

Doç. Dr. Nurcan TÖRENLİ
Ankara Üniversitesi, İletişim Fakültesi, Cebeci 06590 Ankara
Tel: 0312 319 77 14, Fax: 0312 362 27 17
e-posta: torenli@media.ankara.edu.tr

Küreselleşen Dünyada Bilgi Güvenliği ve Türkiye

Özet:

İletişimin sistemli hale gelişinde (kurumsallaşma sürecinde) iletişimin güç ve iktidarla ilişkili kodu oldukça belirgindir. Bu durum çeşitli iktidar yapıları (siyasi-askeri-ekonomik) açısından iletişimden beklenen “azami” yararın elde edilebilmesinin iletişim teknolojilerinin hız, denetim, gizlilik ve güvenlik açısından taşıdığı özelliklerin geliştirilmesiyle yakından ilişkili olduğuna işaret etmektedir.

Nitekim on yıl sonra yeniden gündeme getirilen Ulusal Bilgi Güvenliği Kurumu yasa tasarısı taslağı da günümüzde iletişim teknolojilerinin bu özelliklerinin, hem etkileri hem de bunlardan etkilenen taraflar açısından daha da önem kazandığını göstermektedir.

Sonuç olarak bu çalışmada bilgi güvenliği kavramı, Internet gibi gerek iç kamuya gerekse küresel düzeyde dış kamuya açık iletişim ağlarındaki bilgi güvenliği paradigması bağlamında ele alınarak, “kapalı iletişim ağlarında güvenlik paradigması” temelinde şekillenen bu yasa tasarısıyla Türkiye’de bilgi güvenliğine ilişkin politikalar eleştirel bir bakış açısıyla değerlendirilecektir.

Giriş:

Her yeni iletişim aracının-ortamının ortaya çıkışının altında bir dizi değişkenin yanı sıra güçlü bir toplumsal gereksinimin de yatmaktadır. Bu bağlamda bir genelleme yaparak toplumların var olabilme yanında gelişebilme koşullarını yaratıp, bunları sürdürebilmek için iletişimden “kestirilemez olanı devre dışı bırakma” ya da tümüyle ortadan kaldırma amaçlı olarak yararlandıklarını söyleyebiliriz. Bu noktadan bakıldığında, günümüzde, yeni medyanın yaygınlaşmasıyla gerçeklik, geçerlilik kazanmaya başlayan bir oluşumdan da söz edebiliriz: Tüm araçlı-aracılı iletişim ortamlarında ortaya çıkan, bu ortamlar arasında geçişlilik yaratan ortak bir iletişim ortamı ve ortak bir “elektronik dil”in oluşmaya başlaması. Bu oluşumu anlatmak için kullanılan kavram ise yapılandırılmış iletişimdir.

Hız, içerik, ölçek ve bütünleşme (ya da yöndeşme) olarak özetleyebileceğimiz dört önemli olgu aslında 1980’lerden başlayarak “yapılandırılmış iletişim” kavramının ortaya çıkışının ana dinamikleri oluşturmuştur. İletişim ağlarında (telekomünikasyon altyapısı ve yeni medya bütünleşmesi) zaman ve mekân sınırlılıklarını aşma olanağı veren teknolojik gelişmeler, ‘bilginin-enformasyonun’ maddileşmesine, somutlaşmasına da olanak tanımıştır. Yeni iletişim teknolojilerinde hız, içerik, ölçek

ve bütünleşme (ya da yöndeşme) başlıklarıyla özetlediğimiz gelişmeler, bilgi-enformasyon alış-verişine mekândan bağımsız olarak gerçek zamanlı bir boyut, akışkanlık kazandırmıştır.

Bu bağlamda yapılandırılmış iletişimin temeli, bilişim teknolojilerini bir arada, uyumlu çalışabilir tutan (IP tabanlı ortak iletişim şebekesi) ve bu sayede bilgiyi-enformasyonu akışkan hale getirerek maddi değer kazanmasını sağlayan ağ mimarisine dayanmaktadır. Bu mimariyle küresel ölçekte, *vakit'in nakit'e* önceden görülmemiş bir hızda ve etkinlikte dönüşmesi olanaklı hale gelmiştir. Gereksinim, bilginin-enformasyonun maddi değerini en çoklaştırmak, bunun için de kestirilemez olanı devre dışı bırakmak olduğuna göre ağın güvenliği konusu da kritik bir önem arz etmektedir. Bilgi güvenliği açısından bu bağlamda en hassas bölge haline gelen ağın korunması için de yeni medyanın denetim-kontrol anlamında sahip olduğu teknolojik olanaklar devrededir.

Sorun da aslında burada yatmaktadır: Az gelişmişliğe karşı savaşımında bilgiyi, bilim ve teknolojiyi insani-toplumsal kalkınmanın hizmetine çok daha etkin bir biçimde sokmanın (bilgi toplumu politikaları) yanı sıra demokratik toplumsal yönetimin ve örgütlenmenin de temel platformu olarak öne çıkan bilişim teknolojilerinin bu katkıyı somutlaştırdıkları en geniş ortam anlamında ağ yapılanmasının, bilgi güvenliği açısından da en hassas bölgeyi oluşturuyor olmasının yarattığı çelişki. Bu çelişkiyi kısaca, yarar ve zararın aynı ortamda potansiyel olarak var olması biçiminde de tanımlayabiliriz. Aslında “İnternet’te sansür olmalı mı-olmamalı mı?” tartışmalarının temelinde yine bu çelişki yatmaktadır.

Küreselleşme ve bilginin-enformasyonun maddileşme süreci

Küreselleşme, giderek ekonomi ve sermayeyle ilişkili bir kavram haline gelmiştir. Çünkü küreselleşmenin bu yanı sıra, işle ilgilidir. Bu güçlü ilişki nedeniyle ekonomik küreselleşme söz konusu olduğunda karşımıza bireyleri ve toplumları, ekonomik ve ticari faaliyetler açısından sınırlandıran ya da hareket alanlarını genişleten küresel sınırlar, küresel pazarlar ve bu pazarlardaki ekonomik-ticari rekabet çıkmaktadır.

Küresel pazar, sahnenin büyük, bu oranda da rekabetin çetin olduğu bir alandır. Askeri güç gösterileri, ince politik manevralar, ekonomik-ticari çıkarlar üzerine kurulan ortaklıklar, ekonomik işbirliği anlaşmaları, yeni denge arayışları bu büyük resmin ana temalarını oluşturmaktadır.

II. Dünya Savaşı, endüstriyel hâkimiyetin devamının, siyasal düzeyde “küreselleşmiş bir dünya düzeninin” kurulmasına bağlı olduğunu endüstriyel hâkimiyet için küresel çapta yeni bir denetim mekanizması bulmak gerekliliği gösterdi. Böylece sahneye uluslararası örgütler, bu örgütlerin karar mekanizmalarında söz sahibi güçler, bölgeselleşmiş ekonomik gelişim alanları (ABD/NAFTA, Avrupa Birliği ve JAPONYA/Pasifik) ve dönemin yeni yapılanmasına uygun düşecek biçimde top arabası diplomasisin yerini almaya başlayan ağ diplomasi çıkmıştır.

Haber-enformasyon yer küre üzerinde nasıl serbestçe dolaşıyorsa mallar, hizmetler, sermaye ve işgücü de serbestçe bir yerden diğerine akabilmelidir. Böylece ülkeler arasında adına “karşılıklı

bağımlılık” denilen yeni bir iş bölümü doğar. Bu işbölümüne razı olan ülkeler ekonomik kapasite ve yeteneklerine göre farklı roller üstlenir. Bu işbölümünde başrol iletişime düşmektedir. Fabrika içindeki görev dağılımını, üretim ilişkilerini belirlemede olduğu gibi, küresel fabrikanın düzenlenmesinde de iletişimden yararlanılmış; üretim-tüketim eş zamanlı hale getirilmiştir. Robotların devrede olduğu üretim sistemlerinde mallar, üretilip satılsın diye depolarda stoklanmaz, sipariş gelince üretime geçilir. Şehirler, bölgeler, ülkeler arasındaki hızlı ve güvenilir iletişim ağları, küresel pazarın merkezi sinir sistemi gibi çalışır.

Sermaye gibi enformasyonun-bilginin de akışkanlık kazandığı, maddileştiği sayısal ağ ortamında enformasyonun işlenmesindeki maliyet düşüşü, enformasyonun depolanmasına (sayısal sıkıştırma teknolojileri) dönük yeni yazılımların-donanımların geliştirilmesi ve telekomünikasyon dağıtım şebekelerinin bilgisayarlarla kontrol edilir hale getirilmesi gibi gelişmeler etkili olmuştur. Bu yeni teknolojiler uzaktan komuta-kontrol yetenekleriyle maliyet-kâr dengesinde işbölümünü, üretim sürecinde parçalanmayı, üretimin tüm aşamalarında iç denetimi ve sanayi kuruluşlarında merkezileşmeye yol açmayacak biçimde esnek yönetim yapısının işlerlik kazanmasını sağlamışlardır.

Böylece ürünler ya bütün ya da parçalar halinde, küresel fabrikanın uygun bulduğu ülkelerdeki taşeron firmalara "fason" olarak ürettirilebilir hale gelmiştir. Taşeron firmalar tasarımdan hammadde teminine, üretimden pazarlamaya kadar farklı roller üstlenebilir hale gelmiştir. Yeni bilgi ve iletişim teknolojileri sayesinde siparişi veren firmanın fiziki bir yapıya yani binalara, büyük ofislere sahip olma gereksinimi de göreceli bir durum haline gelmiş ve “hayalet” şirket modeli gündemimize girmiştir.

Üretimin küreselleşmesinde bilgi ve iletişim teknolojileri başroldedir. Bu teknolojiler, üretimin bir bütün olarak yönlendirilmesine ve yönetilebilmesine olanak tanıyarak, merkezi aktöre adına “esnek üretim” denen hareket serbestliğini kazandırmışlardır. Dünya pazarlarına ilişkin verilerdeki en ufak değişiklik, bu teknolojilerinin olanaklarıyla anında üretim bantlarına aktarılır hale gelmiştir. Model, özellik, çeşit ve miktarlar sık sık değiştirilebilir. Tüketicilerin istekleri, tüketim eğilimleri daha yakından takip edilir. Yeni teknolojik bulgular, yeni ve daha gelişmiş bir üründe çabucak yer bulabilir.

Yeni iletişim teknolojilerinin desteklediği esnek üretim aynı zamanda şirketlerin faaliyet alanlarını da esnetmelerine olanak tanımaktadır. İlk bakışta yazılım devi olarak görülen Microsoft kurduğu ortaklıklarla artık büyük medya kuruluşları kadar “haber” içeriği üretmektedir. AT&T, bir telekomünikasyon şirketi olmaktan çok, insanları biraraya getiren bir “ağ” şirkete dönüşmüştür. Çin Demiryolları, bir yolcu ve kargo şirketi olmanın yanı sıra bir telekomünikasyon işletmecisi haline de gelişmiştir. Amerikan Havayolları, yolcu taşımacılığının yanı sıra otel ve araba da kiralamaktadır.

Ekonomik küreselleşmenin ikinci alt sistemi sermayenin küreselleşmesidir. Yani paranın akışkanlık kazanması, bankalar aracılığıyla kolaylıkla el değiştirebilmesidir. Doğal olarak akli başında her yönetim insanlarına daha iyi bir yaşam sunmak ister. Bunun için kalkınmak, kalkınmak için de daha fazla kaynağa gereksinim duyar. İşte bu noktada yani kalkınmak için yeterince kaynak bulunamadığında çoğu zaman geriye tek bir seçenek kalmaktadır: Yabancı sermaye...

Bu arada sermayenin küreselleşmesiyle yatırım amaçlı paranın yanı sıra tek amacı kâr olan ve bir tehditte karşılaştığında kaçmaya hazır sıcak para da akmaya başlar. Döviz girişi ve çıkışı serbest bırakılır. Böylece ekonomiler biraz daha kırılgan, biraz daha dışa bağımlı hale gelir. Ancak kısa dönemli kârlar, bu ülkelerle yatırımcı ülkeler arasındaki ilişkileri baltalar. Çıkarlar keskinleşip, görünür hale geldiğinden korumacı tepkiler alevlenir. Özellikle sıcak para tepki çeker. Bu nedenle kaybedilmesi göze alınamayan pazarlarda ilişkilere daha fazla özen gösterilir. Bankacılık ve finans sistemini güçlendirecek destekler verilir, uzun vadeli krediler açılır.

Bu arada yabancı topraklarda üretim ve üretilen ürünlerin pazarlanması yoğun bir haberleşme gereksinimi de yaratır. Tam da bu nedenle yabancı yatırımcı işler durumunda hızlı-gelişmiş bir iletişim alt yapısı arar, hatta yatırım için bunu şart koşar. Kış aylarında telleri donan, telefon bağlantılarında yaşanan sorunları alay konusu olan, telefon aboneliğinin karaborsaya düştüğü haberleşme altyapısına sahip ülkelerden geri durur.

Ekonomik küreselleşmenin üçüncü alt sistemi olan hizmetlerin küreselleşmesi ise “maddi” olmayan ancak sayısal teknolojinin ölçülebilir dolayısıyla da fiyatlandırılabilir hale getirdiği başta medya ürünleri olmak üzere “ağırlıksız ekonominin” ürünlerin de artık sınırların ötesine taşınır hale gelmesidir. Bu noktada ana sorun, hizmetlerin önündeki küresel sınırlardır. Bunlar da uluslararası ticarete malların yanı sıra hizmetleri de katan Yeni Ticaret Rejimiyle (GATT ve GATS) aşılar. Küreselleşme süreci bir anlamda kurumsallaşır, uluslarüstü bir meşruluk kazanır. Böylece maddi mallar kadar maddi olmayan mallar yani hizmetler de küresel ticaretin konusu olur. Ulus devletlerin sınır duvarları saydamlaşır...

Küresel pazarlar günümüzdeki kapsamına 1970’lerden başlayarak telekomünikasyon teknolojileriyle bilgisayar teknolojisi arasındaki bütünleşmenin hızlanmasıyla 1980’lerden sonra da Internet’in ticari kullanıma açılmasıyla ulaşmıştır. Bu aşamadan sonra işyerleri, bankalar, konutlar, mağazalar, üretim merkezleri ve eğitim kuruluşları arasında sayısal iletişim kanalıyla köprüler kurulur. Küresel pazarlara artık enformasyon otobanlarıyla ulaşılır.

Aynı dönemde Türkiye’de sürecin bir parçası haline gelmeye başlar. Haberleşme alanındaki yatırımları, NATO’nun askeri iletişimin güvenliğiyle ilgili kaygıları bir yana asıl 1980’li yıllarda başlayan dışa açılma politikaları hızlandırır. Ardından Internet’in ticaret ve sermaye akışının hizmetine sunduğu hız ve erişim olanakları görünür hale gelir.

Ancak ekonomik küreselleşmenin aktörleri arasında güçler dengeli değildir. Küresel pazara girişin koşulları her ülke için aynı değildir. Öncelikle yeni iletişim araçları her toplumda aynı ölçüde yaygın ve kullanılabilir durumda değildir. Gelişmiş ve az gelişmiş toplumlar arasındaki bu dengesizliği ifade eden “sayısal uçurum”, az gelişmiş toplumların kendi içlerindeki farklı bölgeler için de geçerlidir. Dahası telekomünikasyon gibi gerek hizmet türleri gerekse teknolojisi son derece karmaşık sistemler, ulusal teknoloji geliştirme yeteneğinin önemsenmediği durumlarda “hazır al kullan” tembelliğini beslemeye uygun ortamlar da yaratır.

Bilgi güvenliği ve toplumsal ilişkiler:

Bilişim teknolojileri sayesinde maddileşen bilgi-enformasyon, küreselleşmeyi de soyut bir olgu olmaktan çıkartarak, etkilerini her bireyin günlük yaşamında hissedebileceği düzeyde somut hale getirmiştir. Böylece sayısal ağların “özgürleştirdiği”, müdahalesiz seçme özgürlüğünün “idealleştirdiği” görsel, işitsel enformasyon-eğlence (infotainment) endüstrisinin ürünlerinin sınırları aşması, salt teknolojik değil hukuki boyutta da gerekli meşruluk zeminini kazanmış olur. Hukuki boyuttaki meşrulaşma sürecinin ekonomik boyuttaki yansıması kendini, toplumların üretim ve dağıtım ilişkilerinin yeniden yapılandırılışında sayısal ağların başat mübadele alanı haline gelişle gösterir. Unutmamak gerekir ki, toplumsal yaşamın ekonomik boyut dışında vatandaşla devletin karşı karşıya geldiği bir kamusal boyutu da bulunmaktadır. Dolayısıyla günümüzde giderek yaygınlaşan e-Devlet uygulamalarından da tanık olduğumuz gibi sayısal ağlar, üretim ve dağıtım ilişkilerinin yanı sıra kamusal ilişkilerin de önemli bir kanalı haline gelmektedir.

Küresel ölçekte yaşanan serbestleşme-özelleştirme ve kurallardan arındırma (*deregulation*) süreci yanında bilişim teknolojilerinin yaygınlaşması ve buna bağlı olarak çok sayıda iletişim kanalının devreye girme süreci birlikte düşünüldüğünde, bu etkilerin maddileşen bilgi-enformasyonun güvenilir ya da yanıltıcı nitelikleriyle de ilişkili olduğu görülebilir. Bu etkilerin, bildik-tanidik “eski” etkiler olduğu söylenebilir ancak sayısal ağlar üzerinde hızla akan, anında erişilebilen maddileşmiş bilgi-enformasyonun yarattığı “etkilenmelerin” çarpıcı hatta “kriz tetikleyicileri” gibi işleyen nitelikleriyle “yeni” olduklarını da kabul etmemiz gerekir.

Günümüz dünyasında bilişim teknolojilerinin yaygınlaşma, çok kanallı-çok seçenekli iletişimi olanaklı kılma sürecine koşut olarak, “iki nokta-yer arasındaki mesafe” anlamındaki bilindik uzaklık kavramı da bu düz anlamını yitirerek uzakta olandan etkilenmeyişi durumundan uzakta olandan tıpkı yanı başımızdaymış gibi etkilenmenin kaçınılmaz olduğu bir duruma doğru dönüşmüştür. Örneğin, ABD’de 10 trilyon doları bulan mortgage sisteminin, geri ödenemeyen krediler (sayıları yüz binleri bulan icra işlemleri) nedeniyle çökeceği endişesinin tetiklediği kriz, binlerce kilometre uzaklıktaki Uzakdoğu piyasalarının yanı sıra İstanbul Menkul Kıymetler Borsası’nı da anında etkilemiştir.

Bu çarpıcı, kriz tetikleyici ve yanı başımızda oluyor hissini güçlendiren dönüşümün ana değişkeni de parayı, emeği, zamanı, mekânı, enformasyonu-bilgiyi ortak tek bir şebekede (Internet ortamı) maddi-akışkan hale gelişidir. Dolayısıyla gerek ekonomik gerekse kamusal ilişkiler boyutunda bilgi güvenliğinden söz edildiğinde akla gelen ilk ve en önemli ortam da bu şebeke yani Internet ve Internet üzerinde dolaşan, paylaşılan, erişilen, iletilen-alınan bilgi-enformasyon olmaktadır.

Bilgi güvenliği kavramını “teknik” anlamda bilginin bir “varlık” olarak hasarlardan korunması olarak tanımlayabiliriz. Hatırlanacağı gibi Internet de, Soğuk Savaş ortamının uygun ikliminde, 1960’ların başında ABD’de, SSCB ve müttefiklerinin ABD ve Batılı ülkelere karşı bir nükleer saldırı olasılığına karşı güvenli, nükleer yıkım durumunda da ayakta kalabilecek bir iletişim sistemi oluşturma amacıyla Pentagon’un Üniversitelerle başlattığı işbirliğinin bir ürünü olarak ortaya çıkmıştır.

Dolayısıyla bilgi güvenliği, salt ticari-ekonomik çıkarlarla değil aynı zamanda devletin kamusuyla ilişkileri bağlamında siyasi-idari çıkarlarla da örtüşen, “istihbarat” anlamında ulusal güvenlikle birlikte düşünülen bir kavram haline gelmiştir.

Bu denli geniş ölçekli ilgi-etki alanıyla bilginin maddileşme sürecinde yaşanan hızlı dönüşüm bir arada düşünüldüğünde sayısal ağlar, hasarın oluşacağı temel ortam haline gelmektedir. Bu nedenle güvenlik gerekçesi ağır basmış ve enformasyonu işlemeye-dağıtmaya ve şirketlerin iletişim ağlarına destek vermeye dönük bilişim teknolojilerinin kullanımı da daha başlangıçta iki temel biçimde yapılandırılmıştır: *Açık* ya da *kapalı* (özel, sınırlandırılmış, *extranets/intranets*) biçim. Örneğin kiralık hatlardan (*leased line*) oluşan ağlar 1960’lardan başlayarak kapalı-özel dediğimiz biçimde büyük ölçekli-çok uluslu şirketlerce geliştirilmiş ve küçük şirketler de bu ağdan paylaşım anlaşmalarıyla yararlanmaya başlamışlardır.

Günümüzün Internet ya da sayısal ağ/şebeke ortamının gelişmiş mimarisi, en alt standart düzeyinde de olsa özü itibariyle geleneksel güvenlik anlayışının temeli niteliğindeki “anahtar-kilit” ilkesine dayanmaktadır: Bilgi güvenliğinin sağlanmasında ya da bilginin bir “varlık” olarak hasarlardan korunmasında temel (teknik) mekanizma, yetkilendirme, şifreleme ve filtreleme uygulamaları (kilitler), bu amaçla geliştirilmiş olan yazılımlardır.

Sisteme kimin girebileceğini, hangi noktalara erişebileceğini ya da hangi bilgileri sorgulayabileceğini tayin etmede “anahtarın” sahiplerine üstünlük sağlayan; farlı ölçeklerdeki egemenlik arayışlarına dönük çekişmelerde gücün nerede-kimde yoğunlaştırılacağına karar vereceklerin elini güçlendiren bu yazılımlar, ağ üzerindeki enformasyonun akışını denetleme, belli merkezlerde toplama olanağını da yararlanılabilir hale getirmişlerdir. Elektronik ortamlarda yürütülen faaliyetler tek tek bireyler düzeyinde sürekli kayıt altına alınarak (e-postaların saklanması), üzerinde çalışılan, başkalarıyla paylaşılan bilgiler görüntülenerek, yapılan tüm işlemler raporlaştırılarak çok daha etkin bir biçimde saklanabilir-denetlenebilir hale gelmiştir. Böylece tozlu raflarda yıllanan dosyalar dolusu evrak, ‘günü geldiğinde’ çıkarılıp kullanılacak birer belge haline gelmiştir.

Ancak iletişim ağının denetim-kontrol amaçlı bu kullanımı bireylere de güçlü şifreleme yeteneği veren yazılımlarla pekâlâ kamusal ilişkilerinde bireylerin kişisel verilerini ve ağ bağlantılarını koruma altına almasına da izin vermektedir. Bu bireysel düzeyin üstünde yani toplumsal düzeyde, iletişim ağlarının dayanışmacı bir yapılanma olduğunu, bu nedenle siyasal-toplumsal yenilenmenin motoru niteliğindeki merkez dışı, alternatif siyaset ve yeni öncelik alma girişimleri için uzun mesafeli ancak hızlı işleyen iletişim sisteminin “güvenli” bir örgütlenme olanağı sunduğunu da görmemezlikten gelemeyiz.

Nitekim yeni iletişim teknolojileri ya da yeni medya sahip olduğu olanakların bolluğuyla yeni iletişim-enformasyon-medya hizmetleri yanında yeni toplumsal örgütlenme biçimlerinin yaratılması için uygun bir zemin sağlamıştır. Bu olanak bolluğu-çeşitliliği birçok toplumbilimci tarafından yeni medyanın “devrimci” karakterinin bir yansıması olarak da değerlendirilmiştir.

Sonuç olarak, “güvenlikle merkezileşme”, “ulusal güvenlik adına denetim” neredeyse ayrılmaz bir bütünlük oluşturmakta buna karşın ağ yapılanması merkez dışında yer alan çevre için “merkez karşıtı” olanlar da dâhil yeni bir örgütlenme olanağı sunmaktadır. Böylece, bilgi güvenliği çok boyutlu-çok değişkenli bir nitelik kazanmakta, dengenin nerede ve nasıl kurulacağı kendiliğinden (*de facto*) tartışmalı bir konu haline gelmektedir. İşte bu noktada kavramın sosyolojik anlamı önem kazanmakta ve teknik tanımın tek başına bu kavramı açıklamakta-anlamlandırmakta yetersizliği ortaya çıkmaktadır.

Bilgi Güvenliği politikaları ve Türkiye:

Korsan içerik (başta müzik ve video-film) paylaşımının örnek oluşturduğu kişisel-ticari hakların ihlalden ayrı olarak devlet-vatandaş ilişkileri bağlamında bilgi güvenliğinin ana felsefesi, yurttaşların anayasayla güvence altına alınmış haklarının, yurttaşlar bunları kullanırken de güvence altında olmasıdır. Ana felsefe bu olduğunda, günümüz dünyasında bireysel-toplumsal yaşam pratiklerine giderek daha fazla oranda ortam oluşturan sayısal ağlar yanında bu ağlar üzerinde dolaşan bilginin de aynı kapsamda güvence altında olması gerekliliği ortaya çıkmaktadır. Ancak kavramın ulusal güvenlik politikalarının da bir parçası olduğu; kamuya açık ağlarda bireylere güçlü şifreleme yeteneği veren yazılımların ulusal güvenlik politikaları açısından bir engel-kara delik oluşturabildiği düşünüldüğünde bilgi güvenliği kavramından kolaylıkla “biri bizi gözetliyor” duygusu yaratılabileceği de unutulmamalıdır. Bu durumda yurttaşların Anayasa’nın güvence altına almış olduğu haklarını kullanma konusunda getirilecek kısıtlamalar için uygun mazeret yaratmak da kolaylaşmaktadır.

Diğer yandan elektronik ticaret uygulamasında örneklandığı üzere küresel düzeyde ekonomik-ticari ilişkilerin hızlandırıcısı ve yeni hizmet türlerinin yeşereceği ortam olarak görülen sayısal ağlarda bu tür ilişkilerin temeli, geleneksel ticarete olduğu gibi “karşılıklı güvenin” yaratılmış olmasıdır. Giderek büyüyen hizmetler alanının ve bu alanın en önemli parçası niteliğindeki elektronik ticaretin yaygınlık kazanması, bireylerin yüz yüze, karşılıklı iletişimin “sanal” olarak kurulduğu bu ortama güven duymasına bağlıdır. Bu durumda karşılıklı güveni yaratmanın yolu, tüketicilerin güçlü şifreleme yeteneğine sahip olmasından geçmektedir.

Konuya Türkiye açısından bakıldığında bilgi güvenliğine ilişkin olarak gündeme taşınan birden çok yasa taslağı olduğu görülmektedir: Bunlar Adalet Bakanlığı’nın, Ulaştırma Bakanlığı’nın ve Milli Savunma Bakanlığı ile Genelkurmay’ın **Ulusal Bilgi Güvenliği Teşkilatı** oluşturulmasını da içeren tasarlardır. Örneğin Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı’nda Ulusal Bilgi Güvenliği (md.3/b), “Ulusal güvenliği ilgilendiren, yetkisiz ellere geçtiği takdirde, Devlet, kamu ve özel kurum ve kuruluşlarının, yerel yönetimlerin, kamu kurumları niteliğindeki meslek kuruluşları ve üniversitelerin faaliyet alanlarında güvenliklerini tehlikeye sokabilecek veya Devlet ve yukarıda belirtilen kurum ve kuruluşlar aleyhine kullanılabilecek, o kurum ve kuruluşlar tarafından, çok gizli, gizli, özel, hizmete özel ve tasnif dışı gizlilik derecelerinde tasnif edilen, belirlenen ve işaretlenen bilgiyi, üretim, kullanım, işleme, saklanma, nakledilme ve imha sırasında yetkisiz kişilerin erişimine ve olası her türlü fiziksel ve elektronik müdahaleye karşı korumaya, bilgiye erişim ve kullanıma ait usulleri açık şekilde belirlemeye ve bilgiyi gerektiğinde hazır bulundurmaya yönelik

tedbirleri, ifade eder” diye tanımlanmaktadır. Kanun, uzun ve ayrıntılı bu tanımla “ulusal güvenlik” gerekçesiyle iletişim ağlarını kullanan her kurum ve kişiyi kapsamayı amaçlayan bir düzenleme getirmektedir.

Bu bakış açısı, “haklar tehdit altında, o halde bunları güvence altına almak için bilgiyi daha fazla güvenlik duvarlarının içine hapsedelim” dolayısıyla da her isteyenin kullanımına izin vermeyelim (kapalı-sınırlandırılmış erişim) anlayışının bir yansımasıdır. Üstelik bu yaklaşım, hakların ve güvencelerin tehdit altına girebileceği kaygısından daha çok, dünyada bilginin güvenlik yanını (elektronik ticareti de dâhil ederek) atlamaksızın en geniş ölçüde paylaşımını hedefleyen gelişmelere ters, tutucu-korumacı bir eğilimi yansıtmaktadır.

Bilgi güvenliğini ulusal güvenliğin bir alt başlığı gibi gören böylesi bir yaklaşım, daha önce de açıkladığımız gibi küreselleşmenin sayısal ağlardan beklediği ticari ve ekonomik yararı özellikle de elektronik ticaretin dünyadaki standartlara ve uygulamalara paralel bir biçimde gelişimini Türkiye bağlantısında engelleyecek niteliktedir. Tasarıda, sınırlandırmanın kapsamı “özel kişi ya da kuruluşların ulusal güvenlikle ilgili olan verileri” biçiminde daraltılmadığından kişisel-ticari çıkarların kolaylıkla çiğnenmesi gibi bir tehlike doğmaktadır. Ayrıca, taslaktaki tanımların esnekliği, kişisel ve ticari hakların kısıtlanabilirliğini kolaylaştırıcı niteliktedir.

Aslında bu yaklaşımın sorunlu olduğu konusunda ilk uyarılar, 2000 yılında tamamlanan Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA) raporunda yer almıştı. Raporda iletişim altyapısına yönelik diğer kurumlaşmaların henüz ortada olmadığı vurgulanarak, sadece güvenlik amaçlı ayrı bir yapının oluşturulmasının sakıncalı olacağı vurgulanmıştır. Gerek Ulusal Bilgi Güvenliği Teşkilatı Yasa tasarısı taslağında gerekse ondan önceki Başbakanlık Genelgesi kapsamında yer alan bilgi güvenliği yaklaşımı, iletişim ağlarında daha önce sözünü ettiğimiz ikili ayrımın **kapalı** yani **özel, sınırlandırılmış güvenlik paradigmasına** dayanmaktadır. Oysa insani-toplumsal gelişim açısından gereksinim duyulan kamusal bilgi paylaşımının en önemli kanallarından birisi olan Internet’ten böylesi bir işlev bekleniyorsa buradaki paradigma tercihinin (kamuya) **açık bilgi güvenliği paradigması** olması gerekmektedir.

Küresel düzeyde de kabul gören, uygulama alanı bulan bu yaklaşımda Internet gibi kamunun erişimine açık ağlarda bilgi güvenliği, kamusal anahtar altyapısına dayalı elektronik imza/elektronik sertifika sistemiyle sağlanmaktadır. Sonuç olarak Türkiye’nin de kapalı-kısıtlanmış ulusal güvenlikçi paradigmayı terk ederek, (kamuya) açık bilgi güvenliği paradigmasını benimsemesi, bilgi güvenliği politikasını kamusal yarar ilkesi temelinde yapılandırması ve sistemin güvenliğini kamusal anahtar altyapısına dayalı elektronik imza/elektronik sertifika araçlarıyla sağlaması gerekmektedir.