TEKNOLOJİ DESTEKLİ CİNSEL ŞİDDET KAVRAMLAR SÖZLÜĞÜ

Cinsel Şiddetle Mücadele Derneği

TEKNOLOJİ DESTEKLİ CİNSEL ŞİDDET

KAVRAMLAR SÖZLÜĞÜ

İçerik: CŞMD

Tasarım: Özge Özgüner

Temmuz 2026

www.cinselsiddetlemucadele.org

info@cinselsiddetlemucadele.org

Bu yayın, **İstanbul Almanya Başkonsolosluğu**nun desteği ile hazırlanmıştır.
Burada dile getirilen görüşler Konsolosluğun resmi görüşlerini yansıtmaz.
Burada verilen bilgi ve sunulan görüşlerin tüm sorumluluğu
Cinsel Şiddetle Mücadele Derneği'ne aittir.

Almanya Federal Cumhuriyeti
Başkonsolosluğu
Istanbul

Cinsel Şiddetle
Mücadele Derneği

İÇİNDEKİLER

Neden Yeni bir Kavramlar Sözlüğü 3
Kavram Tercihlerimiz Üzerine 4
Sözlüğü Okurken: Haklar, Sorumluluklar ve Güvenli Okuma 8

KAVRAMLAR:

1. Şiddetin Kapsamı ve Türleri

Teknoloji Destekli Cinsel/Cinselleştirilmiş Şiddet 12
Görüntüye Dayalı Cinsel Şiddet 13
Cinsel İçerikli Şantaj 14
Yapay Zekâ ile Üretilen Cinsel İçerikler (Sentetik Görüntüler) 15
Çevrim İçi Taciz 16
Onay Dışı Cinsel İçerik Gönderimi 17
Kişisel Bilgilerin Onay Dışı Paylaşılması 18
Dijital Israrlı Takip 19
Siber Zorbalık 20
Dijital / Çevrim İçi Flört Şiddeti 21
Romantik İlişki Dolandırıcılığı 22
Siber Grooming (Çevrim İçi Kandırma ve Cinsel İstismara Hazırlama) 23
Çocukların Cinsel İstismarına / Sömürüsüne İlişkin Materyaller 24
Dijital Kimliğe Bürünme ve Taklit Hesaplar 25

2. Şiddeti Besleyen Söylemler ve Yapısal Mekanizmalar

Dijital Mizenformasyon ve Dezenformasyon 28
Toplumsal Cinsiyete Dayalı Trolleme ve Nefret Söylemi 29
Dijital Linç 30
Dijital Gözetim, Baskı ve Sansür 31
Algoritmik Şiddet 32
Erkosfer / Manosphere 33
İncel İdeolojisi 34
Dijital Uçurum ve Dijital Dışlanma 35

3. Haklar, Kapasite ve Destek

Çevrim İçi Dayanıklılık 38
Dijital Okuryazarlık 39
Hayatta Kalan Odaklı Yaklaşım 40
Travma Bilgili Yaklaşım 41
Dijital Adalete ve Desteğe Erişim 42

4. Koruyucu ve Dönüştürücü Yaklaşımlar

Tasarım Aşamasında Güvenlik 44
Dijital Platformların Hesap Verebilirliği 45
Toplumsal Fayda için Teknoloji 46
Feminist Teknoloji ve Feminist İnternet 47

Yararlanılabilecek Kaynaklar 48

NEDEN
YENİ BİR **KAVRAMLAR SÖZLÜĞÜ**?

Cinsel şiddet, teknolojiyle birlikte yeni biçimler alıyor; gündelik hayatta kullandığımız internet, sosyal medya, mesajlaşma uygulamaları ve akıllı cihazlar şiddetin yeni yöntemlerle uygulanmasına aracılık edebiliyor. Bu şiddet biçimleri çoğu zaman görünmez kalıyor; yaşananlar utanç, suçlanma ve damgalanma korkusu ya da başvuru yollarının zorluğu nedeniyle dile getirilemeyebiliyor.

Şiddetin bu yeni biçimlerini anlamak, adlandırmak ve üzerine konuşabilmek için kavramları da yeniden düşünmeye ihtiyaç duyuyoruz. Bu sözlüğü, teknoloji destekli cinsel/cinselleştirilmiş şiddeti daha görünür kılmak ve onunla mücadele yollarını birlikte çoğaltmak için hazırladık.

Teknolojinin aracılık ettiği şiddet yalnızca kişileri değil, dijital alanlarda var olma ve kendimizi ifade etme özgürlüğümüzü topluluklar olarak da etkiliyor. Tıpkı kamusal alanlarda olduğu gibi, dijital alanlarda da var olmaya, haklarımızı aramaya ve dayanışmayı büyütmeye devam edeceğiz. Sokakları da, geceleri de, dijital meydanları da bırakmıyoruz!

Mağdur suçlayıcılık, hayatta kalan, fail gibi temel kavramlara yer verdiğimiz ilk kavramlar sözlüğümüze göz atmak isterseniz, **burada!**

KAVRAM TERCİHLERİMİZ ÜZERİNE

Kavramlar yalnızca yaşadıklarımızı anlatmamıza değil, onları nasıl anladığımıza da eşlik ediyor. Kullandığımız kelimeler bazı deneyimleri görünür kılarken bazılarını görünmez bırakabiliyor; bazen de farkında olmadan yargılayıcı ya da suçlayıcı anlamlar taşıyabiliyor. Bu nedenle bu sözlüğü hazırlarken yalnızca kavramların ne anlama geldiğini değil, neden o kavramı seçtiğimizi de belirtmeyi önemsiyoruz.

Sözlük boyunca:

"Teknoloji destekli cinsel/cinselleştirilmiş şiddet" kavramını tercih ettik. Siber, çevrim içi, dijital ve sanal kavramları birbiriyle ilişkili olmakla birlikte aynı anlama gelmez. Siber kavramı daha çok bilgisayar ağları, internet ve bağlantılı sistemler üzerinden gerçekleşen faaliyetleri; çevrim içi kavramı internet bağlantısı üzerinden yürütülen etkileşimleri; dijital kavramı ise dijital teknolojiler aracılığıyla üretilen, işlenen ve dolaşıma sokulan içerik, araç ve ortamları ifade eder. Sanal kavramı ise fiziksel olarak mevcut olmayan veya dijital ortamda temsil edilen alanları ve deneyimleri tanımlamak için kullanılır. Teknoloji destekli/teknoloji aracılığıyla gerçekleştirilen şiddet kavramı, teknolojiyi şiddetin gerçekleştiği bir ortam olmanın ötesinde, şiddetin uygulanmasını, sürdürülmesini ve yayılmasını mümkün kılan veya kolaylaştıran bir araç ve altyapı olarak değerlendirmemizi sağlıyor. Şiddetin yalnızca çevrim içi ortamlarda gerçekleşmediğini, dijital teknolojiler aracılığıyla çevrim dışı yaşamla iç içe geçerek ortaya çıkabildiğini ve etkilerinin fiziksel

dünyaya da uzanabildiğini vurgulamak amacıyla kapsayıcı ve güncel bir kavram olarak teknoloji destekli/teknoloji aracılığıyla gerçekleştirilen şiddet kavramını kullanıyoruz.

Yalnızca şiddet türlerine değil, ilişkili diğer kavramlara da yer verdik. Her teknoloji destekli şiddet biçimi doğrudan cinsel şiddet değildir. Bazı davranışlar cinsel/cinselleştirilmiş şiddetin kendisiyken, bazıları bu şiddeti mümkün kılabilir, kolaylaştırabilir veya onunla kesişebilir. Bu ayrımları birlikte anlamanın şiddetin farklı biçimlerini ve aralarındaki bağlantıları daha görünür kılabilmek için önemli olduğunu düşünüyoruz.

"Rıza" yerine, genel olarak "onay" kelimesini tercih ettik. Daha anlaşılır, gündelik dilde karşılığı olan ve güçlendirici kavramlar kullanmayı önemsiyoruz. Rıza kavramının tek yönlülüğüne karşın, onay kavramının karşılıklı iletişim ve evet-hayır ikiliğinin ötesinde sunduğu diyalog alanını önemsiyoruz. Bu nedenle sözlükte "kişinin onayı", "onayı olmadan" ve "onay dışı paylaşım" gibi ifadeleri daha sık kullanıyoruz. Öte yandan, "rıza" ve "onay" her bağlamda, özellikle hukuki ve akademik metinlerde, birebir aynı anlama gelmeyebilir. Belirli bir hukuki kavrama veya mevzuata atıfta bulunduğumuzda özgün terimi koruyoruz ve anlam farklılıklarını gözetiyoruz.

"Mahrem" kelimesi yerine, bağlama göre "özel", "kişisel" veya "cinsel içerikli" gibi daha açıklayıcı ifadeler kullandık. "Mahrem" kelimesi bazı bağlamlarda erkek egemen, kadın bedenini işaret eden ahlaki yargılarla ilişkilendirilebilir. Oysa söz konusu olan kişilerin bedenleri, görüntüleri, bilgileri ve

kendi sınırları üzerindeki hakları. Bu nedenle kapsamı mümkün olduğunca doğrudan anlatan kelimeleri seçtik. Örneğin, bağlama göre "mahrem görüntüler" yerine "özel görüntüler", "kişisel görüntüler" veya "cinsel içerikli görüntüler" ifadelerini kullandık.

Kavramsal tercihlerimizde "onay" odağını koruduk. Kişilerin görüntüleri, bilgileri ve kişisel sınırları söz konusu olduğunda, onayın varlığını veya yokluğunu görünür kılan ifadeleri tercih ediyoruz. Böylece odağı bilgilerin "gizli" ya da "açık", "gündelik" ya da "mahrem" olmasına değil, kişinin bu bilgilerin paylaşılmasına onay verip vermediğine çekiyoruz. Bununla birlikte, bir çocuğun cinsel içerikli görüntüsünün üretilmesi ya da paylaşılmasının her durumda istismar olduğunu hatırlatmak isteriz.

Kavramları şiddeti ve davranışı görünür kılacak şekilde seçtik. Yaygın olarak kullanılan *"intikam pornosu" (revenge porn)* ifadesi yerine, şiddeti ve sorumluluğu daha doğru tanımlayan "görüntüye dayalı cinsel şiddet" ya da "onay dışı cinsel medya içeriği yayma" ifadelerini tercih ediyoruz. "İntikam pornosu" ifadesi, şiddeti failin motivasyonu üzerinden görünmezleştirebilir, bir medya kategorisi olarak sunabilir ve sorumluluğu görüntüsü kullanılan kişiye yükleyebilir. Benzer şekilde, *"çocuk pornografisi"* ifadesini de şiddeti bir kategori olarak normalleştirdiği için kabul edilemez görüyoruz ve bunun yerine *"çocukların cinsel istismarına ilişkin materyaller"* ifadesini kullanıyoruz.

Çocukların ve gençlerin dijital dünyadaki varlığını hakları üzerinden ele aldık. Çevrim içi güvenlik konusunda alınan kararlarda çocukların ve gençlerin deneyimlerinin dikkate alınması gerektiğini savunuyoruz. Güvenlik ve koruma ihtiyacının, kişisel bilgilerin ve özel hayatın korunması, bilgiye erişim ve kendilerini ilgilendiren kararlara katılma haklarıyla birlikte ele alınması gerektiğine inanıyoruz. Gençler, yalnızca korunması gereken kişiler değil, hakları, deneyimleri ve görüşleri dikkate alınması gereken öznelerdir. Dijital güvenliği yasaklama ve kısıtlamalar üzerinden değil, hak temelli ve erişilebilir eğitim, katılım, kapsayıcılık ve güvenilir bilgiye erişim üzerinden ele alıyoruz.

Cinsel/cinselleştirilmiş şiddetle mücadele eden bir dernek olarak amacımız herkese tek bir dil dayatmak değil; şiddeti görünür kılan, kişileri suçlamayan ve şiddetin kaynağını daha iyi anlamamıza yardımcı olan ortak bir dil kurmak. Kavramların farklı bağlamlarda farklı anlamlar taşıyabileceğini, zamanla değişebileceğini ve yeni deneyimlerle dönüşebileceğini biliyoruz. Bu nedenle sözlüğü tamamlanmış ve değişmez bir kaynak olarak değil, birlikte tartışabileceğimiz ve geliştirebileceğimiz bir çalışma olarak görüyoruz. Kendi tercihlerimizi yeniden düşünmeye, gençlerin katılımına alan açmaya, yeni kavramları birlikte keşfetmeye ve dilimizi dönüştürmeye açık tutuyoruz.

SÖZLÜĞÜ OKURKEN:
HAKLAR, SORUMLULUKLAR VE GÜVENLİ OKUMA



Bu sözlükte yer verilen kavramlar, teknoloji destekli cinsel ve toplumsal cinsiyete dayalı şiddetin farklı biçimlerini anlamaya ve görünür kılmaya yönelik açıklayıcı kavramlardır. Bunların tamamı Türk hukukunda bağımsız bir suç kategorisi veya doğrudan hukuki karşılığı bulunan terimler değildir. Türkiye'de bu davranışların bir kısmı, olayın özelliklerine göre Türk Ceza Kanunu'ndaki farklı suç tipleri kapsamında değerlendirilebilir, bir kısmı için henüz özel bir suç tipi yoktur, bir kısmı ise suç oluşturmaz ya da başka mevzuat kapsamında ele alınır. Bir davranışın hukuki niteliği, yürürlükteki mevzuat, olayın koşulları ve ilgili hukuki değerlendirmeler çerçevesinde belirlenir. Bu nedenle sözlükteki tanımlar hukuki danışmanlık veya hukuki görüş yerine geçmez. Bu konuda daha detaylı bilgi için **Çevrim İçi Cinsel Şiddet Hakkında Hukuki Bilgiler** kitapçığını inceleyebilirsiniz.

Teknoloji destekli şiddet gerçek şiddettir. Şiddetin dijital araçlarla uygulanması yarattığı etkileri azaltmaz.

Oturumu kapatmak, bağlantıyı kesmek veya bir fotoğrafı silmek her zaman şiddeti sona erdirmez. Güven duygumuz zedelenebilir; korku, kaygı, panik ve travma yaşamımızı uzun süre etkileyebilir. Şiddete maruz bırakılanlar olarak dijital alanlardan uzaklaşmak, kendimizi ifade etmekten kaçınmak veya başkalarıyla kurduğumuz bağları sınırlandırmak zorunda hissedebiliriz. Şiddet ne biçimde yaşanırsa yaşansın, bizim suçumuz, hatamız ya da sorumluluğumuz değildir. Bir sosyal medya hesabı açmak, fotoğraf veya video paylaşmak, çevrim içi ortamlarda insanlarla tanışmak, iletişim kurmak, fikirlerimizi ifade etmek, birine güvenmek ya da dijital platformlarda var olmak şiddete gerekçe gösterilemez. Şiddetin sorumlusu şiddeti uygulayan kişidir. Deneyimlerimiz birbirinden farklı olsa da hepimiz saygıyı, güvenliği, adaleti ve dayanışmayı hak ediyoruz. Yalnız değiliz.

Bu yayında yer alan bazı kavramlar, anlatılar ve örnekler kendi deneyimlerimizi çağrıştırabilir; bazı anıları veya duyguları canlandırabilir. Okurken zorlandığımızı hissedersek ara verebilir, okumaya daha sonra devam edebilir ya da güvendiğimiz biriyle birlikte okuyabiliriz. Şiddet nereden ve nasıl gelirse gelsin, bizim suçumuz değil. Sorumluluk şiddeti uygulayana ait.

Destek istemek ve desteğe ulaşmak hakkımız.

Kavramlar, başvuru yolları ve öz yardım bilgileri için **csdestek.org** adresini ziyaret edebilir ve destek sistemleri hakkında hazırladığımız videoyu izleyebilirsiniz.



Destek sistemi nedir?

1 Şiddetin Kapsamı ve Türleri

Teknoloji Destekli Cinsel Şiddet

Technology-facilitated Sexual Violence

Teknoloji destekli/teknoloji aracılığıyla gerçekleştirilen cinsel şiddet internet, sosyal medya, mesajlaşma uygulamaları, telefonlar, bilgisayarlar ve akıllı cihazlar gibi teknolojilerin cinsel/cinselleştirilmiş şiddet, taciz, tehdit, istismar ve saldırı amacıyla kullanıldığı ya da bu şiddet biçimlerini mümkün kıldığı durumları kapsayan bir **şemsiye kavramdır**. Tıpkı cinsel şiddet gibi, tek bir davranışı değil, farklı biçimlerde ortaya çıkabilen çok sayıda şiddet türünü kapsar. Özellikle kadınları, LGBTİ+'ları, toplumsal cinsiyet normlarına uymadıkları düşünülen kişileri, çocukları ve gençleri hedef alabilir; hem çevrim içi hem de çevrim dışı yaşamda etkisini gösterebilir.

Teknoloji yalnızca şiddetin gerçekleştiği bir ortam değil; aynı zamanda şiddeti mümkün kılan, kolaylaştıran ve etkilerini artırabilen bir araç. Dijital, sanal veya çevrim içi şiddet gibi ifadeler yaşananların yalnızca ekranların ardında gerçekleşen olaylar olduğunu düşünmemize neden olabilir. Oysa çevrim içi ve çevrim dışı yaşamlarımız iç içedir; dijital ortamda başlayan şiddet gündelik hayatımıza, ilişkilerimize ve fiziksel güvenliğimize uzanabilir. Teknoloji destekli cinsel şiddet ifadesinin tercih edilmesinin nedeni biraz da bu geniş kapsamı işaret edebilmesidir.

Teknoloji destekli cinsel/cinselleştirilmiş şiddet her zaman karmaşık teknolojiler gerektirmez. Bazen bir mesaj, bir konum ya da bir sosyal medya paylaşımı şiddetin bir aracı olabilir.

Görüntüye Dayalı Cinsel Şiddet

Image-based Sexual Abuse

Görüntüye dayalı cinsel şiddet, kişilere ait cinsel/cinselleştirilmiş görüntülerin onayları dışında elde edilmesini, üretilmesini, değiştirilmesini, paylaşılmasını kapsayan bir **şemsiye kavramdır.** Görüntülerin tehdit, şantaj, aşağılama, kontrol etme veya itibarsızlaştırma amacıyla kullanılması da bu kapsamdadır.

Bu şiddet biçimi kişisel görüntülerin izinsiz paylaşılması ***(non-consensual intimate image abuse)***, gizlice görüntü alınması (kameralı akıllı gözlüklerin ya da teknolojik gözetleme araçlarının kullanımı vb.), onay dışı etek altı görüntü alma ***(upskirting)***, cinsel saldırının kaydedilmesi ve/veya kaydının paylaşılması, yapay zekâyla cinsel içerikli görüntüler üretilmesi veya mevcut görüntülerin değiştirilmesi gibi farklı şekillerde karşımıza çıkabilir. Kişilerin cinsel içerikli görüntülerinin onayları dışında yetişkin içerik platformlarında yayımlanması, yeniden dolaşıma sokulması veya ekonomik kazanç amacıyla kullanılması da görüntüye dayalı cinsel şiddettir.

Bir görüntünün çekilmesine veya paylaşılmasına verilen onay, o görüntünün başka amaçlarla kullanılmasına ya da başkalarıyla paylaşılmasına verilmiş bir onay değildir. Görüntünün gerçek veya yapay olarak üretilmiş olması, kişinin onayının ve sınırlarının ihlal edilmesini önemsiz kılmaz.

Cinsel İçerikli Şantaj

Sextortion

Cinsel içerikli şantaj, bir kişinin cinsel içerikli görüntülerinin, kişisel bilgilerinin veya cinsel yaşamına ilişkin içeriklerin paylaşılacağı tehdidiyle para, yeni görüntüler, cinsel eylemler ya da başka bir çıkar elde etmeye çalışılmasıdır. Teknoloji destekli cinsel şiddetin biçimlerinden biridir ve çoğunlukla sosyal medya, mesajlaşma uygulamaları, e-posta veya çevrim içi oyunlar gibi dijital ortamlarda gerçekleşir.

Şantajı uygulayan kişi tanımadığımız biri olabileceği gibi sevgilimiz, eski partnerimiz ya da başka bir tanıdığımız da olabilir. Görüntülerin gerçekten var olması veya tehdidin gerçekleşmesi gerekmez; paylaşma tehdidi tek başına kişiyi korkutmak, kontrol etmek ve baskı altına almak için kullanılabilir. Fail, kişinin onayı olmadan elde ettiği görüntüleri kullanabileceği gibi, başlangıçta onayıyla paylaşılmış içerikleri de şantaj aracına dönüştürebilir.

Cinsel içerikli şantaj görüntü odaklı olmak zorunda değildir; ses kaydı, kişinin cinsel yönelimi, cinsiyet kimliği veya cinsel yaşamına ilişkin bilgilerin onayı dışında açıklanacağı tehdidi de şantaj aracı olarak kullanılabilir.

Herkes bu şiddet biçimiyle karşılaşabilir; ancak gençler, kadınlar ve LGBTİ+'lar toplumsal eşitsizlikler ve ayrımcılık nedeniyle daha fazla risk altındadır. Cinsel içerikli şantaj, kişinin güvenlik duygusunu, ilişkilerini, dijital ve fiziksel alanlarda özgürce var olabilmesini etkileyebilir.

Yapay Zekâ ile Üretilen Cinsel İçerikler (Sentetik Görüntüler)

Yapay zekâ veya başka dijital araçlarla bir kişinin görüntüsünün, sesinin ya da diğer medya içeriklerinin değiştirilerek cinsel içerikli, yanıltıcı veya gerçeğe aykırı materyaller oluşturulmasını kapsar. Sentetik görüntüler, gerçek bir kişinin görüntüsünün manipüle edilmesiyle oluşturulabileceği gibi gerçekte var olmayan kişi veya sahnelerin üretilmesiyle de ortaya çıkabilir. Deepfake, fotoğraftaki kıyafetleri dijital olarak kaldıran uygulamalar (nudify), ses klonlama gibi teknolojilerle bir kişi çıplakmış, cinsel bir eylemde bulunuyormuş, hiç gitmediği bir mekâna gitmiş ya da hiç söylemediği sözleri söylüyormuş gibi gösterilebilir. Bu içerikler kişinin onayı olmadan üretilebilir, paylaşılabilir veya tehdit, şantaj ve baskı amacıyla kullanılabilir.

Öte yandan, her deepfake kullanımı cinsel şiddet oluşturmaz; değerlendirmede içeriğin niteliği, kullanım amacı, tarafların onayı ve ortaya çıkan etkiler dikkate alınır. Çocukların cinsel içerikli görüntülerinin yapay zekâyla üretilmesi her durumda istismardır.

İçeriğin yapay olarak üretilmiş ya da değiştirilmiş olması, kişinin yaşadığı zararı daha az önemli kılmaz.

Çevrim içi Taciz

Online Harassment

Çevrim içi taciz, dijital araçlar ve platformlar aracılığıyla bir kişiyi rahatsız eden, korkutan, aşağılayan, baskı altına alan veya susturan davranışları kapsar. Sosyal medya, mesajlaşma uygulamaları, e-posta, çevrim içi oyunlar ve toplantı platformları gibi farklı dijital ortamlarda gerçekleşebilir.

Israrlı ve istenmeyen mesajlar göndermek, cinsel saldırı tehdidi ya da cinsel içerikli hakaretler iletmek, hedef gösteren paylaşımlar yapmak, farklı hesaplardan kişiye ulaşmaya çalışmak ve çevrim içi toplantılara izinsiz katılımlarla saldırgan veya cinsel içerikli materyaller paylaşmak ***(zoom bombing)*** çevrim içi taciz örnekleridir. Çevrim içi oyunlarda sesli veya yazılı sohbetler üzerinden cinsiyetçi ve cinsel içerikli tacizde bulunmak, oyuncuları cinsiyet kimlikleri veya cinsel yönelimleri nedeniyle hedef almak ya da canlı yayınlarda kişilere yönelik ***taciz ve hedef gösterme kampanyaları yürütmek*** de bu kapsamda değerlendirilebilir.

Taciz tek bir olayla ortaya çıkabileceği gibi, tekrarlayan veya birden fazla kişinin katıldığı koordineli saldırılar biçiminde de yaşanabilir.

Çevrim içi taciz, teknoloji destekli şiddetin geniş bir kategorisidir. Onay dışı cinsel içerik gönderimi, dijital ısrarlı takip ve dijital linç gibi farklı davranışlarla kesişebilir.

Onay Dışı Cinsel İçerik Gönderimi

Cyberflashing

Onay dışı/istenmeyen cinsel içerik gönderimi, bir kişiye onayı olmadan cinsel içerikli fotoğraf ya da videoların dijital araçlar aracılığıyla gönderilmesidir. Sosyal medya ve mesajlaşma uygulamalarının yanı sıra Bluetooth ve AirDrop gibi yakındaki cihazlarla dosya paylaşmayı sağlayan özellikler üzerinden de gerçekleşebilir. Örneğin, bir kişiye istemediği hâlde cinsel organ görüntüsü göndermek bu kapsamdadır.

Bu davranış, kişinin sınırlarını ihlal eden bir cinsel taciz biçimidir. Kişiyi rahatsız etmek, şaşırtmak, korkutmak veya üzerinde baskı kurmak amacıyla gerçekleştirilebilir. Gönderen kişinin tanıdık ya da yabancı olması, davranışın niteliğini değiştirmez. Burada belirleyici olan, karşılıklı onaya dayalı olan cinsel içerikli yazışmadan ***(sexting)*** farklı olarak cinsel içerikli materyalin kişiye onayı olmadan gönderilmesi, yani kişinin bu görüntülere maruz bırakılmasıdır.

Kişisel Bilgilerin Onay Dışı Paylaşılması

Doxxing

Kişisel bilgilerin onay dışı paylaşılması, bir kişiye ait bilgilerin kişinin onayı olmadan ve onu hedef hâline getirebilecek biçimde dijital ortamlarda paylaşılmasıdır. Ev adresi, telefon numarası, işyeri, konum bilgileri, kimlik bilgileri ve kişisel yazışmalar bu bilgiler arasında yer alabilir. Farklı kaynaklardan toplanan bilgilerin bir araya getirilerek kişinin kimliğinin veya nerede bulunduğunun açığa çıkarılması da bu kapsamdadır.

Doxxing, kişiyi tehdit etmek, tacize açık hâle getirmek, itibarını zedelemek veya başkalarını ona saldırmaya yönlendirmek amacıyla gerçekleştirilebilir. Kişinin cinsel yöneliminin veya cinsiyet kimliğinin onayı dışında açıklanması ***(outing)*** ya da transların kullanmadıkları adlarıyla anılması ***(deadnaming)*** da özel hayatın ve güvenliğin ihlalidir.

Bir bilginin daha önce internette paylaşılmış veya herkese açık olması, o bilginin kişinin onayı olmadan hedef gösterme amacıyla yeniden paylaşılmasını zararsız hâle getirmez. Bilginin yalnızca gizli olup olmadığına değil, hangi amaçla ve hangi bağlamda paylaşıldığına da bakılmalıdır.

Dijital Israrlı Takip

Cyberstalking

Dijital/siber ısrarlı takip (cyberstalking), bir kişinin dijital araçlar aracılığıyla tekrarlanan şekilde izlenmesini, istenmeyen iletişim girişimlerine maruz bırakılmasını veya tehdit edilmesini kapsar. Sosyal medya hesaplarının takip edilmesi, farklı hesaplardan tekrar tekrar mesaj gönderilmesi, takip yazılımları (stalkerware) ve konum takip cihazları (AirTag gibi) kullanılarak konum bilgilerinin izlenmesi ya da kişinin çevrim içi faaliyetlerinin kontrol edilmesi bu davranışlara örnek olabilir.

Toplumsal cinsiyete dayalı şiddet bağlamında dijital takip, kişiyi korkutmak, kontrol etmek veya dijital alanlardan uzaklaştırmak amacıyla kullanılabilir. Her çevrim içi iletişim ya da takip davranışı tek başına ısrarlı takip anlamına gelmez; davranışın niteliği, sürekliliği ve bağlamı önemlidir.

Siber Zorbalık

Cyberbullying

Siber zorbalık (cyberbullying), dijital teknolojiler ve çevrim içi iletişim araçları kullanılarak bir kişiye yönelik tekrarlayan, kasıtlı ve zarar verici davranışlara denir. Özellikle çocuklar ve gençler arasında akran şiddetinin dijital ortamlara taşınmasıyla ortaya çıkan bu davranışlar; hakaret etme, aşağılama, tehdit etme, dışlama, hedef gösterme, söylenti yayma, kişisel bilgileri ifşa etme, özel yazışmaları paylaşma veya kişinin izni olmadan küçük düşürücü fotoğraf veya videolarını yaygınlaştırma gibi biçimler alabilir.

Siber zorbalıkta çoğunlukla sosyal çevre, takipçi sayısı, dijital beceriler, anonimlik veya toplu hareket etme kapasitesinden kaynaklanan bir güç eşitsizliği bulunur. Dijital içeriklerin hızla yayılması ve uzun süre erişilebilir kalması, maruz kalınan zararın boyutunu artırabilir.

Çevrim içi taciz, dijital ortamlardaki istenmeyen, rahatsız edici veya tehdit edici davranışları kapsayan daha geniş bir kavramken, siber zorbalık özellikle davranışların tekrarlanması, süreklilik kazanması ve güç dengesizliğiyle ilişkilendirilir.

Dijital / Çevrim İçi Flört Şiddeti

Dijital veya çevrim içi flört şiddeti, mevcut ya da eski bir flört partnerinin dijital araçları kullanarak diğer kişiyi kontrol etmesi, baskı altına alması, tehdit etmesi, izlemesi veya cinsel sınırlarını ihlal etmesidir. Teknoloji destekli şiddetin bir türü olan bu kavram, farklı davranış biçimlerini kapsayan bir **şemsiye kavramdır.** Sosyal medya, mesajlaşma uygulamaları, telefonlar, akıllı ev cihazları ***(Nesnelerin İnterneti, Internet of Things)*** ve konum paylaşım özellikleri bu amaçlarla kullanılabilir.

Sürekli mesaj göndererek nerede veya kiminle olduğunu öğrenmeye çalışmak, şifrelerini istemek, hesapları ya da konumu kontrol etmek, dijital ortamda kimlerle iletişim kurulduğuna müdahale etmek, bankacılık uygulamaları, ortak hesaplar ya da isme alınan borçlar üzerinden kontrol sağlamak bu şiddetin örnekleri arasındadır. Cinsel içerikli görüntü göndermeye zorlamak, görüntülerin paylaşılacağı tehdidiyle baskı kurmak veya görüntüleri onay almadan paylaşmak da dijital flört şiddetinin cinsel/cinselleştirilmiş boyutları arasında yer alabilir.

Kişinin hesabının ele geçirilmesi ve kişinin kendi hesaplarına ya da cihazlarına erişiminin engellenmesi de teknoloji destekli bir şiddet türüdür. Bu davranışlar bir araya gelerek kişinin ilişkilerini, iletişimini ve gündelik yaşamını sürekli denetim altında tutan bir kontrol örüntüsüne dönüşebilir. Teknoloji destekli ***zorlayıcı kontrol*** olarak adlandırılan bu durumda, dijital araçlar kişinin özerkliğini ve hareket alanını kısıtlamak için kullanılır.

Şiddet, ilişki devam ederken yaşanabileceği gibi, ilişki sona erdikten sonra da sürebilir.

Romantik ilişki dolandırıcılığı

Romance Scam

Romantik ilişki dolandırıcılığı, bir kişinin dijital ortamda romantik veya duygusal bir ilişki kuruyormuş izlenimi yaratarak karşısındaki kişinin güvenini kazanması ve bu güveni para, kişisel bilgi, görüntü veya başka çıkarlar elde etmek için kullanmasıdır. Sosyal medya, flört uygulamaları ve mesajlaşma platformları üzerinden gerçekleşebilir.

Fail, karşısındaki kişiyle hiç yüz yüze gelmeden de duygusal bir yakınlık kurabilir; sahte bir kimlik kullanabilir veya zaman içinde güven ilişkisini manipülasyon ve baskı aracına dönüştürebilir. Bazı durumlarda cinsel içerikli görüntüler elde edilerek şantaj yapılması ya da kişisel bilgilerin tehdit amacıyla kullanılması da söz konusu olabilir. Romantik ilişki dolandırıcılığı her zaman cinsel şiddet anlamına gelmez; ancak cinsel içerikli şantaj ve diğer teknoloji destekli cinsel şiddet biçimleriyle kesişebilir.

Çevrim İçi Kandırma ve Cinsel İstismara Hazırlama

Cyber Grooming

Siber grooming, bir yetişkinin ya da yaşça büyük birinin dijital ortamlar aracılığıyla bir çocukla iletişim kurması, güvenini inşa ederek onu cinsel istismara hazırlamasına yönelik davranış ve süreçleri kapsar. Siber grooming, teknoloji destekli cinsel şiddetin çocukları hedef alan biçimlerinden biridir ve sosyal medya, mesajlaşma uygulamaları, çevrim içi oyunlar ve diğer dijital platformlar aracılığıyla gerçekleşebilir. Çevrim içi cinsel istismar, cinsel içerikli şantaj ve görüntüye dayalı cinsel şiddet gibi farklı şiddet biçimleriyle kesişebilir.

Fail çocukla duygusal yakınlık kurabilir; kendisini güvenilir biri gibi tanıtabilir, özel sırlar paylaşarak bağlılık oluşturabilir veya çocuğu ailesinden, arkadaşlarından ve diğer destek kaynaklarından uzaklaştırmaya çalışabilir. Süreç ilerledikçe çocuk cinsel içerikli konuşmalara, görüntü paylaşımına ya da yüz yüze buluşmaya yönlendirilebilir.

Siber grooming her zaman açık bir tehdit, zorlama veya şiddet içermez. Fail çocuğun güvenini ve duygusal bağını istismar ederek sınırlarını aşamalı biçimde ihlal eder ve istismarı normalleştirir. Bu nedenle çocuk yaşadıklarını başlangıçta bir tehdit veya istismar olarak tanımayabilir. Çocuğun iletişimi başlatmış, faile güvenmiş ya da cinsel içerikli görüntü paylaşmış olması, istismarın sorumluluğunu çocuğa yüklemez; sorumluluk faile aittir.

Çocukların Cinsel İstismarına / Sömürüsüne İlişkin Materyaller

Child Sexual Abuse and Exploitation Material, CSAEM

Çocuğun cinsel istismarına/sömürüsüne ilişkin materyaller; bir çocuğun cinsel istismara veya sömürüye maruz bırakıldığı durumları gösteren, betimleyen ya da belgeleyen fotoğraf, video, ses kaydı, dijital görüntü, çizim ve benzeri görsel-işitsel materyalleri ifade eder. Bu materyaller, çocuğun gerçek görüntülerini içerebileceği gibi, gerçek bir çocuğu temsil eden veya çocuk izlenimi yaratan dijital olarak üretilmiş, değiştirilmiş ya da manipüle edilmiş içerikleri de kapsayabilir.

Bu materyallerin üretilmesi, kaydedilmesi, bulundurulması, erişime açılması, paylaşılması, dağıtılması veya yayılması, çocuğun cinsel dokunulmazlığı, mahremiyeti, onuru, güvenliği ve kişisel verilerinin korunması başta olmak üzere temel haklarını ihlal eder ve istismarın etkilerinin sürmesine ya da yeniden üretilmesine neden olabilir.

Çocukların cinsel içerikli herhangi bir materyalin üretim sürecinde kullanılması çocuğa yönelik cinsel istismar türlerinden biridir; aynı zamanda çocuğun cinsel-ticari sömürüsüdür. Çocuklar cinsel istismara veya sömürüye ilişkin içeriklerin üretilmesine ve dolaşıma sokulmasına onay vermiş olarak kabul edilemez. Bu nedenle çocuk, materyalin öznesi veya sorumlusu olarak değil, hakları ihlal edilen kişi olarak ele alınmalıdır.

Dijital Kimliğe Bürünme ve Taklit Hesaplar

Impersonation, Catfishing

Dijital kimliğe bürünme ***(impersonation)***, bir kişinin kimliğinin, fotoğraflarının veya kişisel bilgilerinin onun gibi davranmak ya da başkalarını yanıltmak amacıyla kullanılmasıdır. Taklit hesaplar üzerinden mesaj gönderilmesi, sahte profiller oluşturulması veya bir kişinin adına cinsel içerikli paylaşımlar yapılması bu kapsama dâhil olabilir. Bu davranışlar kişinin itibarını zedelemek, onu hedef göstermek, taciz etmek veya başkalarıyla ilişkilerini bozmak için kullanılabilir.

Çevrim içi ortamda sahte bir kimlik veya profil oluşturarak başkalarıyla ilişki kurmak, ***catfishing*** olarak adlandırılır. Bu yöntem romantik ilişki dolandırıcılığı, kişiyi yanıltma veya güven kazanarak çıkar sağlama amacıyla kullanılabilir; ancak her durumda maddi kazanç hedeflenmez.

2

Şiddeti Besleyen Söylemler ve Yapısal Mekanizmalar

Dijital Mizenformasyon ve Dezenformasyon

Dijital mizenformasyon ve dezenformasyon, yanlış veya yanıltıcı bilgilerin dijital platformlarda üretilmesi ve yayılmasıyla ilgilidir. Mizenformasyon, yanlış bilginin kasıtlı bir aldatma amacı olmadan yayılmasını; dezenformasyon ise yanlış veya yanıltıcı bilginin kasıtlı olarak üretilmesini ya da yayılmasını ifade eder. Doğru bilginin zarar vermek amacıyla kullanılması ise ***malenformasyondur*** ve doxxing ya da özel görüntülerin sızdırılmasıyla doğrudan ilişkilidir.

Yanlış veya yanıltıcı bilgiler, şiddetten etkilenen hayatta kalanların beyanlarını itibarsızlaştırmak, yaşadıklarını inkâr etmek, onları suçlamak veya hedef göstermek amacıyla kullanılabilir. Cinsiyetçi kalıp yargılarla birleştiğinde şiddeti meşrulaştırabilir, ayrımcılığı pekiştirebilir ve kişilerin dijital ortamlarda yeniden hedef alınmasına yol açabilir. Dezenformasyon koordineli karalama ve itibarsızlaştırma kampanyalarının bir parçası olabilir; özellikle siyasetçi, gazeteci ve aktivist kadınları hedef alabilir.

Dijital platformların bildirim mekanizmaları da kötüye kullanılabilir. Hayatta kalanları susturmak veya dijital alanlardan uzaklaştırmak amacıyla bilerek asılsız şiddet ya da taciz bildirimlerinde bulunulması, kişilerin hesaplarının kısıtlanmasına veya kapatılmasına yol açabilir.

Toplumsal Cinsiyete Dayalı Trolleme ve Nefret Söylemi

Toplumsal cinsiyet temelli trolleme ve nefret söylemi, kişileri toplumsal cinsiyetleri, cinsiyet kimlikleri veya cinsel yönelimleri üzerinden hedef alan, onları aşağılamayı, provoke etmeyi, itibarsızlaştırmayı, dışlamayı ya da düşmanlaştırmayı amaçlayan dijital davranış ve ifadeleri kapsar. Kadınları, feministleri ve LGBTİ+'ları hedef alan cinsiyetçi hakaretler, aşağılayıcı veya düşmanlaştırıcı paylaşımlar, toplumsal cinsiyet eşitliğini savunan kişileri provoke etmek amacıyla tekrarlanan yorumlar ve cinsiyetçi kalıp yargılar üzerinden yürütülen alay ve taciz kampanyaları bu kapsamda değerlendirilebilir.

Bu tür dijital pratikler arasında, özellikle sosyal medyada öfke, tepki ve tartışma yaratarak etkileşim elde etmeyi amaçlayan rage bait (öfke tuzağı) içerikleri de yer alabilir. Rage bait, kişileri öfkelendirmek, kışkırtmak veya tepki vermeye yöneltmek amacıyla hazırlanan ya da dolaşıma sokulan içerikleri ifade eder. Bu içerikler, hedef alınan gruplara yönelik önyargıları ve düşmanlığı besleyebilecekleri gibi, ayrımcı söylemlerin daha geniş kitlelere ulaşmasına da neden olabilirler.

Trolleme, kişileri provoke etme, tepki yaratma veya tartışmayı sabote etme amacı taşıyabilir. Rage bait, öfke ve tepki yaratarak etkileşim elde etmeye odaklanan bir içerik üretme ve dolaşıma sokma pratiğidir. Nefret söylemi ise kişileri toplumsal cinsiyetleri, cinsiyet kimlikleri veya cinsel yönelimleri üzerinden aşağılayan, dışlayan ya da düşmanlaştıran ifadeleri kapsar.

Dijital Linç

Dijital linç ***(doppling)***, bir kişi veya grubun dijital platformlarda hedef gösterilerek toplu biçimde aşağılanması, tehdit edilmesi, taciz edilmesi veya itibarsızlaştırılmasına yönelik saldırıları ifade eder.

Toplumsal cinsiyete dayalı şiddet bağlamında, hayatta kalanların kimliklerinin ifşa edilmesi, cinsel geçmişleri üzerinden yargılanmaları ***(slut-shaming)***, şiddet deneyimleri nedeniyle suçlanmaları veya cinsiyet kimlikleri ve cinsel yönelimleri üzerinden hedef alınmaları biçiminde ortaya çıkabilir. Cinsiyetçi söylemlerle beslenen bu saldırılar, hayatta kalanların psikolojik ve toplumsal açıdan zarar görmelerine, sınırlarının ihlal edilmesine ve yeniden şiddete maruz kalmalarına neden olabilir. Ayrıca toplumsal baskı ve itibarsızlaştırılma korkusu, şiddetin bildirilmesini ve destek arayışını zorlaştırabilir.

Dijital Gözetim, Baskı ve Sansür

Dijital gözetim, baskı ve sansür, dijital teknolojiler aracılığıyla kişilerin çevrim içi faaliyetlerinin izlenmesi, denetlenmesi, kısıtlanması veya susturulmasını ifade eder. Devletler, kurumlar, platformlar ya da kişiler tarafından gerçekleştirilebilen bu uygulamalar, ifade özgürlüğünü, gizliliği ve dijital hakları ihlal edebilir. Kişinin konumunun veya iletişiminin onayı dışında izlenmesi, dijital hesaplarının kontrol edilmesi, çevrim içi faaliyetlerinin kısıtlanması ve cinsiyet eşitliğini savunan içeriklerin susturulması gibi biçimlerde ortaya çıkabilir.

Özellikle kadınlar ve LGBTİ+'lar açısından bu uygulamalar, kontrol ve tehdit mekanizmasına dönüşerek kendini ifade etme, destek arama ve destek sunma, dijital alanlara güvenle katılma olanaklarını sınırlayabilir. Bu kavram, bireysel düzeydeki kontrol davranışlarının yanı sıra toplumsal eşitsizlikleri yeniden üreten yapısal mekanizmaları da kapsar.

Algoritmik Şiddet

Algoritmik şiddet, algoritmaların ve algoritmik karar sistemlerinin toplumsal eşitsizlikleri, önyargıları ve güç ilişkilerini yeniden üreterek belirli kişi veya grupların dışlanmasına, ayrımcılığa uğramasına ya da zarara maruz kalmasına yol açan süreçleri ifade eder.

Toplumsal cinsiyete dayalı şiddet bağlamında, cinsiyetçi yanlılıklar içeren algoritmalar kadınları ve LGBTİ+'ları ayrımcılığa maruz bırakabilir; şiddet içeren veya cinsiyetçi içeriklerin yayılmasını kolaylaştırabilir ya da şiddetten etkilenen hayatta kalanların bildirimlerini etkisiz biçimde değerlendirebilir. Bu süreçler, toplumsal cinsiyet eşitsizliklerini dijital ortamlarda yeniden üreterek şiddetin normalleşmesine ve hayatta kalanların yeniden hedef alınmasına sebep olabilir. Örneğin, kadın düşmanlığını ve cinsel şiddeti meşrulaştıran içeriklerin öneri algoritmaları aracılığıyla daha geniş kitlelere ulaştırılması, bu söylemlerin yaygınlaşmasına neden olabilir.

Her algoritmik yanlılık tek başına şiddet olarak değerlendirilemez; kavram, ortaya çıkan zararın niteliği ve toplumsal güç ilişkileri çerçevesinde ele alınmalıdır.

Erkosfer / Manosphere

Erkosfer (manosphere), erkeklik, toplumsal cinsiyet rolleri ve ilişkiler etrafında şekillenen; antifeminist söylemlerin, kadın düşmanlığının ve erkeklerin hak kaybına uğradığı iddialarının öne çıktığı farklı çevrim içi toplulukları ve içerik üreticilerini kapsayan dijital bir ekosistem olarak tanımlanır.

Erkosfer yalnızca kendi içindeki çevrim içi topluluklarla sınırlı bir etkiye sahip değildir. Bu ekosistemde üretilen söylemler, kavramlar, iddialar ve toplumsal cinsiyet algıları ana akım medyaya, popüler kültüre ve gündelik toplumsal tartışmalara taşınabilir. Örneğin red pill (kırmızı hap), alpha/beta erkek sınıflandırması, hypergamy (kadınların kendilerinden daha yüksek statüdeki erkekleri tercih ettiği iddiası) ve kadınların sözde değişmez doğasına ilişkin genellemeler, bu söylemlerin farklı alanlarda yeniden üretilmesine örnek oluşturabilir. Özellikle kadınların ve feministlerin hedef gösterildiği, toplumsal cinsiyet eşitliğinin tehdit olarak sunulduğu veya kadın düşmanlığının tartışmalı bir görüş ya da eğlence unsuru olarak dolaşıma sokulduğu içerikler, toplumsal cinsiyet eşitliği açısından ciddi riskler oluşturur.

Erkosfer tek tip veya merkezi olarak örgütlenmiş bir yapı değildir; içerdiği topluluklar, görüşler, söylemler ve ekonomik faaliyetler bakımından farklılık gösterir. Bazı içerik üreticileri, erkeklik ve toplumsal cinsiyet eşitsizliği etrafındaki kaygıları ve ilişki kurma güçlüklerini takipçi kazanmak ve ekonomik kazanç sağlamak amacıyla kullanır; reklam, abonelik, bağış, ücretli danışmanlık ve ürün satışı gibi yöntemlerle kadın düşmanlığını veya antifeminist söylemleri ticari bir modele dönüştürür.

Erkosfer, cinsel şiddeti meşrulaştıran, hayatta kalanları suçlayan veya kadınlara yönelik taciz ve şiddeti normalleştiren söylemlerin yayılmasına büyük oranda aracılık edebilir.

İncel İdeolojisi

İncel, İngilizce *involuntary celibate* ifadesinin kısaltmasıdır ve "istemsiz bekâr" anlamına gelir. İncel ideolojisi, romantik veya cinsel ilişki kuramamayı kendi isteği dışında yaşadığını düşünen bazı kişilerin bu deneyimi kadın düşmanlığı, antifeminizm ve toplumsal cinsiyet eşitliğine yönelik düşmanlıkla ilişkilendirdiği bir düşünce çerçevesidir. Bu ideolojiyi benimseyen bazı çevrim içi topluluklar, kadınları suçlayan, cinsel şiddeti meşrulaştıran veya şiddet tehditlerini normalleştiren söylemler üretebilir.

Erkosfer örneklerinden biri olan bu topluluklar, özellikle aidiyet ve kabul görme ihtiyacına seslenen söylemler aracılığıyla genç erkeklere de ulaşabilir. Kadınlara yönelik önyargıları pekiştiren, ilişki kurma güçlüklerini kadınlara veya toplumsal cinsiyet eşitliğine bağlayan içerikler, düşmanlık içeren tutumların normalleşmesine neden olabilir. Bazı durumlarda şiddetin yüceltilmesine veya şiddet tehditlerinin yayılmasına da zemin hazırlayabilir.

Bazı içerik üreticileri, genç erkeklerin yalnızlık, dışlanmışlık ve ilişki kurma güçlüklerini hedefleyen söylemler üzerinden takipçi kazanabilir; ücretli danışmanlık, abonelik veya ürün satışı yoluyla maddi manevi kazanç sağlayabilir. Bu durum, kadın düşmanlığını ve toplumsal cinsiyet eşitsizliğini besleyen söylemlerin ticari amaçlarla yeniden üretilmesine neden olur.

Dijital Uçurum ve Dijital Dışlanma

Dijital dışlanma ve dijital uçurum, kişilerin internet, dijital teknolojiler, bilgi ve güvenlik araçlarına erişimindeki eşitsizlikleri ifade eder. Yaş, engellilik, gelir düzeyi, yaşanılan yer ve toplumsal cinsiyet eşitsizlikleri bu farklılıkları derinleştirebilir. Teknoloji destekli cinsel şiddet bağlamında bu eşitsizlikler, kişilerin çevrim içi şiddeti bildirme, dijital güvenliklerini sağlama ve destek mekanizmalarına ulaşma olanaklarını kısıtlayabilir. Örneğin, dijital okuryazarlık eksikliği, erişilebilir olmayan başvuru platformları veya partnerin dijital cihazları kontrol etmesi, kişilerin yardım aramasını zorlaştırabilir. Dijital dışlanma, bu nedenle yalnızca teknolojiye erişim sorunu değil, kişilerin dijital haklarını kullanabilmeleri ve şiddet karşısında destek alabilmeleriyle ilişkili yapısal bir eşitsizlik meselesidir.

Çocuklar ve gençler açısından dijital dışlanma, yalnızca teknolojiye erişememek değil, bilgiye ulaşma, kendini ifade etme ve kendilerini ilgilendiren kararlara katılma haklarının sınırlanması anlamına da gelebilir. Bu nedenle dijital güvenlik politikaları çocukların ve gençlerin korunma ihtiyaçlarını, katılım ve özerklik haklarını birlikte gözetmelidir.

3

Haklar, Kapasite ve Destek

Çevrim içi Dayanıklılık

Çevrim içi dayanıklılık, kişilerin dijital ortamlarda karşılaştıkları taciz, ayrımcılık ve şiddet karşısında iyilik hâllerini destekleyebilmelerini, ihtiyaç duydukları kaynaklara ve dayanışma ağlarına erişebilmelerini ifade eder. Bu kapasite yalnızca bireysel becerilerle değil, güvenli dijital ortamlar ve erişilebilir destek mekanizmalarıyla da ilişkilidir. Toplumsal cinsiyete dayalı dijital şiddet bağlamında bu kapasite, hayatta kalan odaklılık ve travma bilgili yaklaşımlarla desteklenerek güvenliği, gizliliği, seçim hakkını ve yeniden zarar görmenin önlenmesini gözetir.

Çevrim içi dayanıklılık, gizlilik ayarlarını güçlendirmek, hesap güvenliğini artırmak, dijital kanıtları güvenli biçimde saklamak, gerektiğinde destek ağlarına başvurmak ve dijital güvenlik konusunda bilgi edinmek gibi yollarla desteklenebilir. Platformların erişilebilir şikâyet ve destek mekanizmaları sunması, kurumların güvenli başvuru yolları oluşturması ve toplulukların dayanışma geliştirmesi de bu sürecin parçasıdır.

Bu yaklaşım, sorumluluğu yalnızca hayatta kalana yüklemez; platformların, kurumların ve toplumsal çevrenin sorumluluğunu da gözetir. Dayanıklılık, şiddete katlanmak değil, kişinin kendi ihtiyaçları doğrultusunda güvenliğini ve iyilik hâlini destekleyen kaynaklara erişebilmesidir.

Dijital Okuryazarlık

Dijital okuryazarlık, dijital teknolojileri bilinçli, eleştirel ve güvenli biçimde kullanabilme; çevrim içi bilgileri değerlendirebilme ve dijital ortamlardaki hak ve sorumluluklarını tanıyabilme becerilerini ifade eder. Toplumsal cinsiyete dayalı dijital şiddet bağlamında kişisel bilgilerin ve görüntülerin korunması, yanlış ve yanıltıcı bilgilerin ayırt edilmesi, çevrim içi taciz ve manipülasyonun tanınması ve kişinin onayı ile dijital haklar konusunda bilgi sahibi olmak önemlidir.

Her yaş grubunda dijital okuryazarlığın desteklenmesi, kişilerin çevrim içi riskleri tanımasına ve dijital haklarını kullanmasına yardımcı olur. Özellikle gençlere ve yaşlılara yönelik eğitimlerde toplumsal cinsiyet eşitliği, kişisel sınırlar, güvenli internet kullanımı ve çevrim içi şiddetle baş etme konularına yer verilmelidir. Dijital ortamları yasaklamak veya erişimi yalnızca kısıtlamak yerine, eleştirel düşünme ve bilinçli karar verme becerilerini güçlendiren, yaş gruplarının ihtiyaçlarına uygun eğitim yaklaşımları benimsenmelidir. Dijital okuryazarlık, şiddeti önleme sorumluluğunu kişilere yüklemez; platformların, eğitim kurumlarının ve kamu otoritelerinin güvenli ve eşitlikçi dijital ortamlar oluşturma sorumluluğunu da gözetir.

Hayatta Kalan Odaklı Yaklaşım

Hayatta kalan odaklı yaklaşım, teknoloji destekli cinsel şiddet dâhil olmak üzere şiddet deneyimi yaşayan kişilerin ihtiyaçlarını, güvenliğini, tercihlerini, kişisel sınırlarını ve karar verme haklarını merkeze alır. Destek süreçlerinde kişiyi suçlamamayı, kendi kararlarını vermesine alan açmayı, gizliliğini korumayı ve yeniden zarar görme riskini azaltmayı esas alır. Dijital ortamlarda bu yaklaşım, kişinin onayı olmadan kişisel bilgilerinin paylaşılmamasını, hangi destek sistemlerine başvuracağına kendisinin karar verebilmesini ve dijital güvenliğine ilişkin güncel ve geçerli destek seçeneklerini, kendi ihtiyaçları doğrultusunda değerlendirilmesini de içerir. Şiddete maruz bırakılan kişilerin desteğe ihtiyaç duyabilecekleri konular ve desteği değerlendirme tercihleri farklılaşabileceği için, destek sunan kişi ve kurumların genelleyici ve yargılayıcı olmayan, hak temelli ve kişinin özerkliğine saygılı bir yaklaşım benimsemeleri önemlidir.

Mağdur suçlayıcı tutumlar, şiddete maruz kalan kişilerin davranışlarını, paylaşımlarını, dijital ortamlardaki varlıklarını veya verdikleri tepkileri sorgulayarak sorumluluğu şiddeti uygulayandan uzaklaştırabilir ve kişilerin destek aramasını zorlaştırabilir. Türkiye'de şiddet deneyimi yaşayan kişilerin başvurdukları mekanizmalarda ve toplumsal söylemde mağdur suçlayıcı tutumların yeterince aşılmamış olması, hayatta kalan odaklı yaklaşımın benimsenmesini ve yaygınlaştırılmasını daha da önemli kılar.

Travma Bilgili Yaklaşım

Travma bilgili yaklaşım, zorlayıcı ve kişiyi tehdit altında hissettiren deneyimlerin kişiler üzerindeki olası etkilerini gözeterek güven, seçim ve kontrol hakkı, güçlenme ve ihtiyaca uygun desteği esas alan bir yaklaşımdır.

Teknoloji destekli cinsel şiddet bağlamında bu yaklaşım; kişilerin yaşadıklarını anlatmaya veya kanıtlamaya zorlanmamasını, dijital mahremiyetlerinin ve kişisel verilerinin korunmasını, yeniden travmatizasyona yol açabilecek uygulamalardan kaçınılmasını gerektirir. Kişilerin yaşadıklarını anlatmakta zorlanmaları, kararsız görünmeleri veya destek aramayı ertelemeleri yargılanmadan karşılanmalıdır.

Travma bilgili yaklaşım yalnızca hayatta kalan kişilerle kurulan iletişimi değil, bütün destek sisteminin güvenli, erişilebilir ve güçlendirici biçimde yapılandırılmasını kapsar. Bu kapsamda **destek sunan kişilerin de desteklenmesi** temel bir ilkedir. İkincil travmatizasyon ve duygusal yük riskleri gözetilerek destek sunan kişilere düzenli süpervizyon, dayanışma, psikososyal destek ve uygun çalışma koşulları sağlanmalıdır. Böylece hem hayatta kalan kişilerin hem de onlara destek sunanların ihtiyaçlarını gözeten sürdürülebilir bir destek sistemi oluşturulabilir.

Dijital Adalete ve Desteğe Erişim

Teknoloji destekli cinsel şiddete maruz bırakılan kişilerin, haklarını arayabilmeleri, yaşadıkları şiddeti bildirebilmeleri, adalete erişebilmeleri ve ihtiyaç duydukları desteğe ulaşabilmeleri için güvenli, erişilebilir, kapsayıcı ve etkili mekanizmaların sunulmasını ifade eder. Bu yaklaşım, hayatta kalan kişinin ihtiyaçlarını, tercihlerini, haklarını ve kararlarını merkeze almayı; destek ve başvuru süreçlerinde kişinin iradesine, özerkliğine ve özne olma hâline saygı göstermeyi esas alır.

Platformların şikâyet ve içerik kaldırma mekanizmaları, hukuki ve psikososyal destek hizmetleri, dijital güvenlik desteği, ilgili kurumlara güvenli yönlendirme süreçleri ve adli başvuru yolları bu kapsamda değerlendirilir. Dijital adalete ve desteğe erişim, yalnızca başvuru kanallarının varlığını değil, bu kanalların hayatta kalan odaklı ve travma bilgili bir yaklaşım doğrultusunda ayrımcılıktan uzak, ücretsiz veya karşılanabilir, zamanında yanıt veren, erişilebilir ve hayatta kalanların farklı ihtiyaçlarını gözeten bir biçimde işlemesini de içerir.

Koruyucu ve Dönüştürücü Yaklaşımlar

4

Tasarım Aşamasında Güvenlik

Safety by Design

Tasarım aşamasında güvenlik (Safety by Design), dijital platformların ve teknolojik ürünlerin geliştirilmesinden itibaren güvenliğin ve olası zararların önlenmesinin tasarım süreçlerine dâhil edilmesini esas alan yaklaşımdır. Amaç, çevrim içi şiddet ve istismar risklerini erken aşamada öngörmek ve önlemek; güvenlik sorumluluğunu yalnızca kullanıcılara bırakmayarak teknoloji şirketlerinin sorumluluğunu ve hesap verebilirliğini güçlendirmektir. Toplumsal cinsiyete dayalı dijital şiddet bağlamında bu yaklaşım; onay dışı görüntü paylaşımını önleyici mekanizmalar geliştirmek, taciz ve tehditleri bildirmeyi kolaylaştırmak ve kişisel bilgileri korumak gibi uygulamaları kapsar. Cinsel şiddet alanında koruyucu ve önleyici yaklaşımın bir örneği olan tasarım aşamasında güvenlik, zarar ortaya çıktıktan sonra müdahale etmekle yetinmeyip olası zararları tasarımın her aşamasında gözetmeyi ve önlemeyi amaçlar.

Güvenlik önlemlerinin geliştirilmesinde, özellikle çocukların, gençlerin ve dijital şiddetten etkilenen kişilerin deneyimlerinin ve ihtiyaçlarının dikkate alınması; güvenliğin katılım, erişilebilirlik, özel hayat ve ifade özgürlüğü haklarıyla birlikte ele alınması önemlidir.

Dijital Platformların Hesap Verebilirliği

Dijital platformların hizmetlerinde ortaya çıkan şiddet ve zarar risklerini önleme, kullanıcıların bildirimlerini değerlendirme ve gerekli müdahaleleri yapma sorumluluğunu ifade eder.

Toplumsal cinsiyete dayalı dijital şiddet bağlamında bu sorumluluk; onay dışı cinsel içeriklerin bildirilmesi ve kaldırılması için etkili mekanizmalar oluşturmayı, kullanıcıların güvenliğini gözetmeyi ve alınan kararlar konusunda şeffaf olmayı kapsar. Örneğin: içerik moderasyonu, yaş doğrulama ve görüntü parmak izi (hash) eşleştirme teknolojileri gibi. Bu mekanizmaların erişilebilir olması, başvuruların sonuçları hakkında kullanıcıların bilgilendirilmesi ve platform kararlarına karşı etkili itiraz yollarının bulunması da hesap verebilirliğin parçasıdır.

Dijital şiddetle mücadele sorumluluğu yalnızca kullanıcılara yüklenemez; platformların da güvenli bir dijital ortam oluşturma ve uygulamalarının sonuçları konusunda hesap verme sorumlulukları vardır.

Toplumsal Fayda için Teknoloji

Tech for Good

Toplumsal fayda için teknoloji, teknolojinin toplumsal sorunları çözmek, insan haklarını desteklemek ve toplumsal eşitliği güçlendirmek amacıyla kullanılmasını ifade eder.

Toplumsal cinsiyete dayalı şiddetle mücadelede güvenli başvuru mekanizmaları geliştirmek, şiddete maruz bırakılanların destek hizmetlerine erişimini kolaylaştırmak, dijital dayanışma ağları oluşturmak ve şiddet içeriklerinin bildirilmesini sağlayan araçlar geliştirmek bu yaklaşımın örnekleridir. Bu yaklaşım, teknolojinin yalnızca zararları önlemek için değil, güvenliği, dayanışmayı ve haklara erişimi güçlendirmek için de kullanılabileceğini vurgular.

Teknolojinin toplumsal fayda sağlaması, erişilebilirlik, kişisel bilgilerin korunması, kapsayıcılık, ayrımcılık karşıtlığı ve şiddete maruz bırakılanların ihtiyaçlarını ve haklarını merkeze alan bir yaklaşımın benimsenmesine, uygulanmasına ve ihtiyaca bağlı olarak düzenli olarak güncellenmesine bağlıdır.

Feminist Teknoloji ve Feminist İnternet

Feminist teknoloji yaklaşımı, teknolojinin tasarım, geliştirme ve kullanım süreçlerinde toplumsal cinsiyet eşitsizliklerini yeniden üretmemesini; kadınların, LGBTİ+'ların, gençlerin ve farklı toplumsal grupların ihtiyaç, deneyim ve bilgi birikimlerinin merkeze alınmasını savunur. Feminist internet ise internetin toplumsal cinsiyet eşitliğini, insan haklarını, ifade özgürlüğünü ve herkesin dijital yaşama eşit ve güvenli katılımını desteklemesini savunan yaklaşım ve ilkeler bütünüdür.

Onay, mahremiyet, veri güvenliği, anonimlik, ifade özgürlüğü, dayanışma ve şiddetle mücadeleyi bu yaklaşımın temel unsurları olarak görüyoruz. Cinsel şiddet ve teknoloji destekli cinsel şiddetle mücadelede kişilerin bedenleri, cinsellikleri ve kişisel bilgileri üzerindeki haklarını korumayı; hayatta kalanların güvenliğini, özerkliğini ve dayanışma ağlarını güçlendirmeyi önemsiyoruz.

Teknolojiye yalnızca bir iletişim aracı olarak değil, güç ilişkilerinin, eşitsizliklerin, hak ihlallerinin ve direniş biçimlerinin üretildiği bir alan olarak yaklaşıyoruz. Bu nedenle teknolojinin feminist ilkeler doğrultusunda geliştirilmesini, kullanılmasını ve değerlendirilmesini; hayatta kalanların bu süreçlerde söz ve karar sahibi olmasını ve daha adil dijital alanların oluşturulmasını savunuyoruz.

YARARLANILABİLECEK KAYNAKLAR

Cinsel Şiddet Kavramlar Sözlüğü
Cinsel Şiddetle Mücadele Derneği

Çevrim İçi Cinsel Şiddet Hakkında Hukuki Bilgiler
Cinsel Şiddetle Mücadele Derneği

Kadınlara Ve Kız Çocuklarına Yönelik Teknoloji Destekli Şiddet Alanında Küresel Önleme Ve Müdahale Eğilimleri: Gelişen Uygulamalar Derlemesi
Un Women, SVRI

Dijital Şiddet / Teknoloji Destekli Cinsiyete Dayalı Şiddet Rehberi
UNFPA, UN Women

Cinsiyetci Dijital Şiddetle Mücadele Rehberi
Alternatif Bilişim

İnternetin Feminist İlkeleri
Association for Progressive Communications (APC)

bloom.chayn.co/tr
Bloom, Chayn.

Bloom, travma ve toplumsal cinsiyete dayalı şiddete dair bilgileri travmadan iyileşmeye yardımcı olan terapötik uygulamalarla birleştiren uzaktan kurslar sunarak hayatta kalanları bilgilendirir ve güçlendirir.

stopncii.org

Onay dışı kişisel görüntü paylaşımına maruz bırakılan kişilere destek olmak için tasarlanmış ücretsiz bir araçtır.

cs_mucadele

csmd_mucadele

cinselsiddetlemucadele

Cinsel Şiddetle Mücadele Derneği