GÜVENCESİZLİK VE GAZETECİLERİN DİJİTAL GÜVENLİĞİ

Dr. Sarphan Uzunoğlu
Mine Bertan Yılmaz

Bu rapor The Guardian Foundation ve İsveç Uluslararası Kalkınma Ajansı (SIDA) tarafından desteklenen bir eğitim ve araştırma projesinin parçası olarak yayınlanmıştır. Bu raporun içeriğinin sorumluluğu tamamen Dijital Medya Araştırmaları Derneği'ne aittir ve hiçbir koşulda The Guardian Foundation ve SIDA'nın duruşunu yansıtmamaktadır.

Raporda neler var?

RAPOR ÖZETİ

En basit haliyle, belirsiz, öngörülemeyen ve riskli bir çalışma şekli olarak tanımlanabilecek güvencesiz çalışma, gazetecilik sektöründe her geçen yıl yaygınlaşıyor. Küresel trendlere ve dijitalleşmeye bağlı olarak, Türkiye'deki gazetecilik sektöründe de güvencesiz çalışma koşulları giderek derinleşiyor. Sektörde siyasi ve ekonomik nedenlerle artan işsizlik, dijitalleşmeyle birlikte hız kazanırken bu durum, serbest çalışan gazeteci sayısında bir artış meydana getirmekte. Profesyonel haber odalarına ek olarak, yarı profesyonel veya amatör çalışan ve Türkiye kamuoyuna seslenen fakat Türkiye dışında faaliyet gösteren dijital haber merkezleri de genellikle güvencesiz emek paterninde rol oynamakta. Bu koşullar dijital haber odaları için içerik üreten serbest gazetecilerin dijital güvenliğine odaklanmayı değerli kılıyor. Bu çalışma, yurtdışındaki haber odalarına telifli içerik üreten serbest gazeteciler, yurtdışında faaliyet gösteren haber odalarının editörleri ve dijital güvenlik eğitmenleri ile yapılan derinlemesine görüşmelerden yola çıkarak, Türkiye'deki haber üretim süreçlerinin dijitalleşmesinin ve güvencesiz çalışma ilişkilerinin neden olduğu güvensizliğin çerçevesini çizmeyi amaçlıyor.

Bu çalışmada, haber merkezlerinde güvencesiz işgücü ve bilgi güvenliği ile ilgili çalışmalardan yararlanılmış ve dijital güvenlik ve güvencesizlik arasındaki ilişki, serbest gazeteciler gibi niş bir örneklem üzerinden ele alınmıştır. Yedi serbest gazeteci, iki haber odası editörü ve beş dijital güvenlik eğitmeniyle yapılan derinlemesine görüşmelerden yola çıkarak, haber üretim süreçlerindeki dijitalleşmenin ve güvencesiz çalışma ilişkilerinin neden olduğu "güvensizliğin" çerçevesinin çizilmesi amaçlanmıştır.

Yöntem olarak yarı-yapılandırılmış derinlemesine görüşmelere dayalı keşifsel bir yaklaşımı benimseyen bu araştırmanın öne çıkan bulguları şu şekilde:

- Serbest gazetecilerin "kendilerini güvensiz hissettiren" güvencesiz çalışma koşulları nedeniyle birçok dijital güvenlik kaygısı olmasına rağmen, dijital güvenlik konusundaki farkındalıkları kendilerini korumaları için yeterli değil.
- Serbest gazeteciler haber yaparken çoğunlukla kendilerini risk altında hissediyorlar.
- Serbest gazeteciler Türkiye'deki yasal çerçeve nedeniyle finansal mahremiyet ve dijital güvenlik konusunda çaresiz hissediyorlar ve bunu etik bir meseleden ziyade pratik bir mesele olarak görüyorlar.
- Serbest gazetecilerin güvenliksiz hissettiği durumlarda anonim kalma ve takma isim kullanma konusunda ortak bir görüşü yok.
- Şifreli yazılım kullanan gazeteciler, sadece hassas belgeler üzerinde çalışırken bu yazılımlardan faydalanıyorlar. Dolayısıyla dijital güvenliği daha çok hassas konular üzerinde çalışırken önemsiyorlar.
- Serbest gazeteciler arasında hangi uygulamanın veya aracın güvenli olup olmadığı konusunda ortak bir anlayış yok; güvenli olduklarını varsayarak çeşitli araçlar kullanıyorlar fakat bu uygulamaların veya hizmetlerin nasıl tamamen güvenli bir şekilde kullanılacağı hakkında derin bir kavrayışa sahip değiller.
- Serbest gazeteciler aldıkları dijital güvenlik eğitimlerinin Batılı uygulamalar ve eğitim materyalleri tarafından şekillendirildiğine ve eğitimlerin Türkiye'nin kısıtlı medya ortamı ve yasal çerçevesinin yarattığı farklı ihtiyaçlar dikkate alınarak yeterince yerelleştirilmediğine inanıyorlar.
- Serbest gazetecilerin çoğu, polis müdahalesinin her an, her yerde mümkün olması nedeniyle şifreli güvenlik önlemlerinin kendileri için tehdit oluşturacağını düşünüyor.

- Haber odası editörleri/yöneticileri, dijital güvenlik konusunda inisiyatifi çoğunlukla gazetecilere bırakıyorlar. Çeşitli eğitimlerin verildiği söylense de muhabirler işverenlerle aynı fikirde değil.
- Editörler dijital güvenliğin öneminin farkındalar ancak risklerle etkili bir şekilde baş etme yöntemleri yeterli görünmüyor.
- Gazeteciler dijital güvenlik eğitimlerine yeterli ilgi göstermiyor, gösterse de bildiklerini uygulamak konusunda çekinceleri var.
- Dijital güvenlik eğitmenleri de çeşitli güvenlik tehditleri hissediyorlar ve bu yüzden ya halka açık eğitim vermekten imtina ediyor ya da eğitimlerde otosansür uyguluyorlar.

Hem eğitmenlerin hem de gazetecilerin eğitimlerle ilgili ifadeleri, eğitim içeriklerinin ve yöntemlerinin katılımcılardan alınan geri bildirimlerle geliştirilmesi gerektiğini gösteriyor.

GAZETECİLİKTE GÜVENCESİZLİK

Gazetecilik sektörü, son yıllarda ekonomik modellerde meydana gelen belirsizlik, dijital gelişmelere entegrasyon konusundaki problemler ve Google ve Facebook gibi büyük teknoloji firmalarının pazardaki etkisi gibi çeşitli faktörler nedeniyle büyük bir geçiş dönemi yaşamaktadır. Yeni rekabet koşullarına adapte olamayan haber odaları ya kapanmakta ya da bütçe kesintileri ile karşı karşıya kalmaktadır. Bu durum daha az gazetecinin daha az kaynakla çalışmasına neden olmaktadır (Hunter, 2015; Brake, 2017).

Gazetecilik sektörünün siyasi, teknolojik ve finansal dönüşümüne ilişkin en yaygın söylem, "kriz" söylemidir. Batı dünyasının "krizdeki gazetecilik" anlatısı, kamusal alanda ve akademik tartışmalarda sürekli tekrarlanmaktadır. Kimi araştırmacılar ve gazetecilik uzmanları bu krize teknolojik belirlenimcilik perspektifinden yaklaşırken, kimileri ekonomi politik bir yaklaşımı tercih etmektedir (Steen-Johnsen, Kari, Fladmoe ve Midtbøen, 2016: 190). Haber merkezlerindeki kriz ve gazetecilerin çalışma koşulları, emek çalışmaları ve medya araştırmalarında tartışmalı bir durumu tetiklemektedir: Güvencesiz çalışma.

Güvencesiz çalışma, belirsiz, öngörülemeyen ve riskli bir çalışma şekli olarak tanımlanmaktadır (Kalleberg, 2009: 2). Bu çalışmada, güvencesizlik ve güvenlik konuları, gazetecilik sektörünün "krizine" yönelik yaklaşımların kesişim noktası olarak değerlendirilmektedir. Dijitalleşmeyle birlikte meydana gelen yeni değişimler, rekabetçi koşullar, yeni istihdam türleri, editoryal süreçlerdeki ve iş akışlarındaki değişiklikler, neoliberal politikalar, dünya çapında yükselen otoriterleşme ve artan kitlesel gözetim, gazetecilerin ne kadar güvenli şartlarda çalıştığını anlamaya çalışırken dikkate alınması gereken önemli olgulardır.

Günümüzde gazeteciler, fiziksel saldırıların ve hukuki yaptırımların ötesinde, çok sayıda siber saldırıyla karşı karşıya. Bu sebeple gazetecilerin güvenliği, bu dinamik ve yeniliklerle dolu ortamda üzerinde durulması gereken temel bir mesele olarak ön plana çıkmaktadır. Dijitalleşmiş çalışma koşullarında gazetecilerin cep telefonlarıyla bağlantılı coğrafi verileri ve dijital ayak izleri kolayca izlenebilmektedir. Bu durum da onları hem siber hem de fiziksel saldırılara karşı daha savunmasız hale getirmektedir (Henrichsen, Betz ve Lisosky, 2015: 20). Ayrıca, bu saldırılar devlet veya devlet dışı aktörler tarafından da gerçekleştirilebilmektedir. Örneğin, *Google* güvenlik mühendisleri tarafından yürütülen bir araştırmaya göre, Dünyanın En İyi 25 Haber Kuruluşu, devlet destekli siber saldırılara maruz kalmıştır (Henrichsen, Betz ve Lisosky, 2015: 22). Gazetecilerin dijital güvenliği, özellikle son on beş yıldır çok sayıda araştırmaya konu olmaktadır ve bu araştırmaların çoğu gazetecilerin karşılaştığı dijital güvenlik tehditlerini incelemeye odaklanmaktadır (örn. Çalışkan, 2019; Ataman ve Çoban, 2018; Henrichsen, Betz ve Lisosky, 2015; IFJ Report, 2016; Holcomb ve Mitchell, 2015; Ramos, 2015; Bytes for All, 2012; Sierra, 2013). Bu çalışmalar, temel güvenlik tehditlerini ortaya çıkarmak ve çözüm önerileri geliştirmeye yönelik tartışmaları başlatmak için önemli bir zemin oluştursa da, gazetecilerin güvencesizliği ve güvenliği arasındaki ilişki, çoğunlukla kendi risk ve sorumluluklarını sırtlanmak zorunda kalan serbest gazeteciler üzerinden ele alındığında farklı bir boyuta evrilmektedir.

Bu çalışmada, haber merkezlerinde güvencesiz işgücü ve bilgi güvenliği ile ilgili çalışmalardan yararlanılmış ve dijital güvenlik ve güvencesizlik arasındaki ilişki, serbest gazeteciler gibi niş bir örneklem üzerinden ele alınmıştır. Yedi serbest gazeteci, iki haber odası editörü ve beş dijital güvenlik eğitmeniyle yapılan derinlemesine görüşmelerden yola çıkarak, haber üretim süreçlerindeki dijitalleşmenin ve güvencesiz çalışma ilişkilerinin neden olduğu "güvensizliğin" çerçevesinin çizilmesi amaçlanmıştır.

GAZETECİLERİN GÜVENCESİZLİĞİ VE DİJİTAL GÜVENLİĞİ

Dijital güvenlik, kullanıcıların çevrimiçi dünyada kimliklerini ve varlıklarını güvence altına almak için kullanabilecekleri araçları içeren her şeyi kapsamaktadır. Bu araçlar, virüs tarama ve koruma yazılımlarını, güvenli dolaşım sağlayan web hizmetlerini, şifreli iletişim uygulamalarını ve güvenliği artırılmış cihazların kullanımını da kapsamaktadır. Ancak dijital güvenliğin sağlanması yalnızca bireysel düzeyde alınan önlemlerle aşılabilecek bir mesele değildir. Dijital güvenliğe yönelik farkındalık, hükümetler, kurumlar ve profesyoneller düzeyinde de geliştirilmelidir.

Dijital dünya teknolojik, politik, ekonomik, kurumsal ve yasal boyutları olan dijital riskleri de beraberinde getirmektedir. Ancak gazetecilik söz konusu olduğunda riskler sosyal bir boyut kazanmaktadır. Gazetecilerin dijital güvenliği, bilgi güvenliği, mesleğin güvenilirliği, sivil toplum, hükümetler, uluslararası kuruluşlar ve özel sektör için esastır. Daha da önemlisi, demokrasinin anahtarı olan basın özgürlüğünün sağlanması için önem taşımaktadır (Henrichsen, Betz ve Lisosky, 2015). Gazetecilerin bilgi toplamak, depolamak ve raporlamak için kullandıkları dijital platformlar pek çok güvenlik riski taşımaktadır. Dijital platformlar kullanıcı verilerini sürekli olarak toplamakta, kategorize etmekte ve analiz etmektedir. Mark Andrejevic (2012: 91-99) buna "her zaman her yerde bulunan gözetim" adını vermektedir; bu da platformların "veri toplama, depolama ve kategorize etme" pratiklerinden kaçmanın giderek daha zor hale geldiği anlamına gelmektedir. Son yıllarda kullanıcılara ait dijital verilerin çalınması, sızdırılması veya farklı amaçlar için üçüncü şahıslara satılması konularını gündeme getiren pek çok veri skandalı meydana gelmiştir.

Gazetecilik pratikleri dijital alana taşındıkça, gazetecileri hedef alan saldırılar da dijital saldırılara dönüşmektedir (Tsui, 2019: 81). Dijitalin doğası gereği kolay erişilebilir ve manipüle edilebilir olmasından ötürü, gerekli güvenlik önlemleri alınmadığı sürece, gazetecilerin bilgi kaynakları ve soruşturma sırasında topladıkları bilgiler ciddi risk altına girmektedir. Gazeteciler kaynaklarını ve bilgilerini güvende tutmak için dijital güvenlik önlemleri almazlarsa, bu bilgiler çeşitli korsanlık faaliyetleriyle çalınabilmekte ve sızdırılabilmektedir. Bu durum, yalnızca soruşturması yürütülen haber için değil, gazetecinin ve kaynaklarının can güvenliği için de ciddi bir tehdit oluşturabilmektedir (Murthy, 2018).

Ayrıca, hassas belgeler üzerinde çalışan veya hükümetler tarafından "kara listeye" alınan bazı medya kuruluşları ve sivil toplum kuruluşları için haber üreten gazeteciler, sosyal güvenilirliklerini kaybetme riski yaşamaktadır. Yurtdışında faaliyet gösteren bazı haber merkezleri için çalışan serbest gazetecilere yönelik yaptırımlar daha da ağır olabilmektedir. Örneğin, bazı gazetecilerin ülkedeki basın kartları iptal edilirken, yurtdışındaki haber odaları için çalışan bazı gazeteciler ise sınır dışı edilmekte veya ülkeye girişleri engellenmektedir. Bu sebeple, siyasi açıdan "riskli" olduğu düşünülen haber merkezleri için içerik üreten gazeteciler çoğunlukla kimliklerini gizleyerek çalışmak zorunda kalmaktadır. Bu durum özellikle geçimini sağlamak için birden fazla haber odası ile çalışmak ve haber üretmek zorunda olan serbest gazeteciler için geçerlidir. Özellikle yurtdışındaki haber odaları için içerik üreten serbest gazetecilerin dijital güvenliklerine özel bir hassasiyet göstermeleri gerekmektedir çünkü genellikle risklerle kendi başlarına başa çıkmak zorunda kalmaktadırlar.

Haber odalarının gazetecilerin dijital güvenliği konusundaki temel rollerinden biri, çalışanlarına dijital güvenlik eğitimi vermek veya farklı kuruluşlardan bu eğitimleri almalarını sağlamaktır. Örneğin, *Security in a Box* gibi dijital güvenlik okuryazarlığı sağlamaya çalışan birçok proje ve *ijnet, NiemanLab, Reuters Institute of Journalism*, *Poynter*, *Journalist's Resource* ve

UNESCO gibi çevrimiçi olarak halka açık içerik üreten çeşitli kurumlar bulunmaktadır. *NewsLabTurkey*'in altında faaliyetlerini sürdürdüğü *Dijital Medya Araştırmaları Derneği* ve *Alternatif Bilişim Derneği* gibi organizasyonlar da düzenli olarak dijital güvenlik eğitimleri düzenlemektedir. Haber odalarının gazetecileri bu eğitimlere yönlendirerek dijital güvenliğe dair farkındalıklarını ve pratiklerini geliştirmeyi hedeflemesi oldukça önemlidir.

Öte yandan, bu projeler veya kurumsal çabalar, gazetecilerin dijital güvenlik okuryazarlığını geliştirmeye veya dijital güvenliğini garanti altına almaya yetmemektedir. Güvencesiz çalışma, neoliberal çalışma rejimine dayalı küresel bir olgu olmasına rağmen, politik kutuplaşma düzeyi yüksek ve gergin bir siyasi atmosfere sahip ülkelerde güvencesizlik ve güvenlik sorunu farklı şekilde tecrübe edilmektedir. Örneğin, bir ülkede sıradan bir iletişim uygulaması olarak değerlendirilen *Signal* gibi yazılımların kullanılması, başka bir ülkede tutuklanma sebebi olabilmektedir. *The Onion Router* gibi yazılımlar, tek amacı güvenli araştırma yapmak olan bir gazeteciyi terörist olarak suçlamak için kullanılabilmektedir. Ayrıca, PGP/GPG gibi şifreleme sistemleri, şifrelenmiş içeriğin şifresi güvenlik kurumları tarafından çözülmediği durumlarda bile, bir suçun kanıtı olarak manipüle edilip kullanılabilmektedir.

Günümüzde artan güvencesiz çalışma koşullarında gazetecilerin dijital güvenlikleri de en az fiziksel güvenlikleri kadar önemli hale gelmiştir. Dijital çağda güvenliği sağlamanın zorlukları göz önüne alındığında, dijital güvenlik tehditleri gazetecilerin karşılaştığı başlıca endişelerden biri haline gelmiştir (IFJ, 2016). Dijital iletişim teknolojileri gazetecilik mesleğinde zaman ve mekân engellerini neredeyse ortadan kaldırırken, hızlı haber akışını sağlarken, maliyetleri düşürürken ve benzeri daha birçok avantaj sağlarken, öte yandan gazetecilerin ve kaynaklarının güvenliğini tehdit etmekte ve daha fazla ifşa, gözdağı ve kovuşturma riskiyle karşı karşıya bırakmaktadır (McGregor, Charter, Holiday ve Roesner, 2015).

Öte yandan, hükümetlerin belirli güvenlik uygulamalarını ve şifreli yazılım ürünlerin kullanımını kınaması veya kullananları gizli riskli faaliyetler yürüttükleri düşüncesiyle şüpheli addetmesi, gazetecilerin dijital güvenlik önlemleri alma motivasyonlarını olumsuz etkilemektedir. Bu durum, kaynakların gizliliğinin ve bilgi güvenliğinin sağlanması gibi evrensel gazetecilik ilkelerinin göz ardı edilmesine neden olabilmektedir. Bu ihlallere gazetecilik camiasından da yeterli tepki gelmemektedir.

Türkiye'deki medya sektörünün mali durumu, çalışma koşulları ve yasal çerçevesi dikkate alındığında, serbest çalışan gazeteciler için düzenlenecek dijital güvenlik eğitimlerine ihtiyaç olduğu görülmektedir. Serbest gazeteciler, mevcut çevrimiçi güvenlik araçlarının yelpazesi ve en savunmasız oldukları konularda nasıl önlemler almaları gerektiği konusunda eğitimlere ihtiyaç duymaktadır. Bu nedenle bu çalışmada, serbest gazetecilerin, haber odası editörlerinin ve dijital güvenlik eğitmenlerinin deneyimlerine ve tercihlerine başvurulmuş ve dijital güvenlikle ilgili sorunlar ele alınmıştır.

ARAŞTIRMANIN YÖNTEMİ

Daha önce yapılan bazı çalışmalarda da belirtildiği gibi, dijital güvenlik, özellikle kişisel verilerin korunmasına ilişkin yasa ve yönetmeliklerin zayıf olduğu ülkelerde önemli bir konudur. Ancak hükümetlerin kitlesel gözetleme araçlarını yoğun olarak kullandığı ve gazetecilerin dijital medya okuryazarlığının düşük olduğu ülkelerde bu odaktaki çalışmalara yeterli öncelik verilmemektedir. Bunun güvenliğe dayalı endişeler de dahil olmak üzere birçok farklı sebebi olabilir. Örneğin, güvenlikle ilgili bir araştırma yürütmek, hem araştırmacılar hem de katılımcılar için oldukça zahmetli hale gelebilmektedir. Bu araştırma kapsamındaki deneyimimize göre, görüşme yapmak için irtibat kurduğumuz gazeteciler, editörler ve eğitmenler, çeşitli güvenlik endişeleri nedeniyle sorularımızı cevaplama konusunda oldukça isteksizlerdi. Bu sebeple araştırmanın her aşamasında anonimliğin sağlanmasına özen gösterdik ve katılımcıların gerçek isimleri yerine takma isimler kullandık.

Bu çalışmada yarı-yapılandırılmış derinlemesine görüşmelere dayalı keşifsel bir yaklaşım benimsenmiştir. Görüşme soruları, ilgili literatürde daha önce yapılmış araştırmalar dikkate alınarak oluşturulmuştur. Görüşmelerin analizinde betimsel nitel veri analizi yöntemi kullanılmıştır.

Araştırma kapsamında, *Zoom* ve *Skype* üzerinden 14 kişiyle yarı-yapılandırılmış görüşmeler gerçekleştirilmiştir. Görüşmeler, serbest gazetecilerin dijital güvenliği ve güvencesiz çalışma koşulları hakkında kapsamlı bir içgörü elde edebilmek için üç farklı örneklem grubuyla gerçekleştirilmiştir. Örneklem, yurtdışındaki haber odaları için içerik üreten yedi serbest gazeteciden, gazetecilik faaliyetlerini yurtdışında sürdüren iki haber odası editöründen ve gazetecilerin güvenliği konusunda uzmanlaşmış beş dijital güvenlik eğitmeninden oluşmaktadır. Araştırmaya dahil edilen

serbest gazeteciler seçilirken, hiçbir yerde tam zamanlı, sözleşmeli veya sigortalı olarak çalışmaması ve yurtdışında faaliyet gösteren haber odaları için telifli içerik üretmesi kritelerine dikkat edilmiştir. Serbest gazetecilerle görüşme yapılmasının temel amacı, çalışma rejimi ile güvensizlik durumu arasında nasıl bir ilişki olduğunu keşfetmektir. Araştırma kapsamında görüşme yapılan editörler, yurtdışında serbest muhabir çalıştıran haber odalarının editörlerinden seçilmiştir. Editörlerle yapılan görüşmeler, haber odalarının serbest gazeteciler için nasıl dijital güvenlik önlemleri aldıklarının incelenmesini amaçlamaktadır. Dijital güvenlik eğitimi veren profesyoneller ise Türkiye'deki gazetecilik ve ifade özgürlüğü odaklı STK'ların düzenlediği eğitimlerde ders veren kişilerden seçilmiştir. Bu eğitmenlerle görüşme yapılmasının temel amacı, dijital güvenlik eğitimlerinin içeriğini, performansını ve katılımcı profilini anlamak ve uzmanların konuyla ilgili deneyimlerini öğrenmektir.

Son olarak, serbest çalışan gazetecilerin belirli bir kesimine odaklanan bu çalışma, Türkiye'deki tüm gazetecilere odaklanan ve farklı türdeki ulusal ve uluslararası haber merkezlerini ve farklı çalışma rejimlerini açıklayan bir çalışmaya ihtiyaç olduğunu göstermektedir. Çalışmamız, Türkiye kamuoyuna seslenen fakat Türkiye dışında faaliyet gösteren dijital haber merkezlerini ve onlar için haber üreten serbest gazetecilerin sahadaki faaliyetlerini kısmen temsil etse de, sahadaki tüm gazetecilik aktörlerinin demografik ve profesyonel profilleri açısından kapsamlı bir temsilden yoksundur.

GÜVENCESİZ BİR ORTAMDA SERBEST GAZETECİ OLARAK GÜVENDE KALMAK

Görüşme yaptığımız tüm serbest gazetecilerin on yıldan fazla süredir bilgisayar ve cep telefonu kullandıklarını fakat yalnızca dördünün iki aşamalı doğrulama veya kolay tahmin edilemeyen birden fazla şifre kullanmak gibi temel dijital güvenlik önlemlerinden yararlandığını tespit ettik. Daha önce hesaplarının saldırıya uğradığını veya belirli dönemlerde saldırıya uğradığından şüphelendiğini belirten gazeteciler, web'te güvenli gezinme araçlarını veya iki aşamalı doğrulama gibi en temel protokolleri kullanmadıklarını belirttiler. Görüştüğümüz yedi gazeteciden dördü, cihazlarında virüs tarayıcı olmamasının ne kadar riskli olduğunu bilmesine rağmen virüs tarayıcı kullanmıyordu. Öte yandan, gazetecilerin çoğu bilgisayarlarını ve mobil cihazlarını düzenli olarak güncellemenin, dijital güvenliklerini sağlamak için ne kadar önemli olduğunun farkındaydılar.

Farklı bağımsız haber kuruluşlarında çalışan genç bir gazeteci olan Mithat, genellikle çatışma bölgelerinde çalıştığı için PGP şifrelemesini birkaç kez kullandığını ancak daha sonra pratik ve kullanışlı olmadığı için kullanmayı bıraktığını belirtti. Yine genç bir gazeteci olan Ece ise PGP'nin nasıl kullanılacağının öğretildiği eğitimlere katıldığını ancak daha önce hiç kullanmadığını söyledi. Ela, devletin üst yönetimsel kademelerinde çalışan önemli bağlantıları olduğunu ancak hiç PGP kullanmadığını ve ne olduğunu bilmediğini belirtti. Çatışma bölgelerinde de çalışan bir gazeteci olan Fatma ise yasal makamların PGP benzeri teknolojilerin kullanımını yasadışı faaliyet olarak değerlendirdiğini, bu yüzden bu teknolojileri kullandıkları farkedildiğinde çok daha büyük zorluklar yaşadıklarını söyledi. Fatma, polisin bir gazeteciyi durdurmasının ve kişisel eşyalarına bakmasının çok yaygın bir pratik olduğunu ve gazetecilerin sakladığı şifreli dosyaların veya kullandığı şifreli uygulamaların polisler nezdinde sorun yaratabileceğini

belirtti. Fatma'ya göre şifresiz iletişim kurmak pek çok açıdan daha "risksizdi." Bu yüzden katıldığı dijital güvenlik eğitimlerinin çoğunun Türkiye'deki uygulamaları ve yaptırımları görmezden geldiğini ve Avrupa standartlarına göre hazırlandığını söyledi.

Daha önce gazetecilik faaliyetleri sebebiyle yasal soruşturma geçirmiş olan Tamer, tüm dijital ekipmanlarına polisler tarafından el konulduğunu ve serbest kaldıktan sonra da ekipmanlarını hâlâ geri alamadığını belirtti. Tamer bu yüzden dijital teknolojiler vasıtasıyla iş amaçlı iletişim kurmaktan tedirginlik duyduğunu ve güvensiz hissettiğini belirtti. Daha önce gazetecilik faaliyetleri sebebiyle yasal soruşturma geçirmiş olan Mithat ise tutuklanırken el konulan bilgisayarının ve akıllı telefonunun kendi rızası dışında incelendiğini, akıllı telefonunun sekiz sene sonra kendisine geri verildiğini ifade etti. Görüştüğümüz gazetecilerin çoğu, protestoları veya halka açık olayları takip ederken güvenlik görevlilerinin haber yapmalarını engellemek için cep telefonlarını ellerinden almaya çalıştıklarını, ancak cep telefonlarını yetkisi olmayan kişilere vermediklerini söylediler.

Serbest çalışan gazetecilere kaynaklarıyla ve haber odalarıyla iletişim kurarken kullandıkları iletişim uygulamalarını sorduğumuzda, en çok *WhatsApp, Telegram* ve *Signal* kullandıklarını söylediler. Ancak, kimi medya kuruluşlarının daha önce *Signal* kullananları hedef göstermesi nedeniyle, bazı gazeteciler *Signal*'in telefonlarındaki varlığını bile tehdit olarak algıladıklarını, bazıları ise *Signal*'i en güvenli iletişim uygulaması olarak gördüklerini belirttiler. Görüştüğümüz gazetecilerin *WhatsApp*'ın güvenli olup olmadığı konusunda net bir görüşleri yoktu. Bazı gazeteciler *WhatsApp*'ın *Signal* ile benzer protokolleri kullandığının farkında olsa da sahiplik yapısından ötürü güvenlik endişeleri vardı. Bunun bir diğer sebebi de *Signal*'in pazarda kendisini "güvenlikli" bir iletişim uygulaması olarak konumlandırırken *WhatsApp*'ın mesajlaşma uygulaması olarak konumlandırması olabilir. Öte yandan *Telegram* ise hem şifreli hem de şifresiz iletişime açık özellikleri olduğu için gazetecilerin çoğu tarafından

güvenliksiz bir uygulama olarak değerlendirildi. Ancak *Telegram* kullanan bazı gazeteciler güvenilir ve kullanımının kolay olduğunu belirttiler.

Daha önce gazetecilik faaliyetleri sebebiyle yasal soruşturma geçirmiş olan Tamer, banka hesaplarının gözetim altında olduğunu düşündüğü için ödeme yaparken veya bir başkasından ödeme alırken arkadaşlarının banka hesaplarını kullandığını belirtti. Tamer, blokzincir temelli ödeme sistemlerinde güvenli prosedürler olduğunu ve Türkiye'de *PayPal* olmadığı sürece blokzincir ödeme teknolojilerini kullanan haber odalarının sayısının artması gerektiğini de sözlerine ekledi. Ancak görüştüğümüz gazetecilerden yalnızca üçü blokzincir teknolojileri ile nasıl ödeme yapılabileceğini ve alınabileceğini biliyordu. Diğerleri ya blokzincir ödemelerinin nasıl çalıştığını bilmiyorlardı ya da bu sistemler hakkında hiçbir şey bilmedikleri için bu şekilde ödeme almayı tercih etmiyorlardı. Haber merkezlerinden aldığı ödemelerin banka hesapları vasıtasıyla takip edildiğini düşünen Selma, "özellikle yurtdışından direkt Türkiye'ye yapılan ödemelerde güvenli bir yol kullanamamanın çok can sıkıcı" olduğunu belirtti. Birçok farklı dijital haber odası için muhabirlik yapan Vedat ise tüm gazetecilerin banka hesaplarının otoriteler tarafından düzenli olarak takip edildiğini öğrense buna şaşırmayacağını; ancak şu ana kadar herhangi bir blokzincir ödeme sistemini kullanmadığını ve çalıştığı haber odasından da bu yolla ödeme almayı talep etmediğini belirtti.

Görüştüğümüz bazı gazeteciler, güvenlik nedeniyle özellikle Türkiye dışında faaliyet gösteren bazı haber kuruluşları için haber üretirken takma isimler kullandıklarını belirtirken, bazıları ise takma isim kullanmanın haberlere karşı güvensizlik oluşturduğu düşüncesiyle etik olmadığını ifade ettiler. Buna rağmen görüştüğümüz gazetecilerin tamamı takma isim kullanarak haber yayınlamanın gözetimden kaçmak için bir çözüm olmadığı konusunda hemfikirdi. Mithat şunları söyledi: "Şu anda yurtdışında faaliyet gösteren bir haber odası için bir haber üzerinde çalışıyorum ve haberin iletilmesinden

ücretin ödenmesine kadar geçen tüm süreçte kendimi risk altında hissediyorum. Bu yüzden kendi haberimi imzalamıyorum."

Dijital güvenlik eğitimleriyle ilgili olarak ise, görüştüğümüz gazetecilerin çoğunun daha önce hiç dijital güvenlik eğitimi almadığını gördük. Eğitim alanlar ise çoğunlukla eğitimleri yeterli bulmadıklarını belirttiler. Bazı gazeteciler eğitimlere katılma konusunda bile güvenlik kaygısı taşıdığını, bazıları ise eğitim almanın güvenlik risklerini azaltmadığını ve çoğu zaman Türkiye'nin siyasi ortamında bunun bir çözüm olmadığını belirtti. Mithat bu durumu şöyle ifade etti: "Güvenliğimizi sağlamaya çalıştığımızda ve güvenli yazılımlar, hatta VPN'ler kullandığımızda bu bir terör suçu olarak kabul edilebiliyor. Şifreli sistemler kullanmamız, 'saklanacak bir şey mi var?' sorusuyla bizi adalete teslim ediyor. Bizden her zaman gözetime açık olmamız isteniyor."Fatma da Mithat gibi "iz bırakmamak bazen daha çok iz bırakır" dedi ve ekledi: "Özellikle serbest çalışıyorsanız sorun daha karmaşık hale geliyor, çünkü sizi hedef alanlar 'arkalarında koruyacak bir kurumları yok' diye düşünüyor." Selma ise genellikle yaptığı haberlerin yöneticilerini tehdit edecek düzeyde hassas bilgi içermediğini ancak sadece şifreli uygulamalar kullanmanın bile onları riske atabileceğini belirtti ve ekledi "bu yüzden her zaman paranoyak oluyorum." Selma, dijital güvenlik eğitimlerine düzenli olarak katıldığına işaret ederek, "güvenle çalışma fırsatı bulduğum için bu toplantılara katılmanın faydalı olduğunu düşünüyorum. İleri düzey bir siber güvenlik eğitimi almayı planlıyorum. Zaman geçtikçe, serbest gazeteci olarak daha fazlasına ihtiyacım olacağına inanıyorum" dedi.

Görüştüğümüz serbest gazetecilerin hepsi çalışma koşullarıyla ilgili birçok yönden kendilerini güvensiz hissettiklerini belirttiler. En fazla değindikleri ortak sorunlar, serbest çalışmalarından ötürü arkalarında onlara sahip çıkacak bir kurum olmamasıyla ve olası dijital tehditler konusunda iyi eğitilmedikleri için tüm riskleri kendi başlarına üstlenmek zorunda kalmalarıyla ilgiliydi.

GÜVENCESİZ BİR ORTAMDA SERBEST GAZETECİ ÇALIŞTIRMAK

İstihdam ilişkileri karşılıklıdır. Ancak hem siyasi hem de finansal açıdan güvensizlikler barındıran bir ortamda, özellikle gazetecilerin çalışma sözleşmeleri açısından pek çok yasal belirsizlik olması nedeniyle işverenler daha güvenli bir konuma sahiptir. Yine de bu, işverenlerin güvenlik sorunları olmadığı anlamına gelmez; pek çok sebeple haber odalarına erişim yasaklanabilir veya ekonomik gelirleri kısıtlanabilir. Yasal ve ekonomik kısıtlamalar nedeniyle Türkiye'den kısmen veya tamamen taşınan bazı haber merkezleri vardır. Bu haber odalarının birlikte çalıştıkları gazetecilere dijital güvenlik sağlama kapasitelerini anlamak için iki yönetici editörle görüştük.

Yurt dışında faaliyet gösteren dijital bir haber odasının editoryal koordinatörü Kerim, farklı hikâyeler için farklı iletişim teknikleri kullandıklarını belirtti. Kerim, özellikle soruşturmacı gazetecilik faaliyetleri yürüttükleri veya çatışma bölgelerinde birlikte çalıştıkları muhabirlerle iletişim kurdukları zamanlarda şifreli e-posta servislerini veya PGP/GPG benzeri şifreleme teknolojilerini kullanmayı tercih ettiklerini ifade etti. Dijital güvenlik konusunda katı bir politikaları olmadığını ve muhabirlere eğitim vermediklerini belirten Kerim, sadece bir miktar eğitici video kaynağı gönderdiklerini ve birlikte çalıştıkları muhabirlerin kullandıkları iletişim biçimlerine ve aldıkları güvenlik önlemlerine göre hareket ettiklerini ifade etti. Gerektiği zamanlarda muhabirlerini güvenlik konusunda uyardıklarını ve güvenli olmadığı için üstünde çalışmaktan vazgeçtikleri haberler olduğunu da ekledi. Ayrıca, Kerim, genellikle muhabirlerin sahada birbirlerini koruduğunu ve yardım ettiğini söyledi ve "genç muhabirler, muhafazakâr bir zihniyete sahip olan ve yeni teknolojileri kullanmaya direnenlere göre dijital güvenlik konusunda daha bilinçli" dedi. Türkiye'de

düzenlenen dijital güvenlik eğitimleriyle ilgili olarak, Kerim, eğitimlerin yeterince etkili olmadığını ancak etkili olması için Türkiye'deki yasal düzenlemelerin geliştirilmesi gerektiğini belirtti.

Bir başka dijital haber odasının yönetici editörü Cemal, muhabirlerinin hepsinin dijital güvenlik eğitiminden geçtiğini ve sahadaki kaynaklarına ve muhabirlerine güvenlik sağlamak için ellerinden geleni yaptıklarını belirtti. Sorulara daha ayrıntılı yanıtlar almak istediğimizde ise yanıtlamayı reddetti. Bununla birlikte, Cemal, "haber yapmak her zaman belirli riskleri almayı gerektirir ve bu risklere karşı çok iyi organize olamıyoruz" diye ekledi.

Görüştüğümüz her iki editör de hassas konular üzerinde çalışacak serbest muhabir bulmanın zor olduğunu belirtti. Cemal bunun sebebinin özellikle yurtdışında faaliyet gösteren haber odaları ile ilgili olumsuz söylemlerden ve caydırıcı yaptırımlardan kaynaklandığını belirtti. Cemal'e göre serbest gazeteciler yurtdışında faaliyet gösteren haber odaları için çalışmayı tehdit olarak algılıyorlardı. Cemal, çalıştığı haber odasının serbest muhabir telif ödemeleri açısından Türkiye standartlarının üzerinde olduğunu ve muhabirleri aktif olarak destekleyen bir grup avukatla çalıştıklarını fakat buna rağmen serbest gazetecilerin çoğunlukla taleplerini reddettiğini ifade etti. Kerim ise özellikle 2013'te meydana gelen Gezi Parkı protestolarının ardından, gazetecilerin hükümet tarafından "kara listeye alınmaktan" korktukları için yurtdışında faaliyet gösteren haber merkezleri için çalışmak istemediklerini ve bu sebeple serbest çalışan muhabir bulmakta zorlandıklarını söyledi.

Görüştüğümüz editörlerin ifadeleri, dijital güvenlik önlemlerinin genellikle muhabirlerin çabalarına bağlı olduğunu göstermektedir. Yurt dışında faaliyet gösteren bağımsız haber odaları her ne kadar Türkiye'deki endüstriyel standartların üzerinde telif ödemesi yapsa da bazı muhabirler "kara listeye alındığına" inandıkları haber odalarında çalışmayı tercih etmemektedir.

TÜRKİYE'DE GAZETECİLERE DİJİTAL GÜVENLİK EĞİTİMİ VERMEK

Dijital güvenlik eğitmeni Veli, eğitimlerine katılanların profiliyle ilgili olarak, genelde gazetecilik sektörü dışında çalışanların eğitimlere daha fazla ilgi gösterdiğini belirtti. Veli'ye göre, dijital iletişim alanında çalışan beyaz yakalılar ve internet üzerinden çalışarak gelir elde eden serbest çalışanlar bu tür eğitimlere daha fazla ilgi gösteriyor. Bir başka dijital güvenlik eğitmeni Ali, verdikleri eğitimlere ilgi gösterenlerin çoğunlukla genç ve serbest çalışan gazeteciler, gazetecilik öğrencileri ve insan hakları aktivistlerinden oluştuğunu söyledi.

Eğitmenlerden Burak, katılımcıların talep ettiği eğitimlerin düzeyinin mesleğe göre değiştiğini belirtti. Bu nedenle, katılımcılara eğitim öncesi mesleklerini sorduklarını ve daha sonra onları farklı seviyelere ayırdıklarını söyledi. Burak, daha ileri seviye güvenlik biçimleri hakkında eğitimler talep edenlerin, akademik eğitimleri ve ücretli çalışma alanları ne olursa olsun genelde hack kültürüne aşina olan kişilerden oluştuğunu belirtti. Öte yandan, genellikle öğrencilerin (bilgisayar mühendisliği vb. alanlardan gelenler dışında) ve dijital alanlarda çalışan gazetecilerin ve yayıncıların başlangıç seviyesinde dijital güvenlik bilgisine sahip olduklarını ifade etti.

2015'ten bu yana halka açık eğitimler vermediğini fakat özel eğitimler vermeye devam ettiğini söyleyen Tuna, 2015'ten önce güvenlik eğitimi talep edenlerin daha çok erkeklerden oluştuğunu, ancak son yıllarda verdiği özel eğitimlere kadınların da ilgi göstermeye başladığını ve şimdilerde yaş, sosyo-ekonomik durum ve cinsiyet açısından eşit dağılım gösteren gruplara eğitim verdiğini belirtti. Tuna, özel eğitim verdiği grupların çoğunlukla gazeteciler, iş insanları, sivil toplum aktivistleri ve politikacılardan oluştuğunu söyledi. Dijital güvenlik üzerine akademik çalışmalar yürüten ve

eğitimler veren Sefer de, Veli ve Ali ile gibi, gazetecilerin dijital güvenliğe olan ilgisinin sınırlı olduğunu ve eğitimlere başvuranların çoğunun daha az deneyime sahip genç gazeteciler olduğunu belirtti.

Türkiye'deki dijital güvenlik eğitimlerinin nasıl algılandığı ile ilgili olarak, hem Veli hem de Sefer, dijital güvenliğin ve dijital gizliliğin, yalnızca devlet ve iş dünyasında hassas rollerde çalışan kişilerin erişmesi gereken mekanizmalar olarak anlaşıldığına dikkat çekti. Veli, eğitimlere katılan gazetecilerin çoğunun siyasi otoriteler tarafından "kara listeye alınmaktan" çekindiğini ve bu yüzden eğitimlerde önerilen uygulama veya yazılımları kullanmakla ilgili çekinceleri olduğunu belirtti. Veli, bu korkunun özellikle 2016'daki başarısız darbe girişiminden sonra Türkiye'de yayıldığına, bunun temel sebebinin de darbeye teşebbüs eden terör örgütünün iletişim kurmak için şifreli bir ağ kullanmasıyla ilgili olduğuna değindi.

Burak, çok sınırlı bir kitlenin (örneğin, hack kültürünü benimseyen kişiler) dışında, katılımcıların genellikle PGP/GPG benzeri şifreleme araçlarını kullanmaya istekli olmadığını belirtti. Hem Veli hem de Sefer, Çin, Rusya ve Türkiye gibi ülkelerde VPN veya şifreli iletişim uygulamaları kullanmanın suç olduğuna dair ortak bir algı olduğunu ve bunun etkili bir olumsuz faktör olduğunu belirtti. Veli'ye göre şifreli iletişim uygulamalarını ne kadar fazla insan kullanırsa toplum arasında normalleşmesi de o kadar mümkün.

Ali, Türkiye'deki gergin siyasi atmosferin hem güvenlik eğitmenlerini hem de katılımcıları etkileyen genel bir tedirginlik yarattığını söyledi. Ali'ye göre asıl tedirginlik yaratan şey, verdikleri eğitimlerin gazetecilerin ihtiyaçlarına göre şekillenmesine ve hiçbir siyasi bir yönü olmamasına rağmen, çoğunlukla asıl bağlamından koparılıp farklı şekillerde algılanma ihtimaliydi. Bu durumun eğitimler esnasında otosansüre neden olduğunu söyleyen Ali, "bazen güvenlik riskleri hakkında konuşmaktan çekiniyorum ve söyleyeceklerimi söylemeyi bırakıyorum" diye ekledi. Tuna da yanlış

anlaşılma korkusundan dolayı "bugün halka açık eğitimler vermeye devam etseydim konuşmaktan tereddüt edeceğim meseleler olurdu" dedi.

Sefer, eğitimlerdeki gazeteciler tarafından en sık sorulan soruların siyasi otoritelerin veya teknoloji sağlayıcıların ne tür bilgilere erişebileceğine ilişkin sorular olduğunu söyledi. Burak ise sık sorulan soruların özünde korku yattığını belirterek, "her eğitimin sonunda mutlaka birinin sorduğu bir soru var: 'Gereğinden fazla mı önlem alıyoruz?'" dedi. Veli ise katılımcıların genelde çok basit güvenlik soruları sorduklarını, gözetimle ilgili en çok bilinen gerçekler hakkında bile bilgi sahibi olmadıklarını belirtti. Veli'ye göre gazeteciler, özellikle şifre belirleme konusunda oldukça zayıf taktiklere sahipler. Gazetecilerin şifre kontrol yazılımları veya uygulamaları kullanma eğiliminde olmadığına inanan Veli, "eğitimlere katılan çoğu katılımcı, halka açık Wi-Fi'ye bağlanmanın tehditlerinin farkında bile değil" dedi.

Görüştüğümüz bazı eğitmenler, kısa eğitim setlerine katılan gazetecilerin dijital gizlilik endişeleri hakkında sıklıkla kendilerine danıştığını belirttiler. Genelde gazetecilere gönüllü olarak yardım ettiklerini, gerekli gördüklerinde ise kurumsal kuruluşlardan yardım almaya yönlendirdiklerini söylediler. Veli, kişisel ve kurumsal dijital güvenlik konusunda Türkçe bir dijital kaynak oluşturmanın öncelikleri arasında olduğunu söyledi.

REFERANSLAR

Andrejevic, Mark. 2012. "Ubiquitous Surveillance." *Routledge Handbook of Suveillance Studies* içinde, bölüm 1.3. b, ss. 91-99, Kirstie Ball, Kevin Haggerty and David Lyon (Ed). Routledge, New York.

Ataman, Bora, ve Çoban, Barış. 2018. "Counter-surveillance and alternative new media in Turkey." *Information, Communication & Society*, 21(7): 1014-1029.

Çalışkan, Behlül. 2019. "Digital security awareness and practices of journalists in Turkey: A descriptive study." *conflict & communication online*, 18 (1). ISSN 1618-0747.

Brake, David R. 2017. "The Invisible Hand of the Unaccountable Algorithm: How Google, Facebook and Other Tech Companies Are Changing Journalism." *Digital Technology and Journalism* içinde, Tong, J., Lo, SH. (Ed) ss. 25-46. Basingstoke: Palgrave Macmillan.

Bytes for All. 2012. "Digital Security and Journalists: A SnapShot of Awareness and Practice in Pakistan." Internews Center for Innovation & Learning.

Henrichsen, Jennifer R., Betz, Michelle, ve Lisosky, Joanne M. 2015. "Building digital safety for journalism: a survey of selected issues." UNESCO Series on Internet Freedom. ISBN:978-92-3-100087-4.

Hunter, Andrea. 2015. "Crowdfunding Independent and Freelance Journalism: Negotiating Journalistic Norms of Autonomy and Objectivity." *New Media & Society* 17(2): 272-288.

International Federation of Journalists (IFJ) ve the South Asia Media Solidarity Network (SAMSN). 2016. "Safer, Smarter Journalism: Survey on Digital Security in South Asia's Media." Brussels: International Federation of Journalists. https://samsn.ifj.org/digital-security-resources-for-south-asia-journalists/.

Kalleberg, Arne L. 2009. "Precarious Work, Insecure Workers: Employment Relations in Transition." *American Sociological Review,* 74(1): 1-22.

McGregor, Susan E., Charters, Polina, Holiday, Tobin, ve Roesner, Franziska. 2015. "Investigating the Computer Security Practices and Needs of Journalists." *The proceedings the 24th USENIX Security Symposium* içinde, August 12–14, 2015, Washington, D.C.

Murthy, C. S. H. N. 2018. "Safety and Security of Journalists: Yet Awaiting Intervention from Indian Academy and Industry." Asia Pasific Media Educator, 28(1), doi: 10.1177/1326365X18772359.

Holcomb, J. ve Mitchell A. 2015. "Investigative Journalists and Digital Security." *Pew Research Center*. Erişim tarihi: 25 May 2021. https://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/.

Ramos, Javier Garza. 2016. "Journalist Security in the Digital World: A Survey. Are We Using the Right Tools?" Center for International Media Assistance. Erişim tarihi: 25 May 2021. https://www.cima.ned.org/wp-content/uploads/2016/03/CIMA-Journalist-Digital-Tools-03-01-15.pdf.

Sierra, Jorge Luis. 2013. "Digital and Mobile Security for Mexican Journalists and Bloggers." Freedom House & International Center for Journalists. https://freedomhouse.org/sites/default/files/Digital%20and%20Mobile%20Security%20for%20Mexican%20Journalists%20and%20Bloggers.pdf.

Steen-Johnsen, Kari, Fladmoe Audun, ve Midtbøen Arnfinn H. 2016. Ytringsfrihetens Grenser: Sosiale Normer og Politisk Toleranse [Freedom of Speech: Social Norms and Political Tolerances]. Fritt Ord, Oslo: Institutt for samfunnsforskning.

Tsui, Lokman. 2019. "The importance of digital security to securing press freedom." *Journalism*, 20(1).

ARAŞTIRMACILAR HAKKINDA

DR. SARPHAN UZUNOĞLU

NewsLabTurkey Research Hub Direktörü Dr. Sarphan Uzunoğlu, aynı zamanda Bilgi Üniversitesi'nde medya yönetimi üzerine dersler vermekte ve çeşitlik uluslararası sivil toplum örgütlerine danışmanlık yapmaktadır. Doktorasını Galatasaray Üniversitesi'nde yazdığı gazetecilikte güvencesiz emek pratikleri temalı tezle 2017 yılında tamamlayan Uzunoğlu daha önce Lübnan Amerikan Üniversitesi Multimedya Gazetecilik Bölümü'nde Öğretim Üyesi Doktor, Norveç Arktik Üniversitesi Medya ve Dökümantasyon Bölümü'nde Doçent Doktor ve Kadir Has Üniversitesi Halkla İlişkiler ve Tanıtım Bölümü'nde Öğretim Görevlisi doktor olarak çalışmıştır. Uzunoğlu geçmişte Evrensel ve Akşam gibi gazetelere ve Mesele, Varlık, Kaos GL gibi dergilere yazılarıyla katkı sunmuştur.

MİNE BERTAN YILMAZ

Mine Bertan Yılmaz Kadir Has Üniversitesi İletişim Fakültesi'nde Araştırma Görevlisi olarak çalışıyor. Doktora tez çalışmalarına Galatasaray Üniversitesi Medya ve İletişim Çalışmaları programında devam eden Yılmaz'ın araştırma alanları insan-bilgisayar etkileşimi, kullanıcı deneyimi araştırmaları ve sanal gerçeklik teknolojilerine odaklanıyor. Yüksek lisans eğitimini Galatasaray Üniversitesi Stratejik İletişim Yönetimi programında tamamlayan Yılmaz, lisans derecesini İstanbul Bilgi Üniversitesi Halkla İlişkiler ve Medya ve İletişim Sistemleri bölümlerinde çift anadal yaparak aldı.