DİJİTAL Vatandaşlık

Doç. Dr. Rıdvan ATA [*Muğla Sıtkı Koçman Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi*

Ne, Neden ve Nasıl?

Bugünün bireyleri dijital teknolojiler tarafından dönüştürülen, sosyal medya aracılığıyla bağlantı kurmayı ve çok miktarda bilgiye erişmeyi zahmetsizce sağlayan bir dünyada yaşıyor. İnternetin hayatımızda bu denli yer almasıyla birlikte çevrim içi dünyada giderek daha fazla var olmaya başladık. İşte bu ortamda var olmak, çalışmak, öğrenmek, iş yapmak; kısacası gerçek hayatta yaptığımız gibi iletişim kurmak toplumları hızla dijitalleştiriyor ve bizleri bu dijital dünyanın vatandaşları kılıyor. Ancak modern teknoloji eşsiz fırsatlar sunarken aynı zamanda toplumsal sorunlara dijital bir boyut da ekleyerek yeni meseleler ortaya çıkarıyor. Toplumsal ilişkileri düzenleyen kurallar ve kamusal alanda uyulması gereken sorumluluklar gibi ilkelerin birçoğu uygarlık tarihi kadar eski olsa da teknolojideki hızlı gelişmelerin getirdiği toplumsal değişimler, vatandaşlık kavramının dijital çağa uygun hâle getirilmesini gerekli kılıyor.

Sarayut Thaneerat / Alamy

Dijital vatandaşlar olarak hem haklarımız hem de yükümlülüklerimiz var ve bu nedenle dijital vatandaşlık kavramı hakkında daha fazla bilgi edinmemiz son derece önemli. Bununla birlikte, modern çağa uyum sağlamak için vatandaşlık kavramının günlük yaşamla ilişkisinin dijital teknolojiler aracılığıyla nasıl geliştiğini de doğru anlamak gerekir.

Geniş tanımıyla dijital vatandaşlık; dijital teknolojilerin ve internetin kullanımına dair standart ve normlar ile hak ve sorumlulukların da farkında olmak ve bunları içselleştirmek olarak tanımlanabilir. Bu kapsamda dijital vatandaş ister yerel ister ulusal ya da küresel olsun hem çevrim içi hem de çevrim dışı ortamlarda; yani hayatın tüm alanlarında aktif olabilen; etkili ve sorumlu bir şekilde ırk, cinsiyet ve etnik kökenden bağımsız olarak bu ortamlara eşit katılım sağlayabilen kişidir. Aslında bu tanımlama geleneksel vatandaşlık ilkelerinin nezaket, saygı, haklar ve sorumluluklar doğrultusunda dijital çağa uyarlanması diye yorumlanabilir. Bu çerçevede dijital vatandaşlık kavramı eğitimsel, davranışsal ve yasal olmak üzere üç boyutta ele alınabilir. Eğitim boyutu dijital topluma katılım için teknolojiye kaliteli ve sürekli erişimi gerektirir. Ayrıca temel dijital okuryazarlık da dâhil olmak üzere gerekli kaynaklara ve becerilere karşılık gelir. Davranışsal boyut internet üzerinden iletişim kurarken başkalarına saygılı davranmak gibi daha çok çevrim içi etkileşimlere ilişkin normları ifade eder. Üçüncü boyut ise çevrim içi ortamlarda hak ve sorumlulukların yanı sıra iş, ticaret, veri toplama ve kullanımı gibi uygulamalara dair yasal düzenlemeleri kapsar.

Bireylerin sosyal medya ve dijital teknolojilerle çevrili ortamlarına güvenli, etkili, eleştirel ve sorumlu bir şekilde katılmalarını sağlamak; bu konuda öncelikli meselelerden biridir. Dijital teknolojiler doğası gereği karmaşaya yol açabildiği ve sürekli geliştiği için ilkeleri amaca uygun bir şekilde standartlaştırmada kişiler, kurumlar ya da devletler tarafından farklı hedefler gözetilebilir. Mike Ribble'in "dijital vatandaşlığın dokuz ilkesi" diye tanıttığı prensipler, bu noktada tüm dijital teknoloji kullanıcıları için genel kabul görür. Bu ilkeler; erişim, ticaret, iletişim, okuryazarlık, görgü kuralları, hukuk, haklar ve yükümlülükler, sağlık ve sıhhat ile güvenlik başlıkları altında ele alınır.

Dijital vatandaşlığın dokuz ilkesi

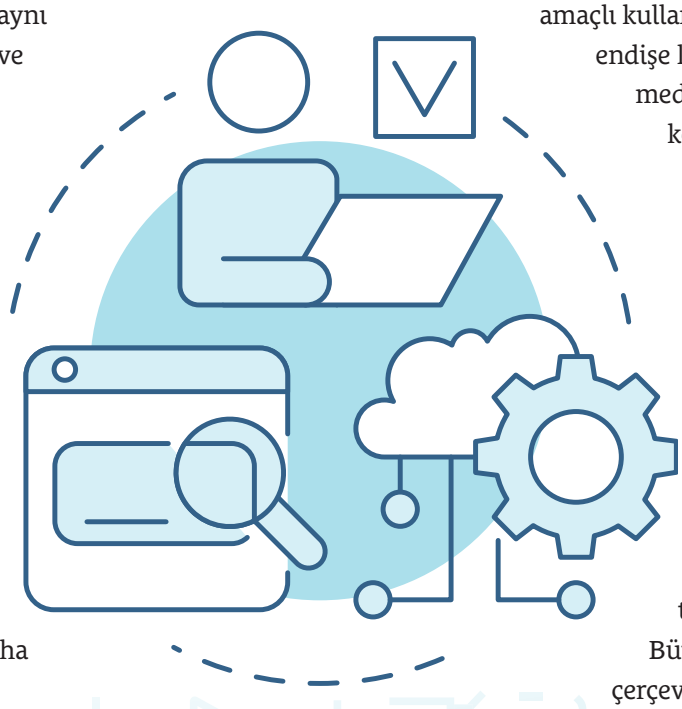
- Erişim
- Ticaret
- İletişim
- Okuryazarlık
- Görgü kuralları
- Hukuk
- Haklar ve yükümlülükler
- Sağlık ve sıhhat
- Güvenlik

Bahsi geçen ilkeleri hayata geçirmek üzere geliştirilen politikaları anlamak için dijital vatandaşlığa doğru dönüşümü yönlendiren sosyal ve politik eğilimleri de göz önünde bulundurmak gerekir. Bu noktada dijital teknolojiler ile internet ve demokratik ilkeler arasındaki ilişkiden bahsetmek faydalı olabilir. Dijital teknolojiler aracılığıyla gerçekleştirilen siyasi, sosyal ve ekonomik faaliyetlerin sayısı giderek artarken bu teknolojilere erişim modern dünyaya katılımı önemli derecede etkiliyor. Hatta dijital erişim yoksunluğu; küresel kalkınmada gecikmelere, refah seviyesinde düşmelere ve eğitimde eşitsizliklerin artmasına sebep olan önemli bir faktör olarak değerlendiriliyor.

İnternet ve dijital teknolojilere erişimdeki eşitsizlikler ve bu teknolojileri kullanmak için gerekli beceri seviyelerindeki farklılıklar, genel olarak dijital bölünme ya da dijital uçurum diye tanımlanır. Dijital bölünme ya da uçurum, zengin ve yoksul uluslar ile daha spesifik olarak nispeten avantajlı ve dezavantajlı gruplar arasındaki eşitsizlikleri gösterir. Eşitsizlik sadece internete erişim noktasında değil, aynı zamanda bilgi iletişim teknolojilerinin elde edilmesi

ve çevrim içi ortamlar için gerekli yeterliklerin kazanılmasında da ortaya çıkar. Ayrıca erişimin kalitesi ve dijital okuryazarlık becerisinin geliştirilmesi de eşitsizlikle ilgilidir.

Diğer taraftan teknoloji sektörünün öncülerine göre, internet ve özellikle sosyal medya herkes için iletişim ve ifade özgürlüğüne erişimi kolaylaştırıyor. Sosyal medya birçok yönden bilgiye erişim ve ifade özgürlüğü gibi temel hakların genişlemesine yardımcı olur. Bununla birlikte, sosyal medya ifade özgürlüğü için nasıl imkân sağlıyorsa aynı zamanda dezenformasyon ve yanlış bilgi yaymak için de kullanılabilir. Örneğin, dezenformasyonun yayılmasının yollarından biri birçok sahte sosyal medya profili oluşturabilen yazılım programlarıdır. Dezenformasyonun sosyal medya mecraları tarafından yayılması, bu profillerin gerçeklerinden ayırt edilmesi zor olduğu için daha zararlı olabilir.



İnternet erişiminde temel meselelerden biri de mahremiyetin korunabilmesidir. Kavramsal olarak mahremiyet kişinin yaşam alanına ve özel hayatına saygı gösterilmesini ve kişisel bilgilerinin güvenliğini kapsar. Örnek vermek gerekirse çevrim içi gerçekleştirilen takip, veri toplama, rahatsızlık verme ve istenmeyen davranışlar kullanıcının gizlilik haklarını ihlal edebilir. Esasen dijital teknolojilerin ve internet özelliklerinin hızlı ve sürekli gelişimi, mahremiyet ve güvenlik meselelerinin ele alınmasını zorlaştırıyor. Birçok internet kullanıcısı, çevrim içi ortamlarda dijital ayak izi bırakarak veri analizi yoluyla izlenme ve tanımlanma riskiyle karşı karşıya kalır. Hemen hemen bütün web platformları kişisel bilgilerin paylaşılmasını gerektirdiğinden kullanıcıların bunu kontrol etmesi oldukça zor olur. Kişisel verilerin istenmesi ve izlenmesi internette o kadar yaygınlaştı ki kullanıcılar ya mahremiyetlerinin korunması ya da bir hizmete erişmek için verilerinin paylaşımı arasında seçim yapmak durumunda kalıyor. Buradaki temel kaygı kullanıcılara fayda sağlamak yerine, dijital izleme araçlarının şirketler tarafından kontrol amaçlı kullanılması. Bir diğer endişe konusu ise sosyal medya platformlarının kendi veri yığınını artırmak için harici verileri satın almasıdır. Bu düzeyde veri elde edildiğinde ve şirketler için herhangi bir düzenleme olmadığında kullanıcı mahremiyeti ciddi tehdit altındadır. Bütün bu meseleler çerçevesinde dijital vatandaşlığın dokuz ilkesini detaylarıyla açıklamaya başlayabiliriz.

Dijital Erişim

Dijital erişim, tüm yönleriyle topluma elektronik katılım şeklinde ifade edilebilir. Burada erişimden maksat, hem düşük maliyetli teknolojik cihazların ve internetin hem de dijital beceri eğitimini sağlayan politikaların herkese fırsat eşitliği sağlayacak şekilde sunulmasıdır. Başka bir ifadeyle, dijital erişim denince cihazların kalitesi, teknolojiyi etkili kullanma becerisi, dijital becerileri geliştirme

fırsatları, eşit erişim için politik ve sosyal destek ile teknoloji için özgün amaçlar belirleme imkânı gibi faktörler ön plana çıkar. Dijital erişim ilkesi diğer kavramların üzerine inşa edildiği dijital vatandaşlığın belki de en temel ilkesidir. Türkiye'de dijital erişimi genişletmek için hükümet öncülüğünde ve özel-kamu sektörü ortaklığında birçok girişim teşvik edildi. Son yıllarda e-devlet uygulaması ile kamu hizmetlerini dijitalleştirmek için büyük çaba sarf edildi. Bu e-girişimin temel amacı bir taraftan nüfus sayımı, arazi, mülk sahipliği ve şirket tescil işlemleri gibi verilerin kayıtlarını oluşturmak iken diğer taraftan devlet kurumlarının genel teknik ve işlevsel kapasitelerini geliştirmektir. E-devlet girişimi sadece devlet hizmetlerinin verimliliğini artırmaya değil, aynı zamanda vatandaşların hizmete erişmesi için dijital okuryazarlık becerilerini geliştirmesine de yardım ediyor. Bununla birlikte çeşitli bakanlıklar da dijital çağa ayak uydurmak için büyük ölçekli projeler gerçekleştirdi. Ulusal Yargı Ağı (UYAP), Merkezi Nüfus İdaresi Sistemi (MERNİS) ve Eğitim Bilişim Ağı (EBA) bunlardan sadece birkaçıdır.

Dijital Ticaret

Mal ve hizmetlerin dijital platformlar aracılığıyla alım satımına dijital ticaret denir. Eğitimden sağlığa, ulaşımdan inşaat sektörüne kadar ekonominin tüm alanları dijitalleşmenin sunduğu avantajlarla değişiyor. Bu avantajlar arasında fiziki altyapı maliyetlerinin en aza inmesi, hizmetlerin sürdürülebilirliğine anlamlı katkı sağlayan müşteri memnuniyetinin artması ile esnek ve uzaktan çalışma imkânlarıyla artan iş gücü verimliliği örnek gösterilebilir. Dijital araçların dâhil edilmesi ile birlikte artık ürün aramaları, satın almalar ve perakendecilerle iletişim kurmak uzaktan gerçekleştirilebilir. Dahası, tüketiciler benzer ürünleri çevrim içi olarak kolaylıkla karşılaştırabilir.

Çevrim içi alışveriş eğilimi, özellikle COVID-19 küresel salgınının da etkisiyle, son yıllarda önemli derecede arttı. Küresel salgın; modern ekonominin büyük ölçüde dijital teknolojilere dayalı olduğunu, gelişmiş dijital platformlara sahip işletmelerin kâr ettiğini ancak yeterli dijital altyapıya sahip olmayanların ayakta kalmak için zorlandığını açıkça gösterdi. Bütün bunlar birlikte değerlendirildiğinde, çevrim içi tüketim eğilimi, tüketimin dijitalleşmesinin gelecekte de artacağını gösteriyor. Dijital ticaret arttıkça çevrim içi bankacılık ve para transferi de artıyor. Bu noktada, çevrim içi ortamda güvenli bir şekilde alışveriş ya da ticaret yapmak için dikkat edilmesi gereken hususların bilinmesi son derece önemli. Aksi takdirde finansal bilgiler veya parolalar gibi kişisel veriler ele geçirilerek kimlik hırsızlığı yapılabilir. Hizmet sağlayıcılar ek

güvenlik önlemleri alsa da çevrim içi işlemler her zaman risk barındırabilir. Özellikle çocuklar finansal dolandırıcılık ya da bilinçsizce çevrim içi para harcama noktasında risklere karşı daha savunmasız olabilir. Bu riski en aza indirmek için güvenli web sitelerinden alışveriş yapılmalı, kredi kartları için iki faktörlü kimlik doğrulama yöntemi aktif edilmelidir.

Dijital İletişim

Dijital iletişim, bilgisayar ve cep telefonu gibi dijital aygıtlar yardımıyla veriler ve mesajların elektronik olarak iletilmesidir. Çevrim içi iletişim e-posta, sosyal medya, çevrim içi medya kanalları, videolar

ya da web siteleri aracılığıyla gerçekleştirilebilir. Çevrim içi iletişim yoluyla hem bilgiye erişim kolaylaşır hem de sosyal bağlantılar rahatlıkla genişletilebilir. Ancak bunun yanında dezenformasyona karşı daha duyarlı olmak gerekir. Dezenformasyon, yani yanlış veya yanıltıcı bilgilerin güvenilir kaynaktanmış gibi sunulup kasıtlı olarak yayılması, önemli bir dijital iletişim sorunudur. Geleneksel medyada bilginin doğruluğu ve güvenirliği için gerekli özen genellikle gösterilir oysa özellikle sosyal medyada paylaşılan bilgilerin doğrulanabilirliği çok zordur. Yanlış bilginin yayılmasını engellemek sansür ve ifade özgürlüğü endişeleri nedeniyle artık daha zor. Hatta medyanın bu denli dönüşmesiyle bilgi meşruiyetinin sağlanması giderek daha da karmaşıklaşıyor. Böylece meşru olmayan kaynaklar ve uydurma haberler ile kamuoyu oluşturuluyor. Bu nedenle yaşadığımız döneme "Gerçeklik/Hakikat Ötesi" de deniyor.

Medya kaynaklarını sorgulama yeteneği 21. yüzyılın önemli becerilerinden birisidir. Dijital vatandaştan beklenen sahte ya da uydurma haber ve dezenformasyonun karakteristik özelliklerini belirleme; meşru haber kaynakları, kişisel görüş ve eğlence amaçlı paylaşımlar arasındaki farkları anlama ve çevrim içi olarak karşılaşılan bilgi kaynaklarını eleştirel bakış açısıyla değerlendirmesidir. Ayrıca ifade özgürlüğü, çevrim içi erişilen bilginin güncelliği ve kişisel bilgilerin korunması noktasında da bilinçli olmasıdır. Bu anlamda dijital vatandaşlar çevrim içi içeriğe her eriştiklerinde içeriğin kim ya da hangi kuruluşlar tarafından yazıldığını, konu hakkında objektif ve eksiksiz bilgi verilip verilmediğini, içeriğin ne zaman oluşturulduğunu, hangi platform üzerinden yayınlandığını ve içeriğin paylaşılma amacını dikkatli bir şekilde değerlendirmelidir. Her ne kadar meşru olmayan bilgi ve dezenformasyon küresel boyutta yaygın bir sorun olsa da eleştirel bakış açısı sahibi bir dijital vatandaş çevrim içi içerikleri sağlıklı bir şekilde değerlendirebilir. Türkiye'de internet kullanıcılarının bilgileri kontrol etmelerine veya haberleri doğrulamalarına yardımcı olacak "Teyit" ya da "Doğrulukpayı" gibi platformlar mevcut. Bu tür platformlar viral olmuş çevrim içi haber içeriği, sosyal medya gönderileri, hikâyeleri, komplo teorileri ve diğer materyalleri doğrulamak için açık kaynaklı materyal ve gazetecilik tekniklerinden faydalanıyor ve böylece kamuoyunun daha güvenilir ve gerçek bilgi edinmesine katkı sağlıyorlar.

Dijital Okuryazarlık

Dijital okuryazarlık kavramı çevrim içi ortamlarda bilginin aranması, oluşturulması ve paylaşılması için bilgi iletişim teknolojilerini etkili kullanma becerisini ifade eder. Son yıllarda internete erişim hızlı bir şekilde arttı ve dijital cihazların maliyetlerinde anlamlı bir düşüş yaşandı. Ancak internet kullanıcılarının dijital okuryazarlık becerisi aynı hızda gelişim gösteremedi. Dijital kaynakları amacına uygun kullanabilmek için, asgari düzeyde, bir arama motorunun nasıl çalıştığı ve arama sonuçlarının nasıl değerlendirilmesi gerektiği

gibi internet hizmetleriyle ilgili temel yetkinliklerin olması gerekir. Bu nedenle dijital okuryazarlık becerisi dijital uçurumu kapatmak için elzem olan temel becerilerden biridir. Bu kapsamda dijital vatandaşlardan beklenen internet erişimi için teknik altyapı ve yapılandırma becerisi; yaygın olarak bilinen ya da yeni tanıtılan uygulamaları, yazılımları ve çevrim içi hizmetleri kullanabilme ve ayarlarını yapılandırabilme; çevrim içi içeriğe erişme, içeriği keşfetme ve değerlendirme; sosyal medya ve diğer platformlarda özgün içerik oluşturabilme ve paylaşabilme gibi dijital okuryazarlığın temel bileşenlerine sahip olmasıdır.

Dijital Görgü Kuralları

Sosyal medya ağları, internet forumları veya çevrim içi doğrudan mesajlaşma sayesinde internet kullanıcıları arasında yeni ilişki formları oluşuyor. Çevrim dışı ilişkilere benzer şekilde, çevrim içi yeni bağların oluşumu ve mevcut ilişkilerin sürdürülmesi de etkileşimlerin uygunluğu ve kalitesine göre değişiyor. Yüz yüze etkileşimde önemli yer tutan yüz ifadesi, ses tonu, beden dili, jest ve mimikler gibi sosyal ipuçları çevrim içi etkileşimlerde gizlenebildiği için dijital ortamlarda gerçekleşen etkileşimin bu eksikliklerden kaynaklanan belirsizlikleri bulunur. Çevrim içi etkileşimde metin tabanlı yorumlamalar yanlış anlamalara ve çatışmalara sebep olabilir. Çevrim içi etkileşim ile ilgili bir diğer mesele de siber zorbalık veya istenmeyen bazı olumsuz davranışların sergilenmesidir. Kullanıcı yönergeleri ve içerik denetimi yoluyla güvenli ve olumlu topluluk etkileşimini teşvik etmeye yönelik girişimlere rağmen, çevrim içi ortamlarda ve sosyal medyada istenmeyen uygunsuz davranışlara rastlamak hâlâ mümkün. Bu nedenle çevrim içi nezaket ve görgü kuralları normları ve standartlarını oluşturmak, özellikle çocuklar ve gençlerin güvenli ve yararlı internet kullanımı için kilit öneme sahiptir. Çevrim içi normların oluşumu; sosyal süreçler, kullanıcı etkileşimleri ve yasal düzenlemeler ile sağlanır.

Ciddi bir ihlal durumunda ise kullanıcı yönergeleri veya topluluk kuralları gereğince yetkili merciler tarafından müdahaleler söz konusu olabilir. Bu kapsamda dijital görgü kuralları farklı çevrim içi iletişim şekillerinde olumlu ve uygun kullanıcı etkileşimlerini teşvik etmeyi amaçlayan bir dizi temel iletişim ilkesidir. Bu ilkeler genel olarak iletişimde açık ve anlaşılır ifadelerin kullanılması, tanınmayan ve iş hayatındaki kişilerle resmî dilin kullanılması, başkalarının kişisel bilgilerinin ve verilerinin gizliliğine saygı gösterilmesi ve siber zorbalık, taciz, takip veya tahrik edici paylaşımlardan kaçınılmasıdır.

COVID-19 salgınının etkisiyle birlikte profesyonel iş hayatında uzaktan çalışma daha fazla benimsendi ve büyük ölçüde Zoom, Microsoft Teams ve diğer görüntülü iletişim teknolojilerine uyum sağlandı. Bu tür platformlar üzerinden gerçekleşen etkileşimlerde gruptaki herkesin tanıtılması, varsayılan olarak kameranın açık tutulması, konuşmadıkça mikrofonun sessize alınması, yorum yapmak veya bir soruya yanıt vermek istenildiğinde el kaldırma özelliği ile söz istenmesi gibi ince davranışlar daha olumlu iletişimin gerçekleşmesine yardımcı olabilir.

Dijital Hukuk

Dijital hukuk internet kullanımıyla ilgili mevzuat ve yasal ilkeleri ifade eder. Hukuksal açıdan internet ve ilgili tüm alanlara dair her türlü olası eylemi ve özneleri kapsadığı için anlaşılması zor olabilir. Kişisel verilerin kötüye kullanılması ve verilerin kontrolündeki artan endişelerle birlikte veri madenciliği teknikleriyle kullanıcı davranışlarının manipüle edilmesi ve siber suç oranlarındaki artış dijital hakları güvence altına alma gerekliliğini daha da belirgin hâle getirdi. Genel anlamda dijital hukuk; telif hakları, e-ticaret işlemlerinin geçerliliği, yetkisiz veri paylaşımı ve sosyal medya mecralarında yasal içerik moderasyonu gibi konularla ilgilidir. Dijital hukuk ilkelerine ilişkin temel bilgiler, internet üzerinden gerçekleşen

hakların ihlali durumunda yasal adımların atılması noktasında dijital vatandaşlık için faydalıdır. Yeni internet hizmetleri; özellikle kişisel verilerin toplanması, saklanması ve işlenmesine dair yasal sorunları da beraberinde getirdi. Ancak dijital hukuk ve veri gizliliği ilkelerine ilişkin farkındalık oluşturma; internet kullanıcılarına dijital kimliklerini kontrol etme ve hem çevrim içi hem de çevrim dışı ortamlarda kendilerini koruma konusunda yardımcı olabilir. Son olarak, yasal bir uygulama alanı olarak dijital hukuk kaidelerinin ülkelere göre farklılık gösterebileceğini de not edelim.

Dijital Haklar ve Yükümlülükler

Dijital haklar internetten ve sağladığı hizmetlerden faydalanmak için gerekli hak ve özgürlükleri ifade eder. Dijital yükümlülükler ise herkes için daha güvenli ve faydalı internet kullanımını teşvik edebilecek sorumlulukları ortaya koyar. Birlikte ele alındığında dijital haklar ve yükümlülükler bireylere ortak değerlere ve karşılıklı saygıya dayalı bir toplumun üyesi olduklarını hatırlatır. Bu yüzden dijital vatandaşlığın gerekli yapı taşlarından biridir. Dolayısıyla, hükümetler, uluslararası kuruluşlar veya birçok düşünce kuruluşu tarafından internet hak ve özgürlüklerini ifade eden çeşitli prensipler tanımlıdır. Bu çerçevede genel olarak herkesin internete erişme ve dijital teknolojileri kullanma, çevrim içi içerik oluşturma ve paylaşma, kişisel veri gizliliği ve güvenli iletişim kurma, çevrim içi ortamlarda kendini ifade etme, güvenli çevrim içi işlemlerde bulunma ve yasa dışı faaliyetleri çevrim içi olarak bildirme hakları vardır.

Dijital haklarla birlikte güvenli ve adil internet kullanımını teşvik etmeye yönelik bireylerin üstlenmesi gereken yükümlülükler de vardır. Dijital sorumluluklar, bireylerin dijital haklarının korunmasını sağlamak için sergilenmesi gereken davranışlardır. Bu çerçevede genel olarak dijital yükümlülükler; siber zorbalık ve çevrim içi uygun olmayan ifadelerden kaçınma, fikrî mülkiyet haklarına uyma, içerik paylaşımı için izin alma ve kaynak gösterme, yasa dışı faaliyetleri ve uygunsuz davranışları çevrim içi olarak bildirme, çevrim içi ortamlarda kendini doğru şekilde temsil etme ve çevrim içi araçların kullanım yönerge ve kurallarına uygun hareket etme gibi prensiplerdir. İnternet erişiminin ve kullanımının bu denli yaygınlaşması göz önüne alındığında dijital hak ve yükümlülüklere ilişkin farkındalık, çevrim içi suiistimallerin önlenmesine ve internetin potansiyelinin faydalı bir şekilde kullanılmasına katkı sağlayabilir.

Dijital Sağlık ve Sıhhat

Dijital sağlık ve sıhhat hâli, kişinin interneti ve mobil cihazları zihinsel ve fiziksel sağlığını bozmayacak şekilde kullanılmasıyla ilgilidir. Problemli internet kullanımı depresyona, anksiyeteye ve diğer psikolojik sorunlara sebep olabilir. İnternetin aşırı kullanımı ayrıca dikkat eksikliği ve odaklanamama gibi bazı davranış bozuklukları riskini artırabilir.

Dijital vatandaşlardan beklenen, internet kullanımıyla ilgili farkındalığa sahip olarak, dijital çağın olumsuz yan etkilerini ve sonuçlarını

azaltmaya yardımcı alışkanlıklar edinmeleridir. Problemli internet kullanımına ek olarak, siber zorbalıkla baş edebilmek de dijital sağlık ve sıhhat ile ilgilidir. Çevrim içi ortamlarda taciz içerikli, kasıtlı ve tekrarlanan davranışlar sergilemek genellikle siber zorbalık olarak ifade edilir. Sosyal medya platformlarında biri hakkında gerçek olmayan haberler yaymak ve onu zor duruma sokacak görüntüleri paylaşmak, incitici ve tehdit edici mesajlar göndermek ya da birinin kimliğine bürünerek onun adına başkalarına mesaj göndermek siber zorbalığa örnektir. Dijital vatandaşların internet kullanımı ve iletişimi ile ilgili psiko-sosyal riskler hakkında bilgi sahibi olması, teknoloji bağımlılığı ve siber zorbalık gibi istenmeyen durumlarla nasıl başa çıkılabileceğini bilmesi gerekir. Siber zorbalıkla başa çıkabilmek için istenmeyen mesajlara cevap vermeme, zorbalık yapan kişiyi engelleme ve rahatsız edici gönderileri yetkili mercilere bildirme gibi önlemler alınabilir.

Dijital Güvenlik

Dijital güvenlik kişinin dijital kimliğinin korunmasını ifade eder. Dijital kimlik kavramı bireyin Facebook, Instagram, TikTok, Twitter ve LinkedIn gibi çeşitli sosyal medya mecralarında veya internet platformlarında paylaştığı kişisel ifadeleri, beğenileri, ilgi alanları ve davranışlarının yanı sıra internetten satın aldığı ürünler ve çevrim içi hizmetlerle etkileşimiyle oluşturduğu kişisel verileriyle şekillenen dijital kişiliği ile ilgilidir. Siber güvenlik ihlalleri sonucu kişisel hesapların veya verilerin başkaları tarafından ele geçirilmesi; kişinin kişisel, mesleki veya finansal durumunu risk altına sokabilir. Siber suçlar bireyin itibarına zarar vermek amacıyla sosyal medya hesaplarının ele geçirilmesi ile gerçekleşebileceği gibi dezenformasyon amaçlı kişisel verilerin elde edilmesi ile de olabilir. Özellikle gündemi manipüle etmek veya kontrol etmek için yapılan dijital korsanlıklar ve veri güvenliği ihlalleri kamuoyu üzerinde etkili olabilir.

Dijital güvenlikte veri gizliliği ihlali ve kimlik avı dolandırıcılığı risklerini en aza indirebilmek için mesajlardaki yazım hatalarına dikkat etme, URL ve web adreslerini kontrol etme, maille gelen şüpheli ekleri açmama, panik oluşturmak için yazılmış mesajlara cevap vermeme ve kişisel onay isteyen mesajlara cevap vermeme gibi temel önlemler alınabilir. Ayrıca yazılımları ve kullanılan cihazın güvenlik duvarlarını güncel tutma, güçlü şifreler oluşturma, güvenli iki faktörlü kimlik doğrulama ve güvenli kablosuz ağlar kullanma gibi önlemler de veri gizliliği ve güvenliğini üst seviyelere çıkarmaya yardımcı olabilir.

Siber suçlar giderek daha da karmaşıklaştığı için kişisel verilerin korunması ve siber suçlarla mücadelede çeşitli yasal düzenlemeler yapılıyor ve bu düzenlemeler sürekli güncelleniyor. Son yapılan güncellemeler ile birlikte sosyal ağ sağlayıcıları hem kullanıcılardan hem de adli ve idari makamlardan gelen talepler üzerine en az bir yerel temsilci bulundurmak ve kullanıcıların gizlilik ihlalleri de dâhil olmak üzere kişisel haklarının ihlal edildiği iddiasıyla ilgili şikayetlerine 48 saat içerisinde yanıt vermekle yükümlüdür. Ancak yapılan yasal değişiklikler ile alınan önlemlerin çevrim içi ifade özgürlüğünü kısıtlayacağına dair endişeler de mevcuttur.

Sonuç

Yukarıda ele alınan meselelere kesin çözümler sunmak kolay olmasa da dijital vatandaşlık hakkında farkındalık oluşturmak ve beceriler geliştirmek çeşitli eğitim ortamlarında erken çocukluk döneminden itibaren başlaması gereken yaşam boyu bir süreçtir. Kural ve normların netliği sadece okullarda değil, aynı zamanda toplum ve devlet iş birliğinde de iyi iletişim bilincinin oluşmasına katkı sunabilir. Sosyal medyanın ve çevrim içi ortamların süregelen gelişimindeki hızlı değişim, dijital vatandaşlık eğitiminin sürekliliğini gerektirir. Bu nedenle herkes için eşit, katılımcı, güvenilir ve demokratik internet ile dijital teknolojilerin kullanılmasını sağlayacak politikalar; dijital vatandaşlık farkındalığının oluşmasında kilit öneme sahiptir. ■

Blackred / iStock

Kaynaklar

Ata, R., Yıldırım, K. Turkish pre-service teachers' perceptions of digital citizenship in education programs. *Journal of Information Technology Education Research*, Cilt 18, s.419-436, 2019.

Hui, B., Campbell, R. Discrepancy between learning and practicing digital citizenship. *Journal of Academic Ethics*, Cilt 16 (2), s.117-131, 2018.

İbrahimoğlu, Z. Digital citizenship and education in Turkey: Experiences, the present and the future. *The Palgrave Handbook of Citizenship and Education*, s.465-482, 2020

Korkmaz, E., Nefes, T., Slavin, A., Akhmetova, R., Keskin, H., Bankston, J., Fu, X. Digital Citizenship in Turkey. Research Paper - University of Oxford, 2021.

Ribble, M. Digital citizenship in schools: Nine elements all students should know. International Society for Technology in Education, Washington DC, 2015.