



TÜRKİYE CUMHURİYETİ
CUMHURBAŞKANLIĞI
İLETİŞİM
BAŞKANLIĞI



TÜRKİYE CUMHURİYETİ
İÇİŞLERİ BAKANLIĞI

MÜLKİ İDARE AMİRLERİNE YÖNELİK

SOSYAL MEDYA REHBERİ



TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
İLETİŞİM BAŞKANLIĞI



TÜRKİYE CUMHURİYETİ
İÇİŞLERİ BAKANLIĞI

MÜLKİ İDARE AMİRLERİNE YÖNELİK

SOSYAL MEDYA REHBERİ



TAKDİM

İletişim teknolojilerinde yaşanan hızlı dönüşüm, kamu yönetiminin vatandaşla kurduğu ilişkinin mahiyetini de yeniden şekillendirmiştir. Dijital platformlar, bilginin üretildiği, dolaşıma girdiği ve kamuoyunun kanaatlerinin olduğu temel mecralar arasında yer almaktadır. Bu yeni iletişim ekosistemi, kamu hizmetlerinin etkinliğini artıracak stratejik imkânlar sunarken, doğru bilginin zamanında paylaşılmasını, kurumsal itibarın korunmasını ve dezenformasyonla etkin mücadeleyi de kamu yönetiminin temel sorumlulukları arasına taşımıştır.

Muhterem Cumhurbaşkanımız Recep Tayyip Erdoğan'ın liderliğinde hayata geçirilen Türkiye Yüzyılı vizyonu, güçlü devlet ve güçlü millet arasındaki bağı daha da kuvvetlendirmeyi esas almaktadır. Şeffaflık, güven, erişilebilirlik ve etkin iletişim anlayışı, bu vizyonun kamu yönetimine kazandırdığı temel ilkeler arasında yer almaktadır. Dijital iletişim araçlarının kamu hizmetlerine sağladığı katkı da bu anlayışın önemli unsurlarından biridir.

Mülki idare amirleri, devletimizin il ve ilçelerdeki en üst temsilcileri olarak kamu düzeninin sağlanmasından kamu hizmetlerinin koordinasyonuna, kriz yönetiminden toplumsal huzurun teminine kadar geniş bir sorumluluk alanını üstlenmektedir. Bu sorumluluğun dijital mecralardaki yansıması da en az sahadaki uygulamalar kadar önemlidir. Sosyal medya platformlarında kullanılan dil, paylaşılan içerikler ve kurulan iletişim, devletimizin kurumsal kimliğini, temsil anlayışını ve vatandaşlarımızla kurduğu güven ilişkisini doğrudan yansıtmaktadır.

Dijital mecralarda yürütülen kamu iletişimi, teknik bir paylaşım faaliyetinin ötesinde, devleti temsil sorumluluğunu da beraberinde taşımaktadır. Bu sebeple mülki idare amirlerimizin sosyal medya kullanımlarında kamu görevinin vakarını koruyan, vatandaşlarımızın mahremiyetini ve kişisel verilerini titizlikle gözetken, hukuki ve etik ilkeleri esas alan ortak bir kurumsal standardın oluşturulması büyük önem taşımaktadır. Devletimizin temsil makamında bulunan her mülki idare amirimizin dijital ortamdaki tutumu da kamu hizmetinin ayrılmaz bir parçasıdır.

Bu anlayışla hazırlanan Mülki İdare Amirlerine Yönelik Sosyal Medya Rehberi; sosyal medya kullanımına ilişkin temel ilkeleri, bilgi güvenliğini, etik sorumlulukları, kriz iletişimini, dezenformasyonla mücadele yöntemlerini ve kurumsal iletişim standartlarını bütüncül bir yaklaşımla ele almaktadır. Rehber, mülki idare amirlerimizin dijital mecralarda güven veren, tutarlı, sorumluluk bilinciyle hareket eden ve kamu yararını esas alan ortak bir iletişim kültürü geliştirmelerine katkı sunmayı hedeflemektedir.

Bilgi çağında güven, hız kadar doğrulukla; görünürlük ise kurumsal ciddiyetle anlam kazanmaktadır. Kamu idaresinin dijital mecralardaki temsil gücü, vatandaşlarımızın devlete duyduğu güveni pekiştiren en önemli unsurlardan biridir. Bu bakımdan sosyal medya, kamu yönetiminin etkinliğini destekleyen stratejik bir iletişim alanı olmasının yanında, devlet ciddiyetinin ve kamu hizmeti anlayışının görünür hâle geldiği önemli bir temsil zemini olarak değerlendirilmelidir.

Cumhurbaşkanlığı İletişim Başkanlığımız ile İçişleri Bakanlığımızın iş birliğiyle hazırlanan bu rehberin, mülki idare amirlerimizin dijital iletişim süreçlerine önemli katkılar sağlayacağına; kamu görevinin vakarını esas alan ortak bir temsil anlayışının güçlenmesine, vatandaşlarımızın mahremiyetinin korunmasına ve devlet-millet arasındaki güven bağının daha da kuvvetlenmesine katkı sunacağına inanıyorum.

Eserin hazırlanmasında emeği geçen Cumhurbaşkanlığı İletişim Başkanlığımıza, İçişleri Bakanlığımızın değerli mensuplarına ve katkı sunan tüm çalışma arkadaşlarımıza teşekkür ediyor; rehberimizin mülki idare teşkilatımız ve ülkemiz için hayırlı olmasını temenni ediyorum.

Mustafa ÇİFTÇİ

Türkiye Cumhuriyeti İçişleri Bakanı





ÖN SÖZ

Yeni iletişim teknolojilerinin hızla gelişmesi, bilginin üretim ve tüketim süreçlerini köklü bir biçimde dönüştürerek yepyeni bir dijital medya ekosistemi inşa etmiştir. Bu dinamik ekosistem, kamu yönetimi ile vatandaş arasındaki etkileşimin sınırlarını genişlettiği gibi devletin dijital ortamdaki görünürlüğünü ve temsil gücünü stratejik bir zemine de taşımıştır. Diğer yandan dijital mecralardaki bilgi akışının doğru, şeffaf ve güvenilir bir zeminde yönetilmesi, sağlıklı bir toplum için vazgeçilmezdir.

Cumhurbaşkanımız Sayın Recep Tayyip Erdoğan'ın "Türkiye Yüzyılı" vizyonu, güçlü devlet geleneğimizi dijital çağın imkânlarıyla bütünleştirmeyi esas almaktadır. Bu vizyon doğrultusunda, kamu idaresinin dijital platformlardaki varlığı, yalnızca bir bilgilendirme faaliyeti değil; devlet ciddiyetinin, vatandaşla kurulan güven bağının ve kriz anlarındaki yönetim gücünün en önemli göstergelerinden biridir. Mülki idare amirlerimiz, devletimizin il ve ilçelerdeki en üst temsilcileri olarak bu güven ilişkisini dijital dünyada da tesis etmekle mükelleftir.

İçinde bulunduğumuz dönemde, dezenformasyon ve bilgi düzensizlikleri ulusal güvenliğimizi ve toplumsal huzurumuzu tehdit eden en büyük sınamalardan biri hâline gelmiştir. Hakikatin manipüle edildiği, sahte içeriklerin hızla yayıldığı bu yeni medya düzeninde, devlet kurumlarımızın ve yöneticilerimizin dijital dayanıklılık kapasitesini artırması kaçınılmaz bir gerekliliktir. Kriz anlarında doğru bilginin kaynağı olmak ve kamuoyunu sağduyuyla yönlendirmek, ancak bu dayanıklılığın kurumsal bir kültüre dönüşmesiyle mümkündür.

İçişleri Bakanlığımız ve Cumhurbaşkanlığı İletişim Başkanlığımızca hazırlanan "Mülki İdare Amirlerine Yönelik Sosyal Medya Kullanım Rehberi", tam da bu hayati ihtiyaca binaen hazırlanmış, mülki idare amirlerimiz için stratejik bir başvuru kaynağıdır. Çalışmanın temel amacı, dijital mecralardaki fırsatları kamu yararına dönüştürürken potansiyel risklere karşı ortak bir iletişim aklı ve duruşu geliştirmektir. Rehber, sosyal medyanın teknik boyutlarının ötesine geçerek etik değerleri, itibar yönetimini ve kriz iletişimi süreçlerini bütüncül bir yaklaşımla ele almaktadır.

Kamu yönetiminde sağlıklı bir bilgi düzeninin korunması, olaylara anında ve doğru reaksiyon gösterebilen kurumsal teyit mekanizmalarının işletilmesine bağlıdır. Bu rehber, dezenformasyon ve türevleriyle mücadelenin yöntemlerini sunarken aynı zamanda mülki idare amirlerimizin vatandaşla kurduğu doğrudan iletişimin kalitesini artıracak standartları belirlemektedir. İdarecilerimizin, sosyal medyayı yalnızca bir duyuru panosu olarak değil, hakikatin savunulduğu bir güven zemini olarak kullanmaları hedeflenmiştir.

Kamu hizmetlerinin dijital düzleme aktarılmasında hız ve verimlilik kadar şeffaflık, erişilebilirlik ve veri mahremiyeti de vazgeçilmez ilkelerimizdendir. Bu çalışma, devleti temsil eden her bir yöneticimizin, sanal ortamda da bu ilkelere sadık kalarak Türkiye İletişim Modeli'ne ve epistemik egemenliğimize güç katması için bir yol haritası sunmaktadır.

Rehberin, mülki idare amirlerimizin dijital dünyadaki iletişim faaliyetlerini daha etkin, güvenli ve kurumsal bir anlayışla yürütmelerine önemli katkılar sağlayacağına yürekten inanıyor; bu çalışmanın hazırlanmasında emeği geçenlere teşekkür ediyorum.

Prof. Dr. Burhanettin Duran

Türkiye Cumhuriyeti Cumhurbaşkanlığı İletişim Başkanı

İÇİNDEKİLER

TAKDİM.....	3
ÖN SÖZ.....	7
GİRİŞ.....	11
SOSYAL MEDYANIN TARİHSEL GELİŞİMİ VE TOPLUMSAL ÖNEMİ.....	13
SOSYAL MEDYADA GÜVENLİK TEDBİRLERİ.....	26
SOSYAL MEDYA MECRALARI GÜVENLİK AYARLARI REHBERİ	29
ANLIK MESAJLAŞMA VE YAYIN KANALLARI	33
KİŞİSEL HESAP GENEL İLKELER.....	38
KURUMSAL HESAP GENEL İLKELER.....	40
SAYFA YÖNETİMİ KONUSUNDA DİKKAT EDİLMESİ GEREKENLER.....	49
KAÇINILMASI GEREKEN İÇERİK TÜRLERİ.....	55
KRİZ İLETİŞİM YÖNETİMİ.....	56
DİJİTAL BİLGİ KİRLİLİĞİNE KARŞI DİJİTAL İLETİŞİM YÖNETİMİ.....	68
DEZENFORMASYONLA MÜCADELE.....	71
SOSYAL MEDYA SÖZLÜĞÜ.....	84
EK1: SOSYAL MEDYA ETİK İLKELERİ.....	98
EK2: ERİŞİLEBİLİRLİK İLKESİNİN ANA ESASLARI.....	101



GİRİŞ

İnsanlık, iletişim tarihinin en köklü dönüşüm dönemlerinden birini yaşamaktadır. Dijitalleşme; yalnızca yeni teknolojilerin yaygınlaşması değil, devletin işleyişini, kamu yönetimini, toplumsal etkileşimi ve vatandaşla kurduğu güven ilişkisini yeniden tanımlayan yeni bir medeniyet eşiğidir. İnternet, sosyal medya, mobil teknolojiler ve yapay zekâ destekli dijital sistemler; devlet-vatandaş etkileşiminin ana omurgasını oluşturarak dijital ekosistemi çağımızın en stratejik yönetim alanlarından biri hâline getirmiştir. Bu yeni düzende dijital iletişim; bilgi paylaşımının ötesinde, devletin meşruiyetini güçlendiren, kamusal dijital itibarını koruyan, toplumsal güveni pekiştiren, krizleri yöneten ve millî iradeyi dijital alanda temsil eden stratejik bir devlet kapasitesidir.

Sosyal medya platformları, günümüzde bilgiye erişim ve bilgi paylaşımının en yaygın araçlarından biri olarak öne çıkmaktadır. Kullanıcıların içerik üretme, görüşlerini ifade etme ve ortak ilgi alanları etrafında etkileşim kurma imkânı bulduğu bu platformlar, toplumsal iletişimin önemli bir parçası hâline gelmiştir. Bununla birlikte sosyal medya ortamlarında doğru ve güvenilir bilginin yanı sıra yanlış veya yanıltıcı içeriklerin de dolaşıma girebilmesi, kamuoyu algısının şekillenmesi ve toplumsal süreçlerin etkilenmesi bakımından dikkatle ele alınması gereken bir husustur.

Kamu kurumları açısından sosyal medya, vatandaşlarla doğrudan ve çift yönlü iletişim kurulmasına imkân sağlayan stratejik bir alandır. Kamu hizmetlerine ilişkin bilgilendirme faaliyetlerinin yürütülmesi, toplumsal beklenti ve ihtiyaçların izlenmesi, kriz ve olağanüstü durumlarda hızlı bilgi paylaşımının sağlanması ve dezenformasyonla mücadele edilmesi, sosyal medyanın kamu idaresine sunduğu temel imkânlar arasında yer almaktadır. Ayrıca sosyal medya platformları, kamu hizmetlerinin görünürlüğünün artırılmasına ve gerçekleştirilen faaliyetlerin etkisinin değerlendirilmesine katkı sunmaktadır.

Dijital ekosistemin sunduğu imkânlar kadar beraberinde getirdiği riskler de kamu kurumları açısından stratejik bir yönetim anlayışını zorunlu kılmaktadır. Bilgi kirliliği, dezenformasyon, manipülatif içerikler, siber tehditler, kişisel verilerin ihlali ve dijital güvenlik riskleri;

kamu otoritesinin güvenilirliğini, kurumsal itibarını ve devlet-vatandaş arasındaki güven ilişkisini doğrudan etkileyebilmektedir. Bu nedenle dijital alanda gerçekleştirilen her paylaşım; doğruluk, hukuka uygunluk, etik sorumluluk, kişisel verilerin korunması, özel hayatın gizliliği ve millî güvenlik hassasiyetleri çerçevesinde değerlendirilmeli; devlet ciddiyetini ve kurumsal sorumluluğu esas alan bir anlayışla yürütülmelidir.

Mülki idare amirlerinin dijital alandaki temsil sorumluluğu, yalnızca bilgi paylaşımıyla sınırlı değildir. Dijital temsil; ilin veya ilçenin sosyal dokusunu, kültürel zenginliğini, ekonomik potansiyelini, coğrafi özelliklerini ve yerel önceliklerini doğru okuyarak vatandaşla güvene dayalı, kapsayıcı ve sürdürülebilir bir iletişim kurabilme kapasitesini de ifade etmektedir. Yerel dinamikleri dikkate alan, toplumsal hassasiyetleri gözetken ve vatandaş odaklı bir iletişim anlayışı, kamu hizmetlerinin etkinliğini artırırken devlet ile millet arasındaki güven bağını da güçlendirmektedir.

Dijital çağda kamu kurumlarının sosyal medya varlığı, yalnızca kurumsal görünürlüğü artıran bir iletişim faaliyeti değil; devletin dijital ekosistemdeki temsil gücünü pekiştiren stratejik bir yönetim aracıdır. Etkin, şeffaf ve güvenilir dijital iletişim; kamu hizmetlerinin görünürlüğünü artırmakta, vatandaş katılımını güçlendirmekte, kriz dönemlerinde doğru bilginin en hızlı şekilde kamuoyuna ulaştırılmasını sağlamakta ve dezenformasyona karşı kurumsal dayanıklılığı artırmaktadır. Bu yönüyle sosyal medya, kamu yönetiminin etkinliğini destekleyen, toplumsal güveni besleyen ve kurumsal itibarı güçlendiren temel stratejik iletişim araçlarından biri hâline gelmiştir.

Bu rehber; mülki idare amirlerinin dijital ekosistemde devleti temsil ederken ortak bir iletişim vizyonu geliştirmelerine katkı sunmak amacıyla hazırlanmıştır. Rehberde; dijital temsil ilkeleri, kurumsal hesap yönetimi, içerik stratejileri, dijital itibar yönetimi, kriz iletişimi, dezenformasyonla mücadele, etik sorumluluklar ve dijital güvenlik konuları bütüncül bir yaklaşımla ele alınmaktadır. Temel hedef; kamu yöneticilerinin dijital ekosistemde devletin vakarını, güvenilirliğini ve temsil gücünü en üst düzeyde yansıtarak vatandaşla güvene dayalı, sürdürülebilir ve etkili bir iletişim anlayışı geliştirmelerine katkı sağlamaktır.

Dijital ekosistemde temsil edilen yalnızca kurumlar değil, devletin itibarı, kamu otoritesi ve milletle kurduğu güven ilişkisidir.



SOSYAL MEDYANIN TARİHSEL GELİŞİMİ VE TOPLUMSAL ÖNEMİ

İnsanlık tarihindeki en büyük medeniyet dönüşümlerinden biri, bilginin üretim, dolaşım ve yönetim süreçlerinin fiziksel sınırları aşarak dijital ekosisteme taşınmasıdır. Bu dönüşüm, yalnızca iletişim araçlarını değiştirmemiş; devletlerin yönetim anlayışını, kamu otoritesinin temsilini, toplumsal etkileşimi ve vatandaşla kurulan güven ilişkisini yeniden tanımlayan yeni bir dijital çağın başlangıcı olmuştur.

İletişim teknolojilerindeki hızlı gelişmeler, dünyanın farklı bölgelerindeki bireyleri birbirine bağlayarak bilgiye erişimi büyük ölçüde kolaylaştırmıştır. Bu süreçte sosyal medya, kullanıcıların yalnızca bilgi tüketicisi değil, aynı zamanda bilgi üreticisi, yorumlayıcısı ve yayıcısı olarak aktif rol üstlendiği dijital platformlar bütünü olarak öne çıkmıştır. Zaman ve mekân sınırlarını büyük ölçüde ortadan kaldıran bu platformlar, bireyler arasında karşılıklı ve etkileşimli iletişim kurulmasına olanak tanımaktadır. Sosyal medya, özellikle pazarlama ve kamu iletişimi alanlarında geleneksel iletişim yöntemlerine göre önemli farklılıklar göstermekte; kullanıcıların içerik üretme, gündem oluşturma ve kamuoyunu etkileme kapasitesini artırmaktadır.

İNTERNETİN İCADI VE TEKNİK TEMELLER

İnternetin ortaya çıkışı, 1960'lı yılların sonlarında Soğuk Savaş döneminin güvenlik ihtiyaçları ile akademik araştırmaların kesişim noktasında gerçekleşmiştir. Amerika Birleşik Devletleri Savunma Bakanlığı bünyesinde faaliyet gösteren Advanced Research Projects Agency (ARPA) tarafından geliştirilen ARPANET, günümüz internetinin ilk örneği olarak kabul edilmektedir. 1969 yılında faaliyete geçirilen bu ağ sistemi, paket anahtarlama (packet switching) teknolojisini kullanarak merkezi olmayan bir iletişim modeli oluşturmuştur. Bu model sayesinde veriler tek bir iletişim hattı üzerinden iletilmek yerine küçük paketlere ayrılarak farklı güzergâhlardan hedef noktaya ulaştırılmış ve böylece iletişim ağının dayanıklılığı artırılmıştır.

1970’li yıllar, internetin teknik standartlarının geliştirildiği ve farklı ağların birbirleriyle iletişim kurabilmesini sağlayan protokollerin oluşturulduğu bir dönem olmuştur. Bu kapsamda Vint Cerf, Yogen Dalal ve Carl Sunshine tarafından 1974 yılında geliştirilen Transmission Control Protocol (TCP), farklı bilgisayar ağları arasında veri iletişimini mümkün kılan ortak bir standart ortaya koymuştur. Daha sonra TCP’nin Internet Protocol (IP) ile bütünleşmesi sonucu ortaya çıkan TCP/IP protokolü, günümüz internet altyapısının temel iletişim standardı hâline gelmiştir. ARPANET’in 1980’li yıllarda tamamen TCP/IP sistemine geçmesiyle birlikte küresel internet ağının teknik temelleri büyük ölçüde tamamlanmıştır.

İNTERNETİN YAYGINLAŞMASI VE SOSYAL MEDYANIN ORTAYA ÇIKIŞI

İnternetin akademik ve askerî alanlarda kullanımının yanı sıra bireysel kullanıma da açılması, 1980’li yılların ortalarından itibaren hız kazanmıştır. Kişisel bilgisayarların yaygınlaşması, işlem kapasitelerinin artması ve maliyetlerinin düşmesi, internet teknolojilerinin ev kullanıcıları tarafından erişilebilir hâle gelmesinde önemli rol oynamıştır. Bu süreçte 1986 yılında National Science Foundation (NSF) tarafından kurulan NSFNet, farklı akademik ağları birbirine bağlayan ilk büyük internet omurgası olarak işlev görmüştür. 1989 yılından itibaren internetin ticari kullanıma açılmasıyla birlikte internet servis sağlayıcıları (ISP) ortaya çıkmış ve internet daha geniş kitlelere ulaşmaya başlamıştır.

İnternetin yaygınlaşmasında dönüm noktalarından biri de 1991 yılında Tim Berners-Lee tarafından World Wide Web (WWW) sisteminin geliştirilmesi olmuştur. HTML dilinin kullanıma sunulması ve ilk web sitesinin CERN bünyesinde yayımlanmasıyla birlikte internet, metin tabanlı bir iletişim ortamından görsel ve hipermetin temelli bir yapıya dönüşmüştür. Ardından geliştirilen Mosaic ve Netscape gibi web tarayıcıları sayesinde internet, teknik uzmanlık gerektiren bir sistem olmaktan çıkarak geniş kullanıcı kitlelerinin erişebildiği küresel bir bilgi ağı hâline gelmiştir.

Bu teknolojik gelişmelerin doğal bir sonucu olarak sosyal medya platformları ortaya çıkmış ve internetin işlevi köklü bir biçimde değişmiştir. İnternet artık yalnızca bilgiye erişim sağlayan pasif bir ortam olmaktan çıkmış; kullanıcıların içerik üretebildiği, paylaşabildiği ve etkileşim kurabildiği dinamik bir iletişim alanına dönüşmüştür.

Özellikle Web 2.0 teknolojilerinin gelişmesiyle birlikte bireyler, bilgi tüketen kullanıcılar olmanın yanı sıra bilgi üreten ve yayan aktörler hâline gelmiştir. Facebook, Twitter (günümüzde X), YouTube, Instagram ve TikTok gibi platformlar, bireylerin düşüncelerini geniş kitlelere ulaştırmasına, toplumsal olaylara anlık tepki vermesine ve kamuoyu oluşturmaya olanak sağlayan dijital kamusal alanlar yaratmıştır. Bu durum, geleneksel medyanın tek yönlü iletişim yapısını dönüştürmüş ve bilgi akışının merkezi kurumlardan bireylere doğru yönelmesine katkı sağlamıştır.

SOSYAL MEDYANIN TOPLUMSAL VE STRATEJİK ÖNEMİ

Günümüzde sosyal medya, kamuoyu oluşturma ve yönlendirme kapasitesi bakımından devletler, özel sektör kuruluşları, medya kurumları ve sivil toplum örgütleri için stratejik bir araç olarak değerlendirilmektedir. Özellikle seçim süreçleri, toplumsal hareketler, kriz dönemleri, afetler ve olağanüstü durumlarda sosyal medya platformları, bilgi paylaşımının ve kamu iletişiminin merkezinde yer almaktadır. Bu platformlar sayesinde bilgi çok kısa sürelerde geniş kitlelere ulaştırılabilmekte ve böylece toplumsal olaylara ilişkin farkındalık oluşturulabilmektedir. Bununla birlikte sosyal medyanın sağladığı hız ve erişilebilirlik çeşitli riskleri de beraberinde getirmektedir. Dezenformasyon, yanlış bilgi, manipülasyon ve bilgi kirliliği gibi sorunlar, sosyal medya ekosisteminin en önemli tartışma alanları arasında yer almaktadır. Doğruluğu teyit edilmemiş içeriklerin kısa sürede milyonlarca kullanıcıya ulaşabilmesi; toplumsal panik, kutuplaşma ve güven kaybı gibi sonuçlar doğurabilmektedir. Bu nedenle sosyal medya, bir yandan ifade özgürlüğünü ve demokratik katılımı güçlendiren bir iletişim ortamı sunarken diğer yandan dijital güvenlik, etik iletişim ve bilgi doğrulama mekanizmaları açısından yeni düzenlemeler ve politikalar gerektirmektedir. Öte yandan sosyal medya yalnızca risklerden ibaret bir iletişim alanı değildir. Sosyal medya aynı zamanda kamu kurumları, özel sektör kuruluşları ve sivil toplum örgütleri açısından hızlı bilgilendirme, kriz iletişimi yürütme, hedef kitlelerle doğrudan etkileşim kurma ve toplumsal farkındalık oluşturma konularında önemli fırsatlar sunmaktadır. Özellikle afetler, salgın hastalıklar ve güvenlik krizleri gibi olağanüstü durumlarda sosyal medya; resmî açıklamaların geniş kitlelere hızla ulaştırılması, yanlış bilgilerin düzeltilmesi ve toplumun doğru yönlendirilmesi açısından kritik bir işlev üstlenmektedir.

Sonuç olarak sosyal medya, günümüzde yalnızca bir iletişim teknolojisi olarak değil; toplumsal algının şekillendiği, kamusal tartışmaların yürütüldüğü, ekonomik faaliyetlerin yönlendirildiği ve kriz yönetim süreçlerinin gerçekleştirildiği stratejik bir dijital güç alanı olarak değerlendirilmektedir. Bu nedenle sosyal medyanın tarihsel gelişimi, teknik altyapısı ve toplumsal etkileri, çağdaş iletişim çalışmalarının temel araştırma alanları hâline gelmiştir.

SOSYAL MEDYA PLATFORMLARI

NEXT SOSYAL / NSOSYAL

NEXT Sosyal, güncel adıyla NSosyal, kullanıcıların metin, görsel, video ve anket gibi farklı içerik türleri aracılığıyla paylaşım yapabildiği yeni nesil sosyal medya platformlarından biridir. Platform, kullanıcıların gündemi takip edebilmesine, fikirlerini paylaşabilmesine, farklı kişi ve topluluklarla etkileşim kurabilmesine imkân sağlayan dijital bir sosyal ağ yapısına sahiptir. Mobil cihazlar üzerinden kullanılabilen uygulama, sosyal medya kullanıcılarının içerik üretme, paylaşma ve etkileşim kurma alışkanlıklarına yerli bir alternatif sunması bakımından dikkat çekmektedir.

Kamu kurumları ve mülki idare amirleri açısından NEXT Sosyal / NSosyal gibi yeni nesil sosyal medya platformları, vatandaşlarla doğrudan iletişim kurulması, yerel gündemin takip edilmesi, resmî duyuruların farklı hedef kitlelere ulaştırılması ve kriz dönemlerinde doğru bilginin yaygınlaştırılması bakımından değerlendirilebilecek mecralar arasında yer almaktadır. Özellikle yerel yönetim, güvenlik, afet, kamu hizmetleri, etkinlik duyuruları ve toplumsal farkındalık içerikleri açısından bu tür platformların gelişimi yakından izlenmelidir.

Kurumsal sosyal medya yönetiminde her platformun kullanıcı profili, teknik özellikleri, içerik formatları ve etkileşim biçimleri farklılık gösterebilmektedir. Bu nedenle NEXT Sosyal / NSosyal üzerinde yürütülecek kurumsal iletişim faaliyetlerinde platformun güncel kullanım özellikleri, hesap güvenliği seçenekleri, doğrulama imkânları, topluluk kuralları ve içerik görünürlüğü düzenli olarak takip edilmelidir. Kurumsal hesap açılması veya aktif paylaşım yapılması hâlinde, kurum kimliğine uygun kullanıcı adı, profil görseli, açıklama metni ve iletişim bilgilerinin doğru şekilde belirlenmesi önem taşımaktadır.

Bu platformda paylaşılacak içeriklerde de diğer sosyal medya mecralarında olduğu gibi doğruluk, tarafsızlık, açıklık, erişilebilirlik ve kurumsal tutarlılık ilkeleri gözetilmelidir. Paylaşımlar kısa, anlaşılır ve teyit edilmiş bilgiye dayanmalı; kişisel verilerin korunmasına, özel hayatın gizliliğine ve kamu güvenliğini ilgilendiren hassas bilgilerin paylaşılmasına özen gösterilmelidir. Görsel ve video içeriklerinde erişilebilirlik ilkeleri dikkate alınmalı; gerekli durumlarda açıklayıcı metin, altyazı ve sade anlatım tercih edilmelidir.

NEXT Sosyal / NSosyal gibi gelişmekte olan platformlar, kamu kurumlarının dijital iletişim kapasitesini çeşitlendirme potansiyeli taşımaktadır. Bununla birlikte kurumsal hesap yönetiminde aceleci davranılmamalı; platformun kurumsal iletişim hedeflerine uygunluğu, hedef kitleye erişim kapasitesi, güvenlik altyapısı ve sürdürülebilir kullanım imkânları değerlendirilmelidir. Yeni platformların takip edilmesi, kamu iletişiminin değişen dijital medya ekosistemine uyum sağlaması açısından önem arz etmektedir.

FACEBOOK

Facebook, bireylerin, kurumların, markaların, kuruluşların ve toplulukların farklı içerik türleri aracılığıyla hedef kitleleriyle iletişim kurabildiği yaygın sosyal medya platformlarından biridir. Platform; metin, fotoğraf, video, canlı yayın, hikâye, etkinlik ve bağlantı paylaşımı gibi farklı içerik formatlarını desteklemekte; kullanıcıların paylaşımlara yorum, beğeni ve paylaşım yoluyla etkileşimde bulunmasına imkân sağlamaktadır. Bu yönüyle Facebook, hem geniş kullanıcı kitlesine ulaşmak hem de farklı yaş gruplarına yönelik bilgilendirme faaliyetleri yürütmek açısından önemli bir dijital iletişim mecrasıdır.

Kamu kurumları ve mükiidare amirleri açısından Facebook, vatandaşlarla doğrudan iletişim kurulması, resmî duyuruların paylaşılması, etkinliklerin tanıtılması, kamu hizmetlerine ilişkin bilgilendirmelerin yapılması ve kriz dönemlerinde doğru bilginin hızlı biçimde yaygınlaştırılması bakımından etkili bir araç olarak değerlendirilebilir. Özellikle yerel düzeyde yürütülen çalışmaların görünürlüğünün artırılması, vatandaşların güncel gelişmelerden haberdar edilmesi ve toplumun farklı kesimleriyle sürekli iletişim kurulması bakımından Facebook sayfaları kurumsal sosyal medya yönetiminde önemli bir yer tutmaktadır.

Kurumsal Facebook sayfalarının yönetiminde profil fotoğrafı, kapak görseli, kullanıcı adı, iletişim bilgileri, kurum açıklaması ve bağlantı adresleri güncel ve kurumsal kimlikle uyumlu olmalıdır. Sayfada yer alan bilgiler, vatandaşların kuruma hızlı ve doğru biçimde ulaşmasını sağlayacak şekilde düzenlenmelidir. Ayrıca sayfa yöneticilerinin görev ve yetkileri kontrollü biçimde tanımlanmalı; hesap güvenliği, iki aşamalı doğrulama, şifre yönetimi ve yetki devri gibi hususlar düzenli olarak gözden geçirilmelidir.

Facebook'ta paylaşılacak içeriklerde doğruluk, açıklık, tarafsızlık ve kurumsal tutarlılık ilkeleri gözetilmelidir. Kamu hizmetleri, afet ve acil durum duyuruları, yol kapanmaları, etkinlikler, başvuru süreçleri ve toplumsal farkındalık çalışmaları gibi konularda hazırlanan paylaşımlar kısa, anlaşılır ve teyit edilmiş bilgiye dayanmalıdır. Paylaşımlarda spekülasyon, ayrıştırıcı veya kesinliği bulunmayan ifadeler yer verilmemeli; özel hayatın gizliliği, kişisel verilerin korunması ve kamu güvenliğine ilişkin hassasiyetler dikkate alınmalıdır.

Facebook'un etkileşim odaklı yapısı nedeniyle yorum ve mesaj yönetimi de kurumsal iletişimin önemli bir parçasıdır. Vatandaşlardan gelen soru, talep ve yorumlar düzenli olarak takip edilmeli; gerekli durumlarda ilgili birimlere yönlendirme yapılmalıdır. Ancak kişisel veri içeren başvuruların yorum alanlarında yürütülmemesine dikkat edilmeli, vatandaşlar resmî başvuru kanallarına yönlendirilmelidir. Kriz dönemlerinde ise tek merkezli, hızlı ve doğrulanmış bilgi akışı sağlanmalı; yanlış veya yanıltıcı içeriklere karşı resmî açıklamalar görünür biçimde paylaşılmalıdır.

Facebook, kurumsal iletişimde geniş kitlelere ulaşma ve vatandaş etkileşimini artırma potansiyeli taşıyan bir platformdur. Bununla birlikte platformun algoritmik yapısı, yorum dinamikleri ve hızlı etkileşim ortamı dikkate alınarak içerikler planlı, ölçülebilir ve sorumlu bir iletişim anlayışıyla hazırlanmalıdır. Kurumsal hesapların düzenli, güvenli ve erişilebilir biçimde yönetilmesi, kamu kurumlarının dijital görünürlüğünü ve vatandaş nezdindeki güvenilirliğini güçlendirecektir.

LINKEDIN

LinkedIn, profesyonel ağ kurma, kurumsal görünürlük oluşturma, uzmanlık paylaşımı ve iş dünyasına yönelik iletişim faaliyetleri için kullanılan sosyal medya platformlarından biridir. Platform; kurumların,

kuruluşların ve profesyonellerin bilgi, deneyim, haber, faaliyet ve duyurularını paylaşmasına imkân sağlamaktadır. LinkedIn'in diğer sosyal medya mecralarından ayrılan temel yönü, daha çok mesleki kimlik, kurumsal itibar, uzmanlık alanları, kariyer gelişimi ve sektörel etkileşim odaklı bir yapıya sahip olmasıdır.

Kamu kurumları ve mülki idare amirleri açısından LinkedIn, kurumsal faaliyetlerin profesyonel hedefkitlelere aktarılması, kamu hizmetlerinde iyi uygulamaların paylaşılması, ulusal ve uluslararası paydaşlarla iletişim kurulması, insan kaynağına yönelik duyuruların yapılması ve kurumsal itibarın güçlendirilmesi bakımından değerlendirilebilecek önemli bir platformdur. Özellikle strateji belgeleri, projeler, çalıştaylar, eğitim faaliyetleri, uluslararası temaslara, kamu-özel sektör iş birlikleri ve kurumsal başarı hikâyeleri LinkedIn'in yapısına uygun içerik türleri arasında yer almaktadır.

Kurumsal LinkedIn sayfalarının yönetiminde kurum adı, logo, kapak görseli, açıklama metni, faaliyet alanı ve iletişim bilgileri kurumsal kimlikle uyumlu ve güncel biçimde düzenlenmelidir. Sayfada kullanılan dil, profesyonel, sade ve güvenilir olmalıdır. LinkedIn'de hedef kitle çoğunlukla profesyoneller, kurum temsilcileri, akademisyenler, medya mensupları, sivil toplum kuruluşları ve ilgili sektör paydaşlarından oluşabileceği için içeriklerin kurumsal ciddiyeti yansıtacak bir üslupla hazırlanması önem taşımaktadır. LinkedIn paylaşımlarında kurumun faaliyetleri yalnızca duyuru diliyle değil, aynı zamanda kamu değeri, stratejik hedef, toplumsal katkı ve kurumsal kapasite boyutlarıyla ele alınmalıdır. Bir etkinlik, toplantı veya proje paylaşılırken yalnızca "gerçekleştirildi" ifadesiyle yetinilmemeli; faaliyetin amacı, katkısı, hedef kitlesi ve kamu yararı açık biçimde belirtilmelidir. Bu yaklaşım, kurumun yalnızca görünürlüğüne değil, aynı zamanda itibarını ve uzmanlık algısını da güçlendirmektedir.

LinkedIn'de paylaşılacak içeriklerde doğruluk, ölçülülük, kurumsal tutarlılık ve profesyonel temsil ilkelerine dikkat edilmelidir. Aşırı gündelik, duygusal veya kampanya diliyle hazırlanmış içerikler yerine; açık, bilgi temelli, dengeli ve kurumsal anlatım tercih edilmelidir. Görsellerde kurumsal kimlik unsurları korunmalı; metin yoğunluğu düşük, sade ve profesyonel tasarımlar kullanılmalıdır. Video, infografik ve belge paylaşımlarında erişilebilirlik ilkeleri gözetilmeli; gerekli durumlarda açıklayıcı metin, alt yazı ve sade anlatım tercih edilmelidir.

LinkedIn, kriz ve acil durum iletişiminden ziyade kurumsal itibar, profesyonel görünürlük ve paydaş iletişimi açısından daha güçlü bir mecradır. Bununla birlikte kamuoyunu ilgilendiren önemli gelişmelerde, kurumun resmî tutumunu destekleyen açıklamalar ve bilgilendirici içerikler LinkedIn üzerinden de paylaşılabilir. Bu tür durumlarda içerikler diğer resmî sosyal medya hesaplarıyla uyumlu olmalı; çelişkili, gecikmiş veya farklı tonlarda açıklamalardan kaçınılmalıdır.

LinkedIn'in kurumsal sosyal medya stratejisindeki yeri, hedef kitle ve içerik türü bakımından doğru belirlenmelidir. Platform, kamu kurumlarının uzmanlık alanlarını, projelerini, kurumsal kapasitesini ve paydaş ilişkilerini görünür kılmak için etkili bir araçtır. Bu nedenle LinkedIn içerikleri, kısa vadeli etkileşimden ziyade uzun vadeli kurumsal itibar, güvenilirlik ve profesyonel iletişim hedefleri doğrultusunda planlanmalıdır.

YOUTUBE

Video görüntüleri, sosyal medya platformlarında en çok tüketilen içeriklerin başında gelmektedir. “*Broadcast yourself*” (kendini yayınla) sloganıyla yola çıkan YouTube dünyada en çok tıklanan video paylaşım sitesi olmasının yanı sıra Türkiye'nin de en popüler sosyal medya platformudur.

YouTube'da video izlemek, beğenmek, yüklemek, canlı yayın açmak, topluluklarla etkileşime girmek mümkünken aynı zamanda kanallara da abone olunabilmektedir. Video yüklemek, yorum yapabilmek ve oynatma listesi oluşturabilmek için ayrıca YouTube kanalı kurmanız gerekmektedir. Kanal simgesi ve kanal resminin profesyonel olarak hazırlanması ve kanalı yansıtmaları oldukça önemlidir.

YouTube'a en fazla 15 dakika uzunluğunda video yüklenebilmektedir. Hesap doğrulamasıyla tek seferde 12 saate (veya 256 GB dosya boyutuna) kadar video yüklenebilmektedir. “YouTube Shorts” özelliğiyle 60 saniyeye kadar dikey, hızlı tüketilen kısa video formatında içerik üretilmesine olanak sağlanmaktadır.

Bireylerin birbirleri hakkındaki izlenimlerinin tanıştıkları ilk saniyede şekillendiği düşünüldüğünde YouTube kanalının temel bileşenlerinin de doğru hazırlanması önemlidir. Ayrıca **izleyicinin ilgisini çekmek**

için ilk üç saniye videonun konusunun ana hatlarıyla çizilmesi gerekmektedir. Çünkü izleyiciler, videonun ilk saniyelerinde ilgilerini çeken bir içerikle karşılaşmadıklarında videoyu izlemeyi bırakabilmekte veya başka bir içeriğe yönelmeyi tercih edebilmektedir.

INSTAGRAM

Türkiye'nin en popüler sosyal medya platformlarından biri olan Instagram, görsel ağırlıklıdır. Önceleri fotoğraf filtreleme ve paylaşma uygulaması olarak kullanılan platform, zamanla hikâye (story) ekleme ve canlı yayın gibi özelliklerle hareketli görüntülerin de yoğun paylaşıldığı bir sosyal medya mecrasına dönüşmüştür.

Instagram'ın Reels özelliği, kullanıcıların dikey formatta video içerikleri üretmesine, bu içeriklere müzik, filtre ve efektler eklemesine ve bunları platformun Reels akışı üzerinden geniş kitlelere ulaştırmasına olanak sağlamaktadır. 24 saat sonra kaybolan fotoğraf ve videolar hikâye şeklinde paylaşılabilmektedir. Ayrıca yapay zekâ destekli soruları yanıtlayan bir asistan da bulunmaktadır. Yapay zekâ içerik üretimi, güvenlik alanı ve doğrudan iletişim gibi birçok süreçte kullanılmaktadır. Özellikle dikey içerik tüketiminin artmasıyla birlikte sosyal medya platformları "vertical-first" olarak adlandırılan mobil öncelikli bir yapıya evrilmiştir. Instagram'ın 2025 sonrası 4:5 formatlarını öne çıkarması da bunun en önemli göstergelerinden biridir. Kurumsal hesaplar için önerilen temel ölçüler; gönderilerde 1080x1350 piksel (4:5), Reels ve hikâyelerde ise 1080x1920 piksel (9:16) formatıdır.

Instagram, mobil kullanım odaklı yapısı ve görsel ağırlıklı içerik formatıyla öne çıkan bir sosyal medya platformudur. Platformun yapısal özellikleri nedeniyle kullanıcılar, diğer hesaplara ait gönderileri kendi akışlarında doğrudan yayımlayamamakta; ayrıca standart akış gönderilerinde tıklanabilir bağlantı kullanımının sınırlı olması, içeriklerin harici kaynaklara yönlendirilmesini güçleştirebilmektedir.

X PLATFORMU

X, kullanıcılar tarafından oluşturulan içeriklerin takipçilerle paylaşılmasına olanak veren, direkt mesaj özelliği ile kullanıcıların birbirleriyle sohbet etme şansı bulabildikleri bir mikroblog olarak nitelendirilen sosyal ağ sitesidir. Paylaşımlar metin, fotoğraf ve video

şeklinde gerçekleştirilmektedir. Paylaşımlar 280 karakterle sınırlıdır. X için önerilen görsel boyutları; yatay içeriklerde 1200 × 675 piksel, dikey içeriklerde ise 1080x1350 piksel formatıdır.

Kullanıcılar, konu veya tür gibi içerikleri dikkate alarak gönderilerini bir araya getirebilmekte, bunu “#” işareti ile başlayan kelimeler veya ifadeler olan etiketleme işlemi ile yapmaktadırlar. Benzer şekilde, “@” işaretinin ardından bir kullanıcı adı eklenerek diğer kullanıcıları etiketleyebilmekte veya onlara cevap verebilmektedirler.

X platformunda yapay zekâ ile üretilen görseller ve deepfake (derin sahte) içerikler kısa sürede geniş kitlelere ulaşabilmektedir. Bu nedenle platform, yapay zekâ tarafından oluşturulmuş veya manipüle edilmiş olabilecek içeriklerin tespit edilmesi ve etiketlenmesine yönelik çeşitli teknolojik araçlar ve doğrulama mekanizmaları kullanmaktadır.

X Platformu, “X Premium” başlığıyla belirli bir meblağ karşılığında abonelik hizmeti sunmaktadır. Abonelik hizmeti içerisinde gönderiyi düzenleme, daha uzun paylaşım gerçekleştirebilme, topluluk oluşturma, mavi onay işareti ve gelir paylaşımı gibi ayrıcalıklar bulunmaktadır.



Platformlara Göre İçerik Formatları

Kurumsal sosyal medya içerikleri için önerilen temel ölçüler

1		NSosyal - Gönderi: 1080 × 1080 px (1:1) - Dikey gönderi: 1080 × 1350 px (4:5) - Video içerik: 1080 × 1920 px (9:16)
2		Facebook - Gönderi: 1080 × 1080 px (1:1) - Dikey gönderi: 1080 × 1350 px (4:5) - Hikâye: 1080 × 1920 px (9:16)
3		LinkedIn - Gönderi: 1080 × 1080 px (1:1) - Dikey gönderi: 1080 × 1350 px (4:5) - Profesyonel, sade ve metin yoğunluğu düşük tasarım tercih edin.
4		YouTube - Video: 1920 × 1080 px (16:9) - Shorts: 1080 × 1920 px (9:16) - Küçük resim: 1280 × 720 px
5		Instagram - Gönderi: 1080 × 1350 px (4:5) - Kare gönderi: 1080 × 1080 px (1:1) - Hikâye / Reels: 1080 × 1920 px (9:16)
6		X - Tek görsel: 1200 × 675 px (16:9) - Dikey görsel: 1080 × 1350 px (4:5) - Birden fazla görselde kırpma kontrolü yapın.

Tasarımda Dikkat Edilecek Noktalar



- ✓ Metin mobil ekranda okunuyor mu?
- ✓ Görselde kurumsal kimlik tutarlı mı?
- ✓ Kritik bilgi ilk bakışta görülüyor mu?
- ✓ Erişilebilirlik unsurları kontrol edildi mi?
- ✓ Platform oranına göre güvenli alan bırakıldı mı?
- ✓ Paylaşım öncesi son ön izleme yapıldı mı?



Not : Platform özellikleri zaman içinde güncellenebilir. Paylaşım öncesinde güncel ölçülerin kontrol edilmesi önerilir.

SOSYAL MEDYADA KİMLİK VE ALGORİTMİK PROFİLLEME

Sosyal medya kullanıcı profili, bireyin çevrim içi ortamda bıraktığı dilsel, içeriksel ve konumsal izlerle ilişkilidir. Çevrim içi dil kullanımı, yaş, cinsiyet, kişilik, politik ideoloji ve mesleki sınıf gibi kullanıcı özelliklerine dair göstergeler sunabilmekte; konum bilgisi içeren sosyal medya gönderileri de demografik verilerle birlikte kullanıcı profillemeye süreçlerinde kullanılabilir. Kullanıcı profili, sabit ve değişmez bir bilgi kümesi değildir. Sosyal ağlarda kullanıcı profili, kişinin özellikleri, ilgileri, düşünceleri ve tercihleriyle ilişkilendirilen, zaman içinde değişebilen dinamik bir yapı olarak ele alınmaktadır.

Sosyal ağ siteleri, depolanmış kullanıcı profillerindeki veriler aracılığıyla bireyleri birbirine bağlamakta; bu profiller diğer kullanıcılar için bir tanımlama işlevi görmektedir. Profil bilgilerindeki bilgi oranı ve düzeni, sosyal ağ siteleri arasındaki önemli ayırt edici unsurlardan biri olarak değerlendirilmektedir.

Sosyal medya kullanıcıları platformları farklı ihtiyaçlarını karşılamak amacıyla kullanmaktadır. Sosyal medya kullanımında sosyal etkileşim, bilgi arama, zaman geçirme, eğlence, rahatlatma, iletişimsel fayda, kullanım kolaylığı, fikir ifade etme, bilgi paylaşımı ve başkalarını gözlemleme gibi temel doyumlar belirlenmiştir. Sosyal medya kullanım motivasyonları, yalnızca bireysel tercihleri değil, platform içindeki davranış biçimlerini de anlamaya yardımcı olmaktadır.

Güncel bir sistematik derlemede, kullanıcıların sosyal medyada çeşitli beklentilerini ve ihtiyaçlarını karşılamak için farklı uygulamaları tercih ettikleri ve bu platformlarda farklı etkinliklere yöneldikleri belirtilmektedir. Sosyal medyada kimlik, fiziksel bedenden ayrılarak sürekli inşa edilebilen bir yapı hâline gelmektedir. Kimliğin temsil süreci, kullanıcılara ait profillerdeki fotoğraflarla başlamakta; Instagram'da oluşturulan profiller ve etkileşimler bu temsil sürecinde önemli hâle gelmektedir. Sosyal medyada benlik ve mahremiyetin sunumu, yalnızca bireysel bir mesele olarak değil, toplumsal anlamı olan bir süreç olarak da ele alınmaktadır.

Benliğin sosyal medyada sunulması, mahremiyetin dönüşümüyle birlikte değerlendirildiğinde kullanıcı profillerinin aynı zamanda toplumsal ilişkiler ve görünürlük kültürüyle bağlantılı olduğu görülmektedir. **Bu nedenle sosyal medya kullanıcı profili, yalnızca teknik bir hesap bilgisi değildir.** Profil, kullanıcının kendisini nasıl görünür kıldığı, hangi kimlik göstergelerini öne çıkardığı ve mahremiyet sınırlarını nasıl düzenlediğiyle doğrudan ilişkilidir.

Algoritmik profillemeye, kullanıcıların dijital ortamda bıraktığı verilerin sınıflandırılması ve yorumlanmasıyla ilişkili bir süreçtir. Bu tür profillemeye uygulamaları finans, pazarlama, hukuk, kültürel tüketim ve sosyal etkileşim gibi farklı toplumsal alanlarda yaygınlaşmış; sosyal medya ve hedefli reklamcılık bağlamında kullanıcıların bu profillemeye ilişkin farkındalıkları ve algıları önemli hâle gelmiştir. Sosyal medya profillemeye alanındaki çalışmalar, kullanıcı profillemenin giderek genişleyen bir araştırma alanına dönüştüğünü göstermektedir.

Algoritmalar, sosyal medya platformlarında kullanıcıların geçmiş davranışlarından hareketle hangi kullanıcıya hangi reklamın ya da içeriğin gösterileceği konusunda belirleyici olmaktadır. Bu durum, profillemenin yalnızca veri toplama ile değil, aynı zamanda karar verme süreçleriyle de ilişkili olduğunu göstermektedir. Bu çerçevede algoritmik sistemler, sosyal medya kullanıcılarını yalnızca açık profil bilgileri üzerinden değil, geçmiş davranışlar, ilgi alanları, etkileşim örüntüleri ve platform içi sınıflandırmalar üzerinden de tanımlayabilmektedir. Sosyal medya profillemesinin etik sorunları, özellikle veri toplama, veri işleme, kullanıcı rızası ve mahremiyet başlıklarıyla ilişkilidir.

Sosyal medya platformları kullanıcı davranışlarını analiz edebilmekte; paylaşılan içerikler, beğeniler, yorumlar, tıklamalar ve cihaz bilgileri gibi geniş veri alanlarından yararlanabilmektedir. Bu veriler kullanıcı deneyimini kişiselleştirmek, hedefli reklam sunmak ve platform işlevselliğini geliştirmek amacıyla kullanılabilir. Sosyal medyada mahremiyet sorunu, kullanıcıların çevrim içi davranışlarının izlenmesi ve analiz edilmesiyle daha belirgin hâle gelmektedir.

Sosyal medya platformlarında kullanıcılar tarafından yapılan faaliyetlerin algoritmalar aracılığıyla takip edilmesi ve analiz edilmesi, özel hayatın gizliliği, kişisel bilgilerin korunması ve çeşitli mahremiyet ihlalleri açısından sorun doğurabilmektedir. Büyük veri çağında sosyal medya kullanıcı mahremiyetinin zedelendiği başlıca durumlar arasında kullanıcı profillemeye, hassas hedefleme ve dolandırıcılık riskleri yer almaktadır.

Mahremiyetin korunması için bireylerin, platformların ve devletlerin birlikte sorumluluk üstlenmesi gerektiği vurgulanmaktadır. Bu nedenle sosyal medya profillemesi yalnızca teknik bir veri işleme faaliyeti değildir. Kullanıcının hangi verilerinin toplandığı, bu verilerin hangi amaçlarla işlendiği, kullanıcıların bu süreçler hakkında ne ölçüde bilgilendirildiği ve algoritmik sistemlerin kullanıcıları nasıl sınıflandırdığı, etik açıdan tartışılması gereken konulardır.

SOSYAL MEDYADA GÜVENLİK TEDBİRLERİ

Türkiye’de internete erişim düzeyinin ve aktif sosyal medya kullanıcı sayısının sürekli artış göstermesi, kamu yönetiminde dijitalleşmeyi bir üst aşamaya taşımaktadır. Vatandaşların önemli bir zaman dilimini bu mecralarda geçirmesi ve kriz anlarında bilgiyi doğrulamak için resmî hesapları referans alması, kurumsal sosyal medya yönetimini kamu güvenliğinin önemli bir unsuru hâline getirmektedir.

Kurumsal sosyal medya hesaplarının güvenliği yalnızca teknik bir bilişim meselesi değil; kamu düzeninin korunması, devlet otoritesinin dijital ortamda doğru temsil edilmesi ve vatandaş güveninin sürdürülebilmesi açısından stratejik bir kamu yönetimi konusudur.

Bu mahiyetteki bir sosyal medya hesabının veya yayın kanalının siber saldırıya uğraması, sadece ilgili kurumun itibarını zedelemekle kalmayıp kitlesel kriz anlarında doğru bilgi akışını kesintiye uğratarak kamu düzenini de riske atabilmektedir. Bu riskleri azaltmak için uygulanabilecek bazı yöntemler şunlardır:

Cihaz ve Hesap Güvenliğini Sağlayın: Kurumsal hesaplara erişim sağlanan cihazlarda güncel yazılımlar kullanılmalı, güçlü parola politikaları uygulanmalı, şifreleme yöntemlerinden yararlanılmalı ve güvenli ağ bağlantıları tercih edilmelidir. Ayrıca kişisel ve kurumsal hesapların birbirinden ayrı tutulması önem arz etmektedir.

İki Aşamalı Doğrulamayı Aktif Edin: Sosyal medya hesaplarının güvenliğini artırmak için iki aşamalı doğrulama sistemi kullanılmalıdır. Bu yöntem, yalnızca şifreyle giriş yapılmasını yeterli görmeyerek ek bir güvenlik katmanı sağlamaktadır. Hesaba giriş sırasında telefona gönderilen doğrulama kodu, mobil uygulama onayı veya biyometrik doğrulama gibi ikinci bir adım talep edilmektedir. Böylece şifre ele geçirilmiş olsa bile yetkisiz kişilerin hesaba erişmesi büyük ölçüde engellenebilmektedir. Özellikle kurumsal hesaplarda iki aşamalı doğrulamanın aktif edilmesi, veri güvenliği açısından önemli bir koruma sağlamaktadır.

Şifre Oluşturma ve Hesap Güvenliği: Sosyal medya hesaplarının her biri için benzersiz ve güçlü parolalar oluşturulması gerekmektedir. Şifrelerde büyük-küçük harf, rakam ve özel karakter kullanımına özen gösterilmelidir. Aynı şifrenin birden fazla platformda kullanılması, olası bir güvenlik ihlalinde tüm hesapların risk altına girmesine neden olabilmektedir. Ayrıca belirli aralıklarla şifreleri güncellemek hesap güvenliğini artıracaktır.

Güvenilir Olmayan Linklerden Uzak Durun: Sosyal medya aracılığıyla gönderilen kaynağı belirsiz bağlantılara tıklamaktan kaçınılmalıdır. Bu tür bağlantılar kötü amaçlı yazılımlar içerebilmekte, kişisel bilgileri ele geçirmeyi amaçlayabilmekte veya cihazlara zarar verebilmektedir. Özellikle yabancı kişilerden gelen mesajlara karşı dikkatli olunmalı ve bağlantının doğruluğu mutlaka kontrol edilmelidir.

Kurumsal Hesaplarda VPN Kullanımından Kaçının: Kurumsal sosyal medya hesaplarına VPN üzerinden erişim sağlanması, çeşitli güvenlik açıklarına neden olabilmekte ve kurum verilerinin tehlikeye girmesine yol açabilmektedir. Güvenliği doğrulanmamış VPN servisleri, kullanıcı verilerinin üçüncü kişiler tarafından izlenmesine veya kayıt altına alınmasına sebep olabilmektedir. Bu nedenle kurumsal hesaplara yalnızca kurum tarafından belirlenen güvenli bağlantılar üzerinden erişim sağlanmalıdır.

Hesap Hareketlerini Düzenli Takip Edin: Sosyal medya hesapları belirli aralıklarla kontrol edilerek olağan dışı girişler veya şüpheli işlemler olup olmadığını incelenmelidir. Bilinmeyen cihazlardan yapılan oturum açma işlemleri, izinsiz paylaşımlar veya hesap ayarlarında yapılan değişiklikler, olası bir güvenlik ihlalinin habercisi olabilmektedir. Bu tür durumlarda hızlı müdahale edilmesi büyük önem taşımaktadır.

Halka Açık Kablosuz Ağlara Dikkat Edin: Kafe, restoran veya benzeri ortak kullanım alanlarında sunulan açık Wi-Fi ağları güvenli olmayabilir. Kurumsal ya da kişisel bilgilerin korunması için bilinmeyen ağlar yerine yalnızca güvenilir internet bağlantıları kullanılmalıdır. Ortak ağlar üzerinden yapılan işlemler, siber saldırganlar tarafından izlenebilmekte veya veri hırsızlığına neden olabilmektedir.

Güvenlik Sorunlarında Hızlı Müdahale Edin: Hesabın ele geçirildiğinden şüphelenildiği takdirde derhal şifre değiştirmeli, kurum yetkililerine bilgi verilmeli ve ilgili sosyal medya platformunun destek birimiyle iletişime geçilmelidir. Ayrıca hesaba bağlı e-posta adresi ve diğer güvenlik bilgilerinin de kontrol edilmesi, olası zararların büyümesini önlemeye yardımcı olacaktır.

KURUMSAL SOSYAL MEDYA HESAPLARINDA GÜVENLİK KONTROLÜ

Kurumsal hesapların güvenli yönetimi için temel kontrol alanları

1



GÜÇLÜ PAROLA KULLANIMI

Tahmin edilmesi zor, güçlü ve benzersiz parolalar tercih edin. Parolaları düzenli aralıklarla güncelleyin.

2



İKİ AŞAMALI DOĞRULAMA

Kurumsal hesaplarda iki aşamalı doğrulamayı etkinleştirin. Mümkünse doğrulama uygulaması kullanın.

3



YETKİ VE ERIŞİM YÖNETİMİ

Hesap erişimlerini görev bazlı tanımlayın. Ayrılan personelin yetkilerini gecikmeden kaldırın.

4



CİHAZ GÜVENLİĞİ

Hesapların kullanıldığı bilgisayar ve mobil cihazlarda ekran kilidi, güncel yazılım ve antivirüs koruması bulundurun.

5



ŞÜPHELİ BAĞLANTI VE E-POSTALARA DİKKAT

Kimlik avı girişimlerine karşı dikkatli olun. Bilinmeyen bağlantılara tıklamadan önce kaynağı kontrol edin.

6



HESAP HAREKETLERİNİ İZLEME

Oturum açma kayıtlarını, yetki değişikliklerini ve olağan dışı hareketleri düzenli olarak kontrol edin.

7



ACİL DURUM VE MÜDAHALE PLANI

Hesap ele geçirilmesi veya yetkisiz erişim durumunda uygulanacak hızlı müdahale planı önceden belirlenmelidir.



PAYLAŞIM VE GÜVENLİK ÖNCESİ HIZLI KONTROL

- | | |
|-------------------------------|--------------------------------------|
| ✓ Parola güncel mi? | ✓ Cihazlar güvenli mi? |
| ✓ 2FA aktif mi? | ✓ Şüpheli hareket kontrol edildi mi? |
| ✓ Erişim yetkileri güncel mi? | ✓ Acil müdahale planı hazır mı? |



SOSYAL MEDYA MECRALARI GÜVENLİK AYARLARI REHBERİ

A. META PLATFORMLARI (INSTAGRAM & FACEBOOK) GÜVENLİK AYARLARI

Meta platformlarında kurumsal hesap güvenliği, “Meta Business Suite” sistemi üzerinden merkezî olarak yönetilmelidir. Kurumsal sayfaların kişisel hesaplardan ayrılması, kullanıcı yetkilerinin kontrollü şekilde tanımlanması ve güvenlik ayarlarının düzenli gözden geçirilmesi, hesap güvenliğinin sağlanması açısından büyük önem taşımaktadır.

İki Aşamalı Kimlik Doğrulamayı (2FA) Aktifleştirin:

Kurumsal hesapların güvenliğini artırmak amacıyla iki aşamalı kimlik doğrulama sistemi mutlaka etkinleştirilmelidir. Bu sistem, kullanıcı adı ve şifrenin yanı sıra ek bir doğrulama adımı talep ederek yetkisiz erişim riskini önemli ölçüde azaltmaktadır. Şifre bilgileri ele geçirilmiş olsa dahi doğrulama kodu olmadan hesaba erişim sağlanamamaktadır.

Bu ayarı etkinleştirmek için:

Ayarlar ve Gizlilik > Hesaplar Merkezi > Şifre ve Güvenlik > İki Aşamalı Kimlik Doğrulama adımları takip edilmelidir.

Doğrulama yöntemi olarak SMS yerine, kurumsal telefona kurulacak olan Google Authenticator veya Microsoft Authenticator gibi kimlik doğrulama uygulamalarının kullanılması tavsiye edilmektedir. SMS tabanlı doğrulama yöntemleri, SIM kart kopyalama saldırıları nedeniyle tek başına yeterli güvenlik sağlayamamaktadır. Ayrıca oluşturulan yedek kurtarma kodları güvenli bir ortamda saklanmalıdır.

Personel Yetkilendirme ve Rol Yönetimi:

Kurumsal sosyal medya hesaplarının güvenliği için kullanıcı yetkileri kontrollü şekilde tanımlanmalıdır. Kurumsal hesap şifreleri personelle doğrudan paylaşılmamalı, erişimler Meta Business Suite üzerinden kişisel hesaplar aracılığıyla yetkilendirilmelidir.

Personeler yalnızca görev alanlarına uygun yetkiler verilmelidir. İçerik paylaşımı yapan kullanıcılara “İçerik Oluşturucu” veya “Moderatör” rolü tanımlanması yeterli olacaktır. “Tam Kontrol (Yönetici)” yetkisi ise yalnızca ilgili birim yöneticilerinde bulunmalıdır. Böylece yanlış işlem yapılması veya hesap güvenliğinin ihlal edilmesi riskleri azaltılacaktır.

Etkileşim ve Yorum Filtreleme Ayarları:

Kurumsal hesaplarda dijital itibarın korunması amacıyla yorum filtreleme sistemleri aktif kullanılmalıdır. Hakaret, spam, provokatif ifadeler veya yanıltıcı içeriklerin otomatik olarak filtrelenmesi, hesap yönetiminin daha güvenli ve kontrollü yürütülmesini sağlamaktadır.

Bu işlem için:

Ayarlar > Gizlilik > Gizlenen Sözcükler bölümünden gelişmiş yorum filtreleme özelliği aktif edilmelidir.

“Özel sözcükler ve ifadeler” alanına kuruma yönelik risk oluşturabilecek kelime ve ifadeler eklenerek bu yorumların otomatik gizlenmesi sağlanabilmektedir. Bu yöntem, özellikle kriz yönetimi süreçlerinde kurumsal itibarın korunmasına katkı sağlamaktadır.

B. X PLATFORMU GÜVENLİK AYARLARI

X platformu, bilgi akışının çok hızlı gerçekleştiği ve dezenformasyon içeriklerinin kısa sürede yayılabildiği bir sosyal medya ağıdır. Aynı zamanda kurumsal hesaplara yönelik kimlik avı, sahte bağlantı ve hesap ele geçirme girişimlerinin yoğun görüldüğü platformlardan biridir. Bu nedenle kurumsal X hesaplarında güvenlik ayarlarının eksiksiz yapılandırılması ve erişim kontrollerinin dikkatli yönetilmesi büyük önem taşımaktadır.

İki Aşamalı Doğrulama ve Şifre Korumasını Aktif Edin:

Kurumsal hesapların güvenliği için iki aşamalı doğrulama sistemi mutlaka etkinleştirilmelidir. Bu sistem, kullanıcı adı ve şifrenin yanı sıra ek bir doğrulama adımı isteyerek yetkisiz erişim riskini azaltmaktadır.



Bu ayarı etkinleştirmek için:

Ayarlar ve Gizlilik > Güvenlik ve Hesap Erişimi > Güvenlik > İki Adımlı Doğrulama adımları izlenmelidir.

Doğrulama yöntemi olarak SMS yerine **Google Authenticator** veya **Microsoft Authenticator** gibi kimlik doğrulama uygulamalarının tercih edilmesi önerilmektedir. SMS tabanlı doğrulama yöntemleri, SIM kart kopyalama saldırıları nedeniyle tek başına yeterli güvenlik sağlamamaktadır.

Aynı bölümde bulunan “**Şifre Sıfırlama Koruması**” özelliğinin de aktif edilmesi gerekmektedir. Bu özellik sayesinde hesap şifresinin sıfırlanabilmesi için ek doğrulama bilgileri talep edilmekte ve hesap ele geçirme girişimlerine karşı ek koruma sağlanmaktadır. Ayrıca yedek kurtarma kodlarının güvenli bir ortamda saklanması önem arz etmektedir.

Kurumsal Erişim ve Yetki Yönetimi:

Kurumsal hesap şifreleri personelle doğrudan paylaşılmamalıdır. Bunun yerine X platformunun ekip yönetimi özellikleri kullanılarak personele görev bazlı erişim yetkileri tanımlanmalıdır.

Bu işlem için:

X Pro (TweetDeck) > Teams (Takımlar) bölümü kullanılmalıdır.

Paylaşım yapacak personele “Contributor (İçerik Sağlayıcı)” gibi sınırlı yetkiler verilmesi önerilmektedir. Yönetici yetkileri yalnızca sorumlu birim yöneticilerinde bulunmalıdır. Böylece yanlış paylaşım yapılması, yetkisiz erişim veya hesap güvenliği ihlali riskleri önemli ölçüde azaltılmış olacaktır.

Etiketleme ve Görünürlük Ayarlarını Kontrol Edin:

Kurumsal hesapların alakasız, yanıltıcı veya itibar zedeleyici içeriklerle ilişkilendirilmesini önlemek amacıyla etiketleme ayarları dikkatli yapılandırılmalıdır.

Bu ayar için:

Ayarlar ve Gizlilik > Gizlilik ve Güvenlik > Etiketleme ve Bahsedilmeler bölümü kullanılmalıdır.

Fotoğraf etiketleme özelliğinin “Kapalı” veya “Sadece takip ettiğin kişiler” şeklinde ayarlanması tavsiye edilmektedir. Ayrıca bahsetme ve mesaj ayarlarının düzenli kontrol edilmesi, kurumun sahte hesaplar veya spam içerikler aracılığıyla hedef alınmasını önlemeye yardımcı olmaktadır.

Şüpheli Bağlantı ve Mesajlara Karşı Dikkatli Olun:

X platformunda doğrudan mesajlar veya gönderiler aracılığıyla paylaşılan bağlantılar dikkatle incelenmelidir. Özellikle doğrulanmamış hesaplardan gelen bağlantılar kimlik avı saldırıları içerebilmektedir. Kurumsal hesap yöneticileri, bağlantıların güvenilirliğini doğrulamadan hiçbir dosya indirmemeli veya giriş bilgilerini paylaşmamalıdır.



ANLIK MESAJLAŞMA VE YAYIN KANALLARI (WHATSAPP VE TELEGRAM) GÜVENLİK REHBERİ

Valilik ve kaymakamlıkların özellikle basın kuruluşları/mensuplarına yönelik bilgilendirme amacıyla kullandıkları WhatsApp ve Telegram grup ve kanalları iletişimde yeni ve pratik çözüm araçları olarak öne çıkmaktadır. Bu mecralardaki iletişim sürecinin dijital ortamlara etkisini dikkate almak gerekmektedir. Bu kanallar üzerinden paylaşılan içeriklerin sosyal medya ve diğer dijital platformlarda hızla yayılabildiği dikkate alınarak iletişim süreçlerinin planlanması önem taşımaktadır.

WhatsApp ve Telegram kanalları, hedef kitleye “anlık bildirim” (Push Notification) ile doğrudan ulaşma gücüne sahiptir. Bu platformlarda kanal güvenliği, doğrudan kanalı yöneten “kurumsal mobil hatların ve cihazların” güvenliğine bağlıdır.

A. WHATSAPP KANALLARI GÜVENLİK AYARLARI

Ana Hesabın İki Adımlı Doğrulaması:

WhatsApp > Ayarlar > Hesap > İki Adımlı Doğrulama adımlarından 6 haneli bir PIN kodu ve kurumsal e-posta tanımlanmalıdır. Bu ayar, kurumsal SIM kart kopyalansa bile hesabın başka cihazda açılmasını engellemektedir.

Kanal Yöneticisi Yetkilendirmesi:

Kanal Bilgisi > Yöneticileri Davet Et sekmesinden, personele kurumsal hatları üzerinden yetki verilmelidir. Görevi değişen personel “Yöneticiliği İptal Et” seçeneğiyle sistemden çıkarılmalıdır.

Kanal Profil Bilgilerinin Kısıtlanması:

Kanal Ayarları > Kanal Bilgilerini Düzenle seçeneği yalnızca “Sadece Asıl Yönetici” (Kurucu) olarak ayarlanmalıdır. Böylece editör personelin hesabı ele geçirilse dahi kanal adı ve logosu değiştirilemeyecektir.

B. TELEGRAM KURUMSAL KANAL GÜVENLİK AYARLARI

İki Adımlı Doğrulama (Bulut Şifresi) Aktivasyonu:

Ayarlar > Gizlilik ve Güvenlik > İki Adımlı Doğrulama sekmesine gidilmelidir. SMS koduna ek olarak hesaba girişte sorulacak güçlü bir “Bulut Şifresi” ve kurumsal bir kurtarma e-postası belirlenmelidir.

Yönetici Haklarının Sınırlandırılması:

Kanal Yönetimi > Yöneticiler > Yönetici Ekle adımları izlenmelidir. Personele yetki verirken “Yeni Yönetici Ekleme”, “Mesajları Silme” veya “Kanal Bilgilerini Değiştirme” yetkileri kapatılmalı; yalnızca “Mesaj Gönderme” yetkisi aktif edilmelidir.

Yönetici Anonimliği ve Mesaj İmzalarının Kapatılması:

Yöneticiler menüsünden ilgili personel üzerine tıklayıp alt kısımdaki “Anonim Kal” seçeneği açık konuma getirilmelidir. Ayrıca genel kanal ayarlarından “Mesajları İmzala” özelliği kapalı tutulmalıdır. Böylece tüm mesajlar personel adı olmadan doğrudan kurum kimliğiyle (ör. X Valiliği) yayımlanabilmektedir. Anonim yönetici özelliği yalnızca yetkili personel tarafından kontrollü kullanılmalıdır.

Gizlilik ve Cihaz Yönetimi Denetimi:

Ayarlar > Gizlilik ve Güvenlik > Cihazlar bölümü düzenli kontrol edilmeli ve şüpheli durumlarda “Diğer Tüm Oturumları Sonlandır” seçeneği kullanılmalıdır. Gizlilik başlığından kurumsal numaranın görünürlüğünü “Hiç kimse” olarak ayarlayarak telefon numarası dış dünyaya gizlenmelidir.

Uygulama Notu:

Anlık mesajlaşma kanallarının güvenliği %100 oranında cihaz ve SIM kart güvenliğine bağlıdır. Bu nedenle, bu kanalları yöneten kurumsal telefonların güçlü şifrelerle ve biyometrik verilerle (parmak izi/yüz tanıma) korunması, harici/güvensiz Wi-Fi ağlarına bağlanmaması idari bir zorunluluk olarak uygulanmalıdır.

KURUMSAL SİBER OLAY MÜDAHALE VE YÖNETİM PROSEDÜRLERİ

Kurumsal Doğrudan Mesaj (DM) Güvenlik Politikası

- DM üzerinden şifre/link paylaşılmamalı,
- Kurum personeli sosyal medya üzerinden kimlik doğrulaması yapmamalı,
- Vatandaş doğrulama talepleri resmî çağrı merkezine yönlendirilmeli,
- “Acil işlem gerekiyor” içerikli mesajlar ikinci kanaldan teyit edilmeli,
- PDF/ZIP/DOC uzantılı bilinmeyen dosyalar açılmamalı,
- Sahte mavi tik/doğrulama mesajlarına dikkat edilmeli.

Kurumsal Sosyal Medya Acil Müdahale Prosedürü

- Tüm aktif oturumlar sonlandırılmalı,
- Şifre ve 2FA bilgileri yenilenmeli,
- Platform destek ekiplerine hızlı bildirim sağlanmalı,
- Kamuoyuna alternatif resmî kanallardan duyuru yapılmalı,
- Siber olay kaydı tutulmalı,
- Gerekirse Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Siber Olaylara Müdahale Ekibi (SOME) koordinasyonu sağlanmalı.

Kurumsal Mobil Cihaz Güvenliği

- Kurumsal hesaplar mümkünse kişisel cihazlardan yönetilmemeli,
- Root/Jailbreak¹ yapılmış cihaz kullanılmamalı,
- Uygulamalar sadece resmî mağazalardan indirilmeli,
- Cihazlarda ekran kilidi zorunlu olmalı,
- Kayıp/çalıntı durumunda uzaktan silme aktif olmalı.

Yapay Zekâ Destekli Dezenformasyona Karşı Önlemler

- Resmî açıklamalar yalnızca doğrulanmış hesaplardan paylaşılmalı,
- Kriz anlarında ekran görüntüsü yerine doğrulanabilir bağlantı kullanılmalı,
- Kurum logoları ve yöneticilerin görüntüleriyle yapılan sahte içeriklere karşı hızlı yalanlama prosedürü oluşturulmalı,
- Özellikle yapay zekâ ile üretilmiş sahte açıklama görselleri ve belgelerine karşı doğrulama mekanizmaları devreye alınmalıdır.

Ele alınan teknik ve idari güvenlik önlemlerinin eksiksiz uygulanması için kamu kurumlarında şu stratejik adımların atılması önerilmektedir:

¹ Jailbreak: Genellikle Apple iOS (iPhone/iPad) cihazlara uygulanır. Fabrika çıkışlı kilitli olan sistemi “kırarak” Apple’ın onaylamadığı mağazalardan (Cydia, Sileo vb.) uygulama yüklemenize, sistem arayüzünü derinlemesine değiştirmenize olanak tanır. Root: Android işletim sistemli cihazlara uygulanır. Sadece üreticinin izin verdiği sınırları kaldırarak telefonun en derin sistem dosyalarına erişmenizi ve müdahale etmenizi sağlar.

1. Siber Dayanıklılık Standartlarının Oluşturulması: İki aşamalı doğrulama sistemlerinin kullanımı, güçlü parola politikalarının uygulanması ve kurumsal erişim yönetim araçlarının tercih edilmesi, bireysel güvenlik önlemleri olarak değil kurumsal bir “Bilişim Güvenliği Standardı” olarak değerlendirilmelidir. Bu uygulamaların tüm birimlerde standart hâle getirilmesi, kurumsal siber dayanıklılığın artırılmasına katkı sağlayacaktır.

2. Yetkilendirme ve Erişim Yönetiminin Güçlendirilmesi: Ortak şifre kullanımına kesinlikle son verilmeli, hesap erişimleri kişiye özel olarak tanımlanmalı ve şifreler düzenli aralıklarla güncellenmelidir. Personele yalnızca görev tanımlarına uygun yetkiler verilmesi sağlanmalı, görev değişikliği veya kurumdan ayrılma durumlarında erişim yetkileri gecikmeksizin kaldırılmalıdır. Böylece yetkisiz erişim ve veri güvenliği riskleri minimize edilecektir.

3. Sürekli Eğitim ve Farkındalık Çalışmaları: Sosyal medya hesaplarını ve dijital yayın mecralarını yöneten personelin; kimlik avı (*phishing*) saldırıları, sosyal mühendislik yöntemleri, mobil cihaz güvenliği ve veri koruma konularında düzenli farkındalık eğitimlerine tabi tutulması gerekmektedir. Güncel tehditlere karşı bilinç düzeyinin artırılması, insan kaynaklı güvenlik zafiyetlerinin önlenmesinde kritik rol oynamaktadır.

Sonuç olarak; dijital çağda güvenli bir kurumsal iletişim mimarisi inşa etmek, en az içerik üretmek kadar kritik öneme sahiptir. Teknik ayarları optimize edilmiş, siber dayanıklılığı yüksek kurumsal hesaplar; kamu hizmetlerinin daha etkin sunulmasına, vatandaş güveninin pekişmesine ve dijital devlet vizyonunun başarıyla sürdürülmesine büyük katkı sağlayacaktır.

KİŞİSEL HESAP GENEL İLKELER

Dijital Ortamda Kurumsal ve Kişisel Temsillerin Geçişkenliğinin Önlenmesi:

Kurumsal e-posta adresi ile kişisel sosyal medya hesabı oluşturulmamalıdır. Kurumsal hesaplardan farklı, güçlü ve benzersiz şifreler kullanılmalıdır. Sosyal medya platformlarında oluşturulan kişisel hesaplar üzerinden göreve, kuruma veya kurumsal faaliyetlere ilişkin herhangi bir bilgi, görsel ya da yorum paylaşmaktan kaçınılmalıdır. Kişisel hesaplarda yer alan içeriklerin kurumsal kimliklerle ilişkilendirilebileceği her zaman göz önünde bulundurulmalıdır. Sosyal medya paylaşımlarında kullanılan fotoğraf ve videolarda yer alan ortamların, kurumun itibarını zedeleyebilecek unsurlar içermemesine dikkat edilmelidir. Kişisel hesaplardan yapılan paylaşımların kurum adına yapılmış gibi algılanmasına neden olabilecek her türlü davranıştan kaçınılmalıdır.

Kişisel Hesabın Gizli (Private) Hâle Getirilmesi:

Kişisel sosyal medya hesaplarının, yalnızca onaylı takipçiler tarafından görüntülenebilir (gizli) şekilde ayarlanması önem arz etmektedir. Bununla birlikte, paylaşımlardan ekran görüntüsü alınarak farklı mecralarda veya kurumsal bağlamda değerlendirilebileceği unutulmamalıdır. Bu nedenle kişisel paylaşımlarda kurumsal kimlikle gelişebilecek içerik ve söylemlerden özellikle kaçınılmalıdır.

Dil ve Söylem Kullanımında Özenli Olunması:

Sosyal medya platformlarında yapılan paylaşımlarda soğukkanlı, saygılı ve sağduyulu bir dil benimsenmelidir. Tüm içeriklerin, toplumsal nezaket ve iletişim kurallarına uygun, yapıcı bir üslupla oluşturulmasına özen gösterilmelidir. Yıkıcı, kırıcı, saldırgan veya provokatif nitelik taşıyan ifadelerden kesinlikle kaçınılmalıdır.

Etkileşimlerde Dikkatli Davranılması:

Sosyal medya platformlarında arkadaşlık isteği gönderirken veya gelen istekleri kabul ederken dikkatli ve seçici olunmalıdır. Görev ve sorumluluklarla ilgili şüphe oluşturabilecek bağlantı ve etkileşimlerden

kaçınılmalıdır. Nefret söylemi, şiddet içeren, ayrımcı, kutuplaştırıcı veya ırkçı içerik üreten kişi ve gruplarla hiçbir şekilde etkileşim kurulmamalıdır. Bu tür hesaplar takip edilmemeli veya arkadaşlık ilişkisi oluşturulmamalıdır.

Aile Üyelerinin Sorumluluğu:

Aile üyelerinin de sosyal medya kullanımı konusunda bilinçlendirilmesi önem arz etmektedir. Özellikle birinci derece yakınların sosyal medya platformlarında hesap oluştururken veya paylaşım yaparken sizin mesleki ve kurumsal kimliğinize atıfta bulunmaması sağlanmalıdır.

Konum Bilgisi ve Günlük Rutinlerin Paylaşılmasından Kaçınılması:

Kişisel sosyal medya hesaplarında anlık konum bilgisi paylaşılmamalı; düzenli olarak bulunulan yerler, günlük rutinler, görev seyahatleri ve kurumla ilişkilendirilebilecek hareketlilik hakkında paylaşım yapılırken dikkatli olunmalıdır. Konum etiketleri, canlı yayınlar ve gerçek zamanlı paylaşımlar; kişisel güvenlik, kurum güvenliği ve bilgi güvenliği açısından risk oluşturabileceğinden gerekli olmadıkça kullanılmamalıdır.

Doğrulanmamış Bilgilerin Paylaşılması:

Sosyal medya platformlarında karşılaşılan haber, görsel, video veya iddialar doğruluğu teyit edilmeden paylaşılmamalı ya da yeniden yayımlanmamalıdır. Yanlış veya yanıltıcı bilgilerin dolaşıma girmesine istemeden katkı sağlanmaması için güvenilir ve resmî kaynaklardan doğrulama yapılmalı; dezenformasyon ve manipülasyon içerebilecek içeriklere karşı dikkatli olunmalıdır.

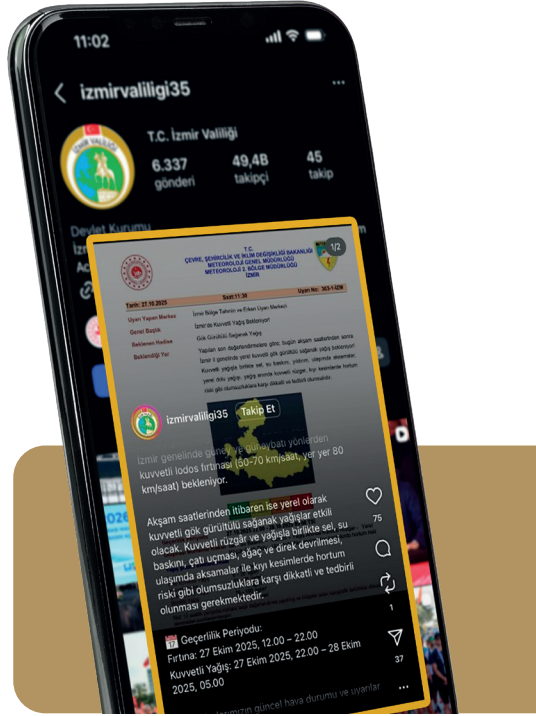
Mesleki Kimlik ve Gizlilik Yükümlülüğüne Riayet Edilmesi:

Kişisel sosyal medya hesaplarında yapılan paylaşımlarda kamu görevlisi olmanın gerektirdiği tarafsızlık, güvenilirlik ve temsil sorumluluğu gözetilmelidir. Görev kapsamında edinilen kamuya açık olmayan bilgi, belge, fotoğraf, toplantı içerikleri veya kurum içi süreçlere ilişkin herhangi bir unsur kişisel hesaplar üzerinden paylaşılmamalıdır. Görev sırasında veya kurum içerisinde çekilen fotoğraf ve videolar paylaşılmadan önce bilgi güvenliği, gizlilik yükümlülüğü ve kurumsal itibar açısından değerlendirilmelidir.

KURUMSAL HESAP GENEL İLKELER

Kamu Yararı:

Sosyal medya içerikleri oluşturulurken ve farklı hesaplarla etkileşim kurarken kamu yararı ilkesi daima ön planda tutulmalıdır. Paylaşımlar; kamuoyunun doğru bilgilendirilmesi, kamu hizmetlerinin etkin şekilde duyurulması, görev yapılan ilin kültürel, ekonomik ve turistik değerlerinin tanıtılması, vatandaşların yaşamını etkileyebilecek gelişmelerin duyurulması ve toplumsal farkındalığın artırılması amacıyla hazırlanmalıdır. İçeriklerin bireysel çıkar veya kişisel görüşlerden ziyade kamu yararına hizmet etmesine özen gösterilmelidir.



Söylem Adabı:

Dijital ortamda oluşturulan içeriklerde düşünceler dürüst, saygılı, net ve ön yargılardan arındırılmış bir üslupla ifade edilmelidir. Nefret söylemi, ayrımcılık ve kutuplaştırıcı ifadelerden kesinlikle kaçınılmalı; siyasi tarafsızlık, kurumsal kimlik ve toplumsal hassasiyetler gözetilmelidir. Ani, tepkisel ve polemik yaratabilecek yorumlardan uzak durulmalı; iletişimde empati ve nezaket esas alınmalıdır. Tamamı büyük harflerle yazılmış içeriklerin “bağırma” algısı oluşturabileceği dikkate alınarak bu tür kullanımlardan kaçınılmalıdır.

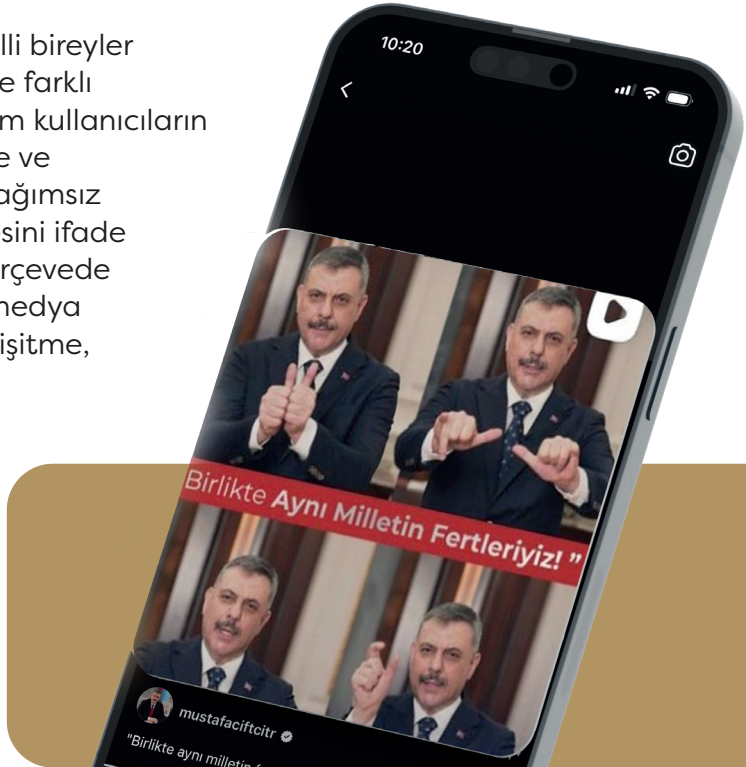
Şeffaflık ve Hesap Verebilirlik:

Sosyal medya hesapları şeffaflık ilkesi doğrultusunda yönetilmeli; paylaşımlar açık, anlaşılır ve doğrulanabilir bilgiler içermelidir. Kamu kaynaklarının etkin ve kamu yararı doğrultusunda kullanıldığı hususu, uygun ve doğru biçimde kamuoyu ile paylaşılmalıdır. Hesap verilebilirlik anlayışı çerçevesinde, paylaşımların güvenilirliği ve tutarlılığı korunmalıdır.

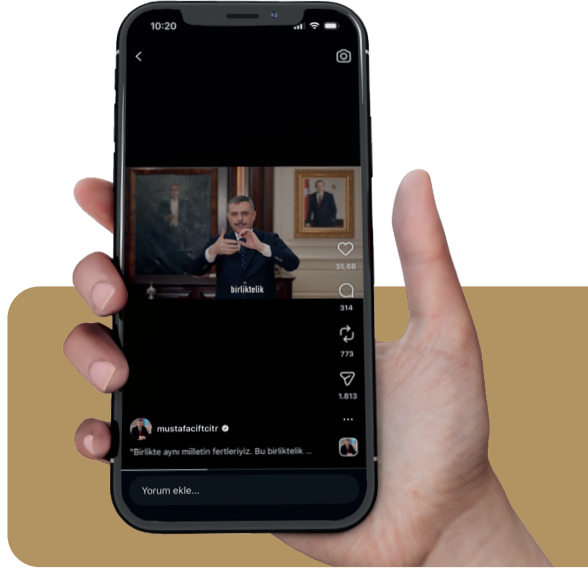
Erişilebilirlik:

Erişilebilirlik, sosyal medya yönetiminde ikincil veya isteğe bağlı bir tasarım unsuru değil; kamu hizmetinin eşitlik, açıklık ve vatandaş odaklılık ilkeleriyle uyumlu biçimde sunulmasının temel şartlarından biridir. Kamu kurumlarının sosyal medya hesaplarında yayımlanan her içerik, toplumun farklı kesimlerinin bilgiye erişim ihtiyacı dikkate alınarak hazırlanmalı; erişilebilirlik, kurumsal iletişim süreçlerinin planlama, üretim, yayımlama ve değerlendirme aşamalarının tamamına dâhil edilmelidir.

Erişilebilirlik, engelli bireyler başta olmak üzere farklı ihtiyaçları olan tüm kullanıcıların bilgiye, hizmetlere ve dijital içeriklere bağımsız şekilde erişebilmesini ifade etmektedir. Bu çerçevede erişilebilir sosyal medya yönetimi; görme, işitme,



fiziksel, bilişsel veya yaşa bağlı farklı gereksinimleri bulunan vatandaşların kamu kurumları tarafından paylaşılan içerikleri takip edebilmesini, anlayabilmesini ve gerektiğinde bu içerikler üzerinden yönlendirilen hizmetlere ulaşabilmesini sağlayacak şekilde yapılandırılmalıdır. Bu kapsamda kurumsal sosyal medya hesaplarında yayımlanan tüm içeriklerde Web Content Accessibility Guidelines (WCAG) 2.2’de yer alan temel ilkeler dikkate alınmalıdır. Konuyla ilgili ayrıntılı bilgiler Ek 2’de yer almaktadır.



Doğru Dil Kullanımı:

Mesleki terimlerin kamuoyunda doğru anlaşılabilmesi için; sade, açık ve anlaşılır Türkçe kullanılmalıdır. Yazılı içeriklerde Türk Dil Kurumu yazım kuralları (sozluk.gov.tr) esas alınmalıdır. Gereğinden uzun, karmaşık ve ağır bir dil yerine doğal, akıcı ve bilgilendirici üslup tercih edilmelidir. Paylaşımlar; kamuoyunu doğru bilgilendirmek, yanlış yönlendirmeyi önlemek ve etkileşimi artırmak amacıyla hazırlanmalıdır.

Uygun Sosyal Medya Platformunun Seçilmesi:

Her sosyal medya platformunun kullanıcı profili ve kullanım amacı farklılık göstermektedir. Bu nedenle içerik stratejisi platforma uygun şekilde belirlenmelidir. Facebook daha çok sosyal etkileşim ve yakın çevre odaklı bir kullanım alanına sahipken LinkedIn profesyonel iletişim ve iş dünyası odaklı bir platformdur. X platformu hızlı bilgi akışı ve gündem takibi açısından önemli olmakla birlikte dezenformasyon riskini de barındırmaktadır. Bu nedenle doğrulanmış ve dikkatle hazırlanmış içeriklerle aktif kullanılmalıdır. Instagram ise görsel anlatım gücü yüksek bir platform olup kurumsal imaj, itibar ve tanıtım açısından etkili bir araçtır.

Söylem Hassasiyeti:

Kamuoyu ile paylaşılan bilgilerin doğruluğu mutlaka güvenilir kaynaklardan teyit edilmelidir. Özellikle kurum dışı kaynaklardan elde edilen bilgilerin doğrulanması kritik önem taşımaktadır. Terör örgütleri veya kötü niyetli yapıların istismar edebileceği içeriklerden kesinlikle kaçınılmalı; gerekli durumlarda paylaşım yapılmamalı veya paylaşım için uygun zaman beklenmelidir.

Gündem Takibi ve Hassas Dönemlerde İletişim:



Güncel ve doğru bilginin kamuoyuna hızlı ve etkin biçimde aktarılması, kurumsal güven açısından büyük önem taşımaktadır. Gecikmiş veya eksik bilgi, kuruma güveni zedeleyebilmektedir. Bu nedenle güncel gelişmelerin yakından takip edilmesi ve uygun içeriklerle zamanında paylaşılması, kurumun güvenilir bilgi kaynağı olarak konumunu güçlendirecektir.

Sosyal medya hesapları, güncel gelişmeler ve kamuoyunun gündeminde yer alan konular açısından düzenli olarak takip edilmelidir. Özellikle toplumsal hassasiyet oluşturan olaylar, afetler, krizler, millî ve manevî değerleri ilgilendiren gelişmeler veya kamuoyunda yoğun tartışmaya neden olan gündem başlıklarında içerik paylaşım süreçleri daha dikkatli yürütülmelidir.

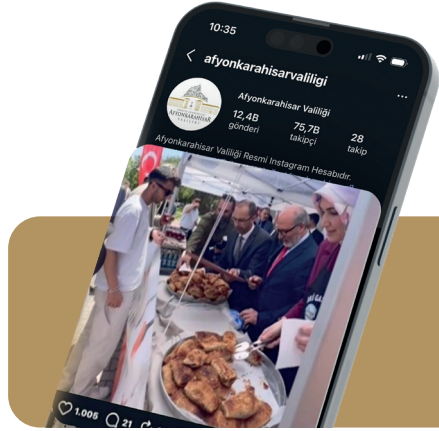
Hassas gündem dönemlerinde kullanılacak dil; sağduyulu, ölçülü, empati temelli ve kamu sorumluluğuna uygun olmalıdır. Bu süreçlerde yanlış anlaşılmaya yol açabilecek ifadelerden, kişisel yorumlardan, tartışmayı artırabilecek söylemlerden ve gündemin hassasiyetleriyle bağdaşmayan içeriklerden kaçınılmalıdır.

Toplumsal hassasiyetin yüksek olduğu dönemlerde eğlence, mizah veya gündemle ilgisiz içeriklerin paylaşılmamasına özen gösterilmelidir. Gerektiğinde iletişim faaliyetlerine kısa süreli ara verilmesi veya yalnızca kamuoyunu bilgilendirmeye yönelik içeriklere yer verilmesi değerlendirilmelidir.

Kurumsal hesapların içerik planlamasında yalnızca paylaşım sıklığı değil; zamanlama, içerik bağlamı ve kamuoyu algısı da dikkate alınmalıdır. Hassas dönemlerde yapılacak her paylaşımın kurumun itibarı, güvenilirliği ve kamu yararı ilkeleri çerçevesinde değerlendirilmesi gerekmektedir.

Düzenleme ve Kararların Duyurulması:

Bölge halkının herhangi bir hak kaybı yaşamaması ve idari yaptırımlarla karşılaşmaması için ülke genelini veya ilgili bölgeyi ilgilendiren yasal düzenlemeler, idari kararlar ve uygulamalara ilişkin bilgilendirmelerin sosyal medya hesapları üzerinden düzenli paylaşılması gerekmektedir. Bu paylaşımlar, vatandaşların doğru ve güncel bilgiye zamanında erişmesini sağlayarak bilgi kirliliğinin önüne geçilmesine katkı sunmaktadır. Aynı zamanda kurumsal sosyal medya hesaplarının güvenilir bilgi kaynağı olarak konumlanmasını güçlendirecek ve hesapların etkililiğini artıracaktır.



Yerel Gündemin Takibi:

Görev yapılan il veya ilçedeki özel günler, gelenekler, güncel gelişmeler, yatırımlar ve hizmetler düzenli takip edilmeli ve kamuoyu ile paylaşılmalıdır. Cenaze, düğün, sportif ve kültürel etkinlikler gibi toplumsal temas noktalarına katılım sağlanmalı ve bu tür faaliyetler uygun bir dille görünür kılınmalıdır. Bu yaklaşım, devlet ile vatandaş arasındaki etkileşimi güçlendirerek kurumsal görünürlüğü ve toplumsal bağları pekiştirmektedir.

Kurumsal Kimliğe Uygunluk:

Sosyal medya paylaşımlarında, icra edilen görev ve ünvanın gereği olarak kurumu temsil bilinciyle hareket edilmelidir. İçerikler, doğrudan görev ve sorumluluk alanınıza giren konularla sınırlı tutulmalı; kurumun ve temsil edilen makamın itibarını zedeleyebilecek nitelikteki paylaşımlardan kesinlikle kaçınılmalıdır. Kurumsal kimliği olumsuz etkileyebilecek her türlü ifade, görsel ve etkileşim dikkatle değerlendirilmelidir.

Söylem Birliğinin Sağlanması:

Kurumsal iletişimde söylem birliği hem devlet politikalarıyla uyum hem de kurum içi iletişim tutarlılığı açısından temel bir ilkedir. Paylaşımlar, yürürlükteki kamu politikaları ile uyumlu olmalı; mevcut uygulamalara veya gündemdeki tartışmalı konulara ilişkin kişisel değerlendirmeler, kişisel hesaplar dâhil olmak üzere kamuya açık şekilde paylaşılmamalıdır. Kişisel görüşlerin paylaşılması durumunda, bunun tamamen bireysel bir değerlendirme olduğu açıkça belirtilmelidir. Kurumun tüm dijital mecralarında yer alan içeriklerin birbiriyle tutarlı, uyumlu ve bütüncül bir iletişim dili taşımasına özen gösterilmelidir.

Sorumluluk İlkesi:

Sosyal medya hesapları üzerinden gerçekleştirilen tüm paylaşımlar, beğeniler ve etkileşimler doğrudan hesap sahibinin sorumluluğundadır. “Yanlışlıkla yapılmış” veya “sehven gerçekleşmiş” olduğu belirtilen işlemler dahi bu sorumluluğu ortadan kaldırmaz. Bu nedenle tüm dijital etkileşimlerde azami dikkat gösterilmeli; hesap güvenliği için gerekli teknik ve idari tedbirler düzenli olarak alınmalıdır.

Şekil Şartlarının Sağlanması:

Görsel ve işitsel içeriklerin doğru, tutarlı ve platforma uygun şekilde hazırlanması, mesajın etkisini doğrudan artırmaktadır. Kurumsal kimliğe uygun görsel standartlar korunmalı; içerikler sosyal medya platformlarının teknik gerekliliklerine göre optimize edilmelidir. Örneğin Instagram için görsel ağırlıklı içerikler, X platformu için ise kısa ve etkili video veya metin içerikleri tercih edilmelidir. Profil ve görsel boyutlarının ilgili platform standartlarına uygun olması sağlanmalıdır.

Hesap Güvenliğinin Sağlanması:

Sosyal medya hesaplarının güvenlik ayarları düzenli olarak kontrol edilmeli ve güncel tutulmalıdır. Kurum veya idareci adına açılmış sahte hesaplar periyodik olarak takip edilerek tespit edilmelidir. Ayrıca görev alanına giren konularda ortaya çıkabilecek yanlış bilgi ve dezenformasyon içerikleri izlenmeli ve gerekli durumlarda hızlı müdahale edilmelidir. Hesap yönetiminden sorumlu kullanıcı veya personelin değişmesi durumunda, hesap güvenliğinin sağlanması amacıyla şifreler derhâl yenilenmeli ve erişim yetkileri güncellenmelidir.

Hesap Yönetiminin Profesyonelleştirilmesi:

Kurumsal sosyal medya hesaplarının yönetimi, alanında yetkin bir iletişim ekibi tarafından yürütülmelidir. Bu ekibin bilgi ve becerilerini güncel tutmak amacıyla düzenli ve sistematik eğitim faaliyetleri planlanmalı ve uygulanmalıdır. Kurumsal iletişim süreçleri profesyonel standartlara uygun yapılandırılmalıdır.

Kurumsal İletişimin Etkililiğinin Analiz Edilmesi:

Sosyal medya faaliyetlerinin etkinliği düzenli ölçülmeli ve analiz edilmelidir. Hangi tür içeriklerin daha yüksek etkileşim aldığı, hangi zaman dilimlerinde görünürlüğün arttığı gibi veriler dikkate alınarak içerik stratejisi geliştirilmelidir. Bu analizler doğrultusunda kurumsal iletişim süreçleri sürekli iyileştirilmelidir. Medya takip hizmeti alınması, bu türden bir analizin yapılmasında kolaylık sağlayacaktır.

İçerik Yönetiminde Yapay Zekâ Kullanımı

Yapay zekâ teknolojileri, kamu kurumlarının iletişim ve içerik yönetimi süreçlerinde etkinliği ve verimliliği artırabilecek önemli araçlar arasında yer almaktadır. İçerik taslağı oluşturma, metin düzenleme, dil ve üslup iyileştirme, rapor ve doküman özetleme, veri analizi, sosyal medya eğilimlerini takip etme, vatandaş geri bildirimlerini sınıflandırma, görsel ve video üretimine destek sağlama gibi pek çok alanda kurumsal çalışmalara katkı sunabilir. Ancak yapay zekâ araçları, karar verici değil; karar süreçlerini destekleyen yardımcı sistemler olarak değerlendirilmelidir.

Yapay zekâ tarafından üretilen hertürlü metin, görsel, ses ve video içeriği; doğruluk, güncellik, tarafsızlık, kurumsal dil, etik ilkeler ve yürürlükteki mevzuat bakımından ilgili birim tarafından kontrol edilmeden yayımlanmamalıdır. Yapay zekâ uygulamalarının zaman zaman gerçeği yansıtmayan bilgiler üretebileceği, eksik veya yanıltıcı sonuçlar oluşturabileceği göz önünde bulundurulmalı; özellikle kamuoyunu ilgilendiren açıklamalar, istatistikler ve hukuki değerlendirmeler güvenilir ve resmî kaynaklar esas alınarak doğrulanmalıdır.

Yapay zekâ uygulamalarına girilen veriler açısından bilgi güvenliği ve gizlilik ilkeleri gözetilmelidir. Kişisel veriler, gizlilik dereceli bilgi ve belgeler, kurum içi yazışmalar, stratejik planlar ve kamuya açıklanmamış bilgiler, gerekli teknik ve idari tedbirler alınmadan yapay zekâ sistemlerine aktarılmamalıdır. Özellikle çevrim içi veya bulut tabanlı yapay zekâ uygulamalarında veri işleme süreçleri dikkatle değerlendirilmeli; 6698 sayılı Kişisel Verilerin Korunması Kanunu ile ilgili diğer mevzuat hükümlerine uygun hareket edilmelidir.

Yapay zekâ tarafından oluşturulan içeriklerde ayrımcı ifadeler, önyargılar, telif hakkı ihlalleri veya dezenformasyona yol açabilecek unsurlar bulunabileceği dikkate alınmalıdır. Bu nedenle içerikler yalnızca dil ve anlatım açısından değil; kamu yararı, toplumsal hassasiyetler, insan hakları, etik ilkeler ve kurumsal itibar bakımından da değerlendirilmelidir. Kamu kurumlarının güvenilirliğini zedeleyebilecek, yanlış yönlendirmeye neden olabilecek veya toplumda bilgi kirliliği oluşturabilecek içeriklerin kullanılmamasına özen gösterilmelidir.

Yapay zekâ ile oluşturulan görsel, ses ve video içeriklerinin gerçek kişileri veya olayları yanıltıcı şekilde yansıtmalarına izin verilmemelidir. Deepfake ve benzeri sentetik medya uygulamalarının kamuoyunda yanlış algı oluşturabilecek şekilde kullanılması uygun değildir. Eğitim, farkındalık veya teknik gösterim amacıyla bu tür içeriklerden yararlanılması hâlinde, içeriğin yapay zekâ ile üretildiği açık ve anlaşılır şekilde belirtilmelidir.

Kurumlar, yapay zekâ kullanımına ilişkin açık kurumsal politika ve prosedürler oluşturmali; hangi uygulamaların kullanılabileceği, hangi verilerin paylaşılabilirliği ve içeriklerin hangi onay süreçlerinden geçeceği belirlenmelidir. Yapay zekâ destekli içerik üretiminde insan

denetimi temel ilke olmalı; yayımlanan her içerikten nihai olarak ilgili kurum ve yetkili personel sorumlu tutulmalıdır.

Uygulama Esasları:

- Yapay zekâ araçları, içerik üretiminde destekleyici araç olarak kullanılmalı; nihai değerlendirme ve onay yetkili personel tarafından verilmelidir.
- Yapay zekâ tarafından üretilen içerikler yayımlanmadan önce doğruluk, tarafsızlık, güncellik ve hukuki uygunluk açısından kontrol edilmelidir.
- Resmî açıklamalar, kriz iletişimi mesajları ve kamuoyunu doğrudan ilgilendiren duyurular yalnızca yapay zekâ çıktısına dayanılarak hazırlanmamalıdır.
- Gizlilik dereceli bilgi ve belgeler ile kişisel veriler yapay zekâ sistemlerine aktarılmamalıdır.
- Kullanılan yapay zekâ araçlarının bilgi güvenliği, veri işleme politikaları ve hukuki uygunluğu değerlendirilmelidir.
- Yapay zekâ tarafından üretilen görsel, ses ve videoların yanıltıcı veya manipülatif amaçlarla kullanılmasına izin verilmemelidir.
- Telif hakları, fikrî mülkiyet hakları ve kişilik haklarına uygun hareket edilmelidir.
- Yapay zekâ kullanımına ilişkin düzenli eğitimler planlanmalı, personelin yapay zekâ okuryazarlığı geliştirilmelidir.
- Kurumlarda yapay zekâ kullanımına yönelik iç denetim ve risk yönetimi mekanizmaları oluşturulmalıdır.
- Yapay zekâ uygulamalarının kullanımında şeffaflık, hesap verebilirlik, insan odaklılık ve kamu yararı ilkeleri esas alınmalıdır.



SAYFA YÖNETİMİ KONUSUNDA DİKKAT EDİLMESİ GEREKENLER

Profil Görselinin Seçilmesi:

Kurumsal sosyal medya hesaplarında kullanılan profil ve kapak görselleri, kurumun dijital kimliğini yansıtan en temel görsel unsurlar arasında yer almaktadır. Bu nedenle söz konusu görsellerin hem teknik hem de tasarımsal açıdan belirlenmiş standartlara uygun şekilde hazırlanması gerekmektedir. Profil görselleri yüksek çözünürlüklü, sade ve ölçeklenebilir bir yapıda olmalı; farklı boyutlarda kullanıldığında da netliğini koruyabilmelidir. Bu kapsamda, kurumsal logo gibi tanımlayıcı ve yüksek kaliteli görsellerin kullanılması tercih edilmelidir.

Görsel tasarımda karmaşık detaylardan, okunabilirliği zorlaştıran yazı tiplerinden ve yoğun arka plan kullanımından kaçınılmalıdır. Profil görsellerinin kare formatta hazırlanması ve sosyal medya platformlarının dairesel kırpma alanlarına uygun şekilde tasarlanması, görsel bütünlüğün korunması açısından önem arz etmektedir. Ayrıca tüm sosyal medya platformlarında tutarlı bir görsel dil ve tasarım standardı kullanılması, kurumsal algının güçlendirilmesine ve marka bütünlüğünün sağlanmasına katkı sunacaktır.

Kapak Görselinin Seçilmesi:

Kapak görselleri, kurumun hizmet alanını, yaklaşımını ve iletişim dilini destekleyen geniş ve bütüncül kompozisyonlar içermelidir. Tasarımda verilmek istenen mesaj açık, anlaşılır ve dikkat çekici biçimde konumlandırılmalıdır. Görsellerin yüksek çözünürlükte hazırlanması, kalite kaybına yol açmayan uygun dosya formatlarının tercih edilmesi ve platformlara özgü ölçü standartlarının dikkate



alınması gerekmektedir. Ayrıca içeriklerin hem mobil hem de masaüstü cihazlarda doğru ve tutarlı şekilde görüntülediği test edilmelidir. Renk kullanımında kurumsal kimlik standartlarına bağlı kalınmalı; tüm sosyal medya platformlarında bütüncül ve tutarlı bir tasarım dili benimsenmelidir.

Profil Bilgileri:

Kurumsal sosyal medya profillerinde kurumun adresi, konum bilgisi, santral telefon numarası, resmî internet sitesi ve vatandaşlara açık iletişim e-posta adresi gibi bilgilere yer verilebilmektedir. Buna karşılık kişisel hesaplarda taraftarı olunan spor kulübü, memleket bilgisi, üye olunan dernekler veya benzeri kişisel tercih ve aidiyetleri yansıtan bilgilerin paylaşılmaması gerekmektedir.



Takip Edilen Hesapların Seçimi:

Kurumsal sosyal medya hesapları aracılığıyla il valisi, il emniyet müdürü, il jandarma komutanı ve müftülük gibi önemli kamu kurum ve makamlarının hesapları takip edilmelidir. Takip edilen hesaplar arasında yakın il ve ilçe makamlarının da bulunmasına özen gösterilmelidir. Vatandaşın bilgilendirilmesinin gerekli olduğu durumlarda bu resmî hesaplardan yapılan paylaşımlara atıf yapılabilir. Bununla birlikte nefret söylemi, şiddet içeren ifadeler, ayrımcılık, toplumsal kutuplaştırma ve ırkçı içerik barındıran kişi veya grupların hiçbir şekilde takip edilmemesi, bu tür hesaplarla etkileşime girilmemesi ve arkadaşlık ilişkisi kurulmasından kesinlikle kaçınılması gerekmektedir.

Yeniden Paylaşım ve Beğeni Politikası:

Toplumsal değerleri zedeleyen, tarafsızlık ve kurumsal bağımsızlık algısını olumsuz etkileyebilecek içeriklerin; sanat, edebiyat veya bilimsel nitelik taşısa dahi paylaşılmaması veya beğenilmemesi gerekmektedir. Resmî kurum ve kuruluşlar tarafından üretilmeyen içeriklerin yeniden

paylaşımında azami dikkat gösterilmeli; içeriklerin kurumsal duruşla uyumluluğu mutlaka değerlendirilmelidir.

Paylaşım Sayısı ve Sıklığı:

Kurumsal sosyal medya hesaplarında düzenli, planlı ve zengin içerik üretimi sağlanmalıdır. Platformlara göre önerilen paylaşım sıklıkları; Facebook'ta günlük 2-3, X platformunda yaklaşık 10, Instagram'da 1-2 ve LinkedIn'de 1-2 paylaşım şeklindedir. Paylaşımlar aynı zaman dilimine yığılmadan, gün içine yayılarak planlanmalıdır. Ayrıca Instagram hikâye özelliği ve WhatsApp durum paylaşımları da kurumsal iletişim aracı olarak etkin kullanılabilir.

Zaman Yönetimi:

Doğru içeriklerin doğru zamanda paylaşılması, etkileşim oranlarını artırmada kritik bir rol oynamaktadır. Paylaşım zamanlaması, platforma ve hedef kitlenin aktif olduğu saatlere göre planlanmalıdır. Platformların kendi analiz araçları (örneğin Instagram Insights ve Facebook Analytics) kullanılarak takipçilerin çevrim içi olduğu zaman dilimleri belirlenmeli ve içerikler bu doğrultuda yayımlanmalıdır. Genel eğilimlere göre Facebook için sabah 06.00-08.00 ve akşam 17.00-19.00 saatleri, X platformu için 17.00-19.00 ve 20.00-23.30 arası, Instagram için ise sabah işe gidiş ve akşam saatleri daha yüksek etkileşim sağlayabilmektedir. Bununla birlikte en düşük etkileşim genellikle gece geç saatlerde (22.00-04.00) görülmektedir.

İçerik Paylaşımının Takvimlendirilmesi:

Gün /Tarih	Platform	Saat	İçerik Türü	Konu
Pazar	Facebook	09.00	Video	Anneler Günü Kutlaması
Salı	Instagram	09.30	Post	Sosyal Yardım Başvuru Duyurusu

Aylık veya haftalık içerik takvimi hazırlanması, içerik üretiminde sürekliliğin sağlanmasına ve rastlantısallığın önlenmesine katkı sunmaktadır. Bu yaklaşım; benzer içeriklerin tekrarını engellemekte,

içerik çeşitliliğini sistematik hâle getirmekte ve genel iletişim stratejisinin bütüncül yönetilmesini sağlamaktadır. Haftanın belirli günlerine tematik içeriklerin planlanması, özel gün ve önemli tarihler için önceden hazırlık yapılması ve mesaj tutarlılığının korunması açısından içerik takvimi kritik bir araçtır. Bu sayede önemli gün ve olayların gözden kaçırılmasının da önüne geçilmektedir.

İçeriğin Çeşitlendirilmesi:

Kurumsal sosyal medya hesaplarında yalnızca toplantı, açılış veya ziyaret içeriklerine yer verilmemelidir. Bunun yerine ilin veya ilçenin turizm potansiyeli, tarımsal faaliyetleri, sanayi yapısı, kültürel değerleri ve gastronomik zenginlikleri gibi alanlara yönelik tanıtıcı içerikler üretilmelidir. Ayrıca sosyal medya okuryazarlığı, kamu hizmetlerine erişim yolları, yasal düzenlemeler ve resmî duyurular gibi bilgilendirici içeriklere de ağırlık verilmesi kamu yararını güçlendirecektir. İçeriklerin görsel ve işitsel açıdan çeşitlendirilmesi, gerektiğinde yapay zekâ destekli görsel üretim araçlarından yararlanılması ve canlı yayın uygulamalarının etkin kullanımı, içeriklerin daha dikkat çekici ve etkileşimli olmasını sağlayacaktır.



Etiket ve Emoji Kullanımı:

Sosyal medya paylaşımlarında yeterli ve dengeli düzeyde açıklayıcı metin kullanılması esastır. Etiket kullanımı etkileşimi artıran bir unsur olmakla birlikte, yalnızca emoji veya etiketlerden oluşan içeriklerin paylaşılmasından kaçınılmalıdır. Sosyal medyada güvenilirlik ve gerçeklik algısının korunması temel önceliktir. Bu nedenle yapay zekâ ile üretilen içeriklerin, uygun durumlarda açık şekilde belirtilmesi şeffaflık ve güvenilirliği artıracaktır.

Bazı Paylaşımların Önceliklendirilmesi:

Vatandaşları doğrudan ilgilendiren yasal düzenlemeler, başvuru süreçleri ve kamu hizmetlerine ilişkin bilgilendirmeler öncelikli olarak görünür ve erişilebilir şekilde paylaşılmalıdır. Ayrıca Instagram’da “Öne Çıkanlar” bölümü aktif kullanılarak hizmet türleri, ilçeler veya konu başlıklarına göre içeriklerin kategorize edilmesi, bilgiye erişimi kolaylaştıracaktır. Instagram’da belirli içeriklerin kurumsal profilinizde öncelikli ve görünür bir konumda tutmalarını sağlayan Pin (Sabitleme) özelliği kullanılarak özel günler, ilin/ilçenin özellikleri, önemli duyurular, bilinçlendirme faaliyetleri gibi önemli hususlar takipçilerin dikkatine sunulmalıdır.



Karşılıklı İletişimin Artırılması:

Sosyal medya üzerinden kurumlara iletilen mesajların dikkate alındığı ve gerekli işlemlerin başlatıldığına dair bilgilendirmelerin paylaşılması, vatandaşların kurumsal muhataplık algısını güçlendirmektedir. Olumsuz yorumlar veya yanlış ihbarlar zaman zaman kaçınılmaz olabilir; bu tür durumlarda küfür, hakaret veya argo içeren yorumların kaldırılması kurumsal itibarın korunması açısından gereklidir. Bunun dışında kalan yorumlara ise silme yerine kurumsal ciddiyet ve nezaket çerçevesinde yanıt verilmesi; şeffaflık, erişilebilirlik ve güvenilirlik ilkelerini güçlendirecektir.

Üçüncü Kişilere Saygı:

Özel hayatın gizliliği ve kişisel verilerin korunması ilkeleri doğrultusunda, üçüncü kişilere ait görsel, bilgi veya içeriklerin açık rıza alınmaksızın paylaşılması gerekmektedir. Aynı şekilde, kişilerin izni olmadan etiketlenmesi veya kimliklerini ifşa edecek paylaşımlarda bulunulması uygun değildir. Bu ilkeye riayet edilmesi hem hukuki hem de etik sorumluluk açısından zorunluluk teşkil etmektedir.

KAÇINILMASI GEREKEN İÇERİK TÜRLERİ

- Irkçı, nefret dolu, cinsiyetçi, iftira niteliğinde, hakaret içeren veya hayatı tehdit eden,
- Kişilere veya kuruluşlara yönelik ciddi, kanıtlanmamış veya yanlış iddialar içeren,
- Saldırgan, kaba, şiddet ve müstehcenlik içeren,
- Yasadışı faaliyeti teşvik eden veya ima eden,
- Herhangi bir finansal, ticari kuruluşa ilişkin tanıtım, reklam veya onay niteliğindeki faaliyetleri gösteren,
- Anonim ya da bot hesaplar tarafından paylaşılan,
- Anlaşılmaz veya gündem dışı içeriklerden kaçınılması gerekmektedir.



KRİZ İLETİŞİM YÖNETİMİ

KRİZ İLETİŞİM YÖNETİMİ

Krizler bireylerin, toplumların veya kurumların yaşamında normal işleyişi bozan, aniden ortaya çıkan ve acil çözüm ile müdahale gerektiren tehlikeli, bunalımlı dönemlerdir. Krizler:

- **Beklenmediktir:** Ani ve genellikle haber vermeden meydana gelmektedir.
- **Yönetimi Krittir:** Hızlı karar verilmesini ve anında müdahaleyi gerektirmektedir.
- **Tehdit Unsurları İçerir:** Kurumlar için finansal, itibar kaybı; bireyler için ise psikolojik veya yaşamsal riskler oluşturmaktadır.
- **Belirsizlik Barındırır:** Olay anında bilgi akışı sınırlıdır, stres ve kaygı seviyesi yüksektir.

Kriz, yalnızca olayın kendisi değildir; **olayın nasıl algılandığıyla da şekillenmektedir.** Bu nedenle kriz anlarında **hızlı, şeffaf ve tutarlı iletişim büyük önem taşımaktadır. Yanlış bilgi, eksik açıklama veya geç yapılan müdahale, krizin etkisini daha da büyütebilmektedir.** Etkili kriz iletişimi ise belirsizliği azaltmakta kurumun itibarını korumakta ve toplumda güven duygusunun yeniden inşa edilmesini sağlamaktadır.

Krizin boyutu ne kadar büyük olursa olsun sakinliği korumak ve kontrollü davranmak oldukça önemlidir. Yaşanan olay, sizin kararlarınızın ve kontrolünüzün önüne geçmemelidir.

“Kriz anında panik yapmadan durumu kontrol altında tutmak, hatalı kararların önüne geçer.”

Kriz iletişim yönetimi üç aşamadan oluşmaktadır: Kriz Öncesi, Kriz Anı ve Kriz Sonrası.

KRİZ ÖNCESİ

Kriz iletişiminde en kritik aşama **kriz öncesi hazırlıktır.**

- Kurumlar önceden kriz iletişim planı oluşturmalı,

- Kriz iletişim yönetimi ekibini kurmalı,
- Görev dağılımını belirlemeli,
- Açıklamaları yapacak sözcü önceden seçilmeli,
- Kriz senaryolarına yönelik eğitimler verilmeli,
- Toplumsal yapı analizi, kriz sinyallerinin analizi ve kurumun yeterlilik-kapasite değerlendirmesi yapılmalıdır.

“Kriz anında görev dağılımının net olmaması zaman kaybına ve krizin büyümesine neden olabilmektedir. “

KRİZ ANI

Kriz tipinin belirlenmesi ile elde edilecek olan bilgi, kriz iletişimde hata yapılmasını önleyebilecektir. Küçük çaplı krizlerin yanlış yönetilmesi ya da büyük krizlerin ciddiye alınmadan iletişim yönetimi yapılması, kriz zamanlarında büyük hataların oluşmasına sebebiyet verebilmektedir. Bu nedenle kriz anlarında öncelikle olayın niteliği, kapsamı, etki alanı, paydaşları ve kamuoyundaki yansımaları doğru şekilde analiz edilmelidir.

Kriz Anında Temel İlkeler:

- Krizin türü, kapsamı ve etkileri doğru analiz edilmeden iletişim sürecine başlanmamalıdır.
- Kriz anında tek seslilik ve kurum içi koordinasyon sağlanmalıdır.
- Açıklamalar yalnızca doğrulanmış bilgiler temelinde hazırlanmalıdır.
- Kamuoyunun bilgi ihtiyacı zamanında ve düzenli biçimde karşılanmalıdır.
- Sosyal medya platformları aktif olarak izlenmeli, dezenformasyona karşı hızlı ve doğru bilgilendirme yapılmalıdır.
- Kriz dönemlerinde kullanılan dil sakin, güven veren ve çözüm odaklı olmalıdır.
- Kişisel görüşler ile kurumsal açıklamalar birbirinden ayrılmalıdır.
- Krizle ilgili hassas bilgi, belge ve görseller paylaşılmadan önce gizlilik ve güvenlik açısından değerlendirilmelidir.

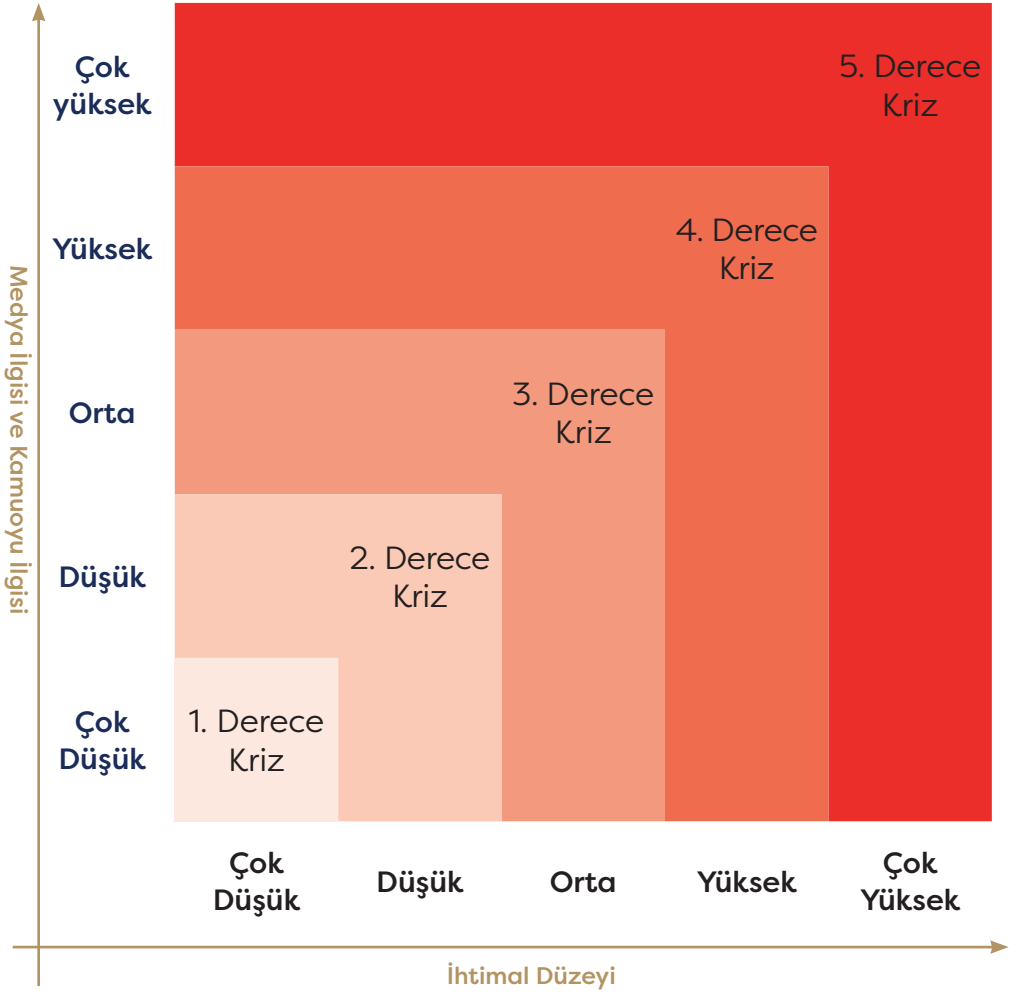
KRİZİ ANLAMLANDIRMA TABLOSU

Gerçekleşti mi?	KRİZ ANLAMLANDIRMA KRİTERLERİ
	Ortaya çıkan kriz kamuoyunun güvenliği açısından acil durum özelliği taşıyor ve hızla kamuoyuyla iletişim kurup, krizin daha fazla zarar vermesini önlemek gerekiyor.
	Kısa bir süre içinde can kaybı olması bekleniyor.
	Medya ve kamu olayı şimdiye kadar yaşanan “en kötü”, “ilk” veya “en büyük” olay olarak algılıyor.
	Tahmin edilenin üstünde bir zarar var.
	Olayı nüfus yoğunluğu büyük olan bir bölgede gerçekleşti ve durumdan etkilenen kişi sayısı yüksek.
	Olay aniden gerçekleşti ve ulusal bir etkiye sahip.
	Hükûmet, olayda sebep ya da sorumlu olarak algılanmaktadır.
	Olayın ağırlıklı olarak etkilediği sosyal bir grup var.
	Olay provokasyon içeriyor, kritik kitlelerin dâhil olma riski var.
	Olayın kontrol altına alınması toplumun bir kesiminin sivil hak ve özgürlüklerine müdahale edilmesini gerektiriyor.
	Olaydan direkt etkilenen kişilerin can güvenliğini sağlamak için acil adımlar atılması gerekiyor.
	Olayın zararını hafifletmek için kurum imkânları yeterli değil.
	Olayların bazı "sıra dışı" yönleri var.
	Olaydan direkt zarar gören bir devlet kurumu var.



KRİZİ ANLAMLANDIRMA TABLOSU

Gerçekleşti mi?	KRİZ ANLAMLANDIRMA KRİTERLERİ
	Olay bir takım hassas dengeleri etkiliyor.(Uluslararası ilişkiler ve politika gibi.)
	Olaydan direkt zarar gören ünlü/önemli bir kişi var.
	Olaya ilişkin devam eden bir soruşturma var.
	Olayın güvenliği ne ölçüde etkilediği kamuoyu tarafından henüz tam anlaşılmamış ya da kamuoyu durumla ilgili tam olarak bilgilendirilmiyor.
	Olay "akut"tur. Olay sırasında ve sonrasında kurum açıklamalarla karşı karşıya kalmaktadır.
	Olay mağdurlarını uzun vadede nelerin beklediği belirsizdir.
	Olay gelişmektedir. Sonucunun bundan daha iyi mi yoksa daha kötü mü olacağı belirsizdir.
	Olayın meydana geldiği bölge imkânları, olaya müdahale etme konusunda (teknik donanım açısından) yetersizdir ve kamuoyu olay konusunda doğru bilgilendirilmemektedir.
	Kriz uluslararası (başka bir ülkede) boyutta oluştu, fakat uzun vadede etkilerinin hissedilmesi söz konusu.
	Olay kişilerin kontrolüyle çözülebilir.



1. Derece Kriz:

Kamuoyu ve/veya medyanın krize ilişkin etkisinin en düşük seviyede olduğu durumdur. Kriz, çok küçük bir alanda ve çok düşük derecede medya ilgisine sahiptir.

2. Derece Kriz:

Kamuoyu ve/veya medyanın krize ilişkin etkisinin düşük seviyede olduğu durumdur. Kriz, yerel ölçeği aşmayacak şekilde kamuoyu etkisine ve medya ilgisine sahiptir.

3. Derece Kriz:

Kamuoyu ve/veya medyanın krize ilişkin etkisinin orta seviyede olduğu durumdur. Kriz, yerel ve il sınırları içerisinde kamuoyu etkisine sahiptir. Yerel medya ile kısmen ulusal medya ilgi göstermektedir.

4. Derece Kriz:

Kamuoyu ve/veya medyanın krize ilişkin etkisinin yüksek seviyede olduğu durumdur. Kriz yerel, il ve çevre illeri de kapsayacak şekilde bölgesel kamuoyunu etkilemektedir. Ulusal ve kısmen uluslararası medya ilgi göstermektedir.

5. Derece Kriz:

Kamuoyu ve/veya medyanın krize ilişkin etkisinin çok yüksek seviyede olduğu durumdur. Kriz ulusal ve uluslararası kamuoyunu etkileyecek düzeydedir. Ulusal ve uluslararası medyanın yüksek seviyede ilgisi bulunmaktadır.

1. derece krizlerde ilçe yöneticilerinin (kaymakam, ilçe jandarma komutanı, ilçe emniyet amiri) açıklama ve bilgilendirme yapması yeterli olabilmektedir. 1. derece kriz tipinde kriz iletişim yönetim ekibinin ilgili birimlerin devreye girmesini ve iletişim stratejilerine paralel olarak açıklama yapmasını temin etmelidir.

2. derece, 3. derece ve 4. derece krizlerde ilçe yöneticilerine ilave olarak il yöneticilerinin (vali, vali yardımcısı, valilik basın ve halkla ilişkiler müdürlüğü, il jandarma komutanı, il emniyet müdürü) açıklama ve bilgilendirme yapması gerekli ve zorunlu olabilmektedir. 2., 3. ve 4. derece kriz tipinde kriz iletişim yönetim ekibinin gecikmeksizin kriz iletişim basın sözcüsünün ve/veya ilgili birimlerin devreye girmesi ve iletişim stratejilerine paralel olarak açıklama yapmasını temin etmelidir.

5. derece krizlerde yani ulusal ve uluslararası kamuoyunu etkileyen krizlerde il yöneticilerine ilave olarak merkezî yönetim birimlerinin devreye girmesi gerekmektedir. Krizin kamuoyunda oluşturacağı/ oluşturduğu etkisi ve medya ilgisinin şiddeti ve derecelendirilmesi işi, kriz iletişim yönetimi ekibi tarafından, açık ve kapalı kaynaklardan elde edilen veriler doğrultusunda belirlenmektedir.



Sosyal medyada kriz yönetimi; hızlı reaksiyon, şeffaflık, empati ve doğru kriz planı gerektirmektedir. Kriz anında sessiz kalmak veya agresif tepkiler vermek yerine çözüm odaklı adımlar atmak en kritik eşiktir.

Kamu kurumları olayın ne olduğu, nerede ve ne zaman gerçekleştiği, nasıl müdahale edildiği ve devletin mağdurların yanında olduğu konusunda **açık bilgi verilmelidir**. Yapılacak açıklamada 5N1K kuralına özen gösterilmelidir.

Kriz dönemlerinde **geleneksel medya ve sosyal medya birlikte yönetilmelidir**. Kurumların resmî sosyal medya hesapları aktif olmalı, yanlış bilgiler hızla düzeltilmeli ve kamuoyu resmî kaynaklara yönlendirilmelidir.

Sosyal medyanın hız faktörü nedeniyle kriz iletişiminde kritik rol oynadığı göz önüne alınarak **kurumlar arasında tek seslilik sağlanmalı, çelişkili açıklamalardan kaçınılmalıdır**.

Sözcü, kurumu temsil ettiğini unutmadan **empatik, güven verici ve açıklayıcı** bir dil kullanılmalıdır.

İÇERİK GELİŞTİRME MODELİ

Yöntem	İçerik
1. Olayı eksiksiz anlatın	• 5N1K ilkesine uygun olarak hazırlayın. Şu sorulara cevap verin: › Ne? (Olay nedir?) › Nasıl? (Olay nasıl gerçekleşti?) › Neden? (Olay neden/niçin yapıldı?) › Nerede? (Olay nerede yaşandı?) › Ne zaman? (Olay ne zaman meydana geldi?) › Kim? (Olayı kim yaptı veya kim etkilendi?)
2. İçeriğinize empati, güven ve şefkat ifadeleri katın.	• Krizin mağdurları, mağdur yakınları ve kamuoyunun genelinin duygu durumunu anladığınızı ve paylaştığınızı ifade edin.
3. Ana mesajı içeren cümleler kullanın	• Kelimeleri sınırlandırın • Olumlu kelimeler kullanın • Tanımlardan ve teknik ifadelerden kaçın • Kalıplaşmış ifadeler kullanmayın
4. Destekleyici ifadeler kullanın	• Somut verilerden yararlanın • Benzetme kullanın • Güvenilir bir üçüncü kişiyi referans gösterin
5. Atılacak sonraki adımlardan bahsedin	• Sonraki adımlar hakkında mümkünse zaman, yöntem ve beklenen sonuç odaklı bilgi verin

Hızlı ve Şeffaf Olun: Kriz başladıktan sonraki ilk birkaç saat çok önemlidir. Olayı saklamak yerine şeffaf bir açıklama yapın.

Empati Kurun: Hedef kitleyi ve mağdurları anladığınızı gösterin; savunmaya geçmekten veya bahaneler üretmekten kaçınin.

Kalıplardan Kurtulun: Otomatik veya robotik cevaplar yerine samimi ve insani bir dil kullanın.

Yorumları Silmeyin: Hakaret içermeyen eleştirileri silmek veya yorumları kapatmak krizi daha da büyütür. Sorunu kamuoyunun gözü önünde çözerek güven tazeleyin.

Süreci Çevrim Dışı İlerletin: Detaylı inceleme gerektiren şikayetleri hızlıca DM (özel mesaj) veya destek kanallarına yönlendirin.

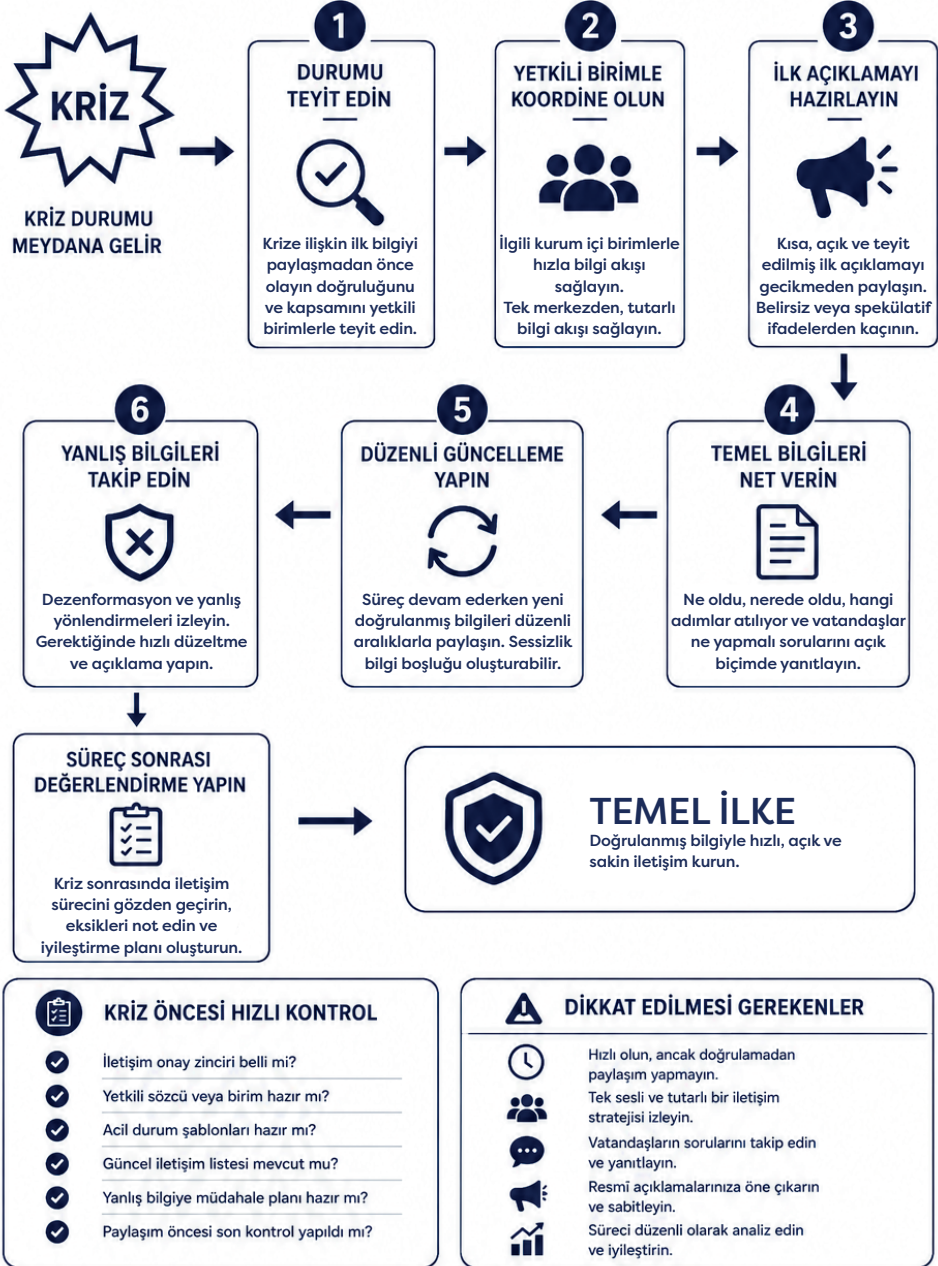
Kriz anında iletişim stratejisinin temel amacı bilgi boşluğunu gidermektedir. Bilgi eksikliği söylenti, dezenformasyon ve kamuoyunda güvensizlik oluşturmaktadır. Bu nedenle ilk açıklama gecikmeden yapılmalı, doğrulanmamış bilgiler paylaşılmamalı ve düzenli bilgi güncellemeleri sağlanmalıdır. Açıklamalar adli süreci etkilemeyecek şekilde hazırlanmalı, masumiyet karinesine zarar verilmemelidir.

KRİZ ANINDA YAPILACAKLAR

- Yurttaşın güvenliği her şeyden önce gelir.
- Sorun çözümleri için sorumluluğu üstlenin.
- Yaşanan krizle ilgili açık ve dürüst bir iletişim kurun.
- Haberleri ve gelişmeleri takip edin.
- Susmak stratejik bir tercih değilse asla “Cevapsız Bırakmayın”
- “Yorum Yok” bir cevap değildir.
- Bilmediğiniz bir konu hakkında yorum yapmayın.
- Bilmediğiniz bir konu varsa uzmanına sorun fakat asla “Cevapsız Bırakmayın”.
- Sürekli ve düzenli bilgi akışı sağlayın.

KRİZ ANINDA SOSYAL MEDYA YÖNETİM AKIŞI

Kurumsal sosyal medya yönetiminde kriz durumları için örnek iletişim süreci



İLK SAAT: GÜVENİN İNŞA EDİLDİĞİ KRİTİK ZAMAN DİLİMİ

Afet ve kriz durumlarında ilk saat, yalnızca olayın yönetilmeye başlandığı değil; kamuoyunun devlete duyduğu güvenin, kurumsal itibarın ve bilgi üstünlüğünün şekillendiği en kritik zaman dilimidir.

Bu süreçte ortaya çıkabilecek bilgi boşluğu; yanlış bilgi, dezenformasyon ve manipülatif içeriklerin hızla yayılmasına zemin hazırlayabilir. Bu nedenle dijital kriz iletişiminde temel ilke; hızlı olmak kadar doğruluk, güvenilirlik ve ölçülülük esaslarına riayet etmektir.

- İlk resmî açıklama, kurumun olaydan haberdar olmasının ardından mümkün olan en kısa sürede yapılmalı; ideal olarak ilk 60 dakika içerisinde kamuoyuyla paylaşılmalıdır.
- İlk açıklamada yalnızca doğrulanmış bilgiler kullanılmalı; teyit edilmemiş bilgi ve değerlendirmelerden kaçınılmalıdır.
- Bilgilerin henüz netleşmediği durumlarda, olayın yakından takip edildiği, ilgili kurumlarla koordinasyonun sürdüğü ve yeni gelişmeler oldukça kamuoyunun düzenli olarak bilgilendirileceği açık şekilde ifade edilmelidir.
- Sosyal medya hesapları, internet siteleri ve diğer resmî iletişim kanalları eş zamanlı ve koordineli kullanılmalıdır.
- Geleneksel medya, dijital medya ve sosyal medya platformları kesintisiz izlenmeli; kamuoyunun bilgi ihtiyacı, beklentileri ve dolaşıma giren yanlış bilgiler anlık olarak analiz edilmelidir.
- Dijital Kriz iletişimi; bireysel reflekslerle değil, önceden belirlenmiş görev dağılımına sahip profesyonel koordineli bir kriz iletişim ekibi tarafından yürütülmelidir.

Bilgi Boşluğu Oluşturulmamalıdır

Kriz anlarında kamuoyu hızlı bilgiye ihtiyaç duyar. Resmî açıklamaların gecikmesi, oluşan bilgi boşluğunun doğrulanmamış içerikler ve dezenformasyonla doldurulmasına neden olabilir. Bu nedenle yeni bilgi bulunmasa dahi belirli aralıklarla kamuoyuna süreç hakkında güncel bilgilendirme yapılmalı; devletin süreci yakından takip ettiği ve gerekli tedbirleri aldığı güçlü şekilde hissettirilmelidir.

Canlı Yayın ve Lider İletişimi

Toplumun yoğun bilgi ihtiyacı duyduğu büyük afet ve krizlerde, kurum yöneticileri veya yetkilendirilmiş sözcüler tarafından; yetkili devlet kurumu ile koordineli şekilde belirlenen iletişim stratejisi doğrultusunda sosyal medya platformları üzerinden gerçekleştirilecek canlı yayınlar; kamuoyunun doğru bilgiye doğrudan erişmesini sağlayan, söylenti ve dezenformasyonun etkisini azaltan önemli bir dijital kriz iletişimi aracıdır. Bu yayınlarda açık, tutarlı, sakin ve güven veren bir iletişim dili benimsenmelidir.

Dijital kriz iletişiminde ilk saat, zamanın değil; güvenin yönetildiği saattir. Bu süreçte kamuoyunun ilk başvurduğu güven kaynağı devlet olmalıdır.



DİJİTAL BİLGİ KİRLİLİĞİNE KARŞI DİJİTAL İLETİŞİM YÖNETİMİ

Dijital ekosistemde bilgi, doğru veya yanlış olduğuna bakılmaksızın hızlı yayılmaktadır. Özellikle afet, kriz ve olağanüstü dönemlerde oluşan bilgi boşluğu; yanlış bilgi, dezenformasyon, manipülatif ve koordineli spekülasyon içerikler, psikolojik harp ve olumsuz algı operasyonları için uygun bir zemin oluşturabilmektedir. Bu nedenle kamu kurumlarının önceliği, yanlış bilgiyi tekrar etmek değil; doğru, güvenilir ve doğrulanmış bilgiyi zamanında kamuoyuyla paylaşarak bilgi üstünlüğünü sağlamak olmalıdır.

Bilgi manipülasyonuna karşı yürütülecek iletişim faaliyetlerinde aşağıdaki hususlar dikkate alınmalıdır:

Dijital Bilgi Manipülasyonunu Analiz Edin

- Bilgi kirliliği veya manipülatif içeriğin kaynağı tespit edilmeye çalışılmalıdır.
- İçeriğin amacı, hedef kitlesi ve oluşturmayı hedeflediği algı analiz edilmelidir.
- Yayılım hızı, etki alanı ve dolaşım ağı değerlendirilmelidir.
- İçeriğin yerel, ulusal veya uluslararası ölçekte organize bir bilgi operasyonunun parçası olup olmadığı analiz edilmelidir.
- Dijital izleme araçları kullanılarak manipülatif içeriklerin yayılım eğilimleri takip edilmelidir.

Doğru Bilgiyi Önceliklendirin

- Kamuoyuyla yalnızca doğrulanmış bilgiler paylaşılmalıdır.
- Yanlış bilgiyi tekrar ederek görünürlüğünü artırabilecek açıklamalardan kaçınılmalıdır.

- Açıklamalar açık, net, anlaşılır ve tereddüde yer bırakmayacak şekilde hazırlanmalıdır.
- Resmî açıklamalar tüm dijital platformlarda eş zamanlı ve koordineli olarak yayımlanmalıdır.
- Bilginin kaynağı açıkça belirtilmeli ve resmî hesaplara yönlendirme yapılmalıdır.

Güven Veren İletişim Dili Kullanın

- Güven veren ve çözüm odaklı bir iletişim dili benimsenmelidir.
- Gerekğinde konuya ilişkin uzmanlar, akademisyenler veya yetkili kurum temsilcileri sürece dâhil edilerek kamuoyunun doğru bilgiye olan güveni güçlendirilmelidir.
- Bilgi boşluğu oluşmasına izin verilmemeli; yeni gelişme bulunmasa dahi düzenli bilgilendirme yapılmalıdır.

Manipülasyonu görünür kılın; hakikati görünür kılın. Kamuoyunun güvenini sağlayan, yanlış bilginin tekrar edilmesi değil; doğru bilginin zamanında, tutarlı ve güvenilir biçimde sunulmasıdır.

KRİZ SONRASI DİJİTAL İLETİŞİM YÖNETİMİ

Kriz sona erdiğinde iletişim süreci tamamlanmış sayılmaz. Kriz sonrası dönem, kurumsal öğrenmenin, itibarın güçlendirilmesinin ve gelecekteki krizlere hazırlığın en önemli aşamasıdır.

Bu kapsamda;

- Kriz süresince uygulanan dijital iletişim stratejisi bütün yönleriyle değerlendirilmelidir.
- Kamuoyu algısı, dijital etkileşimler ve medya yansımaları analiz edilmelidir.
- Dezenformasyon ve bilgi manipülasyonuyla mücadelede kullanılan yöntemlerin etkinliği ölçülmelidir.

- Elde edilen deneyimler kurumsal hafızaya aktarılmalı ve kriz iletişim planları güncellenmelidir.
- Eksiklikler giderilmeli, normalleşme süreci planlı şekilde yönetilmeli ve kurumsal itibarı güçlendirecek iletişim faaliyetleri sürdürülmelidir.
- Kriz sürecinde kurumun güvenilirliği, şeffaflığı, koordinasyon kapasitesi ve dijital temsil performansı kamuoyu geri bildirimleri doğrultusunda analiz edilmelidir.
- Hazırlanacak değerlendirme raporları, gelecekte benzer durumlara yönelik kurumsal kapasitenin geliştirilmesine katkı sağlamalıdır.

Kriz sona erdiğinde iletişim sona ermez. Güveni korumak, kurumsal itibarı güçlendirmek ve öğrenen bir kamu yönetimi anlayışı oluşturmak, kriz sonrası dijital iletişimin temel amacıdır.





Dünya Ekonomik Forumu'nun 2025 Yılı Küresel Risk Raporu'nda dezenformasyon en önemli küresel riskler arasında sayılmaktadır. Küresel risk sıralamasında birinci sırada devletler arası silahlı çatışmalar yer alırken, ikinci sıradaysa dezenformasyon gelmektedir. Rapor ayrıca küresel kamu güvenini, demokratik süreçleri ve kriz yönetimini tehdit eden dezenformasyonun en kritik kısa süreli risk olduğunu belirtmektedir. Dezenformasyonun etkilerinin giderek artacağı öngörülen raporda, 2027 yılında en önemli risk faktörü olacağı tahmin edilmiştir. Yapay zekanın gelişimiyle birlikte deepfake, manipüle edilmiş video ve görsellerin önümüzdeki yıllarda daha çok gündemimizde yer alması beklenmektedir.

Kamuoyunu yanlış yönlendirmek maksadıyla kasıtlı bir şekilde gerçeği gizleyerek ya da çarpıtarak veya tamamen gerçeğe aykırı olarak paylaşılan bilgiye dezenformasyon denir. Kasıt ve yanlış bilgi kavramları, dezenformasyonun belirleyici unsurlarıdır. Kavram İngilizce **“disinformation”** kelimesinden dilimize geçmiştir. İngilizcede

olumsuzluk ön eki olan “dis”, bilgi ve bilgi sağlama anlamına gelen enformasyonu kusurlu bir karaktere büründürmüştür. Yanlış ama kötü niyet olmadan paylaşılan bilgiye ise **misenformasyon** denir. Burada dikkat edilmesi gereken husus, kasıt olmamasıdır. Ancak bilgi her iki durumda da yanlış ya da gerçek dışıdır.

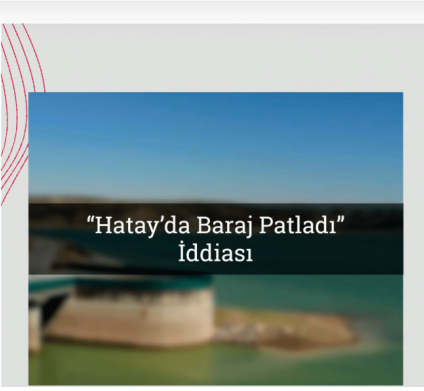
“



BaBaLa TV
@BabalaTv

Hatay Antakya Yarseli Barajı duvarı
çatlamış. Allah aşkına buraya ekip
yollansın
Çok yağmur yağıyor.

”



“Hatay’da Baraj Patladı” İddiası

3.03.2023

“Hatay’da baraj patladı” iddiası, afet bölgesindeki afetzedeleri paniğe sevk etmeye yönelik manipülasyondur. AFAD, Devlet Su İşleri İdaresi ve bölgede afette ilgili çalışma yürüten ekiplerden edinilen bilgilere göre, Hatay’da meydana gelen herhangi bir baraj patlaması söz konusu değildir.

GÜNCEL YALAN HABERLER

Bilgi ekosistemi ile ilgili değinilmesi gereken bir diğer kavram ise “malenformasyon”dur. Kısmen veya tamamen doğru olan bir bilginin sırf bir kişiye, kuruma veya devlete zarar vermek amacıyla sunulmasına malenformasyon denilmektedir. Bu bağlamda paylaşılan bilgi tamamen yanlış değildir ancak paylaşılrken kasten zarar verme motivasyonu bulunmaktadır. Malenformasyon kişilere ya da kurumlara olan güveni ve itibarı zedelemeye hedeflemektedir. Dezenformasyon yanlış bilgilerin yayılmasını, malenformasyon doğru bilginin kötü bir niyet ile farklı bir bağlamda yeniden sunulmasını ifade etmektedir. Önceki kavramlarda geçen “dis”, “mis” ön ekleri olumsuzluk, zıtlık ifade ederken; “mal” ön eki kavrama kötü, kötücül anlamı yüklemektedir. Bahsedilen bilgi kirliliği örnekleri, ortaya çıkışları itibarıyla farklılık gösterebilmektedirler. Ancak kamuoyundaki etkileri benzerdir ve dolayısıyla aynı hassasiyetle ele alınması gerekmektedir.

Farklı tanımlamaları olsa da yanlış, yanıltıcı ve hatalı bilgi örnekleri genel olarak dezenformasyon başlığının altında sayılabilir. Bilgi kirliliği örneklerinde genel olarak 7 yöntem kullanılmaktadır:

- Manipölasyon
- Manipülatif çerçeveleme
- Taklit
- Uydurma
- Yanlış atıf
- Bağlamından koparma
- Parodi (Hiciv)

Hızlı Bilgi ve Doğru Bilgi

Teoride doğru bilgi daha kıymetlidir ancak günümüz kitle dünyasında çoğu zaman hız, kamuoyu oluşturmada daha fazla avantaj sağlamaktadır. İnsanlar bir konu hakkında ilk karşılaştıkları bilgiyi doğru algılama eğilimindedirler. İlk yayılan bilgi gündemi belirlerken daha sonra gelen bilgiler doğru olsa dahi düzeltme gibi algılanabilmektedir. Yanlış bile olsa ilk bilgi hafızada kalıcı olmaktadır. Dolayısıyla “doğru” ve “hızlı” arasındaki denge çok daha önemli hâle gelmiştir.

Özellikle kriz zamanlarında insanlar bir bilgi kırıntısının peşinde sosyal medya taramalarıyla meşgulken azımsanamayacak sayıda bir topluluk ise kamu kurumlarından gelecek resmî bir açıklamayı beklemektedirler. Böyle zamanlarda algoritmalar ilk gelen ve daha sansasyonel olan bilgiyi seçerek çok sayıda insana ulaştırmaktadır. Bu noktada özellikle influencerların bilgiyi kamuoyuna yayma isteği, bilgiyi doğrulama gerekliliğinin önüne geçmektedir. Çoğunlukla siyasi ve ekonomik çıkar sağlama motivasyonu ile toplumsal algıyı yönlendirmeye çalışan influencerlar, kamu kurumlarına güveni olumsuz etkileyebilmektedir.

Reuters tarafından 2013- 2025 yılları arasında yapılan bir çalışmaya göre yeni medyayı haber kaynağı olarak kullananların oranı ABD’de yüzde 54, İngiltere’de yüzde 48, Türkiye’de ise yüzde 56’dır. Yeni medya, bilginin üretim ve dağıtım biçimini kökten değiştirmiştir. Geleneksel medyada haberleşme belirli kurumların kontrolündeyken

yeni medyada herkes hem bilginin üreticisi hem de tüketicisi hâline gelmiştir. Bu dönüşüm, bilgiye erişimi hızlandırmış ve kolaylaştırmıştır. Vatandaş gazeteciliği, tanık videoları ve canlı yayınlar bilginin hızla yayılmasını sağlamaktadır. Ancak bu hız ve kolaylık, doğru ve yanlış bilginin ayırt edilmesini oldukça zorlaştırmıştır.

Dezenformasyon süreci, yeni medyaya özgü bir durum değildir. İletişimin olduğu her ortamda ve zamanda mümkündür. Ancak yeni medyanın gelişimi ile dezenformasyonun üretilmesi ve sunulması çok daha kolay hale gelmiştir. Yeni medyada bilgi, profesyonel olmayan sıradan insanlar tarafından üretilebilmektedir. Geleneksel medyadaki eşik bekçiliği sisteminin yeni medyada olmayışı bilgi paylaşımında denetimsiz bir düzeni doğurmuştur. Bu durum dünyanın en ücra köşesinden dahi haber alınmasını mümkün kılan “vatandaş muhabirliği” kavramını ortaya çıkardığı gibi kontrol edilmesi oldukça zor çok sayıda içeriğin üretilmesine de neden olmuştur. Geleneksel medyada bilginin üretimi editoryal süreçler ve doğrulama mekanizmalarını gerektirmektedir. Dolayısıyla bir sorumluluk zinciri bulunur. Yeni medyada ise her kullanıcının uzmanlık gerekmeksizin üretici olabilmesi, doğru bilginin de yanlış bilginin de aynı hızda yayılmasına neden olmaktadır. Ayrıca bilginin filtrelenmesi, yankı odaları gibi sorunları da beraberinde getirmiştir.

Kriz zamanlarında daha ciddi etkileri olabildiği için dezenformasyon mücadele daha önemli hâle gelmektedir. Yeni medya ile dünya küresel bir köye dönüşürken bilginin kontrolü olanaksız hâle gelmiştir. Bu küresel köy, insanlığın doğru ve faydalı bilgiye erişimini kolaylaştırdığı gibi yanlış, gerçek dışı, kötü niyetli bilgiye erişimi de mümkün kılmıştır.

Sosyal medya algoritmaları doğruluğu değil etkileşimi ödüllendirdiğinden sansasyonel içerikler daha fazla etkileşim almaktadır ve daha geniş kitlelere sunulabilmektedir. Ancak yanlış bir bilgi sonradan düzeltilse dahi daha az ilgi çekici olduğu için aynı kitleye ulaşmayabilmektedir. Bu da yanlış bilginin zihinde daha kalıcı bir iz bırakmasına neden olmaktadır. Sosyal medyada yanlış bilginin hızla yayılabilmesinin önüne geçilmesi, kullanıcıların yalnızca içerik tüketicisi değil aynı zamanda bilgi güvenliğinin aktif bir parçası olmasını zorunlu kılmaktadır.

Bilgiyi Paylaşmadan Önce Kontrol Et

- Haber mi, yorum mu?
- Bilginin kaynağı kurumsal bir yönetici ya da uzman biri mi?
- Bilgi farklı kaynaklarda da yer alıyor mu?
- Başlık ve içerik uyumlu mu?
- Bu konuda resmî bir açıklama var mı?
- Bilginin kamuya faydası var mı?

DEZENFORMASYONLA MÜCADELE MEKANİZMALARI

Ülkemizde dezenformasyonla mücadele çok paydaşlı, bütünleşik bir sistem ile idare edilmektedir. Cumhurbaşkanlığı İletişim Başkanlığı Dezenformasyonla Mücadele Merkezi (DMM) sistemde koordinasyon ve kamuoyunu aydınlatma görevini üstlenmektedir. DMM yedi gün yirmi dört saat esasıyla çalışmakta, kaynağı ne olursa olsun gerçek ve sanal medyada yayılan yalan, yanlış ve yanıltıcı bilgi ve içerikleri incelemekte ve resmî açıklamalarla doğru bilgiyi kamuoyuna sunmaktadır. DMM'nin internet sitesi ve sosyal medya platformlarında yayınlanan Dezenformasyon Bültenleri vasıtasıyla haftalık olarak dezenformasyon ihtiva eden içeriklerin takip edilmesi mümkündür. DMM'nin internet sitesi ve sosyal medya hesaplarının takip edilmesi bilgi kirliliği ile mücadelede büyük önem arz etmektedir.

DMM'nin internet sayfasında yer alan “Yalanı Bildir” sekmesi kullanarak Dezenformasyon Bildirim Servisi'ne (DBS), medyada rastlanan yalan, yanlış ve yanıltıcı içerikler bildirilebilmektedir.

22 MAYIS 2026 Güncel

*Saudi Arabistan ile Yapılan Enerji Santral Anlaşmasının Türkiye Lehine ...



 **DMM**
Dezenformasyonla Mücadele Merkezi

 **TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI**
İLETİŞİM BAŞKANLIĞI

ANA SAYFA **YALANI BİLDİR** Q

Dezenformasyon Bildirim Servisi
Güncel Haberler

Radyo ve Televizyon Üst Kurulu (RTÜK), televizyon ve radyoları denetler. Yanlış ve manipülatif içeriklere yayın durdurma, para cezası, lisans iptali gibi idari yaptırımlar uygulamaktadır.

Bilgi Teknolojileri ve İletişim Kurumu (BTK) ile Cumhurbaşkanlığı Siber Güvenlik Başkanlığı, zararlı içeriklere erişim tedbirleri ve sosyal medya platformlarının sorumluluklarına yönelik görev ve yetkilere sahiptir.

Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı'nın Siber Suçlarla Mücadele Daire Başkanlıkları, sosyal medya hesapları üzerinden işlenen her türlü yalan, yanlış ve yanıltıcı içeriklerin tespit edilmesi ve adli makamlara intikal ettirilmesiyle görevlidir. Cumhuriyet Başsavcılıkları ve Mahkemeler ise intikal ettirilen suç konusu fillerin tahkikat aşamasını yürütmektedir.

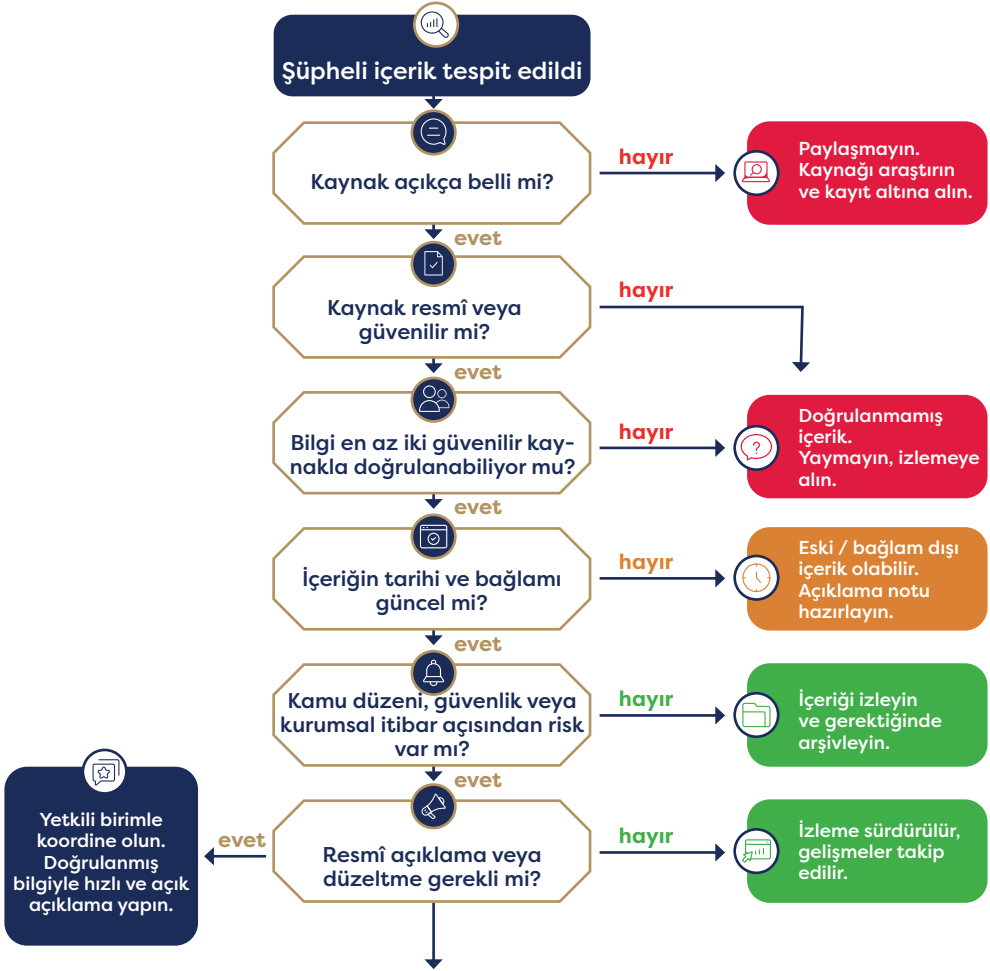
Anadolu Ajansı Teyit Hattı, Anadolu Ajansı bünyesinde faaliyet gösteren ve kamuoyunun doğru, güvenilir ve doğrulanmış bilgiye erişimini desteklemeyi amaçlayan bir birimdir. Bu yapı, özellikle yanıltıcı içerikler, bilgi kirliliği ve bağlamından koparılıp dolaşıma sokulan paylaşımlarla mücadele ederek dijital bilgi ekosisteminin sağlıklı işleyişine katkı sağlamaktadır.

Bireylerin dijital ortamda karşılaştıkları içeriklerin doğruluğunu kendilerinin de kontrol edebilmesi mümkündür. Bu amaçla kullanılan çeşitli ücretsiz ve erişimi kolay araçlar bulunmaktadır. Örneğin Google Görseller üzerinden “Görselle Arama” özelliği kullanılarak bir görsel yüklenebilmekte veya görselin bağlantısı yapıştırılarak internet üzerindeki ilk kaynaklar ve benzer içerikler incelenebilmektedir. Bu yöntem, görselin ne zaman ve hangi bağlamda kullanıldığını anlamada önemli bir kolaylık sağlamaktadır.

Benzer şekilde TinEye platformu da tersine görsel arama için etkili bir araçtır. Görsel dosyasının yüklenmesi veya bağlantısının sisteme eklenmesi yoluyla, görselin daha önce nerelerde ve hangi tarihlerde kullanıldığı tespit edilebilmektedir.

“Doğrulama araçlarının düzenli kullanımı, dijital ortamda karşılaşılan bilgilerin sorgulanmasını kolaylaştırır ve yanlış bilgi yayılımının önüne geçilmesine katkı sağlar.”

Dezenformasyonla Mücadele Karar Akışı



Temel İlke: Doğrulanmamış bilgiyi paylaşmayın

Hızlı Kontrol Noktaları

- ✓ Kaynak belli mi?
- ✓ Bilgi doğrulandı mı?
- ✓ Tarih ve bağlam kontrol edildi mi?
- ✓ Görsel / video eski olabilir mi?
- ✓ Resmî açıklama gerekiyor mu?
- ✓ Paylaşım öncesi son değerlendirme yapıldı mı?

YEREL YÖNETİMİN SOSYAL MEDYA HESAPLARININ YEKNESAKLAŞTIRILMASI

Yerel yönetimlerin sosyal medya platformlarında kurumsal ve doğrulanmış hesaplarla yer alması, kamuoyunun doğru bilgiye hızlı ve güvenilir şekilde ulaşabilmesi açısından büyük önem taşımaktadır. Özellikle sosyal medya mecralarında mavi tik kullanımının yaygınlaştırılması; sahte hesapların önüne geçilmesi, dezenformasyon riskinin azaltılması ve resmî açıklamaların vatandaş nezdinde güvenilirliğinin artırılması bakımından önemli bir tedbir niteliği taşımaktadır.

Instagram platformu üzerinde yapılan genel incelemelerde,

valiliklere ait sosyal medya hesaplarında kullanıcı adı standartlarının farklılık gösterdiği (örneğin; “tcanaravaliliği”, “tc.konya valiliği”, “karsvalilik” vb.) ve bazı hesaplarda doğrulama rozeti (mavi tik) bulunmasına rağmen bazılarında bu uygulamanın yer almadığı görülmüştür. Benzer şekilde kaymakamlıklara ait sosyal medya hesaplarında da kurumsal isimlendirme bakımından yeknesak bir yapı bulunmadığı (“merzifon_kaymakamligi”, “fekekaymakamlık”, “tceldivankaymakamligi” vb.) sınırlı sayıdaki hesap dışında doğrulama rozeti kullanılmadığı anlaşılmaktadır.



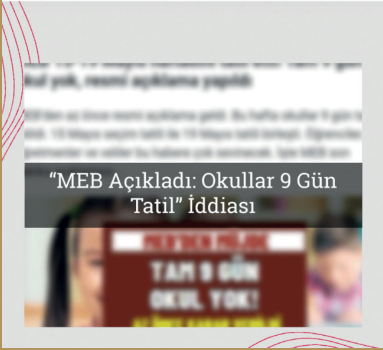
Kurumsal kimliğin dijital mecralarda farklı biçimlerde temsil edilmesi; vatandaşların resmî hesapları ayırt etmesini zorlaştırabilmekte, sahte hesaplar üzerinden yanıltıcı veya hatalı bilgilerin yayılmasına zemin hazırlayabilmektedir. Bu kapsamda; valilik ve kaymakamlıklara ait sosyal medya hesaplarında ortak bir isimlendirme standardının belirlenmesi, tüm resmî hesapların doğrulama süreçlerinin tamamlanarak mavi tik kullanımının yaygınlaştırılması ve kurumsal dijital kimlik bütünlüğünün sağlanması yönünde çalışma yürütülmesinin faydalı olacağı değerlendirilmektedir.



Bununla birlikte; resmî tatil, olumsuz hava koşulları, asayişe ilişkin gelişmeler veya doğal afetler gibi nedenlerle eğitim-öğretime ara verilmesine ilişkin süreçlerde, kamuoyunu yanıltabilecek nitelikteki asılsız haber ve paylaşımların yakından takip edilmesi, gerekli durumlarda ise doğru ve zamanında bilgilendirme yapılarak bu tür dezenformasyon içerikleriyle etkin şekilde mücadele edilmesi önem arz etmektedir.



“



“MEB Açıkladı: Okullar 9 Gün Tatil” İddiası

13.05.2023

Bazı basın yayın organlarında yer alan, “MEB açıkladı: Okullar 9 gün tatil” iddiası doğru değildir. Milli Eğitim Bakanlığı böyle bir açıklama yapmamıştır. Ülkemizde oy verme işlemi okullarda gerçekleştirildiği için haftasonu tatiline ek olarak sadece 15 Mayıs Pazarlığı günü eğitime bir gün ara verilecektir. Resmi açıklamalar dışında yayılan iddialar dikkate alınmamalıdır.

GÜNCEL YALAN HABERLER

”

İDARECİLER NE YAPABİLİR?

Paylaşılan haberde doğruluk, tarafsızlık gibi unsurların korunduğuna; 5N1K gibi temel sorulara cevap verildiğine dikkat edilmeli.

Dezenformasyon içeriklerine karşı doğru bilgiyi esas alan etkili karşıt söylemler geliştirilmeli.

Şeffaflık artırılmalı, yanlış bilginin yayılmasını önleyecek açık bilgilendirme politikaları uygulanmalı.

Doğru bilgiye erişim için farklı hedef kitlelere yönelik iletişim stratejileri oluşturulmalı.

Bilgi düzensizliğinin oluşturabileceği toplumsal risklere karşı farkındalık çalışmaları yürütülmeli, olası kriz senaryoları geliştirilmeli.

Akademik kurumlar, medya kuruluşları ve sivil toplum örgütleriyle ortak projeler ile dezenformasyona karşı iş birliği artırılmalı.

Bakanlık tarafından belirlenen yayın politikası dikkatle takip edilerek merkez ile uyumlu dil geliştirilmeli.

Çalışanlara yönelik medya okuryazarlığı, dijital farkındalık ve siber güvenlik eğitimleri düzenlenmeli.

Güvenilir bilgiye erişimini desteklemek amacıyla kaliteli ve doğrulanmış içerik üretimi teşvik edilmeli.

Sosyal medya hesaplarının görsel unsurlar itibarıyla kurumsal kimliğe uygun biçimde yeknesaklaşması sağlanmalı.

Ulusal ve yerel düzeydeki özel günlerin yanı sıra kriz oluşturabilecek kritik günler takvimi oluşturulmalı ve güncellenmelidir.

Dezenformasyon ihtiva eden içeriklerle ilgili kesin karar verilemediği hallerde Cumhurbaşkanlığı İletişim Başkanlığı Dezenformasyonla Mücadele Merkezi'nin görüşü alınmalı.

MEDYA OKURYAZARLIĞI VE DİJİTAL ÇAĞDA ÖNEMİ

Dijitalleşmenin hız kazanmasıyla birlikte bireylerin ve kurumların bilgiye erişim, bilgi üretme ve paylaşma biçimleri önemli ölçüde değişmiştir. Sosyal medya platformları, çevrim içi haber kaynakları, video paylaşım siteleri ve diğer dijital iletişim araçları, bilgi akışını hızlandırırken aynı zamanda yanlış bilgi, dezenformasyon, manipülatif içerikler ve bilgi kirliliği gibi riskleri de beraberinde getirmiştir. Bu nedenle medya okuryazarlığı, günümüzün en önemli dijital yetkinliklerinden biri hâline gelmiştir.

Medya okuryazarlığı; bireylerin ve kurumların medya içeriklerini bilinçli, eleştirel, güvenli ve sorumlu bir şekilde analiz etme, değerlendirme, kullanma ve üretme becerisi olarak tanımlanabilmektedir. Bu beceri yalnızca medya araçlarını kullanabilmeyi değil, aynı zamanda içeriklerin kaynağını sorgulamayı, doğruluğunu teyit etmeyi ve farklı bakış açılarını değerlendirebilmeyi de kapsamaktadır.

Günümüzde medya okuryazarlığı kavramı yalnızca geleneksel medya araçlarıyla sınırlı değildir. Televizyon, radyo ve basılı yayınların yanı sıra sosyal medya platformları, dijital haber siteleri, çevrim içi forumlar ve mobil uygulamalar da medya ekosisteminin ayrılmaz parçalarıdır. Bu nedenle medya okuryazarlığı, geleneksel ve dijital medyayı birlikte değerlendiren bütüncül bir yaklaşım gerektirmektedir.

Kamu kurumları açısından medya okuryazarlığı, kurumsal itibarın korunması, doğru bilgi paylaşımının sağlanması ve vatandaşlarla güvene dayalı iletişim kurulması bakımından stratejik öneme sahiptir. Kurum çalışanlarının dijital platformlarda karşılaştıkları içerikleri eleştirel bir bakış açısıyla değerlendirebilmeleri, bilgi doğrulama yöntemlerini kullanabilmeleri ve resmî kaynaklara dayalı iletişim kurabilmeleri önem taşımaktadır.

Özellikle sosyal medya ortamlarında yayılan yanlış bilgi ve dezenformasyon içerikleri, kamuoyunun yanıltılmasına ve kurumlara duyulan güvenin zedelenmesine neden olabilmektedir. Medya okuryazarlığı becerileri, bu tür içeriklerin erken tespit edilmesini, doğrulanmasını ve gerektiğinde doğru bilginin hızla kamuoyuyla paylaşılmasını desteklemektedir.

Medya okuryazarlığı aynı zamanda etik iletişim anlayışını güçlendirmektedir. Telif haklarına saygı gösterilmesi, kişisel verilerin korunması, mahremiyet ilkelerine uyulması, ayrımcı ve yanıltıcı içeriklerden kaçınılması gibi konular dijital ortamda sorumlu iletişimin temel unsurlarıdır. Kamu kurumlarının sosyal medya faaliyetlerinde bu ilkelere uygun hareket etmesi, kurumsal güvenilirliğin artırılmasına katkı sağlamaktadır.

Sonuç olarak medya okuryazarlığı, dijital çağın gerektirdiği temel bir yetkinlik olup, bilgiye erişim, bilgiyi değerlendirme, doğrulama ve etkili iletişim kurma süreçlerinde kritik rol oynamaktadır. Kamu kurumlarının sosyal medya kullanımında medya okuryazarlığı yaklaşımını benimsemesi, hem kurumsal iletişim kalitesinin yükselmesine hem de toplumun doğru ve güvenilir bilgiye erişiminin güçlenmesine katkı sağlayacaktır.

SOSYAL MEDYA SÖZLÜĞÜ

AFİŞ (BANNER):

Afiş veya banner, sosyal medya profillerinin en üst kısmında yer alan, görsel marka kimliğini yansıtan geniş grafik alanıdır. Banner; güncel kampanyaları duyurmak, markanın değer önermesini (value proposition) saniyeler içinde iletmek ve profesyonel bir duruş sergilemek için kullanılır.

AKIŞ (NEWSFEED):

Akış veya haber kaynağı, kullanıcının platformda gördüğü içeriklerin sürekli güncellenen listesidir. Akışlar modern anlamda kronolojik olmaktan çıkıp tamamen “algoritmik kürasyon” sistemine dayalı hâle gelmiştir. Bu durum da kullanıcıları bilgiyi aktif olarak aramak yerine algoritmaların kendilerine sunduğu içerikleri tüketen pasif alıcılara dönüştürmüştür.

ALGIDA SEÇİCİLİK (SELECTIVE PERCEPTION):

Algıda seçicilik; bireylerin kendi mevcut inançları, tutumları ve beklentileriyle uyumlu bilgileri fark etmesi, yorumlaması ve hatırlaması yanında çelişen bilgileri görmezden gelmesi veya çarpıtması eğilimidir. Sosyal medya algoritmaları bu süreci “filtre balonları” ve “yankı odaları” yaratarak otomatize eder ve bireyler farklı fikirlere açık olmak yerine kendi dünya görüşlerinin sürekli doğrulandığı dijital dünyayı görürler.

ALGORİTMA TAKİBİ (ALGORITHM CHASING):

Algoritma takibi, içerik üreticilerinin ve dijital pazarlamacıların, hedef kitlelerinin ilgi alanlarını gözetmek yerine platform algoritmalarının o anki önceliklerine (belirli sesler, video formatları veya hashtag’ler) göre içerik üretme stratejisidir.



AVATAR:

Dijital ortamlarda kullanıcıyı temsil eden görsel ya da dijital bir kimlik biçimidir. Diğer kullanıcılarla, varlıklarla ya da çevreyle etkileşimi kolaylaştıran insan kullanıcının dijital temsilidir. Bu nedenle avatar, sosyal medya profili, oyun karakteri, sanal gerçeklik bedeni ya da çevrim içi platformlarda kullanılan kişisel bir temsil biçimi olarak düşünülebilir. İletişim açısından avatar, bireyin çevrim içi ortamda kendisini nasıl sunduğunu ve başkalarıyla nasıl etkileşim kurduğunu gösteren sembolik bir araçtır.

BAHSETME (MENTION):

Sosyal medya platformlarında bir kullanıcıdan söz etmek ya da onu içeriğe dâhil etmek için kullanılan etiketleme biçimidir. Genellikle “@” işaretiyle birlikte kullanıcı adı yazılarak yapılır. X Yardım Merkezi, “gönderinin herhangi bir yerinde başka bir kişinin kullanıcı adını içeren bir gönderi” kavramını tanımlar.

BİLDİRİM (NOTIFICATION):

Mobil telefonlarda kullanıcıları yeni mesajlar, e-postalar, sosyal ağ güncellemeleri ve diğer olaylar hakkında uyaran dijital iletilerdir.

BİLGİ GÜVENLİĞİ

Bilgi güvenliği, yalnızca teknik sistemlerin korunması değil; aynı zamanda insan, süreç ve teknoloji unsurlarının birlikte yönetilmesini gerektiren çok boyutlu bir yapıdır. Bilgi güvenliği, gizlilik, bütünlük ve erişilebilirlik ilkelerine dayanan bir yönetim yaklaşımıdır. Literatürde “CIA Triadı” olarak ifade edilen bu yapı, bilgi güvenliği politikalarının temelini oluşturmaktadır. Gizlilik, bilginin yalnızca yetkili kişiler tarafından erişilebilir olmasını ifade ederken bütünlük, verinin doğruluğunun ve değişmezliğinin korunmasını; erişilebilirlik ise yetkili kullanıcıların ihtiyaç duydukları anda bilgiye ulaşabilmesini ifade eder.

BİLGİSAYAR KORSANI (HACKER):

Bir bilgisayar ya da bilişim sistemiyle tasarımcının öngörmediği yollarla etkileşime giren ve çoğu durumda yetkisiz erişim sağlayan kişidir.

BİLİŞSEL CİMRİLİK:

İnsan zihninin sınırlı bilgi işleme kapasitesi nedeniyle karmaşık durumlarda ayrıntılı düşünmek yerine kısa yolları ve pratik çözümleri tercih etmesidir.

BİYOĞRAFI (BIO):

Gerçek bir kişinin yaşamını, olayları ve dönüm noktalarını belirli bir anlatı düzeni içinde aktaran kurmaca dışı metin türüdür.

BOT ÇİFTLİĞİ (BOT FARM):

Bot çiftliği, çok sayıda sosyal medya hesabının bir yazılım aracılığıyla tek bir merkezden yönetilerek yapay trafik, beğeni ve yorum üretilmesi işlemidir. Bot çiftlikleri, reklam verenleri “sahte tıklamalarla” (ad fraud) dolandırır, siyasi dezenformasyon yayar ve rakip firmaların reklam bütçelerini boş tıklamalarla tüketirler.

BOT HESAP:

Sosyal medya platformlarında yazılım tarafından yönetilen ve paylaşım yapma, beğenme, takip etme veya kullanıcılarla etkileşime girme gibi işlemleri otomatik ya da yarı otomatik biçimde gerçekleştiren hesaptır.

CANLI YAYIN (LIVE STREAM):

Ses veya görüntü verisinin internet üzerinden sürekli bir akış hâlinde, anında izlenebilmesi için aktarılmasıdır.

ÇİFTE DOĞRULAMA (DOUBLE CHECK):

Karşılaşılan bir bilginin doğru olup olmadığını anlamak için aynı iddianın ikinci bir güvenilir kaynak, dış bağlantı ya da bağımsız kanıtla tekrar kontrol edilmesidir.

ÇİFTLİK HESABI (FARM ACCOUNT):

Çiftlik hesapları; genellikle ticari veya manipülatif amaçlarla bot çiftlikleri veya profesyonel “hesap çiftçileri” tarafından toplu hâlde



oluşturulan, jenerik kimliklere sahip sosyal medya hesaplarıdır. Bu hesaplar, platformların güvenlik sistemlerine takılmamak için belirli bir süre sahte etkileşimle aktif gösterilir.

ÇORAP KUKLA HESAPLAR (SOCK PUPPET ACCOUNT):

Çorap kukla hesaplar, bir kullanıcının kendi ana kimliğini gizleyerek başkasıymış gibi davrandığı, genellikle tartışmalarda kendini desteklemek veya rakiplerine saldırmak için kullandığı sahte profillerdir. Bu hesaplar, tek bir “kukla oynatıcısı” tarafından kontrol edilir.

DEEPFAKE:

Yapay zekâ ve derin öğrenme teknikleriyle üretilen ya da değiştirilen; gerçek bir kişinin söylemediği veya yapmadığı bir şeyi söylüyormuş/yapıyormuş gibi gösterebilen sahte ses, görüntü ya da videodur.

DEZENFORMASYON:

Yanlış olduğu bilinen bilginin bir kişi, grup, kurum ya da ülkeye zarar vermek amacıyla kasıtlı olarak üretilmesi veya yayılmasıdır.

DİJİTAL AYAK İZİ:

Bireylerin internet ve dijital platformlardaki etkinlikleri sonucunda geride bıraktıkları izler, bilgiler ve veri kayıtlarıdır.

DİJİTAL GÖÇMENLİK (DIGITAL IMMIGRANTS):

Dijital teknolojilerin içine doğmamış; ancak yaşamının ilerleyen dönemlerinde bilgisayar, internet ve dijital araçları öğrenip kullanmaya başlamış kişileri ifade eder.

DİJİTAL YERLİLİK (DIGITAL NATIVES):

Bilgisayar, internet ve dijital teknolojilerin yaygın olduğu bir dönemde büyüyen kuşağı ifade eder.

DOĞRULAMA YANLILIĞI:

Kişinin mevcut inanç, tutum veya beklentileriyle uyumlu bilgileri daha kolay kabul etmesi; bunlarla çelişen bilgileri ise görmezden gelme, küçümseme ya da farklı yorumlama eğilimidir.

DOĞRULANMIŞ HESAP (VERIFIED):

Bir sosyal medya platformunda veya dijital hizmette, hesabın gerçekten iddia edilen kişiye, markaya veya kuruma ait olduğunun platform tarafından kimlik kontrolü (teyit) ile belirlenmesi işlemidir.

DOĞRULUK DÜRTMESİ (TRUTH NUDGE):

Özellikle dijital platformlarda ve sosyal medyada, kullanıcıların bir bilgiyi paylaşmadan önce o bilginin doğruluğunu kontrol etmelerini teşvik eden, küçük, etkili ve genellikle otomatikleştirilmiş ipuçları veya hatırlatıcılar olarak tanımlanır.

ENFOKRASİ:

Enformasyon (bilgi/haber) ve demokrasi kelimelerinin birleşimiyle türetilen; bireylerin yoğun enformasyon akışı, dijital gözetim ve görünürlük yoluyla manipüle edildiği, özgürlük illüzyonunun hâkim olduğu yeni bir yönetim/egemenlik biçimidir.

ETKİLEŞİM AKLAMA (ENGAGEMENT LAUNDERING):

Etkileşim aklama; kötü niyetli veya yasa dışı içeriklerin, meşru reklam platformları ve güvenilir profiller arkasına saklanarak “temiz” bir görünümle kullanıcılara sunulması sürecidir. Para aklamaya (money laundering) benzer şekilde, etkileşim aklama da kaynağın kirli doğasını (dolandırıcılık, zararlı yazılım) gizlemeyi hedefler.

ETKİLEŞİM ÇİFTÇİLİĞİ (ENGAGEMENT FARMING):

Etkileşim çiftçiliği, dijital platformlarda anlamlı bir değer sunmak veya organik bir topluluk oluşturmak yerine sadece beğeni, yorum ve paylaşım gibi unsurları artırmak için sayısal içerikler üretme pratiğidir. Genellikle sevimli hayvan fotoğrafları paylaşmak, “Bunu görenler bir



kalp bıraksın” gibi doğrudan eylem çağrılarında bulunmak veya popüler tartışmaları hiçbir katma değer sunmadan yeniden dolaşıma sokmak gibi yöntemler kullanılır.

ETKİLEŞİM GRUPLARI (ENGAGEMENT PODS):

Etkileşim grupları (pods), bir grup kullanıcının bir araya gelerek birbirlerinin paylaşımlarını karşılıklı olarak beğenme, yorumlama ve paylaşma taahhüdünde bulunduğu kapalı topluluklardır. Temel amaç, paylaşım sonrası “altın pencere” olarak bilinen ilk dakikalarda yüksek etkileşim sağlayarak algoritmayı yanıltmaktır.

ETKİLEŞİM TUZAĞI:

İnsanları beğenmeye, paylaşmaya, yorum yapmaya veya diğer etkileşim eylemlerini gerçekleştirmeye teşvik ederek sosyal medya platformlarında yapay bir şekilde daha fazla erişim elde etmeyi hedefleyen içerik yaklaşımıdır.

FİLTRE BALONU (FILTER BUBBLE):

İnternet arama motorları ve sosyal medya algoritmalarının, kullanıcının geçmiş tıklamaları, konumu ve ilgi alanlarına göre kişiselleştirilmiş içerik sunması sonucu oluşan “entelektüel izolasyon” durumudur. Bu durum, kullanıcının sadece kendi görüşünü destekleyen bilgilere maruz kalmasına ve farklı bakış açılarından kopmasına neden olan görünmez bir dijital duvardır.

FOMO (FEAR OF MISSING OUT):

Türkçede “günceli kaçırma korkusu” veya “fırsatları kaçırma endişesi” anlamına gelir. Başkalarının daha eğlenceli deneyimler yaşadığına, daha iyi fırsatlar elde ettiğine veya önemli gelişmelerden habersiz kaldığına dair duyulan yoğun kaygı ve huzursuzluk hissidir.

FYP (FOR YOUR PROFILE/PAGE):

Sosyal medya platformlarında kullanıcıya özel olarak algoritmalar tarafından önerilen içeriklerin yer aldığı kişiselleştirilmiş akış sayfasını ifade eden kavramdır.

GÜNDEM BELİRLEME:

Gündem belirleme, kitle iletişim araçlarının ve dijital medya platformlarının hangi konuların önemli olduğu konusunda kamuoyunun dikkatini yönlendirme gücünü ifade eden iletişim kuramıdır.

HAKİKAT SONRASI (POST-TRUTH):

Kamuoyunun bir konuda karar verirken ya da bir konu hakkında kanaat getirirken doğruları belirlemesinde, ortak nesnel deliller yerine birtakım kişisel duygular ve inançların etkili olduğu ortamı ifade eder.

HATALI İLİŞKİLENDİRME:

Bir olaya ait fotoğraf, video, başlık veya bilginin, tamamen farklı, alakasız bir olayla ilişkilendirilerek sunulmasıdır. Dezenformasyonun en yaygın türlerinden olan bu yöntem, eski veya stok görüntülerin güncel bir olay gibi paylaşılmasıyla kitleleri yanıltmayı amaçlar.

HİPERGERÇEKLİK:

Hiper gerçeklik, medya, dijital teknolojiler ve simülasyonlar aracılığıyla üretilen görüntü ve temsillerin, gerçekliğin yerini alması veya gerçeklikten daha etkili hâle gelmesi durumunu ifade eden kavramdır. Özellikle sosyal medya, reklamlar, sanal ortamlar ve yapay zekâ içerikleri bireylerin gerçeklik algısını şekillendirebilmektedir.

İNFOBEZİTE:

Dijital çağda bireylerin maruz kaldığı aşırı, gereksiz ve düzensiz bilgi bombardımanı nedeniyle doğru bilgiye ulaşmakta zorlanması, zihinsel yorgunluk yaşaması ve odaklanma sorunu çekmesi durumudur. Enformasyon ve obezite kelimelerinin birleşimiyle oluşan bu kavram, sindirilemeyecek kadar çok bilginin yarattığı bilişsel yükü ifade eder.

İNFODEMİ:

Salgın gibi durumlarda, dijital ve/veya fiziksel ortamlarda bireylerin doğru davranışlara yönelmesini zorlaştıran yanlış bilgi, çarpıtılmış/kasıtlı yanlış bilgi, bilgi boşluğu, söylenti, doğrulanmamış bilgi, komplo teorisi gibi farklı bileşenleri olan bilgi bolluğudur.



İTİBAR AVCILIĞI (CLOUT CHASING):

İtibar avcılığı, bir kişinin veya hesabın, kendi sosyal statüsünü ve popülaritesini artırmak için daha ünlü kişilerle, trend olan konularla veya viral tartışmalarla zorlama bir şekilde ilişki kurma çabasıdır.

KİTLESEL PANİK:

Büyük bir trajedi, hayalî tehdit veya yoğun korku anlarında insan topluluklarının rasyonel düşünme yetisini kaybederek kontrolsüz, tehlikeli ve kaotik davranışlar sergilemesi durumudur.

KOORDİNELİ İNHANTİK DAVRANIŞ (COORDINATED INAUTHENTIC BEHAVIOR - CIB):

Bir grup hesabın, kullanıcıları yanıltmak veya kamuoyu tartışmalarını bozmak amacıyla ortaklaşa ve aldatıcı bir stratejiyle hareket etmesidir. CIB'nin ana odak noktası içeriğin ne olduğundan ziyade o içeriği yayan ağın "kimliğini gizlemesi ve aldatıcı bir koordinasyon içinde olmasıdır".

MALENFORMASYON:

Gerçek, doğru veya doğrulanabilir bilgilere dayanan, ancak bir kişiye, kuruluşa veya ülkeye zarar verme amacıyla bağlamından koparılarak veya manipüle edilerek kullanılan bilgi türüdür.

MEYDAN OKUMA (CHALLENGE):

Sosyal medyada challenge, "meydan okuma" veya bir görevi yerine getirme amacıyla başlatılan viral akımlara verilen isimdir. Bir kullanıcı veya topluluk, kamera karşısında belirli bir eylemi (komik bir dans, makyaj, zorlu bir hareket) gerçekleştirir ve arkadaşlarını veya tüm takipçilerini aynı şeyi yapmaya davet eder.

MİSİNFORMASYON:

Hatalı veya yanıltıcı bilgidir. Yanlış bilgi genellikle kasıtlı olmadan, çoğunlukla bilgi eksikliği, hata veya basit bir yanlış anlama nedeniyle yayılır. Yanlış bilgi, yanlış, eksik, yanıltıcı veya sahte bilgilerin yanı sıra seçici veya yarı doğruları da içerebilir.

NETLESSFOBİ:

İngilizce “being netless phobia” ifadesinden türetilmiş olup “internetsiz kalma korkusu” anlamına gelir. Bu kavram, internete erişimin olmadığı bir ortamda bulunma durumunda bireyde kaygı, huzursuzluk ya da kontrol kaybı hissi doğması hâlini betimler. Bu korku, internetin aşırı kullanımından ziyade kişinin internet bağlantısı olmayan bir ortamda kalamaması ve internetsizlik endişesi yaşaması şeklinde tanımlanır.

NPC İÇERİĞİ (NPC CONTENT):

NPC içeriği, yayıncıların video oyunlarındaki “Non-Player Character” (Oyuncu Olmayan Karakter) figürlerini taklit ederek tekrarlayan robotik hareketler ve sloganlar sergilediği bir canlı yayın eğilimidir. Bu durum, dijital etkileşimin en mekanik ve paraya dönüştürülebilir hâllerinden birini temsil eder.

NOMOFOBİ:

İngilizcedeki “no mobile phobia” kelimelerinin kısaltmasıdır. Bireylerin cep telefonları olmadığında veya kullanamadıklarında yaşadıkları endişe veya korkuyu ifade eder. Nomofobi, günlük yaşamda bireylerde yoğun kaygı yaşama ile kişiler arası iletişim kurma ve performans gösterme gibi sorunları beraberinde getirebilmektedir.

ÖFKE TUZAĞI (RAGE BAIT):

“Rage-baiting” ya da öfke tuzağı, internet terminolojisinde bir web sayfasına trafik çekmek, etkileşim oranlarını artırmak veya abone sayısını çoğaltmak amacıyla kasıtlı olarak öfke, nefret veya infial uyandıracak içerikler paylaşma taktiğidir. Bu strateji, klasik tıklama tuzağının (clickbait) çok daha agresif ve “kötü ikizi” olarak nitelendirilen bir versiyonudur. Çünkü merak uyandırmak yerine doğrudan ahlaki veya duygusal bir çatışma başlatmayı hedefler.



PROPAGANDA:

Çok sayıda insanın düşünce ve davranışlarını etkilemek amacını taşıyan önceden planlanmış bir mesajlar bütünüdür. Propaganda tarafsız bilgi sağlamak yerine, en temelde kendi kitlesini etkileyecek bilgiyi sunar. Mesaj doğru olsa da yönlü olabilir ve olayın tümünü dengeli bir şekilde sunmayabilir.

RATIO / RATIOLANMAK:

“Ratioed” olmak veya ratiolanmak, sosyal medyada (özellikle X platformunda) bir paylaşımın aldığı beğeni veya yeniden paylaşım sayısından çok daha fazla yanıt alması durumudur.

RESİM ALTI (CAPTION):

Gazeteler, dergiler ve web sitelerinde resim altı yazıları, fotoğrafın tam olarak ne anlattığını belirten, bağlamı sağlayan kısa açıklamalardır.

SAHTE ETKİLEŞİM (FAKE ENGAGEMENT):

Sahte etkileşim, gerçek kullanıcılar yerine botlar veya ücretli “tıklama tarlaları” (click farms) aracılığıyla elde edilen her türlü dijital aksiyonu kapsar. Bu durum, takipçi sayısını prestij göstergesi gören sosyal medya anlayışının bir ürünüdür.

SAHTE HESAP:

Bir bireyin veya kuruluşun gerçek kimliğini gizleyerek, başka birinin bilgilerini taklit ederek ya da tamamen hayali bir karakter oluşturarak sosyal ağlarda açtığı kullanıcı profilidir.

SANAL CASUSLUK (STALK):

Bilgi sahibinin izni ve bilgisi olmadan, internet, ağlar veya bireysel bilgisayarlar üzerinden proxy sunucuları, kırma teknikleri ve Truva atları ve casus yazılımlar dâhil olmak üzere kötü amaçlı yazılımlar kullanarak sırları ve bilgileri elde etme eylemi veya uygulamasıdır.

SARI GAZETECİLİK (YELLOW JOURNALISM):

Çok az dayanağı olan ya da hiçbir dayanağı olmadan yapılmış bir araştırmaya göz alıcı haber başlıkları eklenerek daha çok gazete satmak için yapılan gazetecilik türüdür. Bu teknik, bazen haberlerdeki olayın abartılması, skandal tüccarlığı ya da sansasyonelizm olarak ortaya çıkabilir. Bu terim günümüzde, profesyonel ya da etik olmayan, alçaltıcı şekilde kötüleyici gazetecilik için de kullanılır.

SERİ İZLEME (BINGE WATCH):

Bir dizinin, filmin veya video serisinin çok sayıda bölümünü aralıksız tek oturuşta veya çok kısa bir zaman diliminde peş peşe izleme eylemidir.

SİBER VATAN :

Siber güvenlik ve bilişim alanında kapasite iyileştirilmesini sağlayarak yetişmiş insan gücünün artırılması ve dijital sistem teknolojisinin gelişimine hız katacak yeni ürün/hizmet elde etme amacı taşıyan programdır.

SİBER ZORBALIK:

Dijital teknolojiler kullanılarak gerçekleştirilen zorbalıktır. Bu tür zorbalıklar sosyal medyada, mesajlaşma platformlarında, oyun platformlarında ve cep telefonlarında görülebilir. Hedef seçilen kişileri korkutmaya, kızdırmaya ya da utandırmaya yönelik tekrarlanan davranıştır.

SİBER BALKANLAŞMA:

İnternet kullanıcılarının benzer görüş, ilgi alanı veya ideolojiye sahip küçük gruplara bölünerek yalnızca kendi yankı odalarına kapanması ve farklı fikirlerden izole olması durumudur.

SOSYAL BOTLAR:

Beğenme, içerik paylaşma ve diğer kullanıcılarla sohbet etme gibi çoğu sıradan kullanıcının eylemlerini gerçekleştirmek üzere tasarlanmış, tamamen veya kısmen otomatikleştirilmiş sosyal medya hesaplarını ifade eder.



SUNİ KAMUOYU (ASTROTURFING):

Astroturfing, bir mesajın arkasında çok geniş, bağımsız ve kendiliğinden oluşmuş bir toplumsal destek (grassroots) varmış izlenimi yaratmak için yürütülen organize faaliyettir. Terim, suni çim markası “AstroTurf”ten türetilmiştir; gerçek çim gibi görünür ama plastiktir.

TEYİT:

Bir bilgi, belge veya durumun doğruluğunu kanıtlama, onaylama veya doğrulamadır.

TIKLAMA TUZAĞI (CLICKBAIT):

Dikkat çekmek ve kullanıcıları bu bağlantıyı izlemeye ve bağlantılı çevrim içi içeriği okumaya, görüntülemeye veya dinlemeye ikna etmek için tasarlanmış köprü metni veya küçük resim bağlantısı kullanan yanıltıcı reklam biçimidir.

TREND:

Belirli bir zaman diliminde kullanıcıların yoğun ilgi gösterdiği, hakkında en çok konuşulduğu, paylaştığı ve etkileşim kurduğu konu, müzik, etiket (hashtag), video veya akımları ifade eder.

VATANDAŞ GAZETECİLİĞİ:

Mesleği gazetecilik olmayan kişilerin, dijital araçlar yardımıyla haber üretmek paylaşmasına verilen addır.

VERİ GÜVENLİĞİ:

Dijital ve fiziksel bilgilerin yetkisiz erişime, hırsızlığa veya bozulmaya karşı korunması sürecidir. Verileri onaylanmayan erişime karşı korumak ve veri gizliliğini, bütünlüğünü aynı zamanda erişilebilirliğini korumak amacıyla yapılan bir takım koruyucudur. Veri güvenliğinin en iyi uygulamaları, veri şifreleme, anahtar yönetimi, veri düzeltme, verileri alt kümelere ayırma ve veri maskeleyme gibi veri koruma tekniklerinden oluşabilir.

VERİ MADENCİLİĞİ

Büyük veri yığınları içindeki gizli kalıpları, eğilimleri ve ilişkileri ortaya çıkarmak için makine öğrenimi, istatistik ve yapay zekâ yöntemlerinin kullanıldığı bir süreçtir. Gelişmiş bilgisayar algoritmalarını ve yazılım programlarını kullanarak büyük veri kümelerinin derinlemesine incelenmesine, gizli bilgilerin ortaya çıkarılmasına ve bunların eyleme geçirilebilir verilere dönüştürülmesine olanak tanır.

VİRAL OLMAK:

Bir içeriğin sosyal ağlar üzerinden kullanıcıdan kullanıcıya katlanarak ve kontrolsüzce geniş kitlelere ulaşmasıdır.

YAKINSAMA:

Yazılı metin, ses, video, grafik ve etkileşim gibi farklı medya türlerinin ve teknolojilerinin tek bir dijital platformda (örneğin akıllı telefonlar veya sosyal ağ uygulamaları) birleşmesidir.

YALAN HABER:

Haber olarak sunulan, gerçekliği olmayan, tamamen ya da kısmen uydurma ve yanıltıcı bilgilerdir. Yalan haberler yalan içeren veya hepsinin yanlış olması muhtemel olmayan tüm ifadelerin bir hikâye, bir makale olarak sunulmasıdır. İnternet ortamı sahte haberin üretilmesine ve yayılmasına yardımcı olmaktadır. Yalan haberlerin içeriği ile genel olarak dünya arasındaki bağlantı en iyi ihtimalle şüphelidir. Yalan haberlerin yaratılmasına ve yayılmasına bir kasıtlılık unsuru yüklenmektedir.

YAN OKUMA (LATERAL READING):

Okuyucunun bir yazarın güvenilirliğini daha derinlemesine belirlemek sunulan gerçekleri birden fazla kaynaktan kontrol ederek geçerliliğini sağlamak ve o konuyu detaylıca araştırmak için kullandığı bir tekniktir. Bu gerçek kontrol tekniği, günümüzde gerçek bilgi ile yalan haberleri ayırt etmenize yardımcı olan ve her zaman gerçekten bilgili kalmanıza yardımcı olan son derece önemli bir araçtır. Özellikle dijital çağda karşılaşılan bir bilginin, kaynağın veya haberin güvenilirliğini doğrulamak için kullanılan etkili bir araştırma ve teyit stratejisidir.

YANKI ODASI (ECHO CHAMBER):

Katılımcıların kapalı bir sistem içinde iletişim ve tekrar yoluyla önceden var olan inançlarını güçlendiren veya pekiştiren inançlarla karşılaştığı ve karşıt görüşlerden izole edildiği bir ortam veya ekosistem olarak tanımlanır. Filtre balonlarının da etkisiyle sosyal medya ortamında insanlar kendileri gibi düşünen insanların bulunduğu yankı odalarında bulunur ve karşılıklı etkileşime girer. Yankı odaları, hem içinde iletilen mesajları büyütme hem de onları çürütmeden izole etme potansiyeline sahip sınırlı ve kapalı bir medya alanıdır.

YAPAY GÜNDEM:

Özünde kamuoyunun gerçekten konuştuğu, merak ettiği, ilgilendiği konuları yansıtmayan, bir kişinin veya bir zümrenin kamuoyunca konuşulmasını istediği spesifik bir meseleyi belirli medya araçları kullanarak dolaşıma sokmasıyla oluşan gündemlerdir.

YAPAY ZEKÂ ÇÖPÜ (AI SLOP):

“AI Slop”, yapay zekâ araçları kullanılarak hiçbir insani özen, denetim veya katma değer olmaksızın seri hâlde üretilen düşük kaliteli içerikleri tanımlar. Bu terim, besleyici değeri olmayan ancak her yeri kaplayan “dijital posa” anlamında kullanılır. Yani AI Slop, kaliteli bilginin görünürlüğünü engeller. Böylece kitlelerin güvenini sarsar ve platformlar tarafından tespit edildiğinde hesabın erişiminin kısıtlanmasına (deprioritization) neden olur.

EK 1:

SOSYAL MEDYA ETİK İLKELERİ

Tarafsızlık

Kamu görevlisi;

1. Kamu politikaları hakkında kamuya açık yorumlar yaparken veya bunlar hakkındaki kamuoyu tartışmalarına katılırken yürüttüğü göreve ilişkin tarafsızlığını tehlikeye atan davranışlardan kaçınmalıdır.
2. Bireyler arasında dil, ırk, etnik köken, renk, cinsiyet, siyasi düşünce, felsefi inanç, din, mezhep, servet, medeni hâl, sağlık durumu, engellilik, yaş, kılık ve kıyafet ve benzeri nedenlerle ayrımcılık yapmamalıdır.
3. Siyasi tarafsızlığını korumaya özen göstermeli, kamu hizmetinin tarafsızlığına şüphe düşürecek şekilde, herhangi bir siyasi parti veya girişimin lehine veya aleyhine kampanya yürütmemeli, yorum, paylaşım ya da faaliyette bulunmamalıdır.

Kurum itibarını koruma

Kamu görevlisi;

1. Görev yaptığı kurumun görev ve işleriyle ilgili bilgileri sosyal medya platformlarında paylaşırken ilgili mevzuata uygun davranmalıdır.
2. Görev yaptığı kurumun itibarını ve güvenilirliğini zedeleyecek veya karalayacak nitelikteki paylaşımlardan kaçınmalıdır.
3. Kişisel sosyal medya hesaplarında, uzmanlık alanı çerçevesindeki görüşlerini, kurumun itibarı üzerindeki olası etkilerini dikkate alarak ve kanıtlara dayalı olarak ifade edebilir. Ancak sosyal medyada yer alan sözlü, yazılı veya görsel içerikli paylaşımlarının kişisel görüşü olduğunu belirtmeli, görevine, kurumuna veya kamu hizmetine atfedilmemesi hususlarında dikkatli davranmalıdır.

Çıkar çatışmasından kaçınma

Kamu görevlisi, sosyal medyayı kullanırken mevcut veya gelecekte olma ihtimali bulunan çıkar, çıkar çatışması ya da bu konuda algı oluşturabilecek durumlardan kaçınmalıdır.

Kamu hizmetine ayrılan zamanda sosyal medya kullanımı

Kamu görevlisi, kamu hizmetine ayrılan zamanda sosyal medya kullanımı konusunda dikkatli davranmalı ve kamu hizmetini aksatmamalıdır.

Paylaşılan bilginin içeriği

Kamu görevlisi;

1. Sosyal medyada bilginin işlenmesi kapsamında, bilginin doğruluğunu ve güncelliğini kontrol etmeli ve bilgi kirliliğine yol açmamalıdır.
2. Sosyal medya kullanımlarında şiddet veya cinsel içerikli ve benzeri rahatsız edici gönderilerden kaçınmalıdır.
3. Paylaşımlarında toplum yararını gözetmelidir.

İnsan haklarına saygı

Kamu görevlisi;

1. Bireylerin yaşamı, adı, şeref ve haysiyeti, özel veya aile yaşamı, mesleki ve ekonomik değerleri başta olmak üzere kişilik hakkına zarar verebilecek her türlü davranış ve paylaşımdan kaçınmalıdır.
2. Ayrımcılığa yol açabilecek her türlü nefreti besleyen, savunan ve benzeri hoşgörüsüz ifadelerde bulunmamalıdır.
3. Bireylerin kişisel verilerini, veri sahibinin izni olmaksızın, kullanmamalıdır.

Kurumsal sosyal medya hesabının kullanımı

Kamu görevlisi, kurumsal sosyal medya hesabını kullanırken;

1. Kurum adına yetkilendirilmiş olmalıdır.
2. Dil, ırk, etnik köken, renk, cinsiyet, siyasi düşünce, felsefi inanç, din, mezhep, servet, medeni hâl, sağlık durumu, engellilik, yaş, kılık ve kıyafet ve benzeri nedenlere dayalı olarak ayrımcılık yapmamalı ve kullanıcıları veya yorumlarını silmemeli ya da engellememelidir.
3. Şahsi menfaat, siyasi veya felsefi düşünce ve benzeri amaçla hareket etmemelidir.
4. Nezaket ve saygı kurallarına özen göstermelidir.
5. Kurumsal saygınlığa zarar verecek ifadelerde bulunmamalı, gizliliği ve güvenliği tehlikeye atacak bilgi ve belge paylaşmamalıdır.

Yöneticilerin Sorumluluğu

1. Yönetici kamu görevlisi, kurumsal sosyal medya hesabının etik ilkelere uygun olarak yönetilmesi amacıyla gerekli tedbirleri alır, denetim ve gözetim görevini özenle yürütür. Halkın bilgilendirilmesi amacıyla, kurumsal iş, işlem ve süreçlere ait bilgilerin kuruma ait sosyal medya hesaplarında paylaşılmasını sağlar.

EK 2: ERİŞİLEBİLİRLİK İLKESİNİN ANA ESASLARI

21/6/2025 tarihli ve 32933 sayılı Resmî Gazete’de yayımlanan 2025/10 sayılı “Web Siteleri ve Mobil Uygulamaların Erişilebilirliği” konulu Cumhurbaşkanlığı Genelgesi, kamu kurumlarının dijital erişilebilirlik alanındaki sorumluluğunu güçlendiren güncel düzenlemelerden biridir. Genelge ile web siteleri ve mobil uygulamaların erişilebilirliğine yönelik izleme ve değerlendirme süreçlerinin yürütülmesi öngörülmüş; Aile ve Sosyal Hizmetler Bakanlığı tarafından yayımlanan “Web Siteleri ve Mobil Uygulamaların Erişilebilirliği Kontrol Listesi - A Seviyesi”nin WCAG 2.2 ilkeleri esas alınarak hazırlandığı belirtilmiştir. Sosyal medya platformları teknik olarak kurumların tamamen kontrolünde olmayan alanlar olsa da kamu kurumları tarafından üretilen içeriklerin erişilebilir biçimde hazırlanması, bu genel yaklaşımın sosyal medya iletişimine yansıtılması bakımından önemlidir.

Bu kapsamda kurumsal sosyal medya hesaplarında yayımlanan tüm içeriklerde Web Content Accessibility Guidelines (WCAG) 2.2’de yer alan temel ilkeler dikkate alınmalıdır. WCAG yaklaşımına göre dijital içeriklerin algılanabilir, çalıştırılabilir, anlaşılabilir ve sağlam olması beklenmektedir. Sosyal medya içerikleri bakımından bu ilkeler; görsellerin alternatif metinle desteklenmesi, videolara doğru ve senkronize alt yazı eklenmesi, gerekli durumlarda sesli betimleme veya açıklayıcı metin sunulması, yeterli renk kontrastının sağlanması, bilginin yalnızca renk veya görsel unsur üzerinden aktarılmaması, sade ve açık dil kullanılması ve içeriklerin yardımcı teknolojilerle uyumlu olacak şekilde hazırlanması anlamına gelmektedir.

Görsel içeriklerde, paylaşımın ana mesajını oluşturan bilgi yalnızca görselin içine yerleştirilen metinle sınırlı bırakılmamalıdır. Afiş, duyuru görseli, grafik, tablo, harita, infografik ve benzeri içeriklerde yer alan temel bilgiler gönderi metninde de açık biçimde paylaşılmalıdır. Platformun imkân tanıdığı durumlarda görseller için alternatif metin alanı kullanılmalı; alternatif metin, görselin yalnızca fiziksel görünümünü değil, kamuoyu açısından taşıdığı anlamı ve ilettiği bilgiyi de yansıtmalıdır. Dekoratif nitelikteki görseller ile bilgi taşıyan görseller birbirinden ayrılmalı; bilgi taşıyan görseller mutlaka açıklayıcı metinle desteklenmelidir.

Video içeriklerinde altyazı kullanımı erişilebilirliğin temel unsurlarından biridir. Kamu kurumları tarafından yayımlanan video, kısa video, hikâye, reels, canlı yayın kaydı, tanıtım filmi, bilgilendirme videosu ve kamu spotu niteliğindeki içeriklerde konuşmalar doğru, eksiksiz ve eş zamanlı alt yazılarla desteklenmelidir. Alt yazılarda yalnızca konuşma metni değil, içeriğin anlaşılması için gerekli olan önemli sesler de uygun şekilde belirtilmelidir. Örneğin alkış, siren, uyarı sesi, kapı çalma sesi veya müzik gibi anlam taşıyan ses unsurları gerekli durumlarda alt yazıda gösterilmelidir. Otomatik alt yazı kullanıldığı takdirde, yayımdan önce dil bilgisi, anlam, kişi adları, kurum adları ve teknik terimler bakımından kontrol yapılmalıdır.

Görsel unsurların içeriğin anlaşılması bakımından belirleyici olduğu videolarda sesli betimleme veya açıklayıcı metin kullanılmalıdır. Özellikle grafik, tablo, sunum slaytı, harita, istatistik, ekran görüntüsü veya yalnızca görsel olarak aktarılan kritik bilgilerin yer aldığı videolarda, bu bilgilerin sesli anlatımda veya gönderi açıklamasında karşılığı bulunmalıdır. Görme engelli kullanıcıların yalnızca ses üzerinden içeriği takip edebileceği dikkate alınarak “burada görüldüğü gibi”, “şu grafikte yer aldığı üzere” gibi ifadeler tek başına kullanılmamalı; görselde aktarılan veri ve mesaj sözlü veya yazılı olarak açıklanmalıdır. Canlı yayınlar, basın açıklamaları, kriz iletişimi paylaşımları, afet ve acil durum bilgilendirmeleri ile vatandaşları doğrudan ilgilendiren duyurularda erişilebilirlik özellikle gözetilmelidir.

Canlı yayınlarda mümkün olan durumlarda canlı alt yazı, işaret dili tercümesi veya yayın sonrasında alt yazılı kayıt paylaşımı sağlanmalıdır. Afet, güvenlik, sağlık, ulaşım, kamu hizmetlerine başvuru, hak sahipliği, yardım ve destek süreçleri gibi konularda yapılan paylaşımlar; farklı engel gruplarının, yaşlı bireylerin ve dijital okuryazarlık düzeyi farklı kullanıcıların ihtiyaçları dikkate alınarak sade, açık ve erişilebilir biçimde hazırlanmalıdır.

Renk kullanımı erişilebilir sosyal medya tasarımının önemli unsurlarından biridir. Paylaşımlarda bilgi yalnızca renk üzerinden verilmemelidir. Örneğin “kırmızı alanlar riskli bölgeleri göstermektedir” ifadesi, renkleri ayırt etmekte zorlanan kullanıcılar için yeterli olmayabilir. Bu tür durumlarda renk kullanımına ek olarak açıklayıcı metin, desen, simge, etiket veya doğrudan yazılı bilgi kullanılmalıdır. Metin ve arka plan arasında yeterli kontrastlık bulunmalı; düşük kontrastlı renk

kombinasyonlarından, çok küçük puntolu yazılardan ve yoğun arka plan üzerine yerleştirilen okunması güç metinlerden kaçınılmalıdır.

Hareketli, yanıp sönen veya hızlı geçişlere sahip içeriklerde kullanıcı güvenliği dikkate alınmalıdır. Özellikle kısa süre içinde tekrar eden parlama, yoğun ışık geçişi, hızlı animasyon ve yüksek kontrastlı yanıp sönme efektleri bazı kullanıcılar açısından sağlık riski oluşturabilir. Bu nedenle sosyal medya içeriklerinde saniyede üçten fazla yanıp sönen efektlerden kaçınılmalı; hareketli içerikler gerektiğinde durdurulabilir, anlaşılabilir ve takip edilebilir şekilde tasarlanmalıdır. Kritik bilgiler çok kısa süre ekranda bırakılmamalı; kullanıcıya bilgiyi okuyabilecek ve anlayabilecek yeterli süre tanınmalıdır.

Metin içeriklerinde sade, açık ve doğrudan bir dil tercih edilmelidir. Kamu kurumları tarafından yapılan paylaşımlarda uzun, karmaşık ve çok katmanlı cümleler yerine vatandaşın kolaylıkla anlayabileceği ifadeler kullanılmalıdır. Başvuru, duyuru, tarih, saat, yer, belge, bağlantı ve iletişim bilgileri açıkça belirtilmelidir. “Detaylar linkte”, “başvuru için tıklayınız” gibi belirsiz ifadeler yerine bağlantının amacı ve yönlendirdiği hizmet mümkün olduğunca açıklanmalıdır. Hashtag kullanımında ekran okuyucuların doğru okuyabilmesi için kelime başlarında büyük harf kullanımı tercih edilmeli ve uzun, birleşik, anlaşılması güç etiketlerden kaçınılmalıdır.

Emoji ve sembol kullanımı ölçülü olmalıdır. Emojiler, ekran okuyucular tarafından sesli olarak okunabildiğinden, arka arkaya çok sayıda emoji kullanımı içeriğin anlaşılmasını zorlaştırabilir. Resmî duyurularda emoji ve semboller ana bilgi taşıyıcısı olarak kullanılmamalı; yalnızca destekleyici unsur olarak tercih edilmelidir. Benzer şekilde, yalnızca simgeye dayalı yönlendirmelerden kaçınılmalı; simgelerin yanında açıklayıcı metin de yer almalıdır.

PDF, afiş, broşür, duyuru görseli veya haricî bağlantı içeren paylaşımlarda, bağlantı verilen içeriğin de erişilebilir olması gözetilmelidir. Sosyal medya gönderisinde erişilebilirlik sağlansa dahi, kullanıcıyı yönlendiren PDF veya web sayfası erişilebilir değilse bilgiye erişim bütünlüğü zedelenir. Bu nedenle kamu kurumları, sosyal medya üzerinden paylaşılan bağlantıların güncel, çalışır, anlaşılır ve mümkün olduğunca erişilebilir belge veya sayfalara yönlendirdiğinden emin olmalıdır.

Kurumsal sosyal medya yönetiminde erişilebilirlik süreklilik arz eden bir kalite standardı olarak ele alınmalıdır. İçerik üretiminden sorumlu ekipler, paylaşım öncesinde erişilebilirlik kontrolü yapmalı; görsel, video, metin ve bağlantıların farklı kullanıcı ihtiyaçlarına uygunluğunu değerlendirmelidir. Bu amaçla kurum içinde kısa bir “erişilebilirlik sosyal medya içerik kontrol listesi” oluşturulmalı ve tüm paylaşımlar yayımlanmadan önce bu listeye göre gözden geçirilmelidir.

Paylaşım öncesinde şu sorular dikkate alınmalıdır:

1. Görsel içerik için alternatif metin veya açıklayıcı gönderi metni hazırlandı mı?
2. Video içerikte doğru ve senkronize alt yazı bulunuyor mu?
3. Alt yazılar konuşmaları, konuşmacı değişimlerini ve önemli sesleri içeriyor mu?
4. Görsel olarak aktarılan kritik bilgiler sesli anlatımda veya açıklama metninde yer alıyor mu?
5. İçerikte bilgi yalnızca renk, şekil veya konum üzerinden mi veriliyor?
6. Metin ve arka plan arasında yeterli kontrast bulunuyor mu?
7. Görselin içine yerleştirilen önemli bilgiler gönderi açıklamasında da tekrar ediliyor mu?
8. İçerikte hızlı yanıp sönen, çakan veya kullanıcı sağlığını riske atabilecek efektler bulunuyor mu?
9. Bağlantı, başvuru ve yönlendirme ifadeleri açık ve anlaşılır mı?
10. Hashtag, emoji ve semboller erişilebilirliği zorlaştırmayacak şekilde kullanıldı mı?
11. Paylaşılan PDF, afiş veya harici bağlantı erişilebilirlik açısından kontrol edildi mi?
12. Kriz, afet veya acil durum içerikleri işitme ve görme engelli kullanıcıların ihtiyaçları dikkate alınarak hazırlandı mı?

Sosyal Medya İçeriklerinde Erişilebilirlik Standartları

Kamu kurumları için paylaşım öncesi temel kontrol alanları

1



GÖRSELLER İÇİN AÇIKLAYICI METİN

Fotoğraf, afiş, grafik ve infografikler için açıklayıcı metin ekleyin. Böylece ekran okuyucu kullanan bireyler içeriği anlayabilir.

2



VIDEO İÇERİKLERDE ALTYAZI

Konuşma içeren tüm videolarda altyazı kullanın. Gerekli durumlarda [alkış], [müzik], [uyari sesi] gibi önemli sesleri de belirtin.

3



ÖNEMLİ BİLGİLERİ YALNIZCA GÖRSELDE BIRAKMAYIN

Tarih, saat, yer, başvuru ve iletişim bilgilerini paylaşım metninde de açıkça yazın.

4



RENK KULLANIMINI METİNLE DESTEKLEYİN

Bilgiyi yalnızca renkle vermeyin. Gerekirse 'Açık', 'Kapalı', 'Beklemede' gibi ifadeler kullanın.

5



OKUNABİLİR TASARIM KULLANIN

Büyük punto, sade yerleşim, yüksek kontrast ve mobil ekranda okunabilir yapı tercih edin.

6



YANIP SÖNEN EFEKTLERDEN KAÇININ

Hızlı parlayan veya dikkat dağıtan hareketli unsurlar kullanmayın. İçerik güvenli ve rahat algılanabilir olmalıdır.



PAYLAŞIM ÖNCESİ HIZLI KONTROL

- ✓ Görsel açıklaması var mı?
- ✓ Videoda altyazı var mı?
- ✓ Önemli bilgiler metinde de yer alıyor mu?
- ✓ Bilgi yalnızca renkle mi veriliyor?
- ✓ Yazılar mobil ekranda okunuyor mu?
- ✓ Yanıp sönen efektlerden kaçınıldı mı?



Bu görsel, sosyal medya paylaşımlarında erişilebilirliği güçlendirmek amacıyla hazırlanmış örnek bir infografik taslağıdır.

Notlar:

