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

ISBN 978-605-62169-9-2

Aralık, 2019

Alternatif Bilişim Derneği
Dikmen Cad. No: 220-B/8 Çankaya / Ankara
bilgi@alternatifbilisim.org
http://www.alternatifbilisim.org

“Bu e-rehber, Avrupa Birliği Sivil Düşün Programı kapsamında Avrupa Birliği desteği ile hazırlanmıştır. İçeriğin sorumluluğu tamamıyla TBİD ve Alternatif Bilişim’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.

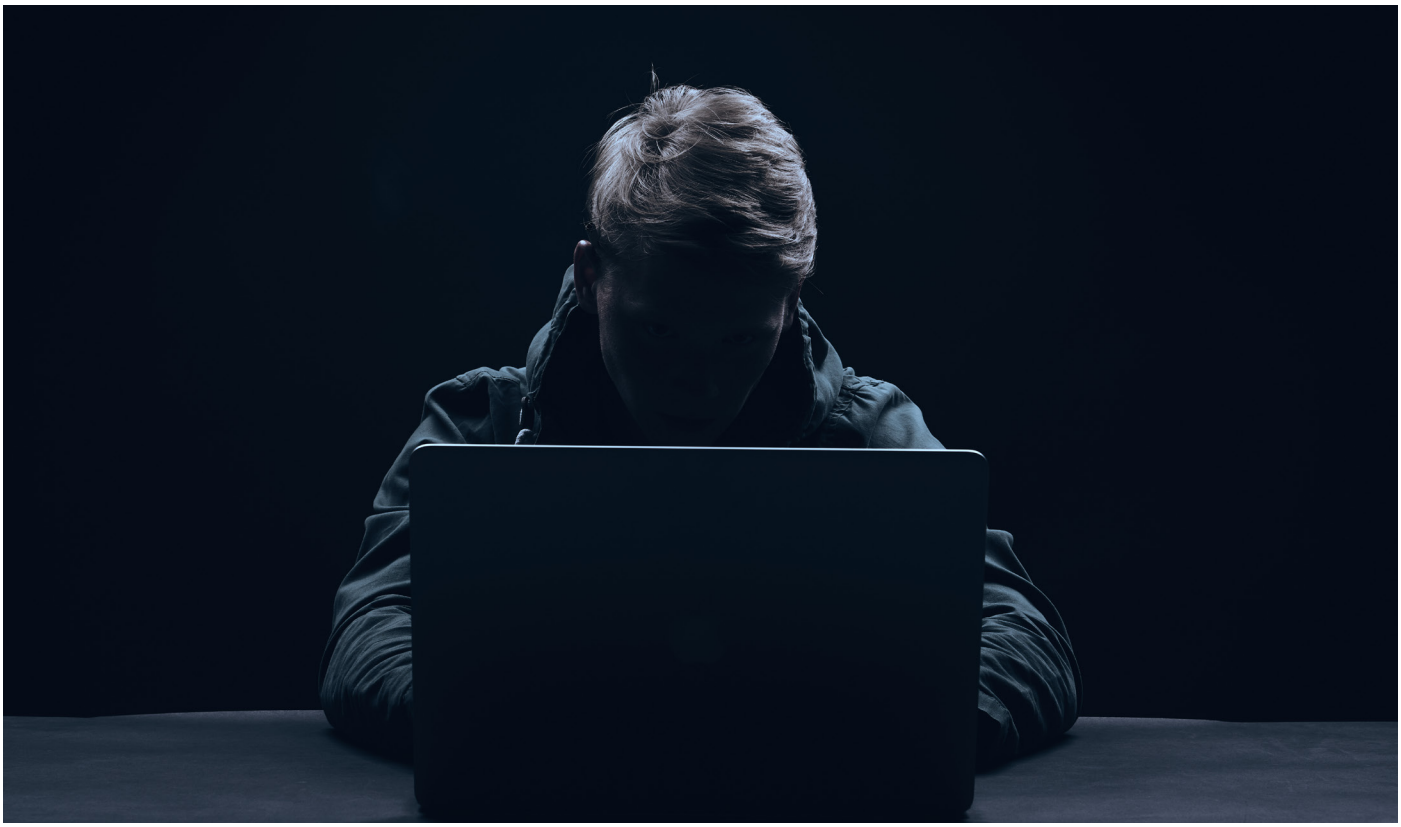
"Toplumsal Cinsiyete Dayalı Şiddet ve Çevrimiçi / Online İstismar" raporunda[4] çevrimiçi veya çevrimdışı ortamlarda öne çıkan kadınlara, çevrimiçi alanda daha fazla suistimale maruz kalabilecekleri çıktısı yer alır. LBTQ+ kadınlar, kadın gazeteciler (blog yazarları dahil), teknoloji endüstrisinde aktif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

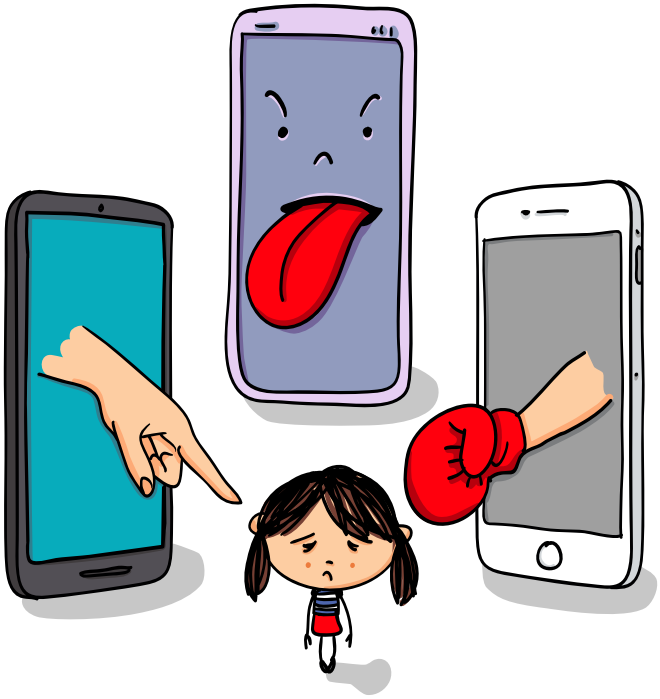
Dijital şiddeti uygulayan kişi eski ya da şu anki eş / partner, komşu, iş / okul arkadaşı, bir yakın ya da bir yabancı olabilmektedir.

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.

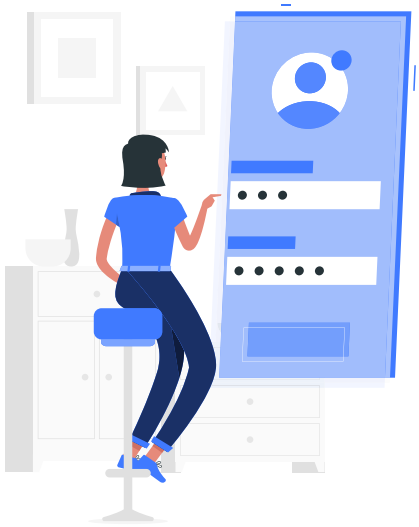
Google verilerinizi indirmek için:
https://takeout.google.com/

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

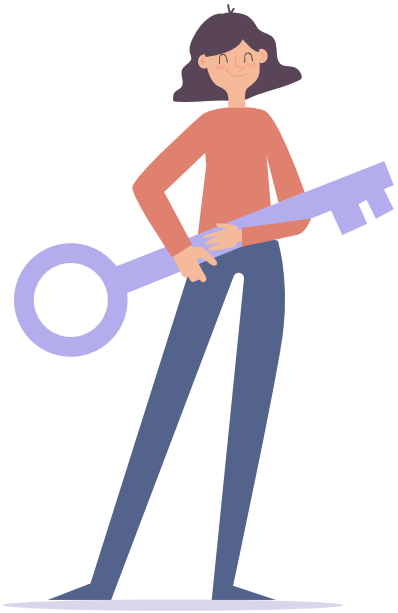
• İnternet kafeler, çıktı almak veya e-mail atmak amacıyla bilgisayar kullandığınız kırtasiyeler, fotokopi merkezleri gibi herkesin erişimine açık mekanlardaki cihazlarda kişisel parolanızı kullanmayın, e-alışveriş yapmayın. Tanımadığınız cihazlarda e-posta veya sosyal medya hesaplarınıza parolanızla 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

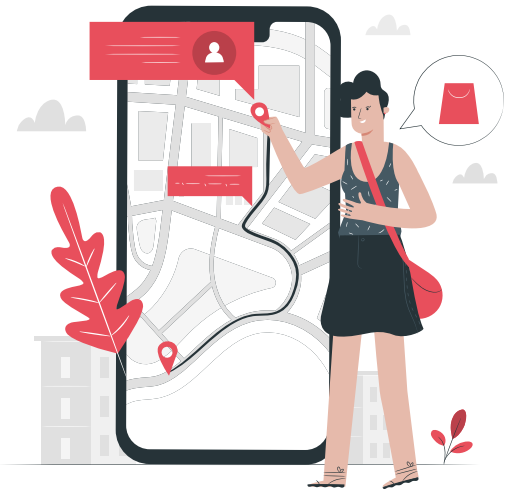
- Sosyal medyada tanıdığınız veya tanımadığınız bir kişi, kişiler ya da gruplar tarafından hedef gösterilirseniz, küçük düşürücü, hakaret içeren, itibarsızlaştırıcı vb. mesajlara maruz kalırsanız ekran görüntüsünü alarak kanıt toplayıp hukuki süreçlere başvurabilirsiniz. Ekran görüntüsünde gönderenin 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:

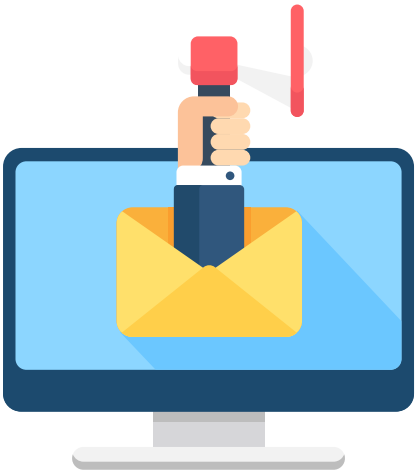
Google:
https://learndigital.withgoogle.com/dijitalatolye/course/online-safety/module/3000

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.

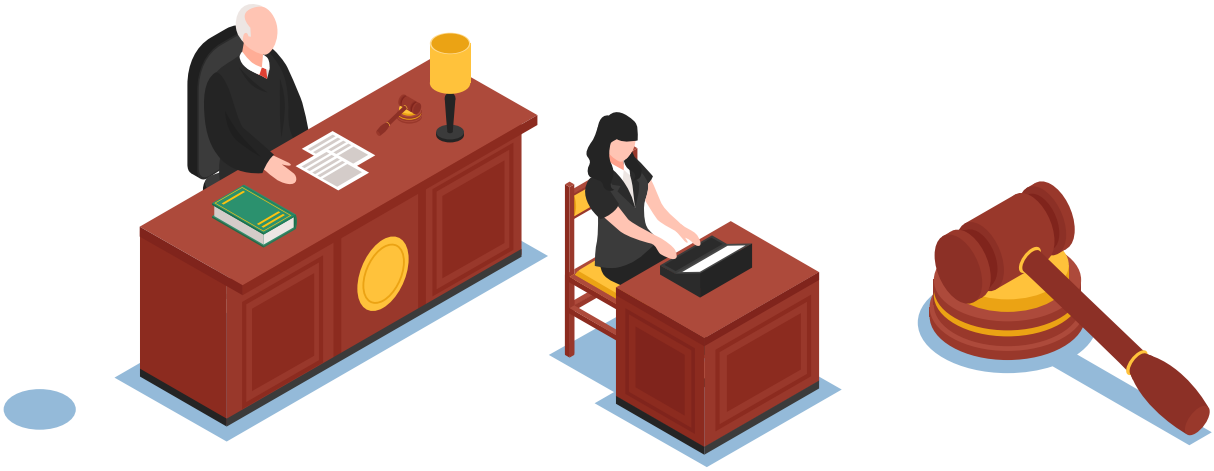
- En yakın kolluk birimi veya savcılığa suç duyurusunda bulunabilirsiniz. Ayrıca acil önlem alınması gereken bir durum varsa, 6284 sayılı yasada düzenlenen uzaklaştırma kararı alınması gibi önlemlere başvurulmalıdır. Maddi, manevi zarar varsa tazminat davası açılabilir.

- 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** Sırf huzur ve sükûnunu bozmak maksadıyla bir kimseye ısrarla; telefon edilmesi, gürültü yapılması ya da aynı maksatla hukuka aykırı başka bir davranışta bulunulması.	Mağdurun şikayeti üzerine faile üç aydan bir yıla kadar hapis cezası verilir.
Kişiler arasındaki özel yazışmaların, görüntülerin ifşası.	**Haberleşmenin Gizliliğini İhlal - TCK Madde 132** Kişiler arasındaki haberleşmenin gizliliğini ihlal etmek. Bu gizlilik ihlalinin haberleşme içeriklerinin kaydı suretiyle gerçekleşmesi. Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa etmek. Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa etmek. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması **Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması TCK Madde 133** Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinlemek veya bunları bir ses alma cihazı ile kaydetmek Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kaydetmek	- Bir yıldan üç yıla kadar hapis cezası - Verilecek ceza bir kat artırılır. - İki yıldan beş yıla kadar hapis cezası - Bir yıldan üç yıla kadar hapis cezası - Bir yıldan üç yıla kadar hapis cezası - Altı aydan iki yıla kadar hapis veya adlî para cezası - 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 İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması 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** Kişilerin özel hayatının gizliliğini ihlal etmek Görüntü veya ses kaydı alarak gizlilik ihlali Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa etmek İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması Aynı zamanda kişisel verilerin ifşası da söz konusu olabilir. **Tehdit – TCK Madde 106** Bir başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden bahisle tehdit etmek Malvarlığı itibarıyla büyük bir zarara uğratacağından veya sair bir kötülük edeceğinden bahisle tehdit 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 Tehdit amacıyla kasten öldürme, kasten yaralama veya malvarlığına zarar verme suçunun işlenmesi	- Bir yıldan üç yıla kadar hapis cezası - Verilecek ceza bir kat artırılır - İki yıldan beş yıla kadar hapis cezası - İki yıldan beş yıla kadar hapis cezası - Altı aydan iki yıla kadar hapis cezası - Altı aya kadar hapis veya adlî para cezası - İki yıldan beş yıla kadar hapis cezası - Ayrıca bu suçlardan dolayı ceza verilir.

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

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

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

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

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

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

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

“Bu e-rehber, Avrupa Birliği Sivil Düşün Programı kapsamında Avrupa Birliği desteği ile hazırlanmıştır. İçerğin sorumluluğu tamamıyla TBİD ve Alternatif Bilişim’e aittir ve AB’nin görüşlerini yansıtmamaktadır.”

ISBN 978-605-62169-9-2