farmafarm

ÖZGÜR KRİPTO

Ruşen Eşref YAZGAN

farmafarm

ÖZGÜR KRİPTO

GÜZELLİĞİN ÇİRKİNLİĞİ

- Kripto; kulağa oldukça itici, soğuk, resmi, askeri, savaşı ve ölümü çağrıştıran bir tabir gibi gelse de, esasında soyut matematiksel güzelliğin günlük hayatımıza yansımasından başka bir şey değildir.
- Mesele şu ki -başka birçok güzellik gibi- çirkin emellere hizmet edebilir.
- Bugüne dek kriptonun genellikle kötü emellere hizmet ettiği sanılıyordu ve bu yüzden devletin sıkı denetimi altındaydı. Tıpkı silah gibi...
- Kripto çalışmaları, araştırmaları, üretimi, ihracı, kullanımı ve el hasılı kripto ile ilgili her şey devletin denetiminde, kalın bir giz perdesi ardındaydı.
- Ve yine toplum için tehlikeli olan her şey gibi, sadece devlet ve devletin müsaade ettikleri tarafından kullanılabiliyordu.

farmafarm

ÖZGÜR KRİPTO

GÜZELLİĞİN YANSIMASI

- Ama dünya değişmekte; devlet tekelinde olan birçok teknoloji toplumun yararına dönüşmekte.
- Bugün halkın kullandığı çoğu sivil teknoloji askeri benzerinden daha ileri seviyeye ulaşmıştır.
  (cep telefonları veya tabletler buna örnek olabilir ama bilinsin ki bir Airbus veya Boeing yolcu uçağı veya F1 yarış arabası askeri teknolojinin çok ötesindedir.)
- Konu yazılım olduğunda fark daha da artmakta, ara açılmaktadır.
- Ne var ki devlet çoğu kez bunu anlamakta geç kalmakta, anladığında ise iş işten geçmiş olmaktadır.
  Gelişimi önceden veya zamanında anlayamayan, takip edemeyen devlet -en hafifinden- ciddiye alınmayan duruma düşmekte; daha önemlisi, tehlikeye açık hale gelmektedir.

farmafarm

ÖZGÜR KRİPTO

SAĞDUYU

- Geçen yüzyılın (1900'lerin) sonuna kadar ABD, kripto konusunda hayli kısıtlayıcı ve ağır müeyyide içeren bir tutum izliyordu.
- Devlete kalsaydı hayli gülünç ve bir o kadar işe yaramaz önlemlere başvuracak, bilgisayarların içine casus donanım ekleyerek herkesi kontrol altına alacaktı ama olmadı; ortak akıl ve izan buna izin vermedi.
- Teknolojinin topluma yayılmasıyla baş edemeyen devlet bu rüzgâra karşı duramadı. Sonunda, kuralları esnetmek, gerçek dünya ile uyumlu hale getirmek zorunda kaldı.
- Sağduyu galip geldi.
- Bundan devlet de kazançlı çıktı.

farmafarm

ÖZGÜR KRİPTO

KUTLANASI ÖNCÜLER

- **ABD'de -ve dünyada- bireyin özgür haberleşme hakkına olduğu kadar devletin akıllanmasına da katkıda bulunan akıl, izan sahibi tüm bilgi güvenliği gurularını kutlamak gerekir.**

  Bunların içerisinde kişisel haberleşmede özgür kripto kullanımını yaygınlaştıran ve önünü açan, PGP'nin yaratıcısı Phil Zimmermann özel takdiri hak etmektedir.
  Bir dolu imkânsızlık ve bürokratik engel ve yasal müeyyideye rağmen -hapse girmeyi göze alarak- hiçbir maddi beklentisi olmadan, tüm ülkeye yaydı PGP'yi. (ve tabii oradan da tüm dünyaya...)

  Phil Zimmermann'ın, PGP'yi niçin yazdığını açıkladığı makalesi kişisel özgür kripto kavramının manifestosu sayılabilir.

  https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

farmafarm

ÖZGÜR KRİPTO

HAK

Phil Zimmermann şunu savunuyor:

- **Kişisel haberleşmenin mahremiyeti bir -anayasal- haktır ve korunmalıdır.**

Burada not düşmekte yarar var: ABD Anayasası özellikle haberleşme mahremiyeti ile ilgili bir hüküm içermemekte; ancak, haberleşmenin mahremiyeti ilkesi ABD anayasasının Dördüncü Değişikliğine dayandırılmaktadır. Dördüncü Değişiklik (Dört Numaralı Tadil - Fourth Amendment) şuna hükmeder:
- Üstlerinin, evlerinin, belgelerinin ve eşyalarının sebepsiz yere aranması ve el konulmasına karşı kişilerin korunuyor olma hakkı (masuniyeti) ihlal edilemez. ...

Dördüncü Değişikliğin yapıldığı tarihte (1789) en ilkel elektrikli haberleşme yöntemi -telgraf- henüz icat edilmemişti. (daha elli sene vardı)
Mektup, zamanın en yüksek teknoloji haberleşme vasıtasıydı.
Değişiklikte sözü edilen "belge" tanımına mektup da girmekte.

farmafarm

ÖZGÜR KRİPTO

YALIN TEZ

- **Şu yalın tezi öne sürüyor, Zimmerman:**
  - ABD Anayasası bu hakkı teslim ettiğinde, elektronik haberleşme söz konusu bile değildi; mahremiyet isteyenler, kalabalıktan biraz uzaklaşıp kendi aralarında, istedikleri şeyi rahatça konuşabiliyorlardı. Bu, kabul edilmiş, doğal bir haktı. Sadece felsefi bakımdan değil -zamanın teknolojik koşullarında- fiziksel bakımdan da doğaldı bu. Dolayısıyla, Dördüncü Değişiklik yazılırken bu hususta bir madde koymaya gerek dahi görülmemişti; belgelerin mahremiyetini korumak yeterliydi.

farmafarm

ÖZGÜR KRİPTO

TELEFON İCAT OLDU...

- Bilahare durum değişti; telefonun icadı ve elektronik haberleşmenin gelişmesiyle mahrem haberleşme diye bir şey kalmadı.
- Pratik ve ucuz olması sebebiyle elektronik haberleşme toplumda yaygın kabul gördü; zamanla, birincil haberleşme şekli haline geldi.
- İki kişi, bir köşede gizlice konuşabilir ama telefon veya diğer elektronik haberleşme yöntemleri kullanıldığında bu mümkün değil artık.
- İşte burada devletin müdahale edip, anayasada teslim edilmiş olan "haberleşmenin mahremiyeti" hakkını koruması ve kollaması gerekir.
- Halbuki, devlet de elektronik haberleşmenin sağladığı bu imkândan (zaaftan) yararlanıp, anayasayı görmezden gelmeyi tercih etti.
- Sadece devlet mi? Teknolojiye bir nebze hakim kişiler veya gruplar da bundan yararlanmaya başladılar.

farmafarm

ÖZGÜR KRİPTO

KİŞİSEL MAHREMİYET

- Gelinen noktada, kişisel haberleşmenin mahremiyeti diye bir şey kalmadı.
- Buna karşılık, bireyler kendilerini -mahremiyetlerini- korumak ihtiyacı duydular ve teknolojinin -özellikle matematiğin- yardımıyla haberleşmelerini gizleme yollarını aradılar ve buldular da: kriptografi...
- Peki, insan niçin gizli haberleşmek ister?
  - Cevap 1: Çünkü bu bir doğal haktır. (İnsan Hakkı da denebilir)
  - Cevap 2: Eşinizle, dostunuzla, arkadaşınızla, sevgilinizle, çocuğunuzla, annenizle konuşmak veya yazışmak istediğiniz bir dolu özel şey vardır.
  - Cevap 3: İş ortağınızla, müşterinizle, bankacınızla, muhasebecinizle, avukatınızla, doktorunuzla, psikoloğunuzla konuştuğunuz, yazıştığınız, rakiplerinizin veya yabancıların bilmesini istemediğiniz şeyler vardır.
  - Cevap 4: Yasadışı işler çeviriyorsunuzdur.

farmafarm

ÖZGÜR KRİPTO

ÖZRÜ KABAHATİNDEN BÜYÜK

- Peki devlet ne yaptı? Kendisinden beklendiği gibi bu en doğal -ve anayasa ile güvence altına alınmış- bireysel hakkı korudu mu?
- Hayır.
  Her türlü teknolojik imkâna ve yasa çıkarma yetkisine sahip olan devlet, bireyin kripto vasıtasıyla gizli haberleşmesini engelleme yoluna gitti.
  Buna gerekçe olarak, anayasanın bu hakkı teslim ederken temel aldığı -bir önceki sayfada belirtilen ilk üç- sebebi görmezden gelip dördüncüsünün arkasına sığındı.
- Yaptığı bu yanlışa bir de yanlış gerekçe buldu ki özrü kabahatinden büyük...
  Devlet, şöyle diyor: Eğer gizli haberleşme ihtiyacı duyuyorsanız büyük ihtimalle yasadışı bir şey yapıyorsunuzdur. Saklayacak bir şeyi olmayan niçin gizli haberleşsin ki? İyi vatandaşlar açık haberleşirler.

farmafarm

ÖZGÜR KRİPTO

KULAKTAN İÇERİ GİRİNCE

- Kulağa mantıklı geliyor, değil mi?
- Evet, kulağa mantıklı geliyor ama kulaktan biraz içeri girip beyne ulaşınca hiç de o kadar mantıklı değil.
- Yani, tercümesi: İyi vatandaşlar birbirleriyle açık posta kartları ile yazışır; kapalı zarfta mektup gönderenden şüphelenmek lazım. Saklayacak bir şeyi olmayan niye kapalı zarfta göndersin ki mektubunu?
- Nasıl?..
  Hak, hukuk, anayasa, masumiyet karinesi, masuniyet karinesi, mahremiyet hakkı, haberleşme özgürlüğü, haberleşme teknolojisi, telekomünikasyon, kriptoloji, matematik, mantık, felsefe ve hatta ilkokul yurttaşlık bilgisi dahi bilmeye gerek kalmadan gülümsetiyor insanı, değil mi?..

farmafarm

ÖZGÜR KRİPTO

KRAL ÇIPLAK

- **Peki, herkes bu saçmalığı görüyor da niçin, "Kral çıplak," demiyor?**
- **Sebep kripto sözcüğünde olsa gerek, herhalde. İnsanları korkutuyor veya hiç değilse çekindiriyor.**
  Halbuki korkacak bir şey yok ortada; hepsi matematik...
  (Gerçi, matematikten korkan bir dolu insan olduğunu düşününce...)

  Hafta sonu kanepeye uzanıp bulmaca çözmekten keyif alan biri, konu kripto olduğunda niçin ürker ki?..

  [ürkmek istemeyen, merak edenler için, bkz. "Muhaberat Muharebatı" adlı derlemem www.farmafarm.com -> hakkımda/about]

farmafarm

ÖZGÜR KRİPTO

AKLIN İTİCİ GÜCÜ

- ABD akıllandı sonunda ama nasıl?
- Aklın itici gücü büyük rol oynadı bunda.
  Akıl, bilime dönüştü; bilim, teknolojiye; teknoloji, topluma yayıldı;
  toplum, teknolojiyi özümsedikçe zihni berraklaştı;
  ve o, "Kral çıplak" diye bağıran çocuğunki gibi berrak ve saf zihinler bağırdı:
  "Devlet çıplak."
- Devlet, bağıranların üstüne biraz gitmeye kalkıştı, önceleri
  ama baktı ki olmuyor, durdu, düşündü ve hak verdi.
  Nihayetinde, akıllıca davranmayı tercih etti.
- Dahası, akıllıca davranmanın kendi yararına olacağını gördü.
  Doğrusu, akılsızca davranma şansı pek yoktu da...
  Tüm haberleşme teknolojisi, bilgi işlem teknolojisi, finans ve bankacılık,
  ulusal ve uluslararası ticaret, medya endüstrisi, yazılım endüstrisi kripto ile
  bu denli iç içeyken nasıl yasaklayacaktı ki?..

farmafarm

ÖZGÜR KRİPTO

ÇİFT KULLANIMLI TEKNOLOJİ

- ABD, geçen yüzyılın sonunda -isteyerek ya da istemeyerek- kuvvetli kripto kullanmanın bireysel hak olduğunu kabul etti; dahası, yurt içi ve yurt dışı dolaşımına ve ticaretine izin verdi.
- Daha önceleri silah muamelesi gören kripto teknolojisi, Wassenaar Düzenlemesi ile -başka birçok teknoloji gibi- çift kullanımlı (Dual Use) olarak sınıflandırıldı.
- Kripto, askeri kullanımın yanı sıra sivil kullanıma da açıldı. İnsanlar artık özgürce gizli haberleşebiliyor. (Olması gerektiği gibi...)
- Peki, yasağı kaldıran devlet kötü niyetlileri izlemekten vaz mı geçti? -- Hayır.
- Sivil uzmanlar devletle, devlet kurumları (NSA, FBI, vb.) da sivil uzmanlarla yarışıyor, artık.
- Sonuçta, her ikisi de daha iyiye evriliyor.

farmafarm

ÖZGÜR KRİPTO

BİZDEKİ DURUM

- Bizde, Türkiye'de durum nasıl?
- Türkiye Cumhuriyeti Anayasası bireysel hakları ve özgürlükleri -Dördüncü Değişiklik'te (Fourth Amendment) olduğu gibi hepsi tek cümle içinde, üstü kapalı değil- günümüz koşullarına uygun şekilde, çok daha açık ve net olarak tanımlamaktadır.
  - Madde 20. Özel hayatın gizliliği... Özel hayatın gizliliğine dokunulamaz.
  - Madde 21. Konut dokunulmazlığı... Kimsenin konutuna dokunulamaz, girilemez, arama yapılamaz, buradaki eşyaya el konulamaz.
  - Madde 22. Haberleşme hürriyeti... Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

farmafarm

ÖZGÜR KRİPTO

İLGİLİ YASA VE YÖNETMELİK

- Anayasamıza baktığımızda ve taraf olarak imza koyduğumuz Wassenaar Düzenlemesi'ni göz önüne aldığımızda, Türkiye'de bireylerin kriptolu haberleşmesinde sorun olmaması gerekir.
- Peki, konu ile ilgili mevzuat, Anayasa ve Wassenaar Düzenlemesi ile ne kadar uyumlu?
- Bilgi Teknolojileri ve İletişim Kurumu (BTK) mevzuatı çerçevesinde ilgili yasa ve yönetmeliğe bakmakta yarar var:
  - 5809 numaralı Elektronik Haberleşme Kanunu (Resmi Gazete tarih: 10 Kasım 2008 sayı: 27050 mükerrer)
  - Kamu Kurum ve Kuruluşları İle Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Yönetmeliği (Resmi Gazete tarih: 23 Ekim 2010 sayı: 27738)

farmafarm

ÖZGÜR KRİPTO

İLGİLİ YASA VE YÖNETMELİK

- **5809 numaralı Yasa**

  Madde 4:
  Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi ilkesi göz önüne alınır.

  Madde 39:
  Telsiz haberleşme sistemleri üzerinden kriptolu haberleşme yapmaya Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı, Milli İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Dışişleri Bakanlığı yetkilidir. Ayrıca yukarıda belirtilen kurumlara ait olanlar dışında kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapma usul ve esasları Kurum (BTK) tarafından belirlenir.

  Madde 63:
  Bu Kanunun 39 uncu maddesine aykırı olarak kodlu ve kriptolu haberleşme yapan ve yaptıranlar beş yüz günden bin güne kadar adli para cezası ile cezalandırılır.

farmafarm

ÖZGÜR KRİPTO

İLGİLİ YASA VE YÖNETMELİK

- **Yönetmelik**

  Madde 1:
  Bu Yönetmeliğin amacı, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununa göre kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme sistemi üretimi, başvuru esasları, değerlendirilmesi, izin işlemleri, emniyet ve muhafaza tedbirleri, denetim, müeyyide ve kayıtlarının tutulmasında uygulanacak usul ve esaslar ile yapılacak iş ve işlemleri belirlemektir.

- **Görüldüğü gibi, Yönetmeliğin amacı sadece üretimi ile ilgili düzenleme yapmak; kullanımla ilgili bir düzenleme amaçlanmamış.**

✧ **Ancak...**

farmafarm

ÖZGÜR KRİPTO

İLGİLİ YASA VE YÖNETMELİK

- **Yönetmelik**

  Madde 2:
  Bu Yönetmelik, elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapmaya yetkili Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı, Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve Dışişleri Bakanlığı ile bu kurumlara ait kodlu veya kriptolu elektronik haberleşme sistemlerinin kullanıldığı kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler hariç, diğer kamu kurum ve kuruluşları ile gerçek ve tüzel kişileri kapsar.

- **"Amaç" sadece üretimine yönelikken, "Kapsam" haberleşme yapmayı da kapsamakta.**

✧ **Soru: Bu yönetmelik, kodlu veya kriptolu elektronik haberleşme yapan gerçek ve tüzel kişileri kapsıyor mu, kapsamıyor mu?**

farmafarm

ÖZGÜR KRİPTO

İLGİLİ YASA VE YÖNETMELİK

- **Yönetmelik**

  Madde 5:
  5809 sayılı Kanunda belirtilen istisnai kurumlar haricindeki tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler bu Yönetmelik hükümlerine aykırı olmamak kaydıyla kodlu ve/veya kriptolu haberleşme yapabilir.
  İzin başvurusu sadece ithalatçı ve/veya imalatçı için geçerlidir.

Sorunun cevabı ortaya çıkıyor: Gerçek ve tüzel kişiler kodlu ve/veya kriptolu haberleşme yapabilirler; yeter ki bu yönetmelik hükümlerine aykırı olmasın. Ayrıca, Anayasa ve ilgili yasanın 4ncü maddesindeki ilke de dikkate alındığında, bu hususta mesele yokmuş gibi görünüyor.

✧ **Yeni soru: Peki, gerçek ve tüzel kişilerin bu yönetmelik hükümlerine aykırı olmayacak şekilde kodlu veya kriptolu haberleşme yapması mümkün mü?**

farmafarm

ÖZGÜR KRİPTO

CATCH-22

- **Yönetmelik -gerçek ve tüzel kişi kullanıcı için değil ama- ithalatçı ve imalatçılar için izin alma mecburiyeti getiriyor. (bkz. Madde 5, 6 ve 7) Ayrıca, yolcu beraberinde getirilen cihazlar için de izin almak gerekiyor.**
- **Tam bir (içinden çıkılmaz) Catch-22 durumu söz konusu.**
  - **Gerçek ve tüzel kişiler kodlu veya kriptolu, yani gizli haberleşebilirler ama kullandıkları cihaz (donanım ve yazılım) için mutlaka izin almaları lazım.**
  - **İzin alabilmek için kripto tasarımı, algoritma ve en önemlisi, anahtarın Kurum'a (BTK) verilmiş olması gerekiyor.**

✧ ***Kapalı zarf içerisinde mektup veya kapalı kutu içerisinde eşya gönderebilirsiniz ama sadece izin verilen, onaylanmış zarf veya kutu kullanmanız kaydıyla.***
Ne kadar mantıklı?..
Denetleyen için olabilir ama kullanıcı için hiç değil...

farmafarm

ÖZGÜR KRİPTO

BÜROKRASİ > YASA VE ANAYASA

- **Özetlersek:** Anayasa, haberleşmenin gizliliği esastır diyor;
  Yasa, haberleşmenin gizliliği ilkesini gözetiyor;
  ama Yönetmelik, ancak anahtarı (şifreyi) bana bildirirsen gizli haberleşebilirsin diyor.

Tipik bir bürokrasinin, yasa ve anayasanın üstüne çıkması durumu...

Tipik bir anayasa ve yasa ile sağlanmış özgürlüğün bürokrasi vasıtasıyla kısıtlanması durumu...

Tipik bir yasaya uymadığı halde, yasadan aldığı yetkiyle cezai müeyyide uygulatma durumu... (bkz. 5809 sayılı Kanun, Madde 63)

farmafarm

ÖZGÜR KRİPTO

YARARDAN ÇOK ZARAR

- **Peki, bu kısıtlamanın bir yararı var mı?**

  -- Hayır. Üstelik, zararı var.

- **Kısıtlayarak, zor kullanarak, kalın giz perdesi ardına sığınarak kurulan bir güvenlik sisteminin yarardan çok zarar getirdiğine bir nebze değinmiştim.** ***(bkz. www.farmafarm.com -> hakkımda/about ve paylaştıklarım/share "Muhaberat Muharebatı" adlı derlemenin "Nasrettin Hoca'nın Türbesi ve Yılan Yağı" başlıklı bölümü ve "Yılan Yağı Kripto - Snake Oil "adlı sunum)***

- **Defalarca çizmekte yarar var altını:**
  Nasrettin Hoca'nın Türbesi ve Yılan Yağı sadece yanıltıcı bir güvenlik hissi yaratır ki bu çok tehlikeli sonuçlara yol açabilir.

farmafarm

ÖZGÜR KRİPTO

KOLAYA KAÇMAK

- **Gizli haberleşme anahtarının (şifrenin) önceden verilmesi isteniyorsa -ki Yönetmelik bunu istiyor- bu esasında kolaya kaçmak demektir.**
- **Kolaya kaçmak, ilk bakışta pratikmiş gibi görünse de uzun vadede ülkenin kriptoloji altyapısını (insan kaynağı, araştırma, geliştirme, uygulama vs.) zayıflatır, hatta dumura uğratır.**

✧ ***Çocuklara verilen hazır mama bile erken yaşta kesilir; ısırarak yiyebileceği yiyecekler verilir. Niye?..***
Ömür boyu, püre haline getirilmiş sebze ve et yesek daha iyi olmaz mıydı?
- Bir sene boyunca püre halinde hazır mama yiyin; bakın ne oluyor... Dişleriniz dökülür, sindirim sisteminiz bozulur ve daha neler...

Yemek yerken gösterdiğimiz basireti konu güvenlik olduğunda niye gösteremiyoruz?..

farmafarm

ÖZGÜR KRİPTO

MİLLİ KRİPTO

- **Özgür Kripto konusu ile alakalı değil ama Yönetmelikte yer aldığı için burada değinmekte yarar gördüğüm bir nokta daha var.**

  Madde 6:
  Kamu kurum ve kuruluşları tarafından kullanılan kodlu veya kriptolu haberleşme sistemlerinde tasarımı ve üretimi Türkiye'de yapılan milli kripto cihazlarının kullanılması esastır.

"Muhaberat Muharebatı" adlı derleme ve "Yılan Yağı Kripto - Snake Oil" adlı sunumda buradaki tehlikeye yeterince dikkat çekiyorum, sanırım.
(bkz. www.farmafarm.com -> hakkımda/about ve paylaştıklarım/share)

farmafarm

ÖZGÜR KRİPTO

KANDIRMACA

- Nasrettin Hoca'nın türbesi... yılan yağı... kolaya kaçmak...
  Bunlar, güvenlik değil, olsa olsa kandırmaca sağlar.

  Başkalarını kandırmak yanlıştır; kendini kandırmak ise tehlikeli...

- Sonuçta,
  - Anayasa ve ilgili hakim yasa ile ters düşen,
  - Gizli haberleşmeyi kısıtlayan,
  - Güvenlik zaafına açık,
    - Kolaya kaçan,
    - Yılan yağını teşvik eden,
  - Tehlikeyi gidermek yerine, tehlikeye zemin hazırlayan
    bir Yönetmelik söz konusu...

farmafarm

ÖZGÜR KRİPTO

OLMASI GEREKEN

- Peki, tehlikeyi önlemek üzere hazırlanan bir Yönetmelik nasıl oluyor da tehlikeye zemin oluşturuyor?
- Çünkü (1) yasak koyarak güvenliği sağlamaya çalışıyor;
  (2) kolaya kaçıyor, kolaycılığı teşvik ediyor.

Halbuki, olması gereken;

- Kuvvetli kripto (gerçek ve tüzel kişilerce de) serbestçe kullanılabilmeli (Anayasa ve 5809 no'lu yasa)

  Kullanılan şifre anahtarı -mahkeme kararı olmadıkça- Kurum'a verilmemeli
- Kuvvetli kriptonun imalat, ithalat ve ihracatı serbestçe yapılabilmeli (Wassenaar Düzenlemesi)

farmafarm

ÖZGÜR KRİPTO

YETKİNLİK ARTAR

- Ancak bu şekilde, bir tarafta haberleşme özgürlüğü temin edilirken, diğer tarafta -topyekun- kriptoloji yetkinliği artırılır.
- Topyekun kriptoloji yetkinliğinden kast edilen:
  konu ile ilgili denetleyici kurumların, uygulayıcı kurumların, eğitim kurumlarının, eğitim düzeyinin, profesyonel kullanıcıların, amatörce ilgilenenlerin yetkinliği...
- Yetkinlik, ancak açık rekabet, çalışma ve eğitim ile artar, kapalı kapılar ardına saklanarak değil.
- ABD'de NSA, FBI, NIST ve benzeri kurumlardaki profesyoneller ile eğitim ve uygulama dünyasındaki profesyoneller ve amatörler arasındaki yarıştan serbest kullanıcılar kadar devlet kurumları da yarar sağlamaktadır.

farmafarm

ÖZGÜR KRİPTO

BİZDEN ÖRNEKLER

- **Bizdeki benzer kısıtlamalar ve sonuçlarından birkaç örnek:**
  - **Yıllar önce, Gümrük Birliği'ne girmenin, uluslararası ticaret serbestisi ve rekabetin ülkeye zarar vereceği iddia ediliyordu.**
  - **Yıllar önce, radyo yayını yapmak bir yana, basit bir verici yapmak hatta kullanmak bile yasaktı. Yapan, kullanan casuslukla suçlanırdı.** ***Elektrik mühendisliği öğrencisi olduğum yıllarda (70'lerde) amatörce, deney amaçlı radyo alıcısı yapardık ama verici yapmaya korkardık. Mühendis olarak çalıştığım şantiyelerde, fabrikalarda kısa mesafeli el telsizi dahi kullanamazdık.***
  - **Yıllar önce, haberleşme (telefon, mektup, koli) devlet tekelindeydi. Çaycı düafonu bile kanuna aykırıydı.**

farmafarm

ÖZGÜR KRİPTO

BİZDEN ÖRNEKLER

- **Sonra ne oldu?**

  Dünyada ve ülkemizde iletişimin yaygınlaşması, teknolojini gelişmesi, toplumun bu gelişmeyi özümsemesi ve talep etmesi, toplumun talebini ve dünyadaki gelişimi algılayan siyasi irade ve daha birçok sebeple;

  - **Rekabet sayesinde teneke buzdolaplarından, arabalardan kurtulduk; şimdi en iyisini biz imal edip ihraç ediyoruz.**
  - **Telsiz vericisi yapmak artık çocuk eğlencesi haline geldi.**
  - **Fabrikasında, şantiyesinde, çiftliğinde, işinde ihtiyaç duyan herkes telsiz kullanabiliyor.**
  - **Çok sayıda serbest radyo ve televizyon vericisi var.**
  - **Telefon hizmeti veren birçok şirket var. Hatta, internet üzerinden dünyanın öbür ucuyla sesli ve görüntülü haberleşebiliyoruz.**
  - **Mektup ve koli taşıyan çok sayıda özel kurye var.**

  Önce değişim yaşandı, mevzuat sonra değişti.

farmafarm

ÖZGÜR KRİPTO

MEVCUT DURUM

- **Kodlu ve kriptolu haberleşme yapan gerçek ve tüzel kişiler -Yönetmelik'te belirtildiği üzere- kripto anahtarlarını teslim ediyorlar mı Kurum'a?**
- **İnternet üzerinden (PGP, vb.) kriptolu haberleşme sistemleri kullanan bir dolu özel kullanıcı anahtarlarını teslim ediyor mu?**
- **Bırakın kriptolu haberleşme için özel olarak tasarlanmış sistemleri, Gmail, Yahoo vb. yazışma uygulamalarını kullanan herhangi bir kimsenin anahtarını alabiliyor mu Kurum?**
- **Peki ya şifreli telsiz telefonlar?..**
- **Özel kullanıcılar bir yana, bankalar, finans kuruluşları, sağlık ve sigorta kuruluşları kullanmakta oldukları profesyonel amaçlı kriptolu haberleşme sistemlerinin şifrelerini veriyorlar mı Kurum'a?**
  (Vermiyorlardır herhalde... Kimse bankada ne kadar parası bulunduğunun veya ne gibi bir sağlık sorunu olduğunun -mahkeme kararı olmaksızın- yetkisiz biri tarafından bilinmesini istemez.)

farmafarm

ÖZGÜR KRİPTO

MEVZUAT < UYGULAMA

- Önceki sayfadaki soruların cevaplarının, “Hayır” olduğunu biliyorum (umuyorum).
- Uygulamada kripto anahtarı teslim edilmezken hâlâ bu ısrar niye?..
- Mevzuat mutlaka uygulamanın gerisinde mi olmalı?..
- Geçmişteki örneklerden ders çıkarılamaz mı?..
- Zamanı gelmiş bir fikir acaba güçlü mü, gerçekten?

SONUÇ

- Özgür kriptonun zamanı geldi artık.
- Özgür kriptodan çekinmeye gerek yok; aksine teşvik edilmeli.
- Bu, bir doğal hakkın teslimi kadar sektördeki gelişmenin de itici gücü olacaktır.

farmafarm

ÖZGÜR KRİPTO

KAYNAKÇA

http://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf

http://www.tk.gov.tr/mevzuat/kanunlar/dosyalar/elektronik_haberlesme_kanunu.pdf

http://www.tk.gov.tr/mevzuat/yonetmelikler/dosyalar/Kripto_Yonetmeligi.pdf

https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

farmafarm

ÖZGÜR KRİPTO

TEŞEKKÜR EDERİM

Ruşen Eşref YAZGAN