

# İnsan Hakları **Veri Tabanları** **Bilgi Notu**



ETKİNİZ  
AB PROGRAMI

## İÇİNDEKİLER

|                                                             |           |
|-------------------------------------------------------------|-----------|
| <b><u>1. Veri Tabanı Nedir?</u></b>                         | <b>2</b>  |
| <b><u>2. Veri Tabanlarının Ana Öğeleri</u></b>              | <b>3</b>  |
| <b><u>3. İnsan Hakları İzlemenin Temel İlkeleri</u></b>     | <b>5</b>  |
| <b><u>4. Veri Tabanını Nasıl Oluşturacağız?</u></b>         | <b>7</b>  |
| <b><u>5. Dijital/Siber Güvenlikle İlgili Endişeler</u></b>  | <b>8</b>  |
| <b><u>6. İnsan Hakları İzleme Veri Tabanı Örnekleri</u></b> | <b>10</b> |
| <b><u>EK: Referanslar ve Yararlı Kaynaklar</u></b>          | <b>12</b> |



Bu yayın Avrupa Birliğinin maddi desteği ile hazırlanmıştır. İçerik tamamıyla WEglobal S.r.l liderliğindeki konsorsiyumun sorumluluğu altındadır ve Avrupa Birliğinin görüşlerini yansıtmak zorunda değildir. Etkiniz Uluslararası uzmanı Veronica Yates tarafından hazırlanan bu içeriği, Etkiniz Teknik Destek Ekibi Türkçeleştirmiş ve uyumlulaştırmıştır.

## 1. Veri Tabanı Nedir?

Veri tabanları, bilgilerin kolay erişim, yönetim ve güncellenmesi için oluşturulmuş sistemlerdir. Genellikle, verilerin veya bilgi dosyalarının depolandığı yerlerdir. Bir veri tabanı oluşturmanın amacı, verileri organize ve analiz edilebilecek şekilde tek bir yerde muhafaza etmektir.

### İnsan Hakları İçin Veri Tabanları

Halihazırda, insan hakları hakkında bilgi toplayan birçok veri tabanı vardır. Bunların çoğu iki kategoriye ayrılabilir:

- Bir insan hakları konusuyla ilgili mevcut bilgilerin koleksiyonu olanlar; örneğin uluslararası antlaşmalar, BM kararları, mahkeme davaları, vb.
- İnsan hakları profesyonelleri tarafından, belirli insan hakları ihlallerine ilişkin olarak, genellikle savunuculuk için izleme amacıyla toplanan bilgileri bir araya getirenler. Bu bilgi notunun odaklandığı veri tabanları bu türdendir.

#### *“Neden bir insan hakları veri tabanı geliştirelim ki?”*

Veri tabanları, insan hakları ihlallerine ilişkin kanıtları toplamaya yardımcı olan bir araçtır. Bu kanıtlar daha sonra insan hakları koşullarını iyileştirecek değişiklikler yapmak için kullanılabilir. Bu, aşağıdakiler gibi bir dizi faaliyetle gerçekleştirilebilir:

- **BM gibi uluslararası mekanizmalara raporlama:** Kanıtlar toplandıktan sonra analiz edilebilir ve BM mekanizmalarına/uzmanlarına sunulabilir. Bunu yaparken, raporunuzu nasıl yazacağınız ve sunacağınızla ilgili yönergeleri takip etmek çok önemlidir; kelime sınırları, takip edilmesi gereken belirli formatlar, doldurulması gereken formlar söz konusu olabilir. Bu mekanizmaların farklı paydaşlardan çok fazla bilgi alabileceğini unutmayın, bu nedenle raporlarınız mümkün olduğunca kısa ve öz olmalıdır. (Araçlar ve tavsiyeler için kaynak listesine bakınız).
- **Ulusal düzeyde politika ve savunuculuk değişikliği için kampanya yürütmek:** Veri tabanınızdaki bilgilerin farklı kullanıcıları olabileceğini unutmayın. Bu nedenle, özellikle web siteniz halka ya da başka paydaşların kullanımına açıksa, veri tabanınızdaki bilgiler açık, öz ve basit bir dille yazılmış ve doğru olmalıdır (İlerleyen bölümlerde ayrıntılı şekilde ele alınacak).
- İnsan hakları kurumlarına yapılan **şikayetlerin izlenmesi** ve uygulamadaki ilerlemenin **takip edilmesi**;
- Ulusal, bölgesel veya uluslararası düzeyde stratejik **davalar** da dahil olmak üzere **mahkemelerdeki davalara ilişkin bilgileri yönetmek**;
- Tarihi gerçekleri **muhafaza etmek**, arşivleme, hafıza ve hikâye anlatımı gibi yollarla gelecekte hesap verebilirliği mümkün kılmak (örneğin devam eden bir insan hakları ihlali durumunda).

### *“İnsan hakları veri tabanları kimin için hazırlanır?”*

Veri tabanını kimlerin kullanacağını (veya kullanabileceğini) akılda tutmak önemlidir. İlk adım bilgileri tek bir yerde depolamak olsa da yukarıda belirtildiği gibi birçok kişi veri tabanını bir dizi faaliyet için kullanabilir. Kullanıcılar arasında şu profiller olabilir:

- İnsan hakları araştırmacıları
- Kampanyacılar ve aktivistler
- Avukatlar
- Politika yapıcılar
- Akademisyenler
- Gazeteciler
- BM personeli ve uzmanları
- Devlet görevlileri, kamu idaresi personeli

## 2. Veri Tabanlarının Ana Öğeleri

Veri tabanı, yalnızca toplanan bilgileri saklamakla kalmamalı, aynı zamanda bu verilerle ilgili soruları yanıtlayabilme kapasitesine de sahip olmalıdır. İhlal vakalarındaki gelişmeleri izlemek amacıyla düzenli olarak güncellenmesi gerekmektedir.

Veri tabanında yer alacak bilgileri nasıl kategorize edeceğinizi düşünmeniz önemlidir; bu, veri tabanının kullanıcılarının kim/kimler olacağı göz önünde bulundurularak yapılmalıdır.

İnsan hakları ihlalleri vakalarını izlemeye odaklandığımızda, temel bilgileri aldığımızdan emin olmamızı sağlamak için sorulacak standart sorularla ilgili; BM, HURIDOCS vb. gibi insan hakları aktörlerinin üzerinde uzlaştığı yöntemler ve prosedürler mevcuttur. Bu unsurlar şunlardır:

- Ne oldu, nerede ve ne zaman oldu;
- Hangi anlaşma veya sözleşme kapsamında, hangi spesifik hakların ihlal edildiği de dahil olmak üzere, gerçekleşen olası insan hakları ihlalleri nelerdir;
- İlgili kişiler: Fail olduğu iddia edilen kişi, hangi hak ihlaline uğrayan kişiye yönelik olarak bu davranışta bulundu ve ne yaptı, bu bilginin kaynakları nelerdir? Bu hak ihlali ile ilgili olarak hangi müdahaleler yapıldı?

## Bilgi Kaynakları

Toplayacağınız bilgiler, çoğu zaman **birincil belgelere** ve **ikincil belgelerden** elde edilir.

**Birincil belgeler**, örneğin ihlale maruz kalan hak sahipleri, tanıklar ve failler gibi kişilerden bilgi toplama faaliyetlerinden elde edilebilir. Kişiler söz konusu olduğunda, bilgi henüz yazıya dökülmemiş ve zihinlerinde yer etmiş olabilir, bu nedenle anket ve mülakat gibi bilgi toplama faaliyetleri yürütülür. İnsan hakları ihlallerini içeren vakalarda, kişilerden bilgi toplanırken, bilgiyi sağlayan kaynağın, araştırılan olay hakkında doğrudan bilgi sahibi olup olmadığının ortaya çıkarılması gerekir.

Diğer birincil belgeler, orijinal kaynaktan toplanan belgesel kaynakları içerir. Bu belgelerin çoğu, bir bilgi toplama faaliyeti sırasında veya hemen sonrasında üretilir. Bazıları araştırma veya soruşturma sırasında keşfedilen belgeler olabilir. Bunlar yeminli ifadeler, gerçek konuşmaların transkriptleri, mektuplar, elle çizilmiş haritalar, el yazmaları veya diğer gerçek orijinal belgeler olabilir.

Birincil belgeler genellikle yasal olarak bu bilgiyi tutmakla ilgili görevleri olan kuruluşlarda, uzmanlaşmış araştırma merkezlerinde, arşivler, müzeler veya insan hakları örgütlerinde bulunabilir. **Birincil belgeler bilginin temelidir.** Bu belgeler genellikle çok değerlidir ve korunmalarına özen gösterilmelidir. Bazı birincil belgeler hukuki süreçlerde kanıt olarak kaydedilebilir, bu nedenle bu belgeler izleme yapan örgütlerce değil, mahkemelerce muhafaza edilir. İzleme yapan örgütler, bu durumlarda ilgili belgelerin kopyalarını veya özetlerini alınmalıdır.

**İkincil belgeler**, birincil belgelere dayalı olarak üretilen belgeleri ifade eder.

Bir gazetecinin bir gazetede yayınlanan anlatısı veya bir araştırmacının araştırma sonucu ortaya çıkan çalışması, çoğu zaman ikincil bir belgedir. Kitaplar ve makaleler ikincil belgelerin en yaygın örnekleridir. Genellikle birincil belgeleri okuyucuların anlayabileceği bir forma çevirirler, bir argüman sunarlar veya bir şeyi belirli bir bakış açısıyla tanımlarlar.

## Önemli Noktalar

Çalışmanız ulusal veya uluslararası düzeyde yasal ve politika değişikliği de dahil olmak üzere hesap verebilirlik ve adalet arayışı amacını gözetiyorsa, birincil bilgi kaynaklarından kanıt sağlamanız gerekecektir. İkincil bilgiler genellikle doğrulanmış bilgiler olarak değil, takip edilmesi gereken ipuçları olarak değerlendirilir.

Olası bilgi kaynakları şunlar olabilir:

- İhlale maruz kalan hak sahipleri, tanıklar ve failler gibi olayda rol oynayan kişiler;
- Askeri yetkililer veya cezaevi görevlileri gibi hükümet yetkilileri,
- Öğretmenler, doktorlar, hak ihlaline uğrayan kişinin yakınları gibi arka plan bilgisi sağlayabilecek diğer kişiler;
- Olayların gerçekleştiği yerler;
- İstatistik kurumları gibi devlet daireleri;

f) Morglarda, hastanelerde, cezaevlerinde ve diğer tesislerde tutulan kayıtlar, örneğin ölüm belgeleri, tapu belgeleri, sağlık raporları, yasal özetler ve önergeler, mahkeme kararlar, basın raporları, vb.

İlgili belgeler kamu idaresi yetkililerinin elinde olabilir ve bu yetkililer her zaman bunları sağlamaya istekli olmayabilir. İnsan hakları örgütleri için ilgili kurum ve kişilerle ilişkilerin kurulmuş olması bu nedenle önemlidir. İnsan hakları örgütleri, mevzuat hakkında da bilgi sahibi olmalıdırlar; özellikle kamu idaresindeki bilgilere erişim için bilgi edinme hakkı talepleri ve benzeri girişimlerin hayata geçirilmesi gerektiğinde yetkililere şikâyetle bulunulabilmesi böylelikle olanaklı kılınmış olur.

### 3. İnsan Hakları İzlemenin Temel İlkeleri

Birleşmiş Milletler gibi uygulayıcılar tarafından geliştirilen temel izleme ilkelerini takip etmek önemlidir. Örneğin, izleme çalışmanız **'zarar vermeme'** ilkesini gözetmelidir; bu çalışmalarınızdan etkilenen kişi ve grupların üzerinde eylemlerinizin olası olumsuz sonuçlarını önlemek ve hafifletmek için önlemler aldığınız anlamına gelir.

Hangi insan hakları ihlallerine odaklandığınıza bağlı olarak daha fazla ilke gözetmek sizin için uygun olabilir. Hassas konular üzerinde çalışıyorsanız veya savunmasız gruplarla çalışıyorsanız, temas ettiğiniz kişilerin her aşamada saygı görmesini ve güvende olmasını sağlamak için ekstra adımlar atmanız gerekir. Örneğin, çocuklarla çalışıyorsanız, uluslararası kabul görmüş çocuk koruma önlemlerine uygun hareket ettiğinizden emin olmalısınız.

Temel ilkeler şunları içerir:

#### **Doğruluk ve hassasiyeti sağlayın**

İnsan hakları ihlallerini izlemenin amaçlarından biri, bu bilgilerin savunuculukta kullanılabilmesi için kesin bilgi ve analiz sağlamaktır. Bu nedenle ihlallerin iyi belgelenmiş bilgilerle desteklenmesi çok önemlidir.

#### **Doğrulama ve kanıt standardını koruyun**

Raporlarınız doğrulanmış bilgilere, yani ilk kanıtları teyit eden bilgilere dayanarak yazılmalıdır. Farklı rapor türleri farklı seviyelerde doğrulama gerektirse de asla söylentilere veya doğrulanmamış bilgilere dayanmamalıdır. Bilgileri doğrulamak için çok çeşitli kaynaklar kullanmalısınız. Medya raporları bilgileri doğrulamak için yeterli olmayabilir. Medya raporlarını kullanırsanız, en azından gazetecinin raporlarını doğrulanmış bilgilere (en az iki kaynak) dayanarak yazdığından emin olmalısınız. Emin değilseniz onlarla iletişime geçmek isteyebilirsiniz. Toplanan bilgiler tematik bir rapor için kullanılacaksa, örneğin bir grup insanı etkileyen bir soruna dikkat çekmek için hazırlanan raporlar gibi, istenen kanıt standardı, örneğin bir cezai kovuşturmanın özel veya acil bir durumu kadar zorlu olmayacaktır. Bu durumda, ilgili kişiler muhtemelen kendi soruşturmalarını kendileri yürüteceklerdir.

Hazırladığınız raporun bütünlüğünü savunmak, kullanılan kaynakların güvenilirliğini ve raporun içerdiği bilgilerin geçerliliğini ortaya koymak, bilgi toplamak ve doğrulamak için kullanılan metodolojiyi de açıklamalısınız. Belirli gerçekleri doğrulayamıyorsanız (örneğin, tam olarak tespit edilemeyen bir olay) veya bir kaynağın güvenilirliğini teyit edemiyorsanız (örneğin, İnternet üzerinden erişilen video görüntüleri), bu durum veri tabanında açıkça belirtilmeli ve bu bilgileri doğrulanmış verilerden ayırmalısınız.

### **Gizliliğe saygı gösterin**

Bilgilerin gizliliğine saygı gösterilmesi esastır çünkü bu ilkenin ihlal edilmesi çok ciddi sonuçlar doğurabilir:

- Görüşülen kişiler, hak ihlaline uğrayan kişiler, tanıklar ve ilgili diğer herkes için;
- Kendi güvenilirliğiniz ve güvenliğiniz için;
- Yerel halk arasında duyulan güven için;
- Ve böylece çalışmanın etkinliği için;

İşbirliği yaptığınız kişilere, kimliklerinin ve uygun olduğu hallerde sağlanan bilgilerin, bu bilgilerin kullanımı için özel bir onay verilmediği sürece (aşağıya bakınız) gizli tutulacağı konusunda güvence vermelisiniz. Bilgilerin kullanımı için onay verilmiş olsa bile, bu eylemin bilgi veren kişinin ve duruma dahil olan diğer kişilerin (örneğin, tanıkların ailesi) güvenliği açısından olası sonuçlarını değerlendirmekle yükümlüsünüz. Bu kişilerden herhangi birini tehlikeye atma riski varsa, bilgiyi ifşa etmemeli veya riski ortadan kaldıracak şekilde yapmalısınız. İhlale maruz kalan hak sahiplerinin, tanıkların ve işbirliği yapılan diğer kişilerin güvenliği her şeyden önemli olmalıdır.

İhlale maruz kalan hak sahiplerinin ve tanıkların kimlikleri de dahil olmak üzere kaydedilen bilgilerin gizliliğini korumak için özel önlemler de alınmalıdır. Bu hem bilgilerin güvenli bir şekilde kaydedilmesi hem de güvenli bir şekilde saklanması ve işlenmesiyle ilgilidir (Daha sonra dijital güvenlik konusuna bakınız).

### **Bilgilendirilmiş rıza alınmasını sağlayın**

İhlale maruz kalan hak sahipleriyle veya hak ihlaline uğrayan kişilerin yakınlarıyla, tanıklarla ve diğer kişilerle görüşmeler yapıyorsanız, sağlanan bilgileri kullanmak ve/veya paylaşmak için görüşülen kişilerin bilgilendirilmiş rızasını almalısınız. Bu, gizlilik ilkesini, bilginin kullanım amacını ve bilginin nasıl korunacağını açıklamak anlamına gelir. Örneğin, görüşülen kişinin kimliği ve kişisel bilgileri gibi hangi bilgilerin tamamen gizli tutulacağını, hangi bilgilerin ister kurum içi ister kamuya açık olsun bir rapora dahil edilebileceğini veya başkalarıyla paylaşılabilirliğini ve bunu kimlerle paylaşabileceğinizi açıklamalısınız. Görüşülen kişileri, bilgilerin kullanımının güvenlikleri ve refahları üzerindeki olası etkileri konusunda tam olarak bilgilendirmekle yükümlüsünüz.

Bilgilerin üçüncü bir tarafa ifşa edilmesi için bilgilendirilmiş onay verilmiş olsa bile, bu eylemin bilgi veren kişinin ve duruma dahil olan kişilerin güvenliği açısından olası sonuçlarını değerlendirme yükümlülüğünüz bulunmaktadır (bkz. Görüşme ve İhlale maruz kalan hak sahiplerinin korunması bölümleri).

### Güvenlik standartlarını dikkate alın

Bilgi sağlayan kişilerin güvenliğini her zaman göz önünde bulundurmalı ve izleme çalışmalarınızda zarar vermeme, gizlilik ve bilgilendirilmiş rıza ilkelerine saygı göstermelisiniz. İşbirliği yapan kişilerin güvenliği konusunda gerçekçi olmayan garantiler vermemelisiniz. Giderek artan bir şekilde, dikkate alınması gereken dijital güvenlik endişeleri de vardır ve bu konuya daha sonra biraz daha ayrıntılı olarak bakacağız.

### Tutarlılığı takip edin

Bilgiler tutarlı bir şekilde ve çeşitli kaynaklardan toplanmalıdır. Bu, izlediğiniz her vaka veya konu için aynı yöntemleri kullanmanız anlamına gelir. Yukarıda belirtildiği gibi, topladığınız bilgilerin her vaka için dikkatle incelenmesi, karşılaştırılması ve doğrulanması gerekecektir. Kapsamlı ve derinlemesine bir soruşturma tamamlanıncaya, olası tüm bilgi kaynakları araştırılıncaya ve duruma ilişkin net ve tutarlı bir anlayış elde edilinceye kadar araştırmanıza devam etmelisiniz.

Topladığınız bilgilerin nasıl doğrulandığını da detaylandırmanız önemlidir. Böylece raporlarınızdan veya veri tabanınızdan bilgi kullanabilecek herkes tam bir kavrayışa sahip olur. Örneğin, bir olay sadece kısmen doğrulanmışsa, bu belirtilmelidir.

### Hassasiyetle davranın

İhlale maruz kalan hak sahipleriyle, yakınlarıyla ya da hak ihlaline uğrayan kişiler ve tanıklara yakın olan diğer kişilerle görüşürken, bireyin yaşamış olabileceği acılara karşı duyarlı olmalı ve bir dereceye kadar empati göstermelisiniz. Ayrıca, insan hakları konusundaki endişeleri karşısında tarafsız olmadığınızı veya önyargılı olduğunuzu gösterebilecek bir davranış veya kelime/ifade konusunda çok dikkatli olmalısınız.

## 4. Veri Tabanını Nasıl Oluşturacağız?

### Bir veri tabanı yönetim sistemi seçme

Bilgilerinizi nasıl düzenleyeceğinize karar vermeden önce, bir veri tabanı yönetim sistemi- teknik altyapısını seçmeniz gerekir. Yeni bir veri tabanı oluştururken izleyebileceğiniz temelde iki yol vardır: kendi veri tabanınızı oluşturmak veya mevcut bir sistemi kullanmak.

1. Bir excel sayfası gibi en basitinden, arka ve ön arayüzleri olan, daha karmaşık aramaya izin veren bir veri tabanı programı ile kendi veri tabanınızı **oluşturmak söz konusu olabilir**. Bu seçenek, ilk kurulumu yapmak ve ortaya çıkan teknik sorunlarla ilgilenmek için belirli bir miktar teknik uzmanlık gerektirir. Eğer seçtiğiniz seçenek buysa, veri tabanının (internet üzerine) nasıl barındırılacağını (sunucular), bilgilerin nerede tutulacağını ve bu yerin güvenli olup olmadığını göz önünde bulundurmanız gerekir (Bu konuda daha fazla bilgi aşağıda dijital güvenlik bölümünde yer almaktadır).

2.Mevcut bir veri tabanı uygulaması/programı kullanın. Özel uygulamalardan, Açık Kaynak'a (open source) kadar pek çok uygulama arasından seçim yapabilirsiniz. Hangi uygulamayı seçeceğinize ilişkin kararınız, teknik personele erişiminize, bütçeye ve dijital güvenliğe bağlı olabilir. Ayrıca, çeşitli insan hakları grupları kullanabileceğiniz insan hakları izleme veri tabanları geliştirmiştir; bunların çoğunun bir maliyeti vardır ancak keşfetmeye ve bağlantıya geçmeye değerdir. Avantajları, bu tür örgütlerin desteği sayesinde teknik personele ihtiyaç duymamanız ve bu sistemlerin güvenli ve emniyetli olmasıdır.

## Bilgiler nasıl kategorize edilir?

Bir veri tabanı teknik altyapısını seçtikten sonra, topladığınız bilgileri nasıl kategorize edeceğinize karar vermeniz gerekecektir. Bunun için, veri tabanının yanıtlayabilmesi gereken sorulara geri dönmeniz gerekecektir (Bölüm 2'de görüldüğü gibi). Ayrıca bilgilerin anahtar kelimeler, açılır listeler, etiketler vb. kullanılarak girilip girilmeyeceğine de karar vermeniz gerekecektir. Veri tabanı için büyük olasılıkla alanlar en azından şunları içerecektir:

- Konum/coğrafya
- Etkinlik tarihi
- İhlale maruz kalan hak sahipleri
- İhlal türü
- Fail(ler)
- Etkilenen haklar
- Alınan önlemler / takip

**Kamuya açık ve özel bilgiler:** Yaptığınız izlemenin türüne ve amacına bağlı olarak, toplanan bilgilerin bir kısmının kamuya açık olmama anlamında gizli tutulması gerekebilir. Bunun nedeni, devam eden bir soruşturma ile ilgili olabileceği, ilgili kişilerin kendi güvenlikleri için anonim kalmaları gerekebileceği veya özellikle anonimleştirilmeyi talep etmiş olmaları olabilir. Bu, veri tabanını oluştururken yapabileceğiniz bir şeydir. Son bölümde bunu gerçekten iyi yapan bir grup örneğini görebilirsiniz

## 5. Dijital/Siber Güvenlikle İlgili Endişeler

Sizin de çok iyi bildiğiniz gibi, siber-güvenlik dünya çapında giderek artan bir endişe kaynağıdır ve hem kişisel güvenlik hem de kuruluşların sahip olduğu altyapı ve bilgilere yönelik tehditler açısından, insan hakları örgütleri ve aktivistler için on yıllardır bir sorun teşkil etmektedir. Küresel siyasi istikrarsızlığın giderek daha fazla ülkeyi etkilediği, insan hakları savunucularına yönelik baskıların arttığı ve teknolojinin birkaç kişinin eline geçtiği bir ortamda, işe başlamadan önce mümkün olan tüm adımları atmak önemlidir.

Hangi teknolojiyi kullanmayı seçtiğinizden, tutulduğu yerin ne kadar güvenli olduğuna ve kendi güvenliğinize kadar veri tabanı çalışmasıyla ilgili tüm hususları göz önünde bulundurmak isteyeceksiniz. Ancak size yardımcı olabilecek bir dizi mükemmel insan hakları teknoloji kuruluşu bulunmaktadır (Bağlantılar için eke bakınız).

Siber güvenlik açısından bir veri tabanı geliştirmeyi düşündüğünüzde kendinize sormanız gereken birkaç temel soruyu burada bulabilirsiniz:

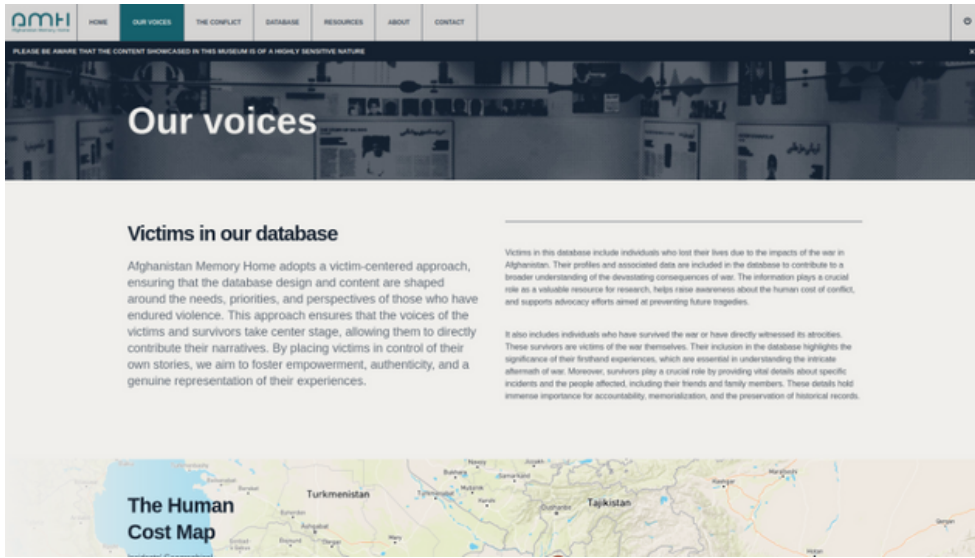
- Örneğin, bir sunucu seçerken, güvenlik etkilerini, verilerin gizliliğini, harici bir tarafın bilgileri ele geçirme olasılığının ne olduğunu, özel bir veri tabanında barındırılıyorsa, verilerin mülkiyetinin sizde olup olmadığını netleştirmeniz gerekir.
- Veri tabanının kendisi güvenli mi? Bu konu, açık kaynaklı teknik altyapılar yerine özel mülkiyete bağlı teknik altyapılar kullandığınızda kritik olabilir: Eğer veri tabanı teknik altyapısı için kullandığınız uygulama özel mülkiyet ise, sahip olan şirketin verilerinize herhangi bir erişimi var mı, verilerle ilgili mülkiyet durumu nedir, verileri kendisi için kopyalayabilir mi?
- Veri tabanınız nerede barındırılıyor? Sunucuların sahibi kim? Hangi ülkelerde bulunuyorlar? Dikkate almamız gereken gizlilik sorunları var mı?
- Erişim: veri tabanının arka arayüzüne (back end) kimin erişimi var, erişimi kim veriyor? Her yerden, telefonlarından ve bilgisayarlarından erişebilirler mi?
- İhlale maruz kalan hak sahiplerinin, tanıkların ve diğer hassas kişilerin gizli bilgilerini nasıl koruyorsunuz?
- Bir kesinti veya saldırı durumunda yedeklenen bir sistem var mı?

**Bu konularda uzmanlaşmış bazı STÖ'lerden tavsiye almanızı şiddetle tavsiye ederiz!**

## 6. İnsan Hakları İzleme Veri Tabanı Örnekleri

### AFGANİSTAN HATIRA EVİ

WEB SİTESİ: <https://afghanistanmemoryhome.org/en/page/cuh5bcdp15u/home>



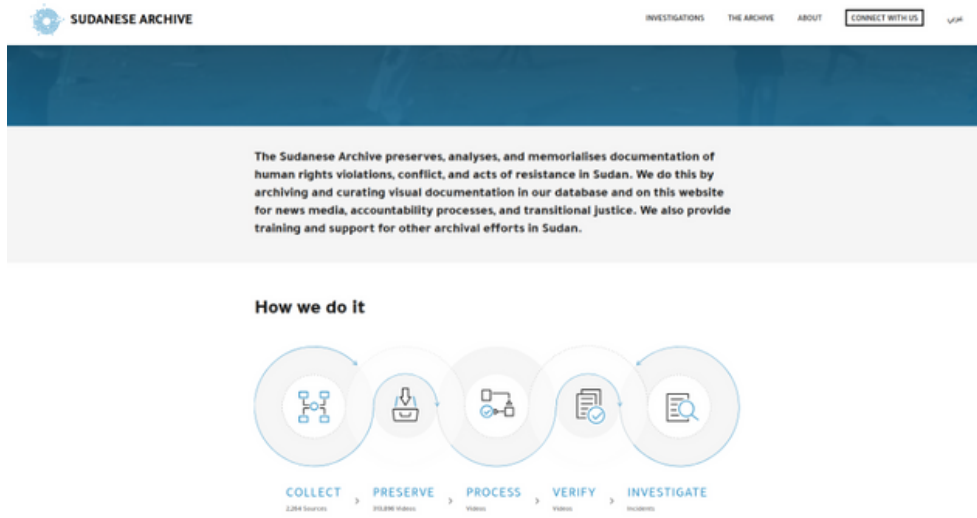
Afganistan Hafıza Evi, Afganistan'daki savaşta hak ihlaline uğrayan kişilere ve hayatta kalanlarına bir saygı duruşudur. Bu çevrimiçi platform, sanal bir müzenin yanı sıra Afgan hak ihlaline uğrayan kişilere ilişkin bir veri tabanı da içermektedir.

Mağdur merkezli bir yaklaşım kullanan Hafıza Evi, hak ihlaline uğrayan kişilerin hayatlarını anmakta ve onlara hikayelerini, deneyimlerini ve beklentilerini paylaşabilecekleri bir platform sağlamaktadır. Bu veri tabanında kamuya açık veya gizli bilgilerle karşılaşacaksınız.

Kamuya açık ve gizli bilgiler arasındaki bu ayrımı koruyarak, şeffaflık ve farkındalık ihtiyacı ile ilgili kişilerin mahremiyetini ve güvenliğini koruma zorunluluğunu dengelemeyi amaçlıyoruz.

## SUDAN ARŞİVİ

WEB SİTESİ: <https://sudanearchive.org/>



Sudan Arşivi, insan hakları savunucularının, insan hakları ihlalleri ve uluslararası suçlarla ilgili dijital bilgileri savunuculuk, adalet ve hesap verebilirliği desteklemek için etkin bir şekilde kullanmalarına yardımcı olmaya adanmış, kâr amacı gütmeyen küresel bir kuruluş olan Mnemonic'in bir projesidir.

Mnemonic, 2019'dan Şubat 2023'e kadar, Mnemonic'in insan hakları ihlallerini ortaya çıkarmak için dijital bilgileri arşivleme, doğrulama ve analiz etme temel misyonuna uygun olarak Sudan Arşivi'ni kurmak için GISA Group ile ortaklık kurdu.

## EK: Referanslar ve Yararlı Kaynaklar

### 1. İnsan Haklarının İzlenmesi

İnsan Hakları İzleme El Kitabı, BM OHCHR. Pdf dosyasını [buradan](#) indirebilirsiniz.

BM İnsan Hakları Yüksek Komiserliği, Veri tabanları:

<https://www.ohchr.org/en/resources/databases>

Sivil Toplum: STK'lar, insan hakları savunucuları ve sivil alandaki diğer aktörler için kaynaklar

<https://www.ohchr.org/en/resources/civil-society>

BMMYK, Acil Durum El Kitabı- risk altındaki kişiler:

<https://emergency.unhcr.org/protection/persons-risk>

Minnesota Üniversitesi İnsan Hakları Kütüphanesi, İnsan Haklarının İzlenmesi Eğitim Kılavuzu:

- Bölüm V: İzlemenin Temel İlkeleri <http://hrlibrary.umn.edu/monitoring/chapter5.html#l>
- Bölüm VII: Bilgi Toplama, <http://hrlibrary.umn.edu/monitoring/chapter7.html>
- Bölüm XX: İnsan Hakları Raporlaması <http://hrlibrary.umn.edu/monitoring/chapter20.html>

Uluslararası İnsan Hakları Servisi: BM organlarıyla ilişki kurarken riskleri ve misillemeleri azaltın,

<https://academy.ishr.ch/security>

Suriye'de Hesap Verebilirlik: bilgi doğrulama için tavsiye ve araçlar ile diğer faydalı kaynakları içerir,

<https://syriaaccountability.org/how-to-document-atrocities-in-the-gaza-war/>

Belgelendirme eğitimi <https://syriaaccountability.org/documentation-practices/>

### 2.HURIDOCS'tan Faydalı Kaynaklar

HURIDOCS modelinden daha fazla veri tabanı örneğini buradan görüntüleyebilirsiniz:

<https://huridocs.org/resource-library/human-rights-research-databases/>

Microthesauri: Microthesauri, insan hakları ihlallerinin farklı yönlerini tutarlı bir şekilde kategorize etmek için 48 terminoloji setinden oluşan bir koleksiyondur. Medeni, siyasi, ekonomik, sosyal ve kültürel hak ihlallerinin kaydedilmesi için bir metodoloji olan Olay Standart Formatları ile birlikte kullanılmak üzere geliştirilmiştir. Ayrıca diğer metodolojileri kullanan belgeleme girişimlerini de bilgilendirmişlerdir:

<https://huridocs.org/resource-library/monitoring-and-documenting-human-rights-violations/microthesauri/>

Terminolojiler, genellikle gönüllüler tarafından çeşitli dillere çevrilmiştir ve Türkçe olarak mevcuttur. Örneğin, ihlal tipolojisine buradan bakabilirsiniz:

<https://docs.google.com/spreadsheets/d/1O9Gfuem8cWJ2ePkGKVkdonWF6Zj3LusD6d3R1t1K-E/edit?gid=0 - gid=0>

### 3. Bilgileri Doğrulama- Tavsiye

İnsan hakları ihlallerini araştırmak ve raporlamak için Yemen Arşivi'ne erişim çok kısıtlıdır ve bağımsız gazeteciler, uluslararası haber ajansları, BM soruşturma organları ve uluslararası insan hakları örgütleri için önemli riskler taşımaktadır. Yemen Arşivi'nin ve diğer belgeleme gruplarının kullanıcı tarafından oluşturulan doğrulanmış içeriğe güvenmesinin başlıca nedeni budur. Bu içerik, insan hakları araştırmalarının yanı sıra ceza davalarının oluşturulmasına da yardımcı olmaktadır. Yemen Arşivi ve diğer belgeleme gruplarının, insan hakları araştırmalarının yanı sıra ceza davası oluşturmaya yardımcı olmak için; doğrulanmış ve kullanıcı tarafından oluşturulan içeriğe güvenmesinin temel nedeni budur.

Veri ve Operasyonel Modeli, Duke Üniversitesi Hukuk Fakültesi tarafından geliştirilen Elektronik Keşif Referans Modeline dayanmaktadır. Aşağıda bu modelin her adımının ayrıntılı bir açıklaması yer almaktadır.

Bilgi toplama süreçleri, dijital içerik için güvenilir kaynaklardan oluşan bir veri tabanının yanı sıra standartlaştırılmış bir meta veri şeması oluşturmayı içeriyordu. Kaynaklar, bireyler ve kuruluşların doğrudan gönderimleri, kamuya açık sosyal medya hesapları ve kanallarının yanı sıra kamuya açık diğer bilgiler olabilir. Metodolojiye ilişkin bölümleri; kaynakların ayrıntılarını, doğrulama kaynaklarını, meta verilerin nasıl düzenleneceğini, videoların nasıl doğrulanacağını vb. içerir: <https://yemeniarchive.org/en/about/methods-tools>

### 4.Dijital Güvenlik Tavsiyeleri ve Bağlantıları

Sivil Haklar Savunucuları veri tabanından örnek: Veri tabanı, bilgilerinizi savunuculuk amacıyla kullanılabilecek ve adalet ve hesap verebilirlik sağlanana kadar saklamak için güvenli bir yer sunar. Bilgisayarınıza saldırılsa veya birisi ofisinize girse bile, verileriniz Civil Rights Defenders'ın sunucularında güvenli olarak saklanır.

Daha fazlası için: <https://crd.org/database/>

**Front Line Defenders (FLD)**, insan hakları savunucularının daha güvenli uygulama ve araçları hayata geçirmelerini amaçlayan pratik, uygulamalı atölye çalışmaları ve uzun vadeli yardım yoluyla insan hakları savunucularını desteklemektedir. Bu desteği 2013'ten bu yana saha tabanlı dijital koruma danışmanlarıyla işbirliği içinde de verir. Bu danışmanlar dünyanın farklı bölgelerinde bulunmakta ve insan hakları örgütleri ve bireysel insan hakları savunucuları ile doğrudan çalışmaktadır. Amaç, ihtiyaçları daha etkili bir şekilde değerlendirmek ve dijital riskleri belirlemek, özel güvenlik politikası tasarlanmasına yardımcı olmak ve bunun uygulanmasında ve uygulamaların günlük iş ve yaşama entegre edilmesinde işbirliği yapmaktır. Bu yaklaşım, en tehlikeli ortamlarda çalışan insan hakları savunucularının bazılarının gerçek yaşam bağamlarına daha doğrudan katılım yoluyla uzun süreli etkiyi kolaylaştırmaktadır. FLD, güvenlik hibeleri programının bir parçası olarak ekipman veya yazılım içerebilen dijital koruma hibeleri de sağlar: <https://www.frontlinedefenders.org/en/programme/digital-protection>

**Security in-a-Box (SiaB)**, 2005 yılında Front Line Defenders tarafından Tactical Technology Collective ortaklığıyla insan hakları savunucularının ve insan hakları örgütlerinin dijital güvenlik taktiklerini ve araçlarını uygulamalarına daha fazla yardımcı olmak amacıyla oluşturulmuştur. SiaB o tarihten bu yana iki kuruluş ve bağımsız uzmanlardan oluşan bir ağ tarafından aktif olarak sürdürülmektedir. SiaB, insan hakları savunucularının bilgisayar veya telefonlarının güvenliğini sağlamalarına, hassas bilgileri daha güvenli bir şekilde depolamalarına ve paylaşımlarına veya internet ve telefon iletişiminin gizliliğini korumalarına yardımcı olan kılavuzlar ile ücretsiz ve açık kaynaklı araçlardan oluşan bir koleksiyondur.

Türkçe olarak mevcuttur: <https://securityinabox.org/tr/>

**The Engine Room**, deneyimli ve kararlı aktivistler, araştırmacılar, teknoloji uzmanları ve toplum örgütleyicilerinden oluşan bir ekibe sahip, kâr amacı gütmeyen bir kuruluştur. Amaçları, sosyal adalet hareketlerinin teknoloji ve verileri güvenli, sorumlu ve stratejik yollarla kullanırken, dijital sistemlerin yarattığı kırılganlıkları aktif bir şekilde azaltmaktır. Pro-bono ortaklıklar ve ücretli danışmanlıklar yoluyla 800'den fazla kuruluşu desteklemişlerdir. Hafif Dokunuş Desteği (Light Touch Support- LiTS) programı ile, sosyal adalet çalışmalarında veri veya teknoloji kullanımı hakkında soruları olan kuruluşlara ve bireylere hafif, ücretsiz destek sunmaktadır: <https://www.theengineroom.org/services-support/light-touch-support/>

**Electronic Frontier Foundation (EFF)**, dijital dünyada sivil özgürlükleri savunan, kâr amacı gütmeyen lider kuruluştur. EFF, etki davaları, politika analizi, taban aktivizmi ve teknoloji geliştirme yoluyla kullanıcı gizliliğini, ifade özgürlüğünü ve yeniliği savunur. Ücretsiz araçlarına buradan gözatabilirsiniz: <https://www.eff.org/pages/tools>