CİNSİYETÇİ DİJİTAL ŞİDDETLE MÜCADELE REHBERİ

Genişletilmiş 2. Baskı

T·B·İ·D
Toplumsal Bilgi ve İletişim Derneği

alternatif bilişim

Avrupa Birliği sivil düşün

Hazırlayanlar:

Gülüm Şener
İlden Dirini
Nurcihan Temur
Şebnem Ahi
Şevket Uyanık
Zeynep Özarslan

Tasarım:
Fatih Akdoğan

Aralık, 2022

Bu e-rehber, Avrupa Birliği Sivil Düşün Programı kapsamında Avrupa Birliği desteği ile hazırlanmıştır. İçeriğin sorumluluğu tamamıyla TBİD ve AltBil'e aittir ve AB'nin görüşlerini yansıtmamaktadır."

İçindekiler

1. TOPLUMSAL CİNSİYETE DAYALI DİJİTAL ŞİDDET NEDİR?

İnternete erişimin artması ile birlikte mobil bilgi ve sosyal medyanın yaygın kullanımı toplumsal cinsiyete dayalı şiddetin yeni bir biçimi olan dijital şiddeti karşımıza çıkarmaktadır.

Sosyal medyada, internet ağlarını kullanmada aktif olan kadınlar, cinsiyetlerine, cinsiyet kimliklerine, güvenliklerine doğrudan saldıran tehdit veya yorumlar ile karşılaşmaktadır.

Kadınlara ve kız çocuklarına yönelik şiddet, kadının insan hakları ihlali ve kadına yönelik ayrımcılığın bir biçimi olarak değerlendirilmektedir. İstanbul Sözleşmesi'nde[1] şiddet, yalnızca fiziksel değil, cinsel, psikolojik ve ekonomik biçimleri ile ele alınmış ve toplumsal cinsiyete dayalı eşitsizliğin sonuçları bağlamında değerlendirilmiştir.

Toplumsal cinsiyete dayalı şiddet genel bir kavram olarak ev içi şiddeti, eş/partner şiddetini, flört şiddetini ve dijital şiddeti kapsamaktadır.

Toplumsal cinsiyete dayalı dijital şiddet herhangi bir şiddet türünün altında değerlendirilmemektedir. Bütün şiddet türlerinin kesişen örnekleri olması nedeni ile yeni bir tür ya da biçim olarak değerlendirilmesi önerilmektedir.

Toplumsal cinsiyete dayalı dijital şiddet, dijital alanlarda gerçekleşen, cinsiyetimizden / cinsiyet kimliklerimizden dolayı yöneltilen ve bizi orantısız bir biçimde etkileyen şiddettir.

[1] İstanbul Sözleşmesi, E. (2011). Kadına Yönelik Şiddet ve Aile İçi Şiddetin Önlenmesi ve Bunlarla Mücadeleye Dair Avrupa Konseyi Sözleşmesi-İstanbul Sözleşmesi. İstanbul Sözleşmesi. https://rm.coe.int/1680462545

Tanımlayıcı Özellikler

"Dijital Mekanlardan Sesler: Kadınlara Yönelik Teknolojik Şiddet" çalışmasında[2] kadınlara yönelik dijital şiddetin tanımlayıcı beş özelliği sıralanmıştır:

- **Anonimlik;** taciz uygulayan fail, şiddete maruz bırakılan tarafından tanınmayabilir.
- **Eylem mesafesi;** istismar fiziksel temas olmadan ve herhangi bir uzaklıktaki yerden yapılabilir.
- **Otomasyon;** teknoloji aracılığı ile yapılan taciz eylemleri daha az zaman ve emek gerektirir.
- **Ulaşılabilirlik;** birçok teknolojinin çeşitliliği ve ekonomik olarak uygunluğu, kadınları failler tarafından kolaylıkla erişilebilir hale getirir.
- **Yayılma ve süreklilik;** internet ortamında çoğaltılan metinler ve fotoğraflar, sınırsız olarak yayılır veya uzun süre ortamda kalır.

Çevrimiçi Şiddet: Çevrimdışı Şiddetin Devamı

Kadınlar, toplumsal cinsiyete dayalı eşitsizliklerden dolayı çevrimdışı hayat şiddetin farklı biçimlerine maruz kalmaktadır. Aynı eşitsizlikler sanal hayatlarda da (çevrimiçi hayat) kadınları (farklı kadınlık halleri ile birlikte) hedef almakta ve onların güvenliklerini tehdit etmektedir.

Dijital şiddetin "çevrimdışı" dünyada yaşanan şiddetten ayrı bir kavram olmadığı ve çevrimdışında yaşanan şiddetin (ev içi şiddet, kadına yönelik şiddet) bir devamı olduğu ve aynı eşitsizliklerden beslendiği unutulmamalıdır.

Toplumsal cinsiyet kalıp yargılarını içeren çevrimdışı ortamlardaki eşitsizlik ve cinsiyetçilik çevrimiçi alanlara da yansıtılmaktadır.

Dijital Şiddet mi? Siber Şiddet mi? Sanal Şiddet mi? Çevrimiçi Şiddet mi?

Konu ile ilgili araştırmalar ve raporlar incelendiğinde kadınların maruz kaldığı dijital şiddet tam olarak kavramlaştırılamamıştır. Konu farklı üst başlıklarda karşımıza çıkmaktadır: siber şiddet, sanal şiddet, dijital şiddet veya çevrimiçi şiddet...

Konu ile ilgili çalışmalar arttıkça kavramlar tam olarak belirlenecektir, ancak tanımlamaların feminist bir perspektifle değerlendirilmesi çok önemlidir. Farklı kurum ve kuruluşlar bu benzer ve yakın anlamlı kavramlar için farklı kavramlar kullanmayı tercih edebilmektedir. Bu konudaki bilimsel çalışmalar arttıkçe kavramlar üzerindeki uzlaşı da artacaktır.

[2] Fascendini, F., & Fialová, K. (2011). Voices from digital spaces: Technology related violence against women. Association for Progressive Communications (APC)

Dijital Şiddete Maruz Kalanlar

Çevrimiçi kötüye kullanım sonucu cinsiyete dayalı şiddet, erkek veya kadınlara yönelik olabilmektedir. Aynı şekilde, erkekler ve çocuklar da çevrimiçi istismar ve şiddete maruz kalabilirler. Bununla birlikte, çevrimiçi kötüye kullanım ve cinsiyete dayalı şiddet diğer toplumsal cinsiyete dayalı şiddet şekilleri ile aynı mevcut yapısal eşitsizliklerden ve ayrımcılıktan kaynaklandığından kadınların maruz kaldığı şiddet oranları daha fazladır. [3]

BM "Kadınlara ve Kız Çocuklarına Yönelik Siber Şiddet - Dünya Geneli Acil Eylem Çağrısı" raporundaki[4] verilere göre tüm dünyada kadınların çevrimiçi şiddete maruz kalma ihtimali erkeklere oranla 27 kat daha fazladır ve diğer her alan gibi internet de toplumsal cinsiyete dayalı şiddetin söz konusu olduğu bir alandır.

Toplumsal Bilgi ve İletişim Derneği ve KONDA'nın beraber yürüttüğü "Türkiye'de Dijital Şiddet Araştırması"nın[5] sonuçlarına göre:

- Türkiye'de her beş kişiden biri dijital şiddete uğruyor.
- Dijital şiddete en çok gençler maruz kalıyorlar. 15-17 yaş arası her beş gençten biri, 18-32 yaş arası her üç gençten biri dijital şiddete maruz kalıyor. 15-17 yaş arası gençler en çok fiziksel görünümleri ve yaşları nedeniyle, 18-32 yaş arası gençler ise cinsiyeti, siyasi görüşleri ve fiziksel görünümleri nedeniyle dijital şiddete maruz kaldıklarını ifade ediyorlar.
- Kadınlar cinsiyetlerinden (%52) ve fiziksel görünümlerinden (%21) ötürü, erkekler siyasi görüşlerinden (%30) dolayı daha fazla dijital şiddete uğradıklarını dile getiriyorlar. Türkiye'de her 10 kadından biri akrabaları tarafından dijital şiddet görüyor.
- Kadınların % 51'i dijital ortamlarda yazılı, sesli veya görüntülü taciz mesajları alıyor, % 46'sı ısrarlı takibe uğruyor.
- Dijital şiddet eylemlerinin en çok gerçekleştiği platformlar Instagram (%53), Facebook (%35) ve Twitter (%19).
- Kişiler, dijital platformlarda en çok tanımadıkları kimseler ve troller tarafından şiddete maruz bırakıldıklarını ifade ediyorlar.
- Toplumun karşılaştığı dijital şiddetin türleri incelendiğinde, çoğunluğun hakaret, küfür ve tehdide, taciz mesajlarına ve ısrarlı takibe maruz kaldığı görülüyor.
- Dijital şiddetle başa çıkmak için en sık başvurulan yöntemler ise bloklamak/engellemek (% 65) ve uygulama içinde şikayet etmek (%39).

[3] IGF. (2015). Internet Governance Forum-Best Practice Forum on Online Abuse and Gender-Based Violence Against Women.

[4] UN. (2015). Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call. http://www.unwomen. org/-/media/headquarters/attachments/sections/library/

[5] TBİD. (2021). Türkiye'de Dijital Şiddet Araştırması. https://dijitalsiddet.org/dijital-siddet-raporu/

Kesişen ayrımcılık ve farklı kadınlık hallerini etkileyen dijital şiddet

Kadınlar; eğitimi, yaşı, etnik kökeni, cinsel yönelimi veya ilişki durumu nedeniyle çeşitli dijital şiddet içeren davranışlara maruz kalma riskiyle karşı karşıya kalabilirler.

"Toplumsal Cinsiyete Dayalı Şiddet ve Çevrimiçi İstismar" raporunda[6] çevrimiçi veya çevrimdışı ortamlarda öne çıkan kadınlara, çevrimiçi alanda daha fazla suistimale maruz kalabilecekleri çıktısı yer alır. LBTQ+ kadınlar, kadın gazeteciler (blog yazarları dahil), teknoloji endüstrisinde aktif olan kadınlar, tanınmış kadınlar (sanatçılar, yazarlar vb.), kadın siyasetçiler, kadın akademisyenler ve feminist aktivistler de dönem dönem dijital şiddet faillerinin açık hedefi haline gelebilmektedir.

Dijital Şiddeti Uygulayan Fail Kim?

Dijital şiddeti uygulayan kişi eski ya da şu anki eş / partner, komşu, iş / okul arkadaşı, bir yakın ya da bir yabancı olabilmektedir.

Dijital şiddet eylemleri, sosyal medya ve mesajlaşma platformları, uygulamalar, oyunların sohbet odaları, forumlar ve e-posta gibi Bilgi ve İletişim Teknolojileri'nin (BİT) kullanılmasıyla gerçekleşir. Failler genellikle kontrolü sürdürme konusunda çok kararlıdır ve teknoloji bunu yapmak için kullandıkları birçok araçtan sadece biridir.[7]

Çevrimiçi kötüye kullanım ve cinsiyete dayalı şiddetin büyük bir kısmı adsız hesaplar veya takma adlar veya sahte isimler içeren hesaplar kullanarak gerçekleştirilmektedir ve bu da olayın faillerini belirlenmesini zorlaştırmaktadır.

[6] a.g.e.

[7] UN Women (2020). Toplumsal Cinsiyete Dayalı Siber Şiddet Rehberi https://2020.atesbocekleri.info/

2. DİJİTAL GÜVENLİK ÖNERİLERİ

Bu bölümde isimleri anılan yazılım ve uygulamalar rehberin hazırlandığı esnada güncelliği ve güvenilirliği kontrol edilerek rehbere dahil edilmiştir. Okuyucunun uygulamaları kullanmadan önce verilen web sitelerini ziyaret edip son güncel bilgilere göz atmasını öneririz.

Dijital ortamlarda yüzde yüz güvenlikten söz etmek mümkün olmasa da bu araçların daha güvenli kullanımı mümkündür. Kullanıcılar dijital okuryazarlıklarını geliştirerek, doğru yöntemleri ve araçları kullanmayı öğrenerek farklı düzeylerde güvenliklerini sağlayabilirler.

Dijital Ayakizim

İnternet kullanıcılarının her hareketi, her tıklaması daha sonra kullanılmak üzerine kayıt altına alınmakta, kişisel bilgiler ticari kuruluşlar için kârlı verilere dönüşmektedir. Gündelik çevrimiçi aktivitelerimiz sırasında birçok dijital iz bırakırız.

Günümüzde basit bir Google aramasıyla herhangi biri sizin hakkınızda birçok bilgi elde edebilir. Bu teknik bir uzmanlık gerektirmez. Başta sosyal ağlar olmak üzere dijital ortamlarda yaptığınız gönüllü paylaşımlar, günlük rutinleriniz, özel bilgileriniz, kişiliğiniz, duygu durumunuz ve sosyal yaşantınız hakkında çok sayıda bilgi içerir. Kötü niyetli kişiler ya da gruplar bu bilgileri toplayarak size zarar verebilirler.

İnternet Güvenliği

- **Gizli modda** açtığınız bir tarayıcı da kişisel bilgilerinizi aratabilir, çıkan sonuçları analiz edebilir, **sizinle ilgili hangi bilgilerin herkesin erişimine açık olduğunu tespit edebilirsiniz.**

- Kullandığınız cihazlarda sık sık **çerezler** ve **geçmiş bölümlerini** temizleyin. Kendinize ait bir cihazda işlem yapıyorsanız "Gizli modda" işlem yapmayı tercih edin.

- Sosyal medya profillerinizin 'Ayarlar' bölümünden paylaşımlarınızın kimler tarafından görülebileceği ve kişisel verilerinizin internet ortamında açık bir şekilde paylaşılıp, paylaşılmasını sınırlandırabilirsiniz. Ayrıca hesabınıza erişen 3. taraf uygulamaları düzenleyebilirsiniz.

- Google, Facebook, Instagram, Twitter gibi platformlardan sizinle ilgili kaydettikleri bilgileri isteyebilir, bilgisayarınıza indirebilirsiniz. Böylelikle bugüne kadar bu hesapları kullanarak yaptığınız etkinlikleri görebilir, arşivleyebilirsiniz. Ancak verilerinizi indirmeniz internetten silinmesini sağlamaz.

Google verilerinizi indirmek için:
https://takeout.google.com/

Facebook verilerinizi indimek için:
https://www.facebook.com/help/212802592074644

Twitter verilerinizi indirme:
https://help.twitter.com/tr/managing-your-account/how-to-download-your-twitter-archive

Instagram verilerinizi indirme:
https://www.instagram.com/download/request

Linkedin verilerinizi indirme:
https://www.linkedin.com/psettings/member-data

Bağlantı Güvenliği

- İnternet kafeler, çıktı almak veya e-mail göndermek amacıyla bilgisayar kullandığınız kırtasiyeler, fotokopi merkezleri gibi herkesin erişimine açık mekanlardaki cihazlarda kişisel parolanızı kullanmayın, e-alışveriş yapmayın. Tanımadığınız cihazlarda e-posta veya sosyal medya hesaplarınıza parolanızla giriş yaptıysanız işinizi bitirdikten sonra **hesabınızdan çıkış yapmayı unutmayın.**

- Kamuya açık kablosuz ağlar (WIFI) üzerinden başta parolalarınız olmak üzere kişisel verilerinizin ele geçirilme ihtimali vardır. Şifrelenmemiş bağlantıları kullanmamaya çalışın.

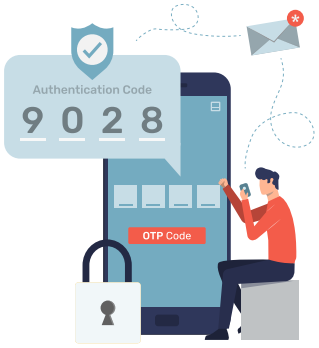
Cihaz Güvenliği

- Kullandığınız cihazlara (bilgisayar, tablet, cep telefonu vs.) başkalarının erişimini engellemek için mutlaka **parola koyun** veya **ekran kilidini etkin hale getirin.**

- Kullandığınız dijital cihazlar ve içerisindeki veriler size aittir. Başkalarının cihazlarınızı kullanmaya, parolanızı istemeye ve cihazınızdaki bilgileri kontrol etmeye hakkı yoktur.

- Sağlıklı bir ilişkide taraflar birbirini kısıtlama ve denetleme ihtiyacı duymazlar. Partnerinizin gittiğiniz her yerden konum atmanızı, fotoğraf çekip göndermenizi, her mesajına hemen yanıt vermenizi beklemesi "ısrarlı takip" göstergesidir.

Parola Güvenliği



- İnternette ve dijital cihazlarınızda kullandığınız parolalarınız, **basit ve kolay tahmin edilebilir olmamalıdır.** İsim, doğum tarihi, kimlik numarası, evlilik yılı, telefon numarası vs. bilgiler içermemelidir.

- Parolalarınızda yakınınızdaki kişilerin tahmin edebileceği özel bilgilerinizi kullanmamaya özen gösterin. Partneriniz, eşiniz, yakınınız, arkadaşınız vb. parolanızı öğrenip internette başkalarıyla iletişiminizi denetlemek isteyebilir. Parolanız size özeldir, sizin dışınızda kimsenin parolanızı bilmeye hakkı yoktur.

- Anlamlı bir bütün oluşturmayan, içinde hem rakam, hem büyük/küçük harf, hem de işaret içeren parolalar tercih edin. Örnek: N/1i2*H3-a4!X8

- Kullandığınız tüm hizmetler, web siteleri, sosyal medya platformları için **ayrı parolalar belirleyin.** Aynı parolayı birçok site için kullanmayın. Saldırıya uğrayıp kullanıcı verilerine erişen bir platformdan sızan parolanızın, e-posta veya sosyal medya hesaplarınıza giriş için kullanılmasını istemezsiniz. En az 6 ayda bir parolanızı yenileyin.

- Parola için güvenlik sorularınıza verdiğiniz yanıtlar "gerçek" olmasın. Örneğin ilk evcil hayvanınızın adını soru olarak seçtiyseniz yanıtınız gerçekte hayvanınızın adı olmamalı, çünkü başkaları tarafından kolay tahmin edilebilir. Benzer şekilde sosyal medyada paylaştığınız bilgiler üzerinden de tahmin edilebilir.

- Tüm parolaları hatırlamak zor olacaktır. Parolalarınızı saklamak ve yönetmek için **parola yöneticisi** kullanın. Bilgisayarınız için açık kaynaklı ve ücretsiz iki yazılımdan yararlanabilirsiniz: **keepassxc.org** ve **bitwarden.com**, IOS ve Android cihazlarınız için ise keepassdx.com, bitwarden.com, strongboxsafe.com ve keepassium.com adreslerinden edineceğiniz uygulamaları kullanabilirsiniz. Böylece tek bir ana parolayla tüm parolalarınızı güvenli bir şekilde saklayabilir ve erişebilirsiniz.

- **İki adımda doğrulama uygulamasını** mutlaka kullanın. E-posta veya sosyal medya hesaplarınıza giriş yaparken iki aşamalı doğrulama yöntemini uygulayarak hesabınızı koruma altına alabilirsiniz. İki adımda/iki faktörlü doğrulama uygulamasını kullandığınızda hesabınıza başka bir cihazdan giriş yapmak isteyen biri olursa sistem size bir uyarı mesajı göndermektedir. Böylece, eğer iki adımda doğrulamayı aktifleştirdiyseniz başka bir cihazdan bağlanan biri sizin parolanızı bilse dahi

hesabınıza ulaşamayacaktır. Kullandığınız sosyal ağ ve e-posta hizmet sağlayıcılarının Ayarlar/Güvenlik Ayarları bölümlerinden iki adımda doğrulama uygulamasını etkin hale getirebilirsiniz.

Sosyal Medya Güvenliği

- Sosyal medya platformlarının **Kullanıcı Sözleşmeleri**'ni ayrıntılı bir şekilde okuyarak paylaştığınız bilgilerin hizmet sağlayan platformun yanı sıra hangi taraflarla paylaşıldığını, kimlerin erişimine açık olduğunu kontrol edebilirsiniz. Birçoğumuzun okumadan onay verdiği Kullanıcı Sözleşmeleri'nde verilerin ticari kuruluşlarla paylaşılması için izin verilebilir şeklinde maddeler yer alabilir.

- Sosyal medya profilinizi ve paylaşımlarınızı kimlerin görebileceğini **Gizlilik Ayarları/Güvenlik Ayarları** bölümlerinden kontrol edebilir ve sınırlandırabilirsiniz. Bunun için hesabınız olan sosyal medya platformlarının Gizlilik Ayarları/Güvenlik Ayarları kısmını ziyaret ederek paylaştığınız bilgilerin gizliliğini ayrıntılı şekilde düzenleyebilirsiniz.

- Facebook'ta **Zaman Tüneli Onayı** ve **Etiketlendiğin Gönderiler Onayı** özelliklerini etkin hale getirirseniz arkadaşlarınız veya tanıdıklarınız sizi bir gönderide etiketlendiğinde veya zaman tünelinizde bir şey paylaşmak istediklerinde onayınız gerekecektir.

- Sizi rahatsız eden mesajlar/bildiriler aldığınızda sosyal medya platformlarının sunduğu **Bildir/Şikayet et** özelliğini kullanabilir, dijital şiddet uygulayan faili **engelleyebilir, hesabının kapatılmasını sağlayabilirsiniz.**

- Doğrudan size yönelik olmasa da **başka kullanıcılara yönelik** ayrımcı, cinsiyetçi yorumları, nefret söylemi içeren paylaşımları da sosyal medya platformlarına bildirerek dijital tacizle mücadeleye katkı sağlayabilirsiniz.

- Facebook'un **izinsiz paylaşılan mahrem görüntülerle** ilgili destek merkezinden yardım alabilirsiniz: https://www.facebook.com/safety/notwithoutmyconsent

- Sosyal medyada tanıdığınız veya tanımadığınız bir kişi, kişiler ya da gruplar tarafından hedef gösterilirseniz, küçük düşürücü, hakaret içeren, itibarsızlaştırıcı vb. mesajlara maruz kalırsanız ekran görüntüsünü alarak kanıt toplayıp hukuki süreçlere başvurabilirsiniz. Ekran görüntüsünde gönderenin adının, tarih ve saatin yer aldığına dikkat edin. Hukuki süreçler için barolardan avukat desteği talep edebilir, toplumsal cinsiyet ve kadın hakları alanında çalışan sivil toplum kuruluşlarıyla, merkezlerle iletişime geçerek bilgi alabilirsiniz.

- Kullandığınız bütün sosyal medya platformlarının (Twitter, Facebook, Instagram, Linkedin, Youtube vs.) uygulamalar bölümünde sizin bilginiz dahilide veya dışında kurulmuş birçok uygulama görebilir siniz. Bunların görevi sizin yerinize mesajları okuyup yazma, sizin yerinize mesaj atma vs. olabilir. Bu uygulamalardan kullanmadıklarınızı mutlaka kaldırın.

- Sosyal medya kişilerarası takibi kolaylaştırır ve kişilerin takıntılarını besleyebilir. Fail, onu engellemediğiniz sürece sizin sosyal medyadaki aktivitelerinizi takip edebilir, konumunuzdan veya paylaştığınız görüntüler aracılığıyla nerede olduğunuzu anlayabilir, sizin hakkınızda bilgi edinerek sizi kontrol etmeye çalışabilir. Kendinizi tehdit altında hissediyorsanız faili **bloklayarak, tüm iletişim ortamlarından silerek** ve **"sıfır iletişim"**le kendinize görece güvenli bir iletişim ortamı yaratabilirsiniz.

- Fail, sosyal medyada arkadaşlarınızla arkadaşlık kurarak da sizi takip etmeye çalışabilir. Bunun için arkadaşlarınızla konuşarak onları durumdan haberdar edebilir, sizinle ilgili hiçbir bilgiyi paylaşmamalarını ve size destek olmalarını talep edebilirsiniz.
- Takip edildiğinizden şüpheleniyorsanız mümkün olduğunca **yer bildirimi** yapmaktan kaçının, yer bildirimi/konum geçmişinizi kullandığınız cihazlardan düzenli olarak temizleyin.

- Güvenli bir ilişkide partneriniz sosyal medyada ne paylaşacağınıza ve kimlerle arkadaşlık kuracağınıza karışmaz. Sosyal medya profiliniz size özeldir ve içerikler sizin kontrolünüzde olmalıdır.

- Sosyal medya platformlarının dijital taciz/çevirimiçi şiddete karşı güvenlik önerileri için aşağıdaki bağlantıları ziyaret edebilirsiniz:

Google:
https://learndigital.withgoogle.com/dijitalatolye/course/online-safety/module/3000

Facebook:
https://www.facebook.com/safety/bullying

Twitter:
https://help.twitter.com/tr/safety-and-security/cyber-bullying-and-online-abuse

Linkedin:
https://www.linkedin.com/help/linkedin/answer/43796/taciz-veya-guvenlik-endisesi?lang=tr

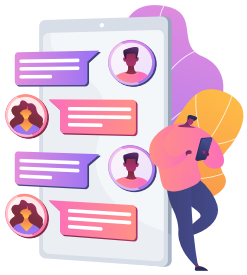
Youtube:
https://www.youtube.com/intl/tr_cy/howyoutubeworks/policies/community-guidelines/

E-posta Güvenliği

- Kimden geldiğini bilmediğiniz, hediye, fırsat vs. kazandığınızı belirten jenerik özel mesajlara veya e-postalara tıklamayın, bunlar virüs içeriyor olabilir, kişisel verileriniz çalınabilir.

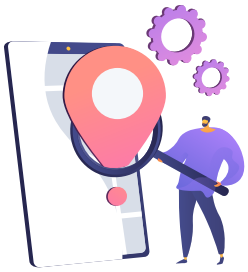
- **PGP** (Pretty Good Privacy), **TutaNota.de, ProtonMail** gibi yazılımlarla e-postalarınızı şifreleyerek güvenli bir şekilde gönderebilirsiniz.

- **RiseUp** vb. alternatif e-posta hizmetlerinden e-posta adresi alabilir, e-posta grupları oluşturabilir ve daha güvenli iletişim sağlayabilirsiniz.



Güvenli Mesajlaşma

- Whatsapp, Telegram yerine daha güvenli mesajlaşma uygulaması olan **Signal**'ı kullanabilirsiniz. **Signal** uçtan uça şifreleme, kısa mesajlarınızı da (sms) şifreli bir şekilde yollama, okunduktan sonra konuşmalarınızı da tüm sunuculardan temizleme ve iki adımda doğrulama imkanları sunmaktadır.



Arama Motoru Güvenliği

• Google gibi ticari bir arama motoru yerine **DuckDuckGo** gibi alternatif ve kişisel bilgilerinizi takip edip ticarileştirmeyen arama motorlarını tercih edebilirsiniz.

Web Sitesi Güvenliği

• Başında **http://** olan web sitelerini değil, daha güvenli olan **https://** ile başlayan web sitelerine girmeyi tercih edin.

• Web tarayıcınıza uBlock Origin ve Electronic Frontier Foundation tarafından üretilen **HTTPS Everywhere**, **PrivacyBadger** eklentilerini ekleyerek daha güvenli ve ticari reklamlardan, çerezlerden uzak bir iletişim sağlayabilirsiniz.

• Bir arkadaşınızdan ya da tanımadığınız bir internet kullanıcısından size gönderilen bir bağlantıyı açmadan önce sitenin güvenilir olup olmadığını, **phishtank.com** veya **urlex.org** gibi web sitelerine girerek doğrulayabilirsiniz.

Metaverileri Silmek

• Cep telefonunuzda fotoğraf veya video çekerken geotag (coğrafi etiket) özelliğini kapatmaya özen gösterin.

• Cep telefonlarınız için Simple Gallery ve benzeri uygulamalar edinebilirsiniz. **https://simplemobiletools.com/**

Özgür Yazılım

Gözetimi azaltmanın yollarından bir tanesi de kapalı kaynak sahipli yazılımlar yerine kodları açık özgür yazılımlar kullanmaktır. Bu yazılımların cihazımızda hangi verilere erişip nasıl kullandığı denetlenebilirdir. Bu sebeple daha güvenlidir.

Android telefonlarda Google Play üzerinden **F-Droid** adlı uygulamayı indirerek halihazırda kullandığınız uygulamaların açık kaynaklı muadillerini bulabilirsiniz.

3. DİJİTAL ORTAMLARDA TACİZLE BAŞA ÇIKMA YÖNTEMLERİ

Dijital şiddetin failleri genellikle kontrolü sürdürmek konusunda çok kararlıdır ve teknoloji bunu yapmak için kullandıkları birçok araçtan biridir. Failin sizinle ilgili çok fazla bilgisi var gibi görünüyorsa, bu bilgileri cihazlarınızı izleyerek, çevrimiçi hesaplarınıza erişerek, konumunuzu izleyerek veya hakkınızda çevrimiçi bilgi toplayarak bu verileri elde ediyor olabilir.

Çevrimiçi hedef olmak işlerin tamamen kontrolden çıktığını hissetmeye neden olabilir. Kendinizi suçlamadan alınabilecek önlemler vardır. Bunlardan bazıları:

- Failin kimliğini belirlemek için bilgi toplayın ve olayları belgeleyin. Bir dizi olayı belgelemek, polise veya mahkemeye, yasal bir takip veya taciz tanımına uyan bir davranış şekli gösterebilir. Belgeler ayrıca, bu davranışların arttığını görmenize ve güvenlik planlamasında size yardımcı olabilir.

- Ekran görüntüsü alın. Ekran görüntüsü internette topladığınız bilgileri saklamak için çok temel bir araçtır ve işinize yarayabilir.

- Taciz edici davranış çevrimiçi olduğunda, tacizin gerçekleştiği web sitesine veya uygulamaya da rapor edebilirsiniz. Davranış platformun hizmet şartlarını ihlal ederse, içerik kaldırılabilir veya kişi yasaklanabilir. Raporlama içeriğinin tamamen kaldırılabileceğini bilmek önemlidir; bu nedenle kanıt raporlarından önce belgelenmelidir.

- Twitter ve sosyal medya hesaplarından faili teşhir etme kararı alabilirsiniz.
  #tacizvar #tacizesesver #sendeanlat #susmabitsin

- Yaşadığınız süreci güvendiğiniz insanlarla paylaşın, kadın hakları için mücadele eden danışma merkezlerinden destek alın.

- Yasal süreçleri öğrenmek için konu ile ilgili çalışan avukatlar ile görüşün. Baroların Kadın Danışma Merkezleri-Komisyonları ile görüşün.

- En yakın kolluk birimi veya savcılığa suç duyurusunda bulunabilirsiniz. Ayrıca acil önlem alınması gereken bir durum varsa, 6284 sayılı yasada düzenlenen uzaklaştırma kararı alınması gibi önlemlere başvurulmalıdır. Maddi, manevi zarar varsa tazminat davası açılabilir.

- 5651 sayılı yasa gereği içeriklerin kaldırılması talep edilebilir ve ilgili içerikler eleştiri kapsamında değilse ve gerçek bir karara dayanmıyorsa, bu içeriklerle birlikte anılmak istemeyen kişi tarafından unutulma hakkı kapsamında da bu içeriklerin kaldırılması mahkemeden talep edilebilir. Adli yardım koşulları oluşmuşsa, avukat talebinde bulunulabilir.

- Her halükarda, yasalar hakkında bilinçlenmek, hangi eylemin suç olabileceğini bilmek ve mağdurun haklarını bilmesi de büyük önem taşır.

- Dijital ortamlarda kendinize değil de bir başkasına yönelik linç girişimi, cinsiyetçi söylemler, dijital şiddet içeren eylemleri de şikayet edebilir, faillerin hesaplarının kapatılmasına yardımcı olabilirsiniz.

- Cinsiyetçi dijital şiddetle mücadele konusunda farkındalık yaratmak için çevrimiçi/çevrimdışı kampanyalar düzenleyebilir, gündem oluşturabilir, böylece hem teknoloji ve sosyal medya şirketlerinin hem de politikacıların bu konuda çözüm üretmelerini sağlamak üzere dijital aktivizm yapabilirsiniz.

4.DİJİTAL ŞİDDET EYLEMLERİ VE HUKUKİ DÜZENLEMELER

Dijital şiddet eylemi	Hangi suç/yasa kapsamında değerlendiriliyor?	Olası Yaptırımlar Nelerdir?
Israrlı takip: Sürekli mesaj göndermek ya da aramak, konum bildirmeye, fotoğraf atmaya zorlamak. Kişi iletişim kurmak istemediğini belirttiği ya da yanıt vermediği halde iletişim kurmakta ısrar etmek.	**Kişilerin huzur ve sükununu bozma - TCK Madde 123** Sırf huzur ve sükûnunu bozmak maksadıyla bir kimseye ısrarla; telefon edilmesi, gürültü yapılması ya da aynı maksatla hukuka aykırı başka bir davranışta bulunulması.	Mağdurun şikayeti üzerine faile üç aydan bir yıla kadar hapis cezası verilir.
Kişiler arasındaki özel yazışmaların, görüntülerin ifşası.	**Haberleşmenin Gizliliğini İhlal - TCK Madde 132** Kişiler arasındaki haberleşmenin gizliliğini ihlal etmek. Bu gizlilik ihlalinin haberleşme içeriklerinin kaydı suretiyle gerçekleşmesi. Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa etmek. Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa etmek. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması **Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması TCK Madde 133** Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinlemek veya bunları bir ses alma cihazı ile kaydetmek Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kaydetmek	- Bir yıldan üç yıla kadar hapis cezası - Verilecek ceza bir kat artırılır. - İki yıldan beş yıla kadar hapis cezası - Bir yıldan üç yıla kadar hapis cezası - Bir yıldan üç yıla kadar hapis cezası - İki yıldan beş yıla kadar hapis cezası - Altı aydan iki yıla kadar hapis veya adlî para cezası

	Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa etmek	- İki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası
	İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması	- İki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası
	Aynı zamanda özel hayatın gizliliğini ihlal, kişisel verilerin ihlali gibi suçlar da oluşabilir.	
Siber sömürü /Cinsel içerikli şantaj : Kişinin mahrem görüntülerini çekmek ve internette, sosyal ağlarda veya özel mesajlaşmalarda başkalarıyla paylaşmakla tehdit etmek ve/veya paylaşmak	**Özel hayatın gizliliğini ihlal TCK Madde 134**	
	Kişilerin özel hayatının gizliliğini ihlal etmek	- Bir yıldan üç yıla kadar hapis cezası
	Görüntü veya ses kaydı alarak gizlilik ihlali	- Verilecek ceza bir kat artırılır
	Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa etmek	- İki yıldan beş yıla kadar hapis cezası
	İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması	- İki yıldan beş yıla kadar hapis cezası
	Aynı zamanda kişisel verilerin ifşası da söz konusu olabilir.	
	Tehdit – TCK Madde 106	
	Bir başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden bahisle tehdit etmek	- Altı aydan iki yıla kadar hapis cezası
	Malvarlığı itibarıyla büyük bir zarara uğratacağından veya sair bir kötülük edeceğinden bahisle tehdit	- Altı aya kadar hapis veya adlî para cezası
	Tehdidin; a) Silahla, b) Kişinin kendisini tanınmayacak bir hale koyması suretiyle, imzasız mektupla veya özel işaretlerle, c) Birden fazla kişi tarafından birlikte, d) Var olan veya var sayılan suç örgütlerinin oluşturdukları korkutucu güçten yararlanılarak, İşlenmesi	- İki yıldan beş yıla kadar hapis cezası
	Tehdit amacıyla kasten öldürme, kasten yaralama veya malvarlığına zarar verme suçunun işlenmesi	- Ayrıca bu suçlardan dolayı ceza verilir.

	Tehdit içeren ifadelerin Sosyal medya üzerinden bir kişiye yönelmesi durumunda da aynı suç işlenmiş Kabul edilecektir. Genellikle hakaret suçu ile birlikte aynı eyleme bağlı olarak neticede bu suçun da oluştuğu görülmektedir.	
	Hakaret **TCK Madde 125**	
	Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat etmek veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldırmak	- Üç aydan iki yıla kadar hapis veya adlî para cezası
	Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilat ederek işlenmesi gerekir.	
	Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi	- Üç aydan iki yıla kadar hapis veya adlî para cezası
	Hakaret suçunun; a) Kamu görevlisine karşı görevinden dolayı, b) Dini, siyasi, sosyal, felsefi inanç, düşünce ve kanaatlerini açıklamasından, değiştirmesinden, yaymaya çalışmasından, mensup olduğu dinin emir ve yasaklarına uygun davranmasından dolayı, c) Kişinin mensup bulunduğu dine göre kutsal sayılan değerlerden bahisle, İşlenmesi	- Cezanın alt sınırı bir yıldan az olamaz.
	<u>Hakaretin alenen işlenmesi</u>	
	Kurul hâlinde çalışan kamu görevlilerine görevlerinden dolayı hakaret edilmesi hâlinde suç, kurulu oluşturan üyelere karşı işlenmiş sayılır. Ancak, bu durumda zincirleme suça ilişkin madde hükümleri uygulanır.	Ceza altıda biri oranında artırılır.

Siber taciz: Kişiye rızası dışında mesajlar ve /veya cinsel içerikli mesajlar ve görüntüler göndermek	**Cinsel taciz** **Madde 105** Bir kimseyi cinsel amaçlı olarak taciz etmek Fiilin çocuğa karşı işlenmesi a) Kamu görevinin veya hizmet ilişkisinin ya da aile içi ilişkinin sağladığı kolaylıktan faydalanmak suretiyle, b) Vasi, eğitici, öğretici, bakıcı, koruyucu aile veya sağlık hizmeti veren ya da koruma, bakım veya gözetim yükümlülüğü bulunan kişiler tarafından, c) Aynı işyerinde çalışmanın sağladığı kolaylıktan faydalanmak suretiyle, d) Posta veya elektronik haberleşme araçlarının sağladığı kolaylıktan faydalanmak suretiyle, e) Teşhir suretiyle, işlenmesi Bu fiil nedeniyle mağdurun; işi bırakmak, okuldan veya ailesinden ayrılmak zorunda kalması.	- Üç aydan iki yıla kadar hapis cezası veya adlî para cezası - Altı aydan üç yıla kadar hapis cezası - Yukarıdaki fıkraya göre verilecek ceza yarı oranında artırılır. - Verilecek ceza bir yıldan az olamaz.
Gizlilik ihlali: Kişinin e-posta ve/ veya sosyal medya parolalarını alıp hesaplarına girmek, kişiden izin almadan cihazlarındaki bilgilere bakmak	**Kişisel verilerin kaydedilmesi** **TCK Madde 135** Hukuka aykırı olarak kişisel verileri kaydetmek Bu kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması	- Bir yıldan üç yıla kadar hapis cezası - Birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.

	Verileri hukuka aykırı olarak verme veya ele geçirme TCK Madde 136	
	Kişisel verileri, hukuka aykırı olarak bir başkasına vermek, yaymak veya ele geçirmek	- İki yıldan dört yıla kadar hapis cezası
	Suçun konusunun, TCK 236/5-6 fıkraları uyarınca kayda alınan beyan ve görüntüler olması	- Ceza bir kat artırılır.
	Nitelikli haller TCK Madde 137	
	Yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi	- Verilecek ceza yarı oranında artırılır.
	Verileri yok etmeme TCK Madde 138	
	Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmemesi	- Bir yıldan iki yıla kadar hapis cezası
	Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde.	- Verilecek ceza bir kat artırılır.
	Bilişim sistemine girme TCK Madde 243	
	Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek	- Bir yıla kadar hapis veya adlî para cezası
	Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi	- Verilecek ceza yarı oranına kadar indirilir.
	Bu fiil nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi	- Altı aydan iki yıla kadar hapis cezası

	Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlemek	- Bir yıldan üç yıla kadar hapis cezası
	Sistemi engelleme, bozma, verileri yok etme veya değiştirme **TCK Madde 244**	
	Bir bilişim sisteminin işleyişini engellemek veya bozmak	- Bir yıldan beş yıla kadar hapis cezası
	Bir bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek	- Altı aydan üç yıla kadar hapis cezası
	Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi	- Verilecek ceza yarı oranında artırılır.
	Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması.	-İki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası
	Banka veya kredi kartlarının kötüye kullanılması **TCK Madde 245**	
	Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa	- Üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası
	Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek	- Üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası

	Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak (fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde) Birinci fıkrada yer alan suçun; a) Haklarında ayrılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin, Zararına olarak işlenmesi hâlinde. Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.	- Dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası -İlgili akraba hakkında cezaya hükmolunmaz
Kişi adına internette sahte hesaplar açarak onun adına paylaşım yapmak	**Verileri hukuka aykırı olarak verme veya ele geçirme** **TCK Madde 136** Ayrıca bu hesaplar aracılığı ile hakaret suçu oluşabilir, özel hayatın gizliliğini ihlal söz konusu olabilir. Ya da kişinin hatırasına hakaret suçu da oluşabilir. Bu suç tüzel kişilere karşı da işlenebilir.	Cezaları yukarıda açıklandı.
Nefret söylemi: İnternette, sosyal medyada, dijital oyunlarda, mesajlaşma uygulamalarında kişi hakkında küçük düşürücü, hakaret içeren, cinsiyetçi mesajlar paylaşmak, kişiyi hedef göstermek ve sanal lince maruz bırakmak	**Hakaret** **TCK Madde 125** **Mağdurun belirlenmesi TCK Madde 126** Hakaret suçunun işlenmesinde mağdurun ismi açıkça belirtilmemiş veya isnat üstü kapalı geçiştirilmiş olsa bile, eğer niteliğinde ve mağdurun şahsına yönelik bulunduğunda duraksanmayacak bir durum varsa, hem ismi belirtilmiş ve hem de hakaret açıklanmış sayılır.	Cezaları yukarıda anlatıldı. TCK md. 126 ile düzenlenen bu hususla, basın yoluyla ya da geleneksel medya araçları üzerinden bir kişiyi ya da bir gruba mensup kişileri hedef göstermek suç olarak düzenlenmiştir.

	Halkı kin ve düşmanlığa tahrik veya aşağılama Madde 216/2 Halkın bir kesimini, sosyal sınıf, ırk, din, mezhep, cinsiyet veya bölge farklılığına dayanarak alenen aşağılamak. Halkın bir kesiminin benimsediği dini değerleri alenen aşağılamak. (Bu fiilin kamu barışını bozmaya elverişli olması halinde)	- Altı aydan bir yıla kadar hapis cezası - Altı aydan bir yıla kadar hapis cezası
Doxxing: Kişi hakkında internet üzerinden ayrıntılı bilgi toplamak ve kişiye zarar vermek üzere bu bilgileri yaymak ve kullanmak.	**Verileri hukuka aykırı olarak verme veya ele geçirme, yayma** **TCK Madde 136**	Cezaları yukarıda açıklandı.
İtibarsızlaştırma: Kişinin ticari itibarını zedeleyecek şekilde paylaşımlar yapmak, ticari sırları açık etmek	**Kişilik haklarının ihlali sebebiyle tazminat Medeni Kanun md.24, Haksız rekabet TTK 56 vd.** **Marka hakkına tecavüz, 6769 s. Yasa hükümleri** **5651 s. Yasa hükümleri.**	İlgili yasalarda belirtilen tazminat hükümleri uygulanır. İlgili yasada belirtilen tazminat ve cezai hükümler uygulanır. Erişim engelleme ve içeriğin kaldırılması.

Kontrol etme: Kişinin sosyal medya paylaşımlarına karışmak, sosyal medya iletişimini sınırlandırmaya çalışmak	**Haberleşmenin engellenmesi** **TCK Madde 124** Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engellemek. Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi. Ayrıca ifade özgürlüğü, haber alma hakkı, bilgi edinme hakkı gibi Anayasal hakların da ihlali söz konusu olabilir.	- Altı aydan iki yıla kadar hapis veya adlî para cezası - Bir yıldan beş yıla kadar hapis cezası - İkinci fıkra hükmüne göre cezaya hükmolunur. TCK ve diğer yasalardaki ilgili cezai hükümler ve tazminat hükümleri, ilgili fiile göre uygulanır.
Tehdit/Şantaj: Kişiyi dijital araçları kullanarak ölümle, cinsel saldırıyla, fiziksel şiddetle tehdit etmek, şantaj yapmak	**Tehdit** **TCK Madde 106** **Şantaj** **TCK Madde 107** Hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle, bir kimseyi kanuna aykırı veya yükümlü olmadığı bir şeyi yapmaya veya yapmamaya ya da haksız çıkar sağlamaya zorlamak Kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunmak.	- Cezaları yukarıda açıklandı. - Bir yıldan üç yıla kadar hapis ve beşbin güne kadar adlî para cezası - Birinci fıkraya göre cezaya hükmolunur.
Kişisel veri ifşası: Kişinin kişisel verilerini ifşa etmek	**Kişisel verilerin kaydedilmesi** **Verileri hukuka aykırı olarak verme veya ele geçirme** **TCK Madde 135, 136, 137, 138** 6698 s. KVKK MADDE 18. Kabahatler Aydınlatma yükümlülüğü ve veri güvenliğine ilişkin yükümlülükleri yerine getirmemek.	- Cezaları yukarıda açıklandı. - 5000 ile 1.000.000 Türk lirasına kadar idari para cezası.

5. DİJİTAL ŞİDDET SÖZLÜĞÜ

Aşk Bombardımanı (Love Bombing):
Genellikle bir ilişkinin başlangıcında failin, karşısındaki kişiyi aşırı derecede ilgiye ve sevgiye boğması. Böyle bir ilişki içerisinde fail, ilişkide olduğu kişiyle sürekli iletişim halinde olmak istemekte, gün içerisinde mesajlar, e-postalar, telefon görüşmeleri, sosyal medya vb. aracılığıyla sürekli iletişim kurmaktadır. Aşk bombardımanı bir istismar türüdür. Narsist özellikler sergileyen failin, bu ilgisi başlangıçta sorun yaratmayabilir, ama zaman içerisinde bunaltıcı hale gelebilir. Narsist fail, bilinçli veya bilinçsiz olarak, karşısındaki kişinin hayatında en önemli yere sahip olduğunu güvence altına almaya çalışır (Strutzenberg, 2016). Pahalı hediyeler almak, sürekli birlikte vakit geçirmek istemek, aşırı iltifatlar, sınır koyulmasından rahatsız olunması aşk bombardımanı göstergesi olabilir. Aşk bombardımanına maruz bırakılan kişi, ilişki içerisinde bağımlı hale gelebilir ve istese de ilişkiyi bitirmekte zorlanabilir.

Atanmış İsmiyle Çağırma (Deadnaming):
Doğumda verilen ismini değiştirmiş olan kişiye eski (ölü) ismiyle hitap etme. Kişiyi tercih ettiği veya yasayla değiştirdiği yeni bir isim kullanmaya başladıktan sonra eski ismiyle çağırma. Bu şiddet türü, genellikle birçok nedenle atanmış ismini reddeden ve değiştiren LGBTIQ+ bireylere karşı kullanılmaktadır (Women Media Center). Atanmış ismiyle çağırma, kazara veya kasıtlı olabilir ve bir kişinin kimliğini geçersiz kılmayı, yanlış cinsiyetlendirmeyi amaçlar (Lieurance vd., 2022, s.341-342).

Beden Ayıplama: (Body Shaming):
Bir kişinin bedeniyle ilgili olumsuz yorumlarda bulunmak, kişiyi bedeni üzerinden ayıplamak, aşağılamak, fiziksel görünüşüyle dalga geçmek. Beden aşağılama hem çevrimdışı hem de çevrimiçi alanlarda gerçekleşebilir. Beden aşağılama, bir kişinin bedeninin şeklini, boyunu, kilosunu, belirli bölgelerini vs. hedef alabilir (Schlüter, Kraag ve Schmidt, 2021, s.8).

Catfishing:
Bir kişinin çevrimiçi kimliğini taklit ederek dijital iletişim ortamlarında o kişiymiş gibi davranma. Fail, hedefindeki kişinin genellikle sosyal medya hesaplarından aldığı görüntüler ve bilgileri kullanarak yeni bir hesap açar ve o kişiymiş gibi hareket eder. Fail, yarattığı kurgusal kimlikle hedef aldığı kişinin itibarını zedelemeyi, ona zarar verecek ilişkiler kurmayı amaçlar (Cybersmile.org)

Çevrimiçi Ekonomik Şiddet:
Ekonomik şiddet, dijital medyayla yeni boyutlar kazanmıştır. Fail, bir kişiye ekonomik baskı uygulamak üzere dijital medyayı kullanabilir. Kimlik hırsızlığı, çevrimiçi hesaplara erişimin engellenmesi, kredi bilgisinin manipüle edilmesi gibi yöntemler çevrimiçi ekonomik şiddet kapsamında değerlendirilir (Women Media Center).

Çevrimiçi Grooming:
Çevrimiçi "grooming", dijital medya kullanılarak gerçekleştirilen çocuklara yönelik bir cinsel istismar türüdür. Failin cinsel ilişkiye girmek veya cinsel sömürü amacıyla bir çocuğun güvenini kazanmak için onunla internet üzerinden iletişim kurmasıdır. Fail, internet ortamında genellikle bir çocuk veya ergen/genç kılığına bürünerek çocukların yoğun olduğu siteler üzerinden çocukla sohbet ederek güvenini kazanır, daha sonra çocuktan mahrem ve kişisel bilgilerini (cinsel içerikli görüntüler gibi) talep ederek ona şantaj yapar (ChildSafeNet). Gunawan vd.'ne göre, çevrimiçi grooming altı aşamadan oluşur: 1- Arkadaşlık kurma: Fail, çocuğun kişisel bilgilerini elde etmeye çalışır. 2- İlişki kurma: Fail ve çocuk, çocuğun ailesi, okulu, ilgi alanları ve hobileri hakkında konuşurlar, fail, çocuğu bir ilişki içinde olduklarına inandırır. 3- Risk değerlendirme: Fail, çocuğun yalnız olmasını ve konuşmalarını başka kimseyle paylaşmamasını sağlar. 4- Özel olma: Fail, çocuğun tam güvenini kazanır, sevgi ve ilgisini sömürür. 5- Cinsellik: Fail ve çocuk, cinsel aktiviteler ve seks fantezileri hakkında konuşurlar. 6- Sonuç: Fail, yüz yüze görüşmek için çocuğa yaklaşır. Bu aşamaların oluşma sıklığı, sırası ve kapsamı sohbetten sohbete değişebilir (Gunawan vd., 2016, s.1).

Çevrimiçi Israrlı Takip (Stalk):
Çevrimiçi ısrarlı takip, bir kişiyi e-posta, mesajlar, sosyal medya, konum bazlı uygulamalar, ve internet üzerinde bıraktığı diğer izler aracılığıyla sistematik olarak takip etmek, gözetlemektir. İzleme/takip, kendi başına zararlı olabilecek ya da olmayacak olayların tekrarlanma durumunda şiddete maruz bırakılanın güvenlik hissini zayıflatır ve sıkıntı, korku ya da alarm durumuna getirir. Çevrimiçi ısrarlı takipte 'stalklama (gizlice izlemek)' terimi de kullanılmaktadır. Takip eden kişiye de 'stalker' denilmektedir. Siber takip/staklama terimi, tekrarlanan tehditler ve/veya tacizlerle, elektronik postayla, diğer bilgisayar temelli iletişim yoluyla bir kişinin korktuğu, güvenliğinden endişe duyduğu çeşitli davranışları tanımlamak için kullanılmaktadır.

Çevrimiçi Nefret Söylemi (Online Hate Speech):
Dijital iletişm ortamlarında nefret içerikli konuşmak, kişiyi kimliği ve özellikleri (ırk, etnik grup, cinsiyet, cinsel yönelim, yaş, engellilik vs.) üzerinden aşağılamak, tehdit etmek ve hedef göstermek. Çevrimdışı ortamlarda varolan nefret söylemi, özellikle sosyal medya kullanımıyla daha yaygın hale gelmekte, nefret suçlarının ve belirli gruplara yönelik şiddet eylemlerinin ortaya çıkmasını kolaylaştırmaktadır. Nefret söylemleri, nefret suçu olarak kabul edilmese de, bir suç işlenmeden önce, suçun işlenmesi sırasında veya suç işlendikten hemen sonra yapılan ve nefret söylemi teşkil eden açıklamalar, nefret suçunu oluşturan 'önyargı saiki'nin varlığını kanıtlamada kuvvetli delil teşkil edecektir" (İnceoğlu, 2012, s. 107). Önyargı saikine göre değerlendirildiğinde nefret söyleminde bulunmak bir suçtur (Özarslan ve Yıldız, 2021).

Çevrimiçi/Siber Taciz (Online Harassment):
Çevrimiçi ya da siber taciz, bir kişinin rızası olmadığı halde onunla iletişim kurma, onu iletişim kurmaya zorlama. Çevrimiçi taciz, çeşitli biçimlerde olabilir: İstenmeyen cinsel içerikli e-postalar, metin (veya çevrimiçi) mesajlar gönderme; sosyal ağ sitelerinde veya internet sohbet odalarında yaşanan uygunsuz veya saldırgan olaylar; e-posta, metin veya çevrimiçi mesajlarla fiziksel ve/ veya cinsel şiddetle tehdit etme; nefret içerikli konuşma, kişiyi kimliğini (cinsiyeti) ve diğer özelliklerini (cinsel yönelim veya engellilik gibi) dayatan, hakaret eden, tehdit eden veya hedefleyen bir şekilde davranma (EIGE)[8].

Çoklu Platform Tacizi:
Fail(lerin) kişiyi(leri) tek bir dijital platform değil, koordineli şekilde birçok dijital platform üzerinden hedef alması. Örneğin, fail(lerin) bir kişiyi(leri) aynı anda Twitter, Facebook, e-posta, Instagram üzerinden dijital şiddete maruz bırakması. Bu taciz türü, sosyal medya hesapları, e-posta, bloglar, çevrimiçi veya çevrimdışı iş çevreleri ve telefon gibi kanallar aracılığıyla kişiye yönelen tehditler, hakaretler ve diğer istenmeyen temasları içerir (Matias vd., 2015, s.19). Çoklu platform tacizi, her dijital platformun yalnızca kendi içeriğini denetlemesi gerçeğinden yararlanır ve bu nedenle dijital şiddete uğrayan bakımından başa çıkılması daha zor olabilir (Women Media Center).

Dijital Dikizcilik (Creepshot):
Kadınların izni ve haberi olmadan onların fotoğraflarını veya görüntülerini çekme ve İnternette yayınlama (Avrupa Kadın Lobisi).

Dijital Seks Ticareti:
İnternet üzerinden insan kaçakçılığı, fuhuş ve seks ticareti yapma. Fail(ler), İnternetin küreselliğinden ve anonimliğinden yararlanır, hedefledikleri kişiler hakkında sosyal medyadan bilgi toplar ve onları seks işçiliğine zorlar (Avrupa Kadın Lobisi).

Doxing:
Birine ait özel ve kişisel bilgileri ele geçirerek internette yaymaktır. Kişisel bilgiler; ev adresi, e-posta, telefon numarası, kimlik numarası, fotoğraflar vb. olabilir. “Doxing” terimi, hacker kültüründen gelmekte ve “dosyaları düşürmek” anlamına gelmektedir (Anderson ve Wood, 2021, s.205). Doxing, genellikle hedeflenen kişiye zarar vermeyi içerir. Doxing, çoğunlukla diğer çevrimiçi taciz biçimleriyle bağlantılı olarak ortaya çıkar, kişinin hem çevrimiçi hem de fiziksel ortamlarda hedef alınmasına yol açar (Eckert ve Metzger-Riftkin, 2020, s.1).

Etek Altı Görüntü Çekme (Upskirting):
Cep telefonu, fotoğraf makinesi veya kamera kullanarak kişilerin eteklerinin giysilerinin altından, izinsiz olarak fotoğraflarının ve videolarının çekilerek internette paylaşılması. Fail(ler), kamusal alanlarda, umumi tuvaletlerde, açık alan etkinliklerinde, sokakta vs. kadınların gizlice etek altı görüntülerini çekebilirler.

[8] EIGE metninde siber taciz kavramı kullanılmakta, ancak literatürde çevrimiçi taciz kavramı da yaygın olarak kullanıldığından bu çalışmada her ikisine de yer verilmiştir.

Gasligthing:
Çeşitli psikolojik manipülasyonlarla birinin kendinden şüphe etmesini sağlamaya çalışma. Gaslighting, duygusal istismar türüdür ve kişinin kendi duygularını, anılarını ve gerçeklik algısını sorgulamasına yol açar (Porter ve Standing, 2020). Gaslighting uygulayan fail, bilinçli ya da bilinçsiz olarak karşısındaki kişinin tepkilerinin, algılarının, anılarının ve/veya inançlarının yanlış ve asılsız olduğu hissini uyandırmaya çalışır, hatta onu "delirmiş olmakla" itham edebilir (Abramson, 2014, s. 2). Gaslighting, herhangi bir ilişki içerisinde (romantik ilişki, aile, arkadaşlık, iş vs.), yüz yüze ve/veya çevrimiçi ilişkilerde gerçekleşebilir.

Ghosting (Hayaletlenme):
İlişkide olunan kişiyle iletişimi hiçbir neden göstermeden bir anda bitirme. Partnerlerden birinin hiçbir açıklama yapmadan mesajlara, telefonlara yanıt vermemesi, karşı tarafı cezalandırıcı şekilde sessiz kalması, ortadan kaybolması, karşı tarafı sosyal medya platformlarında engellemesi, karşı tarafın iletişim kurma çabasını görmezden gelme vs. "ghosting" davranışlarına örnek gösterilebilir (Navarro et.al, 2020, akt. Biolcati vd. 2021, Pancani vd. 2021).

İntikam Pornosu (Siber Sömürü):
Görüntüde yer alan kişinin rızası olmaksızın cinsel içerikli fotoğraflarını veya videolarını çevrimiçi olarak dağıtmak. Bu görüntüleri dağıtmakla tehdit etmek de bir dijital şiddet türüdür. Fail, çoğunlukla önceki bir ilişki esnasında görüntü veya video elde eden eski bir eş ya da sevgilidir ve ilişkiyi sona erdirmek için misilleme olarak kişiyi kamuoyunda utandırmak ve aşağılamak amacı ile görüntüleri kullanır. Bununla birlikte, failler, mutlaka eski eş ya da sevgili olmayabilirler. Faillerin yaptıkları eylemin nedeni her zaman intikam da olmayabilir. Görüntüler, kişinin bilgisayarına, sosyal medya hesaplarına veya telefonuna saldırarak elde edilebilir, hedefin 'gerçek dünyadaki' yaşantısına gerçek bir hasar oluşturmayı amaçlayabilir.

İtibar Suikastı:
İtibar suikastı, bir kişi veya grubu itibarsızlaştırmak için onlar hakkında gerçek olmayan söylentiler, yalan haberler yaymaktır. Günümüzde özellikle sosyal medya, itibar suikasti için yaygın olarak kullanılmaktadır.

Mağdur Suçlayıcılık:
Yaşanılan bir mağduriyette çeşitli gerekçelerle kabahati o mağduriyeti yaşayan kişiye yapıştırarak faili aklayan yaklaşım (Cinsel Şiddetle Mücadele Derneği). İnternette ve özellikle sosyal medyada mağdur suçlayıcı yaklaşım yaygındır. Örneğin cinsel saldırıya uğrayan bir kadın hakkında sosyal medya kullanıcılarının yaptığı çeşitli yorumlar mağdur suçlayıcılık içerebilir.

Sanal Linç:
Çok sayıda istismarcının tehdit, hakaret ve diğer taciz edici taktiklerle bir hedefe toplu olarak saldırması (PEN).

Sexting:
Bir kişiye cinsel içerikli mesajlar, fotoğraflar, görüntüler, ses kayıtları gönderme. "Sexting", başlangıçta cep telefonu metin mesajları yoluyla cinsel içerikli metin mesajları gönderme anlamına gelirken, günümüzde bu tanım, görsel içeriği içerecek şekilde genişletilmiştir (Van Ouytsel vd., 2019). İzin verilmediğinde veya rıza alınmadan yapıldığında bir dijital şiddet türüdür (stopcybersexisme.com).

Sextortion:
Failin, hedefindeki kişiyi istediği şeyi yapmaya zorlamak için çıplak veya cinsellik içeren görüntülerini yaymakla tehdit etmesi, şantaj yapması.

Siber Teşhircilik (Cyber Flashing):
Failin, toplu alanlarda Bluetooth, Airdrop gibi uçtan uca Wi-Fi ağları üzerinden müstehcen (genellikle cinsel organının) görüntülerini tanımadığı kimselere göndermesi. Siber teşhircilik, dijital yollarla gönderilen rıza dışı cinsel görüntüleri içerir ve "teknolojiyle desteklenen cinsel tacizin" bir biçimidir. Siber teşhircilik dahil olmak üzere teknolojiyle desteklenen cinsel taciz, "kadınların halka açık yerlerde güvenini ve güvenliğini" sınırlayabilir (Freeman, 2020).

Siber Zorbalık:
Cep telefonu, e-posta, anlık mesajlaşma, web sitesinde kişileri karalamak için anketler düzenleme gibi elektronik iletişim teknolojilerinin kullanımı yoluyla, bir kişi ya da grup tarafından başkalarına zarar vermek niyetiyle kasten, tekrar edici bir şekilde, düşmanca davranışlar göstermek (Küçük, İnanıcı ve Ziyalar, 2017). Çocuklar ve gençler arasında akran şiddetinin dijital iletişim ortamlarını da kapsayacak şekilde genişlemesiyle ortaya çıkan siber zorbalık, farklı biçimlerde ortaya çıkabilir: küfür, hakaret, tehdit mesajları gönderme, başkalarının e-postalarını izinsiz okuma, kişisel şifrelerini kullanma, küçük düşürücü mesajlar gönderme, kişinin izinsiz küçük düşürücü fotoğraflarını çekerek internette yayma vb. (Baker ve Kavşut, 2017).

Sürtük Olarak Damgalama (Slut-Shaming):
Kadınları ve kız çocuklarını, gerçek veya varsayılan cinsellikleri veya cinsel davranışları üzerinden eleştirme, hedef gösterme, "sürtük" veya başka sıfatlarla damgalama. Fail(ler), kadınları ve kız çocuklarını cinsel normlara uymadıkları gerekçesiyle etiketlemektedir (Karaian, 2014). Sosyal medyanın yaygın kullanımı, beraberinde "sürtük olarak damgalama" eylemlerinin de yaygınlaşmasına yol açmıştır. Kadınlar ve kız çocuklarına yönelik "sürtük olarak damgalama"nın kökeninde cinselliğe ilişkin çifte standart yatmakta, erkeklerin sergiledikleri cinsel davranışlar kabul görürken ve ödüllendirilirken kadınlar cezalandırılmaktadır (Van Royen vd., 2018). Kadınlara atfedilen geleneksel toplumsal cinsiyet rollerinin dışında davranan kadınlar, "sürtük" veya başka sıfatlarla kolaylıkla damgalanmaktadır. Bu damgalama, medya ve sosyal medyada da yaygındır.

Yapay Zekayla Üretilmiş Cinsel İçerikli Sahte Görüntü (Deep Fake Porn):
Yapay zeka teknolojileri kullanılarak bir kişinin rızası olmadan cinsel içerikli sahte görüntülerinin üretilmesi ve internette yayılması.

KAYNAKLAR

Abramson, K. (2014). Turning up the lights on gaslighting. Philosophical Perspectives, 28(1), 1–30. doi:10.1111/phpe.12046

Anderson, B. ve Wood, M. (2021). Doxxing: A scoping review and typology. The Emerald International Handbook of Technology-Facilitated Violence and Abuse, 205–226. doi:10.1108/978-1-83982-848-520211015

Avrupa Kadın Lobisi (2017). #KadınınHakkıKadınınİnterneti. https://www.womenlobby.org/IMG/pdf/hernetherrights_resource_pack_2017_web_version.pdf Erişim tarihi: 08.04.2022.

Biolcati, R., Pupi, V. ve Mancini, G. (2021). Cyber dating abuse and ghosting behaviors: personality and gender roles in romantic relationships. Current Issues in Personality Psychology. doi:10.5114/cipp.2021.108289.

ChildSafeNet(2022). Cyber Grooming. https://www.childsafenet.org/new-page-15. Erişim tarihi: 10.04.2022.

Cinsel Şiddetle Mücadele Derneği (2019). Kavramlar Sözlüğü. cinselsiddetlemucadele.org. Erişim tarihi: 03.04.2022

Cybersmile (2021). Catfishing. https://www.cybersmile.org/what-we-do/advice-help/catfishing Erişim tarihi: 10.04.2022.

Eckert, S. ve Metzger-Riftkin, J.(2020). Doxing. The International Encyclopedia of Gender, Media, and Communication. (ed.) K.Ross, I. Bachmann, V. Cardo, S. Moorti ve M. Scarcelli. John Wiley & Sons, Inc. DOI: 10.1002/9781119429128.iegmc009

EIGE. (2017). Cyber Violence Against Women and Girls. http://eige.europa.eu/rdc/ 6 eige-publications/cyber-violence-against-women-and-girls Erişim tarihi: 03.04.2022

Erdur-Baker, O. ve Kavşut, F. (2007). Akran Zorbalığının Yeni Yüzü: Siber Zorbalık Cyber Bullying: A New Face of Peer Bullying. Eurasian Journal of Educational Research, 27, s.31-42.

Freeman, V. (2020) “Cyber Flashing: Unwanted and Non-Consensual Lewd Photographs as Technology Enhanced Sexual Harassment”. Student Works. 1090. https://scholarship.shu.edu/student_scholarship/1090

Gunawan, F.E. vd. (2016). Detecting online child grooming conversation. 11th International Conference on Knowledge, Information and Creativity Support Systems (KICSS). Yogyakarta, Endonezya.

İnceoğlu, A. A. (2012). Nefret Suçu Kavramı ve Türk Ceza Mevzuatı Açısından Değerlendirilmesi, Nefret Söylemi ve/veya Nefret Suçları içinde (s.103-120), Yasemin İnceoğlu (Der.) İstanbul: Ayrıntı Yayınları.

Karaian, L. (2014). Policing “sexting”: Responsibilization, respectability and sexual subjectivity in child protection/crime prevention responses to teenagers’ digital sexual expression. Theoretical Criminology. 18, 282–299. doi:10.1177/1362480613504331

Van Ouytsel, J., Walrave, M., Ponnet, K. and Temple, J.R. (2018). Sexting. In The

International Encyclopedia of Media Literacy (eds R. Hobbs and P. Mihailidis). https://doi.org/10.1002/9781118978238.ieml0219

Küçük S, İnanıcı, M. A, Ziyalar, N. (2017). Siber Zorbalık Ölçeği Türkçe Uyarlaması. Adli Tıp Bülteni, 22(3), 172 - 176.

Leitão R. (2019). Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums. Human–Computer Interaction, DOI: 10.1080/07370024.2019.1685883

Lieurance, D et. al. (2022). Words matter: how to increase gender and LGBTQIA + inclusivity at Biological Invasions. Biol Invasions 24, 341–344. https://doi.org/10.1007/s10530-021-02665-7

Matias, J. N., Johnson, A., Boesel, W. E., Keegan, B., Friedman, J.,ve DeTar, C. (2015). Reporting, Reviewing, and Responding to Harassment on Twitter. Women, Action, and the Media. May 13, 2015. http://womenactionmedia.org/twitter-report

Özarslan, Z. ve Yıldız, F. (2021). Nefret söylemi araştırmalarında yöntem üzerine bir analiz. Proceedings of the 18th International Symposium Communication in the Millenium, 26-27 Ekim 2021.603-616. Pdf file, E-Book. ISBN: 978-625-7960-45-8.

PEN(2022). Online Harassment Field Manual. https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/ Erişim tarihi: 03.04. 2022

Pancani L, Mazzoni D, Aureli N, Riva P.(2021). Ghosting and orbiting: An analysis of victims' experiences. Journal of Social and Personal Relationships.;38(7):1987-2007. doi:10.1177/02654075211000417

Porter, J. ve Standing K. (2020) Love Island and Relationship Education. Frontiers in Sociology, 4 (79). doi: 10.3389/fsoc.2019.00079

Stop Cyber Sexisme (2022). Sexting. https://www.stop-cybersexisme.com/le-dico-ducybersexisme. Erişim tarihi: 03.04.2022

Schlüter, C., Kraag, G. ve Schmidt, J. (2021). Body Shaming: an Exploratory Study on its Definition and Classification. International Journal of Bullying Prevention https://doi.org/10.1007/s42380-021-00109-3

Strutzenberg, Claire, "Love-Bombing: A Narcissistic Approach to Relationship Formation" (2016). Human Development, Family Sciences and Rural Sociology Undergraduate Honors Theses. 1.http://scholarworks.uark.edu/hdfsrsuht/1

Van Royen K., Poels K., Vandebosch H., Walrave M. (2018) Slut-Shaming 2.0. In: Walrave M., Van Ouytsel J., Ponnet K., Temple J. (eds) Sexting. Palgrave Studies in Cyberpsychology. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-71882-8_6

Women Media Center. https://womensmediacenter.com/speech-project/online-abuse-101#crossPlatformHarassment Erişim tarihi: 03.04.2022

Avrupa Birliği sivil düşün

"Bu e-rehber, Avrupa Birliği Sivil Düşün Programı kapsamında Avrupa Birliği desteği ile hazırlanmıştır. İçeriğin sorumluluğu tamamıyla TBİD ve AltBil'e aittir ve AB'nin görüşlerini yansıtmamaktadır."