

Sosyal Ağlarda Paylaştığınız Verilerin
Gerçek Sahibi Kim?



Kullanıcıların sosyal ağlara ilgisi arttıkça, bu ortamlarda paylaşılan verilerin sahibinin kim olduğu sorusu daha sık sorulmaya başlandı. İşin, başlarda pek dikkat çekmeyen bu yönü bugün giderek daha fazla kullanıcının endişelendiği bir konuya dönüşüyor.

Peki siz Facebook, Twitter, YouTube, Instagram gibi sitelerdeki paylaşımlarınızı hangi koşullarda bu sitelere emanet ettiğinizi, kimlerin bunlara erişim neler yapabileceğini biliyor musunuz?

Geçtiğimiz ay her ne kadar ülkemizdeki ana akım medyada pek fazla yer bulmuş olmasa da, etrafta olup bitene daha geniş bir açıdan bakmayı tercih edenler ve ceplerinde taşıdıkları küçük ekranlarda beliren parlak uyarıları dikkate alanlar, son derece rahatsız edici bir gündemle karşılaştı. Dünya, kendini bir anda uzunca süren bir sessizliğin ardından parlayan küçük bir kıvılcımın başlattığı dev bir tartışma zincirinin ortasında buldu. Betanews'ten Brian Fagoli durumun ciddiyetini şöyle özetliyordu: "İnternet bir daha asla bildiğimiz gibi olmayacak. Baskı ve özgürlük yer değiştirdi. Haklarımız günden güne eriyor. Gün geçmiyor ki yönetim yeni bir skandala imza atmasın."

Her şey, eski bir CIA teknikeri Edward Snowden'in ülkenin güvenlikten sorumlu ajansı NSA'de (*National Security Agency*-Ulusal Güvenlik Ajansı) yaşanan skandalı itiraf etmesiyle patlak verdi. NSA, başta ABD vatandaşları ve dünyanın önde gelen figürleri olmak üzere bütün dünyayı elektronik ortamda izlemeye almıştı. Üstelik ABD'nin 9 teknoloji devi, bir süredir NSA'in bu gözetleme projesi için istediği anda, istediği bilgileri alabileceği birer "arka kapı" bırakmaya zorlanmıştı. Projenin adı PRISM'di.

NSA, bu yolla ilgili servislerden ve projeye katılan telekom operatörlerinden gelen verileri topluyor ve görüşmeleri belli kelimelere göre sınıflandırarak risk analizine tabi tutuyordu. Üstelik kurgulanan sistem bilgi almak için herhangi bir mahkeme kararı olmasını da gerektirmiyordu.

Skandal ve beraberinde getirdiği tartışmalar henüz taze. Ancak eldeki bilgiler, iddiada adı geçen teknoloji şirketlerinin bu sistemden "haberi olmadığını", "kabul etmeden önce hatırı sayılır ölçüde direndiğini" veya "kullanıcı bilgilerine sınırsız erişimi zorlaştıran ara önlemleri devreye aldığını" gösteriyor. Yine de bu durum, bir ülkenin sahip olduğu teknolojik imkânlar sayesinde tüm dünyayı gözetim altına almaya çabaladığı gerçeğini değiştirmiyor (**detaylı bilgi için bit.ly/16Suv14, nyti.ms/ZYKuh ve ars.to/14UQFsG**).

Peki ya birileri, sizinle ilgili bilgilerin de peşine düşmüş, bu bilgileri ele geçirmiş, sahiplenmiş, kullanmış olabilir mi? Belki. Üstelik büyük ihtimalle bu iş için NSA kadar imtiyazlı olmaları bile gerekmiyor.

Her Şeyin Bir Bedeli Var, Güzelliğinin de

Perakende oyun satıcısı GameStation, 2010'da İngiltere'de 1 Nisan şakası olarak web sitesi üzerinden faaliyet gösteren çevrimiçi alışveriş platformunda yer alan satış anlaşması metnine ilginç bir madde eklemeye karar verdi. Eklenen bu yeni maddeye göre GameStation internet sitesinden alışveriş yapanlar, sözleşme gereği şirketin alışveriş sonrasında ruhlarına da el koyacağını kabul etmiş oluyordu. Anlaşma metninde "şirket tarafından talep edilmesi halinde ruhların 5 gün içinde teslim edilmesi gerektiği" ve "ilgili talebin kullanıcıya alev alev yanan bir mektupla iletileceği" gibi süslü ifadeler de yer alıyordu.

Kullanıcılara bu alt koşulu kabul etmeleri halinde anlaşmanın bu hükümlerini geçersiz kılmalarını sağlayacak bir seçenek de sunulmuştu. Ama neredeyse kimse o metni okumadı. Şaka bittiğinde ziyaretçilerden 7500'ü, yani anlaşma metnini onaylayanların %88'i şirketin ruhlarına el koymasını kabul etmişti.

Bu olay, her ne kadar bir şaka olsa da günlük hayatta kullandığımız servislerin kullanım koşullarını ve verilen izinlerin çerçevesini belirleyen anlaşmalara karşı kullanıcıların ne kadar ilgisiz olduğunu göstermesi açısından, düşündürücü bir örnek. Çünkü tek bir tıklamayla, okuyup kabul ettiğinizi beyan ettiğiniz bu anlaşmalar, ilgili hizmet veya servisi kullanırken dikkat etmeniz gereken koşullardan içeriğinin sahipliğine ve olası anlaşmazlıkların çözümüne kadar birçok önemli detay içeriyor.

Diğer yandan bu anlaşmaların onay sırasında etraflıca okunmamasının suçunu hepten kullanıcılara yüklemek de haksızlık olur. Zira anlaşma metinlerinin son derece uzun olmasını bir kenara bırakın, anlaşmaların içinde yer alan bazı noktalar hukuk uzmanlarının bile kafasını karıştıracak ifade ve terimlerle dolu.

Sosyal ağlar da dâhil olmak üzere kayıt olduğunuz servisleri kullanmadan önce altına imza attığınız ve çoğu zaman belli aralıklarla güncellenen kullanıcı sözleşmelerine yansıyan önemli değişiklikler, ancak birilerinin işaret etmesiyle ve tepki göstermesiyle ortaya çıkıyor. Tıpkı bu yılın başlarında fotoğraf paylaşımına dayalı popüler bir sosyal ağ olan Instagram örneğinde olduğu gibi.

Instagram, geçtiğimiz yılın son ayında kullanıcıların okuyup onayladığı anlaşma metnine sessiz sedasız, üyelerinin siteye yüklediği fotoğrafların kullanım hakkını devraldığına ve kullanıcıların rızası olmadan bu fotoğrafları satabileceğine dair bir madde ekledi. Ancak bu kural değişikliği fark edildikten hemen sonra servis kullanıcıların büyük tepkisiyle karşılaştı. Özellikle de servisi kullanan medyatik ve takipçi sayısı yüksek kişilerin de bu tepkiyi paylaşması haberin hızla yayılmasına sebep oldu. Bunun üzerine kullanıcılar tepki olarak hesaplarını kapatmaya başladı. Sadece 1 ay içinde Instagram'ın haftalık aktif üye sayısı 16 milyondan 8 milyona düştü. Instagram yanlış anlaşıldığını savunarak Ocak ayının ortasında ilgili maddeyi geri çekti çekmesine, ancak azımsanmayacak sayıda kullanıcı hesabını silerek platformu terk etmişti bile.

“Ulusal Güvenlik Söz Konusu Olduğunda Verilerinize Erişim Kaçınılmaz Olur”

Popüler sosyal medya servislerinin ağırlıklı olarak ABD’de yerleşmiş olması, içerik sahipliği ve kullanıcılar arasındaki anlaşmazlıklar konusunda farklı bir hukuksal yaklaşım gerektiriyor. Bu konuda hemen hemen her kullanıcının aklına gelen soruları, Türkiye’nin en popüler internet oluşumlarından biri Ekşi Sözlük’ün de avukatı olan Bilişim Hukuku Uzmanı Av. Başak Purut’a yönelttik.

Sosyal ağlardaki kullanıcılar arasındaki hukuksal ihtilaflar en çok hangi nedenle ortaya çıkabiliyor?

İnternet gerçek hayatta yapabileceğimiz neredeyse her şeye kendince bir karşılık üretmiş durumda. Sosyal medya da sosyalleşmek adına yapabildiğiniz neredeyse her şeye kendince bir karşılık barındırıyor. Arkadaş edinme, tartışma, fikrini paylaşma, kabul görme, dışlama, tavır koyma gibi ihtiyaçlar sosyal medyada da karşılanabiliyor.

Normalden farklı olarak, çoğu birebir iletişimin herkesin gözü önünde gerçekleşmesi, insanlara kolayca ve hızla erişebilme, rahatlıkla görmezden gelme ve yok sayabilme, yüz yüze iletişimin olmaması nedeniyle otokontrol mekanizmasının daha az işlemesi gibi durumlar söz konusu. Bu nedenle sosyal medyada hukuka aykırılıklar daha fazla oluyor. Özellikle karşıt görüşlüye veya yazdıklarını eleştirene hakaret, bu gibi platformlarda çok sık rastlanan bir durum. Bu, paylaşımında bulunan kişilerin birbiriyle atışması şeklinde olabildiği gibi, siyasi parti mensuplarına veya seçmenlerine, siyasi figürlere, sanatçılara veya bir sebepten gündemde olan insanlara sebepli veya sebepsiz saldırılması şeklinde de olabiliyor.

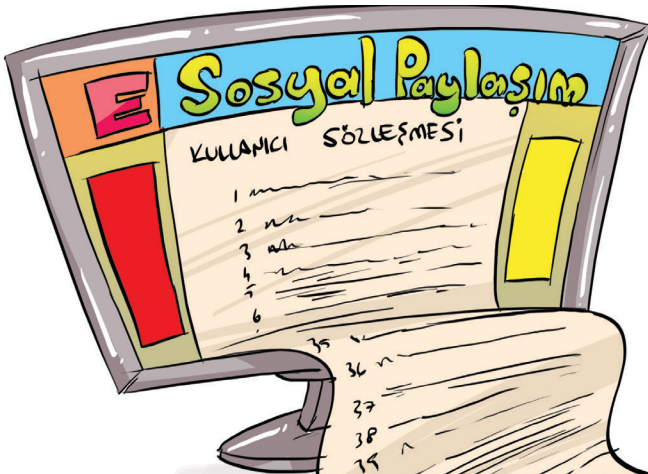
Suç türlerine bakarsak, tehdit, hakaret, haberleşmenin gizliliğini ihlal, özel hayatın gizliliğini ihlal, halkı suç işlemeye tahrik, nefret söylemi olarak adlandırabileceğimiz halkı kin ve düşmanlığa tahrik gibi suçların yoğunlukta olduğunu görüyoruz.

Türkiye’deki bir kullanıcının ABD’de yerleşik bir popüler sosyal ağ üzerinde bir başka kullanıcıya dava açmaya karar vermesi durumunda hukuksal süreç hangi kurallara göre işliyor?

Sosyal medyada işlenen suçun ve failinin tespitinde çeşitli sıkıntılar yaşanabiliyor. Paylaşılan suç unsuru içeriğin site veya fail tarafından yayından kaldırılması, failin gizlemiş olması nedeniyle kimliğinin tespit edilememesi en belirgin sorunlar. Normal şartlarda bu gibi durumlarda savcılık Türkiye’de yerleşik sitelerden IP bilgisini talep ederek suçluyu tespit edebiliyor. ABD’de yerleşik sitelerde ise (ki burada şirketin ABD yasalarına tabi olmasını kast ediyorum), talebin uluslararası adli yardım sistemi kullanılarak yapılması gerekiyor (talepte bulunan ülkenin adalet bakanlığı -> talepte bulunan ülkenin dışişleri bakanlığı -> talepte bulunan ülkenin dışişleri bakanlığı -> talepte bulunulan ülkenin adalet bakanlığı veya muadil kurumu). Bu uzun bir süreç, sonuçlanması bazen altı ayı geçebiliyor.

Bu nedenle çoğu zaman savcılıklar doğrudan platformu sunan şirkete yazı gönderiyorlar ki, bu zaten kanunlara ve uluslararası anlaşmalara aykırı bir talep. Uyulması gereken adli yardım sisteminin sonucunun da ne olacağı belli olmuyor, zira talebin ABD’nin yasalarına da uygun olması gerekiyor.

Çoğu talep, talebe konu suç ABD’de var olmadığı gerekçesiyle reddediliyor. Bu nedenle failin IP numarasının tespit edilmesi için bazı farklı yöntemler kullanılıyor. Bunlar da bazen sonuç vermeyebiliyor. Ancak şunu da belirtmek gerekir ki, bazı ABD menşeli şirketler Türkiye’nin yasal taleplerini karşılama yönünde şirket politikası belirlemiş durumda ve Türk yargı makamlarından doğrudan kendilerine talep gelmesi halinde IP numaralarını paylaşıyorlar. Bu nedenle ABD’de yerleşik sitelerin veya servislerin hiçbiri, hiçbir şekilde IP bilgisi paylaşmıyor dememiz mümkün değil.



Sosyal ağlar da dâhil olmak üzere kayıt olduğunuz servisleri kullanmadan önce altına imza attığınız ve çoğu zaman belli aralıklarla güncellenen kullanıcı sözleşmelerine yansıyan önemli değişiklikler, ancak birilerinin işaret etmesiyle ve tepki göstermesiyle ortaya çıkıyor.

Bu sitelerin faaliyet gösterdikleri ülkelerde, yönetimlerin isteği doğrultusunda milli güvenliği ilgilendiren konularda içeriği paylaşma mecburiyeti var mı? Örneğin ABD merkezli bir sosyal ağa verilerinizi yüklediğinizde, bu veriyi ABD'nin eline teslim etmiş oluyor musunuz?

Şirket merkezi ABD'de yerleşik bazı siteler Türkiye'den gelen talepleri karşılamayınca bunu kullanıcının haklarının korunması gibi algılayanlar oldu. Ancak konunun öyle olduğunu düşünmek yanlış, çünkü bir şirketin zaten uymak zorunda olmadığı bir talebi karşılaması başlı başına garip olurdu. Dediğim gibi, zorunlu olmadığı halde bu talepleri karşılayan ABD şirketleri de var. O nedenle bunun yasal bir zorunluluk değil, ticari bir tercih olduğunu söyleyebiliriz. ABD'de yerleşik şirketlerin tamamının FBI'nın NSL olarak anılan bilgi taleplerini karşılama yükümlülüğü var. NSL, FBI tarafından ilgili siteye gönderilen ve kullanıcılarının bilgilerini almasını sağlayan yasal bir talep. Ancak olması gerekenin aksine bu talebi bir savcı veya hâkim onaylamıyor. FBI bu talepte bulunup dilediği kişinin bilgilerine mahkeme veya savcı kararı olmaksızın ulaşıyor. Üstelik bu talebin varlığından bahsetmek bile yasak (Not: Google PRISM'in ortaya çıkışından sonra bu talepleri açıklamak için girişimde bulundu, detayları dthin.gs/11Ua1fn adresinde bulabilirsiniz).

Özetle verileriniz ABD'de ise, ulusal güvenlik gibi gerekçelerle bilgilerinize mahkeme kararı olmadan dahi erişilebilir. Ancak Türkiye'de durumun daha iyi olduğunu düşünmüyorum açıkçası.

Genele açık sosyal medya verileri üzerinde analizler yapmanın ve bu verileri farklı bir ortamda kopyalayarak depolamanın önünde hukuksal bir engel var mı?

Öncelikle sosyal medya verisini tanımlamak gerekir. Bir sosyal medya verisi bir kelimeden oluşan basit bir cümle de olabilir, eser niteliği ta-

şıyan bir yazı, fotoğraf, video da olabilir. Eser niteliği taşıyan paylaşımların başka bir ortamda yayımlanması veya başkası tarafından kullanılması yazılı izne tabidir, bu nedenle durumun hukukiliği içerik sahibinin tercihine bağlı oluyor daha çok. Açık olarak paylaşılmış verilerin işlenmesi ve sonuçlarının anonim olarak paylaşılmasında ise hiçbir sorun yok. Ancak bir kişinin paylaştığı tüm verileri derleyip o kişiyi hedef gösterecek, rahatsız edecek şekilde paylaşmak kişilik haklarının ihlali olacaktır.

Belki normalde de göz önünde olan ünlüler veya siyasilere de bu konuya biraz daha esnek yaklaşılması söz konusu olabilir.

Bir sosyal medya kullanıcısı öldüğünde geride bıraktığı içerik konusunda dünyada ve Türkiye'de sosyal mecraların tavrı ve hukuki eğilim nedir? Bu konuyla ilgili herhangi bir düzenleme gündeme geliyor mu, konu hukuki platformlarda tartışılıyor mu?

Bu konuda her şirket kendi politikasını belirliyor. Ancak bazı uygulamalar davaya konu olabilmekte. Ekşi Sözlük'te ölen kullanıcının hesabı olduğu gibi bırakılıyor, yakınlarına hesaba erişim hakkı da verilmiyor. Ancak hesaba erişim imkânları zaten varsa hesap yakınları tarafından kullanılmaya devam edilebiliyor. Google mahkeme kararı olmadıkça yakınlarına hesap erişimi vermiyor. Facebook ise ölüm haberi iletildiğinde hesabı donduruyor, duvarını açık bırakıyor. Buna memorialization deniyor, Türkçeye anıtlştırma talebi diye çevirmişler.

Burada esasen mirasa tabi olan şey mülkiyetten çok şirketlerden bir hizmet sözleşmesi karşılığında alınan bir servis olduğundan, bu konuda yasal bir düzenleme olmadıkça her sosyal medya hesabı için ilgili şirketin oluşturacağı politika çerçevesinde davranılması esas olacaktır. Bu konuda bir yasal düzenleme oluşturulana kadar zaten bir etik oluşacağını ve herkesin bu çerçevede uygulamalara gideceği, düzenlemelerin de bu etiğe uygun olarak oluşturulacağı kanaatindeyim.

Arada bu işi daha demokratik yollarla çözmeye çalışıp vazgeçenler de var. Örneğin Facebook 2009 yılında aldığı bir kararla site kullanım koşulları konusunda yapılacak değişiklikleri site içinde yapılacak oylamalarla bizzat kullanıcılar arasında oylama yoluna gideceğini açıkladı. Fakat 2012 yılının sonlarında yaptığı yeni bir değişikliklikle bundan sonra gündeme gelecek değişiklikleri kullanıcı oyuna sunma uygulamasına son vereceğini ilan etti ve bu kararı da oylamaya sundu. 1 milyar civarı Facebook kullanıcısının yaklaşık 670 bini oy kullandı, bunlardan 588 bini yapılacak değişikliklerin aleyhinde oy verdi. Ama yetmedi. Çünkü oylamada çıkacak sonucun kabul edilebilmesi için 300 milyon kişinin katılımı gerekiyordu.

İnternetin En Büyük Yalanı: “Kullanım Sözleşmesini Okudum ve Onaylıyorum”

Tabii bu işin etkisi sadece birkaç popüler sosyal ağ ile sınırlı değil. Az bilinen yerel örnekleri de eklerseniz liste uzadıkça uzuyor. Wikipedia'nın bilinen sosyal ağlara yönelik olarak üstüne basa basa, “Bakın bunların hepsi bu kadar da değil, burada sadece önemli olduğunu düşündüklerimizi sıraladık” notu eşliğinde, wikipedia.org/wiki/List_of_social_networking_websites adresinde yayımladığı listede 200'e yakın sosyal ağ var.

Üstelik iş sosyal ağlarla da bitmiyor. Her gün kullandığınız uygulamalardan sosyal paylaşım amacı gütmeyen, ama

kişisel bilgilerinizi emanet ettiğiniz diğer servislere kadar birçok araç ve yazılım benzer anlaşmalarla karşınıza çıkıyor. Tıpkı bütün ilaçların prospektüslerinde “İçindeki maddelere karşı duyarlılığı olanlar kullanmamalıdır” yazması gibi, en küçük bir bedava yazılım bile beraberinde sorumluluk reddi içeren ifadelerle ve “okudum anladım” demenizi bekleyen anlaşmalarla geliyor. Peki tüm bunları nasıl takip edeceksiniz?

Bu konuyu net ve anlaşılır bir şekilde ortaya koymaya yönelik benim gördüğüm en güzel çaba, 2011 yılında Berlin'de düzenlenen *Chaos Communication Camp* etkinliğinde ortaya çıkan bir fikrin uzantısı olan “Terms of Service; Didn't Read” adlı internet sitesi (tosdr.org).

Sürekli Göz Önündeyken Kontrolü Ele Almak

Buraya kadar işin kişisel bilgilerin korunmasını ve paylaştığımız içeriğin sahiplenilmesini ilgilendiren yönünden bahsettik.

Daha çok Facebook üzerinden sanatsal değeri olan fotoğraflar paylaşıyorsanız veya Twitter üzerinde haku yazıyorsanız ilginizi çekebilecek türden şeyler. Fakat bunun haricinde, hatta bundan daha da önemli olan bir diğer konu var: İçeriği hangi açıklıkla ve kimlerle paylaştığınız, yani kişisel mahremiyetinizi hangi ölçüde gözettiğiniz.

Şu bir gerçek ki, internet üzerinde içeriği bir kez başkaları tarafından erişilebilir şekilde paylaştıktan sonra ne ölçüde yayıldığını veya ne amaçla kullanıldığını kontrol etmek pek mümkün değil. Bazıları sosyal ağlardaki kalabalığın için-

de daha fazla ilgi çekme güdüsü ve Facebook benzeri platformların insanı paylaşma özendirici yapısı nedeniyle normalde sosyal bir ortamda paylaşmaları gerekenden daha fazla şey paylaşabiliyor. İnternet, sosyal ortamlarda uluorta işverenini eleştirdiği için işinden olanlardan tutun da, ayan beyan tatilde olduğunu yazıp döndüğünde evinin soyulduğunu görenlere kadar birçok ilginç hikâyeyle dolu.

Fakat bundan fazlası da var. İnternet üzerinde herhangi bir şey paylaştığınızda bu bilgiyi kimlerin hangi amaçla kopyalayacağını ve kullanacağını bilemeyeceğiniz gibi, paylaştığınız şeylerle farkında olmadan arkanızda etkileşimleriniz ve tercihleriniz hakkında hayli fazla ipucu bırakıyorsunuz.



isteyen kurumlara bu

bilgileri verir, bir değişiklik ya-

pacağı zaman 14 gün önceden size bildirmeyi taahhüt eder, anlaşmazlıklarda Kaliforniya mahkemesi yetkilidir” şeklinde açıklayıcı bilgiler sunuyor. Dilerse-niz her bir maddenin ayrıntısına da bakabiliyorsunuz. Böylece sizden aldıkları bilgileri satıyorlar mı, bu bilgileri kullanarak size özel pazarlama yapıyorlar mı gibi hassas konuları bir bakışta anlamak mümkün.

Sitenin tasarımcıları bu iş için tara-yıcı eklentisi bile yazmış. Eklenti-yi internet tarayıcınıza kurduğunuzda, ziyaret ettiğiniz sitenin kullanım koşulları ve olası riskleri hakkında detaylı bilgi alabiliyorsunuz.

Site, kendi sayfalarında yer alan ifadeyle “Hizmet anlaşmasını okudum ve kabul ettim” butonunu internetin en büyük yalanı olarak görüyor ve bunun için bir çözüm üretmeye çalışıyor.

TOS;DR, popüler sosyal mecralar başta olmak üzere farklı site ve ürünlerin kullanım koşullarını inceleyerek olumlu ve olumsuz yönlerini satır satır özetleyen bir servis. Örneğin Google’ın kullanım koşulları sözleşmesini inceliyor ve ziyaretçilere “Sizin içeriğinizi kendi ürünlerini geliştirmek için kullanabilir, kişisel bilgilerinizi başkalarıyla paylaşabilir, istediği an hizmet vermeyi durdurabilir, kullanıcıları hakkında bilgi

Örneğin 2013 yılının Ocak ayında Amerikan Kongre Kütüphanesi, Nisan ayında da İngiliz Milli Kütüphanesi, vatandaşları tarafından paylaşılan genel erişime açık sosyal medya mesajlarını arşivleyip saklayacaklarını açıkladı. Böylece gelecek nesillerin faydalanabilmesi için bugünün dili, kültürü, alışkanlıkları ve gündemine ışık tutan bir kaynak oluşturmak istiyorlar.

Tabii diğerleri, özellikle de büyük kurumlar ve organizasyonlar sosyal medyadaki paylaşımlarınızla şirket müzesine koymak için ilgilenmiyor. Onların derdi daha başka.

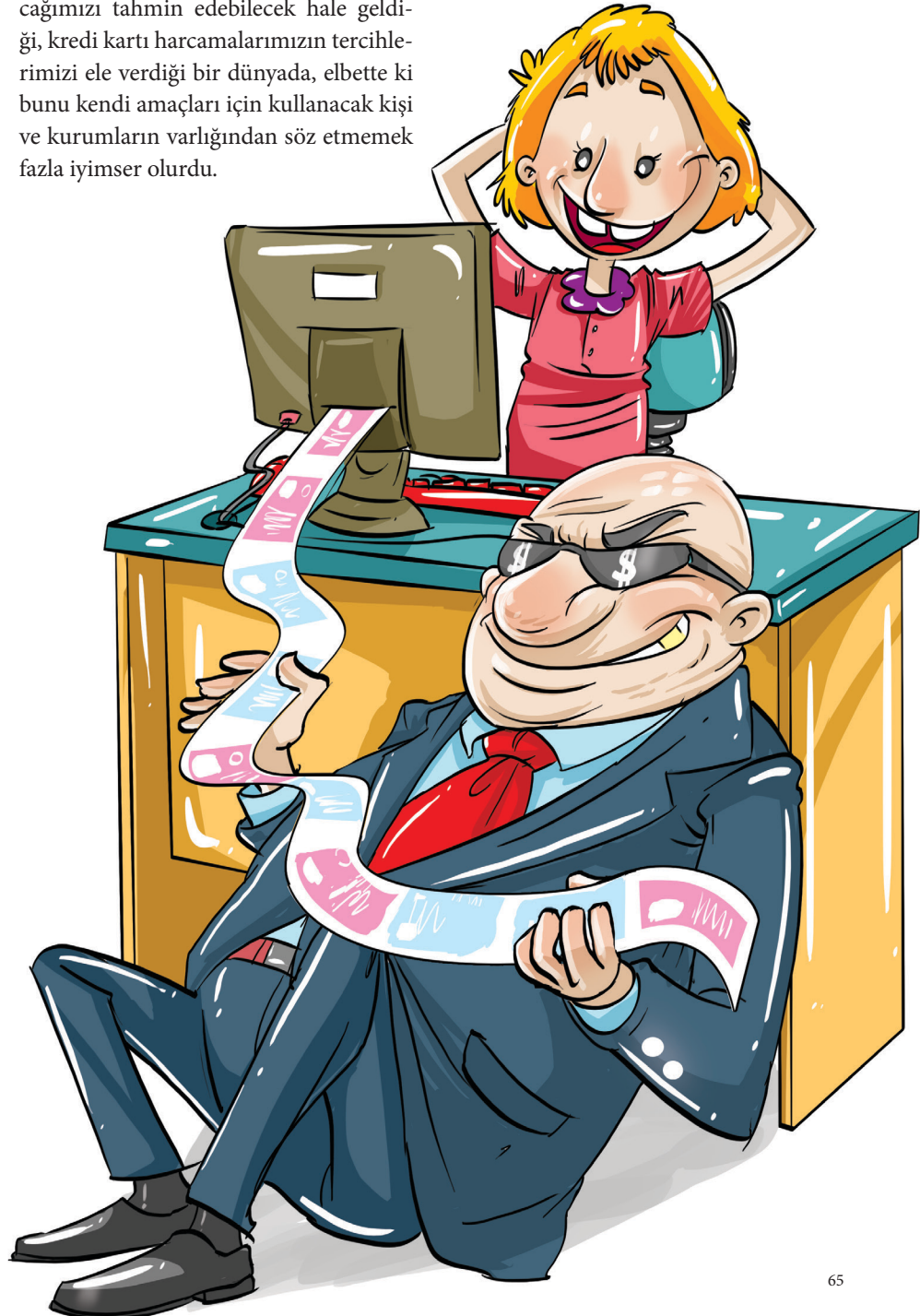
Sizin Arkanızda Bıraktıklarınız Başkalarının En Büyük Hazinesi

Sosyal ağlar ve bireysel bilgiye dayalı servisler her bireyin hayatında var olan, fakat belli bir noktanın ötesinde başkaları tarafından görülemeyen ilişki ağını net bir şekilde ortaya koyuyor. Bunun devamı olarak internet üzerindeki sosyal ağların ortaya koyduğu zengin etkileşim araçları da bireylere kendi çabalarıyla ulaşabileceklerinden çok daha geniş bir topluluğa ulaşabilme ve kendilerini çok farklı yöntemlerle ifade etme şansı tanıyor. Yeni nesil kullanıcılar artık kendilerine sunulana yetinmeyip seçimlerinde özgür olmak, yaşadıkları deneyimi beğenilerine göre şekillendirmek, fikrini belli ederek dönüşüme katkıda bulunmak ve kendilerine benzeyen kişilerle tüm bu deneyimleri paylaşmak istiyor.

Bu bilgiler ışığında, bireylerin sosyal medyadaki paylaşımlarına doğru gözle bakabilenlerin, kalabalık bir kitlenin bir kurumun kendisi ve ürünleri hakkında ne düşündüğünü ve bundan sonraki eğilimlerinin ne olduğunu anlık olarak kestirebilmesi mümkün. Dolayısıyla birey ve grupların tercih ve davranışlarını izleyip ürünleri ve pazarlama yaklaşımını bu veriler etrafında şekillendirerek kullanıcıların beklentilerine daha çok hitap eden ürün ve hizmetler sunmak söz konusu olabiliyor.

Daha önce genellikle bilim ve araştırma çevrelerinin gündeminde olan bu konu, bugün sosyal medya sayesinde toplumsal davranış modellerini de içine alarak kendi başına dev bir endüstri yaratmış durumda. İnsan davranışlarına dair verilerin son derece detaylı bir şekilde toplanarak analiz edilebildiği ve saklanabildiği, kablosuz ağlar üzerinden iletişim kuran her türlü kişisel cihazın kullanıcısı hakkında sayısız bilgi paylaştığı, arama motorlarının arama geçmişimize bakarak bundan sonra neyi arayacağımızı tahmin edebilecek hale geldiği, kredi kartı harcamalarımızın tercihlerimizi ele verdiği bir dünyada, elbette ki bunu kendi amaçları için kullanacak kişi ve kurumların varlığından söz etmemek fazla iyimser olurdu.

Üstelik bu veriler son derece yaratıcı şekillerde kullanılıyor. Örneğin ABD'nin en büyük perakende mağaza zinciri Walmart, sırf buradan gelen verileri analiz ederek müşteriye özel fırsatlar ve çözümler üretmek üzere WalmartLabs adlı bir bölüm kurdu ve *Social Genome* adını verdiği projeyi hayata geçirdi (walmartlabs.com/social/social-genome). Neler yapabildiklerini kendi ifadeleriyle aktaralım:



“Sosyal medyada paylaşılan milyarlarca Facebook ve Twitter mesajı, blog yazıları, YouTube videoları ve diğerleri, yaşayan bir organizma gibi birbirine bağlı ve sürekli evrim geçiriyor.

Social Genome, bu organizmanın yapısını incelemek ve en önemli parçalarını ortaya çıkarmak üzere kurgulandı. Bunun için web üzerinde paylaşılan birçok açık veriyi, kendi topladığımız verileri ve sosyal medya paylaşımlarını yıllarca gözlem altına aldık. Bunları analiz ederek aralarındaki ilişkileri ortaya koyacak yöntemler geliştirdik, bunları farklı verilerle destekledik ve Social Genome yapısının bir parçası haline getirdik.”

Özetle Walmart’ın yaptığı, internet üzerinde kullanıcıların açık olarak paylaştığı bilgileri kendi topladıkları verilerle bir araya getirerek aradaki ilişkileri ortaya koymak ve bundan işletmenin faydalanabileceği yöntemler oluşturmak. Peki neler yapabiliyorlar? Örneğin biri “I love salt” dediği zaman tuz anlamına gelen “salt”ı mı, yoksa Salt isimli filmi mi kastettiğini anlayabiliyorlar. Eğer filmi kastediyorsa ve doğum günü de yaklaşıyorsa, hemen arkadaşına “Hey, bak Yağız’ın doğum günü yaklaşıyor ve Salt isimli filme de bayılmış. Kendisine bununla ilgili bir hediye seçmek ister misin” diye mesaj gidiyor. “Sabah kahvesini içmeden kendime gelemiyorum” diye samimi bir şey mi paylaştınız? Sistem bunu algılıyor ve bir de bakıyorsunuz ki posta kutunuzda “Kahveyi sevdiğini biliyoruz, seçilmiş kahvelerde sana özel yüzde 50 indirim kuponu hazırladık” şeklinde bir mesaj buluyorsunuz.

Dahası da var. Örneğin kürsüye çıktınız, önemli bir konuda konuşuyorsunuz. Karşınıza yerleştirilecek bir ekrandan konuştuklarınızın sosyal medyada yarattığı tepkinin ne ölçüde olumlu olduğunu görmek, konu akışını ve tonunu buna göre anında değiştirmek dahi mümkün. Çok sayıda irili ufaklı teknoloji üreticisi, sosyal medya verilerini mevcut iş süreçlerini ve kampanyaları iyileştirmek amacıyla kullanabileceğiniz yeni platformlar üretmek için büyük kaynak ve çaba harcıyor.

Etkileyici mi, Korkutucu mu

Şu bir gerçek ki 6 milyar insanın cep telefonu kullandığı, sosyal ağların 1 milyardan fazla aboneye sahip olduğu, akıllı telefonunuzda yer alan yazılımların attığınız her adımı takip ettiği bir dünyada hepimiz arkamızda tahmin edebileceğimizden çok daha fazla iz bırakıyoruz. Ve ister inanın ister inanmayın, günlük hayatta alışveriş yaptığımız, hizmetlerinden faydalandığımız, düşüncelerinizi paylaştığımız veya üzerinde arama yaptığımız çoğu servis sizin birçok yönden annenizden, eşinizden, dostunuzdan daha iyi tanıyor. Sorun şu ki bu durum size ürün veya hizmet satmak isteyenlerin de işine yarıyor, ilk fırsatta sizi uçurumdan aşağı atmak isteyenlerin de.

Ama yine de en temel önlemleri bizzat kendiniz almalısınız. Sosyal medya profillerinizin görünürliğini sadece ilgili olabileceğini düşündüğünüz bir çevreyle sınırlamak, sosyal medyada ilgilendiğiniz ve takip ettiğiniz marka ve ürünlerin listesini sadece haber almak istediklerinizle sınırlı tutmak ve belki de en önemlisi gerçek hayatta rahatça söylemekten çekineceğiniz şeyleri sosyal medyada da paylaşmamak, arkanızda bıraktığınız izleri bir yere kadar kendi çizdiğiniz sınırlarda tutabilmenizi sağlayacaktır.

Şunu unutmayın ki bir taşın altına girip tek başınıza yaşamaya karar vermediğiniz sürece, günümüz dünyasında az veya çok arkanızda herhangi bir iz bırakmanın imkânı yok.

Çizimler: Ersan Yağız



Peki ne yapmalı? Bu konuda farklı yöntemler var. Örneğin Peng Zhong adlı bir meraklının kurduğu **prism-break.org** sitesinde günlük hayatta kullandığınız servislerin sizi takip etmeyen veya verilerinizi saklamayan örneklerine yer verilmiş. *Scientific American* **bit.ly/12B3axI** adresindeki blog yazısında Tor gibi birçok platformu bir arada kullanan güvenlik sistemlerinden tek kullanımlık cep telefonlarına kadar, bir dizi yöntem öneriyor. Biraz araştırmayla bunlara çok sayıda yenisini eklemek de mümkün.