Riskli Araştırmalar:

Araştırmacıların Korunması ve Güvenliği için AoIR Rehberi

Çevirenler:
M. Burak Özdemir
Yeliz Dede Özdemir

AoIR Riskli Araştırmalar Çalışma Grubu

Katkıda Bulunanlar: *Alice Marwick, Dafna Kaufman, Jacob Smith, Patricia Aufderheide, Jessica Beyer, Emma L. Briant, Coppélie Cocq, Laura Dilley, Sam DiBella, Radhika Gajjala, Kamile Grusauskaite, Alex D. Ketchum, Zelly Martin, Janice Metzger, Erin McInerney, Rachel Moran, John McNutt, Suay Melisa Oezkula, Victoria O'Meara, Riccardo Nanni, Carolina Parreiras, Katy Pearce, Ryan Payne, Meredith Pruden, Christian Sandvig, Caighlan Smith, Sam Srauy, Zeerak Talat, Leonie Tanczer, Robert Tynes, Antonia Vaughan, Shenja van der Graaf, Courtney Vowles, Michele White.*

alternatif bilişim

RİSKLİ ARAŞTIRMALAR:
Araştırmacıların Korunması ve Güvenliği İçin AoIR Rehberi

Kasım 2025

ISBN 978-605-74852-8-1

Yazarlar:

Alice Marwick, Dafna Kaufman, Jacob Smith, Patricia Aufderheide, Jessica Beyer, Emma L. Briant, Coppélie Cocq, Laura Dilley, Sam DiBella, Radhika Gajjala, Kamile Grusauskaite, Alex D. Ketchum, Zelly Martin, Janice Metzger, Erin McInerney, Rachel Moran, John McNutt, Suay Melisa Oezkula, Victoria O'Meara, Riccardo Nanni, Carolina Parreiras, Katy Pearce, Ryan Payne, Meredith Pruden, Christian Sandvig, Caighlan Smith, Sam Srauy, Zeerak Talat, Leonie Tanczer, Robert Tynes, Antonia Vaughan, Shenja van der Graaf, Courtney Vowles, Michele White.

Çevirenler:

M. Burak Özdemir
Yeliz Dede Özdemir

Kılavuzun orijinali için:
Risky Research: An AoIR Guide to Researcher Protection and Safety (2025).
https://aoir.org/riskyresearchguide/

Alternatif Bilişim Derneği
Kentkoop Mh. 1685. Cadde No:11/10 Batıkent-Yenimahalle/Ankara +90 312 230 1560
bilgi@alternatifbilisim.org http://www.alternatifbilisim.org

alternatif bilişim

SUNUŞ

Alternatif Bilişim Derneği olarak dijital haklar ve özgürlükler alanındaki çalışmalarımızın temelinde, dijital dünyanın daha eşitlikçi, güvenli ve özgür bir yer hâline gelmesi hedefi yer almaktadır. Bu doğrultuda, eleştirel bilgi üretimini desteklemek ve araştırmacıların karşılaştığı risklere karşı dayanıklılığı artırmak önceliklerimiz arasındadır.

İnsan hakları, toplumsal cinsiyet eşitliği, çevre, göç, ayrımcılık, ifade özgürlüğü ve dijital sansür gibi alanlarda çalışan araştırmacılar, gazeteciler, sivil toplum emekçileri ve aktivistler günümüzde hem çevrimiçi hem de çevrimdışı ortamlarda çok yönlü ve giderek ağırlaşan tehditlerle karşı karşıya kalmaktadır. Taciz, itibarsızlaştırma kampanyaları, hukuki soruşturmalar ve fiziksel şiddet tehdidi artık istisna değil, ne yazık ki sık rastlanan ve öngörülebilir birer risk hâline gelmiştir. Bu durum, araştırmacı güvenliğinin bireysel önlemlerle sınırlı kalamayacağını; kolektif sorumluluk, dayanışma ve kurumsal destek gerektirdiğini açıkça göstermektedir.

Association of Internet Researchers (AoIR) tarafından hazırlanan ve Burak Özdemir ile Yeliz Dede Özdemir tarafından çevrilen bu rehberin, tam da bu ihtiyaçlar doğrultusunda önemli bir boşluğu doldurduğuna inanıyoruz. Toplumsal kutuplaşma, baskılar ve dijital tehditlerin arttığı günümüz koşullarında, araştırma güvenliği konusunda ortak bir dil ve dayanışma zemini oluşturmanın özgür ve eleştirel bilgi üretimi için vazgeçilmez olduğuna inanıyoruz.

Alternatif Bilişim Derneği olarak bu çalışmanın Türkçeye kazandırılmasına katkıda bulunmaktan memnuniyet duyuyor; dijital hakların korunmasına yönelik dayanışmacı, kapsayıcı ve güvenli bir ortam yaratmak için araştırmacılar, kurumlar ve tüm bilgi üreticileriyle iş birliğini sürdürme kararlılığımızı vurguluyoruz. Bu rehberin Türkiye'deki eleştirel bilgi üreticileri için koruyucu, güçlendirici ve dayanışmayı besleyen bir kaynak olmasını diliyoruz.

Alternatif Bilişim Derneği
Kasım 2025

İçindekiler

1. Giriş ve Arka Plan

Kasım 2022'de düzenlenen AoIR konferansında, dijital araştırmaların giderek karmaşıklaşan yapısı nedeniyle araştırmacıların yoğun şekilde karşı karşıya kaldıkları riskler tartışmaya açıldı. Aslına bakılırsa aynı konu, önceki AoIR etkinliklerinde de sıklıkla gündeme gelmişti.

Bu rehberde "riskli araştırma" kavramı, dış aktörler kaynaklı zararlara maruz kalma olasılığı bulunan akademik çalışmaları tanımlamak için kullanılmaktadır. Bu tür araştırmalar genellikle dezenformasyon, aşırılık, LGBTQ+ bireyleri ilgilendiren konular, eleştirel ırk teorisi, üreme adaleti, feminizm ve iklim değişikliği gibi politik ya da toplumsal açıdan tartışmalı başlıkları içermektedir. Risk, özellikle ırkçılığa maruz kalan veya marjinalleştirilmiş kimliklere aidiyet hisseden veyahut da güvencesiz ekonomik koşullarda hayatını idame ettirmek zorunda kalan araştırmacılar için çok daha yüksektir.

Riskli araştırmaların olası zararları kapsamlı bir şekilde ortaya konmuştur: çevrim içi taciz, duygusal ve ruhsal sağlık sorunları, mahremiyet ihlalleri, iş kaybı ve itibar zedelenmesi (Doerfler et al., 2021; Massanari, 2018; Sobieraj, 2020). Bu tehlikelerle karşılaşma olasılığı, algoritmik olarak şekillendirilmiş küresel medya ekosisteminin araştırmacının ait olduğu çevrenin ya da kültürel bağlamın ötesinden gelebilecek tehditleri mümkün kılmasıyla daha da artmaktadır.

2016 yılında Data & Society tarafından benzer içerikli riskleri azaltmaya yönelik ilk rehber yayımlanmıştır. Ancak söz konusu rehber, eskimiş bir sosyopolitik ve teknolojik döneme ait olduğundan artık yetersiz kalmaktadır. Daha yakın zamanda, Araştırma Destek Konsorsiyumu çevrim içi tacize maruz kalan araştırmacılar için kapsamlı bir kılavuz yayımlamıştır, ancak kapsamı sadece tacize yönelik olduğu için sınırlı bir içeriğe sahiptir. Dolayısıyla, AoIR bünyesinde bir Riskli Araştırmalar Çalışma Grubu kurulması uygun görülmüştür.

İnternet araştırmaları alanında önde gelen bir kuruluş olan AoIR, eleştirel akademik çalışmalar konusundaki güçlü geçmişiyle bu tür zorlukları tartışmaya açma noktasında iyi bir sicile sahiptir. AoIR Etik Rehberleri dünya genelinde benimsenerek araştırmacıların etik açıdan duyarlı çalışmalar tasarlamalarına ve benzer şekilde etik kurullar ile insan araştırmaları etik komiteleri kapsamındaki sorunları sağlıklı bir şekilde çözüme kavuşturmalarına yardımcı olmaktadır.

Bu belge de benzer şekilde yapılandırılmıştır ve şu konu başlıkları ile ilgili olarak rehberlik etmeyi amaçlamaktadır

- Araştırmacıların karşılaştığı risklerin anlaşılması için bir çerçeve sunmak.
- Tehditlerin bireysel, kurumsal ve kolektif düzeyde azaltılmasına yönelik ilkeler belirlemek.
- Saldırılara karşı anlık müdahale stratejileri geliştirmek.
- Araştırmacıların kariyerlerinin her aşamasında faydalanabilecekleri özenle derlenmiş kaynaklar ve en iyi uygulama setleri önermek.

Çalışma Grubu, araştırmacıların riskleri yönetme konusunda tüm sorumluluğun kendilerine atfedildiği (ve bu çabalar kaçınılmaz olarak başarısız olduğunda sıklıkla suçlandığı) bireyselleştirilmiş bir paradigmadan, akademik topluluğun dirayetli yapısına öncelik veren ve kurumsal hesap verebilirlik talep eden kolektif bir paradigmaya geçilmesi gerektiğini

savunmaktadır. (Mattheis & Kingdon, 2021; Vaughan, 2021). Bu paradigma değişimi, yalnızca geniş kapsamlı bir bilgi ekosistemini güçlendirmekle kalmayacak (Sun et al., 2022), aynı zamanda bu ekosistem içerisinde çalışanlara çok daha güçlü bir koruma sağlayacaktır (Payne et al., 2023).

Araştırmacıların korunması yalnızca zararları azaltmakla ilgili bir durum değildir. Aynı zamanda yüksek risk içermekle birlikte kıymetli addedilen akademik çalışmaların, eleştirelliğe tahammülsüzlüğün giderek arttığı ortamlarda dahi sürdürülebilmesine olanak tanımaya yöneliktir.

2. Ortak Risk Yönetimi ve Zararlara Karşı Alınacak Önlemler

A Akran Destek ve Yardım Ağları

B Kurumsal Sorumluluklar

2. Ortak Risk Yönetimi ve Zararlara Karşı Alınacak Önlemler

Bu belgenin büyük bölümü, bireysel araştırmacıların taciz, şiddet ve diğer risk durumlarında nasıl bir tutum takınacaklarına odaklanmaktadır. Ancak bu tarz zarar verici durumların sorumluluğunun tümüyle araştırmacılara yüklenemeyeceğinin altı bu noktada bir kez daha çizilmelidir. Araştırmacılar bu rehberde bahsi geçen tüm çözüm önerilerini harfiyen uygulasalar dahi, ciddi tehditlerle karşı karşıya kalma ihtimalleri her zaman bakidir.

Risk azaltma yollarına dair mevcut kaynaklar çoğunlukla bireysel düzeyde yapılacakları öne çıkarmaktadır. Ancak hiçbir araştırmacı, arkasında yapısal nedenler bulunduran zararları tek başına önleme ya da kontrol etme gücüne sahip değildir. Özellikle marjinalleştirilmiş kimliklere sahip olan, ekonomik açıdan kırılgan durumda bulunan ya da radikal/eleştirel çalışmalar yürüten (örneğin feminist, sömürgecilik karşıtı veya queer araştırmalar yapan) araştırmacıların dijital ortamlarda tacizi önlemek adına verdikleri, genellikle görünür olmayan emek, kurumlar tarafından tanınmalı ve dikkate alınmalıdır. Bu tür araştırmacılar, akademide ilerleyebilmelerine ve kariyerlerini sürdürebilmelerine doğrudan etkisi olan "güvenli bir çalışma" (Vera-Gray, 2017) yürütmek durumundadırlar.

"Bireysel dirayet" odaklı yaklaşımlar yerine, araştırmacı güvenliği ile ilgili olarak kurumların tutumlarını sorgulamaları gerekmektedir. Risk azaltımı bireyin omzuna bırakılan bir sorumluluk olmaktan çıkarılmalı, kolektif bir çabayla ele alınmalıdır. Benzer biçimde, hem aktivistler hem de araştırmacılar sosyal medya platformlarının, özellikle toplumsal cinsiyete dayalı dijital şiddetle bağlantılı siber şiddet vakalarında mağdurlara kaynak ve destek sağlaması gerektiğini ileri sürmektedir. Bu yöndeki çağrılar, kaynaklara erişim, anahtar kelimeler ve içerik filtrelemesinin iyileştirilmesi, uzmanlarla iş birliği yapılması gibi önleyici tedbirleri konu edinmektedir (Citron, 2023; Suzor ve diğ., 2019). Bu yaklaşıma göre risk yaratımında platformların önemli bir payı vardır ve dolayısıyla katılımcı güvenliğini sağlamaya yönelik önleyici ve destek odaklı uygulamalara ön ayak olmalıdır.

Bu belge genelinde, yüksek riskli araştırmalar yürüten akademisyenleri desteklemek amacıyla kurumların ve yöneticilerin hızlı müdahale ekipleri ya da bilgilendirilmiş-travma protokolleri gibi kalıcı koruma mekanizmalarını nasıl oluşturabileceklerini ele almaktayız. Aynı şekilde araştırmacıların da farklı gruplar ve topluluklar arasında risklerin eşit dağılmadığını kabul etmesi gerekmektedir. Risk azaltımına, güvenlik ve yardım ağlarının tesisine yönelik kolektif yaklaşımlardan hareketle atılacak adımların başarısı, kanıta dayalı stratejiler geliştirmeye, kurumsal hesap verebilirliğe ve yapısal değişimin gerekli olduğuna dair güçlü bir inançla doğru orantılıdır.

A. Akran Destek ve Yardım Ağları

Çevrim içi ortamları araştıran akademisyenler, çoğu zaman yaşadıkları coğrafi bölgelerde ya da kurumlarında kendilerini yalnız hissetmektedir. Bu yalnızlık hissi, toplu hareket etme imkanlarının azaldığı özellikle küresel sağlık krizleri ya da jeopolitik çatışmalar gibi olağanüstü dönemlerde daha da derinleşmektedir. Ancak topluluk kavramını sadece kendi bölümümüzle sınırlamayıp daha geniş bir internet araştırmacıları ağına yayarsak, zararları azaltmaya yönelik daha güçlü ve bütünleşik stratejiler geliştirmek mümkün olacaktır.

Kolektif bir anlayışla riskleri azaltmanın önemli bir adımı, yerel, ulusal ve küresel düzeylerde akran destek ve yardım ağlarının oluşturulmasıdır. Kurumsal düzeyde işleyecek bu yapılar, araştırmacıların olası risklere hazırlanmalarına, deneyimlerine anlam katmalarına ve sadece savunmasız bireylerin omuzlarına yüklenmemesi gereken dışlanmışlık hissinden sıyrılmalarına aracılık edecektir. Kurumlar, çevrim içi ya da yüz yüze toplantılar gibi akran desteği sağlayacak özel alanlar yaratmalı, bu alanlarda araştırmacılar deneyimlerini paylaşmalı, kaygılarını dile getirmeli ve karşılaşılan sorunlarla başa çıkma stratejilerini birbirleriyle konuşabilmelidir. Destek ağları, tacizin kimlik ve konuma bağlı olarak değişkenlik gösterebileceği hususunu da göz önünde bulundurmalıdır. Tek tip yaklaşımlar işe yaramayacak; toplumsal cinsiyet ve ırk gibi farklılıkları göz ardı eden politikalar, herkesi eşit biçimde korumakta başarısız olacaktır.

B. Kurumsal Sorumluluklar

Akademik dünyanın güvencesizliği ve rekabetçi doğası izole edici bir yapı arz ettiği için dayanışma ağlarının varlığı hayati önemdedir. Araştırmacılar sadece bilgi üretiminde değil, herkes için daha güvenli ve adil koşulların oluşturulması noktasında da birlikte çalışmalıdır. Bu birliktelik, doğrudan muhatabı biz olmasak bile tacize maruz kalan meslektaşlarımız için kurumsal destek talep etme gibi beklentileri de dikkate almalıdır. Entelektüel özgürlüğün korunması ve akademisyen güvenliğinin sağlanması için araştırma kurumlarına sorumluk atfedilmesi gerekmektedir. Tacize maruz kalan akademisyenlere yönelik uzun vadeli destekte bulunmak, travma sonrasına yönelik düzenlemeler yapmak ve açık dayanışma kanalları tesis etmek kurumların yükümlülükleri arasında yer almaktadır. Tüm bu riskleri ortadan kaldıracak evrensel bir politikanın varlığından söz etmek mümkün gözükmese de güçlü bir kurumsal adanmışlığın, bireysel araştırmacı üzerindeki yükü hafifletmeye ve daha sağlam bir akademik topluluk inşasına aracılık edeceği muhakkaktır.

Toplumsal cinsiyete dayalı şiddetle mücadelede topluluk temelli müdahale pratikleri, hapishane karşıtı ağlar ve dayanışma girişimleri gibi dönüştürücü gücü yüksek hak temelli toplumsal hareketler üzerine var olan literatüre yaslanan elinizdeki rehber, kolektif destek ve hesap verebilirliğin önemine vurgu yapmaktadır (Rentschler, 2017). Geleneksel kurumsal mekanizmalar, savunmasız araştırmacıları korumada sıklıkla yetersiz kalmakta; bunun yerine onları hiyerarşiler içinde daha da yalnızlaştırmaktadır. Aksine akran temelli, travma hassasiyetli yaklaşımlar ise mağdur ihtiyaçlarını merkeze alarak sorumluluğu akademik topluluk içinde kolektif olarak dağıtmaktan yana tavır almaktadır. Zararın etkilerini azaltmaya, topluluk dayanışmasına ve mağdur merkezli desteğe öncelik veren taban hareketlerinden öğreneceğimiz çok şey vardır. Aşağıdan gelen bu hareketler, yüksek riskli araştırmalar yürüten araştırmacıların korunmasına yönelik etkili ve sürdürülebilir stratejiler geliştirmemize ön ayak olacaktır.

3. Kapsam ve Amaç

3. Kapsam ve Amaç

Bu belge, araştırma yürüten kişilerin maruz kalabileceği risklere odaklanmaktadır. İnsan araştırmaları etik kurulları, kurumsal etik komiteleri ve AoIR gibi kurumların, araştırmada veri kaynağı olarak kullanılan kişilere yönelik potansiyel riskleri tanımlama konusundaki katkılarını içtenlikle destekliyor olsak da bu rehberin öncelikleri başkadır.

Belgenin bu anlamda dört temel hedefi bulunmaktadır:

1. **Yürütmekte oldukları projelerle araştırmacıların kendilerini riske atıp atmadıklarını değerlendirme süreçlerine yardımcı olmak ve karşılaşabilecekleri tehditleri ortaya koymak.**
2. **Araştırmacıların riskleri azaltabilmeleri, tehditlerle başa çıkabilmeleri ve kurum içi savunuculuk faaliyetlerini besleyen kaynaklara erişebilmeleri için somut adım önerisinde bulunmak.**
3. **Üniversiteler, düşünce kuruluşları ve sivil toplum örgütleri gibi kurumlara, riskli araştırmalara dâhil olan çalışanlarını nasıl daha iyi koruyabileceklerine dair yol gösterici olmak.**
4. **Bireysel sorumluluğun ötesine geçen ve daha geniş bir araştırma topluluğunun dayanışma gücünü harekete geçiren kolektif risk azaltma yaklaşımlarını tetkik etmek.**

AoIR Etik Rehberleri üzerine inşa edilen bu rehber, yalnızca araştırma katılımcılarının değil, araştırmacıların kendilerinin de korunmasının önemini vurgulamaktadır. Kurumsal hesap verebilirliğin teşvik edilmesi ve kolektif stratejilerin benimsenmesiyle iş bu rehber, yüksek riskli alanlarda çalışan akademisyenler için güvenli ve destekleyici bir ortam yaratılmasını amaç edinmektedir.

Uluslararası bir okur kitlesine hitap edebilmek amacıyla, rehberde belirli ülke ya da bölgelere özgü risklere de yer verilmiştir ve dolayısıyla bu rehber, dünyanın dört bir yanından araştırmacıların katkılarına açık bir hale getirilmiştir. Her araştırmacının risk teşkil eden durumlarla karşılaşma ihtimali olsa da azınlıklar ve marjinalleştirilmiş kimliklere sahip olan, güvencesiz istihdam koşullarında çalışan ya da faşist/otoriter siyasi rejimlerde faaliyet gösteren kişiler söz konusu risklere karşı çok daha savunmasızdırlar. Bu durum, lisans ve lisansüstü öğrenciler, doktora sonrası araştırmacılar, sözleşmeli öğretim elemanları ve bağımsız araştırmacılar gibi özellikle kadrosuz ve kısıtlı kurumsal güvence sahibi araştırmacılar için geçerlidir.

Zorlu durumların çoğunlukla aşırı sağcı gruplar gibi düşmanlık güden aktörlerden kaynaklandığını kabul etmekle birlikte, araştırmacıların benzer ideolojik pozisyonları paylaştığı kişiler de dahil olmak üzere siyasi yelpazenin her kesiminden kişiler tarafından zarar görebileceği ihtimalini ayrıca kabul etmekteyiz. Riskler, devletlerden, şirketlerden, sosyal medya platformlarından, diğer araştırmacılardan ya da apolitik görünen çevrim içi topluluklardan (örneğin fandomlar) da kaynaklanabilmektedir. Bu rehber, bu çok katmanlı tehdit ortamını göz önünde bulundurmakta ve araştırmacıların bu ortamda nasıl hareket edebileceklerine dair stratejiler geliştirmeyi hedeflemektedir.

4. Risk Altında mıyım?

A Araştırmanız riskli mi?

B Riskli araştırmalar yürütmeli misiniz?

4. Risk Altında mıyım?

Riskli araştırma, araştırmacıyı dışsal zararlara açık hale getiren çalışmalardır. Yönelttikleri araştırma soruları ve bu sorulara verdikleri yanıtlar nedeniyle, araştırmacıların kariyerleri, itibarı, aileleri ya da yaşamları tehdit altına girebilmektedir. Elbette her araştırma beklenmedik sonuçlara gebedir, ancak herhangi bir araştırmanın "riskli" addedilmesi, bağlam bağımlı olarak değişkenlik gösterecektir. Aynı tür bir araştırma projesi, farklı araştırmacılar açısından coğrafi/siyasi bağlama, araştırmacının kimliğine ve kurumsal destek olanakları gibi etmenlere bağlı olarak çok farklı sonuçlar doğurabilmektedir.

Bu bölüm, bir araştırma projesinin risk düzeyinin yüksek olup olmadığını değerlendirmek için temel ölçütleri ve araştırmacıların bu zorluklarla nasıl başa çıkabileceklerine dair çözüm önerilerini ele almaktadır.

A. Araştırmanız riskli mi?

Bazı durumlarda araştırmacılar riskli bir çalışma yürüttüklerinin farkındadırlar. Ancak yine de olası tüm riskleri hesaba katmak noktasında zorlanacaklardır. Başta sorunsuz gibi duran bir proje, politik sebeplerle zaman içerisinde hassas bir konu başlığına karşılık gelebilmekte veya araştırmacı, çalışmasının doğurabileceği muhtemel zararları başlangıçta tam manasıyla ön görmekte başarısız olabilmektedir. Akademik danışman ya da mentorlar, yeni araştırmacıların potansiyel riskleri değerlendirmelerine yardımcı olmada önemli bir yere sahiptir. Bu nedenle, özellikle kariyerlerinin başındaki araştırmacılar için danışmanların ve akademik rehberlerin olası riskleri değerlendirme ve bunlarla başa çıkma stratejileri geliştirme konularında rehberlik sağlaması büyük önem taşımaktadır.

Araştırmacıların karşılaşabileceği riskleri genel olarak dört başlık altında toplamak mümkündür:

1. **Politik açıdan hassas konu başlıkları ve/veya güçlü aktörleri eleştiren bulgular kaynaklı riskler**
2. **Teknoloji şirketlerine meydan okuyan yöntem ya da bulgular kaynaklı riskler**
3. **Araştırmacının kimliksel aidiyetine bağlı olarak ortaya çıkan riskler (örneğin marjinalleştirilmiş ya da ırkçılığa maruz bırakılmış olması)**
4. **Araştırmacının görünürlüğü kaynaklı riskler (örneğin sosyal medyada ya da kamuoyunda bilinirliği)**

Aşağıdaki sorular, araştırmacıların çalışmaları nedeniyle hedef hâline gelip gelmeyeceklerini değerlendirmelerine yardımcı olma potansiyeli taşımaktadır.

1. Politik Açıdan Hassas İçerikli Araştırmalar

Siyaseten hassas konular üzerine çalışan akademisyenler, özellikle de konuları aşırı sağın ilgi alanıyla örtüşüyorsa, ciddi risk altında demektir. Bu alanda çalışan araştırmacılar genellikle konularının tartışma yaratacağını kestirseler de araştırmanın taşıdığı tüm risk türlerini her zaman fark etmeyebilmektedir.

Bu anlamda risk barındıran temel bazı konu başlıklarını şöyle sıralayabiliriz:

- Eleştirel ırk teorisi
- Toplumsal Çeşitlilik, Eşitlik ve Kapsayıcılık (DEI)
- Feminizm
- Üreme adaleti
- İklim değişikliği
- Güçlü şirketler ya da devlete yönelik eleştiriler
- LGBTQIA+ hakları
- Siyasi yansımaları olan seçim güvenliği ve dezenformasyon arasındaki ilişkinin sorgulanması

Yukarıda sıralanan konu başlıkları ile ilgili araştırma yapan akademisyenler, politik ya da toplumsal baskının yoğun olduğu anti-demokratik rejimlerde devlet görevlileri, ideolojik gruplar ya da büyük ölçekli şirketler tarafından hedef alınma riskini her zaman hesaba katmak durumundadır.

Nispeten daha az tartışmalı konular (örneğin gelir eşitsizliği, sosyal medya platformları, şirket sahipliği vb.) üzerine yapılan araştırmalar da benzer şekilde şirketler ile ulus-devlet yapılanmalarındaki iktidar sahiplerinin çıkarlarına ters düşebilmektedir. Bu tür çalışmalar yapan akademisyenler, söz konusu araştırmalardaki "riskleri" tam anlamıyla kavramadan hareket edebilmektedirler.

Bu tarz araştırmalar yürüten bilim insanlarının yöneltmesi gereken sorular şunlardır:

- Bu konu tartışmalı mı? Kimler açısından?
- Yürütülen proje, güçlü aktörlerin (siyasi çevrimiçi/ partilerin, şirketlerin, devletlerin, çevrimdışı grupların) çıkarlarıyla çatışıyor mu?
- Güncel siyasi tartışmalara dolaylı ya da doğrudan bir şekilde dahil oluyor muyum?
- Siyasi yelpazenin uç noktalarını göz önünde bulundurursam, araştırmam aşırı bir grup tarafından benimsenen siyasallaşmış anlatıları destekliyor mu yoksa bu anlatıların karşısında mı konumlanıyor?
- Araştırmam, baskın tarihsel anlatıları sorguluyor mu? Egemen grupların geçmiş hak ihlalleri gibi tarihsel olaylardaki sorumluluklarını ortaya koyuyor mu?
- Çalışmam, aktivistleri/araştırmacıları/gazetecileri baskıcı bir niyetle hedef aldığı bilinen bir hükümet veya grubun—tarihsel olayların çerçevelenmesi de dahil olmak üzere—dolaşımdaki baskın anlatılarını eleştiriyor mu?
- Bulgularım, toplumsal zarar verebilecek teknolojileri veya politikaları meşrulaştırıyor mu? Araştırmamın gerici veya antidemokratik toplumsal veya siyasi hareketler lehine kullanılma ihtimali nedir?
- Araştırmam ne derece görünür durumdadır? Medyada veya dijital ortamlarda çok konuşulan, gündem olmuş bir konu başlığına mı karşılık gelmektedir?

2. Teknoloji Şirketlerine Yönelik Eleştiriler

İkinci olarak, özellikle çevrim içi platformları araştıran akademisyenler, sosyal platformları denetlemek veya platform verilerini kazımak gibi bir platformun Hizmet Şartlarını ihlal ettiği varsayılan yöntemler kullanarak bulgularını yayımladıklarında teknoloji şirketlerinin açık hedefi haline gelebilmektedir. Bu yöntemler, kurumsal veya etik inceleme kurulları tarafından reddedilebilmekte ve hatta cezai veya hukuki suçlamalarla karşılaşabilmektedir. Örneğin

Facebook, platformdaki politik içerikli reklamlar aracılığıyla dezenformasyon yayılımını inceleyen bir araştırma projesinin sonlandırılmasına sebep olmuştur (Ortutay, 2021). Platform, ilgili akademisyenlere ihtarname göndermiş ve ardından onları siteden tamamen yasaklamıştır. Araştırmacılar, incelemelerinin Facebook Reklam sistemindeki kusurları gösterdiğini savunurken, Facebook araştırmacıların yöntemlerinin platformun gizlilik uygulamalarını ihlal ettiğini iddia etmiştir. Kullanılan araştırma yöntemlerinin Hizmet Şartlarını açıkça ihlal etmediği durumlarda bile, X benzeri şirketler yalnızca eleştirildikleri için araştırmacılara karşı hukuki yollara başvurabilmektedir. Örneğin Meta, platformun reklam moderasyonundaki kusur ve ihmallerini gündeme getiren Brezilya'daki Rio de Janeiro Federal Üniversitesi araştırmacılarının güvenilirliklerini geçersiz kılacak adımların atılması için hukuk ekibinden destek almıştır (Nakamura & Orrico, 2024).

Araştırmacılar bu gibi durumlarda şu soruları sormalıdır:

- Yöntemlerim, bir platformun Hizmet Şartları'nı ya da ilgili mevzuatı (ör. ABD'deki Bilgisayar Dolandırıcılığı ve Suistimal Yasası) açıkça ihlal ediyor mu?
- Bulgularım, platformun kamuoyundaki itibarını zedeleyebilir mi? Bulgular, kamuoyuna açıklandığı takdirde dava geçmişi olan bir platforma gölge düşürebilecek savlar öne sürüyor mu?

3. Araştırmacının Konumu ve Kimliği

Üçüncü olarak, ırkçılığa ya da toplumsal dışlanmaya maruz kalan kimliklere sahip ya da akademide yeterince temsil edilmeyen gruplar arasında yer alan akademisyenler, ağ tabanlı taciz ve itibarsızlaştırma girişimleri gibi risklerle çok daha sık karşılaşmaktadır. Çalışmaları politik açıdan birilerinin sinir uçlarına dokunmaya başladığında ağ üzerinden taciz, yıldırma, ekonomik sıkıntı yaratma, itibar zedeleme ve benzer nitelikli diğer istismar biçimlerine hedef olma olasılığı daha da artacaktır.

Ayrıca, ırkçılığa maruz bırakılan ve/veya marjinalleştirilmiş kimliklere aidiyet hisseden araştırmacılar, güncel bir politik meseleyle doğrudan ilişkisi olmayan bir araştırma yürütüyor olsalar bile, çevrimiçi alanlarda "istilacı" olarak görülüp bu alanlardan uzaklaştırılması gereken kişiler olarak etiketlenmektedir. Örneğin, bir hayran topluluğu ya da çevrim içi oyun ortamı üzerine kültürel bir çalışma yürüten bir akademisyen, söz konusu platformun kullanıcıları (örneğin beyaz, biyolojik cinsiyetçi, heteroseksüel, erkek ve genç) tarafından araştırmacının sırf farklı bir aidiyeti olduğu gerekçesiyle ve hatta çalışmanın konusuna dahi bakılmaksızın hedef tahtasına konabilmektedir.

Bu gibi durumlarda araştırmacıların yukarıdakilere ek olarak kendilerine sorabilecekleri bazı sorular şunlardır:

- Irkçılığa maruz bırakılan ve/veya azınlık konumunda olan bir ya da birden fazla demografik gruba aidiyetim var mı?
- İncelediğim kişi ya da ortamlar, kendi topluluklarına dışarıdan gelenleri denetleyen, kültürel olarak bütünlüklü bir yapı teşkil ediyor mu?
- Araştırma konusu olan grubun demografik yapısı hakkında herhangi bir varsayım ya da çıkarımda bulunmak mümkün müdür? Grubun baskın demografik yapısı beni dışarıda tutan nitelikler sergiliyor mu?
- İncelediğim alanlardaki kişiler, belirli bir nüfus grubunu marjinalleştiren söylemleri dillendiriyorlar mı ya da örtük biçimde de olsa belirli demografik grupların kabul

edilemez niteliklere sahip olduğunu mu savunuyorlar? Örneğin, video oyunu topluluklarını inceleyen akademisyenler, topluluk genelinde kadınların oyun gruplarında/klanlarında sorun yarattıklarına ya da erkekler kadar iyi oyuncular olmadıklarına dair kolektif bir görüşle baş etmek durumunda kalabilmektedir.

4. Araştırmacının Görünürlüğü

Son olarak, bir araştırmacının görünürlüğü başlı başına bir risk unsuru teşkil edebilmektedir. Motivasyonlarını bu işe kanalize etmiş aktörlerin eski makalelerini, konferans bildirilerini ya da sosyal medya paylaşımlarını deşmeye yönelik eylemleri ve bunları ağ tabanlı taciz ya da başka zarar verici eylemleri meşru gösterecek şekilde "kanıt" olarak kullanma çabaları neticesinde bazı konu başlıkları bir anda riskli hale gelebilmektedir. Akademisyenler, geçmişte fazlaca dikkat çekmemiş olan çalışmalarının, politik gündemin seyrine göre tartışma yaratabileceğinin farkında olmalıdır. Buna ek olarak bazı kötü niyetli kişiler, çevrim içi arşivleri (örneğin Internet Archive ya da archive.today gibi platformlar) ve araştırmacıların sosyal medya hesapları ya da kurumsal profillerini kullanarak, aksi halde bulunması zor olan eski içerikleri gün yüzüne çıkarabilmektedir.

Akademisyenlerin bu konuyla ilgili olarak kendilerine sorabilecekleri sorular şunlar olabilir:

- Kişisel ya da kurumsal web sayfaları gibi kamuya açık profillerimde araştırma ilgi alanlarıma ya da çalıştığım konulara ilişkin bilgiler yer alıyor mu? İletişim bilgilerime kolayca erişim sağlanabilir mi?
- Daha önce yaptığım araştırmalar hedef gösterilmiş mi?
- Sosyal medyada ne kadar görünür durumdayım? Çalışmalarımı, beni taciz riski altına sokabilecek kişilere iletecek geniş bir takipçi kitlem var mı? Öte yandan, bu görünürlük, eğer kendimi bu alanda uzman olarak konumlandırdıysam ve tehdit durumunda beni destekleyebilecek kaynaklara erişim sağlayabilecek bir pozisyondaysam, çalışmama yönelik bir tür "koruma" kalkanı görevi görebilir mi?
- Basında alıntılanmak, halka açık konferanslar vermek, podcast ya da televizyon programlarına katılmak gibi daha çok kamuya açık akademik faaliyetlerde bulunuyor muyum?
- Irkçılığa maruz bırakılan ve/veya marjinalleştirilmiş grup aidiyetim, geçmişte hakkımda paylaşılan bilgilerin yeniden dolaşıma girmesi halinde hedef alınma riskimi artırıyor mu? (Bu durum özellikle trans bireyler açısından daha zararlı olabilmektedir; çünkü kişinin "eski isminin" kamuoyuna açıklanması travmatik ya da tehlikeli sonuçlar doğurma potansiyeli taşımaktadır.)
- Hedef alınmam halinde, ağlarım arasında kimlik bilgisi tespiti kolay olan arkadaş ya da aile üyeleri bulunuyor mu? Onların iletişim bilgilerine ulaşmak ne kadar kolay? (Bu durum özellikle, aile bireyleriyle paylaşılan nadir soyadlarına sahip kişiler açısından önemlidir.)

B. Riskli Araştırmalar Yürütmeli Misiniz?

Araştırmacı, projesinin riskli olduğunu düşünüyorsa bu projeye devam edip etmeme kararını dikkatlice değerlendirmelidir. Pek çok akademisyen bu risklere rağmen çalışmalarına devam etmektedir. Yine de tespiti yapılan riski almamaya karar vermek de son derece meşru bir eylem biçimidir. Kimi zaman çok tartışmalı bir konuda hiç olumsuz tepki gelmezken, risksiz görülen bir konuda bile ciddi sonuçlarla karşılaşmak mümkündür. Özellikle doktora öğrencileri ve genç

araştırmacılar için danışmanların bu noktada destekleyici bir rol oynaması büyük önem taşımaktadır.

Eğer bir kişi, araştırma projesinin potansiyel riskler barındırdığını düşünüyorsa, devam edip etmeme konusunda kendisine şu soruları sormalıdır:

- Çalışma ne derece görünür durumdadır? Tez mi yazıyorsunuz, akademik dergilerde makale mi yayınlıyorsunuz, yoksa daha geniş kitlelere hitap eden kamuya açık mecralar için mi üretimde bulunuyorsunuz?
- Araştırmanızın "kamusal" bir tarafı olması bekleniyor mu, ya da siz böyle bir görünürlük umuyor musunuz?
- Kariyerinizin hangi aşamasındasınız? Destekleyici bir danışmanınız var mı? İstihdam durumunuz güvencesiz mi, yoksa kadrolu musunuz? Araştırmanızın durdurulması ya da askıya alınması gerektiğinde kendinizi destekleyecek maddi/sosyal kaynaklara sahip misiniz? Şu anda ya da gelecekte, akademisyenlere karşı destekleyici ya da düşmanca bir tavır takınan ülkede bulunma durumunuz söz konusu olabilir mi?
- Sizden daha az ayrıcalığa ve korumaya sahip insanları sürece dahil ediyor musunuz? Lisans öğrencileri, bilgi verenler, araştırma katılımcıları, yüksek lisans ve doktora öğrencileri, doktora sonrası araştırmacılar ya da kadrosuz akademik personel bu kapsamda değerlendirilebilir.
- Ne düzeyde kurumsal desteğe sahipsiniz? Destek ve bakım için başvurabileceğiniz kişiler veya topluluklar kimlerdir? İçinde bulunduğunuz kurumun, araştırmacıları koruma ve destekleme konusundaki geçmiş sicili nasıldır?

Son sorunun yanıtını vermek her zaman kolay değildir. Bu konuda akranlarınıza danışınız veya kurumunuzda başka akademisyenlerin olumsuz sonuçlarla karşılaşıp karşılaşmadığını ve kurumun bu kişileri nasıl desteklediğini ya da desteklemediğini öğreniniz. Bu durum ülkeye, kurumunuzun kamuya mı özel sektöre mi ait olduğuna, bağlı olduğunuz bölüme ve benzeri başka değişkenlere göre farklılık gösterecektir.

5. Risk Azaltma Odaklı Araştırma Tasarımı

A Düşman veya Aldatıcı Topluluklarla Çalışmak

B Büyük Veri ya da Platform Verileriyle Çalışmak

C Öğrenci ve Doktora Sonrası Araştırmacı Danışmanlığı

D Hukuki Destek

E Travmatik İçeriklerle Çalışmak

F Riskli Materyallere Erişim

G Verilerin Korunması

H Hibe Başvuruları

I Gizlilik Sertifikaları

J Saha Çalışması

K Özel İletişim Kanalları

L Araştırmanın Yayınlanması ve Yaygınlaştırılması

M Arkadaşlar, Aile ve Yakın Çevre

5. Risk Azaltma Odaklı Araştırma Tasarımı

Araştırmacılar ve bağlı oldukları kurumlar, araştırmanın planlama ve tasarım aşamasında aşağıdaki ön adımları izleyerek, hem araştırmacıların hem de katılımcıların karşılaşabileceği riskleri en aza indirme ya da etkilerini hafifletme noktasında başarı sağlayabilirler.

Bir araştırma projesi tasarlanırken, araştırmacıların aşağıdaki hususları dikkate alması önerilmektedir:

- Düşmanca tutum sergileyebilecek topluluklarla çalışılıp çalışılmayacağı
- Öğrenciler, doktora sonrası araştırmacılar ve idari ve teknik personelin korunması adına neler yapılacağı
- Çalışmaya travmatik içeriklerin dahil edilip edilmeyeceği
- Veri koruma stratejileri geliştirilip geliştirilmeyeceği
- Fiziksel olarak güvensiz koşullarda saha çalışmaları yapılıp yapılmayacağı

Bu ve benzeri unsurlar üzerine düşünmek, araştırmanın güvenliği ve etik bütünlüğü açısından kritik derecede önem arz etmektedir.

A. Düşman ya da Yanıltıcı Topluluklarla Çalışmak

Bazı araştırma türleri doğası gereği araştırmaya, akademiye ya da kurumlara karşı düşmanca tutum sergileyen gruplarla çalışmayı gerektirmektedir. Geleneksel etik yaklaşımlar, araştırma katılımcılarını araştırmacıya göre daha kırılgan görmüş ve bu doğrultuda katılımcı bireylerin korunmasına öncelik vermiştir. Ancak Adrienne Massanari'nin (2018) de belirttiği gibi, aşırı sağ benzeri gruplar, araştırmayı yürüten kişiye somut zararlar verebilme ihtimalleri nedeniyle bu denklemi karmaşıklaştırmaktadır. Örnek bir durum üzerinden konuşmak gerekirse, araştırmacıların çalışmalarını gizlice yürütmeleri ya da katılımcılarına yanıltıcı bilgi vermeleri tavsiye edilmese de, taciz ya da kişisel bilgi sızdırılması riskinden korunmak için bu tür yöntemlere ihtiyaç duyulabilmektedir (Bireyin rızası olmaksızın ev adresi, telefon numarası, kredi kartı bilgileri, doğum tarihi hatta ulusal kimlik numarası gibi kişisel tanımlayıcı bilgilerinin ifşa edilmesi gibi durumlar Bölüm 7'de ayrıntılarıyla ele alınmaktadır).

Araştırmacıların, yüz yüze görüşmelerden ya da katılımcı gözlem gibi etnografik yöntemlerden kaçınarak bunun yerine dijital etnografi, söylem analizi ya da masa başı araştırmayı tercih ettikleri durumlar vardır. Dezenformasyon ve propaganda gibi konular üzerine çalışan araştırmacılar, yanıltıcı ya da manipülatif davranışlarla karşılaşabilmekte ya da çalışmalarını susturma girişimleriyle yüzleşmek zorunda kalabilmektedir. Emma Briant (2024), akademik araştırmacıların güçlü aktörlerle röportaj yaparken karşılaştıkları etik ikilemlerin gazetecilerin durumuna benzemediğini, dolayısıyla da tezatlığın araştırmacılar açısından bir risk unsuru teşkil ettiğini belirtmektedir. Yanıltıcı ya da asimetrik bilgi üretimine meyilli aktör ve endüstriler üzerine çalışan araştırmacılar için riskler fazladır ve ABD dışındaki yasal bağlamlarda daha büyük sorunlara evrilme ihtimaline sahiptir (Briant, 2024: 386–387).

Düşmanlık sergileyen gruplara yönelik geleneksel insan denekleriyle araştırma yapmayı tercih eden araştırmacılar söz konusu olduğunda, farklı değer ve görüşlere sahip ya da doğrudan karşıt fikirler benimseyen bireylerle güven ilişkisi kurmak zordur. (Segers vd., 2024). Araştırmacının maruz kaldığı risk, cinsiyetçi, ırkçı, homofobik vb. tutumlara sahip gruplarla çalışıldığında daha da artmaktadır. Örneğin bir çalışma, aşırı sağ grupların, daha az tehdit edici gördükleri kadın

araştırmacılarla daha kolay iletişime geçme eğilimi gösterdiklerini bulgulamıştır (Gelashvili & Gagnon, 2024). Eğer araştırmacı, bu tür gruplarla doğrudan temas kuracaksa, yöntemsel açıdan son derece dikkatli olması ve stratejik bir planlama yapması gerekmektedir. Bu rehberin sonunda yer alan **"Ek Okuma"** bölümünde, bu alana yönelik akademik kaynaklar listelenmiştir.

B. Büyük Veri ya da Platform Verileriyle Çalışmak

Büyük veri kümeleriyle, teknoloji şirketlerinden elde edilen verilerle ya da sosyal medya platformlarının verileriyle çalışan araştırmacılar, kendilerine özgü bir dizi riskle karşı karşıyadır. Son yıllarda teknoloji şirketleri, araştırmacılara karşı yasalar aracılığıyla tehditlerde bulunarak—örneğin ihtar mektupları göndererek ya da doğrudan dava açarak—bu tür çalışmaları engelleme yoluna gitmektedir. Şirketlerin sahip oldukları yüksek mali kaynaklar ve güçlü hukuk ekipleri, titizlikle tasarlanmış projeleri bile sona erdirebilmektedir. Bu bölümün ilerleyen kısımlarında, sözü edilen yöntemleri değerlendiren araştırmacılar için, görece uygun maliyetli hukuki danışmanlık sağlama yolları da dahil bazı çözüm önerileri sunmaktayız.

Platformlar ve internet siteleri, içeriden bağlantıya geçilmediği ve/veya yeterli maddi kaynaklar sunulmadığı takdirde büyük veri setlerine erişimi zorlaştırmış olsa da, akademisyenler bu durumlarda "etik istemci taraflı" veri toplama yöntemlerinin kullanılmasını önermektedir (Halavais, 2019). Bilgilendirilmiş onam eşliğinde ilerlemeyi gerektiren bu yaklaşım, verinin asıl üreticileri olan kullanıcılarla ortaklık kurulmasına olanak tanıyarak güç dengesinin hükümetler ve büyük şirketler aleyhine, kullanıcılar lehine kaydırılmasını mümkün kılacaktır.

Öte yandan, ilgili bazı hükümlerinin 2025 yılında yürürlüğe girmesi planlanan **Avrupa Birliği Dijital Hizmetler Yasası (DSA)**, onaylı araştırmacılar için platform verilerine zorunlu erişim hakkı getirmektedir. Ancak bu düzenlemenin nasıl uygulanacağı, araştırmacıların veriye nasıl erişeceği gibi konular henüz netlik kazanmış değildir (Avrupa Komisyonu, 2024).

C. Öğrenci ve Doktora Sonrası Araştırmacı Danışmanlığı

Riskli konular üzerine lisans, yüksek lisans, doktora ya da doktora sonrası araştırmacılarla birlikte çalışma yürüten araştırmacılar, özel önlemler almak durumundadır. Mümkünse, nefret söylemi, şiddet ya da aşırı sağ gibi alanlarda daha önce deneyim sahibi olan ilgili ve bilgili öğrencilerle çalışılması önerilmektedir. Proje yürütücüleri, öğrencilerle muhtemel riskler konusunda açık ve dürüst bir iletişim kurmalı, üniversitenin sunduğu konu ile alakalı kaynaklar (psikolojik danışmanlık, kampüs güvenliği, öğrenciyi koruma politikaları vb.) hakkında bilgi vermelidir. Öğrencilerin ve doktora sonrası araştırmacıların, gerekli durumlarda projeye ara vermeleri ya da daha az riskli konulara geçiş yapabilmeleri veyahut da fon desteği erişimine devam etmeleri garanti altına alınmalıdır.

Benzer şekilde, bir laboratuvar ortamında araştırma grubuyla çalışan proje yürütücüleri, öğrencilere kendi deneyimlerini paylaşabilecekleri destek grupları oluşturmalı ve onları benzer alanda çalışan akademik ağlarla (e-posta listeleri, mesleki dernekler vb.) tanıştırmalıdır. Bazı kurumlar, bir terapist eşliğinde aylık klinik gözetim fırsatları sunabilmektedir. Bu uygulama daha çok psikiyatri ve sosyal hizmet alanlarında yaygın olmakla birlikte diğer alanlarda da araştırma bütçelerine dâhil edilmektedir.

En azından, yüksek riskli ya da travmatik konularda çalışan veya bulundukları konum nedeniyle daha yüksek düzeyde duygusal zorlanma riski taşıyan yüksek lisans/doktora öğrencisi

danışmanlarının, **"psikolojik ilk yardım"** eğitimi alması teşvik edilmelidir. Uygun ve gerekli görülen durumlarda, danışmanlar ve öğrencileri, araştırma sürecinde elde edilen verilerin araştırmacıda duygusal zorlanmaya yol açması halinde uygulanmak üzere bir "zorlanma protokolü" oluşturmayı değerlendirebilirler. Bu protokol, duygusal zorlanma ya da dolaylı travmanın (Moran & Asquith, 2020) erken belirtilerini tanımlamalı ve bu tür durumların etkisini azaltmak veya uygun şekilde müdahale etmek için stratejiler içermelidir. Danışmanla ve/veya bir terapistle düzenli değerlendirme görüşmeleri yapmak, öz-düşünüm günlükleri tutmak gibi yaratıcı seçeneklerin yanı sıra araştırmacının geçici olarak üstlenebileceği alternatif görevleri belirlemek bahsi geçen stratejilere örnek teşkil etmektedir. Danışmanlar, bireysel araştırmacıların—özellikle ruh sağlığı sorunları ve/veya intihar eğilimi geçmişi olanların—başkalarıyla paylaşabilecekleri kişisel bir güvenlik planı oluşturmalarını teşvik etmelidir.

Proje yürütücüleri, yerinde uygulama örneklerine ön ayak olabilirler. Örneğin, riskli araştırmalar yürüten akademik kariyerinin başındaki araştırmacılara, kişisel telefonlarını veya dizüstü bilgisayarlarını kullanmamaları ve araştırma için ayrı bir e-posta adresi oluşturmaları önerilmelidir (birçok üniversite, e-posta hesaplarına birden fazla "takma ad" eklenmesine olanak tanımaktadır). Ortak çalışmaların yayınlanması söz konusu olduğunda ise, araştırmanın yürütücüleri öğrencilere kendi isimlerini kullanıp kullanmama konusunda tercih hakkı tanımalıdır. İsme dayalı yayın yapmak, kariyerlerinin başındaki araştırmacılar için önemlidir; ancak bu durum aynı zamanda potansiyel riskler de barındırmaktadır. Bu nedenle öğretim üyeleri, öğrencilerle bu kararın artılarını ve eksilerini açıkça anlatmalı ve onların bilinçli bir tercih yapmalarını sağlamalıdır. Eğer öğrenciler, adlarının riskli araştırma projeleriyle ilişkilendirilmesini istemezlerse, öğrenci adlarının proje kapsamında kamuya açık içeriklerden çıkarılması ya da sonradan değiştirilebilecek kalıcı takma adlar kullanılması değerlendirilmelidir.

Son olarak, bazı araştırmacılar, aşırı görüşlere maruz kalmanın veya bu görüşlerle yoğun biçimde çalışmanın araştırmacının zamanla bu görüşleri benimsemesine yol açabileceğinden ("radikalleşme") endişe duymaktadır. Ancak, bu durumun gerçekten yaşandığına dair ne bir ampirik kanıt ne de herhangi bir anekdot bilgi bulunmaktadır. Aksine, aşırı sağ görüşleri benimseyen araştırmacıların çoğu durumda, araştırmaya başlamadan önce zaten bu tür görüşlere eğilim gösterdikleri görülmektedir. Bizim bulgularımıza göre, öğrencilerin aşırı uç içeriklere maruz kalmaları sonucunda ikincil travma yaşama riski artmaya başlamaktadır. Bu nedenle, bu tür içeriklerle çalışan öğrencileri denetleyen araştırmacıların bu riskin farkında olmaları ve gerekli önleyici tedbirleri almaları son derece önemlidir.

Kadrolu ya da güvenceli iş pozisyonunda çalışan araştırmacıların, sahip oldukları konum ve ayrıcalıklar itibariyle bölümler ve kurumlar nezdinde öğrencilerinin güvenliği ve haklarına yönelik daha fazla sorumluluk almaları gerekmektedir. Söz konusu sorumluklar arasında, öğrencilere siber güvenlik konusunda en iyi uygulamalara dair eğitim vermeyi, öğrencilerin başka projelerde çalışmasını onaylamayı, risk düzeyi yüksek projelerde çalışma zorunluluğunu kaldırmayı, medya talepleri ve kamuya açık tartışmalarla ilgili sorumluluk üstlenmeyi ya da öğrencilerin riskli araştırmaların etkilerini daha yoğun hissettikleri dönemlerde devreye sokulacak iletişim temelli bir güvenlik planı oluşturmayı saymak mümkündür. Eğer olumsuz ve istenmeyen durumlar ortaya çıkacak olursa, proje sorumluları, öğrencilerinin hak ve ihtiyaçlarını üniversiteye karşı savunmalı ve uygun destek kaynaklarını bulmaları konusunda onlara yardımcı olmalıdır.

D. Hukuki Destek

Eğer araştırmanın yöntemleri bir platformun hizmet şartlarını ihlal ediyorsa, araştırmacılar üniversitelerinin ya da yakında bulunan diğer kurumların sunduğu ücretsiz hukuk büroları hakkında bilgi edinmelidirler. Farklı ülkeler farklı hukuki çerçevelere sahiptir. Bu nedenle araştırmacılar, yürüttükleri çalışmanın doğurabileceği olası hukuki sonuçlarla ilgili gerekli ayrımların farkında olmalıdır. İlgili hukuk büroları, araştırmanın kamu yararına etkileri doğrultusunda özel olarak uyarlanmış hukuki danışmanlık hizmeti sunabilmektedir.

ABD örneğinde, Harvard Üniversitesi'nin Siber Hukuk Birimi öğrencilere ücretsiz danışmanlık sağlamaktadır. Benzer şekilde Tufts Üniversitesi'nin Siber Güvenlik Birimi de kar amacı gütmeyen sivil toplum kuruluşlarına ücretsiz destek sunmaktadır. Ayrıca, birçok ABD üniversitesi, lisansüstü öğrencilerinin genel hukuki danışmanlık hizmeti (örneğin sözleşme inceleme, ihtar mektuplarına yanıt) içeren düşük ücretli hukuksal koruma sigortası edinmelerine imkân tanımaktadır. Buralardaki hukuk çalışanları her ne kadar internet ya da platform araştırmaları konusunda uzmanlaşmışlarsa da sözleşme incelemeleri ve "ihtarname" (cease-and-desist) yazılarına yanıt verilmesi gibi konularda destek sağlayabilme yetkinliğine sahiptirler. Yine de üniversite hukuk ofisinin öncelikli olarak üniversitenin çıkarlarını koruduğunu unutmamak elzemdir ve buna bağlı olarak da söz konusu hizmetlerinde ihtiyatlı davranacakları ve temkinli tavsiyeler verebilecekleri hesaba katılmalıdır. Örneğin, dava riskiyle karşılaşmamak adına, bir yüksek lisans öğrencisine ihtiyati bir önlem kapsamında ilgili konuda tüm araştırma faaliyetlerini durdurması söylenebilir — bu yaklaşım, olası hukuki riskleri düşük maliyetle bertaraf etmenin kestirme bir yolu olarak değerlendirilmektedir. Daha fazla bilgi için bkz. Bölüm 8.

E. Travmatik İçeriklerle Çalışmak

Riskli araştırmalar yürüten akademisyenler, çatışma bölgelerine doğrudan maruz kalma, insanlık suçlarına ilişkin kanıtlarla karşılaşma ya da savaş bölgesinden gelen tanıklıklarla ilgili grafik görüntü ve videolar izleme gibi travmatik içeriklerle çalışmayı gerektiren durumlarla karşı karşıya kalabilmektedir. Pek çok araştırmacı, rahatsız edici medya içerikleriyle bir ofis ortamında veya saha dışı bir mekânda çalışmanın — tekrarlayan maruz kalma nedeniyle — sahada çalışmak kadar travmatik olabileceğinin farkında değildir (Eyewitness Media Hub, 2015). "Araştırma kaynaklı travma" olarak adlandırılan bu durum, ruh hali değişimleri, depresyon, kişilerarası ilişkilerde bozukluk, baş ağrısı, mide bulantısı ve göğüs ağrısı gibi fiziksel ve psikolojik semptomlarla kendini gösterebilmektedir (Loyle ve Simoni, 2017). Ancak tüm bu risklere rağmen, akademik kurumlar genellikle bu tür çalışmaların araştırmacılar üzerinde yaratabileceği uzun vadeli etkileri tanımamakta ya da bu etkilerle yeterince ilgi göstermemektedir.

Travmatik materyaller içeren bir projeye başlamadan önce, araştırmacıların kendi risk faktörlerini değerlendirmesi ve sonrasında da bunları akademik toplulukları arasında veya sosyal ağlarıyla müzakere etmeleri gerekmektedir. Veri toplama sürecinde, örneğin rahatsız edici içeriklere akşam saatlerinde maruz kalmaktan kaçınmak gibi kişisel sınırlar belirlenmeli ve düşünme ile tartışma için zaman ayrılmalıdır. Travmatik medya içerikleriyle çalışırken sesi kısmak ya da tamamen kapatmak, video izlemeye aralıklı devam etmek ve düzenli molalar vermek gibi stratejiler, duygusal zorlanmayı yönetmeye yardımcı olabilmektedir. Araştırmacılar ayrıca, kendilerini en fazla etkileyen içerik türlerini belirlemeli ve bu materyallerle nasıl başa çıkacaklarına dair—örneğin meslektaşları ya da araştırma yürütücülerini bilgilendirmek gibi—bir plan geliştirmelidirler. Hassas içerikleri başkalarıyla

paylaşırken, potansiyel zararları en aza indirmek amacıyla "içerik uyarısı" verilmesi etik bir zorunluluktur. Danışmanlar ya da araştırma yürütücüleri, sürdürülebilir bir çalışma temposu ayarlamak, zararlı içeriklere maruz kalma durumunda ara vermek ve çalışmanın duygusal zorluklarını açıkça kabul etmek gibi sağlıklı çalışma pratikleri geliştirmeye yönelik örnek davranışlar sergilemelidirler.

F. Riskli Materyallere Erişim

Cinsel açıdan uygunsuz içeriklerle, nefret söylemi örnekleriyle ya da aşırılık yanlısı medya ortamlarıyla muhatap olarak çalışma yürütmenin travmatik etkileri yanı sıra bazı pratik sonuçları da bulunmaktadır. Örneğin, bazı ülkelerde terör örgütlerine ait medya içeriklerine erişmek yasal olarak suç teşkil etmektedir. Araştırmacılar, şiddet tehditleri ya da çocuklara yönelik cinsel içerikli görseller gibi yasa dışı ya da zararlı materyallerle karşılaştıklarında bunu bildirip bildirmeyeceklerini ve bildirirlerse bu bildirimi kime ya da nereye yapmaları gerektiğini önceden değerlendirmelidir. Sosyal medya platformlarında içerik bildiriminde bulunmak, araştırmacılar açısından risk faktörü düşük bir edimdir. Bu noktada terörizm üzerine çalışan araştırmacılara yönelik bir çalışmadan çıkan sonuçlara göre, araştırmacıların %42'si "tehlikeli aktörleri ya da hizmet koşullarının ihlallerini" sosyal medya platformlarına bildirdiklerini belirtmişlerdir (Khalil, 2021).

Ancak, bu tür içerikleri marjinal internet sitelerinde, özel sohbet kanallarında ya da çevrim içi arşivlerde tespit etmek ve kolluk kuvvetlerine bildirmek çok daha karmaşık ve riskli hale gelmektedir. ABD veya Birleşik Krallık'ta araştırmacıların yasa dışı içerikleri bildirme yönünde yasal bir yükümlülüğü bulunmamakla birlikte (McLoughlin, 2021; O'Connell, 2010), konuyla alakalı etik bir sorumluluktan söz etmek mümkündür.

Araştırma projesi planlanırken, araştırmacılar aşağıdaki soruları önceden değerlendirmelidir:

- İçerik bildiriminde bulunmaya zihinsel, duygusal ve pratik olarak hazır mısınız?
- İçeriği kime bildireceğinizi biliyor musunuz?
- Bildirip bildirmeme kararını neye göre vereceksiniz?
- İçerik açık ya da ayrıntılı bir tehdit içeriyor mu? Örneğin, belirli bir yer, zaman ve yöntem belirtiliyor mu?
- Tehdit belirli bir kişiyi mi hedef alıyor?
- İçerik, kişisel bilgileri içeriyor mu (örneğin "doxxing" gibi)?
- İçerik, çocukları ya da reşit olmayan bireyleri kapsıyor mu? Çocuklara yönelik cinsel istismar materyalleri, Amerika Birleşik Devletleri dışında olsanız bile **NCMEC'in (Ulusal Kayıp ve İstismara Uğramış Çocuklar Merkezi)** CyberTipline adlı sistemi üzerinden bildirilebilir. Avrupa Birliği, örneğin, çocuklara yönelik cinsel istismar materyalleri tespitinde NCMEC bildirimlerine dayanmaktadır.

Bazı çevrim içi topluluklar—örneğin aşırı sağ mesaj panoları—platformlarına erişen kişilerin IP adreslerini izlediklerini iddia etmektedir. Aşırılık yanlısı çevrim içi alanlara erişirken, araştırmacıların her zaman sanal özel ağ (VPN) kullanan temiz bir tarayıcı üzerinden erişim sağlamaları ve siteye çevrimiçi yeniden bağlanmaktan kaçınmak için ilgili sayfaları PDF formatında kaydetmeleri önerilmektedir. Ayrıca, riskli materyallere üniversiteye ait bilgisayarlardan erişim sağlamak genel olarak tavsiye edilmemektedir.

G. Verilerin Korunması

Riskli konulara odaklanan projelerde, veri koruma stratejileri araştırmanın planlama aşamasında ele alınmalıdır. Bazı üniversiteler ya da fon sağlayıcı kurumlar, proje başlamadan önce risk değerlendirmesi yapılmasını veya veri yönetim planı hazırlanmasını zorunlu kılabilmektedir. Bu tür belgeler, güvenlik önlemlerinin ayrıntılı bir şekilde değerlendirilmesini sağlamaktadır. Etik kurullar ya da insan araştırmaları değerlendirme komiteleri de çoğunlukla katılımcı güvenliğine dair önlemler talep ederler ki bu da dolaylı olarak araştırmacının güvenliğini desteklemeye yönelik bir önlem niyetiyledir.

Riskli konuları içeren projelerde genellikle katılımcılar anonimleştirilmelidir. Örneğin, küçük topluluklara yönelik çalışmalarda, görüşme metinlerinin doğrudan alıntılanması yerine yeniden ifade edilmesi, dil özelliklerinden tanınma riskini bertaraf etme açısından önemlidir. Özellikle hassas gruplarla çalışıldığında kişisel verilerin toplanmasından mümkün olduğunca kaçınılmalıdır. Ancak konum itibariyle mevki sahibi kişiler (örneğin karar vericiler, şirket yöneticileri vb.) araştırılırken isim vererek sorumluluk atfetmek gerekli bir adım şeklinde yorumlanabilmektedir ("utandırma ve ifşa etme" stratejisi).

Hem araştırmacı verisini hem de katılımcı kimliğini korumak adına, araştırmacıların bağlı oldukları kurumun ya da bulundukları yerin veri depolama düzenlemelerine dikkatle uymaları gerekmektedir. Bazı araştırmacılar, bulut depolama sistemleri yerine birden fazla şifrelenmiş ve yedeklenmiş fiziksel bellek araçlarını kullanmayı tercih etmektedir. Mümkün olduğunda, e-posta veya dijital kayıtlar yerine fiziksel not defterleri, el yazısı günlükler ya da yüz yüze iletişim türleri gibi yöntemlerin kullanılması veri güvenliğini artıracaktır. Tüm fiziksel kayıtlar, yalnızca araştırmacının erişebileceği şekilde kilitli ve güvenli bir alanda muhafaza edilmelidir.

Araştırmacı güvenliği açısından veri koruma, özellikle devlet kurumlarının araştırma materyallerini mahkeme celbiyle talep ettiği vakalar göz önüne alındığında, son derece kritik bir unsurdur. "Dava ve Mahkeme Celbi Süreçlerinin Yönetimi" başlığı altında daha ayrıntılı ele alındığı üzere, hassas kişisel verilerin toplanmasını sınırlandırmak ve uygun şekilde kimliksizleştirme süreçlerine tabi tutmak, ileride ortaya çıkabilecek hukuki ve etik riskleri azaltmaya yardımcı olabilmektedir.

H. Hibe Başvuruları

Hibe başvuruları yazılırken risk azaltma stratejileri göz önünde bulundurulmalıdır. Araştırmacılar, araştırmacı güvenliğini artırmaya yönelik bütçe kalemlerini—araştırma personeli ve proje yürütücüleri için eğitim, bilgi güvenliği ve depolama, şifreli cihazlar, gizli deşifre hizmetleri, terapi veya danışmanlık ve/veya gelişmiş güvenlik protokolleri gibi—dâhil etmelidir. Dünya çapındaki üniversiteler birçok tehditle karşı karşıyayken, araştırma verilerinin güvenliği meselesi önemli bir endişe kaynağı hâline gelmiş durumdadır. Bu şartlar altında araştırmacıların, üniversite altyapısının ötesinde güvenli bilgi depolama çözümlerine erişmesi gerekebileceğinden bu ihtiyaç da bütçelemeye dahil edilmelidir.

I. Gizlilik Sertifikaları

Not: Bu bölüm, Amerika Birleşik Devletleri'ndeki araştırmalar için geçerlidir.

ABD bağlamında gizlilik sertifikaları, hassas araştırma ayrıntılarının katılımcının rızası olmadıkça ya da birkaç istisnai durum haricinde, araştırmayla bağlantısı olmayan kişilere

ifşasını yasaklamaktadır. Araştırma katılımcılarının mahremiyetini korumak üzere bir kalkan görevi gören bu sertifikalar, kongre tarafından çıkarılan yasalarla geçerlik kazanmaktadır. Gizlilik sertifikaları, "potansiyel olarak tanımlanabilir verilerin—davalar ve mahkeme celpleri dâhil—ifşasına karşı koruyucu" işlevi görmektedir (Research Support Consortium). Bu anlamda yürütülen bir çalışma, araştırma verilerine ilişkin hukuki taleplerin çoğunun katılımcı bilgileri açıklanmaksızın çözümlendiğini ortaya koymuştur (Wolf ve diğ., 2012).

Ulusal Sağlık Enstitüleri (NIH) ve Sağlık ve Sosyal Hizmetler Bakanlığı (HHS) gibi bazı hibe sağlayıcı kurum ve kuruluşlar, yetki alanlarındaki çalışmalara otomatik olarak gizlilik sertifikası vermektedir. Bir araştırma projesi tasarlanırken, araştırmacılar projelerinin gizlilik sertifikası gerektirip gerektirmediğini dikkate almalıdır. Ayrıca proje için otomatik olarak sertifika verilip verilmeyeceğini ya da araştırma başlamadan önce başvuru yapmalarının gerekip gerekmediğini kontrol etmeleri yerinde olacaktır. Ulusal Sağlık Enstitüleri ile ilişiği bulunmayan araştırmacılar, çevrim içi bir sistem aracılığıyla gizlilik sertifikası başvurusu yapabilmektedirler.

J. Saha Çalışması

Bazı araştırma projeleri, riskli bir sahada—örneğin aşırı sağ katılımcılarla veya otoriter ülkelerde—saha çalışması gerektirebilmektedir. Aşağıdaki öneriler, bu tür saha çalışmasını yürüten araştırmacılar için hazırlanmıştır.

- **Riskli Seyahat Noktalarının Belirlenmesi**

Yurt dışında saha çalışması yapmayı planlayan araştırmacılar, kendi ülkelerinin seyahat edilmemesi tavsiye edilen yerler listesi yayınlayıp yayınlamadığını kontrol etmelidirler. Örneğin Birleşik Krallık Dışişleri, Milletler Topluluğu ve Kalkınma Ofisi seyahat uyarılarını, güvenlik ve emniyet bilgilerini ve sağlık risklerini içeren bir "yurtdışı seyahat tavsiyesi" listesi tutmaktadır. Kişinin kendi ülkesinin ziyaret edilmemesini tavsiye ettiği bir ülkede saha çalışması yürütmek karmaşık durumların ortaya çıkmasına sebep olabilmektedir. Araştırmacının bağlı bulunduğu üniversite bu tür bir seyahati yasaklayabilmekte ya da en azından üniversite yöneticilerinden onay alınmasını şart koşabilmektedir. Bir başka durumda üniversite seyahati onaylasa bile, araştırmacı üniversite ya da genel sigorta kapsamı dışında kalabilmektedir.

- **Belirli Kilit İsimleri Bilgilendirme**

Saha çalışmasına başlamadan önce araştırmacılar, riskli araştırmaları hakkında bilgilendirilecek "kilit isimlerin" bir listesini hazırlamalıdır. Listeye yazılacak kişi isimleri, ulusal ve kurumsal bağlama göre farklılık gösterecektir.

Amerika Birleşik Devletleri'nde araştırmacıların, Bilgi Teknolojileri Direktörü ile Kampüs Güvenlik Birimini saha çalışmalarının yeri ve potansiyel riskleri konusunda bilgilendirmesi gerekmektedir. Lisansüstü öğrenciler ayrıca danışmanlarını, proje yöneticilerini veya kıdemli meslektaşlarını haberdar etmelidirler. Yine mümkünse, araştırmacı sahada yaşadığı herhangi bir olumsuzluğu kurumlarına ve danışmanlarına bildirme yoluna girmelidir. Saha çalışması sırasında ortaya çıkan rahatsızlıkları veya endişeleri kurum ve danışmanlarla paylaşmak, araştırmaya gömülmüşken ve katılımcılarla güven inşa ederken fark edilmesi güç risklerin tanımlanmasına yardımcı olacaktır. (Araştırmanız platformun Hizmet Koşullarını veya Bilgisayar Dolandırıcılığı ve Suistimali Yasasını ihlal etme gerekçesiyle yasadışı

addedilebilecekse, kurum içinde daha temkinli davranmak gerekebilir. Böyle durumlarda deneyimli bir mentörden konuyla ilgili tavsiye alınmalıdır.)

Avrupa'da lisansüstü araştırmacılar saha çalışması planlarken genellikle ilk önce danışmanlarına başvurmaktadır. Danışmanlarıyla potansiyel riskleri tartışmaları ve danışmanlarının araştırma süresince sürekli iletişime açık olup olmadığını teyit etmeleri gerekmektedir. Buna ek olarak araştırmacılardan, üniversitelerinin güvenlik hizmetlerini, etik kurulunu ve varsa araştırma güvenliği komitesini bilgilendirmeleri beklenmektedir. Bu komiteler, araştırmacının seyahat planlarını belgelemekte ve gerekli rehberlik desteği sunmaktadır.

Araştırmacıların ayrıca saha çalışmasının yapılacağı yerde, tercihen yerel dili/dilleri ve gelenekleri bilen güvenilir bir kişi bulundurması gerekmektedir. Bu tür durumlarda önleyici tedbirlere öncelik vermek esastır. Alışılmadık veya endişe verici gelişmeler olursa araştırmacılar destek ağlarını haberdar etmekte tereddüt etmemelidir.

Resmî ve gayri resmî destek ağları, riskli ya da travmatize edici olabilecek saha çalışmaları yürüten araştırmacılar için hayati önemdedir (Schultz ve ark., 2023). Araştırmacılar bu tür ağları, kartopu yöntemiyle, sosyal medya aracılığıyla, konferans e-posta listeleriyle ya da alandaki diğer araştırmacılara e-posta atarak kurabilirler. Saha çalışmasına başlamadan önce bu toplulukların oluşturulması, araştırmacının sahada bir destek sistemine güvenebilmesini sağlayacaktır. Saha çalışması sırasında deneyimli araştırmacılarla mesajlaşmanın, görüntülü arayabilmenin veya diğer sanal iletişim yollarıyla sürekli bağlantıda kalmanın, istikrarı ve güven hissini arttırıcı etkileri vardır (Schultz ve ark., 2023).

- **Yalnız Yürütülen Saha Çalışmalarında Riski En Aza İndirmek:**

Araştırmacılar, tek başlarına saha çalışması yürütmek zorunda kaldıkları son derece rahatsız edici ve tehlikeli durumlarla karşı karşıya kalabilmektedir.

Riskleri en aza indirmek için araştırmacıların aşağıdaki stratejileri göz önünde bulundurmaları gerekmektedir (Demery & Pipkin, 2020):

- Potansiyel riskler konusunda meslektaşlar ve danışmanlar ile konuşun ve hazırlıklarınızı buna göre yapın.
- Uluslararası yasalara, yerel yasalara ve geleneklere aşina olun ve bunlara uygun davranmaya özen gösterin.
- Yüksek riskli bölgelerde saha çalışması yürütme konusunda deneyimi olan diğer araştırmacılarla bağlantı kurun.
- Kendini savunma eğitimi, ilk yardım kursları veya alanın kültürel tarihi hakkında eğitim gibi saha güvenliğini artıracak imkanlar varsa yararlanın.
- İrtibat noktası olarak saha yöneticileriyle düzenli iletişimde olun; planlar ve bulunulacak yerler hakkında onları bilgilendirin.
- Kimlik, ilgili izinler ve üniversite veya kurumsal bağlantıyı kanıtlayan belgeler dâhil olmak üzere uygun yetki belgelerini her zaman yanınızda bulundurun.

Bu yapılandırılmış yaklaşım, araştırmacıların tek başına saha çalışmasının zorluklarını gerekli güvenlik tedbirlerini alarak ve özgüvenli bir şekilde aşmalarına yardımcı olacaktır.

- **Saha Çalışmasında Risk Belgeleme**

Bir araştırmacı kendisini risk altında hissettiğinde, durumu ayrıntılı biçimde belgelemek son derece önemlidir. Bu süreç bunaltıcı ya da duygusal açıdan yorucu geliyorsa, bir arkadaşınızdan ya da güvendiğiniz bir meslektaşınızdan destek alabilir veya onlarla iletişime geçebilirsiniz. Risk ve algılanan tehditler tehlike arz etmekle birlikte değerli veriler sağlayabilme potansiyeline de sahiptir. Ancak, belgelemenin güvenliği, bağlam bağımlı olarak değişkenlik göstereceği için araştırmacıların ilgili ayrıntıların kaydını tutmadan ek riskler oluşturup oluşturmayacağına göre değerlendirmeleri gerekmektedir.

Araştırmacılar hızlı bir risk değerlendirmesi yapmak adına kendilerine şu soruları sormalıdır:

- Kişisel ve dijital alanıma izinsiz erişim olasılığı söz konusu mu?
- Bana risk oluşturan, eşyalarımı ya da dosyalarımı karıştırabilecek kişiler var mı?
- Belirli bir risk tespit edersem, tehdidi kimin oluşturduğunu ve amaçlarının ne olduğunu biliyor muyum?

Araştırmacı yukarıdaki sorulara **"evet"** yanıtını veriyorsa, tehditleri belgelemenin daha büyük risk taşıyabileceğini ve daha fazla özen göstermek gerekeceğini göz önünde bulundurmalıdır. Bu durumda, güvendiği bir kişinin dosyaları güvenli bir şekilde saklayıp saklayamayacağını değerlendirmesi iyi olacaktır. Mümkünse, belgelemenin kopyaları bu kişiye gönderilebilir ve ardından araştırmacının cihazlarından ve çalışma alanından silinerek yetkisiz erişim engellenebilir. Alternatif olarak, araştırmacı fiziksel belgeleri—posta hizmetine güveniyorsa—kendi adresine göndererek hassas materyalleri bulunduğu ortamdan uzaklaştırma yoluna gidebilir.

Araştırmacı bu sorulara **"hayır"** yanıtını veriyorsa, deneyimlerini fiziksel bir not defterine kaydetmeli ve bu defteri üzerinde taşımalı ya da güvenli bir yerde saklamalıdır. Notların riskli kişilerin eline geçebileceği ya da kaybolabileceği yerlerde bırakılmamasına özen gösterilmelidir. Yine araştırmacılar notlarının bir kopyasını almalı, yedeklemeli ve mümkünse bir parola ile koruma altına almalıdırlar.

K. Gizli/Özel İletişim Kanalları

Araştırmacılar, araştırma yürütürken veya meslektaşlarıyla görüşürken şifreli iletişim kanalları kullanmayı düşünmelidirler. Bu durum, özellikle araştırmacı bir kamu kurumunda çalışıyorsa ve bulunduğu yerde e-posta yazışmaları kamu bilgi edinme taleplerine tabi olabiliyorsa kritik bir önem taşımaktadır. Şifreleme ile koruma sağlanan beklemedeki verilere, casus yazılımlar aracılığıyla ya da bir telefon veya bilgisayara doğrudan müdahalelerle erişim sağlanabileceği akılda tutulmalıdır.

Aşağıda şifreli iletişim hizmeti sunan bazı örnekler yer almaktadır:

Hizmet	Açıklama
Proton Mail	Verilerin İsviçre gizlilik yasaları kapsamında korunduğu, ücretsiz ve güvenli bir e-posta hizmetidir.
Signal	Anlık mesajlaşma, sesli arama ve görüntülü arama için ücretsiz, açık kaynaklı ve uçtan uca şifrelemeli bir iletişim hizmetidir. Signal, meta-veri toplamaz ancak telefon numaralarını kaydetmektedir. Genel anlamda en güvenli uçtan uca şifreleme (E2EE) seçeneği olarak tavsiye edilir.
WhatsApp	Ücretsiz anlık mesajlaşma ve IP üzerinden ses hizmetidir. Varsayılan olarak uçtan uca şifreleme kullanmaktadır. Signal protokolüne dayanır, meta-veri toplar ve pazarlama ile kullanıcı profilleme amacıyla Meta ile veri paylaşır.
SecureDrop	Kendi protokolüne sahip, haber odaları ve kar amacı gütmeyen kuruluşlar tarafından ihbarcıların hassas belgeleri güvenli bir şekilde aktarması için kullanılan açık kaynaklı bir dosya gönderim sistemidir.
RiseUp	E-posta, posta listeleri, özel wikiler, gerçek zamanlı ortak metin düzenleyiciler ve dosya yükleme hizmetleri sunan ve işletmecileri gönüllülerden oluşan bir kuruluştur.
Jitsi Meet	Şifreli ve açık kaynaklı bir video konferans hizmetidir.

Kaçınılması Gereken Hizmetler

- **Facebook Messenger** ve **Instagram Direct**: Meta Platforms'un geliştirdiği ücretsiz anlık mesajlaşma servisleridir. Uçtan uca şifreleme sunmazlar ve Meta, bu verilere erişim sağlayabilmektedir.
- **Telegram**: Varsayılan olarak uçtan uca şifreleme kullanmaz.
- **X**: Özel mesajlar varsayılan olarak uçtan uca şifrelenmez; grup mesajları, fotoğraflar veya videolarda da uçtan uca şifreleme bulunmaz. Şifrelemenin kırılmasına imkân tanıyabilecek açıklar rapor edilmiştir.

L. Araştırmanın Yayımlanması ve Yaygınlaştırılması

Bir araştırmacı, riskli olduğunu düşündüğü bir çalışmayı yayımlamadan ya da kamuyla paylaşmadan önce güvendiği meslektaşları ve kurumlarla iletişim halinde olmalıdır. Görüşme sırasında, araştırmasından ötürü olası bir tepki beklediğini ve bu gerçekleşirse ilgili kişi ya da kurumların kendisini nasıl destekleyebileceğini planlamak istediğini söylemelidir. Örneğin, çevrim içi taciz durumunda bir arkadaşının e-posta iletilerini veya BlueSky mesajlarını okuyabilmesine yönelik gerekli izinleri verebilir ya da kendisini hedef alan düşmanca aktörler hakkında kampüs güvenliğini önceden bilgilendirebilirler.

Araştırmacılar, akademik kimliklerinin aileleri ve arkadaşlarıyla bağlantılandırılmasını engellemek amacıyla kalıcı bir takma ad ya da kimlikten farklı bir ön ad kullanarak yayın yapma seçeneğini değerlendirebilirler. Kalıcı takma ad, yazarın daima aynı adı kullanması bakımından "mâhlas" niteliği taşır, ancak yazarın yasal adından farklı bir kategoridedir. Tek başına farklı bir ön ad kullanmak bile, Li, Smith veya Garcia gibi yaygın soyadı durumlarında yazarın bulunmasını oldukça güçleştirebilmektedir.

Lisansüstü öğrenciler tez çalışmalarını erişime açmama hakkına sahiptir. Teze erişim izni verilmemesi, metnin kısıtlanması demektir. Bu durumda yalnızca başlık, özet ve atıf bilgileri açık ve görünür olacaktır. Asıl metin genellikle bir ila beş yıl boyunca erişime kapalı

tutulacaktır. Üniversiteler erişim izni kısıt süreleri ve ilgili diğer şartlar konusunda farklılık gösterebilmektedir. Bu nedenle araştırmacılar lisansüstü enstitüleri veya kurumsal arşiv birimleriyle yakın iletişimde olmak durumundadır. Tezleri riskli içerik barındırıyorsa erişim kısıtı koymak yerinde olacaktır; zira erişim engeli kalktığında araştırmacı, daha istikrarlı bir işe kavuşmuş veya araştırmayla bağlantılı riskler ortadan kalmış ya da azalmış olabilir. Amerika Birleşik Devletleri, Birleşik Krallık ve Avustralya'daki pek çok üniversite erişime kısıt konulmasını desteklerken, diğer bölgelerdeki öğrencilerin kendi üniversitelerinin politikalarını incelemesi uygun olacaktır.

Konferans davetlerini kabul ederken araştırmacılar, sunumlarının kaydedilip YouTube veya benzeri platformlarda yayınlanıp yayınlanmayacağını öğrenmelidirler. Çoğunlukla bu amaçla bir izin formu imzalanması istenir ancak, araştırmacılar bunu reddetme hakkına sahiptir. Konuşmacılar, konuşmalarının tanıtımında kendi fotoğraflarının kullanılmamasını, bunun yerine bir illüstrasyon ya da stok görsel tercih edilmesini de talep edebilirler.

Son yıllarda Amerika Birleşik Devletleri'nde, çoğunlukla muhafazakâr grupların Çeşitlilik, Eşitlik ve Kapsayıcılık (DEI) ya da LGBTQIA+ ile ilgili çalışmalar yürüten eleştirel bakış açısına sahip akademisyenleri hedef alan intihal suçlamalarında artış görülmektedir. Akademisyenler, önceki çalışmalarındaki küçük veya önemsiz hatalar—örneğin eksik kaynak gösterimi—öne sürülerek itibarsızlaştırılmaktadır. Eleştirmenler, eksik tırnak işaretleri, hatalı yeniden ifade biçimleri veya atıf eksikliği gibi sorunların tespiti için yapay zekâ araçlarını kullanmaktadır. Bazı durumlarda, öğretim üyeleri üretken yapay zekâ araçları yoluyla çalışma üretmekle suçlanmakta; ancak bu iddiaları doğrulamak için kullanılan yapay zekâ tespit araçları yüksek hata payı ile işlev görmektedir. Bu eğilimler, benzer tehditlerin diğer araştırmacılara da yöneltilebileceğine dair uyarı niteliğindedir. Dolayısıyla, özellikle Çeşitlilik, Eşitlik ve Kapsayıcılık (DEI) veya queer vatandaş haklarının meşruiyetini savunan alanlarda çalışan araştırmacıların, çalışmalarını yayınlarken ve paylaşırken son derece dikkatli davranmaları gerekmektedir.

M. Arkadaşlar, Aile ve Yakın Çevre

Araştırmacılar, çocukları, eşleri ya da ebeveynleri gibi bakmakla yükümlü oldukları kişilerin, kendileriyle olan bağları nedeniyle risk altında kalıp kalmayacağı hususunu mutlaka göz önünde bulundurmalıdırlar. Yakın akrabalar da olumsuz sonuçlarla karşılaşabileceğinden, çevrimiçi ortamda fotoğraf veya aile ilişkilerini ifşa eden bilgi gibi paylaşmanın doğurabileceği riskleri kendileriyle açıkça tartışmak önemlidir. Aileler veya arkadaş grupları, özel iletişimlerini Signal veya WhatsApp gibi uçtan uca şifreli uygulamalara taşıyarak gizliliklerini artırma yoluna gidebilirler. Ancak tüm yakın çevre, bu tür gizlilik önlemlerine aynı derecede sıcak bakmayabilmekte; bu da destek ağında bünyesinde gerilimlere yol açabilmektedir. Bu endişeler ışığında erken davranmak, olası zorlukları aşmayı ve riskler konusunda ortak bir anlayış geliştirmeyi kolaylaştıracaktır.

6. Siber Güvenlik ve Mahremiyet Risklerinin Azaltılması

A Veri Gizliliği ve Siber Güvenlik Uygulamaları

6. Siber Güvenlik ve Mahremiyet Risklerinin Azaltılması

Herhangi bir araştırmacı, ne kadar önlem alırlarsa alsın, yine de bazı risklere maruz kalmaya devam etmektedir. Bu nedenle, zarar gören birini—kendini korumak için daha fazlasını yapabilirdi düşüncesiyle—eleştirmek veya suçlamak doğru değildir. Bu bölüm, zararlı sonuçları en aza indirmeye yardımcı olmak amacıyla araştırmacıların araştırma sürecinin öncesinde alabilecekleri önlemleri ya da araştırma sırasında atabilecekleri adımları ve bu anlamda bilinen en iyi uygulama örneklerini özetlemektedir.

A. Veri Gizliliği ve Siber Güvenlik Uygulamaları

Bir araştırmacının taciz, doxing, takip veya şantaj riski altında olduğu durumlarda mahremiyeti korumaya yönelik alınabilecek çeşitli teknik önlemler mevcuttur. Temel siber güvenlik ve gizlilik uygulamalarını yerine getirmek, başlangıçtaki zafiyetlerin büyük kısmını giderebilmektedir. Bu nedenle, araştırmasını kamuya sunmadan *birkaç hafta önce* araştırmacının temel operasyonel güvenlik adımlarını atmasını önermekteyiz. Equality Labs'in *Anti-Doxing Guide for Activists* gibi kılavuzlar, çevrimiçi bilgileri koruma ve dijital cihazları daha güvenli hâle getirme konusunda ayrıntılı, adım-adım yapılacakları bildiren talimatlar sunmaktadır. Bu anlamda atılabilecek ilk adım, "öz-doxing" olarak da adlandırılabilecek bir pratik üzerinden hangi kişisel bilgilerin kimlere ve nerelere açık olacağını değerlendirmektir.

Bu anlamda ortaya çıkabilecek riskleri en aza indirmek için aşağıdaki adımları göz önünde bulundurunuz:

Çevrimiçi Ortamlarda Kişisel Bilgileri Araştırın

- Google'da isminizi aratın ve üniversite web sitelerinde listelenmiş ayrıntıları kontrol edin.
- Whitepages.com, Spokeo gibi veri toplayıcı sitelerde adresinizi aratın.
- Üniversitenin web sayfalarında ofis adresinizin veya ofis saatlerinizin yayınlanıp yayınlanmadığını kontrol edin.
- Telefon numaranızın özgeçmişinizde (CV) veya diğer açık belgelerde yer alıp almadığına bakın.

Sosyal Medyayı ve Takma Adları Gözden Geçirin

- Geçmişte veya hâlihazırda kullandığınız takma adların tam adınız ya da başka kimlik bilgileriyle ilişkilendirilip ilişkilendirilmediğini araştırın.
- LinkedIn, Facebook, Twitter/X ve benzeri platformlardaki profilleri inceleyerek arama sonuçlarında nelerin göründüğünü denetleyin.
- Aktif hesaplarınızın gizlilik ayarlarını yalnızca paylaşmaya razı olduğunuz bilgilerin görünür olduğundan emin olacak şekilde ayarlayın.

Eski ve Arşivlenmiş Hesapları Kontrol Edin

- MySpace veya Flickr gibi eski sitelerdeki pasif hesapları aratın.
- Internet Archive ve archive.today üzerinde arama yaparak kişisel bilgilerinizin hâlâ erişilebilir olup olmadığını kontrol edin.

- Kullanılmayan hesapları imkân dahilinde silin.
- Uzun süredir Twitter/X kullanıyorsanız, eski tweetlerinizi arşivlemeyi düşünün.

Paylaşılan belgeleri koruyun:

- Google Dokümanlar gibi bulut tabanlı platformlar kullanıyorsanız, dosyaların yalnızca güvendiğiniz iş arkadaşları tarafından erişilebilir olduğundan emin olun.

İkinci bir gözden geçirme yapın:

- Teknoloji konusunda yetkin arkadaşlarınızdan veya meslektaşlarınızdan gözünüzden kaçan bilgileri bulabilme ihtimali nedeniyle benzer aramalar yapmalarını isteyin.

Araştırmacı, hangi kişisel verilerinin çevrimiçi ortamda erişilebilir olduğunu öğrendikten sonra bunları kaldırmak ya da bilgilere erişimi kısıtlamak için adımlar atmalıdır. Kimlik bilgileri Whitepages, Spokeo veya Acxiom gibi veri aracısı sitelerinde görünüyorsa, sitenin "devre dışı bırak" sayfası üzerinden kaldırma talebi gönderilmelidir. Big Ass Data Broker Opt-Out List elliden fazla site için bağlantılar ve ayrıntılı talimatlar sunmaktadır ve bu siteleri önem derecesine göre sıralamaktadır. DeleteMe gibi ticari hizmetler belirli bir ücret karşılığında toplu "devre dışı bırak" işlemleri gerçekleştirmekte ve farklı platformlardaki kişisel bilgi erişimini düzenli olarak izlemektedir. Büyük bir enstitüye veya araştırma merkezine bağlı kişiler, kurumlarının bu tür bir hizmete aboneliği olup olmadığını kontrol etmelidirler.

Randevu planlaması gerekiyorsa Outlook veya Google Takvim kişiselleştirilmelidir. Herkese açık bir takvim, programınız ve konumunuz hakkında kişisel ayrıntılarınızı doğrulanmamış kişilere ifşa edebilme riski taşımaktadır. Benzer şekilde, herkese açık özgeçmişlerdeki e-posta, telefon ve ofis numarası gibi iletişim bilgilerini kaldırmak da riski azaltacaktır. Üniversite web sitelerinde yer alan kişisel bilgilerin silinmesi için idari personele başvurun ve gizlilik kaygılarınızı diğer akademik personelle paylaşın. Örneğin, bölüme ait telefonu cevaplayan kişiden, açık izniniz olmadan hakkınızda bilgi vermemesini talep edebilirsiniz.

Araştırmanızı yaygınlaştırmadan önce Twitter/X hesabınızı silmeyi veya gizli yapmayı düşünmelisiniz. Zira X, çevrimiçi taciz için önemli bir mecra haline gelmiş durumdadır ve giderek güvensizleşmektedir. BlueSky ve Mastodon gibi platformlar bu noktada iyi alternatifler sunmaktadır. Tüm sosyal medya hesaplarında iki aşamalı kimlik doğrulama uygulamasını etkinleştirin ve güçlü parolalar kullanın. Ayrıca her platformda çevrimiçi bir takma ad ve farklı profil fotoğrafları kullanarak izlenebilirliğinizi azaltabilirsiniz.

Kişisel bilgilerinizin kamuda erişilebilir olmadığından artık emin olduğunuzda, geleceğe dönük siber güvenlik protokolleri oluşturmaya başlayabilirsiniz. Kamuya açık etkileşimler için ayrı bir e-posta hesabı açıp gelen iletileri gerçek adresinize yönlendirebilirsiniz. Bu sayede gerçek e-posta adresiniz gizli kalacaktır ve "geçici" adres ele geçirilse dahi çok fazla karışıklık yaşamadan kapatılabilecektir. Ayrıca, kişisel veya ofis telefon numaranızı vermek istemediğiniz durumlar için Google Voice (ABD, Kanada, Birleşik Krallık ve bazı AB ülkelerinde) ya da Dingtone (daha fazla ülkede kullanılabilir) üzerinden sanal bir numara edinmelisiniz.

Araştırmacılar, kullandıkları tüm hesaplar ve cihazlar için güçlü ve benzersiz parolalar oluşturmalıdırlar. Her bir uygulamanın veya sitenin birbirine hangi izinlerle bağlı olduğunu denetleyip gereksiz erişimleri kaldırmak önemlidir. Parolalarınızı takip etmek ve güvenli bir

şekilde saklamak için KeePassXC, 1Password veya LastPass gibi parola yöneticisi araçlarını kullanmanızı şiddetle tavsiye etmekteyiz. Bulut uygulamalarında verileri saklayan yöneticiler ile yerel cihazda depolayan yöneticiler arasında fark bulunduğunu unutmayınız: Yerel parola yöneticileri daha yüksek güvenlik sunmakla birlikte birden fazla cihazda kullanımları bir nebze zahmetli olabilmektedir.

Araştırmacılar, e-posta adreslerinin, parolalarının ya da hesaplarının bir veri ihlali sırasında ele geçirilip geçirilmediğini düzenli olarak kontrol etmelidirler. HaveIBeenPwned gibi web siteleri ile 1Password ve Chrome gibi parola yöneticileri, kayıtlı parolaları bilinen ihlallere karşı taramakta ve olası sızıntılar için uyarıda bulunmaktadır. Ayrıca, telefon üzerinden iki aşamalı kimlik doğrulama seçeneğini etkinleştirmek, parolanız sızdırılsa bile hesaplarınızı koruyan ek bir güvenlik katmanı sağlamaktadır. Bunun yanında, kullanıcıları kişisel bilgilerini ifşa etmeye veya doğrulanmamış dosyalar indirmeye yönlendiren oltalama saldırılarına karşı dikkatli olunuz. Oltalamaya düşmemek için parola ya da hassas veri girmeden önce web sitesi URL'lerini mutlaka elle kontrol ediniz ve kaynağından emin olmadığınız hiçbir yazılımı yüklemeyiniz ya da indirmeyiniz.

Son olarak, araştırmacı bir partner, ev arkadaşı veya aile üyesiyle birlikte yaşıyorsa onların da benzer siber güvenlik adımlarını uygulaması teşvik edilmelidir. Eş, çocuk veya bakmakla yükümlü olunan diğer bireyler hakkında herkese açık paylaşımlardan kaçınınız ve sevdiklerinizin çevrimiçi güvenlik önlemleri konusunda bilgilendirildiğinden emin olunuz.

7. Riskli Araştırmaların Olası Sonuçlarıyla Mücadele

A Taciz

B Taciz Durumlarında Yapılacaklar

C Israrlı Takip ve Tehditler

D Bilgisayar Korsancılığı ve Doxing

E Şantaj ve Zorlama

F Davalar ve Mahkeme Celpleri

G Bilgi Edinme Özgürlüğü Yasası ve Gizlilik Talepleri

H İtibar Kaybı ya da Mesleki Zararlar

I Araştırma Kaynaklı Akıl ve Ruh Sağlığı Desteği

7. Riskli Araştırmaların Olası Sonuçlarıyla Mücadele

Araştırmacılar taciz ya da başka tür zararlarla karşılaştıklarında, kendilerini suçlamamalı ve düşmanca eylemlerden sorumlu tutulmamalıdır. Pek çok kadına, açık veya örtük yollarla, başkalarının verdikleri tepkilerden şahsen sorumlu olmaları gerektiği telkin edilmektedir. Ancak unutulmamalıdır ki hatalı olan araştırmacı değil, tacizcinin kendisidir (Veletsianos ve Hodson, 2018).

Taciz, doxxing ya da şantaj, kişiyi yalnızlaştırabilmektedir. Bu gibi anlarda araştırmacılar, kendi toplulukları içerisinde çekinik davranmaktan kaçınmalıdır. Örneğin, şantaj ve fidye yazılımı taktikleri genellikle kurbanı izole etmeyi ve durumu başkalarına anlatmanın daha fazla zarara yol açacağı fikrini aşılamayı hedeflemektedir. Bu, mağdura tek seçeneğinin failin taleplerine boyun eğmek olduğu düşüncesini yerleştirmek için bilinçli olarak yapılmaktadır.

Saldırının niteliğine bağlı olarak, araştırmacılar güven çemberlerini dar tutmak ve sırlarını paylaşacakları kişileri özenle seçmek zorundadırlar. Bazı arkadaşlar, meslektaşlar veya mentorlar durumu anlamaya ve anlamlı destek sunmaya diğerlerinden daha yatkın olabilmektedir. (Güvenilir kişilerin ve sağlayabilecekleri destek türlerinin stratejik ve dikkatli biçimde listelenmesi burada fayda sağlayacaktır.)

Birçok araştırmacı için polis veya devlet gücünü sürece dâhil etmek sağduyu gereği gibi görünse de, marjinalleşmiş gruplara mensup kişiler açısından bu adım riskli, rahatsız edici veya korkutucu olabilme riski taşımaktadır. Kaldı ki bu gruplar, polis ayrımcılığı ve şiddetinden orantısız biçimde etkilenmekte ya da ulusal güvenlik konularında araştırma yapan kişilerden oluşabilmektedir. Amerika Birleşik Devletleri'nde ACLU ve NAACP gibi kuruluşlar, marjinalleşmiş topluluklara çeşitli bağlamlarda polisle nasıl etkileşime geçeceklerine ve haklarını nasıl savunacaklarına dair rehberler sunmaktadır.

A. Taciz

Riskli araştırmaların en bilinen sonucu tacizdir. "Taciz" terimi, hakaretlerden ölüm tehditlerine ve fiziksel şiddete kadar uzanan geniş bir eylem yelpazesini kapsasa da araştırmacılar, tacizin birden fazla türünü belirlemiştir. İkili taciz, bir kişinin belirli bir süre boyunca başka bir kişiyi sürekli olarak taciz etmesidir ve bu durum takip ya da siber takibe benzer. Ağ temelli taciz, çoğu kez sosyal medya aracılığıyla gevşek biçimde birbirine bağlı bir grubun bir bireyi hedef almasıyla ortaya çıkmaktadır. Her katılımcı yalnızca bir-iki mesaj göndermiş olsa bile hedef alınan kişi bunun nefret dolu bir saldırı seli olduğunu deneyimlemektedir. Normalleştirilmiş taciz, nefret söyleminin yaygın olduğu ortamlarda (örneğin bazı çevrim içi oyunlarda ya da 4Chan gibi sitelerde) görülmektedir. Buna göre kadınlar, beyaz olmayan kişiler ve LGBTQIA+ bireyler gibi sadece ve sadece varlıkları nedeniyle aşağılayıcı ifadeler ya da cinsel tacizle sürekli olarak karşı karşıya kalabilmektedir (Marwick, 2023). Diğer bazı durumlarda bireyler, meşru eleştirilerle karşılaştıklarında da "taciz" terimini kullanabilmektedir. Örneğin YouTuber Carl Benjamin (Sargon of Akkad), feminist oyun eleştirmeni Anita Sarkeesian'ı kendisine yönelen eleştirilere "siber zorbalık" yaparak karşılık verdiği iddiasıyla defalarca hedef tahtasına koymuştur. Araştırmacıların bu bağlamda en çok ağ temelli taciz konusunda kaygılanması beklenir, ancak ikili tacizden bahsetmek de her zaman geçerli bir durumdur.

Ağ temelli tacizi ana akım gündeme taşıyan olay, 2014-2015 yıllarında kadın oyun geliştiricileri, eleştirmenleri, araştırmacıları ve onların destekçilerini hedef alan ünlü Gamergate kampanyasıdır. Gamergate katılımcıları, feministlerin video oyunu araştırmalarını "sabotaj" amacıyla "ele geçirdiği" yönünde bir komplo teorisi yayarak, Dijital Oyun Araştırma Derneği (DiGRA) üyelerini hedef almıştır. Bu kampanya, özellikle feminist video oyunlarını araştıran akademisyenleri—ki bunların bir kısmı AoIR üyesidir—hedef göstermiştir. Shira Chess ve Adrienne Shaw (2014, s. 218) daha sonra bir makalede kendi deneyimlerini şöyle aktarmışlardır:

> "DiGRA'ya ve çalışmalarımıza odaklanılması, feminist araştırma ve ideolojinin ayrıntılar ya da bağlamdan bağımsız olarak ne kadar sık nefret söylemine hedef olduğunu bize sarsıcı biçimde hatırlatmıştır. Feminist araştırmalar, diğer çalışma alanlarında daha görünür hâle geldikçe, sonuçların çoğu zaman karmaşık olduğunu görmekteyiz. Bizim ve diğer feminist akademisyenlerin araştırmaları, daha fazla farkındalık yaratmaya yardımcı olsa da araştırmacıları bizzat inceledikleri taciz türlerine maruz bırakmaktadır."

Ne yazık ki, üzerinden on yılı aşkın süre geçmiş olmasına rağmen bu sorunlar bugün bile her zamankinden daha fazla güncelliğini korumaktadır.

B. Taciz Durumlarında Yapılacaklar

Bir araştırmacı aktif olarak tacize maruz kalıyorsa, ilk olarak mobil bildirimleri kapatarak stres düzeyini azaltmalıdır. Olanak varsa, bildirimleri bir arkadaşının veya eşinin izlemesini rica edebilir. Bildirimleri ne kadar süreyle kapalı tutacağı, tacizin türüne ve şiddetine göre değişiklik gösterecektir. Kimi araştırmacılar için 72 saat yeterli olurken, kimileri için bu süre günler, hatta haftalar alabilmektedir.

Araştırmacı, tacizcileri anında engellemelidir. Ayrıca, tacizcilerin acil durum ihbarı yapar gibi yanlış bilgi vererek polis veya acil durum ekiplerini araştırmacının adresine yönlendirdiği durumları imleyen SWATTING riski varsa, yerel kolluk kuvvetleriyle önceden iletişime geçilmesi uygun olacaktır. Bu nokta, polislerin silah taşıdığı ülkelerde özellikle kritiktir; zira swatting, yaşamı tehdit eden bir duruma dönüşme ihtimali taşımaktadır. Ek olarak, ilgili kurum— üniversite veya çalışılan kuruluş—muhatap olunan tacizden haberdar edilerek uygun destek ve korunma mekanizmalarının devreye girmesi sağlamalıdır.

C. Israrlı Takip ve Tehditler

Riskli araştırmalar yürüten akademisyenler, kamuoyu öfkesinin boy hedefi haline gelerek takibe düşme durumlarıyla karşı karşıya kalabilmektedirler. İzinsiz takip eylemini gerçekleştirenlerin kurbanları arasında her cinsiyetten bireye rastlamak mümkün olsa da böylesi durumlarda kadınların takibe maruz kalma olasılıkları her zaman daha yüksektir. En aşırı uç şiddet örneği olarak fiziksel saldırı ya da ölümle sonuçlanmasa dahi takip, çoğu durumda uzun vadeli psikolojik, sosyal ve ekonomik zararlara neden olmaktadır (Logan, 2023). Mağdurlar, takipçiden kaçmak için taşınmak veya işlerinden ayrılmak zorunda kalabilmekte, taciz sona erdikten sonra bile güven duygusunu yeniden kazanmakta zorlanabilmektedir (Logan & Showalter, 2023). Siber ortamda karşı karşıya kalınan takipler konusundaysa, bunların çevrimdışı takibin bir uzantısı mı olduğuna yoksa başlı başına ayrı bir davranış biçimine mi karşılık geldiğine yönelik tartışma halen sürmektedir. Çevrimdışı takibe kıyasla çoğu zaman daha az ciddi bir sorun gibi algılansa da siber takip, psikolojik, duygusal ve finansal açıdan hiç de azımsanmayacak zararlar doğurabilmektedir (Kaur vd., 2021).

Siber takibe maruz kalan araştırmacıların attığı ilk adım genellikle tacizciyi engellemek olmaktadır. Ancak platform politikaları bu konuda değişkenlik göstermektedir: X (eski adıyla Twitter) yakın zamanda hesap engelleme özelliğini kaldırırken, BlueSky gibi platformlarda bu seçenek hâlen mevcuttur. Bazı durumlarda, sessize alma, içeriği gizleme ya da erişimi kısıtlama gibi yöntemler doğrudan engellemekten daha uygun olabilmektedir, çünkü bu tercihler tacizcinin sessize alındığını fark etme ihtimalini düşürerek olası misillemeleri azaltabilmektedir. Çevrimiçi Tacizle Mücadele Rehberi, her platform için mevcut sessize alma ve engelleme araçlarını ayrıntılı biçimde açıklamaktadır.

Taciz, takip veya çevrimiçi istismar durumlarını rapor etme kararı kişisel bir tercihtir. Raporlama, belgelenmiş bir iz bırakacağı için platformun zararlı içeriği kaldırması ya da tacizcinin hesabını kapatması gibi sonuçlara evrilebilmektedir. Bununla birlikte, geçmişte platformlar taciz ya da takip bildirimlerine her zaman destekleyici veya hızlı bir yanıt vermemiştir (Amnesty International, 2018). Bu nedenle araştırmacılar, raporlamanın anlamlı sonuçlar doğurmama ihtimaline karşı hazırlıklı olmalıdırlar. Her platformun farklı topluluk kuralları ve gereksinimleri olması nedeniyle araştırmacıların bunlara aşina olması gerekmektedir. Ayrıca, arkadaşlar, aile üyeleri veya güvendiği meslektaşlarından yardım isteyerek tacizi izlemede, ihlalleri raporlamada ve siber takibe verilen duygusal-lojistik tepkiyi paylaşmada destek almaları faydalı olacaktır.

D. Bilgisayar Korsancılığı ve Doxing

Devlet destekli bilgisayar korsancılığı, yalnızca hükümetleri ve siyasetçileri değil, aynı zamanda araştırmacılar, akademisyenler, sivil toplum kuruluşları (STK'lar) ve gazeteciler gibi sivil toplum temsilcilerini her geçen gün daha fazla hedef almaktadır. Bu saldırıların amacı, komplo teorilerini beslemek, güvensizlik yaratmak ya da eleştirmenleri susturmak ve sindirmek için kullanılabilecek belge ya da iletişim kayıtlarına ulaşmaktır (Briant, 2023a, 2023b). Bu tür saldırıların faillerini tespit etmek aylar sürebilmekte ve bir kez ele geçirilen bilgiler sosyal medya üzerinden sızdırıldığında, kamu yararı güden gazetecilik faaliyetleri olarak çerçevelenebilmektedir. Briant'ın (2023a) belirttiği gibi, "bilgisayar korsancılığı ve casus yazılımlar, hem gazetecilerin ifade özgürlüğünü hem de kaynaklarının korunmasını sağlayan Avrupa İnsan Hakları Sözleşmesi'nin 10. Maddesi kapsamındaki hayati gizliliği tehdit etmektedir". Aynı durum araştırmacılar için ayrı bir tehdit unsuru oluşturmaktadır (s. 287). Araştırmacılar, ele geçirilmiş bilgilerin ya da bu bilgilerden türetilmiş dezenformasyonun platformlardan kaldırılması konusunda büyük zorluklar yaşamaktadır. Oysa ki bu şekilde ele geçirilmiş verilerin dağıtılması, sosyal medya politikalarını ihlal etmektedir. Şifreleme ve Çok Faktörlü Kimlik Doğrulama kullanılsa dahi farklı türden korsanlık saldırıları gerçekleşebileceğinden, araştırmacıların hassas iletişimlerinde e-posta kullanımını asgariye indirmeyi düşünmeleri önerilmektedir.

Korsancılık eylemleri, genellikle bireylerin kişisel ve tanımlanabilir bilgilerini–örneğin ev adresini, telefon numarasını, kredi kartı bilgilerini, doğum tarihini veya kimlik numarasını–izinsiz olarak ifşa etmek anlamına gelen doxxing için başlıca bilgi kaynağıdır. Doxxing genellikle hedef kişiyi korkutmayı amaçlamakta ve SWAT çağrıları, fiziksel çatışmalar, hedefin ve yakınlarının maruz kaldığı tehdit veya şiddet eylemleri, mülke zarar verme ve artan gözetim gibi fiziksel şiddete varan sonuçlara yol açabilmektedir (Molas, 2024). Fiziksel risklerin ötesinde doxxing, hukuki ve politik sonuçlar da doğurabilmektedir. Çoğu zaman, bireyleri itibarsızlaştırmak, susturmak veya zarar vermek için hukuki sistemlerin stratejik biçimde kullanılması anlamına gelen "hukuk savaşı" kapsamında kullanılabilmektedir (Kittrie, 2015).

ABD'de doxxing, kamu üniversitelerinde çalışanlar ve araştırmacılar hakkında Bilgi Edinme Hakkı Kanunu (Freedom of Information Act, FOIA) kapsamındaki başvurular şeklini alabilmektedir. Avrupa Birliği'nde ise Genel Veri Koruma Tüzüğü (GDPR) sayesinde veri sahipleri daha geniş haklara sahiptir. "Silinme Hakkı" ya da "Unutulma Hakkı," mağdurların kişisel verilerinin internet sitelerinden kaldırılmasını talep etmelerine imkân tanımaktadır; ancak bunun uygulanması pratikte zorluk teşkil etmektedir. Ayrıntılı bilgi için "GDPR Unutulma Hakkı" web sitesine bakınız.

Bir araştırmacı doxxing'e maruz kaldığında, yaşadıklarını belgelemesi önemlidir. Mümkün olduğunda ekran görüntüsü alınmalı, ilgili web sayfası indirilmeli, archive.today gibi bir web arşivi kullanarak kayıt altına alınmalı veya olayı izlemenin başka yolları denenmelidir. Bu materyallerin, görünür URL'ler eşliğinde zaman damgalı olması şiddetle tavsiye edilmektedir: ayrıntılar için Crash Override'ın *So You've Been Doxed* rehberine bakınız. Bu belgeler, hem araştırmacının kendi başvuruları hem de gelecekte yardımda bulunabilecek kolluk kuvvetleri veya hukuki merciler için hayati önem taşıyabilmektedir. Ancak bu durum, araştırmacının söz konusu doxxing içeriğini internet ortamında bırakması gerektiği anlamına gelmez. İçerik bir kez kaydedildikten sonra, bilgileri barındıran siteyle iletişime geçilmelidir. Örneğin, Pastebin benzeri platformlar, özel bilgilerin kaldırılması için özel prosedürler sunmaktadır.

E. Şantaj ve Zorlama

Riskli araştırmalar, nadir de olsa, şantajla sonuçlanabilmektedir. Siyasi saikli şantaja maruz kalan akademisyenlere dair belgelenmiş örneklerle henüz karşılaşılmamış olsa da gelecekte bunun yaygın hâle gelme ihtimali söz konusudur. Calgary Üniversitesi ve Regis Üniversitesi gibi akademik kurumlar, şantaj amaçlı fidye yazılımı saldırılarıyla karşı karşıya kalmıştır (CERN, 2020). Bu saldırılarda son derece örgütlü ve kaynakları güçlü suç ağları, kurumların bilgisayar sistemlerine erişimi yeniden sağlamak için ödeme talep etmiştir. Benzer taktikler zamanla bireysel araştırmacıları da hedef alabilmekte; araştırmacılar fidye ödemeye zorlanabilmekte ya da belirli araştırma projelerinden vazgeçmeleri için baskı görebilmektedir.

Doxxing, gizlilik ihlalleri veya veri sızıntıları yaşayan araştırmacılar, kişisel ya da cinsel içerikli (sextortion) şantaja da maruz kalabilirler. Hesapları ele geçirilen sosyal medya kullanıcıları arasında yaygın biçimde raporlanan bu tarz şantaj yöntemleri (Hendry, 2021), kamusal alanda çalışan araştırmacılar için artan bir risk teşkil etmektedir.

Çevrim içi şantaj, oltalama dolandırıcılıkları, veri ya da fotoğraf korsancılığı ve sahte kimlik oluşturma gibi çeşitli biçimler alabilmektedir. Bu tarz farklı taktikler, araştırmacılarda duygusal sıkıntı, mali kayıp ve itibar zedelenmesine yol açabilmektedir. Bu kılavuz genelinde vurgulandığı üzere, parola yöneticileri kullanmak, iki aşamalı kimlik doğrulamayı etkinleştirmek ve yaygın oltalama yöntemleri ile dolandırıcılıklara dair bilgi sahibi olmak hali hazırda başvurulabilecek en etkili önleyici adımlar arasında yer almaktadır.

Çoğu şantaj vakasında, araştırmacıların şantajcıyla iletişim kurmaması, pazarlığa girmemesi ve ödeme yapmaması önerilmektedir, çünkü bu tür adımlar hem güvenli değildir hem de genellikle taleplerin artarak devam etmesi demektir. Bunun yerine, şantajcıyla iletişimi derhâl kesmek, güvenilir kişilerden duygusal destek almak ve şantajcıyla yapılan tüm etkileşimleri belgelemek önem arz etmektedir. Bu saldırılarla tek başınıza mücadele etmek yerine bir destek ağına sırt dayamak hem duygusal açıdan güven duyma noktasında hem de durumu yönetmede çok daha etkili sonuçlar doğuracaktır.

F. Davalar ve Mahkeme Celpleri

Not: Bu bölüm, ABD hukukuna özgüdür.

Araştırmacılar, riskli araştırmalar nedeniyle dava veya mahkeme celbiyle karşı karşıya kalabilmektedir. Örneğin, ABD Temsilcisi Jim Jordan, dezenformasyonla mücadelede kamu-özel sektör iştiraklerinde yer alan ya da benzer araştırmalar yürütmek için Ulusal Bilim Vakfı (NSF) fonu alan Amerikalı araştırmacılara Kongre celpleri göndermiştir. Araştırma bulgularının kendilerini olumsuz gösterdiği durumlarda sosyal medya platformları da benzer şekilde araştırmacıları, çoğu zaman Hizmet Koşullarını ya da Bilgisayar Dolandırıcılığı ve Kötüye Kullanım Yasası'nı ihlal ettikleri iddiasıyla hedef alabilmektedir (örneğin "scraping" yoluyla veri kazıma gibi). Elon Musk, Twitter/X'te dezenformasyonun yaygın olduğunu ortaya koyan araştırmaları nedeniyle kâr amacı gütmeyen Center for Countering Digital Hate (CCDH) kuruluşuna dava açmış; bu araştırmaların CCDH'nin Twitter/X verilerini izinsiz kazıdığını ve ayrıca reklam veren kaybına yol açtığını öne sürmüştür. Turning Point USA gibi "taban hareketi" aktivist grupları da üniversite ve kâr amacı gütmeyen kuruluşlardaki araştırmacıları dava etmiştir.

Araştırmacıların ürettiği verilere ilişkin olarak, ABD mahkemeleri henüz doktor-hasta gizliliğine benzer şekilde "araştırmacı-katılımcı" ayrıcalıklarını tanımlamış değildir (Haney-Caron, Goldstein ve DeMatteo, 2015). Örneğin Boston College'daki tarihçiler tarafından yürütülen Belfast Projesi, Kuzey İrlanda'daki paramiliter örgütler ve üyelerine dair sözlü tarih kayıtları toplamıştır. Katılımcılar, bant kayıtlarının ve transkriptlerin "nihai yayımlama yetkisinin" kendilerinde olduğunu belirten anlaşmalar imzalamışlardır. Ancak Birleşik Krallık makamları, 1972'de işlenen bir cinayeti soruşturmak amacıyla projedeki verilere erişim talep edince, bu materyaller mahkeme celbiyle istenmiş ve bir bölge mahkemesi, böyle durumlarda hükümetin akademik araştırmacıları verileri paylaşmaları yönünde zorlayabileceğine hükmetmiştir. ABD özelinde araştırmacıları bu tür mahkeme celplerinden koruyan en güçlü yasal düzenleme, yürütülen proje/araştırma için Gizlilik Sertifikası edinmiş olmaktır (bu tür koruyucu önlemlere "Gizlilik Sertifikası" bölümünde de değinilmektedir). Bununla birlikte, son derece kutuplaşmış ABD siyasi ortamında, bir zamanlar yasal olup bazı eyaletlerde artık yasa dışı sayılan uygulamalarda (örneğin kürtaj veya cinsiyet uyum bakımı) Gizlilik Sertifikalarının mahkeme nezdinde ne derece geçerli sayılıp sayılmayacağı halen daha belirsizliğini korumaktadır.

G. Bilgi Edinme Özgürlüğü Yasası (FOIA) ve Gizlilik Talepleri

ABD, Avustralya veya Avrupa'daki kamu üniversitelerinde çalışan araştırmacılar, e-postalarının, üniversite sunucularında saklanan belgelerinin ve e-postalara eklenmiş her türlü belgenin Bilgi Edinme Özgürlüğü Yasası kapsamında herhangi bir kişi tarafından talep edilebileceğini bilmelidirler. Kamu üniversitelerindeki çalışanlarla yazışan kişiler için de durum farklı değildir. Özel üniversiteler veya düşünce kuruluşlarında görev yapan ve kayıtları Bilgi Edinme Özgürlüğü Yasası kapsamına girmeyen kişiler bile, yapılan başvuru neticesinde kişisel bilgilerinin açığa çıkarılması riskiyle karşı karşıya kalabilmektedir. Ne yazık ki, kamu ya da devlet fonu alan kişilere yönelik Bilgi Edinme Özgürlüğü Yasası taleplerinin "saldırı silahı" hâline getirildiği örnekler giderek artmaktadır.

ABD ve Avustralya'da Bilgi Edinme Özgürlüğü yasaları eyalet bazında düzenlendiği için, üniversitelerin gelen taleplere verdikleri yanıtlar kuruma göre büyük farklılıklar göstermektedir. Bazı üniversitelerde Belge Kayıt Birimleri talebin tamamını bizzat yürütmekte ve sürecin sonunda araştırmacıyı kuru bir bilgilendirmeyle yetinmektedir. Diğer üniversitelerde

ise araştırmacının talebi bizzat yönetmesi beklenmekte, dolayısıyla da talebin kapsamına bağlı olarak bu son derece ağır bir yük anlamına gelmektedir. ABD'deki kamu üniversitelerinde görev yapan araştırmacıların, üniversitelerinin Belge Kayıt Birimleriyle iletişime geçerek Bilgi Edinme Özgürlüğü Yasası kapsamında yapılan başvuru durumunda kendilerinden ne beklendiğini ve hangi kayıt türlerinin süreçte muaf tutulduğunu öğrenmeleri gerekmektedir. Bazı eyaletlerde öğrencileri içeren e-postalar ile devam eden araştırma projelerine dair belgeler istisna kapsamına alınmıştır.

ABD dışında da açık belge yasaları uygulanmaktadır. Örneğin 21. yüzyılda Avustralya ve Birleşik Krallık'ta iklim bilimcileri, bu tür talepler aracılığıyla taciz edilmiştir (Halpern, 2015). Avrupa'daki Genel Veri Koruma Yönetmeliği veya "Unutulma Hakkı" gibi gizlilik düzenlemeleri de, düşmanca tutum sergileyen araştırma katılımcıları tarafından veriye erişim talep etmek için kullanılabilmektedir. Bu veriler en nihayetinde daha sonra araştırma ya da araştırmacı aleyhine yürütülen bir algı operasyonunun parçası haline gelebilmektedir. Aynı zamanda, kritik bilgilerin sansürlenmesine yol açabilecek veri silme talepleriyle de karşılaşılmaktadır. Yasal süreçlerle karşı karşıya kalan araştırmacıların daha güçlü korumalara ihtiyacı vardır; zira Bilgi Edinme Özgürlüğü Yasası ve Genel Veri Koruma Yönetmeliği talepleri eşzamanlı olarak kullanılarak araştırmacı üzerinde baskı kurulabilmektedir. Sürekli denetim ve gözetim ortamı, akademik çalışmaları caydırıcı ve bastırıcı etkiye sahiptir.

Genel Veri Koruma Yönetmeliği veya Bilgi Edinme Özgürlüğü Yasası'na tabi oldukları durumlarda araştırmacılara, riskli araştırmalarıyla ilgili üniversite e-postası kullanmaları yerine Bölüm 5'te (Gizli/Özel İletişim Kanalları) listelenen güvenli iletişim yöntemlerinden birini tercih etmeleri önerilmektedir. Araştırmacılar üniversite tarafından sağlanan bilgisayarı kullanmak yerine kişisel bilgisayar tercih etmeli ve belgelerini OneDrive gibi üniversiteye ait bulut depolama alanlarında saklamaktan kaçınmalıdır. Bu durum üniversite politikalarını ihlal etme ihtimali taşıdığı için kanunen gerekli durumlarda saklanan bilgileri sunma zorunluluğu ortaya çıkabilmektedir. Ancak üniversiteler, kişisel bilgisayarda veya özel hesaplarda tutulan bilgilere büyük olasılıkla erişim talep etmeyeceklerdir.

Bu durumların hiçbirinde araştırmacılar, üniversite avukatlarının kendilerini korumak veya temsil etmekle yükümlü olduğunu varsaymamalıdır. Dikkat edilmesi gereken nokta, araştırmacının çıkarlarıyla üniversitenin ve kurum avukatlarının çıkarlarının çoğu durumda örtüşmeyebileceğidir. Bazı durumlarda, Araştırma Destek Forumu, Amerikan Sivil Özgürlükler Birliği (ACLU), Electronic Frontier Foundation, Bireysel Haklar ve İfade Özgürlüğü Vakfı (FIRE) gibi kurumlar aracılığıyla, araştırmacının davası kamuoyu nezdinde sempati topluyorsa ücretsiz hukuki destek alınabilmektedir. UMass Amherst araç seti de önerilen e-posta kullanımı ve Bilgi Edinme Özgürlüğü Yasası kapsamındaki taleplere ilişkin ayrıntılar konusunda rehberlik sunmaktadır.

H. İtibar Kaybı ya da Mesleki Zararlar

Araştırmacılar çeşitli biçimlerde eleştiriye tabi tutulabilmektedir. Bir araştırmacı, kamuya açık bir ortamda saldırıya uğradığında ya da eleştirildiğinde, kendisine tam olarak ne için ve kim tarafından tepki gösterildiğiyle ilgili durup düşünmelidir. Genel olarak bakıldığında eleştirileri iki temel başlık altında toplamak mümkündür: tehdit içermeyenler ya da doğrudan ve açık düşmanlık besleyenler. Bu belgenin çoğu, düşmanca tutum sergileyen saldırıları temel almaktadır. Örneğin aşırı sağ bir grup bir araştırmacıya saldırma yolunu seçerse, akademik çevresindeki çoğu kişi muhtemelen endişelenecek ve anlayışlı bir tavır takınacaktır. Düşmanca duygularla hareket etmeyenler daha ziyade, araştırmacının politik ya da ideolojik görüşlerini

paylaşanlara ya da akademik camiadaki meslektaşlarına karşılık gelmektedir. Yine de bu cenahtan gelen eleştiriler, kişinin mesleki konumuna duruma göre çok daha fazla zarar verme tehlikesi taşımaktadır. Bir araştırmacı, birinin çalışmasını çalmakla, cinsiyetçi/ırkçı bir ifade kullanmakla, etik dışı araştırma yapmakla ya da başka ortak bir normu ihlal etmekle suçlanırsa, itibarı büyük ihtimalle yerle bir olacaktır.

Düşmanlık beslemediği düşünülen odaklarla mücadele ederken, özellikle de araştırmacı yapmadığına inandığı bir şeyle suçlandığında, Twitter/X veya Medium yazısı gibi kamusal platformlarda kendini açıklama/aklama dürtüsü ağır basmaktadır. "İnsanların hikâyenin tamamını bildiği durumda" kendi bakış açısını benimseyecekleri varsayılır. Ancak bu tutumun geri tepme ihtimali de son derece yüksektir. Kendilerinden daha az iktidara sahip kişiler tarafından güçler dengesini ihlal etmekle suçlanan bir araştırmacı, savunma refleksini bir kenara bırakarak iddiaların doğruluğunu değerlendirme işini ciddiye almalıdır. İddialar doğruysa, araştırmacı samimi bir özür dileyip eylemlerinin zararını telafi etmeye çalışmalıdır. İddialar doğru değilse, muhtemelen hiçbir şey söylememek kendisi adına en iyi tavır olacaktır. Her iki durumda da savunmaya geçmek, hiçbir şey söylememekten çok daha kötü bir izlenim yaratacaktır. Ne var ki araştırmacı, ilgili topluluklarda güven duyulan kişileri tanıyorsa, bu kişilere ulaşıp kendi adına konuşmalarını talep edebilirler.

Düşmanca yaklaşan aktörlerin tacizine uğrayan bir araştırmacı ise durumu farklı şekilde yönetme yolunu seçmelidir. Bu tür durumlarda düşmanlık sergileyen gruplar, araştırmacının yayınlarına ve araştırmasına saldırabilecekleri gibi işten bağımsız kişisel meseleleri de gündeme getirebilmektedir. Tacizin farklı biçimleri farklı yanıtlar gerektirmektedir. Kişisel olarak saldırıya uğramak acı vericidir, fakat faille doğrudan etkileşim kurmak tacizi durdurmaya çoğu zaman yeterli gelmeyecektir. Araştırmacı destekleyici bir akademik kurumda ya da araştırma grubunda çalışıyorsa ve tacizciler araştırması hakkında asılsız iddialar ortaya atıyorsa, hızlı ve kamusal bir açıklama yapmak yarar sağlayabilir. Verilecek yanıt, tacizci(ler) ile doğrudan diyalog kurmayı gerektirmez; bunun yerine araştırmacının kendi seçtiği bir ortamda, "olayın aslını" veya tam olarak ne olduğunu açıklayabileceği bir format biçiminde de kurgulanabilir. Kurumlar genellikle araştırmacılara bu tür tacizlere yanıt vermemelerini tavsiye etmektedir, ancak söylentiler ya da asılsız bilgiler herhangi bir engelle karşılaşmadan dolaşıma girdiğinde aksini iddia etmek çok daha güç bir hal almaktadır. Buna bağlı olarak, benzer durumlarla karşı karşıya kalan araştırmacılar ilgili kurumlarla derhal devreye sokulacak bir acil durum planı hakkında konuşmalı ve medya ile hukuk ortamını bilen güvenilir danışmanlarla irtibatlı olmalıdır.

Bir araştırmacının sahip olduğu konum, kişisel veya entelektüel içerikli tacizle mücadele etme biçimini etkileyecektir. Marjinalleştirilmiş ve güvencesiz topluluk üyeleri, tacize ve en ağır hakaretlere sıklıkla maruz kaldıklarından, entelektüel camiamızın üyelerini koruması hayati derecede önem arz etmektedir.

Sosyal medyada tacize uğramak veya dava edilmek, bir araştırmacının mesleki itibarı için olumsuzluk teşkil etmektedir. Bu durum, özellikle öğretim görevlileri, lisansüstü öğrenciler ve doktora sonrası araştırmacılar gibi güvencesiz çalışma koşullarına sahip kişiler açısından çok daha fazla bir geçerliliğe sahiptir. İlgili kurumlar bazen hedef alınan öğretim üyeleriyle aralarına kamusal mesafe koymakta ve neticede söz konusu istismarı meşrulaştırarak öğretim üyesinin maruz kaldığı tacizin dozajının artmasına neden olmaktadır. Yukarıda belirtildiği gibi, bir saldırı hedef kişinin ruh sağlığı ve esenliği üzerinde önemli neticeler doğurabilmektedir. Taciz, araştırmacının kadroya geçme kriterlerini karşılayamaması ya da terfiden mahrum kalması gibi kariyerini ve iş performansını olumsuz etkileyen sonuçlarla neticelenmektedir.

Araştırmacılar ayrıca iş kaybı, vize başvurusu reddi, kalıcı kadro ya da terfi hakkının engellenmesi ve fakülteye karşı şikâyet mekanizmalarının silah hâline getirilmesi gibi olumsuz mesleki sonuçlarla da yüz yüze kalabilmektedirler.

I. Araştırma Kaynaklı Akıl ve Ruh Sağlığı Desteği

Riskli araştırmaların akıl ve ruh sağlığı açısından ciddi etki ve sonuçları vardır. Bu tür araştırmalar, genellikle tehdit edici ve stresli durumları, kişisel riskleri ve çeşitli olumsuzluklara tanıklık etmenin getirdiği sonuçları kapsamaktadır (Newman, Simpson & Handschuh, 2003; Rager,2005). Bu durum, araştırmacıların huzur içerisinde bir yaşantı sürdürmelerine karşı ciddi tehlikeler yaratma potansiyeli taşımaktadır.

Akademi kültürünün kendisi de ek bir stres ve travma kaynağı olarak ortaya çıkabilmektedir. Akıl ve Ruh sağlığı araştırmacıları, lisansüstü eğitim sürdürmenin ve akademik kariyer yapmanın akıl ve ruh sağlığı bakımından kaygı verici sonuçlarına dikkat çekmektedirler (Gewin, 2021; Murguía Burton ve Cao, 2022; Nicholls, Nicholls, Tekin, Lamb ve Billings, 2022). Araştırmacıların ileriye dönük beklentileri, kimi zaman zararların etkileri ve başa çıkma stratejileri konusunda gerçekçi olmayan standartlar ortaya koymaktadır. Akıl ve ruh sağlığı hastalıkları netice itibariyle, başarısız kariyer ilerlemesi ve ilişki kurma bozuklukları, tükenmişlik, hatta uzun süreli sakatlık ya da intihara eğilim gibi ciddi sonuçlar doğurabilmektedir.

Akıl ve ruh sağlığı ile beden sağlığı birbiriyle yakından ilişkilidir. Dolayısıyla da fiziksel sağlık sorunlarının akıl ve ruh sağlığını, akıl ve ruh sağlığı sorunların da beden sağlığını etkilemesi oldukça olasıdır. Neyse ki, travmayla temas neticesinde ortaya çıkabilecek meslek rahatsızlıkları karşısında araştırmacıların ruh sağlığını korumalarına yardımcı olabilecek birtakım kaynaklar mevcuttur. Korkunç durumlarla karşılaşıldığında stres ve kaygı hissetmenin veya depresyona girmenin normal bir tepki olduğunu takdir etmek önemlidir. Bir cinayete ya da acı içindeki bir çocuğa tanık olan makul bir kişinin olumsuz duygular geliştirmesi kaçınılmazdır. Bazı araştırmaların bünyesinde riskler barındırdığını ve olası tehlikelerle başa çıkmak için hazırlıklı olmanın araştırma planlamasının bir parçası olduğunu hesaba katmak gerekmektedir. Araştırmacılar karşılaşabilecekleri riskler konusunda kendilerine karşı dürüst davranmalıdırlar. Araştırmacıların kendilerine değer vermeleri akıl ve ruh sağlığına yönelik tehditlerden korunma noktasında fayda sağlayacaktır (Lee ve Miller, 2013; Rager, 2005; Steadman, 2023).

Riskli araştırmalar çoğunlukla bireylerin tek başına çözemeyeceği kapsamlı yapısal sorunlarla ilişkili olarak ortaya çıkmaktadır. Bu yapısal engeller nedeniyle, benzer konuları çalışan kişileri de içeren bir destek ağı kurma yoluna giderek güvenlik ve destek stratejileri geliştirmek, riskli araştırmanın akıl ve ruh sağlığına olumsuz yansımalarıyla başa çıkmak adına atılabilecek en faydalı adımlar arasında yer almaktadır. Özellikle travmatik içeriklerle muhatap olunduğu zamanlarda çalışmanın akıl ve ruh ya da beden sağlığı üzerindeki gözlemlenebilir etkisini bu türden araştırma faaliyetleri yürütmeyen arkadaş ve aile üyeleriyle iletişim kurarak değerlendirmeye çalışmak da yine izlenebilecek yollar arasındadır. Riskli içeriklerle çalışanlar zamanla duyarsızlaşabilmekte ya da "kara mizah" gibi riskin etkileriyle başa çıkma mekanizmaları geliştirebilmektedir. Dolayısıyla bazen "halkanın dışındaki" kişilerden görüş almanın bir nebze nefes almaya yararı olabilmektedir (Pearson vd., 2023).

Sağlık sigortası olan ve profesyonel terapiye erişimi bulunan araştırmacılar, akıl ve ruh sağlığı hizmeti almalıdırlar. Düzenli uyku, dengeli beslenme ve düzenli egzersiz gibi akıl ve ruh

sağlığını günlük rutinlerle iyileştirmeye yönelik oldukça standart öneriler mevcuttur. Araştırmacı, akıl ve ruh sağlığının yürüttüğü çalışma nedeniyle bozulduğundan şüpheleniyorsa, mümkün olduğunca uzun süreli bir ara vermesi muhtemelen yerinde olacaktır. Emin olmama durumu mevcutsa, Amerikan Psikiyatri Birliği kişiye profesyonel ruh sağlığı tedavisi gerekebileceğini gösteren semptomların bir listesini sunmaktadır. Daha da önemlisi, araştırma mesleki anlamda bir risktir ve işverenin akıl ve ruh sağlığı hizmetlerine erişim sağlama noktasında sorumluluğu bulunmaktadır. Ancak pratikte bu her zaman geçerli ve gerçekçi bir beklenti değildir. Araştırmacının sağlık sigortası yoksa ücretsiz veya gelir düzeyine göre ücretlendirme yapan akıl ve ruh sağlığı hizmetlerinden yararlanma imkanı bulunmaktadır. Örneğin Amerika Birleşik Devletleri'nde Ulusal Ücretsiz ve Hayırsever Klinikler Birliği ile Amerika Akıl ve Ruh Sağlığı Kurumu, sigortasız veya kapsamı yetersiz sigortalı kişilerin bakım hizmeti almasına yardımcı olmaktadır.

Kriz Anı Kaynakları

Bir araştırmacının hızlı bir şekilde yardıma ihtiyaç duyması halinde faydalanabileceği kriz anı kaynakları arasında; acil arama hatları (ABD'de 911), yardım hatları (bkz. Bölüm 10, Kaynaklar), şahsen başvurulan ayakta kriz merkezleri ve hastane acil servisleri ya da acil bakım üniteleri yer almaktadır. Bu seçeneklerin tümü, araştırmacıların uygun bir kaynağa yönlendirilmesi adına fayda sağlamaktadır.

Bireysel Uygulayıcılar

Tıp ve akıl ve ruh sağlığı uzmanları; tanı/değerlendirme, testler, destekleyici tedaviler, psikoterapi ve psikiyatrik ilaçlar dâhil olmak üzere çeşitli başlıklar altında hizmetler sunabilmektedir.

Akıl ve Ruh Sağlığı Klinikleri/Merkezleri

Bu kurumlar, tek bir uzmana nazaran daha kapsamlı hizmetler sağlamakta ve çoğu zaman ekip yaklaşımını benimsemektedir. Üniversiteler bünyesindeki Çalışan Destek Programları veya Danışmanlık Merkezleri gibi birimler geniş bir yelpazede hizmet sunmaya devam etmektedir.

Hastaneler ve Uzun Süreli Bakım Hizmetleri

Ciddi sağlık sorunları olan ya da hastane yatışı gereken bireyler için gerekli hizmetleri sağlamaktadır. Madde bağımlılığı sıklıkla karşılaşılan sorunlar arasında yer almaktadır. Uygun tedaviler, bireye, yaşadığı sağlık sorununa ve diğer özel durumlarına bağlı olarak değişkenlik göstermektedir. Sağlık personeli veya tedavi ekipleri, tüm bu unsurları değerlendirerek en iyi yol haritasını belirleyeceklerdir. Terapötik müdahaleler arasında öne çıkanlar, içgörü odaklı terapiler, bilişsel davranışçı terapiler, görev odaklı terapiler ve davranışsalcı terapiler gibi çeşitli yaklaşımları içeren psikoterapi yöntemleridir. Terapiler, bireysel, grup veya aile düzeylerinde gerçekleştirilebilmektedir. Psikoterapistlere ek olarak tıp eğitimi almış yetkili diğer personel de olası yan etkilere bağlı olarak ortaya çıkan ve müşahede altında tutmayı gerektiren durumlar için psikotropik ilaçlar reçete edebilmektedir. Ağır vakalarda hastaneye yatış gerekli görülebilmektedir. Akıl ve ruh sağlığına yönelik uzaktan hizmet servislerinin artması, bakım erişimini genişletmiş ve bireylerin sanal ortamda tedavi almasına olanak tanımıştır. Sağlık sigortası olanlar, tedavi masraflarının bir kısmını ya da tamamını kendileri karşılayabilirler. Akıl ve ruh sağlığı sorunları yaşamın doğal bir parçasıdır, dolayısıyla da ahlaki bir mesele ya da karakter zayıflığı olarak algılanmamalıdır.

8. Kurumsal İşbirliği

A Kurumsal Düzeyde Bireysel Savunuculuk

B Kurumlara Yönelik Başarılı Uygulama Örnekleri

C Ders Verme Süreçleri

• Kurumsal İşbirliği

Kurumlarla muhatap olmak, işin belki de en yorucu taraflarından biridir. Çoğu kurum, araştırmacıları ilgilendiren riskler konusunda yeterince bilgi sahibi değildirler. Pek çoğu kamuoyu olumsuzlarından kaçınmaya yatkınlık göstermekte ve kamusal alanda dolaşımda olan eleştiriler yersiz olsa bile tartışma yaratacak projelerden ve proje yürütücülerinden uzak durmayı tercih etmektedir. Bu bölümde, kurumların araştırmacıları bu tür anlara hazırlamakla ve onların dijital, fiziksel ve psikososyal ihtiyaçlarını karşılayacak biçimde desteklemekle yükümlü olduklarını savunuyoruz.

A. Kurumsal Düzeyde Bireysel Savunuculuk

Bir araştırmacının çalışmasına başlamadan önce, kurumunu, kampüs güvenlik ağını, bilgi güvenliği direktörünü ya da eşdeğer konumdakileri ve meslektaşlarını yakın zamanlı araştırma projesi hakkında bilgilendirmesi faydalı olacaktır. Sendikalı araştırmacılar, araştırmalarında karşılaşabilecekleri riskleri sendika temsilcilerine bildirmelidir. Akademisyenler, işverenlerine (proje yürütücüsü, bölüm başkanı, laboratuvar yöneticisi vb.) çevrim içi taciz ve benzeri zararların varlığı ve gerçekliği konusunda eğitim vermekle yükümlüdür. İdeal bir senaryoda araştırmacılar, amir ve yöneticilere yapılması gerekenleri—destekleyici kamuoyu açıklamaları için örnek metinler dâhil—anlatma yoluna başvurmalıdır. Buradaki amaç, işverenleri riskin azaltılması konusunda kısmen sorumlu kılmaktır. (Bu kılavuz ile UMass Amherst ve Araştırma Destek Konsorsiyumu tarafından hazırlanan araç setleri bu noktada yardımcı olabilirler.) Araştırmanın tamamlanmasıyla yayın yapılması ya da medya içeriği üretilmesi planlanıyorsa araştırmacı, olası tepkilere karşı güvendiği meslektaşlarına başvurmalı ve kurumsal anlamda nasıl destek sağlayacaklarını soruşturmalıdır.

B. Kurumlara Yönelik Başarılı Uygulama Örnekleri

Araştırma kurumlarının, çevrim içi taciz ve yıldırma biçimlerinin kamuya dönük araştırma yapan akademisyenler açısından bir mesleki risk olduğunu kabul etmesi gerekmektedir. Bu nedenle, bu akademisyenlere kurumsal destek sözü vermek önemlidir. Her çözümsüz bırakılan taciz olayı, araştırmacı, kurum ve toplum üzerinde oldukça olumsuz sonuçlar doğuracaktır. Böyle durumlarda araştırmacılar, yardım, rehberlik ve kurumsal destek güvencesi için kurumlarına başvurabilmelidirler. UMass Amherst ve Araştırma Destek Konsorsiyumu gibi kurumlar, kriz durumunda araştırmacılarına yardımcı olmak üzere araç setleri geliştirmiştir. Bu setler, Bilgi Edinme Özgürlüğü Yasası (FOIA) kapsamındaki politika dokümanlarını, hazır formları, kontrol listelerini ve taciz sırasında yararlı olabilecek diğer evraklar dâhil çalışanları destekleyecek ayrıntılı tüm materyalleri sunmaktadır.

Bu araç setleri, proaktif önlemleri devreye almanın yapılacak planlamanın kendinden emin ve sağlıklı tepkiler geliştirmeye nasıl imkân tanıdığını vurgulamaktadır. Örneğin Araştırma Destek Konsorsiyumu, özellikle üniversiteler bünyesinde, iletişim uzmanları, güvenlik profesyonelleri, yöneticiler ve halkla ilişkiler personelinden oluşacak araştırma destek ekipleri kurulmasını şiddetle tavsiye etmektedir. Kriz anlarında, araştırmacılar ile onları destekleyen kurum(lar) arasındaki açık ve destekleyici iletişim biçimleri, kritik bir öneme sahiptir. Ayrıca medya, siyasetçiler, diğer kurumlar veya genel kamuoyu gibi dış paydaşlarla kurulacak tutarlı bir iletişime de ihtiyaç vardır. Kriz anları, araştırmacılar ve kurumlar için stresli süreçler anlamına gelse de ön hazırlık ve faydalı uygulamalar her iki taraf için zararı azaltma noktasında oldukça işlevsel bir rol oynayacaktır.

UMass Amherst'in araç seti, olası bir taciz durumunda öğretim üyeleri veya yüksek lisans öğrencilerinin genellikle ilk başvuracağı kişiler olan bölüm başkanlarına hitaben bir müdahale ve önleme rehberi sunmaktadır. Bu rehber, araştırmacıyla iletişim, destek sistemini devreye sokma, tacize verilecek yanıtı belirleme ile uzun vadeli önlemler ve hazırlık planları hakkında önerilerle doludur.

Araştırma Destek Konsorsiyumu, kurumların medya ilişkileri veya iletişim birimi web sitelerine trolleme, doxxing, taciz ve diğer riskler hakkında bilgilendirici kaynaklar eklemesini önermektedir. Bu, kamuya dönük akademisyenleri desteklemede küçük fakat yararlı bir adım olarak görülmelidir. İlgili kurumlar, söz konusu kaynaklara ek olarak araştırmacılarının yanında olduklarını belirten bir destek beyanı ekleyebilirler. Böyle yaprak araştırmacıların tacize maruz kaldıklarında kuruma başvurmaları gerektiğini ve kurumun kendilerine konu ile alakalı yardım sağlayacağını vurgulayacaklardır. Bunun yanında kurumlar, kamusal alanda risk barındıran çalışmaların zararlı sonuçlarını açıkça ele alan ve araştırmacıların kendilerini nispeten daha az savunmasız hissetmelerini sağlayacak alternatif araştırma yöntemlerine yönelik beyin fırtınasını teşvik eden atölyeler düzenleyebilirler.

C. Ders Verme Süreçleri

UMass Amherst araç seti, üniversitelerde ders veren araştırmacılar için de kullanışlı öneriler sunmaktadır. Ders materyallerinin yalnızca parola korumalı web sitelerinde paylaşılması yönünde temel bir tavsiyesi vardır. Buna ek olarak özellikle öğretim üyeleri, öğrencilerin ders materyallerinin telif hakkı kapsamında korunduğunu anlamasını sağlamalı; profesörün açık izni olmaksızın paylaşılmaması gerektiğini vurgulamalıdırlar. Telif hakkı koruması, ders oturumlarında yapılan kayıtlar için de geçerlidir. Çoğu üniversite, bu tür materyallerin izinsiz paylaşımını davranış kurallarının ihlali olarak değerlendirmektedir. Henüz geçerli böyle bir kural söz konusu değilse ilgili başka yönergeler hızlıca üretilmelidir. ABD'de profesörlerin ders izlencelerini çevrim içi yayınlama zorunluluğunun bulunduğu eyaletlerde, "eşitlik" veya "transgender" gibi anahtar kelimeleri içerikten çıkaran sadeleştirilmiş bir sürüm oluşturup tam sürümü yalnızca parola korumalı kampüs öğrenim yönetim sistemine yüklemeleri önerilmektedir.

9. Sonuç

Sonuç

Bu belge, yürüttükleri çalışmalar politik veya toplumsal açıdan tartışmalı içeriklerle, önde gelen kurum ya da devlet çıkarlarıyla veyahut da araştırmacının kendi marjinal kimlikleriyle çatıştığında, araştırmacıların hem çevrim içi hem de çevrim dışı ortamlarda karşı karşıya kaldıkları çok katmanlı riskleri tanımalarının ve yönetme becerileri geliştirmelerinin önemini vurgulamaktadır. Bir projenin tartışmalı bir konu içerip içermediğine, yanıltıcı ya da düşmanca gruplarla karşı karşıya kalma ihtimali taşıyıp taşımadığına ya da ayrıntılı incelemeler gerektiren büyük ölçekli veri setleri kullanmayı gerektirip gerektirmediğine bakılmaksızın, dikkatli bir planlama ve risk değerlendirme analizi yapma zorunluluğu bulunmaktadır. Bu rehber, veri koruma adımlarını gözeterek çalışma tasarlamaya, iletişim protokolleri oluşturmaya ve akıl ve ruh sağlığı kaynaklarına erişim sağlamaya yönelik stratejiler sunmaktadır. Ancak, bir araştırmacı ne kadar dikkatli olursa olsun, riskli araştırmanın sonuçlarından tamamen sakınması mümkün değildir.

Bireysel araştırmacılar kendilerini ne kadar hazırlarsa hazırlasınlar, "riskli araştırma"nın zorluklarını sağlam bir zeminde ele almak için kolektif çözümler ve kurumsal destek mekanizmaları oluşturmak hayati derecede öneme sahiptir. Bölümler, meslek birlikleri ve üniversiteler—yalnızca kriz anlarında değil—rutin biçimde sunacakları hukuki rehberlik, teknik destek ve psiko-sosyal bakım hizmetlerini devreye almadırlar. Buna, danışmanlık veya terapi için daha kapsamlı fon sağlamak, kurumsal inceleme kurulları ve etik kurullarla yakın çalışarak değişen dijital tehditlere uygun protokoller uyarlamak ve araştırmacılara taciz veya potansiyel zarar durumlarında izleyebilecekleri net prosedürler belirlemek dahildir. Bu yönde atılacak adımlar, akademisyenlerin risk yönetiminin yükünü tek başlarına taşımak zorunda kalmadıkları bir çalışma ortamı inşa edecektir.

Daha sağlıklı ve kapsayıcı bir araştırma ekosistemi oluşturmanın yolu, bireysel araştırmacıların, akademik toplulukların ve onlara yön veren kurumların ortak taahhüdünden geçmektedir. Güvenlik protokollerini, kurumsal politika değişikliklerini ve daha güçlü dayanışma ağlarını kolektif olarak destekleyerek aslında önemli meseleleri tartışmalı içeriklerine bakılmaksızın araştırma özgürlüğünü her koşulda korumuş olmaktayız. Sonuç olarak, riski kabul etmek ve ona yönelik planlama yapmak, araştırma sürecini tekil bir çabadan kolektif bir sorumluluğa dönüştürecek ve böylece titiz olduğu kadar çok daha duyarlı ve özenli bir akademik üretim sürecini mümkün kılacaktır.

10. Başvuru Kaynakları

A Kılavuzlar ve Araç Setleri

B Yerel Bazlı Kaynaklar

C Ücretli Hizmetler

D Akıl ve Ruh Sağlığı Kaynakları

Başvuru Kaynakları

A. Kılavuzlar ve Araç Setleri

Genel Kılavuzlar

- Araştırmacı Destek Konsorsiyumu (Researcher Support Consortium)
- Siber Sivil Haklar Girişimi Çevrim İçi Güvenlik Merkezi (Cyber Civil Rights Initiative Online Safety Center) *(mahrem görüntü istismarı mağdurları için)*
- VOX-Pol Araştırmacı Kaynakları
- Akademik Özgürlük Kriz Anı Araç Seti (Academic Freedom Crisis Toolkit)
- Benim Rızam Olmadan: Çevrim İçi Tacizle Mücadele Araç Rehberi (Without My Consent Tool Guide to Fight Online Harassment)
- Gözetimden Korunma: İpuçları ve Araçlar (Surveillance Self-Defense Tips and Tools)
- Günün Tabağı: Dijital Bakım Menüsü *(Dish of the Day: The Digital Care Meal — Portekizce, İspanyolca ve İngilizce sürümleri mevcuttur)*

Feminist Kılavuzlar

- Teknolojiyi Geri Al (Toplumsal Cinsiyete Dayalı Şiddeti Sona Erdirmek İçin Teknolojinin Kontrolünü Ele Al) – Take Back the Tech (Take Control of Technology to End Gender Based Violence)
- Feminist Yardım Hatları (Feminist Helplines) – Dijital Savunucular Ortaklığı (Digital Defenders Partnership)
- CFFP Kesişimsellik ve Siber Güvenlik Araç Seti – CFFP Intersectionality and Cybersecurity Toolkit
- Kamusal Akademik Faaliyete Katılın!: Feminist ve Erişilebilir İletişim İçin Bir Kılavuz, Ketchum 2022 – Engage in Public Scholarship!: A Guidebook on Feminist and Accessible Communication, Ketchum 2022
- Feminist ve Erişilebilir Yayıncılık, İletişim ve Teknolojiler – Feminist and Accessible Publishing, Communications, and Technologies
- Aktivistler İçin Siber Bakım Kiti (Kit de Cibercuidado para Activistas)

Gizlilik, Doxxing ve Taciz Kılavuzları

- Doxlandınız: Bundan Sonra Ne Yapmalısınız Rehberi – *So You've Been Doxed: A Guide on What to Do Next*
- Equality Labs'in Aktivistler İçin Anti-Doxing Rehberi – *Equality Labs' Anti-Doxing Guide for Activists*
- Saldırı Altındaki Aktivistler İçin Anti-Doxing Rehberi – *Anti-Doxing Guide for Activists Facing Attacks*
- Doxing Önleme ve Zarar Azaltma Eğitimi – *Doxing Prevention Harm Reduction Training*
- Aşırı Mahremiyet: Ortadan Kaybolmak İçin Gerekli Olanlar – Dördüncü Baskı. Kişisel Veri Silme Çalışma Kitabı, Sürüm 4.0, Temmuz 2022 [PDF] – *Extreme Privacy: What It Takes to Disappear, 4th Ed., Personal Data Removal Workbook, v. 4.0, July 2022*
- Zoom Bombardımanını Nasıl Önler ve Toplantılarınızı Nasıl Güvenceye Alırsınız – *How to Prevent Zoom Bombing and Secure Your Meetings*
- Gözetimden Korunma Kılavuzu ve Araştırmacılar İçin Öneriler – *Surveillance Self-Defense Guide (EFF) and Their Tips for Researchers*

- Spokeo Gibi Kişisel Bilgi Sitelerinden Elle Çıkış Yapma Kılavuzları – *Manual Opt-Out Guides for Personal Information Sites Like Spokeo*
- Sesini Yükselt ve Güvende Kal: Çevrim İçi Tacizden Korunma Rehberi – *Speak Up and Stay Safe: A Guide to Protecting Yourself from Online Harassment*
- PEN America'nın Çevrim İçi Taciz Saha El Kitabı – *PEN America's Online Harassment Field Manual*

Öz-Bakım ve Akıl ve Ruh Sağlığı Kılavuzları

- Gazeteciler İçin Dijital Güvenlik Kiti – Digital Safety Kit for Journalists
- SPJ Araç Kutusu: Gazeteciler İçin Akıl ve Ruh Sağlığı – SPJ Toolbox Mental Health for Journalists
- Gazeteciler İçin Öz-Bakım İpuçları – Self-Care Tips for Journalists
- Dijital Medyadan Kaynaklanan Dolaylı Travmayla Başa Çıkma Önerileri (Eyewitness Media, Internet Archive aracılığıyla) – Recommendations for Dealing with Vicarious Trauma from Digital Media (Eyewitness Media via Internet Archive)
- Gazetecilik ve Dolaylı Travma: Gazeteciler, Editörler ve Haber Kuruluşları İçin Rehber – Journalism and Vicarious Trauma: A Guide for Journalists, Editors, and News Organizations (First Draft News)
- Akıl ve Ruh Sağlığını Yönetme: Medya Aşırılıkçılığı Uzmanı ile Podcast Bölümü – Managing Mental Health Podcast Episode with Extremist Media Consultant
- Travmatik Görsellerle Başa Çıkma: Standart İşletim Prosedürü Geliştirme – Handling Traumatic Imagery: Developing a Standard Operating Procedure (Dart Center for Journalism & Trauma)

B. Yerel Bazlı Kaynaklar

Genel Kılavuzlar (Amerika Birleşik Devletleri)

- **Arizona**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Arkansas**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
  - ☐ *National Lawyers Guild* (Ulusal Avukatlar Birliği)
- **California**
  - ☐ *Safe at Home Address Confidentiality Program* (Evde Güvende—Adres Gizliliği Programı)
  - ☐ *TechLEAD*
  - ☐ *Citizens Privacy Coalition* (Vatandaş Gizliliği Koalisyonu)
- **Colorado**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Connecticut**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
  - ☐ *Yale Privacy Lab* (Yale Gizlilik Laboratuvarı)
- **Delaware**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **District of Columbia (D.C.)**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Florida**

- ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Georgia**
  - ☐ *Encode Justice Georgia* (Encode Justice Georgia)
- **Idaho**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Illinois**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Indiana**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Iowa**
  - ☐ *Safe at Home Program* (Evde Güvende Programı)
- **Kansas**
  - ☐ *Safe at Home Program* (Evde Güvende Programı)
- **Kentucky**
  - ☐ *Safe at Home Program* (Evde Güvende Programı)
- **Louisiana**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Maine**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Maryland**
  - ☐ *Safe at Home Program* (Evde Güvende Programı)
- **Massachusetts**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
  - ☐ *PrivaZy*
- **Michigan**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Minnesota**
  - ☐ *Safe at Home Program* (Evde Güvende Programı)
- **Mississippi**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Missouri**
  - ☐ *Safe at Home Program* (Evde Güvende Programı)
- **Montana**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Nebraska**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Nevada**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **New Hampshire**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **New Jersey**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
- **New Mexico**
  - ☐ *Safety at Home Program* (Evde Güvenlik Programı)
- **New York**
  - ☐ *Address Confidentiality Program* (Adres Gizliliği Programı)
  - ☐ *New York Cyber Abuse Task Force* (New York Siber İstismar Görev Gücü)
  - ☐ *Clinic to End Tech Abuse* (Teknolojik İstismarı Sona Erdirmek İçin Klinik)
  - ☐ *Black Movement Law Project* (Black Movement Hukuk Projesi)

- *Calyx Institute: Privacy by Design for Everyone* (Calyx Enstitüsü: Herkes İçin Tasarımla Gizlilik)
- *Surveillance Technology Oversight Project* (Gözetim Teknolojisi Denetim Projesi)

- **North Carolina**
  - *Address Confidentiality Program* (Adres Gizliliği Programı)
  - *Encode Justice NC* (Adaleti Tesis Etme, NC)
- **Ohio**
  - *Safety at Home Program* (Evde Güvenlik Programı)
- **Oklahoma**
  - *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Oregon**
  - *Address Confidentiality Program* (Adres Gizliliği Programı)
  - *PDX Privacy*
- **Pennsylvania**
  - *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Rhode Island**
  - *Address Confidentiality Program* (Adres Gizliliği Programı)
  - *Rhode Island Rights* (Rhode Island Hakları)
- **Tennessee**
  - *Safe at Home Program* (Evde Güvende Programı)
- **Texas**
  - *Alternate Address Program* (Alternatif Adres Programı)
- **Vermont**
  - *Safe at Home Program* (Evde Güvende Programı)
- **Virginia**
  - *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Washington (WA)**
  - *Address Confidentiality Program* (Adres Gizliliği Programı)
  - *Stop Surveillance City* (Gözetim Şehrini Durdurun)
  - *Technology Enabled Coercive Control Clinic* – Teknoloji Destekli Zorlayıcı Kontrol Kliniği *(aile içi şiddet mağdurlarına yönelik New Beginnings tarafından yürütülür)*
- **West Virginia**
  - *Address Confidentiality Program* (Adres Gizliliği Programı)
- **Wisconsin**
  - *Safety at Home Program* (Evde Güvenlik Programı)

Genel Kılavuzlar (Amerika Birleşik Devletleri Dışında)

- **AB (Avrupa Birliği)**
  - *Right to be forgotten* (Unutulma Hakkı)
- **Avustralya**
  - eSafety Commission *(bkz. "Find Out What We Can Do" – "Neler Yapabileceğimizi Öğrenin" bölümü)*
- **Hollanda**
  - **https://www.wetenschapveilig.nl/**: Çalışmaları nedeniyle tehditkâr, nefret dolu veya yıldırıcı tepkiler alan akademisyenler için kurulmuş ulusal bir platform
- **Fransa**

- PAUSE: Sansür ya da diğer politik, ekonomik veya toplumsal engeller nedeniyle kendi ülkesinde ya da ikamet ettiği ülkede araştırma yapamayan araştırmacılara yönelik bir program

Hukuki Hizmetler (Amerika Birleşik Devletleri)

- *Cyber Civil Rights Legal Project* — Siber Sivil Haklar Hukuk Projesi
- *Without My Consent's Copyright Registration Guide* — Telif Hakkı Tescil Rehberi
- *Without My Consent's Guide to State Laws — 50 State Project Regarding Laws Against the Non-Consensual Distribution of Sexually Explicit Images* — 50 Eyalet Projesi: Müstehcen Görüntülerin Rıza Dışı Dağıtımına Karşı Eyalet Yasaları Rehberi
- *Stop Non-Consensual Intimate Image Abuse* — Rıza Dışı Mahrem Görüntü İstismarını Durdurun
- *The Foundation for Individual Rights and Expression (*FIRE) — Bireysel Haklar ve İfade Vakfı
- *Faculty Legal Defense Fund (FIRE)* — Öğretim Üyeleri Hukuk Savunma Fonu
- *FIRE's Guide to Student Fees, Funding, and Legal Equality on Campus* — FIRE Rehberi: Kampüste Öğrenci Ücretleri, Fonlama ve Hukuki Eşitlik
- *American Civil Liberties Union (ACLU)* — Amerikan Sivil Özgürlükler Birliği
- *Electronic Frontier Foundation (EFF*) — Elektronik Sınır Vakfı
- *Tufts Cybersecurity Clinic for the Public* Good — Tufts Kamu Yararına Siber Güvenlik Kliniği

Hukuki Hizmetler (Amerika Birleşik Devletleri Dışında)

Birleşik Krallık

- Revenge Porn Helpline – *İntikam Pornosu Yardım Hattı*

C. Ücretli Hizmetler

360 Privacy
Çevrim içi veri kaldırma, dark web izleme vb.
ReputationDefender by Norton
Arama sonuçlarını kaldırma, kişisel bilgileri silme vb.
DeleteMe
Kişisel bilgilerinizi Spokeo ve benzeri sitelerden, kişi bulma servislerinden ve kamu kayıt arama sitelerinden kaldırır. (129 ABD$/yıl)
Kanary
Sizi riske atabilecek herhangi bir web sitesinden gereksiz kişisel verilerinizi bulur ve siler. (179,88 ABD$/yıl)
Not: Bu tür hizmetlerin ücretini bölümünüzün veya okulunuzun karşılamasını talep etmeyi ya da hibe başvurularınıza dâhil etmeyi düşünebilirsiniz. Başkalarıyla (eş, aile üyesi, ev arkadaşı vb.) birlikte yaşıyorsanız, onların kayıtlarında sizi bulmak için kullanılabilecek konum bilgileri yer alabilmektedir. Mümkünse, benzer hizmetleri onlar için de satın almayı değerlendirin.

D. Akıl ve Ruh Sağlığı Kaynakları

Kriz veya Yardım Hatları

Herhangi bir yardım hattını aramadan önce aşağıdakileri göz önünde bulundurunuz:

- Çalışma saatleri nedir?
- Arama ücretsiz mi, yoksa bir ücret talep ediliyor mu?
- Görüşme gizli mi? Örneğin, birçok hizmet, arayanın intihar girişiminden söz etmesi ya da kendine zarar verme planı belirtmesi durumunda izlenecek protokollere sahiptir.
- Hat meşgulse ne yapılmalı? Genellikle birkaç kez denemek, daha sonra tekrar aramak veya alternatif hizmetleri araştırmak bu noktada iyi olacaktır.
- Telefonda konuşmaktan rahatsız oluyorsanız yazışma (SMS veya mesaj) hatlarını değerlendiriniz. Çoğu ülke genelinde bu hizmet mevcuttur.

Dünya Çapında

- *International Directory of Helplines* — Uluslararası Yardım Hatları Dizini
- *Feminist Helplines Index* — Feminist Yardım Hatları Dizini

Brezilya

- *Centro de Valorização da Vida* – 24 saat destek
    - 188 numarasını arayın

Birleşik Krallık

- *NHS* – 7/24 destek
    - 111
- *Samaritans* – 7/24 destek
    - Telefon: 116 123
    - E-posta: jo@samaritans.org
- Yaşamı Sürdürme Kampanyası (CALM) – Her gün 17.00-24.00
    - 0800 58 58 58
- *Shout* Yazışma Hattı – Arama gerekmez
    - 85258 numarasına SHOUT yazıp gönderin

Avustralya

- *Lifeline* – 24 saat danışmanlık, destek grupları ve intiharı önleme hattı
    - Telefon: 13 11 14 | SMS: 0477 13 11 14 | Çevrim içi sohbet
- *Suicide Call Back Service* – İntihardan Vazgeçme 24 saat destek hattı
    - 1300 659 467
- *Beyond Blue* – Depresyon ve anksiyete desteği
    - 1300 22 46 36 (24 saat) | Çevrim içi sohbet
- *Head to Health* – Yönlendirme ve yerel akıl ve ruh sağlığı hizmetleri
    - 1800 595 212
- *MensLine Australia* – Erkekler için 24 saat çevrim içi danışmanlık
    - 1300 78 99 78 | Çevrim içi sohbet

Avrupa Birliği

- Üye ülkelerdeki ulusal yardım hatları listesi
- Aşağıdaki numaralar tüm AB ülkelerinde geçerlidir:

- Samaritans: 116 123
- Give Us a Shout SMS hattı: 85258 numarasına SHOUT yazın
- CALM: 0800 58 58 58

Amerika Birleşik Devletleri

- Acil durum: 911
- 988 İntihar ve Kriz Hattı – Arayın veya mesaj atın: 988
- Disaster Distress Helpline – Arayın veya mesaj atın: 1-800-985-5990
- SAMHSA Ulusal Yardım Hattı – 1-800-662-HELP (4357)
- Akıl ve Ruh Sağlığı Ulusal İttifakı (NAMI)
  - Telefon: 1-800-950-NAMI (6264)
  - SMS: 62640 numarasına HelpLine yazın
  - E-posta: helpline@nami.org
- Crisis Text Line – 741741 numarasına HOME yazıp gönderin
- Amerikan Psikoloji Derneği – Kriz hatları ve kaynaklar

Akıl ve Ruh Sağlığı Uzmanı Bulma

- **Dünya Çapında**
  - International Therapist Directory – Uluslararası Terapist Dizini
  - It's Complicated – Dünya genelindeki büyük şehirler için kapsamlı terapist rehberi
- **Avustralya**
  - Psychologist Locator – Psikolog Bulucu
  - Finding Affordable Mental Health Help in Australia – Avustralya'da Uygun Maliyetli Akıl ve Ruh Sağlığı Desteği Bulma
- **Avrupa Birliği**
  - European Association for Behavioral and Cognitive Therapists – Avrupa Davranışsal ve Bilişsel Terapistler Derneği
- **Birleşik Krallık**
  - Finding Free or Low-Cost Therapy in the UK – Birleşik Krallık'ta Ücretsiz veya Düşük Maliyetli Terapi Bulma
  - Counselling Directory – Danışmanlık Dizini
  - BACP Therapist Directory – BACP Terapist Dizini
- **Amerika Birleşik Devletleri**
  - Psychiatrist Locator – Psikiyatrist Bulucu
  - Psychologists by State – Eyalete Göre Psikologlar
  - Mayo Clinic (ND) Tips for Finding Mental Health Providers – Mayo Clinic (ND) Akıl ve Ruh Sağlığı Uzmanı Bulma İpuçları
  - National Alliance for Mental Illness – Finding a Mental Health Professional – Ulusal Akıl ve Ruh Sağlığı İttifakı (NAMI) – Akıl ve Ruh Sağlığı Uzmanı Bulma

Sosyal Hizmet

- Clinical Social Work Association – Klinik Sosyal Hizmet Derneği
- Association of State Licensing Boards – Eyalet Lisans Kurulları Birliği
- National Association of Social Workers – Ulusal Sosyal Hizmet Uzmanları Derneği

Hemşirelik

- American Psychiatric Nurses Association – Amerikan Psikiyatri Hemşireleri Derneği

Ruh Sağlığı Danışmanlığı

- Psychology Today – Psychology Today (terapist arama dizini)

11. İlgili Okumalar

A Sansür

B Cinsiyet Ayrımcılığına Dayalı Taciz

C Kurumsal Yanıtlar

D Çevrimiçi Taciz

E Araştırma Etiği ve Yöntemleri

F Güvenlik

G Akademisyenlere Yönelik Destek

- # İlgili Okumalar

A. Sansür

Tanczer, L.M., Deibert, R.J., Bigo, D., Franklin, M., Melgaço, L., Lyon, D., Kazansky, B., & Milan, S. (2020). Online Surveillance, Censorship, and Encryption in Academia, I*nternational Studies Perspectives, 21*(1), 1–36. https://doi.org/10.1093/isp/ekz016

Tanczer, L., McConville, R., & Maynard, P. (2016). Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics. *Journal of Global Security Studies*, *1*(4), 346-355.

B. Toplumsal Cinsiyete Dayalı Taciz

Binder, Ines and Hache, Alexandra. (2023). "A Feminist Conversation on Cyber-Security," GenderIt.org, https://www.genderit.org/editorial/feminist-conversation-cybersecurity

Citron, Danielle Keats. (2009). Law's Expressive Value in Combating Cyber Gender Harassment. *Michigan Law Review,* 108: 373-415.

Eckert, S., & Riftkin-Metzger, J. (2020). Doxxing, privacy and gendered harassment: The shock and normalization of veillance cultures. *M&K Medien & Kommunikationswissenschaft, 68*(3), 273-287. https://doi.org/10.5771/1615-634X-2020-3-273

Haché, A., Fong, M., Jiménez, G., & Sánchez, M. (2022). *Digital security and feminist holistic protection as part of temporary relocation programmes for Human Rights Defenders*.

Hodson, J., Gosse, C., Veletsianos, G., & Houlden, S. (2018). I get by with a little help from my friends: The ecological model and support for women scholars experiencing online harassment. *First Monday* 23(8).

Jane, E. A. (2018). Gendered cyberhate as workplace harassment and economic vandalism. *Feminist Media Studies, 18*(4), 575–591. https://doi.org/10.1080/14680777.2018.1447344

Linabary, J. and Batti, B. (2019). "'Should I Even Be Writing This?': Public Narratives and Resistance to Online Harassment," in *Gender Hate Online: Understanding the New Antifeminism*, ed. Debbie Ging and Eugenia Siapera (Cham: Palgrave Macmillan), 317–46.

Pevac, M. (2022). The darker side of feminist scholarship: How online hate has become the norm. *Feminist Media Studies*, 22(5), 1287–1289.

Rentschler, C. (2017) Bystander intervention, feminist hashtag activism, and the anti- carceral politics of care. *Feminist Media Studies*, 17(4), 565-584, DOI: 10.1080/14680777.2017.1326556

Sobieraj, S. (2018). Bitch, slut, skank, cunt: Patterned resistance to women's visibility in digital publics. *Information, Communication & Society*, 21(11), 1700–1714.

Sobieraj, S. (2020). *Credible Threat: Attacks Against Women Online and the Future of Democracy*. Oxford University Press.

C. Kurumsal Yanıtlar

Gosse, C., O'Meara, V., Hodson, J., & Veletsianos, G. (2023). Too rigid, too big, and too slow: institutional readiness to protect and support faculty from technology facilitated violence and abuse. *Higher Education* 87: 923-941.

D. Çevrim İçi Taciz

Cocq, C.; Liliequist, E.; Okonski, L. Protecting the Researcher in Digital Contexts. Proceedings of the 6th Digital Humanities in the Nordic and Baltic Countries Conference (DHNB 2022): 195-202. https://ceur-ws.org/Vol-3232/paper16.pdf

Ferber, A. L. (2018)."“Are you willing to die for this work?” Public targeted online harassment in higher education: SWS presidential address." *Gender & Society*, 32 (3), 301- 320.

Gosse, C., Veletsianos, G., Hodson, J., Houlden, S., Dousay, T. A., Lowenthal, P. R., & Hall, N. (2021). The hidden costs of connectivity: nature and effects of scholars' online harassment. *Learning, Media and Technology*, 46(3), 264-280.

Marwick, A. E. (2021). Morally Motivated Networked Harassment as Normative Reinforcement. *Social Media & Society*, 7(2). https://doi.org/10.1177/20563051211021378

Phillips, W. (2015). *This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture*. MIT Press.

E. Araştırma Etiği ve Yöntemleri

Ashe, S. D., Busher, J., Macklin, G., & Winter, A. (2020). *Researching the far right: Theory, method and practice.* Routledge.

Briant, Emma, L. (2024) Researching and Conceptualizing the Influence Industry. In: Emma L. Briant & Vian Bakir (Eds.) (2024). *The Routledge Handbook of the Influence Industry*. London: Routledge. Pp 379-394.

Conway, M. (2021). Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines, *Terrorism and Political Violence, 33*(2), 367-380, DOI: 10.1080/09546553.2021.1880235

Damhuis, K., & de Jonge, L. (2022). Going Nativist. How to Interview the Radical Right? *International Journal of Qualitative Methods*, 21. https://doi.org/10.1177/16094069221077761

Dickson-Swift, V., James, E. L., Kippen, S., & Liamputtong, P. (2008). Risk to researchers in qualitative research on sensitive topics: Issues and strategies. *Qualitative Health Research, 18*(1), 133–144

Kaul, A., Chavendera, D. D., Saunders, K., & Paphitis, S. A. (2024). Improving Emotional Safety, Coping, and Resilience Among Women Conducting Research on Sexual and Domestic

Violence and Abuse. *Journal of Interpersonal Violence, 39*(5-6), 1327-1350. https://doi.org/10.1177/08862605231207617

Lee-Treweek, G., & Linkogle, S. (2000). *Danger in the field: Risk and ethics in social research.* Psychology Press.

Moncur, W. (2013). The emotional wellbeing of researchers: considerations for practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1883-1890). https://dl.acm.org/doi/10.1145/2470654.2466248

Ong, J.C. (2020). "Limits and Luxuries of Slow Research in Times of Radical War: How Should We Represent Perpetrators?" *Journal of Digital War 1*(1): 1-6.

Pearce, K. E. (2020). Unintended consequences of using digital methods in difficult research sites. In B. Foucault Welles & S. Gonzalez-Bailon (Eds.), *The Oxford handbook of networked communication*. (pp. 577-598). Oxford University Press. http://doi.org/10.1093/oxfordhb/9780190460518.013.26

Pollard, A. (2009). Field of screams: difficulty and ethnographic fieldwork. *Anthropology Matters*, 11(2).

Schrag, Z. (2010). *Ethical Imperialism*. Johns Hopkins University Press. https://doi.org/10.1353/book.471.

Toscano, E. (Ed.). (2019). *Researching Far-Right Movements: Ethics, Methodologies, and Qualitative Inquiries. Routledge*. https://doi.org/10.4324/9780429491825

Van Baalen, S. (2018). 'Google wants to know your location': The ethical challenges of fieldwork in the digital age. *Research Ethics*, 14(4), 1-17.

Vaughan, A., Braune, J., Tinsley, M., & Mondon, A. (2024). *The ethics of researching the far right: Critical approaches and reflections*. Manchester University Press.

Voss, G. (2012). 'Treating it as a normal business': Researching the pornography industry. *Sexualities*, 15(3–4), 391–410. https://doi.org/10.1177/1363460712439650

F. Güvenlik

Garfinkel, S. L. 2018. "Privacy and Security Concerns When Social Scientists Work with Administrative and Operational Data." *The Annals of the American Academy of Political and Social Science* 675 (1): 83–101. https://doi.org/10.1177/0002716217737267.

Hilhorst, D. J. M., Hodgson, L., Jansen, B., & Mena, R. (2016). *Security guidelines for field researchers in complex, remote and hazardous places*. International Institute of Social Studies.

Pearson, E., Whittaker, J., Baaken, T., Zeiger, S., Atamuradova, F., & Conway, M. (2023). *Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field.* Vox-Pol Researcher Security, Safety, and Resilience Project (REASSURE).

Smith, C. H., Ó Cluanaigh, D., Ravi, A.G., & Steudtner, P. (2016). “Holistic Security: A Strategy Manual for Human Rights Defenders.” *Tactical Technology Collective*.

G. Akademisyenlere Yönelik Destek

Haney-Caron, Emily; Goldstein, Naomi E.; and DeMatteo, David (2015) "Safe From Subpoena? The Importance of Certificates of Confidentiality to the Viability and Ethics of Research," *Akron Law Review*: Vol. 48 : Iss. 2 , Article 5.

Houlden, S., Hodson, J., Veletsianos, G., Gosse, C., Lowenthal, P., Dousay, T., & Hall, N. C. (2022). Support for scholars coping with online harassment: An ecological framework. *Feminist Media Studies*, 22(5), 1120-1138.

San Roman Pineda, I., Lowe, H., Brown, L. J., & Mannell, J. (2022). Viewpoint: acknowledging trauma in academic research. *Gender, Place & Culture*, 30(8), 1184–1192. https://doi.org/10.1080/0966369X.2022.2159335

Kaynakça

Amnesty International. (2018). #toxictwitter: Violence and Abuse Against Women Online (No. ACT 30/8070/2018). Amnesty International. https://www.amnestyusa.org/wp-content/uploads/2018/03/Toxic-Twitter.pdf

Briant, E. L. (2023a). Hack Attacks: How Cyber Intimidation and Conspiracy Theories Drive the Spiral of 'Secrecy Hacking'. in Steel, J and Petley, J. Routledge Companion To Freedom of Expression and Censorship, London: Routledge.

Briant, E.L. (2023b). Hacking is far more than a security issue. It chills free speech. Index on Censorship.

Briant, E. L. (2024). Researching and Conceptualizing the Influence Industry. In: Emma L. Briant & Vian Bakir (Eds.) (2024). The Routledge Handbook of the Influence Industry. London: Routledge. Pp 379-394.

CERN. (2020). Computer Security: Blackmailing Academia: Back to pen and paper? CERN. https://home.cern/news/news/computing/computer-security-blackmailing-academia-back-pen- and-paper

Chess, S., & Shaw, A. (2015). A Conspiracy of Fishes, or, How We Learned to Stop Worrying About #GamerGate and Embrace Hegemonic Masculinity. Journal of Broadcasting & Electronic Media, 59(1), 208–220. https://doi.org/10.1080/08838151.2014.999917

Citron, D. K. (2023). How to fix section 230. Boston University Law Review, 103(3), 713–761.

Demery, A.-J. C., & Pipkin, M. A. (2020). Safe fieldwork strategies for at-risk individuals, their supervisors and institutions. Nature Ecology & Evolution, 5(1), 5–9. https://doi.org/10.1038/s41559- 020-01328-5

Doerfler, P., Forte, A., De Cristofaro, E., Stringhini, G., Blackburn, J., & McCoy, D. (2021). "I'm a Professor, which isn't usually a dangerous job": Internet-facilitated Harassment and Its Impact on Researchers. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), 341:1-341:32. https://doi.org/10.1145/3476082

European Commission. (2024, December 10). Delegated Regulation on data access provided for in the Digital Services Act [Text]. European Commission -Have Your Say. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13817-Delegated-Regulation-on-data-access-provided-for-in-the-Digital-Services-Act_en

Eyewitness Media Hub. (2015). "New research details full impact of graphic images on newsrooms – and how to cope." Eyewitness Media Hub, now hosted by First Draft News. https://firstdraftnews.org/articles/new-research-details-full-impact-of-graphic-images-on-newsrooms-and-how-to-cope-with-it/

Gelashvili, T., & Gagnon, A. (2024). One of the Boys: On Researching the Far Right as a Woman. Studies in Conflict & Terrorism, 0(0), 1–22. https://doi.org/10.1080/1057610X.2024.2361953 Gewin, V. (2021). Pandemic burnout is rampant in academia. Nature, 591 (7850), 489.

Halavais, A. (2019). Overcoming terms of service: a proposal for ethical distributed research. Information, Communication & Society, 22(11), 1567–1581. https://doi.org/10.1080/1369118X.2019.1627386

Halpern, M. (2015). Freedom to Bully: How Laws Intended to Free Information are Used to Harass Researchers. Center for Science and Democracy. https://www.ucs.org/resources/freedom-bully

Haney-Caron, E., Goldstein, N. E., and DeMatteo, D. (2015). Safe From Subpoena?
The Importance of Certificates of Confidentiality to the Viability and Ethics of Research. Akron Law Review: Vol. 48 : Iss. 2 , Article 5.

Hendry, N. H. (2021). Sextortion. In K. Miller & K. Wendt (Eds.), The Fourth Industrial Revolution and Its Impact on Ethics (pp. 315–320). Springer International Publishing. https://doi.org/10.1007/978-3-030-57020-0_23

Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. Technological Forecasting and Social Change, 163, 120426. https://doi.org/10.1016/j.techfore.2020.120426

Kittrie, O. F. (2015). Lawfare: Law as a weapon of war. Oxford University Press.

Lee, J. J., & Miller, S. E. (2013). A Self-Care Framework for Social Workers: Building a Strong Foundation for Practice. Families in Society, 94(2), 96-103. https://doi.org/10.1606/1044-3894.4289

Logan, T. (2023). Online Stalking Experiences and Harms Among Female Acquaintance Stalking Victims. Victims & Offenders, 1–21. https://doi.org/10.1080/15564886.2023.2172503

Logan, T., & Showalter, K. (2023). Work Harassment and Resource Loss Among (Ex)partner Stalking Victims. Journal of Interpersonal Violence, 38(1-2), 1060-1087. https://doi.org/10.1177/08862605221086649

Loyle, C. E., & Simoni, A. (2017). Researching under fire: Political science and researcher trauma. PS: Political Science & Politics, 50(1), 141–145.

Marwick, A. E. (2023). The private is political: networked privacy and social media. Yale University press.

Marwick, A. E., Blackwell, L., & Lo, K. (2016). Best practices for conducting risky research and protecting yourself from online harassment (Data & Society Guide). New York: Data and Society Research Institute. https://datasociety.net/pubs/res/Best_Practices_for_Conducting_Risky_Research-Oct-2016.pdf

Massanari, A. L. (2018). Rethinking Research Ethics, Power, and the Risk of Visibility in the Era of the "Alt-Right" Gaze. Social Media + Society, 4(2). https://doi.org/10.1177/2056305118768302

Mattheis, A. A., & Kingdon, A. (2021). Does the Institution Have a Plan for That? Researcher Safety and the Ethics of Institutional Responsibility. In A. Lavorgna & T. J. Holt (Eds.), Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches (pp. 457–472). Springer International Publishing. https://doi.org/10.1007/978-3-030-74837-1_23

Molas, B. (2024). Doxing: A Literature Review [ICCT Project Report]. International Centre for Counter-Terrorism. https://icct.nl/sites/default/files/2025-01/Molas_Doxing%20A%20Literature%20Review.pdf.

Moran, R. J., & Asquith, N. L. (2020). Understanding the vicarious trauma and emotional labour of criminological research. Methodological Innovations, 13(2). https://doi.org/10.1177/2059799120926085

Murguía Burton, Z.F. & Cao, X.E. (2022). Navigating mental health challenges in graduate school. Nat Rev Mater 7, 421–423. https://doi.org/10.1038/s41578-022-00444-x

Newman, E., Simpson, R., & Handschuh, D. (2003). Trauma exposure and post-traumatic stress disorder among photojournalists. Visual Communication Quarterly, 10(1), 4–13. https://doi.org/10.1080/15551390309363497

Nicholls, H., Nicholls, M., Tekin, S., Lamb, D., & Billings, J. (2022). The impact of working in academia on researchers' mental health and well-being: A systematic review and qualitative meta- synthesis. PLOS ONE, 17(5). https://doi.org/10.1371/journal.pone.0268890

Ortutay, B. (2021). Facebook shuts out NYU academics' research on political ads. AP News August 4, 2021. https://apnews.com/article/technology-business-5d3021ed9f193bf249c3af158b128d18

Payne, R., Martin, B. A., Tuzovic, S., & Wang, S. (2023). Defining biometrics with privacy and benefits: A research agenda. Australasian Marketing Journal, 31(4), 294-302.

Pearson, E., Whittaker, J., Baaken, T., Zeiger, S., Atamuradova, F., & Conway, M. (2023). Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field. Vox- Pol Researcher Security, Safety, and Resilience Project (REASSURE).

Rager, K.B. (2005). Compassion Stress and the Qualitative Researcher. Qualitative Health Research, 15 (3), 423-430. doi:10.1177/1049732304272038

Rager, K. B. (2005). Self-Care and the Qualitative Researcher: When Collecting Data Can Break Your Heart. Educational Researcher, 34 (4), 23-27. https://doi.org/10.3102/0013189X034004023

Rentschler, C. (2017) Bystander intervention, feminist hashtag activism, and the anti-carceral politics of care. Feminist Media Studies, 17(4), 565-584, DOI: 10.1080/14680777.2017.1326556

Schulz, P., Kreft, A.-K., Touquet, H., & Martin, S. (2023). Self-care for gender-based violence researchers – Beyond bubble baths and chocolate pralines. Qualitative Research, 23(5), 1461–1480. https://doi.org/10.1177/14687941221087868

Segers, I. B., Gelashvili, T., & Gagnon, A. (2024). Intersectionality and care ethics in researching the far right. Feminist Media Studies, 24(5), 1219–1224. https://doi.org/10.1080/14680777.2023.2280884

Sobieraj, S. (2020). Credible Threat: Attacks Against Women Online and the Future of Democracy. Oxford University Press.

Steadman, C. (2023). Remembering and anticipating researcher vulnerability: an autoethnographic tale. Journal of Marketing Management, 39 (9–10), 807–828. https://doi.org/10.1080/0267257X.2022.2158905

Sun, H., Yuan, C., Qian, Q., He, S., & Luo, Q. (2022). Digital resilience among individuals in school education settings: a concept analysis based on a scoping review. Frontiers in psychiatry, 13, 858515.

Suzor, N., Dragiewicz, M., Harris, B., Gillett, R., Burgess, J., & Van Geelen, T. (2019). Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online. Policy & Internet, 11(1), 84–103. https://doi.org/10.1002/poi3.185

Vaughan, A. (2021, September 15). Problematising Ethics and Individual Responsibility for Researchers Studying the Far Right. AoIR Selected Papers of Internet Research. AoIR 2021. https://doi.org/10.5210/spir.v2021i0.12135

Vera-Gray, F. (2017) 'Talk about a Cunt with too Much Idle Time': Trolling Feminist Research." Feminist Review 115(1), 61-78.https://doi.org/10.1057/s41305-017-0038-y

Wolf, L. E., Dame, L. A., Patel, M. J., Williams, B. A., Austin, J. A., & Beskow, L. M. (2012). Certificates of Confidentiality: Legal Counsels' Experiences with and Perspectives on Legal Demands for Research Data. Journal of Empirical Research on Human Research Ethics, 7(4), 1–9. https://doi.org/10.1525/jer.2012.7.4.1

Teşekkür

Uzman hakemlerimiz Adrienne Massanari ve Beatrys Rodrigues'e; Dafna Kaufman ile Jacob Smith'in bu projedeki çalışmalarını finanse eden North Carolina Üniversitesi Bilgi, Teknoloji ve Kamusal Yaşam Merkezi'ne (CITAP); ve Alice Marwick'in bu projedeki çalışmalarını finanse eden Princeton Üniversitesi Bilgi Teknolojisi Politikaları Merkezi'ne teşekkür ederiz. Editoryal katkı, Data & Society Araştırma Enstitüsü'nden Kiara Childs tarafından sağlanmıştır. Mizanpaj ve tasarım CITAP'ten Felicity Gancedo ve Ifeoma Obioha tarafından gerçekleştirilmiştir; bu katkıları için hem Data & Society hem de CITAP'e teşekkür ediyoruz. Bu çalışmaya ilham veren tüm AoIR topluluğuna ve Riskli Araştırma Çalışma Grubu'nun geçmiş, şimdiki ve gelecekteki üyelerine özellikle minnettarız.