve ses insan kimliğinin güçlü göstergeleridir; fakat hukuki ve teknik açıdan dikkatli sınıflandırma gerekir. Bir kişinin fotoğrafı kişisel veri niteliği taşıyabilirken, her fotoğraf otomatik olarak biyometrik veri kabul edilmemelidir. Biyometrik nitelik tartışması, kişinin fiziksel veya davranışsal özelliklerinin özel teknik işlemle benzersiz tanımlama ya da doğrulama amacıyla kullanılması hâlinde belirginleşir.

Bu ayrım sosyal medya akımları açısından önemlidir. Bir uygulamanın yalnızca geçici bir görsel efekt uygulaması ile yüzün kalıcı bir kimlik şablonuna dönüştürülmesi aynı risk düzeyinde değildir. Kullanıcı açısından dışarıdan benzer görünen iki hizmet, arka planda çok farklı veri işleme mimarilerine sahip olabilir.

Ses de benzer şekilde yalnızca bir kayıt olarak değil, konuşmacıyı tanımaya yarayan özelliklerin çıkarılması hâlinde daha hassas bir kimlik katmanına dönüşebilir. Yüz ve ses birlikte işlendiğinde çok modlu doğrulama veya taklit kapasitesi artar. Bu nedenle “tek bir fotoğraf ne

kadar zarar verebilir?” sorusu yerine, farklı platformlarda biriken veri parçalarının birleşik etkisi değerlendirilmelidir.

Biyometrik özelliklerin güvenlik açısından özel önemi değiştirilebilirliklerinin sınırlı olmasıdır. Bir parola sızdığında değiştirilebilir; kişinin yüzü veya doğal sesi aynı şekilde değiştirilemez. Bu nedenle biyometrik şablonların ve bu şablonları üretmeye elverişli veri setlerinin korunmasında daha yüksek güvenlik beklentisi doğar.

6.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Yüz ve ses insan kimliğinin güçlü göstergeleridir; fakat hukuki ve teknik açıdan dikkatli sınıflandırma gerekir. Bir kişinin fotoğrafı kişisel veri niteliği taşıyabilirken, her fotoğraf otomatik olarak biyometrik veri kabul edilmemelidir. Biyometrik nitelik tartışması, kişinin fiziksel veya davranışsal özelliklerinin özel teknik işlemle benzersiz tanımlama ya da doğrulama amacıyla kullanılması hâlinde belirginleşir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

6.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Bu ayrım sosyal medya akımları açısından önemlidir. Bir uygulamanın yalnızca geçici bir görsel efekt uygulaması ile yüzün kalıcı bir kimlik şablonuna dönüştürülmesi aynı risk düzeyinde değildir. Kullanıcı açısından dışarıdan benzer görünen iki hizmet, arka planda çok farklı veri işleme mimarilerine sahip olabilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

6.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Ses de benzer şekilde yalnızca bir kayıt olarak değil, konuşmacıyı tanımaya yarayan özelliklerin çıkarılması hâlinde daha hassas bir kimlik katmanına dönüşebilir. Yüz ve ses birlikte işlendiğinde çok modlu doğrulama veya taklit kapasitesi artar. Bu nedenle “tek bir fotoğraf ne kadar zarar verebilir?” sorusu yerine, farklı platformlarda biriken veri parçalarının birleşik etkisi değerlendirilmelidir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi

yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

7. SOSYAL MEDYA FOTOĞRAF AKIMLARININ VERİ EKONOMİSİ

Sosyal medya akımlarının temel gücü katılımın gönüllü ve kitlesel olmasıdır. Kullanıcılar aynı temaya uygun görseller yükler, sonuçları paylaşır ve arkadaşlarını davet eder. Bu davranış, kısa sürede çok sayıda yüksek kaliteli portre ve bağlamsal veri üretebilir. Risk, yalnızca tek bir hizmetin ne yaptığı değil, kullanıcıların yıllar içinde farklı hizmetlere benzer verileri tekrar tekrar vermesidir.

Veri ekonomisi açısından bir görsel, içerdiği piksel bilgisinden daha fazlasını temsil eder. Dosya üst verileri, çekim bağlamı, paylaşım zamanı, açıklama metni, etiketlenen kişiler ve sosyal bağlantılar bir araya geldiğinde profil zenginleşebilir. Platformlar veya üçüncü taraf hizmetler bu verileri farklı amaçlarla işleyebilir; hukuki meşruiyet ise her somut işleme faaliyeti bakımından ayrı değerlendirilmelidir.

“Ücretsiz” veya düşük maliyetli bir yapay zekâ hizmetinin ekonomik modeli kullanıcı açısından her zaman açık değildir. Hizmet abonelikle, reklamla, kurumsal lisansla veya başka gelir modelleriyle finanse edilebilir. Kullanıcının güvenlik açısından sorması gereken soru, “ücret ödedim mi?” değil, “verim hangi amaçla ve ne kadar süreyle işleniyor?” olmalıdır.

Fotoğraf akımları veri minimizasyonu ilkesinin gündelik hayattaki karşıt örneklerini de oluşturabilir. Kullanıcı tek bir sonuç için gereğinden fazla fotoğraf yükleyebilir. Sistem üç fotoğrafla çalışabilecekse yirmi fotoğraf yüklemek, sonuç kalitesini artırsa bile maruziyet

yüzeyini büyütebilir. Güvenli tasarım, mümkün olan en az veriyle istenen sonuca ulaşmayı hedeflemelidir.

7.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Sosyal medya akımlarının temel gücü katılımın gönüllü ve kitlesel olmasıdır. Kullanıcılar aynı temaya uygun görseller yükler, sonuçları paylaşır ve arkadaşlarını davet eder. Bu davranış, kısa sürede çok sayıda yüksek kaliteli portre ve bağlamsal veri üretebilir. Risk, yalnızca tek bir hizmetin ne yaptığı değil, kullanıcıların yıllar içinde farklı hizmetlere benzer verileri tekrar tekrar vermesidir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

7.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Veri ekonomisi açısından bir görsel, içerdiği piksel bilgisinden daha fazlasını temsil eder. Dosya üst verileri, çekim bağlamı, paylaşım zamanı, açıklama metni, etiketlenen kişiler ve sosyal bağlantılar bir araya geldiğinde profil zenginleşebilir. Platformlar veya üçüncü taraf hizmetler bu verileri farklı amaçlarla işleyebilir; hukuki meşruiyet ise her somut işleme faaliyeti bakımından ayrı değerlendirilmelidir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

7.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. “Ücretsiz” veya düşük maliyetli bir yapay zekâ hizmetinin ekonomik modeli kullanıcı açısından her zaman açık değildir. Hizmet abonelikle, reklamla, kurumsal lisansla veya başka gelir modelleriyle finanse edilebilir. Kullanıcının güvenlik açısından sorması gereken soru, “ücret ödedim mi?” değil, “verim hangi amaçla ve ne kadar süreyle işleniyor?” olmalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin

belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

8. FOTOĞRAF AKIMLARININ BİREYSEL GÜVENLİK RİSKLERİ

Bireysel risklerin ilki kontrol kaybıdır. Kullanıcı bir fotoğrafı kendi hesabından silebilir; ancak aynı fotoğraf daha önce indirilmiş, ekran görüntüsü alınmış, başka bir hizmete aktarılmış veya farklı bir içerikte kullanılmış olabilir. Dijital çoğaltmanın maliyeti düşük olduğu için "silme" eylemi her zaman tüm kopyaların ortadan kalktığı anlamına gelmez.

İkinci risk bağlam kaymasıdır. Tatil fotoğrafı, iş başvurusu bağlamında; aile fotoğrafı sahte bir profil bağlamında; profesyonel portre ise sahte reklamda kullanılabilir. Görüntünün kendisi gerçek olsa bile bağlamın değiştirilmesi yanıltıcı bir temsil üretir. Yapay zekâ bu bağlam kaymasını daha inandırıcı hâle getirebilir.

Üçüncü risk, profil zenginleştirmedir. Farklı yaşlarda çekilmiş fotoğraflar, aile üyeleri, meslek, kurum ve coğrafi ipuçları bir araya geldiğinde sosyal mühendislik için güçlü bir hedef profili oluşabilir. Buradaki güvenlik problemi tek bir gizli bilginin çalınması değil, açık kaynak parçalarının birleştirilerek ikna edici bir hikâye kurulabilmesidir.

Dördüncü risk psikolojik ve itibari zarardır. Kişinin rızası dışında üretilmiş sahte görüntüler, doğru olmadığı kanıtlansa bile dolaşımda kalabilir. Özellikle hızlı yayılan içeriklerde düzeltmenin erişimi ilk paylaşımın erişiminden düşük olabilir. Bu nedenle mağduriyet yalnızca maddi zarar üzerinden ölçülmemelidir.

8.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Bireysel risklerin ilki kontrol kaybıdır. Kullanıcı bir fotoğrafı kendi hesabından silebilir; ancak aynı fotoğraf daha önce indirilmiş, ekran görüntüsü alınmış, başka bir hizmete aktarılmış veya farklı bir içerikte kullanılmış olabilir. Dijital çoğaltmanın maliyeti düşük olduğu için "silme" eylemi her zaman tüm kopyaların ortadan kalktığı anlamına gelmez.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

8.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. İkinci risk bağlam kaymasıdır. Tatil fotoğrafı, iş başvurusu bağlamında; aile fotoğrafı sahte bir profil bağlamında; profesyonel portre ise sahte reklamda kullanılabilir. Görüntünün kendisi gerçek olsa bile bağlamın değiştirilmesi yanıltıcı bir temsil üretir. Yapay zekâ bu bağlam kaymasını daha inandırıcı hâle getirebilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

8.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Üçüncü risk, profil zenginleştirmedir. Farklı yaşlarda çekilmiş fotoğraflar, aile üyeleri, meslek, kurum ve coğrafi ipuçları bir araya geldiğinde sosyal mühendislik için güçlü bir hedef profili oluşabilir. Buradaki güvenlik problemi tek bir gizli bilginin çalınması değil, açık kaynak parçalarının birleştirilerek ikna edici bir hikâye kurulabilmesidir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

9. SUÇ VE SUÇ ÖRGÜTLERİ AÇISINDAN KÖTÜYE KULLANIM SENARYOLARI

Organize suç yapıları teknolojiyi çoğu zaman tek başına değil, mevcut dolandırıcılık ve baskı yöntemlerini ölçeklendirmek için kullanır. Yapay zekâ destekli kimlik taklidi bu açıdan maliyeti düşüren ve inandırıcılığı artıran bir araç hâline gelebilir. Bir hedefin sosyal medya paylaşımlarından toplanan açık bilgiler, kişiselleştirilmiş temas girişimlerinde kullanılabilir.

Risk senaryolarından biri sahte profil ve güven inşasıdır. Gerçek bir kişinin görüntüleriyle oluşturulan veya yapay zekâyla çeşitlendirilen profil, zaman içinde normal bir hesap görünümü kazanabilir. Amaç romantik dolandırıcılık, para talebi, bilgi toplama veya başka kişilere erişim olabilir. Burada mağdur hem kandırılan kişi hem de kimliği kullanılan gerçek kişi olabilir.

Bir diğer senaryo otorite taklididir. Yönetici, kamu görevlisi, şirket yetkilisi veya aile büyüğü gibi güven duyulan bir kişinin ses ve görüntüsünün taklit edilmesi, aciliyet hissi yaratmak için kullanılabilir. Savunma açısından kritik ilke, finansal veya hassas işlemlerde yalnızca görüntülü görüşmeyi yeterli doğrulama kabul etmemek ve bağımsız ikinci kanal kullanmaktır.

Suç örgütleri açısından yapay zekânın asıl tehlikesi otomasyon ve ölçeklenebilirliktir. Aynı sahte içerik şablonu çok sayıda hedefe uyarlanabilir. Bu nedenle kurumların yalnızca tekil olay müdahalesi değil, örüntü tespiti, hızlı bildirim, delil koruma ve platformlarla koordinasyon kapasitesi geliştirmesi gerekir.

9.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Organize suç yapıları teknolojiyi çoğu zaman tek başına değil, mevcut dolandırıcılık ve baskı yöntemlerini ölçeklendirmek için kullanır. Yapay zekâ destekli kimlik taklidi bu açıdan maliyeti düşüren ve inandırıcılığı artıran bir araç hâline gelebilir. Bir hedefin sosyal medya paylaşımlarından toplanan açık bilgiler, kişiselleştirilmiş temas girişimlerinde kullanılabilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

9.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Risk senaryolarından biri sahte profil ve güven inşasıdır. Gerçek bir kişinin görüntüleriyle oluşturulan veya yapay zekâyla çeşitlendirilen profil, zaman içinde normal bir hesap görünümü kazanabilir. Amaç romantik dolandırıcılık, para talebi, bilgi toplama veya başka kişilere erişim olabilir. Burada mağdur hem kandırılan kişi hem de kimliği kullanılan gerçek kişi olabilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

9.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Bir diğer senaryo otorite taklididir. Yönetici, kamu görevlisi, şirket yetkilisi veya aile büyüğü gibi güven duyulan bir kişinin ses ve görüntüsünün taklit edilmesi, aciliyet hissi yaratmak için kullanılabilir. Savunma açısından kritik ilke, finansal veya hassas

işlemlerde yalnızca görüntülü görüşmeyi yeterli doğrulama kabul etmemek ve bağımsız ikinci kanal kullanmaktır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

10. SOSYAL MÜHENDİSLİK, DOLANDIRICILIK VE KİMLİK TAKLİDİ

Sosyal mühendislik, teknik bir güvenlik açığından çok insanın güven, korku, merak, otoriteye uyum ve aciliyet gibi bilişsel eğilimlerini hedefler. Yapay zekâ, saldırganın hedefe özgü mesaj üretmesini ve gerçek bir kişiyi taklit etmesini kolaylaştırabilir. Bu nedenle güvenlik farkındalığı eğitimleri yalnızca şüpheli bağlantılara değil, sentetik ses ve görüntülere de odaklanmalıdır.

Kimlik taklidinde en kritik unsur “inandırıcı bütünlük”tür. Sadece yüz benzerliği yeterli olmayabilir; isim, meslek, konuşma tarzı, sosyal çevre ve güncel olaylar da taklidi destekler. Sosyal medya bu bağlamsal malzemenin önemli bölümünü açık biçimde sunabilir. Kullanıcıların profil görünürlüğü ve eski paylaşımları bu nedenle periyodik olarak gözden geçirilmelidir.

Finansal dolandırıcılıkta doğrulama prosedürleri insan ilişkilerinden bağımsızlaştırılmalıdır. “Beni tanıyorsun” veya “kameradayım” gibi kanıtlar tek başına yeterli olmamalıdır. Kurumlarda

geri arama, işlem limiti, çift onay ve önceden tanımlı güvenli kanallar; aile içinde ise farklı kanaldan doğrulama ve kişisel güvenlik soruları gibi basit yöntemler etkili olabilir.

Kimlik taklidine karşı mağdurun hızlı hareket etmesi önemlidir: sahte hesabın veya içeriğin bağlantısını kaydetmek, ekran görüntüsü ve zaman bilgisini korumak, platforma bildirmek, çevresini uyarmak ve gerekli hâllerde yetkili mercilere başvurmak. İçeriğin öfkeyle tekrar paylaşılması ise istemeden yayılımı artırabileceğinden dikkatli olunmalıdır.

10.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Sosyal mühendislik, teknik bir güvenlik açığından çok insanın güven, korku, merak, otoriteye uyum ve aciliyet gibi bilişsel eğilimlerini hedefler. Yapay zekâ, saldırganın hedefe özgü mesaj üretmesini ve gerçek bir kişiyi taklit etmesini kolaylaştırabilir. Bu nedenle güvenlik farkındalığı eğitimleri yalnızca şüpheli bağlantılara değil, sentetik ses ve görüntülere de odaklanmalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

10.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Kimlik taklidinde en kritik unsur “inandırıcı bütünlük”tür. Sadece yüz benzerliği yeterli olmayabilir; isim, meslek, konuşma tarzı, sosyal çevre ve güncel olaylar da taklidi destekler. Sosyal medya bu bağlamsal malzemenin önemli bölümünü açık biçimde sunabilir. Kullanıcıların profil görünürlüğü ve eski paylaşımları bu nedenle periyodik olarak gözden geçirilmelidir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

10.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Finansal dolandırıcılıkta doğrulama prosedürleri insan ilişkilerinden bağımsızlaştırılmalıdır. “Beni tanıyorsun” veya “kameradayım” gibi kanıtlar tek başına yeterli olmamalıdır. Kurumlarda geri arama, işlem limiti, çift onay ve önceden tanımlı güvenli kanallar; aile içinde ise farklı kanaldan doğrulama ve kişisel güvenlik soruları gibi basit yöntemler etkili olabilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak

gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

11. DEEPFAKE ŞANTAJI, İTİBAR SALDIRILARI VE MAĞDURİYET

Deepfake tabanlı itibar saldırılarında failin amacı her zaman içeriğin uzun süre gerçek sanılması değildir. Bazen kısa süreli şüphe yaratmak bile yeterlidir. Bir yöneticinin, sağlık çalışanının, öğretmenin veya kamuya açık bir kişinin sahte görüntüsü, doğrulama tamamlanana kadar kurumsal güveni zedeleyebilir. Bu nedenle kriz iletişimi teknik inceleme kadar önemlidir.

Şantaj senaryolarında sentetik içerik, mağdura "yayınlarım" tehdidiyle baskı kurmak için kullanılabilir. İçeriğin sahte olması mağduriyetin gerçek olmadığı anlamına gelmez. Korku, aile veya iş çevresine açıklama zorunluluğu, itibar kaygısı ve maddi talepler ciddi sonuçlar doğurabilir. Kurumların mağduru suçlayıcı değil, delil koruyucu ve destekleyici prosedürler geliştirmesi gerekir.

İtibar saldırılarının başka bir boyutu "yalancının temettüsü" olarak ifade edilen durumdur: Sentetik içeriklerin yaygınlaşması, gerçek bir kayıtla karşılaşan kişinin de "bu deepfake" diyerek inkâr etmesini kolaylaştırabilir. Böylece teknoloji hem sahteyi gerçek gibi gösterebilir hem de gerçeğin güvenilirliğini aşındırabilir. Bu ikili etki toplumsal bilgi ekosistemini zorlaştırır.

Çözüm yalnızca daha iyi dedektör değildir. İçeriğin üretim kaynağını doğrulayan köken teknolojileri, platform politikaları, hızlı düzeltme mekanizmaları, hukuki başvuru yolları ve

medya okuryazarlığı birlikte gereklidir. Özellikle mağdurun gerçekliğini ispat yükünün sınırsız biçimde üzerine bırakılması adil değildir.

11.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Deepfake tabanlı itibar saldırılarında failin amacı her zaman içeriğin uzun süre gerçek sanılması değildir. Bazen kısa süreli şüphe yaratmak bile yeterlidir. Bir yöneticinin, sağlık çalışanının, öğretmenin veya kamuya açık bir kişinin sahte görüntüsü, doğrulama tamamlanana kadar kurumsal güveni zedeleyebilir. Bu nedenle kriz iletişimi teknik inceleme kadar önemlidir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

11.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Şantaj senaryolarında sentetik içerik, mağdura “yayınlarım” tehdidiyle baskı kurmak için kullanılabilir. İçeriğin sahte olması mağduriyetin gerçek olmadığı anlamına gelmez. Korku, aile veya iş çevresine açıklama zorunluluğu, itibar kaygısı ve maddi talepler ciddi sonuçlar doğurabilir. Kurumların mağduru suçlayıcı değil, delil koruyucu ve destekleyici prosedürler geliştirmesi gerekir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

11.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. İtibar saldırılarının başka bir boyutu “yalancının temettüsü” olarak ifade edilen durumdur: Sentetik içeriklerin yaygınlaşması, gerçek bir kayıtla karşılaşan kişinin de “bu deepfake” diyerek inkâr etmesini kolaylaştırabilir. Böylece teknoloji hem sahteyi gerçek gibi gösterebilir hem de gerçeğin güvenilirliğini aşındırabilir. Bu ikili etki toplumsal bilgi ekosistemini zorlaştırır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin

belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

12. ÇOCUKLAR, AİLE FOTOĞRAFLARI VE KUŞAKLARARASI DİJİTAL İZ

Çocuk fotoğrafları özel bir risk alanıdır; çünkü paylaşım kararını çoğu zaman çocuk değil yetişkin verir. Çocuğun yıllar boyunca oluşan dijital izi, ileride kendi tercihleriyle uyuşmayabilir. Yapay zekâ ile yaşlandırma veya yüz dönüşümü akımları, çocuk görüntülerinin yeni sentetik türevlerini de üretebilir.

Aile fotoğrafları ilişkisel veri taşır. Kim kimin ebeveyni, kardeşi veya yakınıdır; hangi tarihlerde bir aradadır; hangi okul, kurum veya şehirle bağlantılıdır gibi bilgiler görüntü ve açıklamalardan anlaşılabilir. Bu ilişkisel katman sosyal mühendislik açısından tekil portreden daha değerli olabilir.

Çocukların korunmasında “paylaşmadan önce düşün” ilkesi yeterli değildir; ebeveynler uygulamanın veri işleme koşullarını, görünürlük ayarlarını ve paylaşımın gerçekten gerekli olup olmadığını değerlendirmelidir. Özellikle herkese açık profillerde okul forması, konum, rutin saatler ve kimlik belgeleri gibi ek bilgilerden kaçınılmalıdır.

Kuşaklararası dijital iz, bugün verilen kararların yıllar sonra etkili olabileceğini gösterir. Bir çocuğun biyometrik özellikleri büyümeyle değişse de yüz kimliği süreklilik taşır. Bu nedenle çocuk verilerinde daha yüksek ihtiyat, daha kısa saklama ve daha güçlü varsayılan gizlilik yaklaşımı etik açıdan savunulabilir.

12.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Çocuk fotoğrafları özel bir risk alanıdır; çünkü paylaşım kararını çoğu zaman çocuk değil yetişkin verir. Çocuğun yıllar boyunca oluşan dijital izi, ileride kendi tercihleriyle uyuşmayabilir. Yapay zekâ ile yaşlandırma veya yüz dönüşümü akımları, çocuk görüntülerinin yeni sentetik türevlerini de üretebilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

12.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Aile fotoğrafları ilişkisel veri taşır. Kim kimin ebeveyni, kardeşi veya yakınıdır; hangi tarihlerde bir aradadır; hangi okul, kurum veya şehirle bağlantılıdır gibi bilgiler görüntü ve açıklamalardan anlaşılabilir. Bu ilişkisel katman sosyal mühendislik açısından tekil portreden daha değerli olabilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

12.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Çocukların korunmasında "paylaşmadan önce düşün" ilkesi yeterli değildir; ebeveynler uygulamanın veri işleme koşullarını, görünürlük ayarlarını ve paylaşımın gerçekten gerekli olup olmadığını değerlendirmelidir. Özellikle herkese açık profillerde okul forması, konum, rutin saatler ve kimlik belgeleri gibi ek bilgilerden kaçınılmalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

13. SOSYAL MEDYADA GÜVEN VE GERÇEKLİK KRİZİ

Sosyal medyanın temel sermayelerinden biri kullanıcıların gördükleri içeriğin en azından belirli bir ölçüde gerçek dünyayla bağlantılı olduğuna dair varsayımdır. Sentetik medya bu varsayımı zayıflatmaktadır. Kullanıcı artık yalnızca "Bu doğru mu?" değil, "Bunun gerçekliğini hangi kanıtla doğrulayabilirim?" sorusunu sormak zorundadır.

Gerçeklik krizi iki yönlüdür. Birinci yönde sahte içerik gerçek sanılır; ikinci yönde gerçek içerik sahte olduğu iddiasıyla reddedilir. Bu durum gazetecilik, adli süreçler, kurumsal iletişim ve bireysel ilişkiler için yeni doğrulama maliyetleri yaratır. Sosyal medya platformlarının içerik kökeni ve manipülasyon etiketleri bu nedenle giderek daha önemli hâle gelmektedir.

Güven kaybı platformdan bireye de yayılır. Bir kişinin hesabı ele geçirilmemiş olsa bile adına açılmış sahte hesaplar veya yapay zekâyla üretilmiş içerikler çevresindeki insanların güvenini sarsabilir. Böylece hesap güvenliği ile kimlik güvenliği arasındaki fark görünür hâle gelir.

Uzun vadede çözüm, kullanıcıyı her görüntüden şüphe eden bir duruma sürüklemek değildir. Amaç doğrulanabilirlik altyapısı kurmaktır. Kaynak işaretleri, güvenilir hesap doğrulaması, şeffaf yapay zekâ etiketleri ve bağımsız doğrulama kanalları güveni yeniden kurmanın bileşenleri olabilir.

13.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Sosyal medyanın temel sermayelerinden biri kullanıcıların gördükleri içeriğin en azından belirli bir ölçüde gerçek dünyayla bağlantılı olduğuna dair varsayımdır. Sentetik medya bu varsayımı zayıflatmaktadır. Kullanıcı artık yalnızca “Bu doğru mu?” değil, “Bunun gerçekliğini hangi kanıtla doğrulayabilirim?” sorusunu sormak zorundadır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık,

anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

13.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Gerçeklik krizi iki yönlüdür. Birinci yönde sahte içerik gerçek sanılır; ikinci yönde gerçek içerik sahte olduğu iddiasıyla reddedilir. Bu durum gazetecilik, adli süreçler, kurumsal iletişim ve bireysel ilişkiler için yeni doğrulama maliyetleri yaratır. Sosyal medya platformlarının içerik kökeni ve manipülasyon etiketleri bu nedenle giderek daha önemli hâle gelmektedir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

13.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Güven kaybı platformdan bireye de yayılır. Bir kişinin hesabı ele geçirilmemiş olsa bile adına açılmış sahte hesaplar veya yapay zekâyla üretilmiş içerikler çevresindeki insanların güvenini sarsabilir. Böylece hesap güvenliği ile kimlik güvenliği arasındaki fark görünür hâle gelir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

14. 6698 SAYILI KANUN AÇISINDAN HUKUKİ DEĞERLENDİRME

6698 sayılı Kişisel Verilerin Korunması Kanunu bakımından yapay zekâ fotoğraf akımlarının değerlendirilmesi, her somut veri işleme faaliyetinin ayrı incelenmesini gerektirir. Bir görüntünün yüklenmesi, saklanması, analiz edilmesi, başka bir hizmete aktarılması, model geliştirmede kullanılması veya kimlik doğrulama amacıyla özellik çıkarımına tabi tutulması farklı hukuki sorular doğurur.

Kanunun temel yaklaşımı kişisel verilerin hukuka ve dürüstlük kurallarına uygun, doğru ve gerektiğinde güncel, belirli-açık-meşru amaçlarla, işlendikleri amaçla bağlantılı-sınırlı-ölçülü ve gerekli süre kadar muhafaza edilerek işlenmesini gerektirir. Yapay zekâ hizmetlerinde özellikle amaç belirliliği ve ölçülülük önem kazanır; çünkü teknik olarak yapılabilen her işlem hukuken gerekli veya ölçülü olmayabilir.

Kullanıcı fotoğraf yükledi diye her türlü ikincil kullanıma sınırsız onay vermiş sayılmamalıdır. Veri işleme şartının ne olduğu, aydınlatmanın anlaşılır olup olmadığı, hizmetin asıl amacıyla model eğitimi veya başka ikincil amaçların ayrıştırılıp ayrıştırılmadığı incelenmelidir. Rıza gerekiyorsa rızanın özgür iradeye dayanması ve belirli olması önem taşır.

Bu nedenle çalışmanın hukuki sonucu “tüm yapay zekâ fotoğraf uygulamaları 6698 sayılı Kanunu ihlal eder” şeklinde kurulamaz. Daha doğru sonuç, rızasız veya hukuki işleme şartı bulunmayan toplama, amaç dışı kullanım, gereğinden fazla veri işleme, şeffaf olmayan aktarım ve yetersiz güvenlik gibi uygulamaların ciddi hukuka aykırılık riski taşıdığıdır.

14.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu bakımından yapay zekâ fotoğraf akımlarının değerlendirilmesi, her somut veri işleme faaliyetinin ayrı incelenmesini gerektirir. Bir görüntünün yüklenmesi, saklanması, analiz edilmesi, başka bir hizmete aktarılması, model geliştirmede kullanılması veya kimlik doğrulama amacıyla özellik çıkarımına tabi tutulması farklı hukuki sorular doğurur.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

14.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Kanunun temel yaklaşımı kişisel verilerin hukuka ve dürüstlük kurallarına uygun, doğru ve gerektiğinde güncel, belirli-açık-meşru amaçlarla, işlendikleri amaçla bağlantılı-sınırlı-ölçülü ve gerekli süre kadar muhafaza edilerek işlenmesini gerektirir. Yapay

zekâ hizmetlerinde özellikle amaç belirliliği ve ölçülülük önem kazanır; çünkü teknik olarak yapılabilen her işlem hukuken gerekli veya ölçülü olmayabilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

14.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Kullanıcı fotoğraf yükledi diye her türlü ikincil kullanıma sınırsız onay vermiş sayılmamalıdır. Veri işleme şartının ne olduğu, aydınlatmanın anlaşılır olup olmadığı, hizmetin asıl amacıyla model eğitimi veya başka ikincil amaçların ayrıştırılıp ayrıştırılmadığı incelenmelidir. Rıza gerekiyorsa rızanın özgür iradeye dayanması ve belirli olması önem taşır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin

belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

15. AÇIK RIZA, AYDINLATMA VE AMAÇLA SINIRLILIK

Açık rıza, kullanıcı deneyiminde çoğu zaman uzun kullanım koşullarına verilen tek bir onaya indirgenmektedir. Oysa veri koruma mantığında rızanın belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan bir irade beyanı olması gerekir. Görsel işleme hizmetlerinde "fotoğrafımı dönüştür" talebi ile "fotoğrafımı gelecekte model geliştirmede kullan" tercihi aynı amaç olmayabilir.

Aydınlatmanın niteliği de önemlidir. Teknik olarak erişilebilir bir metnin varlığı, kullanıcının veri akışını gerçekten anlayabildiği anlamına gelmez. Katmanlı aydınlatma, kısa özetler, saklama süresinin açık gösterimi, üçüncü taraf aktarımının anlaşılır biçimde belirtilmesi ve silme seçeneklerinin görünür olması daha güvenli tasarım örnekleridir.

Amaçla sınırlılık ilkesi, veri toplama anında belirtilen amaçla sonraki kullanım arasında bağ kurulmasını gerektirir. Eğlence amaçlı filtre için yüklenen görüntünün farklı bir kimlik analizi amacıyla kullanılması, ayrıca değerlendirilmesi gereken bir işlem olabilir. Aynı şekilde hizmetin gerektirmediği konum, rehber veya cihaz verilerine erişim talep edilmesi ölçülülük sorunu doğurabilir.

Kullanıcı kontrolünün gerçek olması gerekir. Silme, hesap kapatma veya model geliştirmeye katılmama seçenekleri varsa bunların karmaşık menülerde gizlenmemesi önemlidir. Tasarımın kullanıcıyı daha fazla veri vermeye zorlayan karanlık örüntüler yerine veri minimizasyonunu teşvik etmesi gerekir.

15.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Açık rıza, kullanıcı deneyiminde çoğu zaman uzun kullanım koşullarına verilen tek bir onaya indirgenmektedir. Oysa veri koruma mantığında rızanın belirli bir konuya

ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan bir irade beyanı olması gerekir. Görsel işleme hizmetlerinde “fotoğrafımı dönüştür” talebi ile “fotoğrafımı gelecekte model geliştirmede kullan” tercihi aynı amaç olmayabilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

15.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Aydınlatmanın niteliği de önemlidir. Teknik olarak erişilebilir bir metnin varlığı, kullanıcının veri akışını gerçekten anlayabildiği anlamına gelmez. Katmanlı aydınlatma, kısa özetler, saklama süresinin açık gösterimi, üçüncü taraf aktarımının anlaşılır biçimde belirtilmesi ve silme seçeneklerinin görünür olması daha güvenli tasarım örnekleridir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli

yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

15.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Amaçla sınırlılık ilkesi, veri toplama anında belirtilen amaçla sonraki kullanım arasında bağ kurulmasını gerektirir. Eğlence amaçlı filtre için yüklenen görüntünün farklı bir kimlik analizi amacıyla kullanılması, ayrıca değerlendirilmesi gereken bir işlem olabilir. Aynı şekilde hizmetin gerektirmediği konum, rehber veya cihaz verilerine erişim talep edilmesi ölçülülük sorunu doğurabilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

16. BİYOMETRİK VERİ VE YÜZ GÖRÜNTÜLERİNİN HUKUKİ NİTELİĞİ

Yüz görüntüsünün hukuki niteliği konusunda en önemli akademik hassasiyet, fotoğraf ile biyometrik şablonu birbirine eşitlememektir. Fotoğraf bir kişiyi belirlenebilir kılıyorsa kişisel veri olabilir. Ancak biyometrik veri niteliği, genellikle fiziksel, fizyolojik veya davranışsal özelliklerin belirli teknik işlemlerle kişinin benzersiz biçimde tanımlanması veya doğrulanması amacıyla işlenmesi bağlamında ortaya çıkar.

Bu ayrım, riskin küçümsenmesi anlamına gelmez. Tam tersine, sıradan bir fotoğrafın daha sonra biyometrik işleme tabi tutulabilmesi, veri yaşam döngüsünü önemli hâle getirir. Kullanıcının yüklediği ham görüntünün hangi teknik dönüşümlerden geçtiği ve bu dönüşümlerin kalıcı olup olmadığı şeffaf olmalıdır.

Yüz şablonları veya benzer matematiksel temsiller, doğrudan insan gözüyle okunabilir olmayabilir; ancak kişileri eşleştirme kapasitesi taşıyabilir. Bu nedenle güvenlik ihlali hâlinde yalnızca fotoğraf dosyasının sızması değil, türetilmiş temsilin sızması da dikkate alınmalıdır. Saklama, erişim kontrolü ve şifreleme politikaları bu türetilmiş verileri de kapsamalıdır.

Biyometrik işlemede ölçülülük ayrıca kritik bir ilkedir. Aynı amaç daha az müdahaleci bir yöntemle gerçekleştirilebiliyorsa biyometrik yöntemin zorunluluğu sorgulanmalıdır. Eğlence amaçlı bir hizmette kalıcı kimlik doğrulama şablonuna gerçekten ihtiyaç olup olmadığı bu çerçevede sorulabilecek temel sorulardan biridir.

16.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Yüz görüntüsünün hukuki niteliği konusunda en önemli akademik hassasiyet, fotoğraf ile biyometrik şablonu birbirine eşitlememektir. Fotoğraf bir kişiyi belirlenebilir kılıyorsa kişisel veri olabilir. Ancak biyometrik veri niteliği, genellikle fiziksel, fizyolojik veya davranışsal özelliklerin belirli teknik işlemlerle kişinin benzersiz biçimde tanımlanması veya doğrulanması amacıyla işlenmesi bağlamında ortaya çıkar.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

16.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Bu ayrım, riskin küçümsenmesi anlamına gelmez. Tam tersine, sıradan bir fotoğrafın daha sonra biyometrik işleme tabi tutulabilmesi, veri yaşam döngüsünü önemli hâle getirir. Kullanıcının yüklediği ham görüntünün hangi teknik dönüşümlerden geçtiği ve bu dönüşümlerin kalıcı olup olmadığı şeffaf olmalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

16.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Yüz şablonları veya benzer matematiksel temsiller, doğrudan insan gözüyle okunabilir olmayabilir; ancak kişileri eşleştirme kapasitesi taşıyabilir. Bu nedenle güvenlik ihlali hâlinde yalnızca fotoğraf dosyasının sızması değil, türetilmiş temsilin sızması da dikkate alınmalıdır. Saklama, erişim kontrolü ve şifreleme politikaları bu türetilmiş verileri de kapsamalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

17. PLATFORMLARIN VE YAPAY ZEKÂ HİZMET SAĞLAYICILARININ SORUMLULUĞU

Platform güvenliği yalnızca zararlı içeriği kaldırmakla sınırlı değildir. Tasarım aşamasında veri minimizasyonu, güvenli varsayılanlar, erişim kontrolü, saklama sınırları ve şeffaflık mekanizmaları kurulmalıdır. Sentetik medya için açık etiketleme ve kullanıcıların taklit/izinsiz kullanım şikâyetlerini hızlı iletebileceği kanallar önemlidir.

Yapay zekâ hizmet sağlayıcıları açısından veri zinciri karmaşık olabilir: uygulama geliştiricisi, bulut sağlayıcısı, model sağlayıcısı, analiz hizmeti ve içerik dağıtım altyapısı farklı kuruluşlar

olabilir. Kullanıcı bakımından bu zincirin anlaşılır hâle getirilmesi, hangi tarafın hangi amaçla veri işlediğinin açıklanması gerekir.

Şikâyet mekanizmasının etkili olması özellikle kimlik taklidi vakalarında kritiktir. Mağdurun sahte hesabı veya deepfake içeriği bildirirken uzun ve belirsiz süreçlerle karşılaşması, zararın büyümesine yol açabilir. Yüksek riskli bildirimlerde önceliklendirme, geçici görünürlük sınırlaması ve hızlı inceleme mekanizmaları düşünülebilir.

Platformların içerik doğrulama sorumluluğu ifade özgürlüğü ve yanlış pozitif riskleriyle dengelenmelidir. Otomatik sistemlerin her manipüle içeriği kötü niyetli sayması doğru değildir. Parodi, sanat ve açıkça etiketlenmiş kurgu ile aldatıcı kimlik taklidi arasında bağlam temelli ayrım yapılmalıdır.

17.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Platform güvenliği yalnızca zararlı içeriği kaldırmakla sınırlı değildir. Tasarım aşamasında veri minimizasyonu, güvenli varsayılanlar, erişim kontrolü, saklama sınırları ve şeffaflık mekanizmaları kurulmalıdır. Sentetik medya için açık etiketleme ve kullanıcıların taklit/izinsiz kullanım şikâyetlerini hızlı iletebileceği kanallar önemlidir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

17.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Yapay zekâ hizmet sağlayıcıları açısından veri zinciri karmaşık olabilir: uygulama geliştiricisi, bulut sağlayıcısı, model sağlayıcısı, analiz hizmeti ve içerik dağıtım altyapısı farklı kuruluşlar olabilir. Kullanıcı bakımından bu zincirin anlaşılır hâle getirilmesi, hangi tarafın hangi amaçla veri işlediğinin açıklanması gerekir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

17.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Şikâyet mekanizmasının etkili olması özellikle kimlik taklidi vakalarında kritiktir. Mağdurun sahte hesabı veya deepfake içeriği bildirirken uzun ve belirsiz süreçlerle karşılaşması, zararın büyümesine yol açabilir. Yüksek riskli bildirimlerde önceliklendirme, geçici görünürlük sınırlaması ve hızlı inceleme mekanizmaları düşünülebilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi

yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

18. KURUMSAL RİSKLER VE KAMU KURUMLARI AÇISINDAN DEĞERLENDİRME

Kurumsal düzeyde deepfake riski, üst yönetici taklidi ve sahte talimatların ötesine geçer. Kurumun çalışanları, bina görüntüleri, kimlik kartları, toplantı ekranları ve sosyal medya paylaşımları saldırganlara bağlamsal malzeme sağlayabilir. Bu nedenle kurumsal sosyal medya politikası yalnızca kurumsal hesabın yönetimini değil, hassas görsel bilgilerin paylaşımını da kapsamalıdır.

Kamu kurumlarında güven boyutu daha kritiktir; çünkü sahte bir duyuru veya yönetici videosu geniş kitleleri etkileyebilir. Resmî iletişim kanallarının önceden tanımlanması, önemli duyuruların birden fazla doğrulanabilir kanaldan yayımlanması ve kriz anında tek merkezli doğrulama sayfası kullanılması faydalıdır.

Çalışan farkındalığı eğitimlerinde “görüntülü arama gerçeklik kanıtıdır” varsayımı terk edilmelidir. Para transferi, erişim yetkisi, parola sıfırlama, kritik sistem değişikliği veya hassas veri paylaşımı gibi işlemler için prosedür dışı görüntülü talimat yeterli kabul edilmemelidir.

Kurumsal olay müdahale planlarında sentetik medya vakası için ayrı bir alt süreç bulunabilir: içeriğin korunması, teknik inceleme, hukuk ve iletişim ekiplerinin koordinasyonu, platform bildirimi, etkilenen kişilerin bilgilendirilmesi ve gerektiğinde kolluk/yargı süreçlerine uygun delil muhafazası.

18.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Kurumsal düzeyde deepfake riski, üst yönetici taklidi ve sahte talimatların ötesine geçer. Kurumun çalışanları, bina görüntüleri, kimlik kartları, toplantı ekranları ve sosyal medya paylaşımları saldırganlara bağlamsal malzeme sağlayabilir. Bu nedenle kurumsal sosyal medya politikası yalnızca kurumsal hesabın yönetimini değil, hassas görsel bilgilerin paylaşımını da kapsamalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

18.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Kamu kurumlarında güven boyutu daha kritiktir; çünkü sahte bir duyuru veya yönetici videosu geniş kitleleri etkileyebilir. Resmî iletişim kanallarının önceden tanımlanması, önemli duyuruların birden fazla doğrulanabilir kanaldan yayımlanması ve kriz anında tek merkezli doğrulama sayfası kullanılması faydalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi

yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

18.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Çalışan farkındalığı eğitimlerinde “görüntülü arama gerçeklik kanıtıdır” varsayımı terk edilmelidir. Para transferi, erişim yetkisi, parola sıfırlama, kritik sistem değişikliği veya hassas veri paylaşımı gibi işlemler için prosedür dışı görüntülü talimat yeterli kabul edilmemelidir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık,

anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

19. TEKNİK VE İDARİ GÜVENLİK ÖNLEMLERİ

Bireysel düzeyde ilk önlem veri minimizasyonudur. Kullanıcı, yapay zekâ hizmetine mümkün olan en az sayıda ve en düşük gereklilik düzeyinde görsel vermelidir. Kimlik belgesi, kart, adres, okul, plaka veya kurum içi bilgi içeren arka planlar temizlenmeli; gereksiz meta veriler paylaşılmamalıdır.

İkinci önlem hesap güvenliğidir: benzersiz parola, çok faktörlü kimlik doğrulama, kurtarma kanallarının güncelliği ve oturum kontrolü. Bunlar deepfake'i doğrudan engellemez; fakat sahte içerikle birlikte gerçek hesabın ele geçirilmesi hâlinde oluşacak birleşik zararı azaltır.

Kurumsal düzeyde rol tabanlı erişim, kayıt tutma, veri sınıflandırma, saklama politikası, tedarikçi değerlendirmesi ve olay müdahale planı gereklidir. Yapay zekâ hizmeti satın alınırken yalnızca model kalitesi değil, veri konumu, alt işleyenler, silme mekanizması, model eğitiminde kullanım ve güvenlik sertifikasyonları da değerlendirilmelidir.

İçerik kökeni ve filigran teknolojileri yardımcı olabilir; ancak tek başına mutlak çözüm değildir. Filigran kaybolabilir, meta veri silinebilir veya içerik yeniden kodlanabilir. Bu nedenle katmanlı güvenlik yaklaşımı benimsenmeli; teknik işaretler bağlamsal doğrulama ve kurumsal prosedürlerle desteklenmelidir.

19.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Bireysel düzeyde ilk önlem veri minimizasyonudur. Kullanıcı, yapay zekâ hizmetine mümkün olan en az sayıda ve en düşük gereklilik düzeyinde görsel vermelidir. Kimlik belgesi, kart, adres, okul, plaka veya kurum içi bilgi içeren arka planlar temizlenmeli; gereksiz meta veriler paylaşılmamalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

19.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. İkinci önlem hesap güvenliğidir: benzersiz parola, çok faktörlü kimlik doğrulama, kurtarma kanallarının güncelliği ve oturum kontrolü. Bunlar deepfake'i doğrudan engellemez; fakat sahte içerikle birlikte gerçek hesabın ele geçirilmesi hâlinde oluşacak birleşik zararı azaltır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

19.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Kurumsal düzeyde rol tabanlı erişim, kayıt tutma, veri sınıflandırma, saklama politikası, tedarikçi değerlendirmesi ve olay müdahale planı gereklidir. Yapay zekâ hizmeti satın alınırken yalnızca model kalitesi değil, veri konumu, alt işleyenler, silme mekanizması, model eğitiminde kullanım ve güvenlik sertifikasyonları da değerlendirilmelidir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

20. TÜRKİYE İÇİN YAPAY ZEKÂ GÖRSEL GÜVENLİĞİ MODELİ

Türkiye için önerilen model beş katmandan oluşmaktadır: bireysel farkındalık, hizmet sağlayıcı tasarımı, platform yönetişimi, kurumsal dayanıklılık ve hukuki/idarî gözetim. Katmanların birbirini tamamlaması gerekir; yalnızca kullanıcıyı bilinçlendirmek veya yalnızca platformu sorumlu tutmak yeterli değildir.

Birinci katmanda vatandaşlara dijital kimlik okuryazarlığı kazandırılmalıdır. Yüz ve sesin parola gibi değiştirilebilir olmadığı, fotoğraf akımlarında veri minimizasyonunun önemi, sentetik içerik doğrulama yöntemleri ve mağduriyet hâlinde başvuru yolları anlaşılır biçimde anlatılmalıdır.

İkinci ve üçüncü katmanda hizmet sağlayıcılar ile platformlar, yüksek riskli yüz/ses işleme özellikleri için açık ve kısa bilgilendirme, varsayılan kısa saklama, kolay silme, model eğitimine ilişkin ayrı tercihler ve kimlik taklidi bildirimlerinde hızlı işlem sunmalıdır. Sentetik içerik etiketleri kullanıcıyı yanıltmayacak biçimde standardize edilebilir.

Dördüncü ve beşinci katmanda kamu ve özel sektör kurumları deepfake olay müdahale prosedürleri geliştirmeli; düzenleyici yaklaşım ise teknolojik nötrlük, ölçülülük ve temel hak dengesi üzerinde kurulmalıdır. Amaç inovasyonu engellemek değil, kimlik güvenliğini tasarımın doğal bir parçası hâline getirmektir.

20.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Türkiye için önerilen model beş katmandan oluşmaktadır: bireysel farkındalık, hizmet sağlayıcı tasarımı, platform yönetişimi, kurumsal dayanıklılık ve hukuki/idarî gözetim. Katmanların birbirini tamamlaması gerekir; yalnızca kullanıcıyı bilinçlendirmek veya yalnızca platformu sorumlu tutmak yeterli değildir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

20.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Birinci katmanda vatandaşlara dijital kimlik okuryazarlığı kazandırılmalıdır. Yüz ve sesin parola gibi değiştirilebilir olmadığı, fotoğraf akımlarında veri minimizasyonunun önemi, sentetik içerik doğrulama yöntemleri ve mağduriyet hâlinde başvuru yolları anlaşılır biçimde anlatılmalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

20.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. İkinci ve üçüncü katmanda hizmet sağlayıcılar ile platformlar, yüksek riskli yüz/ses işleme özellikleri için açık ve kısa bilgilendirme, varsayılan kısa saklama, kolay silme, model eğitimine ilişkin ayrı tercihler ve kimlik taklidi bildirimlerinde hızlı işlem sunmalıdır. Sentetik içerik etiketleri kullanıcıyı yanıltmayacak biçimde standardize edilebilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi

yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

21. TARTIŞMA

Yapay zekâ fotoğraf akımlarına ilişkin tartışmanın iki uç arasında sıkışması verimsizdir. Bir uç tüm uygulamaları tehlikeli ve yasaklanması gereken araçlar olarak görürken, diğer uç kullanıcı rızasını her riski ortadan kaldıran mutlak bir meşruiyet gibi değerlendirebilir. Oysa güvenlik ve hukuk açısından bağlam, amaç, veri miktarı, saklama, aktarım ve kullanıcı beklentisi birlikte ele alınmalıdır.

Teknolojik ilerleme tespit araçlarıyla üretim araçları arasında sürekli bir yarış yaratmaktadır. Bugün kolayca tespit edilen bir sentetik içerik yarın daha gerçekçi üretilebilir. Bu nedenle dayanıklı çözüm, sadece “sahteyi bulmak” değil, “gerçeğin kökenini kanıtlamak” yönünde gelişmelidir. Dijital imza, içerik kökeni kayıtları ve güvenilir yayın kanalları bu dönüşümün parçalarıdır.

6698 sayılı Kanun bağlamında da yapay zekâ ayrı bir hukuk evreni yaratmamaktadır; mevcut veri koruma ilkeleri yeni teknik süreçlere uygulanmaya devam eder. Ancak uygulama karmaşıklığı arttıkça kullanıcıların gerçek anlamda bilgilendirilmesi zorlaşmaktadır. Bu nedenle şeffaflık, sadece hukuki metin yayımlamak değil, veri akışını anlaşılır tasarlamak olarak ele alınmalıdır.

Toplumsal açıdan en ciddi risklerden biri güven erozyonudur. İnsanlar gerçek görüntülere de güvenmemeye başladığında kamu iletişimi, medya, adalet ve kişilerarası ilişkiler etkilenir. Bu

nedenle sentetik medya güvenliği bir siber güvenlik alt konusu olmanın yanında toplumsal güven politikası olarak da değerlendirilmelidir.

21.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Yapay zekâ fotoğraf akımlarına ilişkin tartışmanın iki uç arasında sıkışması verimsizdir. Bir uç tüm uygulamaları tehlikeli ve yasaklanması gereken araçlar olarak görürken, diğer uç kullanıcı rızasını her riski ortadan kaldıran mutlak bir meşruiyet gibi değerlendirebilir. Oysa güvenlik ve hukuk açısından bağlam, amaç, veri miktarı, saklama, aktarım ve kullanıcı beklentisi birlikte ele alınmalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

21.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Teknolojik ilerleme tespit araçlarıyla üretim araçları arasında sürekli bir yarış yaratmaktadır. Bugün kolayca tespit edilen bir sentetik içerik yarın daha gerçekçi üretilebilir. Bu nedenle dayanıklı çözüm, sadece “sahteyi bulmak” değil, “gerçeğin kökenini kanıtlamak” yönünde gelişmelidir. Dijital imza, içerik kökeni kayıtları ve güvenilir yayın kanalları bu dönüşümün parçalarıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

21.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. 6698 sayılı Kanun bağlamında da yapay zekâ ayrı bir hukuk evreni yaratmamaktadır; mevcut veri koruma ilkeleri yeni teknik süreçlere uygulanmaya devam eder. Ancak uygulama karmaşıklığı arttıkça kullanıcıların gerçek anlamda bilgilendirilmesi zorlaşmaktadır. Bu nedenle şeffaflık, sadece hukuki metin yayımlamak değil, veri akışını anlaşılır tasarlamak olarak ele alınmalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin

belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

22. SONUÇ VE ÖNERİLER

Bu çalışma, yapay zekâ tabanlı fotoğraf ve video akımlarının eğlence ve yaratıcılık potansiyelinin yanında yeni bir dijital kimlik güvenliği problemi yarattığını ortaya koymaktadır. Riskin kaynağı yalnızca bir fotoğrafın internete yüklenmesi değildir; görüntünün analiz edilebilir, yeniden üretilebilir, başka bağlamlara taşınabilir ve gerçek kişiyi taklit eden sentetik içeriklere dönüştürülebilir olmasıdır.

Sosyal medya güvenliği bu nedenle parola güvenliğinin ötesine geçmelidir. Yüz, ses, davranışsal özellikler, sosyal bağlam ve geçmiş paylaşımlar bir araya geldiğinde kişinin dijital ikizi sayılabilecek zengin bir temsil oluşabilir. Suç ve suç örgütleri bu temsili sosyal mühendislik, dolandırıcılık, şantaj, sahte profil, otorite taklidi ve itibar saldırılarında kullanabilir.

6698 sayılı Kanun açısından kategorik genellemelerden kaçınılmalıdır. Her fotoğraf biyometrik veri değildir ve her yapay zekâ işlemi hukuka aykırı sayılamaz. Buna karşılık kişisel verilerin hukuki işleme şartı olmaksızın toplanması, amaç dışı kullanılması, gereğinden fazla tutulması, şeffaf olmayan biçimde aktarılması veya yetersiz güvenlikle korunması ciddi uyum sorunları doğurabilir. Benzersiz tanımlama/doğrulama amacıyla özel teknik işlem gören yüz verileri ise daha yüksek hassasiyetle ele alınmalıdır.

Sonuç olarak önerilen yaklaşım “yapay zekâdan kaçınmak” değil, “yapay zekâyı kimlik güvenliğiyle birlikte tasarlamak”tır. Bireylerin veri minimizasyonu alışkanlığı kazanması; kurumların ikinci kanal doğrulama ve sentetik medya olay müdahalesi kurması; platformların hızlı kimlik taklidi bildirimi ve içerik kökeni mekanizmaları geliştirmesi; hizmet sağlayıcıların saklama ve ikincil kullanım politikalarını sadeleştirmesi gerekmektedir. Dijital kimliğin

korunması, önümüzdeki dönemde kişisel veri güvenliğinin en önemli başlıklarından biri olacaktır.

22.1 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Bu çalışma, yapay zekâ tabanlı fotoğraf ve video akımlarının eğlence ve yaratıcılık potansiyelinin yanında yeni bir dijital kimlik güvenliği problemi yarattığını ortaya koymaktadır. Riskin kaynağı yalnızca bir fotoğrafın internete yüklenmesi değildir; görüntünün analiz edilebilir, yeniden üretilebilir, başka bağlamlara taşınabilir ve gerçek kişiyi taklit eden sentetik içeriklere dönüştürülebilir olmasıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

22.2 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. Sosyal medya güvenliği bu nedenle parola güvenliğinin ötesine geçmelidir. Yüz, ses, davranışsal özellikler, sosyal bağlam ve geçmiş paylaşımlar bir araya geldiğinde kişinin dijital ikizi sayılabilecek zengin bir temsil oluşabilir. Suç ve suç örgütleri bu temsili sosyal mühendislik, dolandırıcılık, şantaj, sahte profil, otorite taklidi ve itibar saldırılarında kullanabilir.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

22.3 Derinleştirilmiş Değerlendirme

Bu alt başlık altında konu, riskin oluşma koşulları, etkisi ve azaltım seçenekleri bakımından derinleştirilmektedir. 6698 sayılı Kanun açısından kategorik genellemelerden kaçınılmalıdır. Her fotoğraf biyometrik veri değildir ve her yapay zekâ işlemi hukuka aykırı sayılamaz. Buna karşılık kişisel verilerin hukuki işleme şartı olmaksızın toplanması, amaç dışı kullanılması, gereğinden fazla tutulması, şeffaf olmayan biçimde aktarılması veya yetersiz güvenlikle korunması ciddi uyum sorunları doğurabilir. Benzersiz tanımlama/doğrulama amacıyla özel teknik işlem gören yüz verileri ise daha yüksek hassasiyetle ele alınmalıdır.

Risk değerlendirmesinde olasılık ve etki birbirinden ayrılmalıdır. Bir olayın teknik olarak mümkün olması, mutlaka yaygın biçimde gerçekleşeceği anlamına gelmez; ancak gerçekleştiğinde geri döndürülmesi güç sonuçlar doğuruyorsa koruyucu önlemlerin seviyesi yükseltilmelidir. Özellikle yüz ve ses gibi kalıcı kimlik göstergelerinde ihtiyat ilkesi, düşük maliyetli önlemlerin erken uygulanmasını destekler.

Ayrıca veri zincirinin parçalı yapısı göz önünde bulundurulmalıdır. Kullanıcı, uygulama arayüzünde tek bir hizmet görse de arka planda farklı altyapı sağlayıcıları bulunabilir. Güvenli yönetişim; sorumlulukların tanımlanması, erişimlerin sınırlandırılması, saklama süresinin

belirlenmesi, olay kayıtlarının tutulması ve kullanıcı taleplerinin izlenebilir biçimde yerine getirilmesini gerektirir.

Toplumsal boyutta ise çözümün korku üretmemesi önemlidir. Amaç, kullanıcıyı tüm yapay zekâ araçlarından uzaklaştırmak değil, risk temelli seçim yapabilmesini sağlamaktır. Şeffaflık, anlaşılır izinler, güvenli varsayılanlar ve bağımsız doğrulama kanalları teknolojinin faydalarından yararlanırken maruziyeti azaltabilir.

23. RİSK SENARYOLARI VE VAKA MODELLEMESİ

Sahte Yönetici Görüşmesi

Bir çalışan, yöneticisine benzeyen görüntü ve sesle yapılan çevrimiçi görüşmede acil işlem talebi alır. Risk, görüntünün gerçek kabul edilmesidir. Koruma: prosedür dışı finansal/hassas taleplerde ikinci kanal doğrulama, çift onay ve işlem limiti.

Bu senaryoda mağduriyetin erken belirtileri arasında tanımadık kişilerden gelen doğrulama soruları, olağandışı hesap bildirimleri, kişinin çevresinden “bu hesap sana mı ait?” mesajları ve bağlam dışı içeriklerin dolaşıma girmesi sayılabilir. Olay müdahalesinde panik yerine kanıtların korunması, hesapların güvenliğinin kontrol edilmesi, ilgili kişilerin bilgilendirilmesi ve resmî başvuru kanallarının kullanılması esastır.

Senaryo aynı zamanda veri minimizasyonunun önemini göstermektedir. Saldırganın ikna edici bir kurgu oluşturması için gerekli bağlamsal parçalar ne kadar azsa saldırının maliyeti o kadar yükselir. Bu, tüm sosyal medya kullanımının bırakılması gerektiği anlamına gelmez; ancak kimlik, aile, kurum ve rutin bilgilerinin gereksiz biçimde bir arada sunulmaması yararlı bir savunmadır.

Sahte Sosyal Medya Profili

Gerçek kişinin kamuya açık fotoğrafları kullanılarak yeni bir profil oluşturulur ve çevresindeki kişilere ulaşılır. Koruma: görünürlük ayarları, doğrulanmış iletişim kanalı, hızlı sahte hesap bildirimi ve çevrenin uyarılması.

Bu senaryoda mağduriyetin erken belirtileri arasında tanımadık kişilerden gelen doğrulama soruları, olağandışı hesap bildirimleri, kişinin çevresinden “bu hesap sana mı ait?” mesajları ve bağlam dışı içeriklerin dolaşıma girmesi sayılabilir. Olay müdahalesinde panik yerine kanıtların

korunması, hesapların güvenliğinin kontrol edilmesi, ilgili kişilerin bilgilendirilmesi ve resmî başvuru kanallarının kullanılması esastır.

Senaryo aynı zamanda veri minimizasyonunun önemini göstermektedir. Saldırganın ikna edici bir kurgu oluşturması için gerekli bağlamsal parçalar ne kadar azsa saldırının maliyeti o kadar yükselir. Bu, tüm sosyal medya kullanımının bırakılması gerektiği anlamına gelmez; ancak kimlik, aile, kurum ve rutin bilgilerinin gereksiz biçimde bir arada sunulmaması yararlı bir savunmadır.

Sentetik İtibar Saldırısı
Kişinin söylemediği sözleri söylüyormuş gibi gösteren kısa video dolaşıma sokulur. Koruma: orijinal kaynak doğrulaması, kurumsal hızlı açıklama, delil koruma ve platform bildirim süreci.

Bu senaryoda mağduriyetin erken belirtileri arasında tanımadık kişilerden gelen doğrulama soruları, olağandışı hesap bildirimleri, kişinin çevresinden “bu hesap sana mı ait?” mesajları ve bağlam dışı içeriklerin dolaşıma girmesi sayılabilir. Olay müdahalesinde panik yerine kanıtların korunması, hesapların güvenliğinin kontrol edilmesi, ilgili kişilerin bilgilendirilmesi ve resmî başvuru kanallarının kullanılması esastır.

Senaryo aynı zamanda veri minimizasyonunun önemini göstermektedir. Saldırganın ikna edici bir kurgu oluşturması için gerekli bağlamsal parçalar ne kadar azsa saldırının maliyeti o kadar yükselir. Bu, tüm sosyal medya kullanımının bırakılması gerektiği anlamına gelmez; ancak kimlik, aile, kurum ve rutin bilgilerinin gereksiz biçimde bir arada sunulmaması yararlı bir savunmadır.

Aile Üyesi Taklidi
Aile fotoğrafları ve açık paylaşımlardan elde edilen bağlam, acil para talebini inandırıcı hâle getirir. Koruma: aile içinde önceden belirlenen doğrulama yöntemi ve farklı kanaldan geri arama.

Bu senaryoda mağduriyetin erken belirtileri arasında tanımadık kişilerden gelen doğrulama soruları, olağandışı hesap bildirimleri, kişinin çevresinden “bu hesap sana mı ait?” mesajları ve bağlam dışı içeriklerin dolaşıma girmesi sayılabilir. Olay müdahalesinde panik yerine kanıtların korunması, hesapların güvenliğinin kontrol edilmesi, ilgili kişilerin bilgilendirilmesi ve resmî başvuru kanallarının kullanılması esastır.

Senaryo aynı zamanda veri minimizasyonunun önemini göstermektedir. Saldırganın ikna edici bir kurgu oluşturması için gerekli bağlamsal parçalar ne kadar azsa saldırının maliyeti o kadar yükselir. Bu, tüm sosyal medya kullanımının bırakılması gerektiği anlamına gelmez; ancak kimlik, aile, kurum ve rutin bilgilerinin gereksiz biçimde bir arada sunulmaması yararlı bir savunmadır.

Çocuk Görselinin İzinsiz Kullanımı

Çocuğa ait açık fotoğraflar sahte profilde veya sentetik içerikte kullanılır. Koruma: sınırlı paylaşım, okul/konum ipuçlarının azaltılması, düzenli tersine görsel kontrol ve hızlı kaldırma başvurusu.

Bu senaryoda mağduriyetin erken belirtileri arasında tanımadık kişilerden gelen doğrulama soruları, olağandışı hesap bildirimleri, kişinin çevresinden "bu hesap sana mı ait?" mesajları ve bağlam dışı içeriklerin dolaşıma girmesi sayılabilir. Olay müdahalesinde panik yerine kanıtların korunması, hesapların güvenliğinin kontrol edilmesi, ilgili kişilerin bilgilendirilmesi ve resmî başvuru kanallarının kullanılması esastır.

Senaryo aynı zamanda veri minimizasyonunun önemini göstermektedir. Saldırganın ikna edici bir kurgu oluşturması için gerekli bağlamsal parçalar ne kadar azsa saldırının maliyeti o kadar yükselir. Bu, tüm sosyal medya kullanımının bırakılması gerektiği anlamına gelmez; ancak kimlik, aile, kurum ve rutin bilgilerinin gereksiz biçimde bir arada sunulmaması yararlı bir savunmadır.

EK A. RİSK DEĞERLENDİRME MATRİSİ

Risk	Olasılık	Etki	Öncelik	Temel Kontrol
Sahte profil / kimlik taklidi	Yüksek	Yüksek	Çok yüksek	Görünürlük sınırı, bildirim, hesap doğrulama
Deepfake itibar saldırısı	Orta	Çok yüksek	Çok yüksek	Kaynak doğrulama, kriz

				iletişimi, delil koruma
Ses taklidiyle finansal talep	Orta	Çok yüksek	Çok yüksek	İkinci kanal, çift onay, işlem limiti
Fotoğrafın amaç dışı işlenmesi	Orta	Yüksek	Yüksek	Aydınlatma, minimizasyon, saklama sınırı
Çocuk görselinin izinsiz kullanımı	Orta	Çok yüksek	Çok yüksek	Varsayılan gizlilik, sınırlı paylaşım
Biyometrik şablon sızıntısı	Düşük-Orta	Çok yüksek	Çok yüksek	Şifreleme, erişim kontrolü, kısa saklama
Yanlış deepfake suçlaması	Orta	Yüksek	Yüksek	Köken doğrulama, bağımsız inceleme

EK B. BİREYSEL DİJİTAL KİMLİK GÜVENLİĞİ KONTROL LİSTESİ

- Yapay zekâ hizmetine yüklemeden önce fotoğrafın gerçekten gerekli olup olmadığını değerlendirin.
- Gereğinden fazla referans fotoğraf yüklemeyin; veri minimizasyonunu uygulayın.
- Kimlik belgesi, adres, okul, kurum kartı, plaka veya hassas ekran görüntülerini kadrajdan çıkarın.
- Hizmetin saklama, silme, aktarım ve model geliştirme koşullarını inceleyin.
- Sosyal medya hesaplarında çok faktörlü kimlik doğrulamayı etkinleştirin.
- Finansal veya hassas talimatları yalnızca sesli/görüntülü görüşmeyle doğrulanmış saymayın.
- Yakınlarınızla acil para talepleri için bağımsız doğrulama yöntemi belirleyin.
- Adınıza açılan sahte hesapları platforma bildirin ve delilleri saklayın.
- Çocukların fotoğraflarında okul, konum ve günlük rutin bilgilerini azaltın.
- Şüpheli sentetik içerikleri doğrulamadan yeniden paylaşmayın.

GENEL DEĞERLENDİRME NOTU

Bu çalışma kaynakça kullanılmadan hazırlanmış kavramsal-akademik bir incelemedir. Hukuki değerlendirmeler genel niteliktedir; somut olaylarda veri işleme faaliyeti, tarafların sıfatları, hukuki işleme şartı, aktarım zinciri ve güncel mevzuat/ikincil düzenlemeler ayrıca değerlendirilmelidir. Çalışmanın temel amacı, yapay zekâ görsel teknolojilerinin risklerini abartmadan fakat küçümsemeden, dijital kimlik güvenliği perspektifinde sistematik bir çerçeveye oturtmaktır.

DIGITAL IDENTITY SECURITY IN THE AGE OF ARTIFICIAL INTELLIGENCE

Social-Media Photo Trends, AI-Based Image and Video Processing, Deepfakes, Criminal Misuse Risks, and an Assessment under Türkiye's Law No. 6698

Academic Review Study

Selçuk DİKİCİ

Bursa, Türkiye - 2026

ABSTRACT

The rapid diffusion of generative artificial intelligence has transformed image and video production into an everyday activity. Viral social-media trends that invite users to upload portraits, childhood photographs, family images, or voice samples may appear harmless and creative; however, they also create a new class of digital-security and personal-data risks. High-quality facial imagery, contextual information, repeated representations of the same person, and voice samples may be misused for identity impersonation, synthetic-media fraud, social engineering, extortion, reputational attacks, targeted profiling, and other forms of criminal exploitation.

This study examines AI-driven photo and video trends from technical, social, security, and legal perspectives. Its central argument is that an image should no longer be regarded merely as a photograph. It can function as a multilayered data object containing facial geometry, age-related features, expressions, contextual relationships, location clues, social connections, and behavioral indicators. At the same time, the study maintains an important legal distinction: not every photograph is automatically biometric data. The biometric-data question becomes particularly relevant when an image is subjected to specific technical processing for the purpose of uniquely identifying or authenticating an individual.

The study discusses deepfakes, face swapping, image-to-image generation, facial embeddings, face matching, lip synchronization, voice cloning, synthetic avatars, and related technologies at a conceptual and defensive level. It further evaluates the risks created when such technologies are used by criminals or organized criminal groups. Within the framework of Türkiye's Law No. 6698 on the Protection of Personal Data, the study considers consent, transparency, purpose limitation, proportionality, data minimization, retention, transfers, and data security. It concludes that social-media security can no longer be reduced to password protection and account access: a person's face, voice, and synthetic representation increasingly constitute a persistent digital identity asset that requires protection.

Keywords: artificial intelligence, generative AI, deepfake, social media, photo trends, digital identity, biometric data, personal data, Law No. 6698, identity impersonation, synthetic media, social engineering, digital security.

TABLE OF CONTENTS

1. Introduction

2. Research Problem, Purpose and Scope

3. Conceptual Framework: Digital Identity and Synthetic Media

4. AI-Based Image Processing Techniques

5. AI-Based Video Processing and Deepfake Technologies

6. Face, Voice and the Biometric Identity Layer

7. The Data Economy of Social-Media Photo Trends

8. Individual Security Risks of Photo Trends

9. Criminal and Organized-Crime Misuse Scenarios

10. Social Engineering, Fraud and Identity Impersonation

11. Deepfake Extortion, Reputational Attacks and Victimization

12. Children, Family Photographs and Intergenerational Digital Footprints

13. The Crisis of Trust and Reality on Social Media

14. Legal Assessment under Law No. 6698

15. Explicit Consent, Transparency and Purpose Limitation

16. Legal Nature of Biometric Data and Facial Images

17. Responsibilities of Platforms and AI Service Providers

18. Institutional Risks and Public-Sector Considerations

19. Technical and Administrative Security Measures

20. A Proposed AI Visual-Security Model for Türkiye

21. Discussion

22. Conclusion and Recommendations

23. Risk Scenarios and Case Modelling

Appendix A. Risk Assessment Matrix

Appendix B. Personal Digital-Identity Security Checklist

1. INTRODUCTION

During the early period of digitalization, online security was mainly associated with usernames, passwords, malware, and account takeover. The widespread adoption of generative AI has expanded this framework. Today, a person's identity may be imitated without compromising the person's actual account. A face, voice, or speaking style can be reproduced in synthetic content, shifting the object of security from the online account to the individual's broader digital representation.

Social-media photo trends are a visible example of this transformation. Users typically focus on the result: looking younger, appearing in another historical period, animating an old photograph, or obtaining a cinematic portrait. Technically, however, the process may require facial and contextual data to be transferred to a third-party system. Users may not always understand where the data is processed, how long it is retained, whether subcontractors are involved, or whether it is used for secondary purposes.

The starting point of this study is not opposition to technology. Generative AI offers substantial opportunities in creative production, accessibility, education, communication, and visual design. The problem lies in the speed gap between technological capability and social, legal, and technical safeguards. A photograph uploaded for entertainment may later have implications that the user did not anticipate.

The study therefore treats AI photo and video trends as a digital-identity issue rather than a narrow privacy issue. The central risk is not merely that an image becomes visible, but that it becomes reproducible, transformable, relocatable into new contexts, and potentially usable as a persuasive representation of a real person.

1.1 Extended Assessment

During the early period of digitalization, online security was mainly associated with usernames, passwords, malware, and account takeover. The widespread adoption of generative AI has expanded this framework. Today, a person's identity may be imitated without compromising the person's actual account. A face, voice, or speaking style can be reproduced in synthetic content, shifting the object of security from the online account to the individual's broader digital representation.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

1.2 Extended Assessment

Social-media photo trends are a visible example of this transformation. Users typically focus on the result: looking younger, appearing in another historical period, animating an old photograph, or obtaining a cinematic portrait. Technically, however, the process may require facial and contextual data to be transferred to a third-party system. Users may not always understand where the data is processed, how long it is retained, whether subcontractors are involved, or whether it is used for secondary purposes.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

1.3 Extended Assessment

The starting point of this study is not opposition to technology. Generative AI offers substantial opportunities in creative production, accessibility, education, communication, and visual design. The problem lies in the speed gap between technological capability and social, legal, and technical safeguards. A photograph uploaded for entertainment may later have implications that the user did not anticipate.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

2. RESEARCH PROBLEM, PURPOSE AND SCOPE

The primary research problem is how AI-based visual trends on social media affect the security of users' digital identities. Three subsidiary questions follow: what identity-related information can contemporary image and video systems use or infer; how can these capabilities be transformed into victimization by malicious actors; and to what extent can existing personal-data protection principles address these risks?

The purpose is not to accuse every AI product of unlawful conduct. Rather, the study makes the data life cycle visible: collection, upload, preprocessing, feature extraction, generation, storage, sharing, deletion, and secondary use. Each stage can create a different level and type of risk.

The study adopts a conceptual and normative method. Technical concepts are explained at a defensive level and misuse examples are discussed for risk modelling, not operational

instruction. Legal analysis focuses on the principles of Law No. 6698 and does not constitute case-specific legal advice.

The scope is limited to social media, generative AI services, face and video processing, voice synthesis, synthetic identity, platform security, and personal-data protection. The aim is to develop preventive recommendations at the individual, institutional, and platform levels.

2.1 Extended Assessment

The primary research problem is how AI-based visual trends on social media affect the security of users' digital identities. Three subsidiary questions follow: what identity-related information can contemporary image and video systems use or infer; how can these capabilities be transformed into victimization by malicious actors; and to what extent can existing personal-data protection principles address these risks?

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

2.2 Extended Assessment

The purpose is not to accuse every AI product of unlawful conduct. Rather, the study makes the data life cycle visible: collection, upload, preprocessing, feature extraction, generation, storage, sharing, deletion, and secondary use. Each stage can create a different level and type of risk.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger

preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

2.3 Extended Assessment

The study adopts a conceptual and normative method. Technical concepts are explained at a defensive level and misuse examples are discussed for risk modelling, not operational instruction. Legal analysis focuses on the principles of Law No. 6698 and does not constitute case-specific legal advice.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

3. CONCEPTUAL FRAMEWORK: DIGITAL IDENTITY AND SYNTHETIC MEDIA

Digital identity is the collection of data elements through which a person can be recognized, associated, or represented online. Names and usernames are only the most visible layer. Facial

images, voice, writing style, social connections, occupational information, family relationships, interests, and behavioral patterns also contribute to the digital-identity mosaic.

Synthetic media refers to images, audio, or video that are wholly or partly generated or meaningfully altered by algorithmic systems. Synthetic content is not inherently harmful. It has legitimate applications in film production, accessibility, education, art, and communication. Risk increases when the synthetic nature or origin is concealed and the content is presented as an authentic act or statement of a real person.

A defining feature of digital identity is reproducibility. In physical life, a face is attached to the body; once converted into digital imagery, it can be copied at very low cost. Generative models can further produce variations in lighting, pose, expression, age, or context.

This makes identity integrity an important concept. Privacy asks who can access information, whereas identity integrity asks which representation of a person is accepted as genuine. A person may suffer harm from a fabricated representation even when no confidential information has been disclosed.

3.1 Extended Assessment

Digital identity is the collection of data elements through which a person can be recognized, associated, or represented online. Names and usernames are only the most visible layer. Facial images, voice, writing style, social connections, occupational information, family relationships, interests, and behavioral patterns also contribute to the digital-identity mosaic.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

3.2 Extended Assessment

Synthetic media refers to images, audio, or video that are wholly or partly generated or meaningfully altered by algorithmic systems. Synthetic content is not inherently harmful. It has legitimate applications in film production, accessibility, education, art, and communication. Risk increases when the synthetic nature or origin is concealed and the content is presented as an authentic act or statement of a real person.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

3.3 Extended Assessment

A defining feature of digital identity is reproducibility. In physical life, a face is attached to the body; once converted into digital imagery, it can be copied at very low cost. Generative models can further produce variations in lighting, pose, expression, age, or context.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

4. AI-BASED IMAGE PROCESSING TECHNIQUES

Modern AI image systems go beyond traditional filters. They can identify semantic structures such as faces, expressions, lighting, hair, backgrounds, and objects, and use these elements in a new generation process. Generative models can create images from text instructions or reference images while attempting to preserve selected identity-related characteristics.

Image-to-image generation uses an existing image as a structural or identity reference. Identity-preservation mechanisms may attempt to maintain recognizable facial features across different scenes. These techniques are valuable for legitimate creative work, yet they create impersonation risks when real-person references are used without authorization.

Face-matching systems can transform an image into a numerical representation, often described as an embedding. An embedding is not the original photograph; nevertheless, it can enable mathematical comparison between faces. When such processing is used to uniquely identify or authenticate a person, the legal and security sensitivity increases.

Age transformation, facial restoration, and super-resolution are also dual-use technologies. Improving an old family photograph may be beneficial, while the same technical capacity may make previously low-quality identity material more usable. Risk must therefore be assessed according to data source, purpose, retention, and use rather than the name of the technology.

4.1 Extended Assessment

Modern AI image systems go beyond traditional filters. They can identify semantic structures such as faces, expressions, lighting, hair, backgrounds, and objects, and use these elements in a new generation process. Generative models can create images from text instructions or reference images while attempting to preserve selected identity-related characteristics.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

4.2 Extended Assessment

Image-to-image generation uses an existing image as a structural or identity reference. Identity-preservation mechanisms may attempt to maintain recognizable facial features across different scenes. These techniques are valuable for legitimate creative work, yet they create impersonation risks when real-person references are used without authorization.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

4.3 Extended Assessment

Face-matching systems can transform an image into a numerical representation, often described as an embedding. An embedding is not the original photograph; nevertheless, it can enable mathematical comparison between faces. When such processing is used to uniquely identify or authenticate a person, the legal and security sensitivity increases.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

5. AI-BASED VIDEO PROCESSING AND DEEPFAKE TECHNOLOGIES

Video contains temporal information that a single photograph does not: facial movement, blinking, head pose, speech rhythm, and expressions across frames. AI video generation attempts to maintain these characteristics consistently over time. Advances in this field have brought capabilities that once required specialist production tools into consumer applications.

The term deepfake commonly describes highly realistic synthetic or manipulated media that imitates a real person's face, voice, or performance. From a security perspective, the key issue is whether an observer is likely to believe that the represented event actually occurred.

Lip-synchronization and talking-avatar systems can align mouth movement with generated or recorded speech. These tools have legitimate uses in dubbing, accessibility, and education. Misuse can make a real person appear to say words they never uttered. Voice cloning can amplify the effect by creating multimodal impersonation.

Defensive strategy should not rely on a single deepfake detector. Source verification, provenance information, platform labels, contextual analysis, account history, independent confirmation, and forensic review where necessary should operate together.

5.1 Extended Assessment

Video contains temporal information that a single photograph does not: facial movement, blinking, head pose, speech rhythm, and expressions across frames. AI video generation attempts to maintain these characteristics consistently over time. Advances in this field have brought capabilities that once required specialist production tools into consumer applications.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

5.2 Extended Assessment

The term deepfake commonly describes highly realistic synthetic or manipulated media that imitates a real person's face, voice, or performance. From a security perspective, the key issue is whether an observer is likely to believe that the represented event actually occurred.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined

responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

5.3 Extended Assessment

Lip-synchronization and talking-avatar systems can align mouth movement with generated or recorded speech. These tools have legitimate uses in dubbing, accessibility, and education. Misuse can make a real person appear to say words they never uttered. Voice cloning can amplify the effect by creating multimodal impersonation.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

6. FACE, VOICE AND THE BIOMETRIC IDENTITY LAYER

Face and voice are powerful indicators of identity, but careful legal and technical classification is necessary. A photograph may constitute personal data when it relates to an identifiable person, yet not every photograph should automatically be treated as biometric data. Biometric sensitivity becomes especially relevant when physical or behavioral characteristics are technically processed for unique identification or authentication.

This distinction matters for social-media trends. A temporary visual effect and the creation of a persistent identity template are not equivalent. Two services that look similar to the user may have very different data-processing architectures.

Voice follows a similar logic. A recording can be ordinary personal data in one context, while extracted speaker-recognition characteristics may create a more sensitive identity layer in another. Combining face and voice increases the potential for multimodal authentication as well as multimodal impersonation.

Biometric identifiers have special security significance because they are difficult to replace. A compromised password can be changed; a person's natural face and voice cannot be replaced in the same way. Consequently, stronger safeguards are justified for biometric templates and source material capable of producing them.

6.1 Extended Assessment

Face and voice are powerful indicators of identity, but careful legal and technical classification is necessary. A photograph may constitute personal data when it relates to an identifiable person, yet not every photograph should automatically be treated as biometric data. Biometric sensitivity becomes especially relevant when physical or behavioral characteristics are technically processed for unique identification or authentication.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

6.2 Extended Assessment

This distinction matters for social-media trends. A temporary visual effect and the creation of a persistent identity template are not equivalent. Two services that look similar to the user may have very different data-processing architectures.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

6.3 Extended Assessment

Voice follows a similar logic. A recording can be ordinary personal data in one context, while extracted speaker-recognition characteristics may create a more sensitive identity layer in another. Combining face and voice increases the potential for multimodal authentication as well as multimodal impersonation.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

7. THE DATA ECONOMY OF SOCIAL-MEDIA PHOTO TRENDS

The power of social-media trends comes from voluntary mass participation. Users upload images under a common theme, publish the results, and invite others to participate. In a short period, this behavior can generate large volumes of high-quality portraits and contextual information.

An image may carry more than visible pixel content. File metadata, upload time, captions, tagged people, and social connections can enrich a profile. The legal basis and legitimacy of processing must be assessed for each concrete use rather than assumed from the fact that the user voluntarily uploaded an image.

The business model of a free or inexpensive AI service may not always be obvious. A service may be funded through subscriptions, advertising, enterprise licensing, or other models. The relevant security question is not merely whether the user paid money, but how the user's data is processed, retained, transferred, and reused.

Photo trends can also illustrate the opposite of data minimization. A user may upload twenty photographs where three would be sufficient. Even when additional images improve output quality, they enlarge the exposure surface. Privacy-preserving design should seek the desired result with the least necessary data.

7.1 Extended Assessment

The power of social-media trends comes from voluntary mass participation. Users upload images under a common theme, publish the results, and invite others to participate. In a short period, this behavior can generate large volumes of high-quality portraits and contextual information.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

7.2 Extended Assessment

An image may carry more than visible pixel content. File metadata, upload time, captions, tagged people, and social connections can enrich a profile. The legal basis and legitimacy of processing must be assessed for each concrete use rather than assumed from the fact that the user voluntarily uploaded an image.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

7.3 Extended Assessment

The business model of a free or inexpensive AI service may not always be obvious. A service may be funded through subscriptions, advertising, enterprise licensing, or other models. The relevant security question is not merely whether the user paid money, but how the user's data is processed, retained, transferred, and reused.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

8. INDIVIDUAL SECURITY RISKS OF PHOTO TRENDS

The first individual risk is loss of control. A user can delete a photograph from an account, yet copies may already have been downloaded, captured, transferred, or reused elsewhere. Digital replication makes complete withdrawal difficult.

The second risk is contextual displacement. A holiday photograph may be used in a fake professional profile, a family photograph in a fraudulent account, or a professional portrait in a fabricated advertisement. The source image may be authentic while its new context is deceptive.

The third risk is profile enrichment. Photographs from different ages, family relationships, occupations, institutions, and geographic clues can be combined into a persuasive social-engineering profile. The security problem is often not the theft of one secret but the aggregation of many open fragments.

The fourth risk is psychological and reputational harm. Fabricated imagery may continue circulating even after it is disproved. Corrections may receive less attention than the initial viral content, meaning that victimization cannot be evaluated solely in financial terms.

8.1 Extended Assessment

The first individual risk is loss of control. A user can delete a photograph from an account, yet copies may already have been downloaded, captured, transferred, or reused elsewhere. Digital replication makes complete withdrawal difficult.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

8.2 Extended Assessment

The second risk is contextual displacement. A holiday photograph may be used in a fake professional profile, a family photograph in a fraudulent account, or a professional portrait in a fabricated advertisement. The source image may be authentic while its new context is deceptive.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

8.3 Extended Assessment

The third risk is profile enrichment. Photographs from different ages, family relationships, occupations, institutions, and geographic clues can be combined into a persuasive social-

engineering profile. The security problem is often not the theft of one secret but the aggregation of many open fragments.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

9. CRIMINAL AND ORGANIZED-CRIME MISUSE SCENARIOS

Organized criminal groups often use technology to scale existing forms of fraud, coercion, and deception rather than invent entirely new crimes. AI-supported impersonation can lower the cost and increase the persuasiveness of targeted approaches.

One scenario involves fake profiles used to establish trust. Real photographs may be copied or synthetically diversified to create an apparently ordinary social-media history. The purpose may include romance fraud, financial requests, information gathering, or access to other people. Both the deceived target and the real person whose identity is misused may become victims.

Another scenario involves impersonation of authority figures, executives, public officials, or family members. Synthetic audio and video may create urgency and pressure. A crucial defensive principle is that high-risk transactions should not be authenticated solely by a video call; an independent second channel should be used.

The most significant criminal advantage of AI is scalability. A single deceptive template can be adapted to many targets. Institutions therefore need pattern detection, rapid reporting, evidence preservation, and coordination procedures rather than relying only on case-by-case reactions.

9.1 Extended Assessment

Organized criminal groups often use technology to scale existing forms of fraud, coercion, and deception rather than invent entirely new crimes. AI-supported impersonation can lower the cost and increase the persuasiveness of targeted approaches.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

9.2 Extended Assessment

One scenario involves fake profiles used to establish trust. Real photographs may be copied or synthetically diversified to create an apparently ordinary social-media history. The purpose may include romance fraud, financial requests, information gathering, or access to other people. Both the deceived target and the real person whose identity is misused may become victims.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

9.3 Extended Assessment

Another scenario involves impersonation of authority figures, executives, public officials, or family members. Synthetic audio and video may create urgency and pressure. A crucial defensive principle is that high-risk transactions should not be authenticated solely by a video call; an independent second channel should be used.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

10. SOCIAL ENGINEERING, FRAUD AND IDENTITY IMPERSONATION

Social engineering exploits human tendencies such as trust, fear, curiosity, urgency, and deference to authority. AI can make a deceptive message more personalized and can imitate familiar people. Security awareness must therefore extend beyond suspicious links to synthetic voices and images.

Successful impersonation depends on contextual coherence. Facial resemblance alone may not be enough; name, occupation, speaking style, social connections, and recent events can support the deception. Social media can supply much of this contextual material.

Financial controls should be designed independently of personal familiarity. Statements such as 'you know me' or 'you can see me on camera' should not constitute sufficient proof. Callback

procedures, transaction limits, dual authorization, and trusted channels can substantially reduce risk.

When impersonation is detected, victims should preserve links, screenshots, timestamps, and relevant account information, notify the platform, warn affected contacts, and use competent legal or law-enforcement channels when appropriate. Reposting harmful material in anger may unintentionally amplify it.

10.1 Extended Assessment

Social engineering exploits human tendencies such as trust, fear, curiosity, urgency, and deference to authority. AI can make a deceptive message more personalized and can imitate familiar people. Security awareness must therefore extend beyond suspicious links to synthetic voices and images.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

10.2 Extended Assessment

Successful impersonation depends on contextual coherence. Facial resemblance alone may not be enough; name, occupation, speaking style, social connections, and recent events can support the deception. Social media can supply much of this contextual material.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger

preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

10.3 Extended Assessment

Financial controls should be designed independently of personal familiarity. Statements such as 'you know me' or 'you can see me on camera' should not constitute sufficient proof. Callback procedures, transaction limits, dual authorization, and trusted channels can substantially reduce risk.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

11. DEEPFAKE EXTORTION, REPUTATIONAL ATTACKS AND VICTIMIZATION

In reputational attacks, the perpetrator may not need the fabricated content to remain believable for a long time. Temporary uncertainty can be sufficient to damage a manager, healthcare

professional, teacher, public figure, or ordinary citizen. Crisis communication is therefore as important as technical analysis.

Synthetic content can be used as leverage in extortion by threatening publication. The fact that the content is fabricated does not make the victimization unreal. Fear, family consequences, professional reputation, and financial demands can produce substantial harm.

A further problem is the so-called liar's dividend: as synthetic media becomes common, authentic recordings can also be dismissed as fake. Technology can therefore both make falsehood look true and make truth easier to deny.

Mitigation requires more than improved detection. Content provenance, platform policies, rapid correction mechanisms, legal remedies, victim support, and media literacy should function as a combined system.

11.1 Extended Assessment

In reputational attacks, the perpetrator may not need the fabricated content to remain believable for a long time. Temporary uncertainty can be sufficient to damage a manager, healthcare professional, teacher, public figure, or ordinary citizen. Crisis communication is therefore as important as technical analysis.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

11.2 Extended Assessment

Synthetic content can be used as leverage in extortion by threatening publication. The fact that the content is fabricated does not make the victimization unreal. Fear, family consequences, professional reputation, and financial demands can produce substantial harm.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

11.3 Extended Assessment

A further problem is the so-called liar's dividend: as synthetic media becomes common, authentic recordings can also be dismissed as fake. Technology can therefore both make falsehood look true and make truth easier to deny.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

12. CHILDREN, FAMILY PHOTOGRAPHS AND INTERGENERATIONAL DIGITAL FOOTPRINTS

Children's photographs create a distinct risk because the decision to publish is often made by an adult. A digital footprint created over many years may later conflict with the child's own preferences. AI age-transformation or animation trends can generate additional synthetic derivatives of children's images.

Family photographs contain relational information: parent-child relationships, siblings, locations, schools, institutions, and recurring routines. This relational layer may be more valuable for social engineering than a single portrait.

Protecting children requires more than the slogan 'think before you share.' Adults should consider data-processing terms, visibility settings, and whether public sharing is necessary. School uniforms, location information, routine schedules, and identity documents should be treated with particular caution.

Intergenerational digital footprints demonstrate that today's sharing decisions can have long-term effects. This supports stronger default privacy, shorter retention, and heightened caution for children's data.

12.1 Extended Assessment

Children's photographs create a distinct risk because the decision to publish is often made by an adult. A digital footprint created over many years may later conflict with the child's own preferences. AI age-transformation or animation trends can generate additional synthetic derivatives of children's images.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

12.2 Extended Assessment

Family photographs contain relational information: parent-child relationships, siblings, locations, schools, institutions, and recurring routines. This relational layer may be more valuable for social engineering than a single portrait.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

12.3 Extended Assessment

Protecting children requires more than the slogan 'think before you share.' Adults should consider data-processing terms, visibility settings, and whether public sharing is necessary. School uniforms, location information, routine schedules, and identity documents should be treated with particular caution.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger

preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

13. THE CRISIS OF TRUST AND REALITY ON SOCIAL MEDIA

Social media depends partly on an assumption that visible content has some relationship with real-world events. Synthetic media weakens this assumption. Users increasingly need to ask not only whether something is true, but how its authenticity can be demonstrated.

The reality crisis is bidirectional. Fabricated content may be believed, while authentic content may be rejected as artificial. Journalism, justice systems, institutional communication, and interpersonal relationships all face higher verification costs.

Trust erosion also affects individual account owners. A person's real account may remain secure while fake accounts and synthetic media damage confidence among friends, colleagues, or the public. This reveals the distinction between account security and identity security.

The long-term objective should not be to make users suspicious of every image. It should be to create verifiability through provenance indicators, trusted account verification, transparent AI labels, and independent confirmation channels.

13.1 Extended Assessment

Social media depends partly on an assumption that visible content has some relationship with real-world events. Synthetic media weakens this assumption. Users increasingly need to ask not only whether something is true, but how its authenticity can be demonstrated.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger

preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

13.2 Extended Assessment

The reality crisis is bidirectional. Fabricated content may be believed, while authentic content may be rejected as artificial. Journalism, justice systems, institutional communication, and interpersonal relationships all face higher verification costs.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

13.3 Extended Assessment

Trust erosion also affects individual account owners. A person's real account may remain secure while fake accounts and synthetic media damage confidence among friends, colleagues, or the public. This reveals the distinction between account security and identity security.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

14. LEGAL ASSESSMENT UNDER LAW NO. 6698

Assessment under Türkiye's Law No. 6698 requires each concrete processing activity to be examined separately. Uploading, retaining, analyzing, transferring, using an image for model improvement, or extracting identity-related features can raise different legal questions.

Core data-protection principles include lawful and fair processing, accuracy where necessary, specific and legitimate purposes, relevance and proportionality, and retention only for the period required by the processing purpose. In AI services, purpose specification and proportionality are especially important because technical possibility does not automatically establish legal necessity.

A user's decision to upload a photograph should not automatically be treated as unlimited permission for every secondary use. The applicable processing condition, quality of notice, distinction between service delivery and model improvement, and any required consent must be evaluated.

Accordingly, the defensible conclusion is not that every AI photo application violates Law No. 6698. Rather, processing without an appropriate legal condition, secondary use beyond stated purposes, excessive retention, opaque transfers, and inadequate security may create serious compliance risks.

14.1 Extended Assessment

Assessment under Türkiye's Law No. 6698 requires each concrete processing activity to be examined separately. Uploading, retaining, analyzing, transferring, using an image for model improvement, or extracting identity-related features can raise different legal questions.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

14.2 Extended Assessment

Core data-protection principles include lawful and fair processing, accuracy where necessary, specific and legitimate purposes, relevance and proportionality, and retention only for the period required by the processing purpose. In AI services, purpose specification and proportionality are especially important because technical possibility does not automatically establish legal necessity.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

14.3 Extended Assessment

A user's decision to upload a photograph should not automatically be treated as unlimited permission for every secondary use. The applicable processing condition, quality of notice, distinction between service delivery and model improvement, and any required consent must be evaluated.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

15. EXPLICIT CONSENT, TRANSPARENCY AND PURPOSE LIMITATION

Consent is often reduced in user interfaces to a single acceptance of lengthy terms. Data-protection logic requires more careful analysis. Where consent is the relevant basis, it should be specific, informed, and freely given. A request to transform a photograph is not necessarily identical to permission to use that photograph for unrelated future model development.

Transparency requires more than making a legal text technically accessible. Layered notices, concise summaries, visible retention periods, understandable descriptions of third-party involvement, and easy deletion options can provide more meaningful control.

Purpose limitation requires a relationship between the reason data was collected and its later use. An image supplied for an entertainment filter should not automatically be treated as

available for unrelated identity analysis. Requests for unnecessary location, contacts, or device data can also raise proportionality concerns.

User control should be genuine. Deletion, account closure, and model-training preferences should not be hidden behind confusing interfaces. Design should encourage minimization rather than nudging users toward unnecessary disclosure.

15.1 Extended Assessment

Consent is often reduced in user interfaces to a single acceptance of lengthy terms. Data-protection logic requires more careful analysis. Where consent is the relevant basis, it should be specific, informed, and freely given. A request to transform a photograph is not necessarily identical to permission to use that photograph for unrelated future model development.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

15.2 Extended Assessment

Transparency requires more than making a legal text technically accessible. Layered notices, concise summaries, visible retention periods, understandable descriptions of third-party involvement, and easy deletion options can provide more meaningful control.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

15.3 Extended Assessment

Purpose limitation requires a relationship between the reason data was collected and its later use. An image supplied for an entertainment filter should not automatically be treated as available for unrelated identity analysis. Requests for unnecessary location, contacts, or device data can also raise proportionality concerns.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

16. LEGAL NATURE OF BIOMETRIC DATA AND FACIAL IMAGES

The most important analytical distinction is between a photograph and a biometric template. A photograph relating to an identifiable person may be personal data. Biometric status generally becomes relevant where physical, physiological, or behavioral characteristics undergo specific technical processing for unique identification or authentication.

This distinction does not minimize risk. An ordinary image can later become the source material for biometric processing. Therefore, transparency about technical transformations and retention of derived representations is essential.

Derived facial representations may not be visually interpretable to humans but can still enable matching. Security controls must therefore protect not only original photographs but also mathematical representations and other derived data.

Proportionality is particularly important in biometric processing. If the same objective can reasonably be achieved with a less intrusive method, the necessity of biometric processing should be questioned.

16.1 Extended Assessment

The most important analytical distinction is between a photograph and a biometric template. A photograph relating to an identifiable person may be personal data. Biometric status generally becomes relevant where physical, physiological, or behavioral characteristics undergo specific technical processing for unique identification or authentication.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

16.2 Extended Assessment

This distinction does not minimize risk. An ordinary image can later become the source material for biometric processing. Therefore, transparency about technical transformations and retention of derived representations is essential.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

16.3 Extended Assessment

Derived facial representations may not be visually interpretable to humans but can still enable matching. Security controls must therefore protect not only original photographs but also mathematical representations and other derived data.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

17. RESPONSIBILITIES OF PLATFORMS AND AI SERVICE PROVIDERS

Platform security should extend beyond content removal. Data minimization, secure defaults, access controls, retention limits, and transparent design should be built into services. Synthetic-media labeling and rapid reporting channels for impersonation are increasingly important.

The AI data chain can involve multiple actors: application developers, cloud providers, model providers, analytics services, and content-delivery infrastructure. Users should be able to understand which parties process which data for which purposes.

Effective complaint mechanisms are critical in impersonation cases. Long and uncertain reporting procedures can allow harm to spread. High-risk reports may require prioritization, temporary visibility restrictions, and accelerated review.

Platform responsibility must also be balanced with freedom of expression and the risk of false positives. Parody, art, and clearly labeled fiction should be distinguished from deceptive impersonation through contextual assessment.

17.1 Extended Assessment

Platform security should extend beyond content removal. Data minimization, secure defaults, access controls, retention limits, and transparent design should be built into services. Synthetic-media labeling and rapid reporting channels for impersonation are increasingly important.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

17.2 Extended Assessment

The AI data chain can involve multiple actors: application developers, cloud providers, model providers, analytics services, and content-delivery infrastructure. Users should be able to understand which parties process which data for which purposes.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

17.3 Extended Assessment

Effective complaint mechanisms are critical in impersonation cases. Long and uncertain reporting procedures can allow harm to spread. High-risk reports may require prioritization, temporary visibility restrictions, and accelerated review.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

18. INSTITUTIONAL RISKS AND PUBLIC-SECTOR CONSIDERATIONS

At the institutional level, deepfake risk goes beyond executive impersonation. Employee photographs, buildings, badges, meeting screens, and public social-media posts can supply contextual material. Corporate social-media policies should therefore include visual-information security.

Public institutions face heightened trust risks because fabricated announcements or synthetic videos may affect large populations. Official communication channels should be defined in advance and major announcements should be verifiable through more than one trusted channel.

Employee training should abandon the assumption that a video call proves identity. Requests involving money, access rights, password resets, critical system changes, or sensitive data should follow formal procedures even when the requester appears on camera.

Incident-response plans should include a synthetic-media pathway covering evidence preservation, technical review, legal and communications coordination, platform reporting, affected-person notification, and appropriate engagement with authorities.

18.1 Extended Assessment

At the institutional level, deepfake risk goes beyond executive impersonation. Employee photographs, buildings, badges, meeting screens, and public social-media posts can supply contextual material. Corporate social-media policies should therefore include visual-information security.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined

responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

18.2 Extended Assessment

Public institutions face heightened trust risks because fabricated announcements or synthetic videos may affect large populations. Official communication channels should be defined in advance and major announcements should be verifiable through more than one trusted channel.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

18.3 Extended Assessment

Employee training should abandon the assumption that a video call proves identity. Requests involving money, access rights, password resets, critical system changes, or sensitive data should follow formal procedures even when the requester appears on camera.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

19. TECHNICAL AND ADMINISTRATIVE SECURITY MEASURES

At the individual level, the first measure is data minimization. Users should provide the fewest images reasonably necessary and remove unnecessary identity documents, addresses, badges, vehicle plates, or sensitive screens from the frame.

Account security remains important: unique passwords, multi-factor authentication, updated recovery channels, and session monitoring do not prevent deepfakes directly, but they reduce the impact of combined impersonation and account takeover.

At the institutional level, role-based access, logging, data classification, retention policies, vendor assessment, and incident response are essential. Procurement of AI services should evaluate data location, subprocessors, deletion, model-training practices, and security assurances in addition to model quality.

Provenance and watermarking technologies can help but should not be treated as absolute solutions. Watermarks may be lost and metadata can be stripped. Layered security combining technical signals with contextual and procedural verification is more resilient.

19.1 Extended Assessment

At the individual level, the first measure is data minimization. Users should provide the fewest images reasonably necessary and remove unnecessary identity documents, addresses, badges, vehicle plates, or sensitive screens from the frame.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

19.2 Extended Assessment

Account security remains important: unique passwords, multi-factor authentication, updated recovery channels, and session monitoring do not prevent deepfakes directly, but they reduce the impact of combined impersonation and account takeover.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

19.3 Extended Assessment

At the institutional level, role-based access, logging, data classification, retention policies, vendor assessment, and incident response are essential. Procurement of AI services should evaluate data location, subprocessors, deletion, model-training practices, and security assurances in addition to model quality.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger

preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

20. A PROPOSED AI VISUAL-SECURITY MODEL FOR TÜRKİYE

The proposed model has five layers: individual awareness, service-provider design, platform governance, institutional resilience, and legal/administrative oversight. No single layer can solve the problem independently.

Citizens should receive practical digital-identity literacy: faces and voices are difficult to replace, data minimization matters, synthetic content requires verification, and victims need clear reporting pathways.

Service providers and platforms should offer concise notices for high-risk face or voice processing, privacy-preserving defaults, short retention where feasible, easy deletion, separate choices for model development, and rapid impersonation reporting.

Public and private institutions should develop deepfake incident procedures, while regulatory approaches should remain technology-neutral, proportionate, and rights-conscious. The objective is not to block innovation but to make identity security a normal design requirement.

20.1 Extended Assessment

The proposed model has five layers: individual awareness, service-provider design, platform governance, institutional resilience, and legal/administrative oversight. No single layer can solve the problem independently.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger

preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

20.2 Extended Assessment

Citizens should receive practical digital-identity literacy: faces and voices are difficult to replace, data minimization matters, synthetic content requires verification, and victims need clear reporting pathways.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

20.3 Extended Assessment

Service providers and platforms should offer concise notices for high-risk face or voice processing, privacy-preserving defaults, short retention where feasible, easy deletion, separate choices for model development, and rapid impersonation reporting.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

21. DISCUSSION

Debate about AI photo trends is often trapped between two extremes: treating all applications as inherently dangerous or treating user participation as unlimited authorization. A more useful approach considers context, purpose, volume of data, retention, transfers, and reasonable user expectations.

Technological progress creates a continuing contest between generation and detection. A synthetic artifact that is easily detected today may become harder to identify tomorrow. Durable security therefore requires a shift from merely detecting false content toward proving the provenance of authentic content.

Law No. 6698 does not create a separate legal universe for AI; established data-protection principles continue to apply to new technical processes. The challenge is practical transparency. A lengthy privacy policy is not sufficient if users cannot understand the actual data flow.

The broadest social risk is erosion of trust. If people cease trusting authentic imagery, public communication, journalism, justice, and interpersonal relations are affected. Synthetic-media security should therefore be considered part of social trust infrastructure.

21.1 Extended Assessment

Debate about AI photo trends is often trapped between two extremes: treating all applications as inherently dangerous or treating user participation as unlimited authorization. A more useful

approach considers context, purpose, volume of data, retention, transfers, and reasonable user expectations.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

21.2 Extended Assessment

Technological progress creates a continuing contest between generation and detection. A synthetic artifact that is easily detected today may become harder to identify tomorrow. Durable security therefore requires a shift from merely detecting false content toward proving the provenance of authentic content.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

21.3 Extended Assessment

Law No. 6698 does not create a separate legal universe for AI; established data-protection principles continue to apply to new technical processes. The challenge is practical transparency. A lengthy privacy policy is not sufficient if users cannot understand the actual data flow.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

22. CONCLUSION AND RECOMMENDATIONS

This study finds that AI-based photo and video trends create a digital-identity security problem alongside their legitimate creative value. The central risk is not simply uploading a photograph, but enabling images to be analyzed, reproduced, transformed, relocated into new contexts, and used to create persuasive synthetic representations.

Social-media security must consequently move beyond password protection. Face, voice, behavioral characteristics, social context, and historical posts can combine into a rich representation of an individual. Criminal actors may exploit this representation for social engineering, fraud, extortion, fake profiles, authority impersonation, and reputational attacks.

Legal analysis should avoid categorical claims. Not every photograph is biometric data and not every AI process is unlawful. Nevertheless, collection without an appropriate legal basis, incompatible secondary use, excessive retention, opaque transfers, or inadequate security may create significant compliance problems. Facial data subjected to specific technical processing for unique identification or authentication requires heightened sensitivity.

The appropriate response is not avoidance of AI but security-by-design for AI. Individuals should practice minimization; institutions should use independent verification and synthetic-media incident response; platforms should accelerate impersonation reporting and provenance mechanisms; and service providers should make retention and secondary use understandable. Digital identity protection is likely to become one of the defining personal-data security challenges of the coming years.

22.1 Extended Assessment

This study finds that AI-based photo and video trends create a digital-identity security problem alongside their legitimate creative value. The central risk is not simply uploading a photograph, but enabling images to be analyzed, reproduced, transformed, relocated into new contexts, and used to create persuasive synthetic representations.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

22.2 Extended Assessment

Social-media security must consequently move beyond password protection. Face, voice, behavioral characteristics, social context, and historical posts can combine into a rich representation of an individual. Criminal actors may exploit this representation for social engineering, fraud, extortion, fake profiles, authority impersonation, and reputational attacks.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger

preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

22.3 Extended Assessment

Legal analysis should avoid categorical claims. Not every photograph is biometric data and not every AI process is unlawful. Nevertheless, collection without an appropriate legal basis, incompatible secondary use, excessive retention, opaque transfers, or inadequate security may create significant compliance problems. Facial data subjected to specific technical processing for unique identification or authentication requires heightened sensitivity.

Risk analysis should distinguish likelihood from impact. Technical possibility does not prove that an event is common, yet high-impact and difficult-to-reverse harms justify stronger preventive controls. This is particularly important for persistent identity indicators such as face and voice.

The fragmented data chain should also be considered. A user may see one application while several infrastructure providers operate in the background. Sound governance requires defined responsibilities, restricted access, retention rules, auditability, and traceable handling of user requests.

The social response should avoid fear-based technology rejection. The goal is to enable risk-informed choices through transparent processing, understandable permissions, secure defaults, data minimization, and independent verification channels.

23. RISK SCENARIOS AND CASE MODELLING

Synthetic Executive Call

An employee receives an urgent request during an online call that appears to show a senior executive. The defensive response is to require an independent second channel, dual authorization, and transaction limits for sensitive actions.

Early indicators may include unexpected verification questions from acquaintances, unusual account alerts, messages asking whether a new profile is genuine, or contextually inconsistent media circulating online. Response should prioritize evidence preservation, account-security checks, notification of affected contacts, and appropriate official reporting.

The scenario also illustrates the value of minimization. The fewer contextual fragments available to a malicious actor, the more difficult it becomes to construct a coherent deception. This does not require abandoning social media, but it supports more deliberate separation of identity, family, workplace, and routine information.

Fake Social-Media Profile

Publicly available photographs of a real person are used to construct a new account and contact that person's network. Defensive measures include visibility controls, trusted communication channels, rapid platform reporting, and notification of contacts.

Early indicators may include unexpected verification questions from acquaintances, unusual account alerts, messages asking whether a new profile is genuine, or contextually inconsistent media circulating online. Response should prioritize evidence preservation, account-security checks, notification of affected contacts, and appropriate official reporting.

The scenario also illustrates the value of minimization. The fewer contextual fragments available to a malicious actor, the more difficult it becomes to construct a coherent deception. This does not require abandoning social media, but it supports more deliberate separation of identity, family, workplace, and routine information.

Synthetic Reputational Attack

A short fabricated video makes a person appear to make a statement they never made. Defensive measures include source verification, evidence preservation, rapid institutional communication, and formal reporting.

Early indicators may include unexpected verification questions from acquaintances, unusual account alerts, messages asking whether a new profile is genuine, or contextually inconsistent media circulating online. Response should prioritize evidence preservation, account-security checks, notification of affected contacts, and appropriate official reporting.

The scenario also illustrates the value of minimization. The fewer contextual fragments available to a malicious actor, the more difficult it becomes to construct a coherent deception. This does not require abandoning social media, but it supports more deliberate separation of identity, family, workplace, and routine information.

Family-Member Impersonation

Family photographs and public contextual information are used to make an urgent financial request persuasive. Families can reduce risk by using an independent verification method for unusual requests.

Early indicators may include unexpected verification questions from acquaintances, unusual account alerts, messages asking whether a new profile is genuine, or contextually inconsistent media circulating online. Response should prioritize evidence preservation, account-security checks, notification of affected contacts, and appropriate official reporting.

The scenario also illustrates the value of minimization. The fewer contextual fragments available to a malicious actor, the more difficult it becomes to construct a coherent deception. This does not require abandoning social media, but it supports more deliberate separation of identity, family, workplace, and routine information.

Unauthorized Use of a Child's Image

A child's publicly available photographs are reused in a fake profile or synthetic media. Stronger default privacy, reduced location and school clues, and rapid removal requests can reduce exposure.

Early indicators may include unexpected verification questions from acquaintances, unusual account alerts, messages asking whether a new profile is genuine, or contextually inconsistent media circulating online. Response should prioritize evidence preservation, account-security checks, notification of affected contacts, and appropriate official reporting.

The scenario also illustrates the value of minimization. The fewer contextual fragments available to a malicious actor, the more difficult it becomes to construct a coherent deception. This does not require abandoning social media, but it supports more deliberate separation of identity, family, workplace, and routine information.

APPENDIX A. RISK ASSESSMENT MATRIX

Risk	Likelihood	Impact	Priority	Primary Control
Fake profile / identity impersonation	High	High	Very high	Visibility controls, reporting, account verification
Deepfake reputational attack	Medium	Very high	Very high	Source verification, crisis communication, evidence preservation
Voice impersonation for financial request	Medium	Very high	Very high	Second channel, dual authorization, transaction limits
Purpose-incompatible image processing	Medium	High	High	Transparency, minimization, retention limits

Unauthorized use of child imagery	Medium	Very high	Very high	Privacy defaults, limited sharing
Biometric-template compromise	Low-Medium	Very high	Very high	Encryption, access control, limited retention
False allegation that authentic media is deepfake	Medium	High	High	Provenance verification, independent review

APPENDIX B. PERSONAL DIGITAL-IDENTITY SECURITY CHECKLIST

- Assess whether uploading a photograph to an AI service is genuinely necessary.
- Upload no more reference photographs than required.
- Remove identity documents, addresses, school or workplace badges, vehicle plates, and sensitive screens from images.
- Review retention, deletion, transfer, and model-development terms.
- Enable multi-factor authentication on social-media accounts.
- Do not treat a voice or video call alone as sufficient authorization for sensitive transactions.
- Use an independent verification method for unusual requests from family members or colleagues.
- Preserve evidence and report fake accounts using your identity.
- Reduce school, location, and routine information in children's photographs.
- Do not redistribute suspicious synthetic media before verification.

GENERAL NOTE

This is a conceptual academic review prepared without a formal bibliography at the user's request. Legal observations are general and do not replace case-specific legal advice. Concrete processing activities should be assessed according to the roles of the parties, the applicable processing condition, the data-transfer chain, and the legislation in force at the relevant time.