DET

Dijital Özgürlük ve Etik Teknoloji

www.xmeroriginals.com

DET kapsamlı gizlilik rehberine hoş geldiniz. Dijital dünyada kendinizi güvende tutmanın yollarını birlikte keşfedeceğiz.

Öncelikle “Neden sanal dünyada kendimizi güvende tutmalıyız? Şirketler verilerimizi ne yapsın?” sorularına cevap verelim;

Bu sorular, dijital çağda yaşayan pek çok kişinin aklından geçen, oldukça meşru sorulardır. Hatta sıkça duyduğumuz bir argüman vardır: "Benim saklayacak bir şeyim yok ki, verilerimi istedikleri gibi kullanabilirler." Ancak mesele, saklanacak bir sır olmasından çok daha derindir. Mesele, kontrolün kimde olduğudur. Tıpkı evimizin kapısını kilitlerken içeride yasa dışı bir şey sakladığımız için değil, mahremiyetimizi, güvenliğimizi ve özel alanımızı korumak için yaptığımız gibi, dijital dünyada da kapılarımızı kilitlemeliyiz.

Peki, neden bu kadar önemli?
Dijital ayak izimiz, yani internette bıraktığımız her bir beğeni, arama, yorum ve konum bilgisi, devasa bir yapbozun parçalarını oluşturur. Bu parçalar birleştiğinde, kim olduğumuzu, ne sevdiğimizi, nelerden korktuğumuzu, politik görüşümüzü ve hatta sağlık durumumuzu ortaya çıkaran detaylı bir portre çizer. Bu portrenin yanlış ellere geçmesi şu riskleri doğurur:

1. **Kimlik Hırsızlığı ve Finansal Dolandırıcılık**: En somut tehlikedir. Adınız, adresiniz, T.C. kimlik numaranız gibi temel bilgileriniz, adınıza kredi kartı çıkarılmasına, banka hesaplarınızın boşaltılmasına veya sahte profiller oluşturulmasına zemin hazırlayabilir.

2. **Manipülasyon ve Davranış Yönlendirme**: Verileriniz, sadece size ayakkabı reklamı göstermek için kullanılmaz. Siyasi tercihlerinizi etkilemek, sizi belirli bir düşünce kalıbına sokmak (yankı odaları yaratmak) ve hatta tüketim alışkanlıklarınızı kökten değiştirmek için kullanılabilir. Gördüğünüz haberler, karşınıza çıkan içerikler, sizin zaaflarınıza ve eğilimlerinize göre özenle seçilir.

3. **İtibar ve Kariyer Yönetimi**: Yıllar önce yaptığınız bir yorum, uygunsuz bir fotoğraf veya katıldığınız bir grup, gelecekte bir iş başvurusunda veya sosyal çevrenizde karşınıza bir engel olarak çıkabilir. İnternet unutmaz ve bu dijital geçmiş, itibarınızı kolayca zedeleyebilir.
4. **Kişisel Güvenlik ve Taciz**: Konum bilgileriniz, günlük rutinleriniz ve kişisel detaylarınız, kötü niyetli kişiler (stalker'lar) tarafından takip edilmenizi ve tacize uğramanızı kolaylaştırır. Nerede olduğunuz bilgisi, en kritik kişisel verilerden biridir.

Şirketler Verilerimizi Ne Yapsın?
Bu sorunun cevabına **Para** ve **Daha Çok Para** diyebiliriz. Dijital ekonomide veri, petrolden daha değerlidir. Ücretsiz kullandığınızı sandığınız sosyal medya platformları, arama motorları ve uygulamalar için aslında en değerli varlığınızla, yani kişisel verilerinizle ödeme yaparsınız. "Eğer bir ürün için para ödemiyorsanız, ürün sizsiniz demektir." (Andrew Lewis).

Şirketler verilerinizi temel olarak şu amaçlarla kullanır:
Hedefli Reklamcılık: Bu, en bilinen yöntemdir. İnternette arattığınız bir ürünün, ziyaret ettiğiniz her sitede karşınıza çıkmasının sebebi budur. Şirketler, reklamlarının doğru kişiye ulaşması için veri profillerini kullanarak nokta atışı yaparlar.

Profil Oluşturma (Profiling): Şirketler, topladıkları verilerle sizin bir "dijital ikizinizi" yaratır. Yaşınız, gelir düzeyiniz, ilgi alanlarınız, alışveriş alışkanlıklarınız gibi onlarca kritere göre sizi kategorize ederler. Bu profiller, size ne satılacağını, hangi fiyattan satılacağını ve ne tür mesajların sizi etkileyeceğini belirlemek için kullanılır.

Veri Satışı ve Aracılığı (Data Brokering): Belki de en endişe verici olan budur. Verilerinizi toplayan şirket, bu verileri genellikle "veri simsarları" olarak bilinen başka şirketlere satar. Bu simsarlar, farklı kaynaklardan topladıkları verileri birleştirerek çok daha detaylı profiller oluşturur ve bunları sigorta şirketlerinden pazarlama ajanslarına kadar geniş bir müşteri kitlesine pazarlar.

Risk Analizi ve Fiyat Belirleme: Sigorta şirketleri veya bankalar, sizin dijital alışkanlıklarınıza bakarak ne kadar "riskli" bir müşteri olduğunuza karar verebilir. Örneğin, sürekli riskli sporlarla ilgili aramalar yapıyorsanız, hayat sigortası priminiz bu durumdan etkilenebilir.

Kısacası, "benim verimi ne yapsınlar?" sorusunun cevabı nettir: Sizi analiz etmek, davranışlarınızı tahmin etmek, kararlarınızı yönlendirmek ve en nihayetinde sizin üzerinizden devasa bir ekonomi yaratmak içindir. Ve bu oyun, sadece verilerinizi verdiğiniz tek bir şirketle sınırlı değildir. Asıl tehlike, buzdağının görünmeyen kısmında yatar. Verileriniz, adını bile duymadığınız yüzlerce veri simsarının, reklam ağının ve iş ortağının dahil olduğu dev bir ekosistemde sürekli alınıp satılır. Siz bir uygulamaya "**kabul et**" dediğinizde, aslında o uygulamanın tüm bu görünmez ortaklar ağına da kapıyı açmış olursunuz. Daha da endişe verici olanı, bu durum sadece sizi etkilemez. Bir uygulamaya "**kişilere izin ver**" izni verdiğinizde, o uygulamayı hiç kullanmamış arkadaşlarınızın, ailenizin, iş çevrenizin bilgilerini de kendi rızaları olmadan bu veri havuzuna hediye etmiş olursunuz. Şirketler, bu verileri birleştirerek sizin sosyal çevrenizi ve ilişki ağınızı kusursuz bir şekilde haritalandırır. Bu yüzden, “saklayacak bir şeyim yok” argümanı artık geçerli değildir.

Dijital Kalenizin Kapıları
Uygulama İzinlerini Yönetme Sanatı

Artık pratiğe geçelim. Dijital dünyadaki en büyük gedikler, cebimizde taşıdığımız akıllı telefonlardaki uygulamalardır. Peki bu kapıları nasıl kontrol altında tutabiliriz? İşe en popüler ve aynı zamanda en çok veri talep eden uygulamalardan biriyle, Instagram (ve genelleme yaparak tüm Meta uygulamaları/ürünleri) ile başlayalım. Sadece Instagram çok veri topluyor gibi düşünmeyin, Meta gibi tekel ve veri mahremiyetinin V’si olmayan korkunç bir sürü şirket bulunmakta. Instagram’a değinme sebebimiz milyarlarca kullanıcısı olan bir uygulamaya olması, tehlikenin daha kolay anlaşılmasını sağlayacaktır.

Örnek Vaka: Bir Veri Canavarını Evcilleştirmek (Instagram) Meta gibi şirketlerin uygulamaları, işlevlerini yerine getirmek için gerekenden çok daha fazla veriye erişmek üzere tasarlanmıştır. Onlara karşı alabileceğimiz en etkili önlemler şunlardır:

1. **En Güçlü Kalkan**: Derin Uyku Modu Çoğu Android cihazda bulunan "Derin Uyku" özelliği, kullanmadığınız zamanlarda bir uygulamanın arka planda çalışmasını, veri toplamasını ve internete erişmesini tamamen engeller. Instagram gibi bir uygulamayı derin uykuya almak, en önemli önlemlerden biridir. Evet, bildirimleriniz gecikebilir veya hiç gelmeyebilir, ancak bu küçük bedel, büyük bir güvenlik kazanımı sağlar. **Neden bu kadar önemli?** Unutmayın, Meta gibi geçmişi veri skandallarıyla dolu bir şirket, yakın zamanda kullanıcıların bilgisi dışında cihazlarda port açan ve uygulama içi tarayıcı üzerinden tüm aktiviteleri dinleyen yapılar kurmakla suçlandı. Gün yüzüne çıktıktan sonra "kaldırdıklarını" söyleseler de bu, bize şu gerçeği hatırlatır: “Bir şirketin dün yaptıkları, yarın neler yapabileceğinin en net göstergesidir.” Bu yüzden, geçmişi kirli ve doymak bilmez bir iştahla izin isteyen uygulamalara asla tam güvenmeyin.

2. **İzinleri Mikroskop Altına Alın**: Parça Parça Kontrol Bir uygulamaya "tüm izinleri ver" demek, evinizin anahtarını tanımadığınız birine teslim etmek gibidir. Bunun yerine kontrolü elinize alın: **Kamera** ve **Mikrofon** bu izinleri kalıcı olarak vermeyin. "**Sadece uygulamayı kullanırken izin ver**" veya "**Her defasında sor**" seçeneğini işaretleyin. Böylece uygulama, sadece siz istediğinizde bu hassas donanımlara erişebilir. * **Galeri/Depolama** uygulamanın tüm galerinizi taramasına izin vermek yerine, "**Belirli fotoğrafları/videoları seç**" iznini kullanın. Bu sayede sadece paylaşmak istediğiniz içeriği görür, geri kalan özel anılarınız size ait kalır. **Kişiler (Rehber) a**sla vermeyin, Bir sosyal medya uygulamasının rehberinize erişmesi için geçerli bir sebep yoktur. Bu izni vermek, sadece kendi mahremiyetinizi değil, aynı zamanda rehberinizdeki arkadaşınızın, ailenizin verilerini de onların rızası olmadan bir şirketlere hediye etmektir. Bu izni vermemek, çevrenizdeki insanların mahremiyetine duyduğunuz saygının bir göstergesidir.

Her Uygulama İçin Altın Kurallar

Güvenme, Sorgula, Kontrol Et. Bu prensipler sadece Instagram için değil, telefonunuza kurduğunuz her bir uygulama için geçerlidir. Unutmayın, uygulama mağazaları (Play Store, App Store vb.) birer süpermarket gibidir; raflarda güvenli ürünler olsa da son kullanma tarihi geçmiş veya içeriği şüpheli olanlar da bulunabilir. Bir uygulamayı indirmeden önce kendinize şu soruları sorun:

1. **Gerçekten İhtiyacım Var Mı?**
Anlık bir hevesle indirilen ve unutulan uygulamalar, arka planda çalışan birer casusa dönüşebilir. Sadece gerçekten ve sürekli kullanacağınızdan emin olduğunuz uygulamaları kurun.

2. **Yayıncı Kim?**
Uygulamayı indirmeden önce yayıncının adına tıklayın. Geçmişini, diğer uygulamalarını ve kullanıcı yorumlarını hızlıca araştırın. Adı sanı duyulmamış, şüpheli bir şirket mi, yoksa sektörde itibarı olan bir geliştirici mi?

3. **Bu İzin Neden Gerekli?**
Uygulama sizden bir izin istediğinde, otomatik olarak "kabul et" butonuna basmayın. Bir saniye durun ve kendinize şu sihirli soruyu sorun: "**Bu uygulamanın temel işlevini yerine getirmesi için bu izne gerçekten ihtiyacı var mı?**". Bir el feneri uygulamasının kişilerinize erişmesi şüphelidir. Basit bir not defteri uygulamasının konumunuzu istemesi anlamsızdır. Bir fotoğraf düzenleme uygulamasının mikrofonunuza erişmesi tehlike çanlarını çaldırmalıdır.

Geçmişi ne kadar temiz olursa olsun, hiçbir şirkete körü körüne güvenmeyin. Her zaman "**en az ayrıcalık prensibi**" ile hareket edin: Bir uygulamaya, çalışması için gereken minimum düzeyde izin verin. Kontrol sizde ve bu kontrolü kullanmak, dijital dünyadaki en temel hakkınızdır.

Dijital Dünyaya Açılan Pencereniz

Tarayıcı Gizliliği Dijital kalenizin ana kapısı ve pencereleri, her gün saatlerce kullandığınız internet tarayıcınızdır. E-postalarınızı kontrol ettiğiniz, haber okuduğunuz, alışveriş yaptığınız bu pencere, aynı zamanda en savunmasız olduğunuz yerdir. Hatta durum sandığınızdan daha da kritik: Kullandığınız birçok mobil uygulama (örneğin sosyal medya uygulamalarının içindeki linklere tıkladığınızda açılan sayfalar) aslında "WebView" adı verilen mini, gömülü tarayıcılardır (ki bu tarayıcıda yaptığınızı uygulama adım adım takip edebilir).

Bu da demek oluyor ki, tarayıcınızdaki güvenlik açıkları ve gizlilik ayarları, sadece bilgisayarınızda gezinirken değil, telefonunuzdaki uygulamaları kullanırken bile sizi doğrudan etkiler. Peki bu görünmez tehlikeler nelerdir ve pencerelerinize nasıl sağlam kilitler takabilirsiniz?

Görünmez Takipçiler: Çerezler ve Script'ler İnternette gezindiğinizde, arkanızda dijital ekmek kırıntıları bırakırsınız. Bu kırıntıların en yaygın olanları şunlardır:

Çerezler (Cookies): Küçük metin dosyalarıdır. Bazıları (1. taraf çerezler) işe yarardır; örneğin bir siteye tekrar girdiğinizde sizi hatırlamasını sağlarlar. Ancak asıl tehlike **3. taraf çerezlerdir**. Bunlar, ziyaret ettiğiniz siteye değil, o sitedeki bir reklamcıya veya veri analiz şirketine aittir. Bu çerezler sayesinde aynı reklam şirketi, sizi A sitesinden B sitesine, oradan da C sitesine kadar takip edebilir ve hakkınızda detaylı bir profil oluşturabilir.

Takip Script'leri (Trackers): Web sitelerine gömülmüş küçük kod parçacıklarıdır. Fare hareketlerinizi, ne kadar süreyle hangi içeriğe baktığınızı, hangi linklere tıkladığınızı ve daha birçok detayı kaydederek sizi adeta dijital bir gölge gibi izlerler. Siz farkında bile olmadan, onlarca farklı şirket sizin internet kullanım alışkanlıklarınızı analiz eder. İşte bu takibi kırmanın yolları:

Adım 1 Doğru Aracı Seçin veya Mevcut Aracınızı Güçlendirin
1.1 Gizlilik Odaklı Bir Tarayıcıya Geçin (Öneri: Firefox) Piyasada Google Chrome gibi popüler tarayıcılar olsa da, unutmayın ki bu tarayıcıların arkasındaki şirketlerin ana gelir modeli reklamcılıktır. **Mozilla Firefox** ise, kâr amacı gütmeyen bir vakıf tarafından geliştirilir ve temel misyonu kullanıcı gizliliğini ve açık interneti savunmaktır. Firefox, kutudan çıktığı haliyle bile "Gelişmiş Takip Koruması" özelliği sayesinde birçok 3. taraf çerezini ve takip script'ini otomatik olarak engeller.
1.2 Mevcut Tarayıcınızın Ayarlarını Sıkılaştırın. Eğer kullandığınız tarayıcıdan vazgeçmek istemiyorsanız, kaputun altını açıp birkaç vidayı sıkmanız gerekir1. **3. Taraf Çerezlerini Engelleyin,** Tarayıcınızın gizlilik ayarlarına gidin (Ayarlar > Gizlilik ve Güvenlik) ve "**Tüm üçüncü taraf çerezlerini engelle**" seçeneğini bulun ve etkinleştirin. Bu tek başına, siteler arası takibi büyük ölçüde azaltacaktır. 2. "**Hepsini Reddet**" Alışkanlığı Edinin, Bir siteye girdiğinizde karşınıza çıkan "**Çerezleri Kabul Et**" penceresi bir tuzaktır. Genellikle "**Tümünü Kabul Et**" butonu büyük ve renkliyken, "Reddet" veya "Ayarları Yönet" linkleri küçücük ve saklıdır. O bir-iki saniyeyi ayırıp "**Tümünü Reddet**" seçeneğini bulun. Eğer yoksa, "**Ayarları Yönet**" kısmına girip tüm isteğe bağlı çerezleri kapatın. Bunu bir refleks haline getirin.

Adım 2 Tarayıcınıza Güçlü Zırhlar Ekleyin (Eklentiler)
Tarayıcınızı koruma eklentileri, dijital kalenizin bekçileri gibidir. Doğru eklentilerle, siz farkına bile varmadan yüzlerce tehdidi kapıda durdurabilirsiniz. İşte olmazsa olmaz bir eklenti: **uBlock Origin** veya **uBlock Origin Lite**: Bu, sadece bir reklam engelleyiciden çok daha fazlasıdır; internetin İsviçre çakısıdır. **uBlock Origin**, bilinen reklam ağlarını, takip script'lerini ve hatta bazı zararlı yazılım sitelerini siz onlarla karşılaşmadan önce engeller. **uBlock Origin**'in size sağladığı faydalara örnek verelim:
Gizlilik - Sizi siteden siteye takip eden yüzlerce görünmez takipçiyi bloke eder.
Hız - Reklamlar ve script'ler yüklenmediği için web sayfaları çok daha hızlı açılır.

Güvenlik - Kötü amaçlı yazılım içeren sahte reklamlara tıklama riskinizi ortadan kaldırır.
Tasarruf - Özellikle mobil veri kullanıyorsanız, gereksiz içerikler indirilmediği için kotanızdan tasarruf etmenizi sağlar.

Bu eklentiyi tarayıcınızın resmi eklenti mağazasından (Chrome Web Mağazası, Firefox Eklentileri vb.) birkaç tıkla kurabilirsiniz. Kurduktan sonra yapmanız gereken başka bir şey yok, arka planda sizin için sessizce çalışmaya başlar. Bu basit ama etkili iki adımın yanı sıra başka bir sürü güvenlik sağlayan tarayıcı eklentilerinide birlikte kullanabilirsiniz. Artık Tarayıcınızda da kendinizi güvence altına aldınız, dijital dünyadaki genel güvenliğiniz için atacağınız en büyük adımlardan birini tamamladınız.

Varsayılan Zincirleri Kırmak
Etik Alternatiflerle Özgürleşin

Dijital kalenizi güçlendirdiniz, pencerelerinizi (tarayıcılar) ve kapılarınızı (uygulamalar) güvence altına aldınız. Şimdi en önemli adımı atma zamanı: Kalenizin içinde kiminle konuştuğunuzu ve bilgiye nasıl ulaştığınızı seçmek. Unutmayın, "ücretsiz" hizmetler genellikle en pahalı olanlardır; çünkü para birimi sizin mahremiyetinizdir. Google ve Meta (Facebook/Instagram/WhatsApp) gibi devlerin ekosistemleri, size kolaylık sunarken arka planda her hareketinizi birer veri noktasına çevirir. Dijital özgürlük, bu ekosistemlere mahkum olmadığımızı fark etmekle başlar.

1. **İletişim**: Konuşmalarınız Sadece Size Aittir Sorun, **Meta'nın Gözetimindeki Sohbetler** WhatsApp uçtan uca şifreleme (E2EE) sunsa da, bu resmin sadece bir parçasıdır. Meta, mesajlarınızın **içeriğini** göremese de, en az onun kadar değerli olan **üst veriyi (metadata)** toplar: Kiminle, ne zaman, ne kadar süreyle ve ne sıklıkla konuştuğunuzu bilir. Bu bilgiler, sosyal çevrenizin haritasını çıkarmak ve sizi profillemek için yeterlidir. Instagram ve Facebook Messenger ise çok daha zayıf bir gizlilik sunar.

Çözüm: Gerçek Mahremiyet Sunan Etik Bir Alternatif: **Signal**.
Signal, dijital iletişimde altın standarttır. Kâr amacı gütmeyen bir vakıf tarafından geliştirilir ve tek bir amacı vardır: Kullanıcılarına güvenli ve özel bir iletişim platformu sunmak.

Neden Signal?
Kapsamlı Şifreleme: Sadece mesajlar değil, aramalar, grup sohbetleri, dosyalar ve üst veriler de dahil olmak üzere her şey mümkün olan en güçlü şekilde şifrelenir.
Sıfır Takip: **Signal**, kiminle konuştuğunuzu bilmek için tasarlanmamıştır. Hakkınızda sakladığı tek veri, hesabınızın ne zaman oluşturulduğu ve en son ne zaman bağlandığınız gibi teknik bilgilerdir. Reklam yok, takipçi yok, gizli ajanda yok.
Şeffaflık: Tamamen açık kaynak kodludur. Bu, dünyanın her yerinden güvenlik uzmanlarının kodları inceleyip güvenli olduğunu teyit edebileceği anlamına gelir.

Eyleme Geçin - Bugün en az bir arkadaşınıza Signal kurmasını önerin ve sohbetlerinizi oraya taşıyın. Özgürlük, küçük adımlarla kazanılır.

2. **Bilgiye Erişim**: Arama Geçmişiniz Kişilik Raporunuzdur Sorun, **Google'ın Hafızası** Google'da yaptığınız her arama, dijital kimliğinize eklenen bir satırdır. En derin korkularınız, sağlık sorunlarınız, meraklarınız, politik eğilimleriniz, finansal planlarınız... Hepsi bir araya getirilerek size reklam göstermek, sizi belirli içeriklere yönlendirmek ve davranışlarınızı tahmin etmek için kullanılan devasa bir profil oluşturur. Arama geçmişiniz, Google'ın en değerli ticari malıdır.

Çözüm: Sizi Profillemeyen Arama Motorları Dijital özgürlük, merakınızın bir reklam ürününe dönüştürülmediği araçları kullanmayı gerektirir. Neyse ki, harika alternatifler var:

DuckDuckGo, En popüler gizlilik odaklı arama motorudur. Aramalarınızı asla kaydetmez, sizi takip etmez ve arama sonuçlarını

tüm kullanıcılara aynı şekilde gösterir (filtre baloncuğu yaratmaz).

Brave Search, Gizliliğe odaklanan Brave tarayıcısının geliştiricileri tarafından geliştirilen, kendi arama indeksini kullanan bağımsız ve şeffaf bir alternatiftir.

Eyleme Geçin - Hemen şimdi tarayıcınızın ayarlarına gidin ve varsayılan arama motorunuzu bu alternatiflerden biriyle değiştirin. Bu, sadece 1-2 dakikanızı alacak ama gizliliğiniz üzerinde devasa etki yaratacak bir değişikliktir.

Bu etik araçları seçerek, sadece kendi verilerinizi korumakla kalmaz, aynı zamanda internetin daha adil, şeffaf ve kullanıcı odaklı bir yer olması için güçlü bir mesaj gönderirsiniz.

Unutmayın Mükemmel Gizlilik Bir Efsanedir, Ama Daha İyi Bir Gelecek Mümkündür, Bu rehber boyunca attığımız adımları uyguladıktan sonra kendinize şu soruyu sorabilirsiniz: "Peki şimdi %100 güvende miyim?" Cevabı dürüstçe verelim: **Hayır.** Dijital dünyada %100 gizlilik veya güvenlik diye bir şey yoktur. Çevrimiçi olduğumuz sürece, dijital bir iz bırakırız. **Amaç, dijital bir hayalete dönüşmek, teknolojiden kaçmak veya paranoyak bir yaşam sürmek değildir.** Bu, hem imkansız hem de sürdürülemez bir çabadır. **Asıl amaç, kontrolü geri almak ve oyunun kurallarını yeniden yazmaktır.** Bugün karşı karşıya olduğumuz **gözetim kapitalizmi**, bir gecede ortaya çıkmadı. Bizlerin yıllar boyunca süren sessiz kabullenişi, “**saklayacak bir şeyim yok**" argümanının konforu ve ücretsiz hizmetlerin cazibesi üzerine inşa edildi. Ancak bu, geleceğimiz olmak zorunda değil.

Her Seçim Bir Oydur - Geleceği Şekillendiren Hareket
Bunu, çevre hareketinin ilk günleri gibi düşünün. Bir kaç kişinin geri dönüşüm yapması gezegeni kurtarmaz. Bir kaç kişinin plastik poşet yerine bez çanta kullanması okyanusları temizlemez. Ancak milyonlarca insan bu bilinçli tercihleri yapmaya başladığında, devasa bir değişim tetiklenir:

Şirketler, sürdürülebilir ürünler yaratmak için ticari modellerini değiştirir.
Toplumda, çevreye duyarlılık bir norm haline gelir.
Ve en önemlisi, hükümetler ve yasa koyucular, bu kolektif iradeyi yansıtan yeni kanunlar ve düzenlemeler yapmak zorunda kalır.

Bizim durumumuz da bundan farksız. Attığınız her adım, daha adil ve etik bir dijital dünya için verilmiş bir **oydur**.
Tek başımıza teknoloji devlerini dize getiremeyiz ama milyonlarca **bilinçli kullanıcı**, veri toplamayı kârsız hale getiren, mahremiyete saygıyı ise bir rekabet avantajına dönüştüren bir pazar baskısı yaratabilir.

Bugün attığımız bu adımlar, yarının teknoloji liderlerine ve yasa koyucularına mahremiyetin değerli ve talep edilen bir şey olduğunu gösteren en güçlü kanıttır. Bu talep yeterince büyüdüğünde, bugün gri alanda olan birçok veri toplama pratiğinin gelecekte yasa dışı hale gelmesi kaçınılmaz olacaktır.

Dijital dünyada sadece birer tüketici değil, geleceği şekillendiren bilinçli birer yurttaş olalım. Çünkü dijital özgürlük, bize hediye edilmeyecek; onu her gün yaptığımız küçük ama kararlı seçimlerle hep birlikte inşa edeceğiz.

DET – Dijital Etik ve Teknoloji İnisiyatifi

Dijital özgürlük için birlikte.

www.xmeroriginals.com