# CİNSİYETÇİ DİJİTAL ŞİDDETLE MÜCADELE REHBERİ


Toplumsal Bilgi ve İletişim Derneği
alternatif bilişim
AVRUPA BİRLİĞİ
SivilDüşün

**Hazırlayanlar:**

Gülüm Şener
İlden Dirini
Nurcihan Temur
Şebnem Ahi
Şevket Uyanık

**Tasarım:**
Fatih Akdoğan

**Aralık, 2019**




“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

# 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.

[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

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.

### Çevrimiçi Şiddet: Çevrimdışı Şiddetin Devamı

Kadınlar, toplumsal cinsiyete dayalı eşitsizliklerden dolayı gerçek hayatta (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 "gerçek" 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.

BM "Kadınlara ve Kız Çocuklarına Yönelik Siber Şiddet - Dünya Geneli Acil Eylem Çağrısı" raporundaki[3] 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.

### 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.[2]

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

[3] UN. (2015). Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call. http://www.unwomen. org/-/media/headquarters/attachments/sections/library/ publications/2015/cyber_violence_gender%20report. pdf?vs=4259

**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.

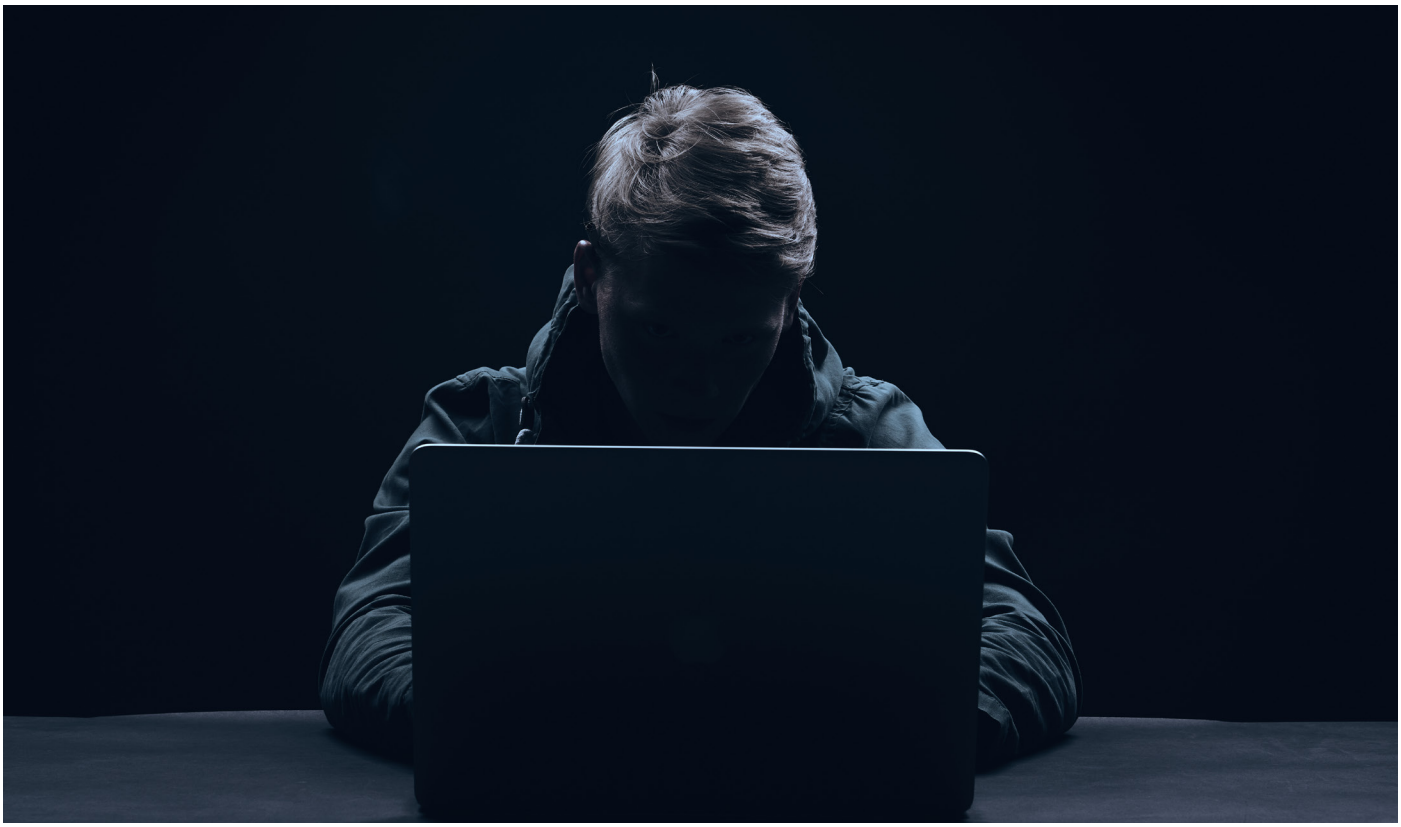
"Toplumsal Cinsiyete Dayalı Şiddet ve Çevrimiçi / Online İstismar" raporunda[4] çevrimiçi veya çevrimdışı ortamlarda öne çıkan kadınlara, çevrimiçi alanda daha fazla suistimale maruz kalabilecekleri çıktısı yer alır. LBTQ+ kadınlar, kadın gazeteciler (blog yazarları dahil), teknoloji endüstrisinde aktif 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?**

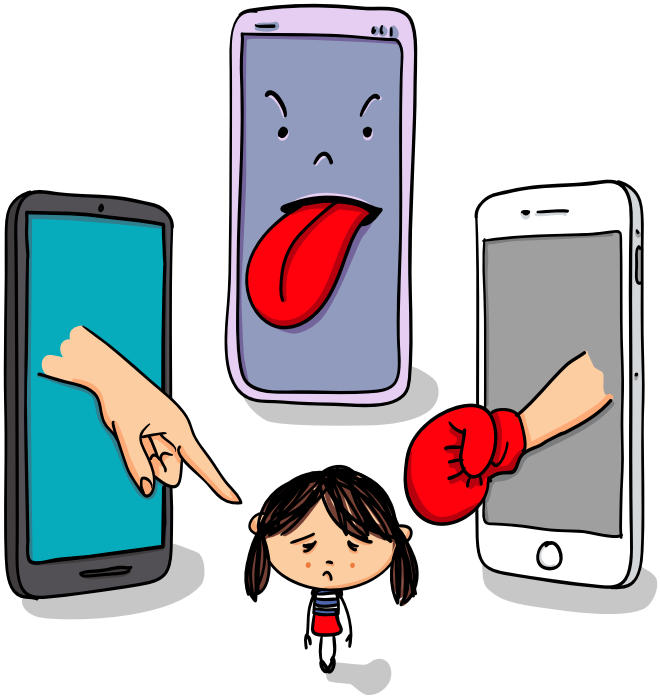
Dijital şiddeti uygulayan kişi eski ya da şu anki eş / partner, komşu, iş / okul arkadaşı, bir yakın ya da bir yabancı olabilmektedir.

Dijital şiddette, şiddet uygulayan kişi; sosyal ağlar, mesajlaşma uygulamaları, Global Positioning System-Küresel Konumlama Sistemi (GPS) destekli uygulamalar, akıllı telefonlar ve/veya e-mail kullanılarak şiddete maruz kalan kişinin kendi güvenliğinden endişe etmesine neden olmaktadır.

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.



[4] a.g.e.



# TOPLUMSAL CİNSİYETE DAYALI DİJİTAL ŞİDDETİN TÜRLERİ

**Tanımlayıcı Özellikler**

"Dijital Mekanlardan Sesler: Kadınlara Yönelik Teknolojik Şiddet" çalışmasında[5] 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 resimler, sınırsız olarak yayılır veya uzun süre ortamda kalır.

Avrupa Toplumsal Cinsiyet Eşitliği Enstitüsü "Kadınlara ve Kız Çocuklarına Yönelik Siber Şiddet" raporunda[6] konunun kategorileştirilmesine "siber takip" ile başlamıştır.

---

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

**Siber Takip**

Siber takip, e-posta, metin (veya çevrimiçi) mesajlar veya internet yoluyla izlenmedir. 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.

Siber 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.[7]

"Kadınlara ve Kız Çocuklarına Yönelik Siber Şiddet"[8] raporu, "siber takip" dışında siber şiddetin alt türleri olarak belirttiği "siber taciz" ve "siber sömürü"nün de tanımını yapar:

**Siber Taciz**

Siber taciz çeşitli biçimlerde olabilir, eylemler aşağıdaki şekilde çeşitlenmiştir:

- İstenmeyen cinsel içerikli e-postalar, metin (veya çevrimiçi) mesajlar;
- Sosyal ağ sitelerinde veya internet sohbet odalarında yaşanan uygunsuz veya saldırgan olaylar;
- E-posta, metin (veya çevrimiçi) mesajlarla fiziksel ve/ veya cinsel şiddet tehdidi;
- Nefret içerikli konuşma, kişiyi kimliğini (cinsiyeti) ve diğer özelliklerini (cinsel yönelim veya engellilik gibi) dayatan, hakaret eden, tehdit eden veya hedefleyen bir şekilde davranma.

[6] EIGE. (2017). Cyber Violence Against Women and Girls. Retrieved from http://eige.europa.eu/rdc/ 6 eige-publications/cyber-violence-against-women-and-girls

[7] Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology, and stalking. Violence against women, 13(8), 842-856

[8] a.g.e

**Siber Sömürü**

Aynı zamanda intikam pornosu[9] olarak da bilinen siber sömürü, görüntüde yer alan kişinin rızası olmaksızın cinsel içerikli fotoğrafları veya videoları çevrimiçi olarak dağıtma anlamına gelir.

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.

**Diğer Türler ve Tanımlar**

Birleşmiş Milletler tarafından gerçekleştirilen İnternet Yönetişim Forumu'nda "Toplumsal Cinsiyete Dayalı Şiddet ve Çevrimiçi/Online İstismar" konusu ele alınmıştır. Forum sonucu hazırlanan raporda[10] toplumsal cinsiyete dayalı dijital/siber/çevrimiçi şiddet kavramları örnekleri ile birlikte altı alt kategoride yer almıştır:

**1. Gizlilik İhlali:**

- Bireyin izni olmadan özel verilere erişilmesi (kişisel hesapların ele geçirilmesi, şifrelerin çalınması, kimliklerin kullanılması/çalınması, bir kullanıcının hesaplarına giriş yaparken bir başka kullanıcının bilgisayarına erişmek vb. 'siber sömürü' dahil olmak üzere),

- Fotoğraf ve videoları bireyin izni dışında alma, erişme, kullanma, manipüle etme, dağıtma,

- Bireyin bilgisi dışında veya onayı olmadan (cinsel içerikli) görüntüler, ses klipleri, video klipler de dahil olmak üzere özel bilgi ve içeriği paylaşma, yayma,
- Doxing (sanal ortamda kişisel bilgiye ulaşma-bilgi toplama), taciz ve başka amaçlarla bireyin izni/ rızası olmadan bir kişi hakkında şahsi olarak tanımlanabilen bilgileri araştırmak ve yayınlamak, bunu "gerçek" dünyadaki kadına şiddet ve taciz amaçlı kullanma,

- Bir kullanıcıyla temas kurmak için onun çocuklarına, ailelerine, meslektaşlarına ulaşma ve onları taciz etme.

[9] Yaygın kullanımı intikam pornosu olan kavram şiddete maruz bırakılanı daha fazla ayrımcılığa uğratacağı için siber sömürü tanımlaması tercih edilmiştir.

[10] IGF. (2015). Internet Governance Forum-Best Practice Forum on Online Abuse and Gender-Based Violence Against Women. http://www.intgovforum.org/cms/documents/best-practice-forums/623-bpf-online-abuse-and-gbv-against-women/file.

**2. Gözetim ve izleme:**

- Çevrimiçi ve çevrimdışı etkinliklerin izlenmesi ve gözetlenmesi,
- Kullanıcının izni olmaksızın casus yazılım veya klavye kaydedicilerin kullanılması,
- Bir kadının rızası olmadan hareketlerini izlemek için GPS ya da yazılımların kullanılması,
- Stalking (ısrarlı takip).

**3. İtibara ve güvenilirliğe zarar verilmesi:**

- E-postaları ve içeriği onay olmadan silme, gönderme, değiştirme,
- Kullanıcısının itibarına zarar vermek amacıyla gerçek dışı kişisel veriler (çevrimiçi hesaplar, reklamlar veya sosyal medya hesapları gibi) oluşturma ve paylaşma,
- Sahte fotoğraf ve video düzenleme, oluşturma,
- Kimlik hırsızlığı (örneğin bir profil oluşturup onu herkese açık olarak yayınlama ve paylaşımlar yapma),
- Birinin itibarını zedelemek amacıyla özel (kültürel olarak hassas/tartışmalı) bilgileri yayma,
- Bir kişinin itibarını zedelemek üzere (saldırganlık/ hakaret içeren) rahatsız edici, aşağılayıcı ve yanlış bilgi içeren çevrimiçi yorumlar ve ilanlar yapma.

**4. Taciz (buna çevrimdışı taciz eşlik edebilir):**

- İstenmeyen mesajlar yoluyla “siber zorbalık” ve tekrarlanan taciz ile dikkat çekme,
- Cinsel ve fiziksel şiddet tehditleri de dahil olmak üzere doğrudan şiddet tehditleri (örneğin ‘sana tecavüz edeceğim’ gibi tehditler),
- Küfürlü yorumlar,
- Cinsel içerikli materyallerin istenmeyen şekilde gönderilmesi, alınması,
- Fiziksel şiddete teşvik,
- Sosyal medya mesajları ve e-posta yolu ile cinsiyeti, cinsel kimliği hedef alan nefret içerikli konuşma,
- Kadınları cinsel nesneler olarak gösteren çevrimiçi içerik,
- Cinsiyetçi yorumlar yapma
- Bir bireyden ziyade bir grup insan tarafından mobbing yapılması veya taciz amaçlı bir hedef seçme ve özellikle teknoloji tarafından kolaylaştırılan bir uygulama olarak mobbing kullanılması.

**5. Doğrudan tehditler ve şiddet:**

- Kişi seçimi (planlanan cinsel saldırı, teknoloji kullanımı yoluyla kadın ticareti dahil),
- Cinsiyetleştirilmiş şantaj ve gasp,
- Kimlik, para ve mülkiyet hırsızlığı,
- Fiziksel saldırıya neden olan kimliğe bürünme.

**6. Topluluklara yönelik hedefli saldırılar:**

- Bazı kuruluşların ve toplulukların web sitelerinin, sosyal medya hesaplarının, e-posta hesaplarının ele geçirilmesi,
- Faaliyetlerin gözlemlenmesi ve izlenmesi,
- Topluluk üyelerine doğrudan şiddet tehditleri,
- Sığınmaevi adresleri gibi gizli bilgilerin açıklanması.

# DİJİTAL GÜVENLİK ÖNERİLERİ

İnternette % 100 güvenlikten söz etmek mümkün olmasa da kullanıcıların daha güvenli iletişim kurmaları mümkün. İnternet kullanıcıları yeni medya okuryazarlıklarını geliştirerek, doğru yöntemleri ve araçları kullanarak farklı düzeylerde dijital 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 olarak çevrimiçi aktivitelerimizle kişisel bilgilerimize dair arkamızda birçok dijital iz bırakırız.

Günümüzde basit bir Google aramasıyla herhangi biri sizin hakkınızda birçok bilgi elde edebilir. Bunun için **hacker** olmasına gerek yoktur. Sosyal medyada yaptığınız gönüllü paylaşımlar, sizin rutinleriniz, özel bilgileriniz, kişiliğiniz hakkında bilgiler içermekte ve başkalarına sizin kişiliğiniz, duygu durumunuz, sosyal yaşantınız hakkında fazlasıyla bilgi vermektedir. Kötü niyetli kişiler ya da gruplar bu bilgileri toplayarak size zarar verebilirler.

- **Gizli modda** açtığınız bir tarayıcıda kişisel bilgilerinizi aratabilir, çıkan sonuçları analiz edebilir, **sizinle ilgili hangi bilgilerin herkesin erişimine açık olduğunu tespit edebilir,** Facebook, LinkedIn vb. profillerinizde hangi bilgilerin erişimine izin verdiğinizi kontrol edebilir, hesabınıza erişim sağlayan uygulamaları görüp değiştirebilirsiniz.

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


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

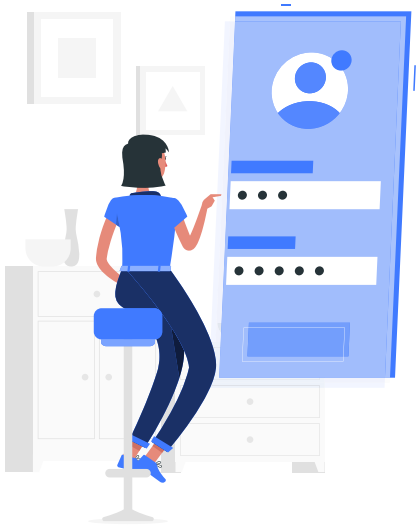
**Google verilerinizi indirmek için:**
https://takeout.google.com/

**Facebook verilerinizi indirmek 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

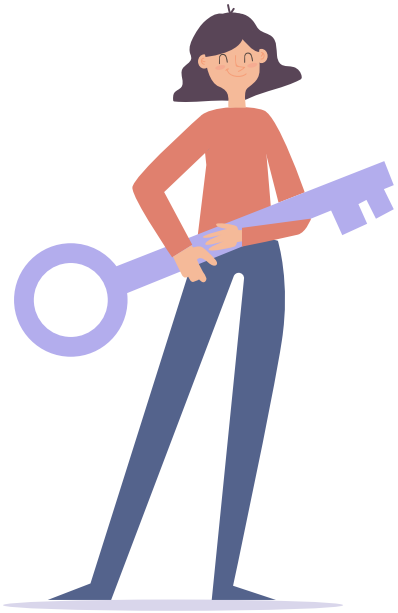
• İnternet kafeler, çıktı almak veya e-mail atmak amacıyla bilgisayar kullandığınız kırtasiyeler, fotokopi merkezleri gibi herkesin erişimine açık mekanlardaki cihazlarda kişisel parolanızı kullanmayın, e-alışveriş yapmayın. Tanımadığınız cihazlarda e-posta veya sosyal medya hesaplarınıza parolanızla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

• Kamuya açık kablosuz ağlar (WIFI) üzerinden şifrelerinizin ve 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 ve başkalarının sizin izniniz olmadan 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. Çünkü bir site üzerinde şifrenizi kıran biri, aynı şifreyi başka sitelerde de deneyecektir.

- 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 olduğu için bunları saklamak ve yönetmek için açık kaynaklı ve ücretsiz iki yazılımdan yararlanabilirsiniz: **keepassx.org** ve **encryptr.org.** IOS ve Android cep telefonu için ise **keepass.info** yazılımı. Bu yazılımlarla tek bir ana parolayla tüm şifrelerinizi güvenli bir şekilde saklayabilirsiniz.


- **İki adımda doğrulama uygulamasını** mutlaka kullanın. Hesabınızın bulunduğu Facebook, Twitter, Instagram gibi sosyal ağlarınıza giriş yaparken iki aşamalı doğrulama yöntemini uygulayarak hesabınızı koruma altına alabilirsiniz. İki adımda/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. Google/Gmail hesabınızı korumak için **Authenticator**'ı kurarak iki aşamalı doğrulama sağlayabilirsiniz.

**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. Genellikle okumadan onay verdiğimiz Kullanıcı Sözleşmeleri'nde verilerinizin ticari kuruluşlarla paylaşıldığına dair 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 **İzinsiz paylaşılan mahrem görüntülerle** ilgili destek merkezinden yardım alabilirsiniz: https://www.facebook.com/safety/notwithoutmyconsent

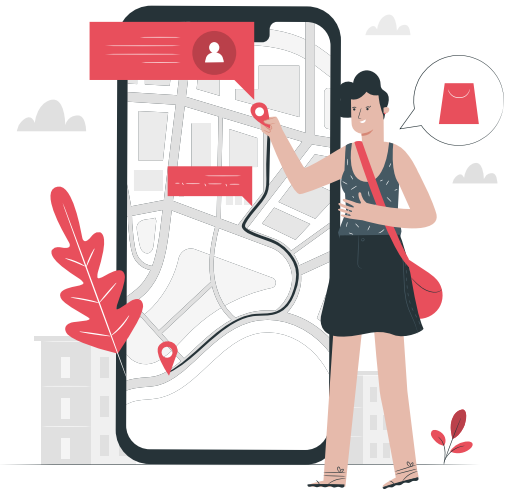
- Sosyal medyada tanıdığınız veya tanımadığınız bir kişi, kişiler ya da gruplar tarafından hedef gösterilirseniz, küçük düşürücü, hakaret içeren, itibarsızlaştırıcı vb. mesajlara maruz kalırsanız ekran görüntüsünü alarak kanıt toplayıp hukuki süreçlere başvurabilirsiniz. Ekran görüntüsünde gönderenin 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 platformlarında (Twitter, Facebook, Instagram, Linkedin, Youtube vs.) uygulamalar bölümünde sizin dışınızda kurulmuş birçok uygulama göreceksiniz. 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 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:

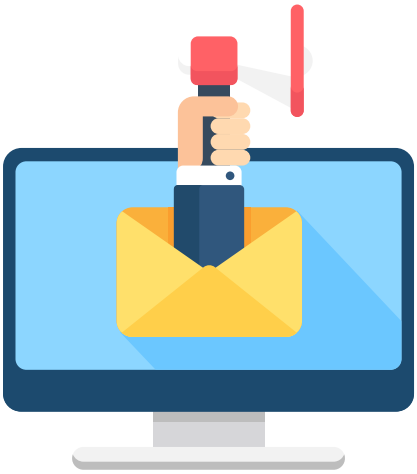
**Google:**
https://learndigital.withgoogle.com/dijitalatolye/course/online-safety/module/3000

**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/about/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 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.

- IRC eski olmasına rağmen hala en güvenli mesaj gönderme programlarından biridir.

**Arama motoru güvenliği**

- Google gibi ticari bir arama motoru yerine **DuckDuckGo** gibi alternatif ve kişisel bilgilerinizi takip edip satmayan 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 Electronic Frontier Foundation tarafından üretilen **HTTPS Everywhere** ve **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 **urlsan.io, 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.

- Exif Tag Remover (www.rlvision.com/) kullanarak da görüntülerinizde yer alan metaveriyi kaldırabilirsiniz.

**Özgür yazılım**

- Şirket gözetimini azaltmak için kullandığınız uygulamaların/programların özgür yazılım olanlarını tercih etmeye çalışın. Çünkü kullandığımız kapalı kaynak uygulamaların birçoğu cihazlarımızdaki özel verilerimize (konum, rehber, medya, fotoğraf, video vs.) ulaşmak ve ağ trafiğimizi kaydetmek için bizlerden izin istemektedir. Açık kaynaklı özgür yazılım uygulamalar bu izinleri istemez, kişisel verilerinizi ticari amaçlarla kullanmak için depolamazlar.

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


**VPN**

- **TOR** gibi VPN programlarını kullanarak sansürü aşabilirsiniz. Bu programlar IP numaranızı değiştirerek sizi farklı ülkelerden giriş yapar gibi gösterir ve yasaklı sitelere erişim sağlar. Bilgisayarınıza TOR kurabilmek için gettor@torproject.com adresine e-posta atarak talepte bulunabilirsiniz. Cep telefonunda TOR kurmak istediğinizde **Orbot** programını indirebilirsiniz.

**Bulut güvenliği**

- Kullandığınız cihazların ve hizmet sağlayıcıların çoğu, verilerinizin kaybolmaması için ücretli veya ücretsiz bulut hizmeti sunarlar. Google Drive, iCloud gibi size sunulan bulut sistemleri, cihazınız çalındığında ya da bozulduğunda verilerinizin kaybolmaması için pratik bir çözüm olarak görünse de aslında kullanıcı üzerindeki gözetimi daha da derinleştirirler. Sizin için özel olan ve başkalarıyla paylaşmak istemediğiniz bilgileriniz/görüntüleriniz varsa kullandığınız cihazlarda **Otomatik yedekle/senkronize et** seçeneklerini tercih etmeyerek verilerinizin otomatik olarak buluta yüklenmesinin önüne geçebilirsiniz.

- Verilerinizi yedeklemek için **SpiderOak** ve **Mega** gibi daha güvenli bulut hizmetlerini kullanabilirsiniz. Dosyalarınızı şifreleyip kullandığınız bulut sistemlerine şifrelenmiş halini atabilirsiniz.


# 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 gibi çeşitli kaynaklardan 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, işlerin 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, bir kadın danışma merkezinden destek alın.

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

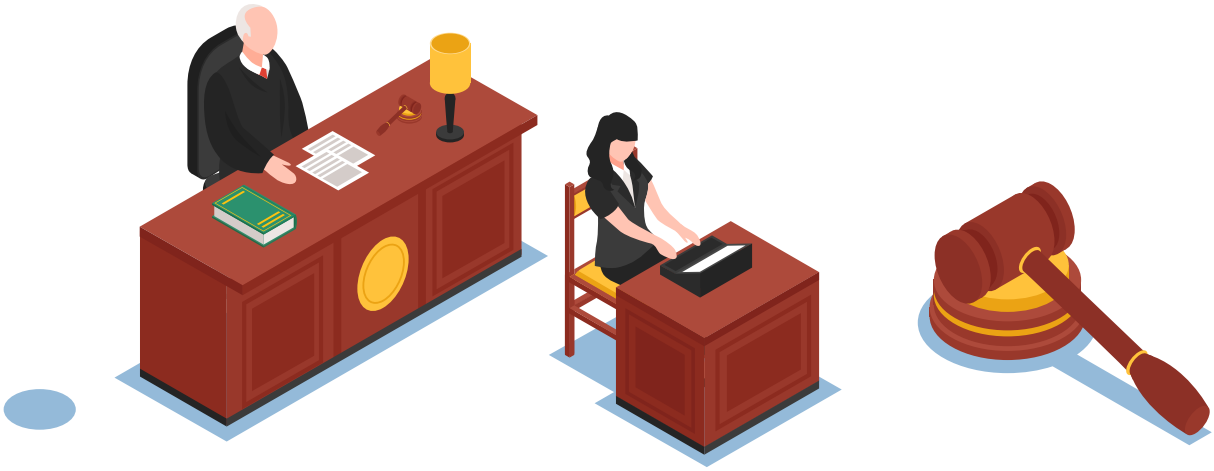
- En yakın kolluk birimi veya savcılığa suç duyurusunda bulunabilirsiniz. Ayrıca acil önlem alınması gereken bir durum varsa, 6284 sayılı yasada düzenlenen uzaklaştırma kararı alınması gibi önlemlere başvurulmalıdır. Maddi, manevi zarar varsa tazminat davası açılabilir.

- 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 internet şirketlerinin hem de politikacıların bu konuda çözüm üretmelerini sağlamak üzere dijital aktivizm yapabilirsiniz.



# 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**<br><br>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**<br><br>Kişiler arasındaki haberleşmenin gizliliğini ihlal etmek.<br><br>Bu gizlilik ihlalinin haberleşme içeriklerinin kaydı suretiyle gerçekleşmesi.<br><br>Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa etmek.<br><br>Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa etmek.<br><br>İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması<br><br>**Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması TCK Madde 133**<br><br>Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinlemek veya bunları bir ses alma cihazı ile kaydetmek<br><br>Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kaydetmek | - Bir yıldan üç yıla kadar hapis cezası<br><br>- Verilecek ceza bir kat artırılır.<br><br>- İki yıldan beş yıla kadar hapis cezası<br><br>- Bir yıldan üç yıla kadar hapis cezası<br><br>- Bir yıldan üç yıla kadar hapis cezası<br><br>- Altı aydan iki yıla kadar hapis veya adlî para cezası<br><br>- İki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası |

| | | |
|---|---|---|
| | Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa etmek<br><br>İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması<br><br>Aynı zamanda özel hayatın gizliliğini ihlal, kişisel verilerin ihlali gibi suçlar da oluşabilir. | - İki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası |
| 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**<br><br>Kişilerin özel hayatının gizliliğini ihlal etmek<br><br>Görüntü veya ses kaydı alarak gizlilik ihlali<br><br>Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa etmek<br><br>İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması<br><br>Aynı zamanda kişisel verilerin ifşası da söz konusu olabilir.<br><br>**Tehdit – TCK Madde 106**<br><br>Bir başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden bahisle tehdit etmek<br><br>Malvarlığı itibarıyla büyük bir zarara uğratacağından veya sair bir kötülük edeceğinden bahisle tehdit<br><br>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<br><br>Tehdit amacıyla kasten öldürme, kasten yaralama veya malvarlığına zarar verme suçunun işlenmesi | - Bir yıldan üç yıla kadar hapis cezası<br><br>- Verilecek ceza bir kat artırılır<br><br>- İki yıldan beş yıla kadar hapis cezası<br><br>- İki yıldan beş yıla kadar hapis cezası<br><br>- Altı aydan iki yıla kadar hapis cezası<br><br>- Altı aya kadar hapis veya adlî para cezası<br><br>- İki yıldan beş yıla kadar hapis cezası<br><br>- 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**<br>**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**<br>**Madde 105**<br><br>Bir kimseyi cinsel amaçlı olarak taciz etmek<br><br>Fiilin çocuğa karşı işlenmesi<br><br>a) Kamu görevinin veya hizmet ilişkisinin ya da aile içi ilişkinin sağladığı kolaylıktan faydalanmak suretiyle,<br><br>b) Vasi, eğitici, öğretici, bakıcı, koruyucu aile veya sağlık hizmeti veren ya da koruma, bakım veya gözetim yükümlülüğü bulunan kişiler tarafından,<br><br>c) Aynı işyerinde çalışmanın sağladığı kolaylıktan faydalanmak suretiyle,<br><br>d) Posta veya elektronik haberleşme araçlarının sağladığı kolaylıktan faydalanmak suretiyle,<br><br>e) Teşhir suretiyle, işlenmesi<br><br>Bu fiil nedeniyle mağdurun; işi bırakmak, okuldan veya ailesinden ayrılmak zorunda kalması. | - Üç aydan iki yıla kadar hapis cezası veya adlî para cezası<br><br>- Altı aydan üç yıla kadar hapis cezası<br><br>- Yukarıdaki fıkraya göre verilecek ceza yarı oranında artırılır.<br><br>- 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**<br>**TCK Madde 135**<br><br>Hukuka aykırı olarak kişisel verileri kaydetmek<br><br>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<br><br>- 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;<br><br>a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,<br><br>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**<br>**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**<br>**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)<br><br>Birinci fıkrada yer alan suçun;<br><br>a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,<br><br>b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,<br><br>c) Aynı konutta beraber yaşayan kardeşlerden birinin, Zararına olarak işlenmesi hâlinde.<br><br>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<br><br>-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**<br><br>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**<br><br>**Mağdurun belirlenmesi TCK Madde 126**<br><br>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.<br><br>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**<br><br>Halkın bir kesimini, sosyal sınıf, ırk, din, mezhep, cinsiyet veya bölge farklılığına dayanarak alenen aşağılamak.<br><br>Halkın bir kesiminin benimsediği dini değerleri alenen aşağılamak.<br>(Bu fiilin kamu barışını bozmaya elverişli olması halinde) | - Altı aydan bir yıla kadar hapis cezası<br><br>- 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**<br><br>**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.**<br><br>**Marka hakkına tecavüz, 6769 s. Yasa hükümleri**<br><br>**5651 s. Yasa hükümleri.** | İlgili yasalarda belirtilen tazminat hükümleri uygulanır.<br><br>İlgili yasada belirtilen tazminat ve cezai hükümler uygulanır.<br><br>Erişim engelleme ve içeriğin kaldırılması. |

| | | |
|---|---|---|
| Kontrol etme: Kişinin sosyal medya paylaşımlarına karışmak, sosyal medya iletişimini sınırlandırmaya çalışmak | **Haberleşmenin engellenmesi**<br>**TCK Madde 124**<br><br>Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi<br><br>Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engellemek.<br><br>Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi.<br><br>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<br><br>- Bir yıldan beş yıla kadar hapis cezası<br><br>- İkinci fıkra hükmüne göre cezaya hükmolunur.<br><br>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**<br>**TCK Madde 106**<br><br>**Şantaj**<br>**TCK Madde 107**<br><br>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<br><br>Kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunmak. | - Cezaları yukarıda açıklandı.<br><br>- Bir yıldan üç yıla kadar hapis ve beşbin güne kadar adlî para cezası<br><br>- Birinci fıkraya göre cezaya hükmolunur. |
| Kişisel veri ifşası: Kişinin kişisel verilerini ifşa etmek | **Kişisel verilerin kaydedilmesi**<br>**Verileri hukuka aykırı olarak verme veya ele geçirme**<br>**TCK Madde 135, 136, 137, 138**<br><br>6698 s. KVKK<br>MADDE 18. Kabahatler<br>Aydınlatma yükümlülüğü ve veri güvenliğine ilişkin yükümlülükleri yerine getirmemek. | - Cezaları yukarıda açıklandı.<br><br>- 5000 ile 1.000.000 Türk lirasına kadar idari para cezası. |

AVRUPA BİRLİĞİ
SivilDüşün

“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.”

# A GUIDE TO FIGHT DIGITAL GENDER-BASED VIOLENCE


Toplumsal Bilgi ve İletişim Derneği

alternatif bilişim

AVRUPA BİRLİĞİ
SivilDüşün

**Authors:**
Gülüm Şener
İlden Dirini
Nurcihan Temur
Şebnem Ahi
Şevket Uyanık

**Translation:**
Sevda Akyüz
Nedime Mercangöz

**Design:**
Fatih Akdoğan

**December, 2019**



“This e-guide has been prepared for the European Union Sivil Düşün Program with the EU support. The TBİD and AltBil are solely responsible for the content and this e-guide does not reflect the EU perspective.”

# Contents

# WHAT IS DIGITAL GENDER-BASED VIOLENCE?

As internet access increased, the widespread use of mobile information and social media brought on digital violence, which is a new form of gender based violence.

Women actively using social media and internet platforms encounter threats and comments directly targeting their gender, sexual identity and personal security.

Violence against women of all ages is considered as a violation of human rights and a type of sexist discrimination. In the Istanbul Convention,[1] violence is defined not only in physical, but also sexual, psychological and economic forms, and as a consequence of gender-based inequality.

Gender-based violence includes domestic violence, spouse violence, dating violence and digital violence.

Digital gender-based violence is not categorized under any type of violence. As it contains cases that overlap with all other types of violence, it needs to be classified as a new type or form.

[1] Istanbul Convention, E. (2011). Council of Europe Convention on preventing and combating violence against women and domestic violence. Violence against women and domestic violence. https://rm.coe.int/1680462545

**Online violence: Continuation of offline violence**

Women are subjected to different forms of violence in real life (offline life) due to gender-based inequalities. Those same inequalities target and threaten the security of women in cyberspace (online life) in different demographic statuses.

It must not be forgotten that digital violence is not a separate concept from violence in 'real' life; and that it is a continuation of offline violence (domestic violence, violence against women) fed by the same inequalities.

The gender stereotypes that involve inequality and sexism in offline environment are also reflected in online environment.

**Digital violence? Cyber violence? Virtual violence? Or online violence?**

When the relevant studies and reports are examined, it can be seen that the digital violence women are subjected to is not entirely conceptualized. We encounter this subject under different headings: cyber violence, virtual violence, digital violence or online violence.

As the number of studies on the subject increases, concepts will be formulated more precisely, but it is vital that the definitions have a feminist perspective.

**Who's exposed to digital violence?**

Gender-based violence as a result of online abuse can target men or women. Similarly, children can also be subjected to online abuse and violence. However, as online abuse and gender-based violence stems from the same structural inequalities and sexual discrimination as the other types of violence, the rate of violence women are subjected to is higher.[2]

According to the data in the UN report titled "Cyber Violence Against Women and Girls –a Worldwide Wake up Call,"[3] the probability of women's exposure to violence all over the world is 27 times higher than that of men. Just like any area, the internet is also a domain where gender-based violence is seen.

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

[3] UN. (2015). Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call. http://www.unwomen. org/-/media/headquarters/attachments/sections/library/ publications/2015/cyber_violence_gender%20report. pdf?vs=4259

**Intersectional discrimination and digital violence that affect different demographic statuses of women**

Women can be exposed to cyber bullying based on their education, age, ethnic background, sexual orientation or relationship status.

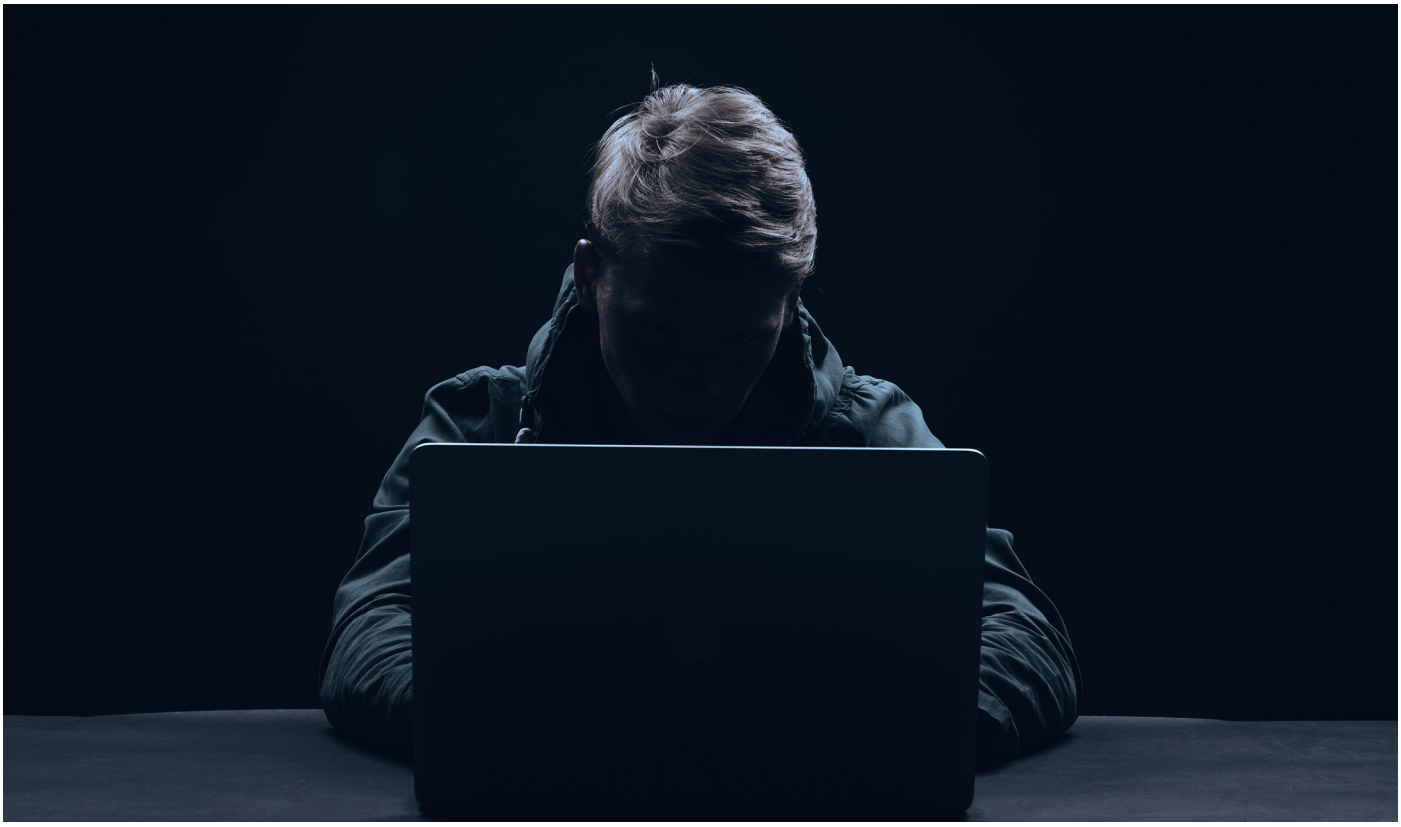
In the report titled “Gender based Violence and Online Abuse,”[4] it is predicted that women who are more visible in online and offline environments can be exposed to abuse more in online platforms. LBTQ+ women, female journalists (including blog writers), women active in tech industries, female public figures (artists, writers, and so on), female politicians, female academics, and feminist activists can be openly targeted from time to time by the perpetrators of digital violence.

**Who are the perpetrators of digital violence?**

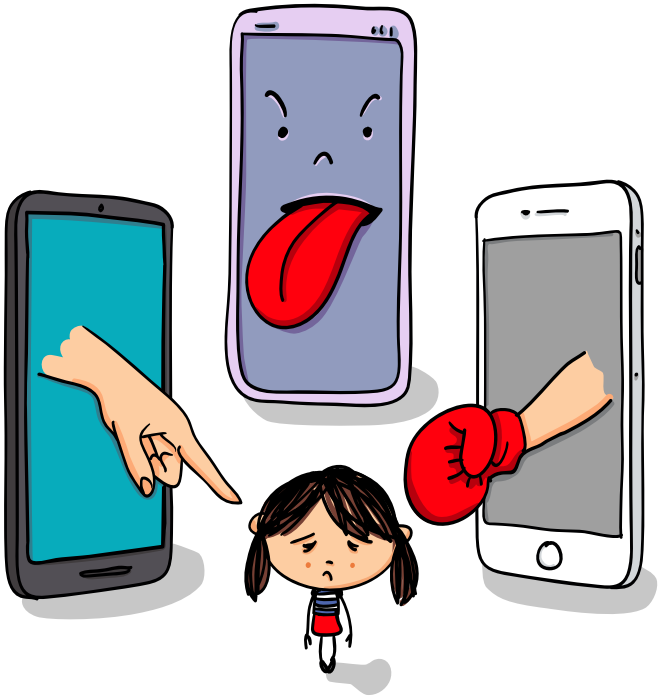
The perpetrators of digital violence can be ex- or current spouses/partners, neighbours, work/school friends, relatives or strangers.

The perpetrators of digital violence use social media, messaging apps, Global Positioning System (GPS)-based apps, smart phones and/or e-mail to cause anxiety in their victims about their personal security.

Most online abuse and gender-based violence is committed via anonymous or fake name accounts, which makes it hard to track down the perpetrators.



[4] ibid.



# TYPES OF GENDER-BASED DIGITAL VIOLENCE

**Defining characteristics**

In the study titled "Voices from digital spaces: technology related violence against women,"[5] five defining characteristics of digital violence against women have been listed:

**Anonymity** the perpetrator may not be known by the victim.

**Action Distance** the abuse may be directed from any distance without physical contact.

**Automation** the online abusive acts or cyber bullying require less time and effort.

**Accessibility** the technological variety and economic feasibility render women as easy prey for perpetrators.

**Distribution and Continuity** texts and photos copied on the internet can spread without limits or can stay there for a long time.

European Gender Equality Institute started to categorize cyber stalking in its report titled "Cyber Violence Against Women."[6]

---

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

[6] EIGE. (2017). Cyber Violence Against Women and Girls. Retrieved from http://eige.europa.eu/rdc/ 6 eige-publications/cyber-violence-against-women-and-girls

**Cyber Stalking**

Cyber stalking means following somebody via e-mail, texts (online messages) or the Internet. When done repeatedly, harmless or not, stalking/following undermines the stalked person's sense of security, and causes anxiety, fear or alarm.

Stalking is following somebody in stealth mode. The person doing this act is called a stalker. The term stalking is used for repeated acts of threats and/or harassment that cause fear and anxiety via email or other computer-based communication channels.

The report titled "Cyber violence against women and girls"[8] also defines "cyber harassment" and "cyber exploitation" as subclasses of cyber violence:

**Cyber Harassment**

Cyber harassment can manifest itself in various forms as listed below:

- Unwanted email, texts (or online messages) with sexual content;
- Inappropriate or aggressive acts on social media or internet chat rooms;
- Threats of physical and/or sexual violence via e-mail, text (or online messages);
- Hate speech, or behavior that insults, threatens, or targets someone for their identity (gender), and other characteristics (sexual orientation or disability).

[7] Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology, and stalking. Violence against women, 13(8), 842-856.

[8] ibid.

**Cyber Exploitation**

Cyber exploitation is also known as revenge porn.[9] It refers to online distribution of photos or videos without permission of the person featuring in them.

The perpetrator is usually an ex-partner or spouse who took or recorded the images during a former relationship and uses it to retaliate and humiliate the person. However, the perpetrators may not always be ex-spouses or lovers. It may not always be done for revenge, either. The images may be obtained by hacking into a person's computer, social media accounts or phone, aiming to cause real damage to the 'real life' of the target.

**Other Types and Definitions**

The Internet Governance Forum hosted by the UN dealt with "Gender-Based Violence and Online Abuse." The report prepared at the end of the Forum[10] categorized concepts of gender-based digital/cyber/online violence into six sub-categories with examples:

**1. Violation of privacy:**

- Access to personal data without the permission of the individual (including hacking of personal accounts, stealing of passwords, identity theft, accessing another user's computer while using an account, and 'cyber exploitation'),
- Taking, accessing, using, manipulating, and distributing photos and videos without someone's permission,
- Sharing and distributing personal information including images (of a sexual nature), sound bites, and video clips without a person's knowledge and consent,
- Doxing (online researching and reaching personal information), searching for and publishing private or identifying information without the consent of the individual for harassment or other malicious intent, using that information for violence and harassment of a woman in the 'real' world,
- Contacting a user via their kids, families or co-workers, and harassing them.

**2. Spying and monitoring:**

- Spying and monitoring online and offline activities,
- Using spyware or keyboard recorders without the consent of the user,
- Using GPS or software to track the movements of a woman without her consent,
- Stalking.

[9] The concept widely used as revenge porn may further exacerbate the discrimination against the victim; therefore, the term cyber exploitation is preferred.

[10] IGF. (2015). Internet Governance Forum-Best Practice Forum on Online Abuse and Gender-Based Violence Against Women. http://www.intgovforum.org/cms/documents/best-practice-forums/623-bpf-online-abuse-and-gbv-against-women/file.

**3. Character defamation:**

- Deleting, sending, altering e-mail messages and content without the consent of the individual,
- Fabricating and sharing fake personal data to discredit someone (such as via online accounts, ads or social media profiles),
- Creating fake photos and videos,
- Identity theft (for example, creating, and publishing a profile and sharing public posts there),
- Publishing private (culturally sensitive or controversial) information in order to discredit someone,
- Making disturbing, humiliating and false comments and announcements online (containing aggressiveness or insults) in order to discredit someone

**4. Harassment (this can be accompanied by offline harassment):**

- Attracting attention through cyber bullying and repeated harassment by sending unwanted messages,
- Direct threats of violence including those of a sexual and physical kind (for example, 'I'll rape you'),
- Comments with swear words,
- Sending and receiving unsolicited material with sexual content,
- Encouragement for physical violence,
- Hate speech through social media messages and e-mail, targeting gender and sexual identity,
- Online content that objectifies women,
- Making sexist comments,
- Mobbing by a group rather than by an individual, targeting someone for harassment and use of mobbing as an application especially facilitated by technology.

**5. Direct threats and violence:**

- Selection of the person (including planned sexual attack, and trafficking in women by using technology),
- Sexual blackmail or sextortion and assault,
- Identity, money and property theft,
- Assuming the identity of someone, leading to physical assault.

**6. Targeting groups:**

- Hacking the websites, social media accounts and e-mail accounts of some institutions and communities,
- Monitoring and spying on their activities,
- Direct threats of violence targeting community members,
- Revealing classified information such as the addresses of women's shelters.

# DIGITAL SECURITY TIPS

Even though it is not possible to talk about a 100% security on the Internet, users can establish more secure communication. Internet users can improve their new media literacy and use the right methods and tools to ensure digital security at different levels.

**Digital footprint**

Every move and click of internet users are recorded for later use; and personal information turn into lucrative data for corporations. We leave a lot of digital footprints with our online activities on a daily basis.

Today, anyone can get a lot of information about you by a simple Google search. They don't need to be a **hacker** to do that. Your voluntary shares on social media reveal your routine, private information, personality, mood, and social life to others. People or groups with malicious intent can harm you by collecting this data.

- On a browser you open in **Incognito mode**, you can search for your personal information, analyze the results, and detect **what kind of information is public about you**. You can also check what kind of information you allow public access on your Facebook, LinkedIn, etc. profiles, and change the privacy settings.

- Clear your browser **history** and **cookies** in your devices often. If you do not work in your own devices, use 'Incognito mode.'


• You can ask platforms like Google, Facebook, Instagram, and Twitter to share the information they gathered on you and download them to your computer. This way, you can see and archive your activities so far using these accounts. However, this will not delete your data from the internet.

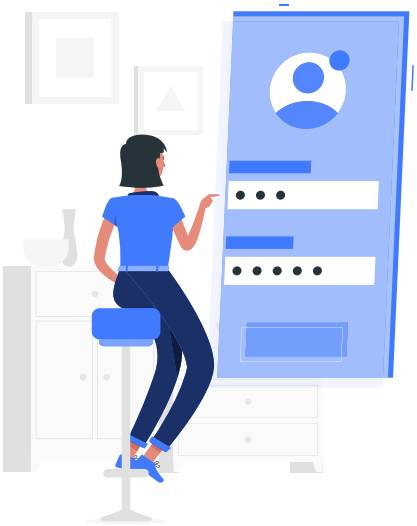
**To download your Google data**
https://takeout.google.com/

**To download your Facebook data:**
https://www.facebook.com/help/212802592074644

**To download your Twitter data:**
https://help.twitter.com/tr/managing-your-account/how-to-download-your-twitter-archive

**To download your Instagram data:**
https://www.instagram.com/download/request

**To download your Linkedin data:**
https://www.linkedin.com/psettings/member-data



**Connection Security**

• Do not use your personal password or do online shopping on computers in public places like internet cafes, photocopiers or stationery stores to get print outs or send email. If you access your email or social media accounts on unknown devices, do not forget to **log out** when you are done.

• Your passwords and personal data can be hacked over public access WIFI. Try not to use such connections.

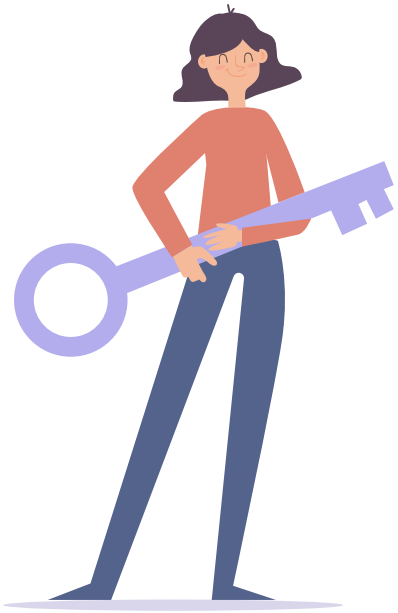
**Device security**

• Always use **passwords** and **screen locks** in your devices (computer, tablet, smart phone, etc.) to prevent access by others. The data in your digital devices belong to you and unauthorized people should not ask for your passwords or use your devices and check the information on them.

• In a healthy relationship, people do not feel the need to restrict and check up on each other. If your partner expects you to send your location, take and send photos from everywhere you go, and answer every message instantly, this is an indication that he is stalking you.

**Password security**

- Your passwords for internet platforms and digital devices should **not be simple or easily predictable**. They should not contain names, birthdates, ID numbers, wedding anniversaries, phone numbers, etc.



- In your passwords, try not to use your personal information that can be predicted by people in your life. Your partner, spouse, friend, etc. may find out what your password is and use it to check up on your online communication with others. Your password is personal, and no one has the right to know it.

- Prefer passwords that are not coherent wholes, and that contain numbers, upper and lower case letters, as well as signs. **For example: N/1i2*H3-a4!X8**

- Set **different passwords** for all the services, websites, social media platforms. Don't use the same password for a variety of sites because if it is hacked, it can be tried in other platforms as well.

- Renew your password at least every six months.

- Your answers to the security questions when setting your password should not be 'real.' For example, if you choose the name of your first pet as your security question, you should not give the real name of your pet as it can be easily guessed by others. Similarly, it can also be predicted through the information you share on social media.

- As it is difficult to remember all these passwords, you can use two open source and free software programs to store and manage them: **keepassx.org** and **encryptr.org.** For IOS and Android cell phones, you can use keepass.info. With the help of these programs, you can safely keep all your passwords using one main password.


- Make sure to use the **two-step verification** system. You can protect your accounts on social media platforms like Facebook, Twitter, Instagram by using this two-step verification. In this system, if someone tries to access your account from a different device, you get a warning message. So, if you activated the two-step verification, they cannot access your account even if they know your password. You can activate this system in the Settings/Security Settings sections of your social media and email accounts. In order to protect your Google/Gmail account, you can set up **Authenticator** and use this two step system.

**Social media security**

- You can check who gets to see your information other than the social media platforms you shared them with if you read the Terms of Service carefully and in detail. The terms of service that we usually approve without reading may contain articles stating that your data is shared with corporations.

- You can check and restrict who you want to share your social media profile and posts in the **Privacy Settings/ Security Settings** sections. To do that, just visit these sections in your social media platforms and manage the settings in detail.

- If you activate **Timeline Approval** and **Tag Approval** features on Facebook, your approval will be asked when your friends or acquaintances want to tag you in a post or share something on your timeline.

- When you receive irritating messages/posts, you can use the **Report** feature offered by social media platforms, **block the perpetrator** of digital violence, and get their account to be closed.

- You can also report discriminatory, sexist comments or hate speech posts **directed at others** on social media platforms to contribute to the fight against digital violence.

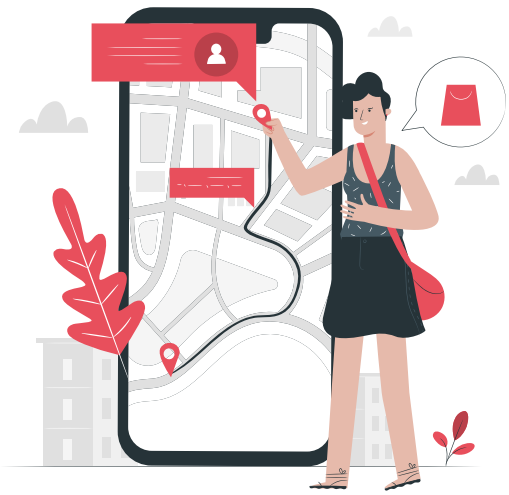
- You can get help from **Facebook's support center** about private images shared without consent: https://www.facebook.com/safety/notwithoutmyconsent

- If you are targeted and subjected to humiliating, insulting and discrediting messages by people or groups known or unknown to you on social media, you can get a screenshot, gather evidence, and start the legal process. Make sure that the name of the sender, as well as the date and time of the post appear on the screenshot. You can ask for legal support from the bar associations; get information from civil society organizations and centers working on gender and women's rights.

- You will see many applications that you do not use in all social media platforms (Twitter, Facebook, Instagram, Linkedin, Youtube, etc.). These are tasked with reading and writing messages or texting on your behalf. Make sure to remove the unused ones.

- Social media facilitates stalking between people and may feed their obsessions. The perpetrators may track your activities, get information about you and your location to gain control over you on social media unless you block them. If you feel threatened, you can **block the perpetrator and delete them** from all means of communication. You can create a safe communication environment with "zero communication."

- The perpetrators may try to befriend your friends on social media to track your activities. In that case, you can inform your friends, and ask them not to share any information related to you, and to support you.



- If you suspect you are being followed, **avoid sharing your location** as much as possible. Regularly clean your location history on your devices.

- In a trusting relationship, your partner wouldn't interfere with what you share on social media or who you befriend. Your social media profile is personal; and you should be in charge of its content.

- You can visit the links below for security suggestions against digital harassment/online violence on social media platforms:

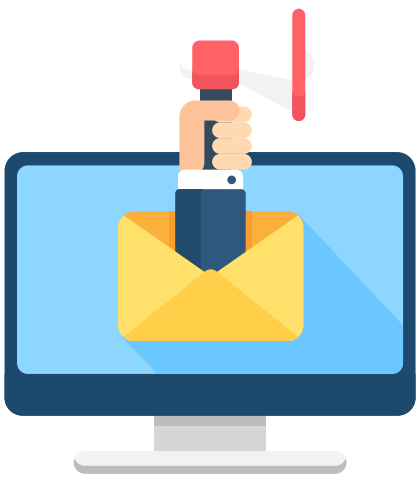
**Google:**
https://learndigital.withgoogle.com/dijitalatolye/course/online-safety/module/3000

**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/about/policies/#community-guidelines



**E-mail security**

- Do not click on generic private messages or email claiming you won something and whose origin or sender you do not know. They may be carrying a virus and steal your personal information.

- You can encode and safely send your email messages via software like **PGP (Pretty Good Privacy), TutaNota.de, ProtonMail.**

- You can have an alternative email address from **RiseUp** etc, form e-mail groups and get more secure communication service.

**Secure messaging**

- You can use **Signal** as a more secure alternative to Whatsapp messaging app. Signal offers end-to-end encoded messages for your short texts as well as clearing your chats from all servers after reading and two step confirmation.

- Even though it is old, **IRC** is still one of the most secure messaging programs.

**Search engine security**

- You may want to prefer an alternative search engine to Google like DuckDuckGo, which is not commercial, and does not track or sell your personal information.


**Website security:**

- You should prefer websites starting with the more secure **https://** instead of http:// website addresses.

- You can add the extensions **HTTPS Everywhere** and **PrivacyBadger** on your web browser, produced by Electronic Frontier Foundation. This way, you can stay away from commercials and cookies and have a more secure communication.

- You can verify the security of a link sent to you by a friend or unknown user by consulting websites such as **urlsan.io, phishtank.com** or **urlex.org** before clicking on them.

**Deleting metadata**

- Make sure to turn off the geotag feature on your mobile phone when you take photos or shoot videos.

- You can also remove the metadata on your images by using Exif Tag Remover (www.rlvision.com/).

**Open source**

- Try to choose open source apps or programs in order to decrease corporation monitoring because many closed source apps ask to access your private data in your devices (location, contact list, media, phots, videos, etc) and record your network traffic. Open source free apps do not ask for such permissions, and they do not store your personal data for commercial purposes.

- ou can download **F Droid** in Google Play for Android phones and find the open source equivalents for the apps you are currently using.

**VPN**

- You can bypass censorship by using VPN programs like **TOR**. These programs change your IP number to make you look as if you connect from a different country and give you access to banned sites. You can send an email to gettor@torproject.com in order to set up TOR on your computer. If you want to set up TOR on your cell phone, you can download **Orbot** program.


**Cloud security**

- Most servers and devices you use offer cloud service with a charge or for free in order to store your data. Even though cloud systems like Google Drive, iCloud seem to be practical solutions to keep your data intact in case your device is stolen or gets broken down, they actually deepen the surveillance on the user. If you have private information or images that you do not want to share with others, do not use the automatic Back-up / Synchronize options on your devices in order to avoid automatic upload of your data onto the cloud.

- In order to back up your data, you can use more secure cloud servers such as SpiderOak and Mega. You can also encode your files and upload them to the cloud in that secure mode.


# TACTICS AGAINST DIGITAL HARASSMENT

Perpetrators of digital violence are usually very determined to stay in control; and technology is one of many tools they use to do just that. If the perpetrator seems to know a lot about you, he/she may be collecting this information by tracking your devices, accessing your online accounts, monitoring your location or collecting online data about you.

Becoming an online target may make you feel as if things are getting out of control. There are, however, protective measures you can take without blaming yourself. Here are some of them:

- Gather data to identify the perpetrator and document what happened. Documenting a series of events may demonstrate to the police or the court that there is a pattern of stalking or harassment. The documents can also help you see an increase in activity and plan your security accordingly.

- Get a screenshot. Screenshots are very fundamental and useful tools to store information you gather on the internet.

- You can report the irritating online behavior to the website or app it happened on. If the behavior is in violation of the terms of service of the platform, that content can be removed or the person can be banned. It is important to know that the report content can be totally removed; therefore, evidence should be documented before reporting.

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

- Share your experience with people you trust, get support from a women's consultation center.

- Consult lawyers specializing in this area to learn about the legal processes. Talk to Women's Consultancy Centers of the Bar Organizations.

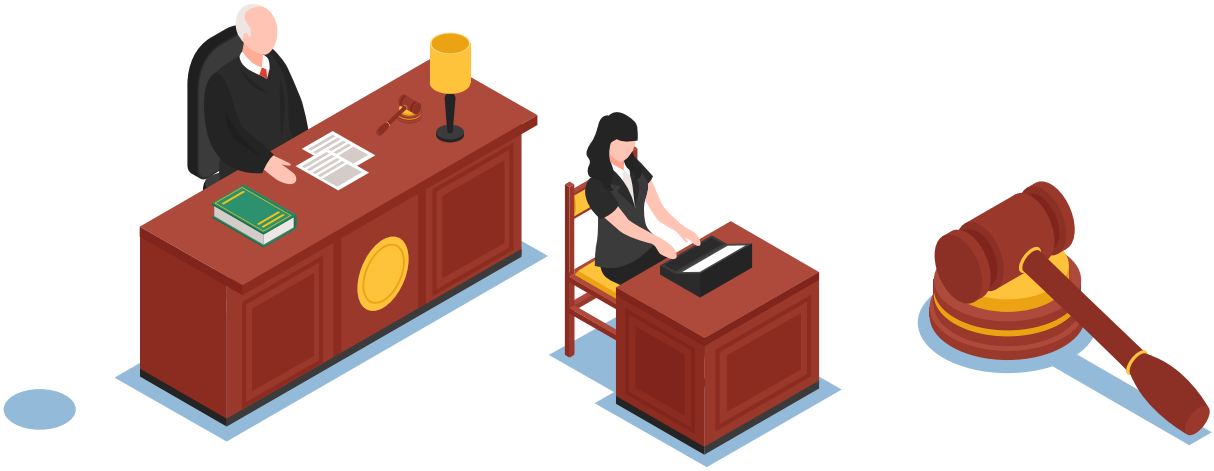
- You can file a complaint with the nearest police precinct or the prosecutor's office. Also, if urgent intervention is required, you should demand a restraint order regulated in Act 6284. It is also possible to file a lawsuit for punitive damages.

- You can demand that the content be removed according to Act 5651. If the related content is not considered critical, and if it is not based on a real decision, the person who does not want to be associated with this content can still demand its removal as part of their right to be ignored. If the right conditions for legal counselling have emerged, a lawyer can be demanded.

- In any case, it is vital for the victim to know their rights in the eyes of the law and raise their awareness about the legal process as well as knowing what constitutes a crime.

- You can complain about acts of lynching, sexist rhetoric, and digital violence against other people, too. This way, you can help the accounts of the perpetrators get terminated.

- You can organize online and offline campaigns to raise awareness about the fight against gender based digital violence; create an agenda; and engage in digital activism to get both internet companies and politicians to come up with solutions.



# LEGAL ASPECTS OF DIGITAL VIOLENCE IN TURKEY

| Digital Violence Action | Under the scope of which crime/law | What are the possible sanctions? |
|---|---|---|
| Persistent tracking: Sending messages or calling continuously, forcing to report location or send photos. Insisting on establishing communication even though he/she states that he/she does not want or respond. | **Deterioration of peace and order of people**<br>**Turkish Penal Code Article 123**<br><br>Calling another person insistently or making noise with the intention of deteriorating peace and order or executing any other unlawful act for this purpose. | Upon the complaint of the victim, the perpetrator is sentenced to imprisonment from three months to one year. |
| Disclosure of private correspondence and images | **Violation of Communicational Secrecy**<br>**Turkish Penal Code**<br>**Article 132**<br><br>Violation of secrecy of communication between persons.<br><br>Secrecy is violated by by recording contents of communication between persons<br><br>Unlawful disclosure of contents of communication between himself and others without obtaining their consent.<br><br>Unlawful and public disclosure of the content of communication with himself without obtaining the consent of the other party<br><br>Disclosure of data through press and broadcast<br><br>**Tapping and recording of conversations between individuals**<br>**Turkish Penal Code Article 133**<br><br>Any non-general conversations between the individuals listened to through a device without obtaining the consent of any of the parties or recording these conversations by use of a recorder | - One to three years of imprisonment<br><br>- The sentence is increased by one half.<br><br>- Two to five years of imprisonment<br><br>- One to three years of imprisonment<br><br>- One to three years of imprisonment<br><br>- Six months to two years of imprisonment or punitive fine |

| | | |
|---|---|---|
| | Recording a conversation not open to public with a recorder without the consent of the participants<br><br>Disclosing unlawfully the data obtained by recording conversations not open to public between persons<br><br>Disclosure of data through press and broadcast<br><br>Other crimes such as violation of privacy and violation of personal data may occur at the same time. | - Two to five years of imprisonment and punitive fine up to four thousand days<br><br>- Two to five years of imprisonment and punitive fine up to four thousand days |
| Cyber exploitation / Sexual blackmail: Shooting intimate images of a person and threatening by sharing them and/or sharing them with others on the Internet, social networks or private messaging | **Violation of Privacy**<br>**Turkish Penal Code Article 134**<br><br>Violating secrecy of private life<br><br>Privacy violation by use of audio-visual recording<br><br>Unlawful disclosure of images or sounds of one's private life<br><br>Disclosure of data through press and broadcast<br><br>Disclosure of personal data is also possible. | - Imprisonment from one to three years<br><br>- The penalty to be imposed is increased by one half<br><br>- Two to five years of imprisonment<br><br>- Two to five years of imprisonment |
| | **Threat –**<br>**Turkish Penal Code**<br>**Article 106**<br><br>Threatening another person by saying that he intents to kill himself or one of his relatives, or to violate corporal or sexual immunity of others<br><br>Threatening by causing a great property loss or other misconduct | - Six months to two years of imprisonment<br><br>- Up to six months of imprisonment or punitive fine |

| | | |
|---|---|---|
| | Threatening; a) with a gun, b) by unsigned letter or use of special signs concealing one's identity, c) by more than one person, d) by taking advantage of the terror actions of existing or potential organized groups, | - Two to five years of imprisonment |
| | In case of commission of defense by threat resulting from felonious homicide, felonious injury or damage to property<br><br>If threatening statements are directed to a person through social media, the same crime will be considered as committed. Together with the offense of insult and in connection with the same action, this crime is also committed. | - Additional punishment from these offenses. |
| | **Defamation**<br>**Turkish Penal Code**<br>**Article 125** | |
| | Any person who attacks with the intention to harm the honor, reputation or dignity of another person through concrete performance or giving impression of intent<br><br>In order to punish the offense committed in absentia of the victim, the act should be committed in presence of at least three persons. | - Three months to two years of imprisonment or punitive fine |
| | The commission of offense in writing or by use of audio and visual means directed to the aggrieved party. | - Three months to two years of imprisonment or punitive fine |
| | In case of commission of offense with defamatory intent a) against a public officer b) due to disclosure, change or attempt to spread religious, political, social and philosophical belief, opinions and convictions and to obey the orders and the restriction of one's religion; c) by mentioning sacred values in view of the religion with which a person is connected, | - The minimum limit of the punishment to be imposed may not be less than a year. |

| | | |
|---|---|---|
| | Open Defamation<br><br>In case of public officers working as a committee to perform a duty, then the offence is considered to have committed against the members forming the committee. In this case, the provisions of the article relating to successive offense applies. | The punishment to be imposed is increased by one sixth. |
| Cyber Harassment: Sending a person messages and/ or messages or images with sexual content without his/her consent | **Sexual harassment**<br>**Article 105**<br><br>If a person is subject to sexual harassment by another person<br><br>- Commission of the offense against a child<br><br>- a) by taking advantage of the convenience of public office or service relationship or family relationship;<br><br>b) by persons who offer services as guardian, educator, instructor, caregiver, foster family or healthcare or persons with the obligation of protection, care and supervision<br><br>c) benefiting from the convenience of working in the same workplace,<br><br>d) benefiting from the convenience offered by post or electronic communication tools,<br><br>e) by exposure<br><br>The victim is obliged to leave the business place, school or house for this reason | - Three months to two years of imprisonment or punitive fine<br><br>- Six months to three years of imprisonment<br><br>- The punishment to be imposed according to the above paragraph is increased by one half.<br><br>- The punishment to be imposed may not be less than a year. |

| | | |
|---|---|---|
| Privacy violation: Retrieving the person's e-mail and/or social media passwords and accessing their accounts, checking the information on their devices without permission | **Recording of personal data Turkish Penal Code Article 135** | |
| | Recording of personal data unlawfully | - One to three years of imprisonment |
| | Recording the political, philosophical or religious concepts of individuals, or recording unlawfully personal information relating to their sexual origins, ethical tendencies, health conditions or connections with syndicates | - The punishment to be imposed in accordance with the first paragraph shall be increased by half. |
| | **Giving or acquiring data unlawfully Turkish Penal Code Article 136** | |
| | Giving, disseminating or acquiring personal data unlawfully | - Two to four years of imprisonment |
| | The subject of the offense shall be the statements and images recorded in accordance with paragraphs 236 / 5-6 of the Turkish Penal Code | - The punishment to be imposed is increased by one half. |
| | **Qualified forms of offense**<br>**Turkish Penal Code Article 137** | |
| | In case of commission of the offenses defined in above articles; a) by a public officer or due influence based on public office, b) by exploiting the advantages of a performed profession and art, | - The punishment to be imposed is increased by one half. |
| | **Destruction of data Turkish Penal Code Article 138** | |
| | Failure to fulfill the duties of those responsible for destroying the data within the system despite the expiry of the legally prescribed period | - One to two years of imprisonment |
| | If the subject of the offense is data that need to be eliminated or destroyed according to the provisions of the Code of Criminal Procedure. | - The punishment to be imposed is increased by one half. |

| | | |
|---|---|---|
| | **Accessing the data processing system**<br>**Turkish Penal Code Article 243** | |
| | Accessing a part or whole of the data processing system and remaining there unlawfully | - Up to one year of imprisonment or punitive fine |
| | Committing the abovementioned offenses which involve systems which are benefited against charge | - The punishment to be imposed is increased up by one half. |
| | Deletion or alteration of data within the content of the system due to this offense | - Six months to two years of imprisonment |
| | Monitoring illegally the data transmissions that occur in an information system itself or between the information systems without entering the system by means of technical tools | - One to three years of imprisonment |
| | **Hindrance or destruction of the system, deletion or alteration of data**<br>**Turkish Penal Code**<br>**Article 244** | |
| | Hindering or destroying operation of a data processing system | - One to five years of imprisonment |
| | Garbling, deleting, changing or preventing access to data, or installing data in the system or sending available data to other places | - Six months to three years of imprisonment |
| | Committing these offenses on the data processing systems of a bank or credit institution or a public institution or corporation | - The punishment to be imposed is increased by one half. |
| | Execution of the abovementioned acts not constituting any other offense apart from unjust benefit secured by a person for himself or others | - Two to six years of imprisonment and up to five thousand days of punitive fine |

| | | |
|---|---|---|
| | **Improper Use of Bank or Credit Cards**<br>**Turkish Penal Code**<br>**Article 245** | |
| | Any person who acquires or holds bank or credit cards of another person(s) whatever the reason is, or uses these cards without consent of the card holder or the receiver of the card, or secures benefit for himself or third parties by allowing use of the same by others | - Three to six years of imprisonment and up to five thousand days of punitive fine |
| | Producing, selling, transferring, purchasing or accepting counterfeit bank or credit cards by linking them with the bank accounts of others | - Three to seven years of imprisonment and up to ten thousand of punitive fine |
| | Any person who secures benefit for himself or others by using a counterfeit or falsified bank or credit card (unless the act constitutes an offense that requires a more severe punishment) | -Four to eight years of imprisonment and up to five thousand years of punitive fine |
| Kişi adına internette sahte hesaplar açarak onun adına paylaşım yapmak | If the offense in the first paragraph is committed to the detriment of<br><br>a) one of the spouses whose separation decision has not been made,<br><br>b) lineal kinship or one of such a brother-in-law or adopted,<br><br>c) one of the siblings living together in the same dwelling. The effective remorse provisions relating to crimes against the assets of this Law shall apply to the acts falling within the scope of the first paragraph. | - No punishment is imposed on the relative |

| | | |
|---|---|---|
| Opening fake accounts on the internet on behalf of the person and sharing posts | **Unlawful delivery or acquisition of data**<br>**Turkish Penal Code**<br>**Article 136**<br><br>In addition, through these accounts, the insult crime may occur, or secrecy of private life may be violated. Or a person's memory may be insulted. Such an offense may also be committed against legal persons. | The punishments are explained above. |
| Hate speech: Sharing humiliating, insulting, sexist messages on the Internet, social media, digital games, messaging applications, targeting people and exposing them to virtual lynch | **Defamation Turkish Penal Code Article 125**<br><br>**Determination of the aggrieved party Turkish Penal Code Article 126**<br><br>Even if the name of the aggrieved party is not clearly indicated or the accusation is implicitly expressed, both the name of the aggrieved party and the act of defamation is assumed to have been declared provided that there is clear indication of defamation of a person's character based on the quality of the offense.<br><br>**Provoking people to be rancorous and hostile**<br>**Article 216/2**<br><br>Any person who openly provokes a group of people belonging to different social class, religion, race, sect, or coming from another origin, to be rancorous or hostile against another group<br><br>Openly disrespecting the religious belief of group. (If this act is conducive to disrupt public peace) | The punishments are described above.<br><br>Regulated by Article 126 of the Turkish Penal Code, targeting a person or a member of a group through media or through conventional means of media is a criminal offense<br><br>- Six months to one year of imprisonment<br><br>- Six months to one year of imprisonment |

| | | |
|---|---|---|
| Doxxing: To collect detailed information about the person on the internet and to disseminate and use this information to cause harm to the person. | **Unlawful delivery or acquisition of data**<br><br>**Turkish Penal Code Article 136** | The punishments are explained above. |
| Defamation: Sharing posts in a way that damages a person's commercial reputation, revealing trade secrets | **Compensation for violation of personal rights**<br>**Civil Code Article 24**<br><br>**Turkish Commercial Code Article 56 Unfair Competition**<br><br>Infringement of trademark right, Provisions of the Law No. 6769<br><br>Provisions of the Law Number 5651 | The compensation provisions specified in the relevant laws shall apply.<br><br>Compensation and penal provisions specified in the relevant law shall apply.<br><br>Blocking access and removing content. |
| Checking: Checking a person's social media posts, trying to limit social media communication | **Prevention of communication**<br>**Turkish Penal Code Article 124**<br><br>Unlawful prevention of communication among persons<br><br>Unlawful prevention of communication among the public institutions<br><br>Unlawful prevention of broadcasts or announcements of all kinds of press and publication organs.<br><br>In addition, violation of constitutional rights such as freedom of expression, the right to receive information and the right to information could also be possible. | - Six months to two years of imprisonment or punitive fine<br><br>- One to five years of imprisonment<br><br>- Punishable according to paragraph two.<br><br>The relevant penal provisions and compensation provisions of the Turkish Penal Code and other laws shall apply according to the relevant act. |

| | | |
|---|---|---|
| Threat / Blackmail:<br>Using digital means to threaten and blackmail with death, sexual assault and physical violence | **Threat**<br>**Turkish Penal Code Article 106**<br><br>**Blackmail**<br>**Turkish Penal Code Article 107**<br><br>Any person who forces a person to perform an act contrary to the law; or to execute or not to execute a duty beyond his responsibility; or to derive unjust benefit from a thing by declaring his will to perform or not to perform an obligation which he is entitled to do so<br><br>Threatening to reveal or charge with issues that may harm the dignity or prestige of a person to derive benefit for himself or others | - Punishment is explained above.<br><br>- One year to three years of imprisonment and up to five thousand days of punitive fine<br><br>- Punishable according to paragraph one. |
| Disclosure of personal data: disclosing personal data of persons | **Recording personal data**<br>**Unlawful delivery or acquisition of data**<br>**Turkish Penal Code**<br>**Articles 135, 136, 137, 138**<br><br>Law No. 6698 for the Protection of Personal Data<br><br>ARTICLE 18. Misdemeanors<br>Failure to comply with the obligations of disclosure and data security. | - Punishment is explained above.<br><br>- Punitive fine of up to 5000 to 1,000,000 Turkish Lira |


“This e-guide has been prepared for the European Union Sivil Düşün Program with the EU support. The TBİD and AltBil are solely responsible for the content and this e-guide does not reflect the EU perspective.”