Yapay Zekâ Çağında Sivil Toplum ve Dijital Güvenlik

Bilgi ve veri güvenliği üzerine bir saha dosyası

Aynı teknoloji bir yandan savunmayı güçlendiriyor, bir yandan dolandırıcılığı ucuzlatıyor. Bu dosya, sivil toplumun bu iki gerçekle aynı anda nasıl yaşayacağına dair sakin bir çerçeve öneriyor.

SECURE-CS · SAHA DOSYASI
ERASMUS+ KA220-YOU
İSTANBUL · ARALIK 2025

PROJE
SECURE-CS: Civil Society Initiatives Strengthened with Information and Data Security

REFERANS NO / PROGRAM
2023-1-TR01-KA220-YOU-000161230 · Erasmus+ KA220-YOU (Gençlik Alanında İşbirliği Ortaklıkları)

HAZIRLAYAN
Gülşen Nişli · Uzman Araştırmacı, ANKA Gelecek ve Yenilik Derneği (Proje Ortağı) adına

FİNANSMAN
Avrupa Birliği tarafından ortak finanse edilmektedir · Co-funded by the European Union

Başlarken

Çoğu derneğin bir sunucu odası yoktur. Bir dizüstü bilgisayar, birkaç e-posta hesabı, yıllar içinde birikmiş bir üye listesi ve bulutta duran proje klasörleri vardır. Gündelik iş bu kadar sade görünürken bilgi güvenliği sözü kulağa büyük şirketlerin meselesi gibi gelir. Oysa o dizüstü bilgisayarda gençlerin kimlik bilgileri, velilerin imzaları, gönüllülerin telefon numaraları ve bir kurumun yıllar içinde kazandığı itibar durur. Kaybedilecek şey sanılandan fazladır.

SECURE-CS, tam adıyla *Civil Society Initiatives Strengthened with Information and Data Security*, bu sade görüntünün arkasındaki sorumluluğu ciddiye alan bir ortaklık. Erasmus+ Gençlik Alanında İşbirliği Ortaklıkları (KA220-YOU) kapsamında yürütülen proje, Aralık 2023'ten bu yana eğitim, gençlik ve spor alanında çalışan kurumların dijital, siber güvenlik ve veri koruma becerilerini güçlendirmek için çalışıyor. Türkiye'den Norveç'e, Belçika'dan Kuzey Makedonya'ya uzanan buluşma ve eğitimlerle altı ortak kurum aynı masada çalışıyor. Projenin iki somut çıktısı var: sivil toplum eliyle dijital güvenlik kapasitesi geliştirmeye dönük bir müfredat ve araç seti ile kurumların kendi dijital güvenlik hazırlıklarını sınayabildikleri çevrimiçi bir analiz platformu. Bu birikimin, proje tamamlanana dek düzenlenecek yaygınlaştırma etkinlikleriyle üç yüzü aşkın katılımcıya ulaşması hedefleniyor.

Elinizdeki dosya, bu çabanın yanına güncel bir tartışmayı koyuyor: yapay zekâ. ANKA Gelecek ve Yenilik Derneği adına uzman araştırmacı Gülşen Nişli tarafından kaleme alınan bu çalışmanın amacı ne bir teknoloji güzellemesi ne de bir felaket senaryosu. Yapay zekânın sivil toplumun güvenlik gündemine nasıl dokunduğunu, sahada çalışan insanların diliyle ve elimizdeki verilerle anlatmaya çalıştık.

BİR BAKIŞTA BU DOSYA	
D-01	**Değişen zemin.** Yapay zekâ istisna olmaktan çıktı; kurumların büyük bölümü onu bir biçimde kullanıyor, çoğu zaman yazılı bir kural olmadan.
D-02	**Madalyonun iki yüzü.** Aynı teknoloji savunmada ihlal maliyetini düşürüyor, saldırıda oltalamayı ucuzlatıyor ve inandırıcılaştırıyor.
D-03	**Hedefteki sivil toplum.** Küçük olmak görünmez olmak anlamına gelmiyor; elde tutulan veriler ve duyulan güven, başlı başına birer değer.
D-04	**Verilmiş bir söz olarak veri koruma.** KVKK ve Avrupa Birliği kuralları, yararlanıcıya duyulan saygının hukuki karşılığı olarak okunabilir.
D-05	**Küçük adımlar.** Bütçe değil alışkanlık isteyen on önlem ve kurumların kendini sınayabildiği bir öz değerlendirme platformu.

KAYIT: ZEMİN TESPİTİ

%78

2024'TE EN AZ BİR İŞ SÜRECİNDE YAPAY ZEKÂ KULLANAN KURUMLAR; BİR YIL ÖNCE %55 (STANFORD HAI, 2025)

%88

MCKINSEY'NİN 2025 KÜRESEL ARAŞTIRMASINDA YAPAY ZEKÂ KULLANIMI BİLDİREN KURUMLAR

233

2024'TE KAYDA GEÇEN YAPAY ZEKÂ BAĞLANTILI OLAY; YILLIK ARTIŞ %56'NIN ÜZERİNDE (STANFORD HAI, 2025)

DOSYA 01

Değişen zemin: Yapay zekâ istisna olmaktan çıkarken

Yapay zekâ üzerine konuşmanın en zor yanı, abartı ile küçümseme arasında sıkışmamak. Bir uçta her sorunu çözecek bir sihir anlatısı, diğer uçta gelip geçici bir moda yakıştırması var. Rakamlar ikisini de doğrulamıyor; daha sakin bir şey söylüyor: bu teknoloji, kurumların gündelik iş yapma biçimine yerleşti.

Stanford Üniversitesi'nin 2025 tarihli Yapay Zekâ Endeksi raporuna göre 2024 yılında kurumların yüzde 78'i en az bir iş sürecinde yapay zekâ kullandı; bir yıl önce bu oran yüzde 55'ti. McKinsey'nin 2025 küresel araştırması da benzer bir tabloyu, yüzde 88'e ulaşan bir kullanım oranını işaret ediyor. Bu tablo bir devrim ilanı değil, bir zemin tespiti: yapay zekâ artık ayrıksı bir tercih değil, olağan bir araç.

Sivil toplum da bu tablonun dışında değil. Bir proje raporunun ilk taslağı, bir sosyal medya duyurusunun çevirisi, bir etkinlik metninin düzeltisi derken yapay zekâ pek çok derneğin masasına çoktan oturdu. Sorun kullanımın kendisinde değil; kullanımın çoğu zaman yazılı bir kural, ortak bir akıl ve güvenlik süzgeci olmadan gerçekleşmesinde.

Aynı raporlar madalyonun öteki yüzünü de kaydediyor: Stanford'un derlediği verilere göre 2024'te raporlanan yapay zekâ bağlantılı olay sayısı 233'e ulaştı; bu, bir önceki yıla göre yüzde 56'yı aşan bir artış demek. Kullanım yaygınlaştıkça yan etkiler de görünür hale geliyor. Bir sonraki bölüm, bu iki eğilimin, yaygınlaşma ile riskin, güvenlik alanında nasıl aynı anda büyüdüğüne bakıyor.

KAYIT: İKİ CEPHE

4,88

MİLYON DOLAR: ORTALAMA VERİ İHLALİ MALİYETİ, %10 ARTIŞLA REKOR SEVİYE (IBM, 2024)

2,2

MİLYON DOLAR: GÜVENLİKTE YAPAY ZEKÂ VE OTOMASYONU YAYGIN KULLANANLARIN İHLAL BAŞINA ORTALAMA TASARRUFU (IBM, 2024)

%60

YAPAY ZEKÂ İLE OTOMATİK ÜRETİLEN OLTALAMA E-POSTALARINA KANAN KATILIMCILAR (HEIDING VD., 2024)

DOSYA 02

Madalyonun iki yüzü: Aynı teknoloji, iki ayrı cephe

Siber güvenlikte yapay zekânın tuhaf bir özelliği var: masanın iki tarafında da oturuyor. Savunan da saldıran da aynı raftan besleniyor. Bu yüzden soru, yapay zekânın güvenlik için iyi mi kötü mü olduğu değil; kimin elinde, hangi özenle çalıştığı.

Savunma tarafında: daha erken fark etmek, daha az kaybetmek

IBM'in 2024 tarihli veri ihlali maliyeti araştırması, bir ihlalin kurumlara ortalama 4,88 milyon dolara mal olduğunu ortaya koydu; bu, bir önceki yıla göre yüzde 10 artış ve o güne dek ölçülen en yüksek seviye. Aynı araştırmanın daha az konuşulan bulgusu ise şu: güvenlik süreçlerinde yapay zekâ ve otomasyonu yaygın biçimde kullanan kurumlar, ihlal başına ortalama 2,2 milyon dolar daha az kayıp yaşadı ve ihlalleri belirgin biçimde daha kısa sürede tespit edip kontrol altına aldı. Teknoloji, doğru kurgulandığında, olayı büyümeden yakalayan bir erken uyarı sistemine dönüşüyor.

Saldırı tarafında: oltalama ucuzladı ve ustalaştı

Aynı yetenekler kötü niyetli ellerde de çalışıyor. Harvard Business Review'da 2024'te yayımlanan ve Fredrik Heiding ile Bruce Schneier'in de aralarında bulunduğu araştırmacılarca yürütülen deneyde, tamamı yapay zekâ ile otomatik üretilen oltalama e-postaları katılımcıların yaklaşık yüzde 60'ını tuzağa düşürdü; bu, insan uzmanların elle hazırladığı e-postalarla aynı seviye. Üstelik sürecin otomasyonu, bir oltalama kampanyasının maliyetini yüzde 95'ten fazla düşürüyor. Daha ucuz ve daha ikna edici saldırı, daha çok saldırı demek.

KAYIT: VAKA + İNSAN

%68

İÇİNDE KÖTÜ NİYET TAŞIMAYAN İNSAN UNSURU BULUNAN İHLALLER (VERIZON, 2024)

<60sn

BİR OLTALAMA E-POSTASINA KANMA SÜRESİ, MEDYAN (VERIZON, 2024)

25

MİLYON DOLAR: TEK BİR DEEPFAKE GÖRÜNTÜLÜ TOPLANTIYLA AKTARILAN TUTAR (CNN, 2024)

VAKA NOTU · ŞUBAT 2024 · HONG KONG

Toplantıdaki herkes sahteydi. Bir şirketin finans çalışanı, görüntülü toplantıda gördüğü finans direktörünün talimatıyla yaklaşık 25 milyon dolarlık transferi onayladı. Toplantıdaki yöneticilerin tamamı, ses ve görüntüsü yapay zekâ ile üretilmiş taklitlerdi; şirketin uluslararası mühendislik firması Arup olduğu sonradan doğrulandı.

Vakanın dersi teknik değil, davranışsal: görüntü ve ses artık tek başına kimlik kanıtı sayılamaz. Para ve veri talepleri, tutar ve aciliyet ne olursa olsun, ikinci bir kanaldan teyit edilmeli.

İnsan tarafı da tabloyu tamamlıyor. Verizon'un 2024 veri ihlali araştırmasına göre ihlallerin yüzde 68'inde kötü niyet taşımayan bir insan unsuru var: yanlış tıklama, yanlış alıcıya gönderim, sahte bir talebe iyi niyetle yanıt. Aynı rapor, bir oltalama e-postasına kanma süresinin medyanda bir dakikanın altında olduğunu kaydediyor.

Avrupa Birliği Siber Güvenlik Ajansı ENISA'nın 2024 tehdit görünümü raporu da aynı eğilimi kurumsal ölçekte doğruluyor: sosyal mühendislik yükselişte ve bilgi manipülasyonunun yapay zekâ ile beslenen biçimleri artık ayrı bir başlık olarak izleniyor. Saldırının hedefi çoğu zaman sistem değil, sistemin başındaki insan; bu yüzden savunmanın da ilk katmanı teknoloji değil, teyit alışkanlığı.

> Savunan da saldıran da aynı raftan besleniyor. Fark, teknolojide değil; kimin elinde, hangi özenle çalıştığında.

Bu iki cepheli tablo, sivil toplum için soyut bir uzmanlık tartışması değil. Bir sonraki bölümün konusu tam olarak bu: bütçesi küçük, verisi kıymetli kurumlar bu denklemin neresinde duruyor?

KAYIT: HEDEF ANALİZİ

600mn+

MICROSOFT MÜŞTERİLERİNİN HER GÜN KARŞILAŞTIĞI SALDIRI GİRİŞİMİ (MICROSOFT, 2024)

MICROSOFT'UN TEHDİT İSTİHBARATI, DÜŞÜNCE KURULUŞLARI VE SİVİL TOPLUM ÖRGÜTLERİNİ DEVLET BAĞLANTILI AKTÖRLERİN EN ÇOK HEDEF ALDIĞI SEKTÖRLER ARASINDA SAYIYOR.

DOSYA 03

Hedefteki sivil toplum: Küçük olmak görünmez olmak değil

Sivil toplumda sık duyulan bir cümle var: bizde çalınacak ne var ki? Cevap, kasada aranınca bulunamıyor; çünkü aranacak yer orası değil. Bir gençlik derneğinin arşivinde kimlik fotokopileri, veli izin formları, sağlık beyanları, banka dekontları, kırılgan gruplara ait iletişim listeleri durur. Bunların her biri, kötü niyetli biri için başlı başına bir değerdir. Kurumun adı ve güveni de öyle: ele geçirilen bir dernek hesabından gönderilen sahte bağış çağrısı, yıllarda kurulan güveni dakikalarda harcayabilir.

Ölçek konusunda da yanılsamaya yer yok. Microsoft'un 2024 Dijital Savunma Raporu, müşterilerinin her gün 600 milyondan fazla saldırı girişimiyle karşılaştığını kaydediyor; aynı rapor, düşünce kuruluşları ile sivil toplum örgütlerinin devlet bağlantılı aktörlerin en çok hedef aldığı sektörler arasında yer aldığını not ediyor. Saldırıların büyük bölümü ise kimseyi özel olarak seçmiyor: otomatik taramalar, zayıf parolaları ve güncellenmemiş sistemleri kim olursa olsun buluyor. Kapıyı deneyen el, tabeladaki ismi okumuyor.

Sivil toplumu ayrıca kırılgan kılan, kendi çalışma biçimi. Gönüllüler gelir ve gider; hesaplar ortak kullanılır; işler kişisel telefonlardan ve ev bilgisayarlarından yürür; biten projenin alan adı ve yönetim paneli kimseye zimmetli olmadan açıkta kalır. Bunların hiçbiri bir kusur değil, sahanın gerçeği. Ama her biri, küçük bir düzenlemeyle kapatılabilecek birer kapı.

> Saldırıların çoğu kurumun büyüklüğüne bakmıyor; açık kapıya bakıyor. Küçük olmak koruma sağlamıyor, düzenli olmak sağlıyor.

KAYIT: HUKUKİ ÇERÇEVE

6698

SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU: DERNEKLER DE BİRER VERİ SORUMLUSU

72saat

KURUL UYGULAMASINDA VERİ İHLALİNİN KURUMA BİLDİRİLMESİ İÇİN BEKLENEN SÜRE

2026

AB YAPAY ZEKÂ YASASI'NDA YÜKSEK RİSKLİ SİSTEM YÜKÜMLÜLÜKLERİNİN BÜYÜK BÖLÜMÜNÜN BAŞLANGICI (AĞUSTOS)

DOSYA 04

Verilmiş bir söz olarak veri koruma

Bir gencin veli izin formu yalnızca bir evrak değildir; ailesinin kuruma duyduğu güvenin imzalı halidir. Veri koruma mevzuatını bir yük gibi değil, bu güvenin hukuki karşılığı gibi okumak, işi hem kolaylaştırır hem anlamlandırır. Kural, özen borcunun yazıya dökülmüş biçimidir.

Türkiye'de çerçeveyi 6698 sayılı Kişisel Verilerin Korunması Kanunu çiziyor ve dernekler de bu kanun karşısında birer veri sorumlusu. Bunun pratik anlamı birkaç cümleyle özetlenebilir: kişiye verisinin neden istendiğini açıkça söylemek, veriyi yalnızca söylenen amaç için kullanmak, gerekenden fazlasını hiç toplamamak, işi biten veriyi saklamayıp yok etmek ve bir ihlal yaşanırsa bunu saklamamak. Kurul uygulamasında veri ihlallerinin öğrenilmesinden itibaren 72 saat içinde Kuruma bildirilmesi beklenir. En sağlam ilke ise en yalını: toplamadığınız veri sızamaz.

Avrupa boyutu da uzak değil. Erasmus+ ortaklıklarında katılımcı listeleri, fotoğraflar ve raporlar sınırlar arasında dolaşır; bu da Avrupa Birliği'nin veri koruma ilkeleriyle uyumu kendiliğinden gündeme getirir. Buna 2024'te bir katman daha eklendi: Avrupa Birliği Yapay Zekâ Yasası, 2024/1689 sayılı tüzük olarak yürürlüğe girdi ve yapay zekâ sistemlerini taşıdıkları riske göre kademelendirdi. Kabul edilemez uygulamalara ilişkin yasaklar Şubat 2025'te, genel amaçlı modellere ilişkin yükümlülükler Ağustos 2025'te devreye girdi; yüksek riskli sistemlere ilişkin yükümlülüklerin büyük bölümü ise takvim gereği Ağustos 2026'da uygulanmaya başlayacak.

Sivil toplum için buradaki mesaj mevzuat ezberi değil; kullanılan aracın ne yaptığını bilmek, insan gözetimini elden bırakmamak ve şeffaf olmak. Bu üç tutum, hem KVKK'nın hem de Avrupa çerçevesinin özüne denk düşüyor ve bir sonraki bölümdeki adımların da omurgasını oluşturuyor.

KAYIT:
UYGULAMA FORMU

%66

ÖNÜMÜZDEKİ YIL SİBER GÜVENLİĞİ EN ÇOK YAPAY ZEKÂNIN ETKİLEYECEĞİNİ DÜŞÜNEN YÖNETİCİLER (WEF, 2025)

%37

YAPAY ZEKÂ ARAÇLARINI DEVREYE ALMADAN ÖNCE GÜVENLİĞİNİ DEĞERLENDİREN BİR SÜRECE SAHİP KURUMLAR (WEF, 2025)

DOSYA 05

Küçük adımlar: Sahada gerçekten işe yarayanlar

Dünya Ekonomik Forumu'nun 2025 Küresel Siber Güvenlik Görünümü, konunun bilinirliği ile kurumsal hazırlık arasındaki açıklığı iyi özetliyor: yöneticilerin yüzde 66'sı önümüzdeki yıl siber güvenliği en çok yapay zekânın etkileyeceğini düşünüyor; buna karşılık kurumların yalnızca yüzde 37'si bir yapay zekâ aracını devreye almadan önce güvenliğini değerlendiren bir sürece sahip. Farkındalık var, alışkanlık yok. SECURE-CS'in çalıştığı yer tam olarak bu aralık.

Aşağıdaki on adımın hiçbiri pahalı bir yazılım gerektirmiyor; hepsi karar, düzen ve biraz süreklilik istiyor. Kurumun bir kişilik de olsa, bu liste aynı listedir. Kutucuklar bilerek boş bırakıldı: bu sayfa okunmak için değil, işaretlenmek için tasarlandı.

- ☐ 01 **Çok faktörlü doğrulamayı her yerde açın.** E-posta, bulut depolama, sosyal medya ve bankacılık başta olmak üzere kritik hesapların tamamında ikinci doğrulama adımı kullanın; tek başına bu adım, ele geçirme girişimlerinin büyük bölümünü boşa çıkarır.

- ☐ 02 **Parola yöneticisine geçin.** Her hesap için ayrı ve güçlü parolayı akılda tutmak mümkün değil; bir parola yöneticisi bunu kurumsal bir alışkanlığa çevirir ve ortak parola dolaşan kağıtları ortadan kaldırır.

- ☐ 03 **Güncellemeleri kendiliğinden hale getirin.** İşletim sistemi, tarayıcı ve eklentilerde otomatik güncellemeyi açın; bilinen açıkların çoğu, yaması aylardır hazır olduğu halde kapatılmadığı için istismar edilir.

- ☐ 04 **Yedeği alın ve geri dönüşü deneyin.** Önemli verinin birden fazla kopyasını, en az biri farklı ortamda olacak biçimde tutun; yılda bir kez de gerçekten geri yükleyip çalıştığını görün, denenmemiş yedek yedek değildir.

- ☐ 05 **Hesap envanteri çıkarın, ayrılışta erişimi kapatın.** Hangi hesap kimde, hangi yetkiyle var, tek bir listede dursun; bir gönüllü ya da çalışan ayrıldığında erişimlerinin kapatılması, veda kahvesi kadar doğal bir adım olsun.

KAYIT:
UYGULAMA FORMU

BU FORMUN ÇEVRİMİÇİ KARŞILIĞI: PROJENİN ÖZ DEĞERLENDİRME PLATFORMU ÜZERİNDEN KURUMUNUZUN DİJİTAL GÜVENLİK FOTOĞRAFINI ÇEKEBİLİRSİNİZ.

civilsociety security.net

- ☐ 06 **Para ve veri taleplerini ikinci kanaldan teyit edin.** E-posta, mesaj ya da görüntülü aramayla gelen transfer ve bilgi taleplerini, aciliyet baskısına aldırmadan bilinen bir numaradan geri arayarak doğrulayın; ses ve görüntünün taklit edilebildiği bir dönemde bu tek cümlelik kural çok şey kurtarır.

- ☐ 07 **Yetkileri sadeleştirin.** Herkese her yetki yerine, herkese işi kadar yetki verin; kullanılmayan yönetici hesaplarını ve ortak kullanılan oturumları kapatın.

- ☐ 08 **Yapay zekâ kullanımına dair bir sayfalık kural yazın.** Hangi bilgilerin araçlara girilebileceğini ve girilemeyeceğini, çıktının yayımlanmadan önce kimin gözünden geçeceğini ve gerektiğinde yapay zekâ desteğinin nasıl belirtileceğini yazılı hale getirin; bir sayfa yeter.

- ☐ 09 **Olay anı planınız hazır olsun.** Bir şey ters gittiğinde kimin aranacağı, hangi parolaların değiştirileceği ve gerekiyorsa ihlal bildiriminin nasıl yapılacağı tek sayfada yazsın; kriz anı, plan yazma anı değildir.

- ☐ 10 **Kendinizi düzenli aralıklarla sınayın.** Güvenlik bir kerelik proje değil, aralıklarla tekrarlanan bir kontrol alışkanlığıdır; yılda bir öz değerlendirme, tabloyu güncel tutar.

Bu adımların kurumunuzdaki karşılığını görmek isterseniz, projenin dijital güvenlik analizi platformu **civilsocietysecurity.net** üzerinden kendi kurumunuzun fotoğrafını çekebilirsiniz. Müfredat ve araç seti dahil projeye dair tüm bilgi ve yayınlar ise projenin web sitesi **civilsocietysecurity.com** adresinde bir arada; iki çıktı da tüm ekosistemin kullanımına açık.

KAYIT: SONUÇ

6

ORTAK KURUM · TÜRKİYE, BELÇİKA, NORVEÇ, BOSNA-HERSEK

2

TEMEL ÇIKTI: DİJİTAL GÜVENLİK MÜFREDATI/ ARAÇ SETİ VE ÇEVRİMİÇİ ANALİZ PLATFORMU

2026

PROJENİN TAMAMLANACAĞI YIL (30 HAZİRAN)

KAPANIŞ

Kapanırken

Bu dosyada hız kesmeyen bir teknolojiyi telaşsız anlatmaya çalıştık. Çünkü sahadaki deneyim şunu söylüyor: güvenlik, panikle değil düzenle kurulur. Araçlar değişecek, modeller yenilenecek, bugün konuşulan tehditlerin yerini başkaları alacak. Değişmeyecek olan, insanların verisini emanet aldığımız gerçeği ve bu emanete gösterilecek özen.

SECURE-CS ortaklığı, bu özenin öğrenilebilir ve paylaşılabilir olduğunu gösteriyor. Farklı ülkelerde ve farklı ölçeklerde çalışan altı kurum aynı sonuçta buluşuyor: dijital güvenlik bir ürün değil, ekipçe edinilen bir alışkanlıktır. Müfredat, araç seti ve öz değerlendirme platformu bu alışkanlığın başlangıç malzemeleri olarak ortada duruyor.

Gerisi, her kurumun kendi masasında başlıyor: bir parola yöneticisi kurmakla, bir yetki listesi çıkarmakla, bir teyit telefonu açmakla. Küçük adımlar, tam da bu yüzden küçümsenmemeli.

> Teknoloji değişir; emanete gösterilen özen değişmez. Güvenlik bir ürün değil, ekipçe edinilen bir alışkanlıktır.

Yararlanılan Kaynaklar

CNN. (2024, 4 Şubat). *Finance worker pays out $25 million after video call with deepfake 'chief financial officer'.* https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk

European Commission. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024.* ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Heiding, F., Schneier, B., & Vishwanath, A. (2024, 30 Mayıs). *AI will increase the quantity - and quality - of phishing scams.* Harvard Business Review. https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams

IBM. (2024). *Cost of a data breach report 2024.* IBM Security. https://www.ibm.com/reports/data-breach

Kişisel Verilerin Korunması Kanunu, Kanun No. 6698. (2016, 7 Nisan). *Resmî Gazete* (Sayı: 29677). https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

McKinsey & Company. (2025). *The state of AI: How organizations are rewiring to capture value.* QuantumBlack, AI by McKinsey. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

Microsoft. (2024). *Microsoft digital defense report 2024.* Microsoft Security. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Stanford University, Institute for Human-Centered Artificial Intelligence. (2025). *Artificial intelligence index report 2025.* Stanford HAI. https://hai.stanford.edu/ai-index

Verizon. (2024). *2024 data breach investigations report.* Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

World Economic Forum. (2025). *Global cybersecurity outlook 2025.* WEF. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

Proje Künyesi

YAYIN BAŞLIĞI

Yapay Zekâ Çağında Sivil Toplum ve Dijital Güvenlik: Bilgi ve veri güvenliği üzerine bir saha dosyası

YAYIN TÜRÜ

Proje yaygınlaştırma yayını / saha dosyası

PROJE REFERANS NO

2023-1-TR01-KA220-YOU-000161230

PROJE SÜRESİ

01.12.2023 - 30.06.2026

KOORDİNATÖR

SETA - Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı (Türkiye)

HAZIRLAYAN

Gülşen Nişli · Uzman Araştırmacı, ANKA Gelecek ve Yenilik Derneği (Proje Ortağı) adına

PROGRAM / EYLEM

Erasmus+ · KA220-YOU (Gençlik Alanında İşbirliği Ortaklıkları)

HİBE MODELİ

Götürü bedel (Lump Sum) · 250.000,00 €

PROJE WEB SİTESİ / ANALİZ PLATFORMU

civilsocietysecurity.com · civilsocietysecurity.net

YER VE TARİH / DİL

İstanbul, Aralık 2025 · Türkçe

ANKA'NIN ROLÜ

Proje Ortağı

ORTAKLAR

BRAVO - Bosnian Representative Association for Valuable Opportunities (Bosna-Hersek) · TtB (Norveç) · SETA Foundation for Political, Economic and Social Research (Belçika) · Türkiye Gençlik Vakfı - TÜGVA (Türkiye) · ANKA Gelecek ve Yenilik Derneği (Türkiye)

ÖNERİLEN ATIF · APA 7

Nişli, G. (2025). *Yapay zekâ çağında sivil toplum ve dijital güvenlik: Bilgi ve veri güvenliği üzerine bir saha dosyası* [Proje yayını]. SECURE-CS: Civil Society Initiatives Strengthened with Information and Data Security (Erasmus+ Proje No. 2023-1-TR01-KA220-YOU-000161230). ANKA Gelecek ve Yenilik Derneği.

SORUMLULUK REDDİ · DISCLAIMER

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Avrupa Birliği tarafından finanse edilmektedir. İfade edilen görüş ve düşünceler yalnızca yazar(lar)a ait olup Avrupa Birliği'nin veya Avrupa Eğitim ve Kültür Yürütme Ajansı'nın (EACEA) görüşlerini yansıtmayabilir. Ne Avrupa Birliği ne de EACEA bunlardan sorumlu tutulabilir.

EKOSİSTEMİN KULLANIMINA AÇIKTIR
SECURE-CS · 2025