ONTHELINE NEWSROOMS
DEFENDING PRESS FREEDOM

# Haber merkezlerinin çevrimiçi tacize hedef olan gazetecileri desteklemesi için protokol

Uluslararası Basın Enstitüsü (IPI)



## *Giriş*

Tehditler, hakaretler ve karalama kampanyaları dahil olmak üzere gazetecilere yönelik çevrimiçi taciz ve saldırılar, gazetecileri susturmaya ve kamuoyundaki güvenilirliklerini gölgelemeye yönelik bir araç olarak gittikçe artan bir şekilde kullanılmaktadır. Çevrimiçi tacizin ve bunun bilginin serbest dolaşımı üzerindeki olumsuz etkisinin ele alınması çok aktörlü bir yaklaşım gerektirirken, haber merkezlerinin gazetecilerini tacizin yol açabileceği mesleki ve kişisel zararlardan korumak için üstlenmesi gereken anahtar bir rolü vardır. Bu Protokolde, haber merkezlerinin atabileceği belirli adımlar ve alabileceği önlemler verilmektedir.

Bu Protokolde yer alan önlemler, Nisan ve Aralık 2018 arasında beş Avrupa ülkesindeki - Finlandiya, Almanya, Polonya, İspanya ve Birleşik Krallık - 45 haber merkezine yapılan fiziki ziyaretler sırasında ve ayrıca çeşitli ülkelerden uzmanlarla gerçekleştirilen toplantılarda IPI tarafından derlenen verilere dayanmaktadır. IPI hukuk uzmanlarına, sivil toplum temsilcilerine ve akademisyenlere ek olarak, toplamda 110'dan fazla yazı işleri müdürü, gazeteci ve topluluk yöneticisi ile görüşmüştür. Ülke içi ziyaretlerin bir parçası olarak, çevrimiçi tacizin özellikle kadın gazeteciler ve serbest çalışanlar üzerindeki etkisini tartışmak amacıyla bu gruplar ile toplam sekiz odak grup görüşmesi yapılmıştır.

IPI'ın Newsrooms Ontheline programının bir parçası olarak yayınlanan bu Protokol her duruma uygun bir talimat kümesi olarak değil, haber merkezi yöneticilerinin kendilerine özgü koşullar için işe yarayan ve uzun vadede sürdürülebilir olan bir sistem oluşturmalarına yönelik bir başlangıç noktası olarak tasarlanmıştır.

## *İçindekiler*

# Adım 1: Raporlama

## a Haber merkezinde çevrimiçi taciz konusunda bir güvenlik kültürü yaratın

*Yönetim, personelinin ve kuruma katkıda bulunanların karşı karşıya kaldığı saldırı türlerini anlamak ve bu saldırılar hakkındaki tartışmaları normalleştirmek için gerekli tüm adımları atmalıdır.*

- *Dahili bildirim*: Tüm personele bir e-posta göndererek medya kuruluşunun çevrimiçi saldırıları ciddiye aldığını açıkça belirtin. Bu önlem, haber merkezinde güven oluşturmak açısından önemlidir. Bunun yapılması, iki önemli mesaj verir: Birincisi, gazeteciler arasındaki sosyal medyada suistimale hedef olmanın yeni normal olduğu şeklindeki yaygın düşünüşü çürütür ve ikincisi, gazetecilere medya kuruluşunun kendilerini destekleyeceği şeklinde bir emniyet duygusu aşılar.

- *Yazı işleri toplantılarında sürekli olarak çevrimiçi suistimal hakkında konuşun*: Yazı işleri müdürlerinin konuyu gündeme getirmelerinin bir yolu, gazetecilerin yakın zamanda hedef alınıp alınmadığını gayri resmi olarak sormak ve ayrıca gazetecileri suistimale yol açması muhtemel hikayeler ile görevlendirirken saldırı riski konusunda farkındalık oluşturmaktır. Siyasi bir kriz veya toplumsal karmaşa sırasında veya seçimlerden önce, bu tartışmalar daha sık yapılmalıdır.

- Çevrimiçi tacizin etkisini ve bununla mücadele etmeye yönelik önlemlerin etkililiğini değerlendirmek için haber merkezinde *isimsiz bir anket dağıtın*.

> *İspanyol çevrimiçi haber sitesi Publico.es, suistimalin personeli üzerindeki etkisini ve aldığı önlemlerin etkililiğini ölçmek için bir personel anketi gerçekleştirmiştir.*

- Gazetecilerin çalışmalarının sosyal medyadaki yansımaları veya çevrimiçi yorum ve tartışmalar üzerine bir "sağlık kontrolü" yapmak için *sosyal medya ekipleri ile gazeteciler arasında düzenli toplantılar gerçekleştirin*.

- Medya organının kurum içi ağında, şirketin çevrimiçi taciz ile ilgili politikaları ve şirketin bu sorunla başa çıkmak için oluşturduğu araçlar ve protokoller hakkında bilgi içeren *kolay erişilebilir bir bölüm oluşturun*.

> *BBC'nin kurum içi ağında, gazetecilerin bu alandaki travmaları ve kendileri üzerindeki etkisini tartıştığı eğitim filmleri mevcuttur. Bu filmler, travma konusunda bir tür "yeni başlayanlar için kılavuz" görevi görmekte ve konunun anlaşılmasını kolaylaştırmaktadır.*

## b Net raporlama hatları ve raporlama kanalları oluşturun

*Personelin tüm üyeleri ve katkıda bulunanlar, suistimal vakalarının kime ve nasıl rapor edileceğini bilmelidir. Haber merkezleri, saldırıların kolayca rapor edilebileceği ve gazetecilerin destek mekanizmalarına erişebileceği çeşitli kanallar oluşturmalıdır.*

*Gayri resmi raporlama mekanizmaları*:

- *Meslektaşlar ile gayri resmi sohbetleri teşvik edin*: Haber merkezleri, gazetecileri taciz deneyimlerini akranları ve yazı işleri müdürleri ile paylaşmaya teşvik etmelidir. Çevrimiçi saldırılar hakkında açıkça konuşmanın bir zayıflık veya aşırı hassasiyet göstergesi olmadığı açıklanmalıdır.

- WhatsApp, Messenger veya benzer bir platformda (Signal, Telegram, Threema, vb.) gazetecilerin taciz olaylarını paylaşabileceği bir *sohbet grubu oluşturun.* Ortak bir sohbet alanı, konu hakkındaki farkındalığı artırabilir ve bir dayanışma ve topluluk duygusu oluşturabilir.

*Resmi raporlama mekanizmaları*:

- Hedef alınan gazetecilerin çevrimiçi bir saldırıyı kolayca rapor edebilecekleri *çevrimiçi bir form oluşturun*. Form kısa ve doldurması kolay olmalı, ancak saldırı ile ilgili tüm gerekli bilgileri kapsamalıdır.

- Gazetecilerin çevrimiçi tacizi rapor edebileceği özel bir *e-posta adresi oluşturun*.

Resmi raporlama mekanizmaları, bir aksiyon beklentisi yaratır. Bu nedenle gazetecilere, personelin diğer üyelerine ve kuruma katkıda bulunanlara, raporların alınmasından kimin sorumlu olduğu ve söz konusu kişinin hangi adımları atabileceği açıklanmalıdır. Bu kişi taciz konusunda bilgili (tercihen eğitim almış) olmalıdır ve bu kişinin haber merkezindeki konumu, vakaları kurumda resmi bir karşılık verebilecek pozisyondaki kişilere bildirmesine olanak vermelidir.

Olayın üst makamlara bildirilmesinin gerekli olup olmadığına bakılmaksızın, raporlarının dikkate alındığını göstermek ve mekanizmanın güvenilirliğini korumak için olayı rapor eden kişilere bir şekilde yanıt verilmelidir. Son olarak haber merkezleri, kadınların ve azınlıkların orantısız bir şekilde taciz hedefi olduklarını dikkate alarak, raporlama mekanizması koordinatörlerinin bu grupların temsilcilerini içermesini ve/veya kadınları ve azınlıkları hedefleyen belirli saldırı türlerine karşı duyarlı olmalarını sağlamalıdır.

### c Çevrimiçi saldırı ve taciz olaylarını belgeleyin

Bu, bir yandan, saldırılara hedef olan gazetecilerin saldırıların ekran görüntülerini almaları ve ilgili diğer bilgileri kaydetmeleri anlamına gelmektedir. Saldırının kaynaklarını anlamak, bir risk değerlendirmesi yapmak ve medya kuruluşunun - varsa - hangi önlemleri uygulaması gerektiğine karar vermek için yeterli belgelendirme şarttır. Bazı saldırıların yoğunluğu dikkate alındığında, gazeteciler kendi üzerilerindeki yükü azaltmak için belgelendirme sürecinde akranlarından, yazı işleri müdürlerinden veya moderatörlerden yardım almaya teşvik edilmelidir.

Öte yandan, raporlama mekanizmalarının koordine edilmesinden sorumlu olan kişiler, kendilerine bildirilen çevrimiçi taciz olaylarını ve bunlara verilen karşılıklara ilişkin bilgileri takip etmek için bir veri tabanı oluşturmalıdır. Bu veri tabanı, sağlanan destek önlemlerinin ve bunların etkililiğinin izlenmesi için önemlidir (Adım 4 altındaki ilave bilgilere bakın).

## Adım 2: Risk Değerlendirmesi

Çevrimiçi bir saldırı durumunda en uygun destek türünü belirlemek için kapsamlı bir risk değerlendirmesi yapılması önemlidir. Aşağıdaki risk türleri değerlendirilmelidir:

- Çevrimiçi bir saldırının fiziksel bir saldırıya dönüşmesi olasılığı.
- Hedef alınan gazeteciler üzerindeki potansiyel duygusal etkisi ve çalışmaları üzerindeki etkisi.
- Çevrimiçi bir karalama kampanyasının gazetecinin ve/veya haber kuruluşunun itibarına ve güvenilirliğine zarar verme ihtimali.

Bu risk değerlendirmesine dahil olan kişiler, vakadaki belli kriterleri tespit etmelerine ve olayın ne zaman üst makamlara bildirileceğini anlamalarına olanak veren uygun bir eğitim almalıdır. Aşağıda, riskin düzeyini değerlendirmek için kullanılabilecek bir dizi faktör verilmiştir. Risk değerlendirmesi süreci, saldırıların hedeflerini de içermelidir.

### a Fiziksel zarar riski

*Dikkate alınması gereken faktörler:*

- Genel emniyet ortamı (basına yönelik fiziksel saldırıların sıklığı, bu tür saldırıların cezasız kalması, basına yönelik genel düşmanlık ortamı).
- Bireysel bir saldırganın söz konusu olduğu durumlarda, bu birey hakkında bilinen bilgiler temelinde fiziksel saldırı riskinin değerlendirilmesi.
- Saldırı kampanyalarının söz konusu olduğu durumlarda, bireylerin fiziksel bir saldırıda bulunma cesareti bulmaları veya saldırının meşru olduğunu düşünmeleri olasılığı.

### b Psikolojik zarar riski

*Dikkate alınması gereken faktörler:*

Dış unsurlar:

- Hem içerik hem de sıklık olarak tacizin yoğunluğu (tekrar eden “düşük seviyeli” taciz zarar verici olabilir).
- Hedef üzerinde özellikle ciddi bir etkisi olabilecek (cinsiyete, ırka, cinsel yönelime, vb. dayanan) ayrımcı içeriğin varlığı.
- Travma yaratabilecek görüntülerin varlığı.
- Korku ve güven eksikliği oluşturabilecek, gazetecinin gizlice izlendiğini işaret eden mesajlar.
- Hedefin genel destek ağının gücü.

İç unsurlar:

- Hedefin psikolojik durumu: Depresyon veya travma belirtileri.

## c İtibarın zarar görmesi riski

*Dikkate alınması gereken faktörler:*

- Toplumda medyaya yönelik mevcut kutuplaşma ve düşmanlığın derecesi.
- Karalamaların halk nezdinde itibar görmesi olasılığı.
- Çevrimiçi saldırıların daha hızlı yayılmasına olanak veren, örneğin aşağıdakiler gibi faktörler dahil, saldırıların ve karalama kampanyalarının hacmi ve etki alanı:
  - İnternet görselleri *(memes)* ve ayrıntılı grafik tasarımların kullanılması.
  - Zombi bilgisayar ağlarının *(botnets)* kullanılması.
  - Gelecekte tekrar çevrime sokulma potansiyeli olan etiketlerin ve karalamaların kullanılması.
  - Saldırının dezenformasyon üreten internet siteleri tarafından daha da yayılması.
  - Karalama kampanyalarının siyasi, ekonomik ve diğer çıkarlar için düzenlendiği belirtisi.

Yukarıdaki faktörler kişiye özel değildir. Haber merkezlerinin, organize karalama kampanyalarına işaret eden belirtiler dahil olmak üzere fiziksel, psikolojik ve itibarın zarar görmesi risklerini tanımlayabilmek için mesleki eğitime yatırım yapması şiddetle önerilir.

# Adım 3: Destek Mekanizmalarının Uygulanması

Bu bölümde, gazetecilerin çevrimiçi saldırılar veya taciz ile hedef alınması durumunda devreye alınabilecek destek mekanizmalarına genel bir bakış verilmiştir. Bu mekanizmaların hepsinin amacı, gazetecilerin işlerini güvenle yapabilmelerini sağlamaktır.

## a Dijital emniyet desteği

*Bu destek, örneğin aşağıdakileri içerebilir:*

- Tehditleri sosyal medyadaki isimsiz hesaplardan göndermiş olsalar bile, saldırıların arkasındaki kullanıcıların izini sürmek.
- Riski en aza indirmek için hedefin tüm hesaplarını kilitlemek, parolaları değiştirmek, vb.
- Hedefin daha fazla suistimale maruz kalmaması için, yazı işleri müdürü ve meslektaşları hedefin sosyal medya hesaplarını devralmayı önermelidir.

Önleyici tedbirler:

- Gazetecilerin, sosyal medya hesapları yoluyla halkın erişebileceği kişisel bilgiler hakkında bilgi sahibi olmalarını sağlayın. Herhangi bir hassas bilginin kasıtsız olarak açıklanmadığından emin olun.
- Gazetecileri, bilgisayar korsanlarının kişisel verilerine erişmesine ve alenen açığa vurmasına olanak verebilecek potansiyel zayıflıkları belirlemek üzere elektronik cihazlarını tarama konusunda eğitin.

## b Hukuki destek

*Çevrimiçi tacize karşı yasal girişimde bulunulup bulunulmayacağına ilişkin karar, bir dizi faktör dikkate alınarak verilmelidir. Bu faktörler şöyle sıralanabilir:*

- Paylaşımda, bulunduğunuz yargı yetkisi alanına göre yasa dışı içerik bulunup bulunmadığı.
- Dava açmanın, genel olarak gelecekteki çevrimiçi saldırganları engelleme olasılığı.
- Dava açmanın, bu olaydaki belirli saldırganın eylemlerini engelleme olasılığı.
- Belirli bir bağlamda dikkate alındığında, yasal girişimde bulunmanın ilgiyi söz konusu gazeteciye çekme ve diğer saldırıları güçlendirme ve teşvik etme olasılığı.
- Yasal girişimde bulunmanın, çevrimiçi saldırganların halihazırda iddia etmekte olabileceği "güçlü" medya kuruluşlarının "sıradan vatandaşa" saldırdığı hikayesini istemeden pekiştirip bu yüzden ilave saldırılara yol açıp açmayacağı.
- Saldırıları gerçekleştiren bireyin tek başına mı hareket ettiği, yoksa koordine edilmiş bir kampanyaya mı katıldığı. İkinci durumda, yasal girişimde bulunmak ters etki edebilir ve daha fazla saldırıya yol açabilir.
- Saldırının yöneltildiği gazeteci üzerindeki olası etki: Hukuk davası etkilenen gazeteci için bir tatmin sağlayacak mı, yoksa daha fazla duygusal zarara mı yol açacak?
- Savcıların da bir ceza davasından yana olup olmadıkları; olmaları durumunda söz konusu çabayı desteklemek daha kolay olabilir.

İLAVE KAYNAK: IPI'ın Newsrooms Ontheline internet sitesi, bir hukuk davası açarken dikkate alınması gerekenler hakkında bir video serisi içermektedir

## c Duygusal ve psikolojik destek

### Profesyonel psikolojik destek

Profesyonel zihinsel sağlık desteği, gazetecilere yönelik çevrimiçi taciz ve suistimallerin sonuçlarını hafifletmeye yardımcı olmada önemli bir rol oynayabilir. Medya organları, iyi bir uygulama olarak, gazetecilerin kuruluşun sağlık planı yoluyla veya medya organı ile zihinsel sağlık uzmanları arasında yapılan geçici düzenlemeler yoluyla zihinsel sağlık desteğine erişebilmelerini sağlamalıdır.

### Akran desteği

Çevrimiçi taciz ve suistimale hedef olan gazeteciler için, benzer deneyime sahip meslektaşları önemli bir kuvvet, ayrıca saldırılar ve potansiyel sonuçları ile en iyi nasıl başa çıkılabileceği konusunda önemli bir bilgi kaynağı olabilir.

- Yapılandırılmış akran desteği ağları: Çevrimiçi suistimale hedef olmuş akranlarının deneyimlerini dinleyecek ve onlara suistimalin etkileri ile başa çıkma konusunda yol gösterecek haber merkezi personelinden oluşan resmi bir ağ geliştirin. İdeal olarak, bu programlara katılan personel üyeleri yapılandırılmış sohbetler yoluyla travma değerlendirmesi yapma konusunda özel eğitime sahip olmalı ve hedef alınan gazeteciyi haber merkezinde bulunan ve sağlık yardımının yanı sıra hukuki danışmanlık, izleyici moderasyonu, dijital emniyet ve diğer güvenlik mekanizmaları gibi diğer destek türlerine erişimi kolaylaştırabilecek ilgili aktörlere yönlendirebilmelidir.

> *Dart Center'ın akran destek ağının derinlemesine analizini ve Avustralya Yayın Kuruluşundaki uygulamasını inceleyin.*
>
> *BBC'nin akran destek ağını inceleyin.*
>
> *Reuters'in akran destek ağını inceleyin.*

- Mentorluk programları: Daha az deneyimli meslektaşlarına mentorluk etmeleri için kıdemli bir gazeteci görevlendirin. Mentorlar, kendilerine danışan kişilere çevrimiçi suistimali, tipik olarak çevrimiçi suistimale yol açabilecek konuları ve suistimalin alabileceği şekilleri tanıma konusunda yardımcı olmalıdır.
- WhatsApp, Messenger veya benzer bir programdaki bir sohbet grubu sadece tehditleri rapor etmek için değil, aynı zamanda saldırı durumunda destek sağlamak için de kullanılabilir.
- Düzenli sohbetler: Yazı işleri müdürleri, grup ortamlarında çevrimiçi taciz konusunu tartışmaya yönelik fırsatlar yaratmaya teşvik edilmelidir. Buna aşağıdaki gibi örnekler verilebilir:
  - Haber merkezindeki veya diğer medya organlarındaki gazetecilerin, kahvelerini içerken çevrimiçi tacizle başa çıkma deneyimlerini paylaşabilecekleri "kahve sohbetleri" düzenlemek. Bunu deneyimlemiş gazeteciler, çevrimiçi suistimalle mücadeleye dair değerli içgörüler ve ipuçları sağlayabilir ve suistimalin açıkça tartışılabilmesi için alan oluşturmaya yardımcı olabilir.
  - Çevrimiçi tacizi mizahla alt etmek. Saldırılara hedef olan kişiler örneğin aldıkları yorumları bir duvara asmayı düşünebilir. Bu yorumları meslektaşları ile birlikte sesli okumanın veya bunlara gülmenin arındırıcı bir etkisi olabilir. Haber merkezleri, bu tür önlemlerin endişeyi ve gerginliği azaltmaya ve bazı durumlarda saldırıları bir perspektife oturtmada yardımı olduğunu bildiriyor.

### Gazeteciler için öz-bakım planı

Gazeteciler, haber merkezleri ve diğer kuruluşlar tarafından sağlanan önlemler dışında, yoğun çevrimiçi tacize maruz kalmaktan kaynaklanan uzun vadeli travma riskini en aza indirgemek için bir öz-bakım planı geliştirmeye teşvik edilmelidir.

İLAVE KAYNAK: IPI'ın Newsrooms Ontheline internet sitesi, başa çıkma mekanizmaları ile ilgili bir video serisi içermektedir

## d Geçici izin, yer değiştirme ve/veya başka göreve atanma

Hedef alınan gazetecinin yaşadığı duygusal sıkıntının bir değerlendirmesi temelinde, kısa dönemli bir geçici izin oluşabilecek travmayı en aza indirgeyebilir. Bu tür durumlarda izin verilmesi haber merkezlerinde, özellikle kullanıcıların oluşturduğu içerik (KOİ) gibi şiddet içeren veya yüksek ölçüde stresli içeriklere sıklıkla maruz kalan departmanlarda yaygın bir uygulamadır.

> *Fin gazetesi Turun Sanomat, bir dizi çevrimiçi tehdidin ardından sokakta doğrudan tehditlere dönüşen saldırılara maruz kalmasından sonra kadın gazetecilerinden birinin yerini değiştirerek (yaklaşık 250.000 kişinin yaşadığı) Turku şehrinden çok daha büyük bir şehir olan başkent Helsinki'ye almıştır. Büyük bir şehirde, gazetecinin tanınması olasılığı çok daha azdır.*

## e Kurumsal destek açıklaması

Haber kuruluşu açısından, saldırıya uğrayan bir gazeteci için resmi bir destek açıklamasında bulunmak, kuruluşun personelinin arkasında olduğu ve gazetecilerine yapılan saldırıları bir bütün olarak kuruluşa yapılmış saldırılar olarak gördüğü mesajını gönderir. Bununla birlikte, olaya bağlı olarak, dikkati gazeteciye çekmekten ve dolayısıyla daha şiddetli saldırıları teşvik etme olasılığından kaçınmak için düşük bir profil oluşturmak daha iyi olabilir. Bir destek açıklaması yayınlayıp yayınlamamayı değerlendirirken aşağıdaki kriterler göz önüne alınmalıdır:

- Saldırıyı güçlendirecek mi?
- Daha fazla tacize yol açacak mı?
- Haber kuruluşunun açmayı düşündüğü hukuk davalarına zarar verecek mi?

## f Çevrimiçi suistimalin moderasyonu

*Diğer kabul edilemez yorumların yanı sıra gazetecileri ve haber kuruluşlarını hedef alan saldırıların hızla kaldırılmasını sağlamak amacıyla, kullanıcı yorumlarının moderasyonuna yönelik kapsamlı ve iyi geliştirilmiş bir strateji gereklidir.*

### Çevrimiçi suistimalin önlenmesi

- Hem kullanıcılar hem de moderatörler için temel kurallar görevi görecek Topluluk İlkeleri veya İnternet Etiği politikaları geliştirin. Bu katılım ilkeleri, eleştirilerin hoş karşılandığını ancak hakaret, saldırı, nefret ve tehditlerin hoş görülmeyeceğini açıkça belirtmelidir.

> *Guardian'ın topluluk ilkelerini ve katılım ilkelerini okuyun.*
> *Deutsche Welle'nin internet etiği politikasını okuyun.*

- Bir topluluk oluşturun: Çevrimiçi topluluklar oluşturmak ve sürdürmek biraz zaman alabilir, ancak çevrimiçi tacize karşı koymak söz konusu olduğunda bu topluluklar çok önemlidir. Kendisini bir topluluğun parçası olarak hisseden okuyucuların, medya platformlarında ve haber organlarının yorumlar kısımlarında karalandığı veya tehdit edildiğinde medya kuruluşunu veya hedef alınan gazeteciyi savunması daha olasıdır.

- Medya organınız için bir kayıt şeması oluşturun: Kullanıcılardan yorum yapabilmeleri için kayıt olmalarını istemek iyi bir uygulamadır. Bu gereklilik, sadece potansiyel yasal yükümlülükler açısından değil, aynı zamanda saldırganları ve robot hesapları caydırmaya yönelik ön bir engel olarak da önem taşımaktadır.

- Seçilmiş içeriklerde yorumlara izin verin: Yorumların moderasyonu için kullanılabilecek kaynaklar sınırlıysa, içeriğinizin sadece bir kısmının yorumlara açılması iyi bir stratejidir. Bunu yaparken, topluluğunuzun farklı alanlardaki görüşlerini belirtme olanağına sahip olabilmesi için bir dizi farklı konu seçin.

- Belirli zamanlarda yorumları engelleyin: Gece boyunca, hafta sonları veya moderatörlerin bu iş için yeterli zaman ayıramayacağı başka zamanlarda tartışmaların moderasyonunu yapamayacağınızı düşünürseniz, ilgili süre boyunca yorum yapılmasını engellemeyi göz önüne alın. Bunu yaparsanız, kullanıcılara tekrar ne zaman yorum yapabilecekleri konusunda bilgi verildiğinden emin olun.

- Yorum yapılabilecek süreyi sınırlayın: Kullanıcılara görüşlerini paylaşma olanağı vermek ama ekibinizin üzerindeki yükü sınırlamak için başka bir strateji, yorumlara haber yayınlandıktan sonra sınırlı bir süre boyunca izin vermektir.

- Kullanıcıların faaliyetlerini izlemek için alarmlar oluşturun: Bazen, bir süredir yorum yapılmayan konuşmalar aniden tekrar aktif hale gelir. Yorumları kapatmak istemiyorsanız, moderatörlerin dikkatini bu değişikliğe çeken bir bildirim sistemi kullanın.

### Çevrimiçi suistimalin moderasyonu ve bunlara tepki gösterilmesi

Gazetecileri hedef alan saldırıları, tehditleri ve hakaretleri kaldırmanın, saldırgandan kaynaklanan fiziksel şiddet riskini ortadan kaldırmadığını unutmayın. Moderatörler bir gazeteciyi hedef alan, özellikle de bir tehdit içeren saldırgan mesajlar gördüklerinde, sadece bu mesajları kaldırmakla kalmayıp bunları söz konusu saldırıların hedefinde

olan kişi de dahil olmak üzere haber kuruluşundaki ilgili kişilerin dikkatine sunmalıdır.

Sitedeki yorumlar:

- Yorumların kaldırılması: Bir gazeteciye karşı bir tehdit, hakaret veya başka bir saldırı içeren yorumların, söz konusu yorumun meşru eleştiri sınırları içinde mi olduğunu yoksa Topluluk İlkelerini ihlal ettiğini ve bu nedenle kaldırılmasının mı gerekli olduğunu belirlemesi gereken moderatörler tarafından dikkatle analiz edilmesi gereklidir. Bir gazeteciye yönelik bir saldırı içeren yorumların kaldırılması ile ilgili kararlar, sadece saldırının içeriğini değil, aynı zamanda gazetecinin savunmasızlığını da dikkate almalıdır. Kullanıcıların, yorumlarının neden kaldırıldığı ve yorumun Topluluk İlkelerinizin hangi maddesini ihlal ettiği konusunda bilgilendirilmeleri iyi bir uygulamadır.

- Kullanıcıların uyarılması ve engellenmesi:

  - Topluluk İlkelerini tekrar tekrar ihlal eden kullanıcıları uyarın: Topluluk İlkelerini tekrar tekrar ihlal eden kullanıcıları uyarmanın iyi bir yolu, yorum paylaşmalarını belirli bir süreyle engellemektir. Bu adımı attığınızda, kullanıcının sizden bu kararın neden verildiği konusunda bir mesaj aldığından emin olun.

  - Hesapları silindiği zaman kullanıcılara bilgi verin: Bir kullanıcının yorumlara erişiminin tamamen silinmesi ciddi bir adımdır ve ciddi saldırganlıklara karşı verilebilecek uygun bir yanıttır. Hesapları silinen kullanıcılara, bu kararın neden verildiğine ilişkin bir mesaj gönderilmelidir.

- Moderatörlerin kullanıcı sohbetlerine katılımı: Moderatörler, medya organının hesabı altında hareket etmeli ve Topluluk İlkeleri kapsamındaki kuralları kullanıcılara hatırlatmalıdır. Gazetecilerin sohbetlere katılımı sohbetin kalitesini artırabilir, ancak bu katılım zorunlu olmamalıdır ve riskler dikkatle değerlendirilmelidir.

Sosyal medya platformlarında:

Medya kuruluşları, sosyal medya platformlarını daha büyük bir izleyici kitlesine ulaşmak, belirli konularda toplumsal tartışma oluşturmak ve nihai olarak bir topluluk yaratmak için kullanmaktadır. Medya organları, resmi sosyal medya kanallarında kendi tartışma forumlarındaki standartlar ile aynı topluluk standartlarını uygulama eğilimindedir; bu forumlarda moderasyon ekipleri kendi okuyucu kitleleri ile ilişkiler kurarak kullanıcılar ile ve kullanıcılar arasında sağlıklı toplumsal tartışmalar için bir ekosistem oluşturmaktadır.

Facebook'ta çevrimiçi suistimalin yönetilmesi:

- Saldırgan veya tehdit edici içeriğe sahip veya küçük düşürücü sözler ve hakaretler içeren yorumları silin. Ancak ne kadar sert olursa olsun, eleştirilere izin verilmelidir.

- Küfür içeren yorumları gizleyin. Moderatörler genellikle bunun silme önleminden daha az etkili olduğunu düşünür, çünkü diğer kişiler göremese de kullanıcı ve kullanıcının arkadaşları hala söz konusu içeriği görebilir.

- Bir kullanıcı, uyarıldıktan sonra bile tekrar tekrar nefret içeren veya küfürlü yorumlar paylaştığında, bu kullanıcının medya organının Facebook sayfasına girişini yasaklayın. Bu işlem, açık tartışmaların değerlerine sürekli olarak zarar verdiği görülen kullanıcıları engellemek için yapılır.

- Diğer küfürlü yorumları engellemeye yönelik bir uyarı olarak bir kullanıcıyı sayfadan çıkarın. Bu işlemin sonuçları, kullanıcı sayfayı tekrar beğenebileceği veya izleyebileceği için yasaklama işleminden daha hafiftir.

- Yorumları devre dışı bırakın/kapatın, ancak bu özellik sadece video paylaşımları için kullanılabilir. Bu işlem, moderasyon ekibi bir video veya canlı yayındaki yorum akışının moderasyonu için yeterli kaynağa sahip olmadığında yapılır.

- Bazı sözcükleri engelleyin ve küfür filtresinin gücünü ayarlayın.

- Hem Facebook'un hem de medya organının kendi topluluk ilkelerini ihlal eden bir paylaşımı veya Facebook Sayfasını rapor edin.

Twitter'da çevrimiçi suistimalin yönetilmesi:

- Susturma: Hem medya organının hem de Twitter'ın topluluk ilkelerini ihlal eden çevrimiçi suistimaller söz konusu olduğunda, moderatörler hesapları engelleme yerine susturma eğilimi göstermektedir. Bu seçenek suistimalin doğrudan etkisini hafifletmekle kalmaz, aynı zamanda susturulan kullanıcı susturma hakkında bilgi sahibi olmadığından

olası bir öfke tepkisini de engeller. Son olarak, susturma işlemi moderatörlerin susturulan hesaplar tarafından üretilen içeriği hala görebilmelerini, böylece olası muteber tehditler konusunda tetikte kalmalarını sağlar.

- Engelleme: Moderatörler sürekli olarak istenmeyen e-posta veya dolandırıcılık mesajı gönderen hesapları engelleme eğilimi gösterir; diğer durumlarda ise moderatörler bu önlemi, engellendiğinde kullanıcıya bildirim gitmesinden dolayı doğabilecek tepkileri önlemek amacıyla genellikle son çare olarak kullanır. Ayrıca, moderatör engellenen hesaba erişemeyeceğinden, bu durum moderatörün olası tehditleri izlemesini zorlaştırır.

- Rapor etme: Moderatörler, muteber ve olası tehditler yayan veya şiddet görüntüleri içeren tweet veya hesapları genellikle Twitter'a rapor eder.

- Yanıtları gizleme: Moderatörler, tweet'lerine verilen yanıtları gizleme seçeneğine sahiptir. Tüm kullanıcılar, gizlenmiş yanıtları orijinal tweet'te gösterilen gizlenmiş yanıt simgesi yoluyla hala görebilir. Ancak Twitter, trolleme amaçlı veya hakaret içeren yorumların etkisini en aza indirerek sohbete hakim olmalarını önlemek amacıyla bu seçeneği geliştirmiştir. Moderatör bir yanıtı gizlediğinde, yanıtın yazarına bir bildirim gönderilmez.

# Adım 4: İzleme ve Yeniden Değerlendirme

*Haber merkezleri, rapor edilen çevrimiçi taciz olaylarını izlemeli ve gazetecileri çevrimiçi tacizden korumaya yönelik güvenlik ve destek mekanizmalarını tekrar değerlendirmelidir.*

Haber kuruluşları, çevrimiçi taciz vakalarını ve bunlara verilen karşılıkları takip etmek için bir veri tabanı oluşturmalıdır. Bu veri tabanının her taciz olayını içermesi gerekli değildir, ancak en azından personel üyeleri tarafından resmi raporlama mekanizmaları yoluyla rapor edilen veya bir risk değerlendirmesi sonucunda destek önlemlerinin uygulanmasının gerektiği olayları kapsamalıdır.

Bu veri tabanının birincil amacı, rapor edilen çevrimiçi taciz olaylarını araştırmak ve yeni veya farklı önlemlerin gerekli olup olmadığı dahil olmak üzere, uygulanan destek önlemlerinin düzenli olarak (yeniden) değerlendirmesine olanak sağlamaktır.

Haber merkezleri, destek önlemlerinin değerlendirilmesine ek olarak, tacize yönelik genel yanıt mekanizmalarının yapılarının etkinliğini de düzenli bir şekilde yeniden değerlendirmelidir. Bu değerlendirme, personel üyelerinin ve kuruma katkıda bulunanların ne ölçüde bu konunun ciddiye alındığını görebileceği nitel anketlerin yanı sıra, herhangi bir formda karşılık verilen vakaların sayısına ilişkin nicel incelemeleri de içermelidir.

# Roller ve Görevler

*Burada, dikkate alınması gereken rollerin ve görevlerin bir açıklaması verilmiştir. Küçük ölçekli haber merkezlerinde, bu rollerin bazıları tek bir kişi tarafından üstlenilebilir.*

### Çevrimiçi Güvenlik Koordinatörü

Bu profil, personel üyeleri arasında açık bir biçimde dağıtılabilecek veya belirli tek bir kişiye verilebilecek bir dizi görevi kapsamaktadır:

- Gazetecilerin çevrimiçi taciz olaylarını rapor edebileceği kişi olarak görev yapmak.
- Hedef alınan gazeteciler, yazı işleri müdürü ve okuyucu temsilcisi ile koordinasyon içinde her bir çevrimiçi taciz olayını değerlendirmek ve hedef alınan gazetecinin ihtiyaç duyduğu destek mekanizmalarını önermek.
- Gereken durumlarda, yönetim ve hukuk uzmanları ile birlikte, medya organı tarafından verilecek kurumsal karşılığı koordine etmek.
- Uygulanan önlemlerin etkililiğini izlemek ve değerlendirmek amacıyla, çevrimiçi suistimal olaylarını içeren veri tabanını tutmak.
- Çevrimiçi saldırıların değişen niteliği nedeniyle, haber merkezinin çevrimiçi tacizi önlemek ve bunlara karşılık vermek için uyguladığı önlemleri düzenli olarak gözden geçirmek.
- Bu önlemler için bir koordinasyon ve eğitim noktası olarak görev yapmak. Çevrimiçi Güvenlik Koordinatörü tüm haber merkezi önlemleri hakkında kapsamlı bilgi sahibi olmalı, bunları çevrimiçi suistimale uğrayan gazetecilere açıklayabilmeli ve bunların uygulanması için öncü kişi olmalıdır.
- Çevrimiçi suistimale yol açabilecek yeni içerikler hakkında bilgi sahibi olmak için yazı işleri toplantılarına düzenli olarak katılmak.

### Yönetim

- Çevrimiçi tacizin ciddi bir endişe konusu olduğunu ve personel üyelerinden birine yapılan bir saldırının medya kuruluşunun tamamına yapılmış olduğunu kabul etmek. Bu duruşu haber merkezine ve çalışanlarına düzenli olarak bildirmek.
- Haber merkezinde, çevrimiçi suistimali rapor etmenin damgalanmaya yol açmadığı, yardımcı bir ortam oluşturmaya yönelik yapısal değişiklikleri benimsemek. Bu yeni yapıları sürdürmek ve güncellemek için zaman ve finansman açılarından yeterli kaynağın ayrılmasını sağlamak.

Yukarıda belirtilen şekilde bir veya birkaç Çevrimiçi Güvenlik Koordinatörü görevlendirmek.

- Çevrimiçi saldırılara hedef olan kişileri, kendilerini etkileyen karar verme süreçlerine dahil etmek.

### Yazı işleri müdürleri

- Çevrimiçi tacizin modern gazeteciliğin bir özelliği değil, ciddi ve kabul edilemez bir sorun olduğunu kabul etmek.
- Çevrimiçi taciz konusunu sürekli olarak yazı işleri toplantılarının gündemine dahil etmek. Konu hakkında açıkça konuşulması, gazetecilerin saldırıları rapor etme konusunda kendilerini daha rahat hissedecekleri bir atmosfer yaratacaktır.

### Moderatörler

- Sosyal medya platformlarında ve yorumlar kısmında personel üyelerini hedef alan bireysel tehditleri ve düzenlenmiş kampanyaları tanımlamak, bunları bir veri tabanına kaydetmek ve gazeteciye, yazı işleri müdürüne ve çevrimiçi güvenlik uzmanına iletmek.
- Çevrimiçi suistimalin tehdit seviyesinin değerlendirilmesine katkıda bulunmak.
- Hedef alınan gazetecinin sosyal medya hesaplarını devralarak söz konusu gazetecinin şiddet içeriklerine maruz kalmasını azaltmak ve potansiyel travmaları en aza indirgemek.

### Gazeteciler

- Çevrimiçi tacizin günümüz gazeteciliğinin bir özelliği değil, ciddi ve kabul edilemez bir sorun olduğunu anlamak.
- Farkındalık, dijital emniyet ve travma risk yönetimi eğitimleri dahil, medya organı tarafından sunulan ilgili tüm eğitim olanaklarına katılmak.
- Hem resmi hem de gayri resmi akran desteği yapılarına katılmak.
- Suistimalin herhangi olumsuz bir sonuca yol açmayacağı düşünülse bile, çevrimiçi suistimal olaylarını meydana geldiklerinde rapor etmek. Bu olayların rapor edilmesi, haber merkezinin sorunun kapsamını anlamasına ve karşılık vermek için gerekli önlemleri geliştirmesine yardımcı olur.

# IPI hakkında

1950 yılında kurulan Uluslararası Basın Enstitüsü (IPI), nitelikli ve bağımsız gazeteciliğe yönelik ortak bir bağlılığı paylaşan yazı işleri müdürleri, gazeteciler ve medya yöneticilerinden oluşan küresel bir ağdır. Birlikte, gazeteciliğin kamusal işlevini yerine getirmesine olanak sağlayan ve en önemlisi medyanın müdahaleler ve misilleme korkusu olmadan özgürce çalışma yetisi olan koşulları sağlamak için çalışıyoruz. Misyonumuz, tehdit altında olduğu yerlerde medya özgürlüğünü ve haberlerin serbest akışını savunmaktır.

# IPI'ın Newsrooms Ontheline programı hakkında

IPI'ın Newsrooms Ontheline programının hedefi, medya organlarına ve gazetecilere yöneltilen çevrimiçi taciz ve suistimalleri önlemeye, ele almaya ve karşılık vermeye yönelik kaynakları ve en iyi uygulamaları derlemek ve paylaşmaktır. Bu araçları haber merkezlerine sağlayarak, sadece çevrimiçi suistimalin gazeteciler üzerindeki olumsuz kişisel ve mesleki etkilerine karşı çıkmayı değil, aynı zamanda çevrimiçi saldırılardan kaynaklanan ve halkın haberlere erişimini tehdit eden oto-sansürün önlenmesine de yardımcı olmayı amaçlamaktadır.

Bu Protokolün hazırlanması, Adessium Vakfı ile Demokrasi ve Medya Vakfının maddi desteği ile mümkün olmuştur.



# Haber merkezlerinin çevrimiçi tacize hedef olan gazetecileri desteklemesi için protokol

Yayımlayan
Uluslararası Basın Enstitüsü (IPI)
Şubat 2020

International Press Institute
I·P·I

## Uluslararası Basın Enstitüsü

Telefon: + 43 1 512 90 11

E-posta: info@ipi.media

Web: ipi.media