Avrupa Birligi tarafindan finanse edilmektedir

POLİTİKA BELGESİ

Kadınların Dijital Güvenliği ve Mahremiyetinin Güçlendirilmesi

Koruyucu ve Önleyici Yaklaşımlar

WomBound

Erasmus+ KA154 Gençlik Katılımı Projesi

Eskişehir ASHM koordinatörlüğünde; Batman Akademik ve Sosyal Aktiviteler Derneği ve Ankara Üniversitesi ortaklığında

20 Eylül 2025 – 19 Eylül 2026 · Eskişehir · Batman · Ankara

Ankara final faaliyetinde gençler tarafından üretilen çıktılar temel alınarak hazırlanmıştır.

İÇİNDEKİLER

1. Yönetici Özeti 3
2. Bağlam ve Gerekçe 3
3. Proje Deneyimi ve Katılımcı Katkısı 3
4. Politika Amaçları ve İlkeleri 4
5. Dijital Dünyada Yaşanan Temel Zorluklar 4
6. Bireysel Düzeyde Koruyucu Önlemler 5
7. Dijital Sınır İhlali Anında Eylem Protokolü 6
8. Kurumsal Politika Önerileri 6
9. Uygulama Planı (Kısa – Orta – Uzun Vade) 9
10. İzleme ve Değerlendirme Gösterge Seti 9
11. Beklenen Etkiler 10
12. Sonuç ve Çağrı 10

1 YÖNETİCİ ÖZETİ

Dijital teknolojiler gündelik yaşamın merkezine yerleşirken, dijital alan kadınlar açısından aynı zamanda bir risk alanına dönüşmektedir. Israrlı dijital takip, izinsiz görüntü paylaşımı, şantaj, dijital taciz ve tehdit; kadınların yalnızca çevrim içi güvenliğini değil, psikolojik iyi oluşunu, sosyal görünürlüğünü ve kamusal katılımını da doğrudan etkilemektedir.

Bu politika belgesi, dijital güvenliği teknik bir tedbirler listesi olarak değil; kişisel sınırların tanınması, mahremiyetin korunması, öz-denetim ve psikolojik dayanıklılığın güçlendirilmesi boyutlarıyla bütüncül biçimde ele alır. Belge, WomBound projesinin Ankara'daki final faaliyetinde genç katılımcılar tarafından üretilen çıktılara dayanmakta; bireysel, kurumsal ve politika düzeyinde uygulanabilir öneriler sunmaktadır.

Belgenin üç temel katkısı bulunmaktadır: bireyin bir ihlal anında izleyebileceği beş adımlı eylem protokolü; on dört kurum ve kuruluş için ayrıştırılmış somut öneri seti; ve önerilerin hayata geçirilmesine yönelik kısa–orta–uzun vadeli uygulama planı ile izleme göstergeleri.

2 BAĞLAM VE GEREKÇE

Dijital ortamların hızlı ve yaygın kullanımı; bireyin kişisel sınırlarını, mahremiyetini, güvenliğini ve psikolojik iyi oluşunu tehdit edebilmektedir. Sosyal medya platformları gündelik hayatı kolaylaştırırken; kişisel bilgilerin kontrolsüz paylaşılması, kalıcı dijital ayak izi, siber zorbalık, dijital şiddet, ısrarlı takip ve manipülatif içerikler gibi sorunlara da zemin hazırlamaktadır.

Bu sorunlar kadınlar açısından niteliksel olarak farklılaşmakta ve ağırlaşmaktadır. Israrlı dijital takip, izinsiz görüntü paylaşımı, şantaj ve cinsiyetçi taciz yalnızca tekil olaylar değildir; çoğu zaman fiziksel şiddetin dijital uzantısı ya da öncülü olarak işlev görür. Sonuçları da yalnızca bireysel değildir: itibar kaybı, sosyal dışlanma ve kadının dijital alandan tümüyle çekilmesi, kadınların kamusal görünürlüğünü ve ifade özgürlüğünü daraltan toplumsal bir mesele hâline gelir.

Bu nedenle dijital güvenlik yalnızca teknik bir mesele değildir. Kişisel sınırların farkına varılması, mahremiyetin korunması, öz-denetim ve psikolojik dayanıklılık boyutlarıyla birlikte; hak temelli, koruyucu ve önleyici bir politika alanı olarak ele alınmalıdır.

Bu belge, WomBound projesinin Ankara'daki final faaliyetinde gençlerin ürettiği çıktılar temel alınarak; kadınların dijital güvenliğini ve mahremiyetini güçlendirmeye yönelik bireysel, toplumsal ve kurumsal düzeyde alınabilecek önlemleri ortaya koymayı amaçlamaktadır.

3 PROJE DENEYİMİ VE KATILIMCI KATKISI

WomBound, Erasmus+ KA154 Gençlik Katılımı Projesi kapsamında yürütülmüştür. Proje; Eskişehir ASHM koordinatörlüğünde, Batman Akademik ve Sosyal Aktiviteler Derneği ve Ankara Üniversitesi ortaklığında, 20 Eylül 2025 – 19 Eylül 2026 tarihleri arasında Eskişehir, Batman ve Ankara'da uygulanmıştır.

3 İL	12 AY	3 KURUM
Eskişehir · Batman · Ankara	20.09.2025 – 19.09.2026	Koordinatör ve ortaklar

Erasmus+ Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Ancak burada yer alan görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.

Proje, yaygın öğrenme ilkeleri temelinde atölye tabanlı, etkileşimli ve uygulamalı bir yaklaşımla yürütülmüş; genç katılımcılar dijital mahremiyet, kişisel sınırlar ve dijital şiddetle mücadele başlıklarında hem eğitim almış hem de içerik üretmiştir.

Bu belgenin ayırt edici yönü, önerilerin kaynağıdır: aşağıdaki başlıklar uzman görüşünden önce genç katılımcıların kendi deneyimlerinden, önceliklerinden ve final faaliyetinde yürüttükleri grup çalışmalarından türetilmiştir. Bu yönüyle metin, gençlik katılımı ilkesinin somut bir çıktısıdır.

4 POLİTİKA AMAÇLARI VE İLKELERİ

Bu belge aşağıdaki politika amaçlarını desteklemektedir:

- Kadınların dijital alanda kişisel sınırlarını tanıma, koruma ve ihlal karşısında harekete geçme kapasitesini güçlendirmek.
- Dijital mahremiyeti teknik bir tedbir meselesi olmaktan çıkarıp hak temelli, koruyucu ve önleyici bir politika alanı olarak tanımlamak.
- Dijital şiddete maruz kalan kadınların psikolojik, hukuki ve sosyal desteğe gecikmeden ve tek noktadan erişimini sağlamak.
- Eğitim, sosyal hizmet, kolluk, sağlık ve adalet kurumlarının dijital şiddeti tanıma, doğru yönlendirme ve ikincil örselenmeyi önleme kapasitesini artırmak.
- Genç kadınların politika geliştirme süreçlerine katılımını süreklileştirmek ve akran eğitimiyle etkinin yayılmasını sağlamak.

İLKELER

- Hak temelli ve kadın odaklı yaklaşım
- Mağduru suçlamayan dil
- Kadınların ve gençlerin doğrudan katılımı
- Kapsayıcılık ve eşit erişim
- Gizlilik, rıza ve veri minimizasyonu
- Kurumlar arası koordinasyon ve hesap verebilirlik

5 DİJİTAL DÜNYADA YAŞANAN TEMEL ZORLUKLAR

Final faaliyetinde genç katılımcılar tarafından öne çıkarılan başlıca zorluk alanları aşağıda tanımlanmıştır.

- **Siber zorbalık ve çevrim içi taciz.** Hakaret, tehdit, ısrarlı mesajlar ve rahatsız edici içeriklerle karşılaşma biçiminde ortaya çıkar. Kadınlar açısından çoğu zaman cinsiyetçi söylem ve cinsel içerikli tacizle iç içe geçer; süreklilik kazandığında mağdurun dijital alandan tümüyle çekilmesine yol açabilir.
- **Dijital mahremiyet ihlalleri.** Fotoğraf, video veya kişisel bilgilerin kişinin izni olmadan paylaşılmasıdır. İzinsiz görüntü paylaşımı ve intikam amaçlı içerik, kadınlar için en ağır sonuçları doğuran ihlallerdendir; itibar kaybı, sosyal dışlanma ve ciddi psikolojik travmayla sonuçlanabilir.

Erasmus+ Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Ancak burada yer alan görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.

- **Israrlı dijital takip ve dijital şiddet.** Konum takibi, hesap izleme, sahte profillerle gözetleme ve sürekli iletişim kurma yoluyla kişinin özerk alanının ihlalidir. Çoğu zaman fiziksel şiddetin veya ısrarlı takibin dijital uzantısıdır ve mağdurda sürekli gözetlenme kaygısı yaratır.
- **Sosyal medya bağımlılığı ve dijital baskı.** Aşırı ve kontrolsüz kullanım; uyku düzenini, akademik ve mesleki performansı ve gerçek yaşam ilişkilerini olumsuz etkiler. Sürekli çevrim içi olma baskısı, karşılaştırma ve onay arayışı kaygı ile öz-değer sorunlarını besleyebilir.
- **Yanlış ve sahte bilgilerin yayılması.** Dezenformasyon ve manipülatif içerikler doğru karar almayı zorlaştırır. Kadınları hedef alan itibar suikastı ve dijital linç kampanyaları bu zeminde hızla büyüyebilir; yapay zekâ ile üretilen sahte görüntüler bu riski daha da derinleştirmektedir.
- **Dijital eşitsizlik ve erişim sorunları.** Cihaza, internete veya dijital okuryazarlığa eşit erişimin olmaması bazı grupları dezavantajlı kılar. Kadınlar, özellikle kırsalda ve dijital okuryazarlığı düşük kesimlerde, hem erişimde hem de kendini koruma becerilerinde geride kalabilmektedir.
- **İnsan ilişkilerinin ve sosyal destek ağlarının zayıflaması.** Yüz yüze iletişimin yerini ekran temelli etkileşimin alması, sosyal destek ağlarını zayıflatır. Destek ağının zayıflaması, dijital şiddet yaşayan bir kadının yalnızlaşmasını ve yardım aramasını güçleştirir.

6 BİREYSEL DÜZEYDE KORUYUCU ÖNLEMLER

Önemli ilke: Aşağıdaki öneriler bireyin kendi güvenlik alanını genişletmeye yöneliktir. Ancak bireysel tedbirler yalnızca koruyucudur; bir ihlalin sorumluluğu hiçbir koşulda mağdura ait değildir. Önlem almamış olmak, yaşanan şiddeti açıklamaz ve meşrulaştırmaz.

- **Güçlü ve hesaba özel şifreler kullanılmalı.** Tahmin edilmesi zor, her hesap için farklı şifreler tercih edilmeli ve mümkün olan her yerde iki aşamalı doğrulama etkinleştirilmelidir. Bu, hesap ele geçirme ve kimlik taklidi risklerini doğrudan azaltır.
- **Kişisel bilgiler herkese açık paylaşılmamalı.** Adres, konum, iş yeri, okul, telefon ve kimlik bilgileri gibi veriler açık hesaplarda paylaşılmamalıdır. Tekil olarak zararsız görünen bilgiler bir araya geldiğinde kişinin fiziksel olarak bulunmasını mümkün kılabilir.
- **Güvenilir olmayan bağlantılara tıklanmamalı.** Tanınmayan kaynaklardan gelen bağlantı ve dosyalar oltalama ve zararlı yazılım taşıyabilir. Şüpheli mesajlardaki bağlantılar açılmadan önce kaynağı doğrulanmalıdır.
- **Gizlilik ayarları düzenli olarak gözden geçirilmeli.** Hesapların kimler tarafından görülebildiği, konum paylaşımının açık olup olmadığı ve bağlı üçüncü taraf uygulamalar belirli aralıklarla kontrol edilmelidir. Platform güncellemeleri ayarları değiştirebildiği için bu kontrol süreklilik gerektirir.
- **Bilginin doğruluğu paylaşmadan önce teyit edilmeli.** Bilgi, resmî ve güvenilir kaynaklardan doğrulanmalıdır. Bu, hem dezenformasyonun yayılmasını hem de kişinin manipülasyona açık hâle gelmesini önler.
- **Rahatsız edici hesaplar engellenmeli, içerikler raporlanmalı.** Engelleme ve platforma raporlama ilk adımdır; tehdit, şantaj ve tacizin sürmesi hâlinde kolluğa başvurulmalıdır. Sessiz kalmak değil, kayıt altına alıp bildirmek esastır.
- **Kullanım süresi bilinçli biçimde sınırlanmalı.** Cihazların sunduğu ekran süresi araçları, bildirim yönetimi ve çevrim dışı zaman aralıkları hem bağımlılık riskini azaltır hem de gerçek yaşam dengesini korur.
- **Çevrim dışı sosyal bağlar güçlü tutulmalı.** Yüz yüze ilişkiler ve etkinlikler psikolojik dayanıklılığı besler. Güçlü bir destek ağı, dijital bir sorun yaşandığında kişinin yalnız kalmamasını ve daha hızlı destek almasını sağlar.

Erasmus+ Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Ancak burada yer alan görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.

7 DİJİTAL SINIR İHLALİ ANINDA EYLEM PROTOKOLÜ

Bir sınır ihlali veya dijital şiddet durumunda kişinin ne yapacağını bilmesi, farkındalık kadar önemlidir. Aşağıdaki beş adımlı protokol, hem güvenliği hem de psikolojik bütünlüğü koruyacak biçimde tasarlanmıştır; kurumlar tarafından afiş, kart veya el broşürü olarak da kullanılabilir.

1 — Fark Et

Yaşanan durumun bir sınır ihlali olup olmadığı ve risk taşıyıp taşımadığı değerlendirilmelidir. Rahatsızlık, korku ve tehdit hissi normalleştirilmemeli; sorumluluğun kendisinde olmadığı bilinmelidir.

2 — Güvenliğini Sağla

Şifreler değiştirilmeli, iki aşamalı doğrulama devreye alınmalı, konum paylaşımı ve gizlilik ayarları kontrol edilmelidir. İlk hedef, failin dijital erişim kanallarını kapatmaktır.

3 — Kanıtları Koru

Mesajlar, ekran görüntüleri, hesap adresleri ile tarih ve saat bilgisi saklanmalıdır. Kanıtlar, ileride yapılacak hukuki başvuruların temelini oluşturur; içerik silinmeden önce kayıt altına alınmalıdır.

4 — Sınır Koy

Kişi kendini açıklamak ya da her an ulaşılabilir olmak zorunda değildir. Engelleme, iletişimi kesme ve raporlama; bir hak ihlaline verilen meşru yanıtlardır.

5 — Destek Al

Psikolojik, hukuki ve güvenlik alanlarında uygun destek mekanizmalarına başvurulmalıdır (ALO 183, ŞÖNİM, kolluk, baro adli yardım, üniversite danışma birimleri). Hiç kimse bu süreçle yalnız başa çıkmak zorunda değildir.

8 KURUMSAL POLİTİKA ÖNERİLERİ

Aşağıda, kadınların dijital güvenliğini ve mahremiyetini güçlendirmeye yönelik olarak ilgili kurum ve kuruluşlara sunulabilecek öneriler yer almaktadır. Öneriler, kurumların işlev alanlarına göre beş başlıkta gruplandırılmıştır.

8.1 Eğitim, Önleme ve Farkındalık

◆ Millî Eğitim Bakanlığı

- **Okullarda seminer programı:** "Dijital Mahremiyet, Dijital Şiddet ve Ruh Sağlığı" konulu, sınıf düzeyine göre uyarlanmış düzenli seminerler yürütülmeli; içerik yaş grubuna uygun senaryo ve örnek vakalarla desteklenmelidir.
- **Rehber öğretmen ve psikolojik danışmanlara eğitim:** Okul PDR kadrosu, dijital şiddet belirtilerini tanıma ve öğrenciyi doğru birime yönlendirme konusunda eğitilmeli; böylece okul, erken müdahalenin ilk halkası hâline gelmelidir.
- **Öğrencilere beceri eğitimi:** Kişisel sınır koyma, dijital öz-denetim ve güvenli sosyal medya kullanımı kazandırılmalı; kız öğrencilerin sık karşılaştığı taciz ve mahremiyet ihlallerine özel modüller eklenmelidir.
- **Dijital Risk Değerlendirme Formu:** Dijital şiddet risklerini erken fark etmek için standart bir değerlendirme formu kullanılmalı; risk tespit edilen öğrenciler ilgili birimlere yönlendirilmelidir.

Erasmus+ Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Ancak burada yer alan görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.

◆ Gençlik ve Spor Bakanlığı

- **"Dijital Güçlü Kadın" atölyeleri:** Gençlik merkezlerinde genç kadınlara yönelik, uygulamalı ve süreklilik taşıyan atölye programları düzenlenmelidir.
- **Beceri temelli eğitim:** Dijital öz-denetim, mahremiyet, güvenlik ve sınır koyma becerileri teorik anlatım yerine senaryo ve rol oynama yoluyla kazandırılmalıdır.
- **Akran eğitmen ağı:** Eğitim alan genç kadınların akran eğitmen olarak sertifikalandırılması ve yerel düzeyde sürekli yayılım sağlaması desteklenmelidir.

◆ Üniversiteler

- **Disiplinler arası araştırma:** Psikoloji, PDR, hukuk, sosyoloji, iletişim ve bilişim alanlarının iş birliğiyle kadına yönelik dijital şiddet üzerine araştırmalar yürütülmelidir.
- **"Kadın ve Dijital Mahremiyet Raporu":** Politika ve uygulamaların etkisini ölçmek amacıyla periyodik akademik değerlendirme raporları hazırlanmalıdır.
- **Kampüs içi destek ve müfredat:** Kadın çalışmaları merkezleri ve öğrenci danışma birimleri aracılığıyla dijital güvenlik desteği verilmeli; ilgili modüller seçmeli derslere entegre edilmelidir.

8.2 Sosyal Destek, Koruma ve Sağlık

◆ Aile ve Sosyal Hizmetler Bakanlığı

- **Kadın danışma merkezlerinde ücretsiz eğitim:** Kadınlara yönelik ücretsiz dijital güvenlik ve farkındalık eğitimleri düzenli sunulmalı; dijital okuryazarlığı düşük kadınları da kapsayacak biçimde sadeleştirilmelidir.
- **Psikolojik destek hizmetleri:** Dijital şiddete bağlı kaygı, stres ve travma yaşayan kadınlara ücretsiz psikolojik destek sağlanmalı, gerektiğinde uzman danışmanlığa yönlendirilmelidir.
- **Dijital Mahremiyet Güvenlik Kılavuzu:** Sade dille hazırlanmış bir kılavuzla mahremiyeti koruma, kanıt saklama ve başvuru yolları adım adım anlatılmalıdır.
- **Yönlendirme mekanizmalarının güçlendirilmesi:** Dijital şiddete maruz kalan kadınlara psikolojik, sosyal ve hukuki yönlendirme tek elden ve gecikmesiz işletilmelidir.

◆ ŞÖNİM'ler (Şiddet Önleme ve İzleme Merkezleri)

- **Dijital güvenlik kontrol listesi:** Başvuru alınırken standart bir dijital güvenlik kontrol listesi uygulanmalı; kadının hesap, cihaz ve konum güvenliği hızlıca değerlendirilmelidir.
- **Kişiye özel Dijital Güvenlik Eylem Planı:** Risk altındaki her kadın için bireysel bir eylem planı hazırlanmalı; plan, failin dijital erişim kanallarını kapatmayı önceliklendirmelidir.
- **Risk değerlendirmesi:** Şifre ve konum paylaşımı, hesap ele geçirme, özel görüntü ve dijital takip riskleri sistematik biçimde değerlendirilmelidir.
- **Çok disiplinli yönlendirme:** Gerekli durumlarda kadın; psikolog, sosyal hizmet uzmanı, hukukçu ve kolluk birimlerine koordineli biçimde yönlendirilmelidir.

◆ Sağlık Bakanlığı

- **Sağlık çalışanlarına eğitim:** Sağlık personeli, dijital şiddetin psikolojik etkilerini (kaygı, uyku sorunu, travma belirtileri) tanıma ve doğru birime yönlendirme konusunda eğitilmelidir.
- **Değerlendirmede farkındalık:** Kadınlarda dijital şiddete bağlı kaygı, stres ve travma konusunda kurum içi farkındalık artırılmalı; başvuran kadınların dijital şiddet öyküsü de değerlendirilmelidir.

◆ ALO 183 ve 112

- **Hızlı ve standart yönlendirme:** Dijital şiddet vakaları hızlı ve standart biçimde ilgili kurumlara yönlendirilmeli; çağrıyı alan personel dijital şiddeti tanıyacak şekilde bilgilendirilmelidir.

Erasmus+ Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Ancak burada yer alan görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.

- **İlk anda kanıt uyarısı:** Çağrı sırasında kişiye, içerik silinmeden önce kanıtların nasıl korunacağına dair kısa ve net bir yönlendirme yapılmalıdır.

8.3 Adli Süreçler ve Hukuki Erişim

◆ Emniyet Genel Müdürlüğü / Siber Suçlarla Mücadele

- **Personele "ilk yaklaşım" eğitimi:** Kolluk personeline dijital şiddet mağduruna ilk yaklaşım eğitimi verilmeli; ikincil örselenmeyi önleyecek, mağduru suçlamayan bir dil benimsenmelidir.
- **Standart başvuru prosedürü:** Dijital taciz, tehdit, şantaj, izinsiz görüntü paylaşımı ve dijital takip başvuruları için standart ve öngörülebilir bir prosedür oluşturulmalıdır.
- **"Dijital şiddette ilk 24 saat" kılavuzu:** Mağdura, ilk saatlerde ne yapması gerektiğini (kanıt koruma, hesap güvenliği, başvuru) anlatan pratik bir kılavuz verilmelidir.
- **Delil ve başvuru bilgilendirmesi:** Dijital delillerin korunması ve güvenli başvuru yolları konusunda mağdur açıkça ve yazılı olarak bilgilendirilmelidir.

◆ Adalet Bakanlığı

- **Sade başvuru rehberi:** Kadınların dijital mahremiyet ve dijital şiddet karşısındaki hakları sade dille açıklanmalı; nereye ve nasıl başvuracağı adım adım gösterilmelidir.
- **Adli yönlendirme:** Dijital şiddet vakalarında mağdurlar adli ve hukuki mekanizmalara doğru biçimde yönlendirilmelidir.
- **Hukukçulara farkındalık eğitimi:** Hâkim, savcı ve avukatlara dijital şiddet ve mahremiyet ihlalleri konusunda güncel farkındalık eğitimleri düzenlenmelidir.

◆ Barolar

- **Ücretsiz hukuki bilgilendirme:** Kadınlara yönelik ücretsiz "Dijital Mahremiyet ve Hukuki Haklar" bilgilendirme çalışmaları yapılmalıdır.
- **Hukuki erişimin kolaylaştırılması:** Dijital şiddet mağdurlarının adli yardım ve hukuki destek mekanizmalarına erişimi kolaylaştırılmalı; başvuru süreci sadeleştirilmelidir.

8.4 Kişisel Veri Güvenliği ve Dijital Düzenleme

◆ Kişisel Verileri Koruma Kurumu (KVKK)

- **Farkındalık programı:** Kadınlara yönelik "kişisel verilerimi ve dijital mahremiyetimi koruyorum" temalı, uygulamalı bir farkındalık programı hazırlanmalıdır.
- **Pratik koruma rehberi:** Konum, fotoğraf, adres, telefon, kimlik ve biyometrik verilerin korunmasına yönelik somut adımlar içeren bir rehber sunulmalıdır.
- **Yeni teknolojilere yönelik bilgilendirme:** Sosyal medya ve yapay zekâ uygulamalarında kişisel veri güvenliği konusunda düzenli bilgilendirme yapılmalıdır.

◆ Bilgi Teknolojileri ve İletişim Kurumu (BTK)

- **Hızlandırılmış içerik süreci:** İzinsiz görüntü paylaşımı ve şantaj içerikli başvurular için öncelikli ve hızlandırılmış bir değerlendirme akışı tanımlanmalıdır.
- **Platformlarla iş birliği:** Sosyal medya platformlarının Türkiye temsilcileriyle, kadına yönelik dijital şiddet başvurularında standart yanıt süresi ve geri bildirim yükümlülüğü belirlenmelidir.
- **Şeffaflık raporlaması:** Kadına yönelik dijital şiddet kaynaklı başvuru, kaldırma ve sonuçlandırma verileri düzenli olarak kamuoyuyla paylaşılmalıdır.

8.5 Yerel Uygulama ve Kurumlar Arası Koordinasyon

Erasmus+ Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Ancak burada yer alan görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.

Belediyeler

- **Yerel ücretsiz eğitim:** Kadın danışma merkezlerinde ücretsiz dijital güvenlik ve farkındalık eğitimleri sunulmalıdır.
- **Yerel koordinasyon:** Risk altındaki kadınlara yönelik kurumlar arası koordinasyon yerel düzeyde sağlanmalı ve düzenli izlenmelidir.
- **Kamusal görünürlük:** Bilgilendirme materyalleri kadın danışma merkezleri, kültür merkezleri ve toplu taşıma gibi kadınların yoğun kullandığı alanlarda erişilebilir kılınmalıdır.

Kurumlar Arası Koordinasyon

- **Ortak yönlendirme mekanizması:** ASHB, EGM, BTK, KVKK, MEB, Sağlık Bakanlığı, Adalet Bakanlığı ve yerel yönetimler arasında ortak bir yönlendirme mekanizması kurulmalıdır.
- **Tekil başvuru sistemi:** Kadının farklı kurumlarda aynı öyküyü tekrar tekrar anlatmasını önleyecek, tek noktadan yönlendirme sistemi geliştirilmelidir.
- **Ortak Dijital Şiddet Kılavuzu:** Tüm kurumlarda kullanılmak üzere ortak, standart bir dijital şiddet kılavuzu hazırlanmalı ve düzenli güncellenmelidir.

9 UYGULAMA PLANI

Önerilerin hayata geçirilmesi için önerilen aşamalı yol haritası aşağıda sunulmuştur.

KISA VADE · 0–6 AY	ORTA VADE · 6–18 AY	UZUN VADE · 18 AY+
◆ Belgenin ilgili bakanlıklara, ŞÖNİM'lere, barolara ve yerel yönetimlere resmî olarak sunulması. ◆ Eylem protokolünün sade dille afiş, kart ve dijital görsel formatına dönüştürülmesi. ◆ Proje ortakları önderliğinde bir izleme ve savunuculuk çalışma grubunun kurulması.	◆ En az üç ilde okul, gençlik merkezi ve kadın danışma merkezi iş birliğiyle pilot eğitimlerin yürütülmesi. ◆ Dijital güvenlik kontrol listesinin ŞÖNİM ve kolluk birimlerinde test edilip revize edilmesi. ◆ Eğitici eğitimi paketinin hazırlanması ve açık erişimle paylaşılması.	◆ Dijital güvenlik ve mahremiyet modüllerinin MEB ve YÖK düzeyinde kalıcı entegrasyonu. ◆ Kurumlar arası tek noktadan yönlendirme sisteminin kurulması. ◆ "Kadın ve Dijital Mahremiyet Raporu"nun periyodik olarak yayımlanması.

10 İZLEME VE DEĞERLENDİRME GÖSTERGE SETİ

Politika önerilerinin etkisini ölçmek için aşağıdaki gösterge seti önerilmektedir:

- Erişim: eğitim ve atölyelere katılan kadın ve genç sayısı; belgenin ulaştığı kurum sayısı.
- Bilgi ve beceri: gizlilik ayarı yapma, iki aşamalı doğrulama kullanma ve kanıt saklamayı bilme oranlarında ön test–son test değişimi.
- Davranış: sınır koyma, engelleme/raporlama ve resmî başvuru yapma niyetindeki artış.
- Kurumsal kapasite: dijital güvenlik kontrol listesi uygulayan ŞÖNİM ve kolluk birimi sayısı; eğitim alan personel sayısı.
- Süreç kalitesi: başvurudan yönlendirmeye geçen ortalama süre ve mükerrer başvuru sayısındaki azalma.

Erasmus+ Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Ancak burada yer alan görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.

- Kapsayıcılık: kırsalda yaşayan, dijital okuryazarlığı düşük ve dezavantajlı gruplardaki kadınların katılım oranı.
- Politika etkisi: önerilerden kurumsal belge, genelge veya programa dönüşenlerin sayısı.

11 BEKLENEN ETKİLER

- Kadınların dijital alanda kendini koruma becerilerinin güçlenmesi ve dijital alandan çekilme eğiliminin azalması.
- İhlal anında ne yapılacağının bilinmesiyle kanıt kaybının azalması ve hukuki süreçlerin daha etkin işlemesi.
- Kurum personelinin mağduru suçlamayan bir dil benimsemesiyle ikincil örselenmenin azalması.
- Kurumlar arası koordinasyonun güçlenmesi ve kadının mükerrer başvuru yükünün hafiflemesi.
- Genç kadınların politika üretim süreçlerine katılım deneyimi kazanması ve akran eğitimiyle etkinin yaygınlaşması.
- Dijital mahremiyetin bireysel bir tedbir konusu olmaktan çıkıp kamusal bir sorumluluk alanı olarak tanınması.

12 SONUÇ VE ÇAĞRI

Kadınların dijital güvenliği, yalnızca bireylerin daha dikkatli davranmasıyla sağlanamaz. Farkındalık gereklidir; ancak tek başına yeterli değildir. Israrlı takip, siber zorbalık, tehdit, şantaj ve dijital taciz gibi durumlarda kişinin ne yapacağını bilmesi kadar, başvurduğunda karşısında hazırlıklı ve koordineli bir kurumsal yapı bulması da belirleyicidir.

Bu belge, gençlerin kendi deneyimlerinden hareketle; eğitim kurumları, sosyal hizmet birimleri, kolluk, sağlık, adalet ve yerel yönetimlerin birlikte uygulayabileceği, ölçülebilir ve kapsayıcı bir yol haritası sunmaktadır. Bu yaklaşımla, dijital sınır ihlali yaşayan bireyler için fiziksel ve psikolojik bütünlüğü koruyan, koruyucu ve önleyici bir politika alanı ortaya çıkacaktır.

12.1 Belge kimlere sunulabilir?

- **Merkezî kamu kurumları.** MEB, ASHB, Adalet, Sağlık ve Gençlik ve Spor bakanlıkları ile EGM, KVKK ve BTK'nın ilgili genel müdürlükleri ve strateji birimleri.
- **Yerel yönetimler ve ŞÖNİM'ler.** Kadın danışma merkezleri ve eşitlik birimleri aracılığıyla doğrudan uygulamaya aktarılması için.
- **Üniversiteler.** Kadın çalışmaları uygulama ve araştırma merkezleri, PDR ve iletişim bölümleri; müfredat ve araştırma entegrasyonu için.
- **Meslek örgütleri ve sivil toplum.** Barolar, tabip odaları ve kadın örgütleri; savunuculuk ve ücretsiz danışmanlık hizmetleri için.
- **Gençlik yapıları.** Gençlik merkezleri ve öğrenci toplulukları; akran eğitimi yoluyla yayılım için.
- **Medya ve dijital platform temsilcileri.** İçerik kaldırma, raporlama ve şikâyet süreçlerinin iyileştirilmesi için.

Özetle; amaç teknolojiyi yasaklamak değil, teknolojiyi kullanırken birbirimizin haklarına ve kişisel sınırlarına saygı duyulan, daha güvenli dijital ve kamusal alanlar yaratmaktır. Çünkü kişisel sınır bir lüks değil, **en temel haktır.**

Erasmus+ Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Ancak burada yer alan görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.

WomBound

ERASMUS+ KA154 GENÇLİK KATILIMI PROJESİ

Eskişehir ASHM · Batman Akademik ve Sosyal Aktiviteler Derneği · Ankara Üniversitesi

20 Eylül 2025 – 19 Eylül 2026 · Eskişehir · Batman · Ankara



Erasmus+ Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Ancak burada yer alan görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.