MART 2023 | SAYI 2

BİLİŞİM HUKUKU KOMİSYONU BÜLTENİ

BU SAYIDA

BÜLTENİMİZDE

Teknoloji, bizlerin takip edemeyeceği hızda gelişmekte ve hayatımızın ayrılmaz bir parçası haline gelmektedir. Her gün gelişen teknolojiye ayak uydurmak biz hukukçular için zorunlu hale gelmiştir. Yapay zeka, blockchain, fintech, NFT, fikri ve sınai mülkiyet, internet, e-ticaret, kişisel verilerin korunması gibi kavramların insan hakları, ceza hukuku, sözleşmeler hukuku gibi hukukun temel alanlarında incelemek ve bunlar hakkında bilgi sahibi olmak biz hukukçuların bakış açısını geleceğe yönlendirecektir.

Aynı zamanda bu kazanımlar ile hukukçular, bilişim dünyasında yoğun zaman geçiren milyarlarca insanın işlem güvenliğini sağlamak ve dijital anlamda da geleceğe temiz bir dünya bırakmak görevi de üstlenmektedir .

Bu düşünceler ile bizler de bilişim ve hukukun kesiştiği alanlardaki gelişmeleri takip ederek siz değerli okuyucularımıza aktarabilmek, *yeni çıkan yasal düzenlemeleri sizlerle buluşturabilmek adına Bursa Barosu Bilişim Hukuku Komisyonu olarak sizlere her ay bülten hazırlıyoruz.

Bilişim hukuku alanında meslektaşlarımızın sizler için hazırladığı makaleleri, haberleri, dizi, film ve kitap önerilerini ve daha birçok içeriği her ay bültenimizden takip edebilirsiniz.

Bültenimizin siz okuyucularımız için bilgi verici olmasını ve okurken keyifli zaman geçirmenizi temenni ediyoruz.

Saygılarımızla.

Av. Oğuzhan SEYMEN

1- Giriş-Depremde Bilişim Hukuku:

Ülkemizde asrın felaketi olarak anılacak olan 6 Şubat Doğu Depremi; gerek arama, kurtarma ve koordinasyon çalışmalarında gerekse afetin yol açtığı zararlarda sorumlulukların tayini konusunda hukukumuza, bilişimi ve teknolojiyi ivedilikle uygulama zorunluluğunu gözler önüne sermiştir. Dolayısıyla gündemdeki bu acil alarma yönelik, Bültenimizin 2.Sayısındaki işbu Ter**mal Kamera İle Enkaz Altında Arama, Kurtarma ve Delil Tespiti konulu yazı ile** ışık tutulması hedeflenmektedir.

2- Termal Kamera-Görüntüleyici Nedir? Nasıl çalışmaktadır?

Termal kamera tanımlanırken birtakım aşamalara değinmekte fayda vardır:

a- Bütün nesneler, ısı imzası denilen, gözle görülemeyen IR enerjisi-kızılötesi enerji yaymaktadır. Bu kızılötesi enerji,
özellikle afet gibi acil durumlarda arama kurtarma ve delil tespitinde ısının bulunduğu yeri görebilmede kolaylık sağlamaktadır.

b- Termal kamera da bünyesinde, bu kızılötesi enerjiyi ızgara şeklindeki özel detektör çipine sensör dizisine odaklayan optik bir sistemi barındırmaktadır.

c- Sensör dizisindeki her piksel, odaklanılan kızılötesi enerjiye

d- tepki verir ve birer elektronik sinyal üretir. Kamera işlemcisi de bu sinyali alır, matematiksel hesaplama uygular ve nesnenin belirgin sıcaklığının bir renk haritasını oluşturur.

e- Her sıcaklık değeri farklı bir renk ile gösterilir. Nihayetinde oluşan renk matrisi, nesnenin sıcaklık resmi yani termal görüntüsü olarak kameranın ekranında ve belleğinde görüntülenmektedir. *(1-Özet alıntı olarak bkz: https://www.fluke.com/tr-tr/bilgi-edinin/blog/termal-goruntuleme/termal-kameralar-nasil-calisir)*

3- Termal Kamera-Görüntüleyicinin 6 Şubat Depremine İlişkin Arama, Kurtarma ve Delil Tespitindeki Önemi

a- Deprem felaketinde, bilişimin afet koordinasyonuna bilhassa termal görüntüleyiciler ile nasıl etkin katkı sunduğu, cihazın kullanıldığı ülkeler tarafından kabul edilen bir gerçektir. Nitekim Türkiye Milli Savunma Bakanlığı Jandarma G. Komutanlığı çalışmalarının yanı sıra Meksika 2017 yılında yaşanan depremde de bu

termal görüntüleyiciler ile nesnelerin ısılarından yararlanmak suretiyle nice delillerin tespitini kolaylaştırmıştır. Bu nedenledir ki termal görüntüleyiciye işbu yazıda delil tespiti bakımından dikkat çekilmek istenmektedir.

b- Can Kaybının Önlenmesi, Ölüm ve Yaralanma Verilerinin Toplanması-Bildirilmesi

Tüm imkanların seferber edildiği deprem felaketinde ısıl değişkenliklerin tespit edilebildiği termal kameralar da askeri alandan çıkıp acilen afet bölgesine seferber edilebilmiştir. Deprem bölgesi enkaz alanında termal kameralar; canlı varlıkların yerini bulabilmesi, can kaybının önlenmesi, bunun yanı sıra da ölüm ve yaralanma verilerinin toplanması-bildirilmesi açısından kayda değerdir.

c- Cezai ve Hukuki Boyut İle Delillerin Toplanması-Sorumlulukların Tayini

Felaketin ardından deprem bölgelerinde elektrik, su ve doğalgaz hatları ciddi anlamda zarar görmüştür. **Elektrik ve gaz kaçakları**, ışık elde etmek için ateş yakılması sonucunda dahi deprem anında yangınlar çıkmasına, yangın sebepli ölümlere yol açtığı görülmüştür.

İlk olarak vurgulamak gerekir ki ceza adalet sistemi, olası kast cinayetinde ve hizmet nedeniyle görevi kötüye kullanma suçunda faillerin kimler olduklarının araştırılmasını, yurt dışına firar etmeden yakalanmalarını ve **suç delillerinin karartılmadan toplanılmasını** kamu vicdanının tatmini için acil görmelidir.

Depremin sonucu meydana gelen tüm kayıplar, mimarlar, mühendisler ve hukukçular tarafından, ilgili Özel Kanunlar, Yönetmelikler ve Türk Borçlar Kanunu kapsamında müteahhitlerin ve diğer tehlike sorumlularının, yapı denetim şirketlerinin, kamu kurum-kuruluşlarının ve idarecilerinin ve yapı malikinin **sorumluğunun belirlenmesini, faillerin araştırılmasını** da zorunlu kılmıştır.

d- Termal Kamera-Görüntüleyici ile Teknik Anlamda Delillerin Nasıl Toplandığı

Termal görüntüleyici özellikle depremin hemen akabinde ihtiyaç duyulan bir delil toplama vasıtasıdır:

i) Kurtarma çalışmaları sırasında insan gücüne her daim ihtiyaç olmasına karşın; enkazdaki canlıları tespit etmede canlıların duyuları algı duyarlılığı açısından yetersiz kalabilmekte ve dar alanlarda hareket kabiliyeti de sınırlı olmaktadır.
İnsanlar tarafından girilmesi teknik olarak pek mümkün olmayan ya da daha tehlikeli olan enkazlar da otonom veya manuel olarak kontrol edilebilen sinüsoidal(360*sinüsleri ile) manevra kabiliyetine sahip, **termal görüntü işleme** ve gaz algılama özellikleriyle donatılmış 70 x 1170 x 80 mm boyutlarında bir

biyonik yılan robotlar da termal kameranın bir üst tasarımı olarak delil toplama sürecine dahil edilmiştir. *(2022; Göçük Altında Kalanların Tespiti için Biyonik Yılan Robot Tasarımı; Gökhan Çetin, Esra Aksakal, Sezai Taşkın)*

ii) **Termal görüntüleyicinin prototip(henüz ilk) tasarımında**, Panasonic AMG8833 Grid-EYE® görüntüleyicisi kullanılmıştır. Algılama çözünürlüğü 8X8 piksel olup endüstriyel bir üründür. Algılama hızının oldukça yüksek olması ve yüksek kazançlı olması sebebiyle tercih edilmiştir. 3.3V DC gerilimle çalışan termal görüntüleyici 0-80 °C arasında sıcaklık değerlerini ölçebilmektedir. Bu sayede ortamdaki nesneleri, sıcaklık farklarını yakalayarak tespit etmektedir *(Anonim, 2022d)*.

Prototipte iki farklı mikro denetleyici türü kullanılmıştır. Ana kontrolör olarak Raspberry Pi 4 kullanılmış olup yardımcı kontrolör olarak Arduino UNO R3 kullanılmıştır. Termal görüntüleyici Raspberry Pi 4 ile kontrol edilirken, diğer tüm algılayıcılar Arduino UNO R3 ile kontrol edilmektedir. Raspberry Pi 4 ile Arduino UNO R3 mikro denetleyicileri USB arayüzü üzerinden seri port haberleşmesi aracılığıyla birbiriyle iletişim kurmaktadır. *(Anonim, 2022g)*

Servo motorların yönelim hareketini sağlıklı bir şekilde gerçekleştirebilmesi için termal görüntüleyici ve gaz algılayıcıların birlikte çalışmasının gerekliliği öngörülmüştür. Canlılar tarafından doğal yollarla üretilen aseton gazı ve yine canlıların yaşamsal etkinliklerini sürdürdükleri sürece açığa çıkan sıcaklık bu iki algılayıcı tarafından algılanabilmektedir.

Termal görüntüleyici ile algılanan sıcaklık verileri frekans filtrelemeye dayalı görüntü işleme yöntemleri ile işlenerek 33.238.2° C sıcaklıkları görüldüğünde Raspberry Pi 4 üzerinde seçilen çıkışı aktif etmektedir. Bu çıkış, Arduino UNO R3 üzerinde bulunan motorun yönelim hareketini kontrol eden girişe bağlıdır. Bu yüzden motor, kendisine bağlı olan servo ekseni belirtilen aralıklardaki sıcaklık değerleri görülen alana doğru yönelimini gerçekleştirdiğinde hareketini durdurmaktadır.

Benzer şekilde, WSP2110 algılayıcısının algıladığı belirli bir miktar aseton gazıyla birlikte Arduino UNO R3 üzerinde bulunan motor yönelim hareketini durduran giriş lojik 1 olarak motor hareketini durdurmaktadır. Aseton gazı miktarı, seri port üzerinde okunan değerlerle kontrol edilmektedir. Otonom sistemin blok diyagramı Şekil 1'de gösterilmiştir.

Şekil 1:

DC sinyal → PWM sinyal üretici → WSP 2110 gas sensörü → "Termal Görüntüleyici"→ MH-Z14 gas sensör → Nextion2.4.*HMI→ I2C

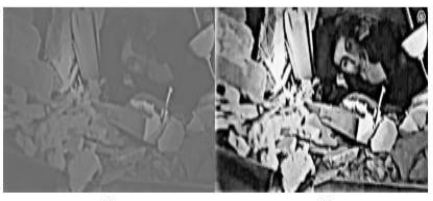
haberleşme modülü→ Arduino UNOR3 → Rasberry P4 →Motor yönelim hareketi

Şekil 1'de görüldüğü üzere, sisteme MH-Z14 gibi karbondioksit gazının algılanması için gerekli algılayıcı da eklenebilmektedir. Yine Şekil 1'de görüldüğü gibi, sistem PWM anahtarlaması, analog ve dijital sinyallerin bir arada çalışabilmesi üzerine kurgulanmıştır. Bu prototipte gaz ve termal görüntü kontrolleri yapılırken, servo motor 30° açı hassasiyeti ile yönelim hareketinde bulunmaktadır. Başka bir deyişle, 30° bir alan taraması gerçekleştirilirken istenen gaz yoğunluk değeri ve/veya termal sıcaklık değeri elde edilirse motor yönelim hareketini durdurmaktadır.

iii) **<u>Termal görme bakımından</u>** ise Prototip üzerinde kullanılan Panasonic AMG8833 Grid-EYE® termal algılayıcı; endüstriyel alanda ve otomotiv üretiminde kullanılmak üzere geliştirilmiş, çözünürlüğü 8x8 piksel olan pasif termal kızılötesi algılayıcıdır (Anonim, 2022d).

iv) Termal algılayıcının yazılımsal olarak geliştirmeye açık bir yapısı bulunmaktadır. Raspberry Pi üzerinde sıklıkla kullanılan Camera soketini kullanmayan, SDA ve SCL bağlantı noktaları ile haberleşme sağlayan bir görüntüleyici çeşididir. Termal görüntüleyici, doğal olarak, ortamdaki nesnelerin sıcaklık farkları ile kızılötesi ışınları da kullanarak görüntü algılamayı sağlar. Ancak, bu görüntüleme çeşidi enkaz gibi farklı parlaklık dereceleri bulunması mümkün olan mekanlarda tek başına yeterli olmamaktadır. Bu nedenle, elde edilen gerçek zamanlı termal görüntüler üzerinde dijital görüntü işleme süreçlerinin gerçekleştirilmesi gerekmektedir. (2) 2022; *Göçük Altında Kalanların Tespiti için Biyonik Yılan Robot Tasarımı; Gökhan Çetin, Esra Aksakal, Sezai Taşkın)*

Enkaz altında daha önceki afetlerde normal kamera ile çekilmiş bir görüntünün (Termal Görüntüleyici Destekli Biyonik Yılan Robotuna ilişkin) **<u>bu çalışmada kullanılan görüntü işleme sonucu elde edilen çıktıları</u>** Şekil 12'de verilmiştir: (Çalışmada atfı bulunan bütün yazarlar; bilinen herhangi bir çıkar çatışması veya herhangi bir kurum/kuruluş ya da kişi ile ortak çıkar bulunmadığını onaylamışlardır.)



(a) (b)

Şekil 12. (a) Yüksek geçiren filtre uygulanmış görüntü, (b) Histogram eşitlemesi uygulanmış görüntü

4- Sonuç ve Temenni

<u>Bilişim hukuku vasıtası ile</u> yakın gündemde yaşanan Kahramanmaraş Pazarcık ve Elbistan'da yaşanan 7.6 ve 7.4 büyüklüğündeki ve Hatay'daki 6.4 ve 5.8 büyüklüğündeki <u>depremlerde</u>

delillerin toplanmasına nasıl etkin katkı sunulabileceği ve bu hukuk dalının ülkemizde ne kadar geliştirilmeye muhtaç bir dal olduğu işbu çalışma ile açıkça gösterilmektedir. Bu hukuk dalımızın hukukçular, yazılım mühendisleri ve bütün bilim insanlarınca geliştirilmesini, termal kameralar başta olmak üzere bilişim teknolojilerinin insan hayatına hukuk güvenliğini de tesis edebilmesini temenni ediyorum. Teşekkürlerimle.

Kaynakça:

1) https://www.fluke.com/tr-tr/bilgi-edinin/blog/termal-goruntuleme/termal-kameralar-nasil-calisir
2) *2022; Göçük Altında Kalanların Tespiti için Biyonik Yılan Robot Tasarımı; Gökhan Çetin, Esra Aksakal, Sezai Taşkın*

KRİPTO VARLIKLARLA YARDIM TOPLAMA

Stj. Av.İrem NALBANT

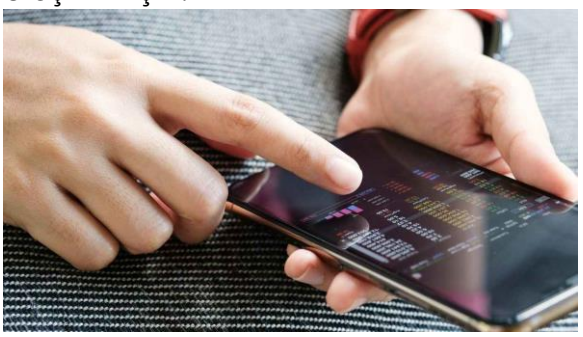
6 Şubat 2023'te ve devamında Kahramanmaraş ve Hatay illerimizde gerçekleşen, başta bu illerimiz olmak üzere civar illerimizi de etkileyerek büyük acılara neden olan deprem felaketi için hepimize sabır diliyoruz.

Söz konusu depremlerde kaybedilen canların acısının, hayatta kalanların yaşam mücadelesine karıştığı mezkur bölgelerde Türkiye'nin her yerinden yola çıkan ayni yardımların ardından nakdi yardımlar da gündeme gelmiş ve yardım seferberlikleri oluşturulmuştur. Yurt dışından ve yurt içinden bölgeye yardım etmek isteyen sayısız insan, başlatılan seferberliklere yardım göndermiştir.

Ülkemizde yaşanan felaketin boyutu neticesinde yurt içinden ve dışından birçok insan depremden etkilenmiş, insanımız çok büyük kayıplar yaşamıştır. Facianın teknik ve sosyal olarak büyüklüğü, onu dünya gündemine de taşımış ve diğer ülkelerden hem kamu otoriteleri hem de halk bazında yardım istekleri doğmuştur. Yurtdışından ülkemize çok ciddi miktarlarda nakdi yardım ulaştırıldığı da bilinmektedir.

Yurt dışından gönderilecek nakdi yardımlar için bankaların kullanılması elzem olup bazı bankalar yüklü miktarlar için kaynak araştırması talep etmekte iken daha makul miktarlar için dahi öncelikle paranın bir kısmının banka komisyonuna ayrılması, ardından işlemin çıkış bankasından varış bankasına ulaşmasının beklenmesi gerekmektedir. Kaldı ki, varış bankasındaki hesabın da ayrıca ülkemizdeki idareden izin alınarak açılması gerekliliği düşünüldüğünde süreç ivedilikten bir hayli uzaktır.

Görüldüğü üzere, aktarılmak istenen para büyüdükçe yardımın ve zamanın ciddi bir kısmının aktarım işlemlerine feda edildiğini görüyoruz. Acil ihtiyaçlar doğurmuş olan bir felaket bölgesine gönderilen paranın klasik bankacılık işlemlerinin hantallığına takıldığı gayet açıktır.Bunun farkında olan birtakım gerçek ve tüzel kişiler, maliyet ve süre konularında ciddi anlamda kolaylık sağlayabilecek olan ve farklı ülkelerin vergi sistemlerinden en az şekilde etkilenecek olan kripto varlıkları tercih etmişlerdir. Kripto varlıklar sayesinde dünyanın herhangi bir yerinden, çok yüklü miktarlarda paralar çok kısa süreler içinde aktarılabilmiştir. Ayrıca işlemler şeffaf olarak tüm kullanıcılar tarafından gözlemlenebilmiş ve bağışlanan kriptoların daha sonra hangi cüzdanlara aktarıldığı veya ne zaman itibari paraya çevrildiği takip edilebilmiştir. Ucuz, hızlı ve şeffaf bir şekilde yardımlar afet bölgesine ulaştırılmıştır.



Bahsedilen bu avantajların, klasik yöntemle bağış yapmayı zor bulduğu için geri duran veya küçük de olsa bir yardımda bulunmak istemesine rağmen yardım tutarından çok daha da yüksek bir

maliyet çıkaracak olan transfer işlemleri nedeniyle alıkonan insanların da yardım etmesine ön ayak olduğu kanaatindeyiz.

Peki hukukumuzda kripto varlıkların kendisini ayni veya nakdi nitelikte bir yardım olarak kabul edilmesi mümkün müdür? Kripto varlık ile yapılan yardımın akıbeti nedir?

Bilindiği üzere hukukumuzda, kanunun öngördüğü istisnalar dışında yardım toplamak devletin iznine özgülenmiş bir faaliyet olup, usulüne uygun olsun olmasın toplanan ayni veya nakdi yardım devlet malı sayılmaktadır. Bu nedenle, yardımın amacına ulaşması ve usule ilişkin engelleri aşabilmesi için yardım faaliyetlerinin kanunda öngörülmüş usul ve esaslara uygun olarak gerçekleştirilmesi önem arz etmektedir.

2860 s. *Yardım Toplama Kanunu*'na göre yardım toplama faaliyetine girişen kişi, bir gerçek veya tüzel kişi olması fark etmeksizin, yürüteceği yardım faaliyetinin sebebini, konusunu, süresini ve elde edilmek istenen miktarı; yardım edilecek mahallin en büyük mülki idare amirine bildirmek ve ondan izin almak mecburiyetindedir. Söz konusu yardımın internet üzerinden toplanıldığı durumlarda ise yardım toplanılan sitenin IP'si, alan adı gibi verilerinden elde edilen bilgiler doğrultusunda e-posta veya sair yöntemlerle yardım toplayana ulaşılmaya çalışılacak, yirmi dört saat içinde netice alınamaması halinde idare tarafından sulh ceza hakimliğinden erişim kararı talep edilebilecektir. Nitekim izin koşulu sağlanmaksızın gerçekleştirilen yardım toplama faaliyetleri kolluk tarafından engellenecek ve bu fiile girişenler hakkında soruşturma evresi atlanarak doğrudan kovuşturma başlatılacaktır. Ülkemize yurt dışından yardım gönderilebilmesi için ise nakdin banka aracılığı ile gönderilmesi ve gönderimin bir derneğe yapılması gerekmektedir.

Tüm bu düzenlemelerde kripto varlıklara yönelik bir kısım bulunmamaktadır. Nitekim hukukumuzda kripto varlıkların niteliğine dair bir düzenleme mevcut olmadığı gibi kullanımı yasaklanmıştır. Bu açıdan kripto varlıkların yardım toplama faaliyetine konu olup olamayacağı açısından yapılabilecek tek tahlil mevzuattaki tanımlara girip girmediğinin teşhisi yönündedir.

"Yardım Toplama Esas ve Usulleri Hakkında Yönetmelik'te ayni ve nakdi yardımın tanımına yer verilmiştir. Buna göre ayni yardım, nakit ve nakit benzeri dışındaki tüm maddi varlıklarla yapılan yardımları; nakdi yardım ise nakit ve nakit benzeri olarak yapılan yardımları ifade etmektedir. Nakit kelimesinin para teriminin bir karşılığı olduğu ve kripto varlıkların "Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik" ile bir ödeme aracı olmaktan dışlandığı gözetildiğinde kripto varlıkların nakdi bir yardım niteliğinde olamayacağı sonucu çıkmaktadır. Ayrıca, yine aynı yönetmelikte kripto varlıkların "gayri maddi varlık" olduğu belirtildiğinden ayni (maddi) yardım olma niteliğini de karşılamayacaktır. Neticede söylenebilir ki pozitif hukukumuz çerçevesinde

henüz kripto varlıkları oldukları haliyle yardım etmekte kullanmamız mümkün değildir.

Yine de, örneklerine rastlamanın mümkün olduğu bir şekilde, kripto paraların fiziki mesafe, hız ve şeffaflık konularında sunduğu kolaylıkların kullanılması ve ardından toplanan kripto varlıkların TL cinsine çevrilerek valilikçe yardım toplamak için açılmış hesaplara transfer edilmesi ile mevcut duruma çözüm getirilmiş ve işlemler hızlandırılmıştır. Kişilerin tercih edeceği kripto varlıkların dalgalanmadan uzak, stabil coinler olması önerilmiş ve bu sayede toplanan yardımların TL cinsine çevrilmesine kadar geçecek sürede maddi bir kayıp yaşanmaması sağlanmıştır.

Yardımların en kısa sürede deprem bölgesine ulaştırılması ve oradaki insanlarımıza merhem olması dileklerimizle.

Türkçeye yemleme veya oltalama olarak çevrilen phishing saldırısı günümüzde çoğu insanın maruz kaldığı bir siber saldırı türüdür. İnternetin kullanımı bugün zorunlu hale gelmiş olup alışverişler, bankacılık işlemleri, finansal işlemler, kurum içi iletişimler ve benzeri birçok kritik veri internet üzerinde yaygın olarak kullanılmaya başlanmıştır. Hayatımızın her alanında var olan internet çoğunlukla kurtarıcımız olsa da bu durum siber saldırganlar tarafından bir fırsata çevrilmiş durumdadır. Phishing saldırısı saldırganlar tarafından çeşitli yöntemlerle -çoğunlukla güvenilir kurumlar kullanarak- kullanıcıyı inandırarak kişisel verilerin ele geçirilmesi şeklinde işlemektedir.

PHISHING SALDIRI YÖNTEMLERİ

Bu yöntem ile temelde saldırgan tarafından hazırlanan yemin bir kurban tarafından yenilmesi amaçlanmaktadır. Daha çok bilinçsiz kullanıcılar için hazırlanan bu yemler genelde maaş zammı, hediye, ücretsiz tatil, para ödülü şeklinde cezbedici senaryolardan oluşmaktadır. Fakat üzülerek söylemek gerekir ki sadece bu senaryolar ile değil geçtiğimiz günlerde yaşanan deprem felaketinde ilgili kurumların isimleri kullanarak ''bağış sekmesi'' adı altında bu saldırılara devam edilmiştir.

İnternet tarihinin en eski ve en etkili yöntemlerinden biri olan phishing saldırıları yaygın olarak e-posta aracılığıyla gerçekleştirilmektedir. Günümüzde sosyal medyanın popüler olması ve çok büyük kitlelere ulaşmasıyla virüs worm gibi zararlı kodların yayılmasına neden olmuştur.

E-posta ile Oltalama

E-posta yöntemini kullanarak yapılan dolandırıcılıkta farklı yollar izlenmektedir. Genellikle hedef kullanıcının sık sık irtibat halinde olduğu kuruluşlardan veya güvenilir şirketlerden gönderilmiş izlenimini veren e-posta hazırlanır. Burada önemli nokta kullanıcının ilgisinin olduğu kuruluş ve şirketlerin e-postasına benzerliğidir. Bu ilginin varlığı sosyal mühendislik ve açık kaynak istihbaratı ile sosyal medyadan kullanıcının takip ettiği sayfalardan kolayca tespit edilebilmektedir. Farklı yollar izlenilebilen bu yöntemde kullanılan yollar genellikle şu şekildedir:

- Hedef kullanıcının e-postasına sürekli irtibatta olduğu kuruluştan geliyormuş gibi e-posta gönderilir. Bu mail içeriğinde şifrenin

dondurulduğu, değiştirilmesi gerektiği, başkası tarafından kırılmaya çalışıldığı vb. mazeretlerle şifresinin değiştirilmesi gerektiği bildirilir. Genellikle şifre değiştirme sayfası için e-posta içerisinde bir link verilir ve bu link sayesinde kişi, saldırgan tarafından hazırlanmış olan web sitesine yönlendirilir. Tüm hareketler saldırganın kontrolünde olduğundan kullanıcı şifresini değiştirdiğinde veriler saldırgan tarafından kopyalanır. Şifreye sahip olan saldırgan artık kurum veya şirketin kendi web sayfasında kullanıcının şifresini girerek para transferi, alışveriş gibi işlemleri kolayca yapabilmektedir.

- Bir diğer yöntem ise sahte bir çekiliş düzenlemektir. Bu yöntemde hedef kullanıcının e-postasına çekilişi kazandığına dair bir mail gönderilir. Bu mailde çekilişi alması için bazı bilgilerin verilmesi istenir. Hedef kullanıcı bilgileri verdiği takdirde tüm kişisel verileri saldırganın eline geçmiş olur.
- Eposta yoluyla yapılan phishing saldırılarından biri de epostanın kotasının dolduğu, bilgilerini güncellemesi gerektiğine dair mail gönderilerek yapılmaktadır.
- Son zamanlarda ise bu yöntemlere ek olarak yeni bir yöntem daha gelişmiştir. Bankaların cep telefonuyla para transferi işlemini yapmasını sağlayan sistem çalınarak hedef kullanıcılara kendi hesaplarına para transferi yapıldığına dair bilgilendirme mesajı gönderme şeklinde yapılmaktadır. Burada kullanıcının hesabını kontrol etmesini sağlayarak sahte bir web sayfasına yönlendirir ve bilgilerini girmesi sağlanır.

Sosyal Ağlar Üzerinden Oltalama

Günümüzde her yaştan kullanıcının olduğu sosyal ağlarda insanlar ilgi alanlarına dair paylaşım ve etkileşim içerisine girmektedirler. Çok fazla ve hızlı bir etkileşimin olduğu sosyal ağlarla birlikte kullanıcılar daha dikkatsiz hale gelmektedir. Hal böyle olunca kullanıcıların siber saldırılara karşı önlem alması biraz daha zorlaşmaktadır. Hedef kullanıcının ilgi alanına bağlı olarak gelen mesajlarla kullanıcıyı ikna etme olasılığı yükselmektedir. Özellikle sosyal ağlar kullanılarak yapılan saldırılarda çoğunlukla

interneti temel seviyede kullanan kitle hedef alınır.

İnternet çağında olmamız sebebiyle günlük hayatta kullandığımız tüm hizmetlere web üzerinden kolayca erişilebilmekteyiz. Artık zorunlu bir ihtiyaç haline gelen akıllı telefonların yaygınlaşmasıyla verilen tüm hizmetlerin bir mobil uygulaması da bulunmaktadır. Erişimi kolay olan bu uygulamalar her ne kadar kullanım rahatlığı sunsa da kişiyi siber saldırılara açık hale getirmektedir.

Oltalama Saldırılarına Karşı Alınabilecek Önlemler

Yapılan bu siber saldırılarda kullanılan mailin gerçeği yansıtıp yansıtmadığını ayırt etmek için dikkat edilmesi gereken bazı unsurlar bulunmaktadır. Oltalama saldırılarında gönderilen e-postalarda genellikle yazım kuralları ve diğer kurallara dikkat edilmemektedir. Gerçekte ise kurum ve şirketlerden gönderilen maillerde bu kurallara son derece uyulmaya çalışılmaktadır. Herhangi bir kurum veya şirket kullanıcıya link gönderip hesabına giriş yapmasını istemez. Eğer gelen mailde bir web sayfasına yönlendiren link bulunuyorsa büyük ihtimalle siber saldırıyla karşı karşıyasınız demektir. Oltalama yöntemi kullanılırken genellikle hedef kullanıcıyı baskı ve korku altında bırakma amacı vardır. Örneğin ''24 saat içerisinde şifrenizi değiştirmeniz gerekmektedir'' gibi bir ifadeyle kullanıcıyı zorunda bırakma eğilimi görülür. Ayrıca belirtmek gerekir ki bu tip saldırılarda SSL sertifikası kullanılmamaktadır. Sertifikaya dikkat edildiği takdirde saldırının farkına varılabilir.

Bu saldırılardan korunmak adına aşağıda sayılan önlemler dikkate alınabilir:

- E-ticaret sitelerinde alışveriş yaparken her site için farklı şifre kullanılmalı,
- Kişisel bilgiler mesajla veya telefonla paylaşılmamalı,
- Sosyal ağlardaki profiller için iki kademeli şifreler tercih edilmeli,
- Ücretsiz ve herkesin kullanımına açık olan ağlar kullanılmamalı,
- Yasal anti-virüs uygulamaları kullanılmalı,
- Mobil uygulamalarda kaynağı belli olmayanlar indirilmemeli,
- En önemlisi ise bu konuda bilgili ve bilinçli olunmalıdır.

Her ne kadar yukarıda sayılan önlemler basit düzeyde olsa da oldukça etkili olabilecek önlemlerdir.

DerinGÖRÜ TÜBİTAK BİLGEM tarafından geliştirilmiş yüz tanıma ve eşleştirme yazılımıdır. TÜBİTAK tarafından DerinGÖRÜ Yüz Tanıma ve Akıllı Turnike Sistemi tesis/binalarda kullanılan kartlı geçiş sistemlerinin yüz tanıma teknolojisi kullanılarak daha güçlü/gürbüz hale getiren, Yapay Zekâ Teknolojileri ile "Sürekli Öğrenen" ve 1-N Yüz Tanıma yapabilen bir teknolojiye sahip bir sistem olarak tanımlanmıştır. [1]

6 Şubat 2023 tarihinde Kahramanmaraş merkezli iki büyük depremde çok fazla insan hayatını kaybetti, pek çoğu maddi manevi yaralar aldı. Depremlerden şüphesiz en çok etkilenenler de çocuklar oldu. Enkazdan çıkarılan, kimliği belirsiz, ailelerine ulaşılamayan, ailelerini kaybeden çocuklar için herkes perişan oldu. Ailelerine ulaşılamayan ve ailelerin ulaşamadıkları çocuklar hakkında özellikle sosyal medyada pek çok paylaşım yapıldı. Aile ve Sosyal Hizmetler Bakanlığı depremzede refakatsiz çocukları aileleri ile buluşturmak için "DerinGörü" yazılımını kullandığını duyurdu. Bakanlık bünyesinde kurulan çağrı merkezine gelen ihbarlarda, çocukların fotoğrafları ve diğer tüm bilgileri (boyu, kilosu, kıyafeti, hangi mahallede veya evde yaşadığı, bulunduğu hastane vs.) ile sisteme giriş yapılıyor. Sisteme aynı zamanda TÜBİTAK çalışanlarının sosyal medyada yaptıkları taramalarda edindikleri veriler, hastanelerden gelen fotoğraflar ve veriler yükleniyor. Sonunda sistemde eşleştirmeler yapılıyor, kimlik tespiti ile diğer ek bilgiler de eşleştiriliyor ve sosyal incelemeler yapıldıktan sonra çocuklar ailelere teslim ediliyor. Aile ve Sosyal Hizmetler Bakanı Derya Yanık, 206 çocuğun kimlik tespitinin bu yazılım sayesinde yapıldığını belirtmiştir.[2]

Deringörü yazılımından yola çıkarak afetzede çocukların kişisel verilerinin korunmasının hukuki boyutunu kısaca ele almak istiyorum.

Kişisel verilerin korunmasındaki temel amaç özel hayatın gizliliğini sağlamak, kişinin temel hak ve özgürlüklerini korumaktır. Kişinin mahremiyet hakkı ve bilgi güvenliği hakkının korunması da bu kapsamdadır. Çocuklara ait verilerle ilgili özel bir düzenleme 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yoktur fakat çocuklara ait verilerin işlenmesinde ayrı özen ve koruma gerektiği tartışmasızdır. [3]

Çocuk verileri işlenirken göz önünde bulundurulması gereken, çocuğun üstün yararı ilkesidir. Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme'nin 3. maddesi uyarınca,

[1] https://bilgem.tubitak.gov.tr/tr/icerik/deringoru-yuz-tanima-ve-akilli-turnike-sistemi

[2] https://www.ulusal.com.tr/yurt/bu-uygulama-ile-1314-depremzede-cocuk-ailesine-kavustu-bakan-yanik-duyurdu-15017931

[3] Çocuklara ait kişisel verilerin işlenmesi Avrupa Veri Koruma Tüzüğü 8. maddede rıza unsuru üzerinden ele alınmıştır. Kişisel verilerin işlenmesi için 16 yaşından büyük olması koşulu aranmaktadır. Eğer 16 yaşından küçük ise, o halde onun yasal olarak tayin edilmiş velisi ya da vasisinin izninin alınması gerektiği düzenlenmiş, Avrupa Birliği'ne üye devletlerin kendi iç hukuk düzenlemelerinde bu yaşı değiştirebilecekleri fakat bu değişimin 13 yaştan az olmayacak şekilde yapılması gerektiği de düzenlenmiştir.

-Kamusal veya özel kuruluşlar, mahkemeler veya yasama organları veya idari makamlar tarafından yapılan ve çocukları ilgilendiren bütün faaliyetlerde çocuğun yararı temel düşüncedir.

Verilerin işlenmesine ilişkin KVKK'nun 4.maddesinde belirlenen genel ilkelerin hepsi çocuk verilerinin işlenmesinde de geçerlidir.

Olağanüstü hâl durumlarında da kişisel verilerin korunmasına ilişkin düzenlemeler geçerlidir. O halde çocukların verileri işlenirken;

-Hukuka ve dürüstlük kurallarına uygun olma,
-Doğru ve gerektiğinde güncel olma,
-Belirli, açık ve meşru amaçlar için işlenme,
-İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
-İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine azami ölçüde önem gösterilmelidir.

Yaşanan afet sonrası genç yaşlı demeden neredeyse herkes deprem bölgesindeki halka yardım eli uzatmaya çalıştı. Kimi fiziken deprem bölgelerine giderek, kimi maddi destekleriyle, iletişim araçları ve sosyal medya organları aracılığıyla depremzedelere fayda sağlamaya, yardımcı olmaya çalıştı. Bu gibi olağanüstü hâl durumlarında kişilerin bireysel olarak, duygu durumlarını kontrol etmesi, bilinçli hareket etmesi güçleşmektedir. Bu sefer de böyle oldu. Enkazdan çıkarılan, enkaz altında kalmış, evsiz kalmış yüzlerce çocuğun verisinin paylaşıldığına şahit olduk. Bu verilerin bir kısmının paylaşılması faydalı bir amaca hizmet etti, birçok çocuk ailesine kavuştu, enkaz altında kaldığı öğrenildi ve kurtarıldı.

Ayşe Xx'in daha önce çekilmiş bir fotoğrafı, "*Y apartmanında kalıyordu enkazda bulunamadı*" veya "*enkazda kurtarılmayı bekliyor*" veya "*ailesi kayıp*" yazısıyla paylaşıldığı örneği ele alalım. Veri paylaşımının amaçla sınırlılık ve bağlılık ilkesine uygun olduğunu varsayabiliriz. Peki ya enkaz altında kurtarılmayı bekleyen çocuk videoları, görselleri, enkazdan perişan halde çıkarılan çocukların görsellerini işlemekteki amaç neydi? Depremin üzerinden 21 gün geçmişken, bölgedeki çocukların yüzlerine kameraları yaklaştırarak neler hissediyorsunuz, neler yaşadınız gibi sorular sorarak paylaşımlar yapmak?

Çocuğun üstün yararı gözetilerek yapılan paylaşımlarda, veri paylaşım amacının sona ermesi durumunda verinin imha edilmesi gerektiği, bir diğer önemli noktadır. Verilerin aktarıldığı ortamlardan da verilerin imha edilmesi gerekir. Bu ortamlardaki paylaşımların bir kısmının çocukların kurtarılmasında etkilerinin olduğu yadsınamaz fakat bundan sonraki süreç için verilerin paylaşıldığı ortamlarda fotoğrafların bulanıklaştırılması yöntemleri gibi yöntemler kullanılması zarurettir. Bundan sonraki paylaşımlarda da gerek gerçek kişilerin gerek basının gerekse STK, kurum ve kuruluşların anonimleştirmeye dikkat etmesi gerekir.

Kişisel verilerin hukuka aykırı olarak elde edilmesi, yayılması ve başkasına verilmesinin aynı zamanda Türk Ceza Kanunu'nda düzenlendiği ve cezai yaptırımlarının olduğu unutulmamalıdır.

Teknolojiden yaşanan bu afet zamanında da etkin bir şekilde faydalandık. Deringörü yazılımı sayesinde 105 çocuğun ailesine

kavuşturulması büyük bir sevinç.[4] Fakat yazılımın biyometrik veri olan yüz verisini işlemesi ve biyometrik verilerin özel nitelikli veri olması sebebiyle yeterli hassasiyetin sağlanması, gerekli ve yeterli aydınlatmanın yapılması, işleme amacının sona ermesi halinde imha edilmesi gibi konularda kanuna uyulması, veri güvenliğine ilişkin yeterli önlemlerin alınmasına önem verilmesi gereklidir. Bu konuda Kişisel Verileri Koruma Kurulu'nun 2018/10 sayılı kararında özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler belirlenmiştir.[5] Bakanlığın veri işlenmesi süreçlerinde yer alan çalışanlarla veri güvenliğine ilişkin süreçleri hukuka uygun yürütmesi, verilerin muhafaza edildiği ve/veya erişildiği ortamlara göre güvenlik önlemlerini ve yetkileri belirlemesi, mümkün olduğunca aktarım yapılmaması, yapılması gerekiyorsa yapay zekâ tabanlı sistemlerin kullanılmaması ve araçların sunucularının yurtiçinde olmasına önem gösterilmesi gerekir. DerinGörü ile yüz verileri alınan çocukların ailelerine kavuşturulması, sonrasında verilerinin imha edilmesi ve bu konuda kamuoyunun bilgilendirilmesi de önem arz eder.

Çocukların mahremiyet hakkı ihlal edilmeden çocukların korunması temel prensip olmalıdır. Olağanüstü hallerin varlığı, çocukların haklarının ihlal edilebileceği anlamına gelemez.

Kaynakça

https://bilgem.tubitak.gov.tr/tr/icerik/deringoru-yuz-tanima-ve-akilli-turnike-sistemi

https://www.ulusal.com.tr/yurt/bu-uygulama-ile-1314-depremzede-cocuk-ailesine-kavustu-bakan-yanik-duyurdu-15017931

Özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler, https://www.resmigazete.gov.tr/eskiler/2018/03/20180307-7.pdf

[4] https://www.ulusal.com.tr/yurt/bu-uygulama-ile-1314-depremzede-cocuk-ailesine-kavustu-bakan-yanik-duyurdu-15017931

[5] https://www.resmigazete.gov.tr/eskiler/2018/03/20180307-7.pdf

Öncelikle, ülkemizde Kahramanmaraş il merkezli meydana gelen depremde birçok cana ve ihtiyaç sahiplerine ulaşılmasında başta Twitter olmak üzere, birçok sosyal medya uygulamasının büyük fayda sağladığını; getirilen kısıtlama ve yavaşlatmaların ise elbette birçok yanlış ve yalan bilginin paylaşılmasını engellediği gibi, doğru ve gerekli bilgilerin de yetkili birimlere ulaşmasında sorun teşkil edebileceğini görmüş olduk. Bilişimin günümüzde zararlarından çok yararlarına odaklanılmasını temenni eder; dünyamızın bu ve benzeri tüm felaketlerin tekrarını yaşamamasını dilerim. İyi okumalar.

TANIMLARI VE AÇIKLAMALARIYLA VPN NEDİR?

Açılımı **Virtual Private Network olan VPN; normal hayatımızda kullandığımız internet ağından farklı olarak, sanal özel bir ağı taklit ederek kullanım sağlamaktadır. Ağlar arasında iletişim kurmak için kullanılan dijital bir etiket olarak tanımlanan "internet protokol" *(IP)* adreslerini maskeleyerek ve verileri şifreleyerek çalışır. Böylece veriler, alma yetkisi olmayan hiç kimse tarafından okunamaz.**

VPN, internete bağlandığınız cihazı sanal olarak farklı bir konumda gösterir. Bunun için karşıdaki ağa kriptolu bir tünel açar. Aktarılan bilgiler bu tünelden karşılıklı olarak paylaşılır. Böylece VPN sayesinde bağlanılan ülkenin ağ usullerine göre internet kullanımı sağlanabilir.

Masaüstü bilgisayarlarda, laptoplarda, tablet ve telefonlarda, genellikle kurumsal çalışma ortamlarında çalışanların ofis dışındayken ve uzaktan çalışırken özel işletim sistemlerine güvenli bir şekilde erişebilmesi için ortaya çıkmış olan bu ağ, aynı zamanda kullanıcıların çevrimiçi aktivitelerini başka ülkelerdeki bilgisayarlara yönlendirerek devletlerin internet erişimine uyguladığı sansür ve kısıtlamaları aşmak için de etkili olabilmektedir.

VPN NE İÇİN KULLANILIR?

VPN hizmetlerinin temel işlevi, genellikle verileri internet üzerinden güvenle göndermek üzerine kuruludur. VPN'lerin kullanım şekilleri üç temel başlık altında sıralanabilir:

1. Gizlilik

VPN'ler, özellikle de genel Wİ-Fİ ağlarına bağlandığınızda kişisel verilerini ve bilgilerinizi gizli tutmak için şifreleme kullanır.

2. Anonimlik

IP adresiniz, konumunuz ve gezinme etkinliğiniz ile ilgili bilgiler içerir. İnternetteki tüm web siteleri, çerezleri ve benzer teknolojileri kullanarak bu verileri izler. Web siteleri, her ziyaretinizde sizi tanımlayabilir. VPN bağlantısı, IP adresinizi gizleyerek internette anonim olmanızı sağlar.

3. Güvenlik

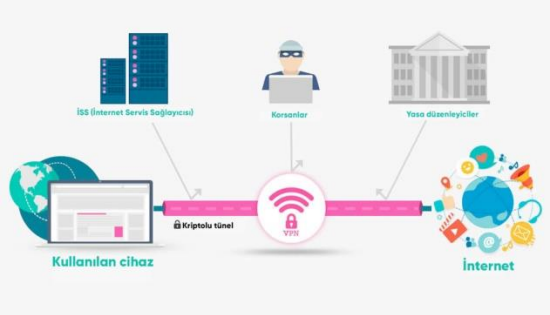
Bir VPN hizmeti, internet bağlantınızı yetkisiz erişimden korumak için şifrelemeden yararlanır. Şüpheli internet etkinliklerinin tespit edilmesi durumunda önceden seçilmiş programları sonlandıran bir kapatma mekanizması olarak da çalışır. Bu, verilerin ele geçirilme olasılığını azaltır. Bu özellikler, şirketlerin iş ağları üzerinden yetkili kullanıcılara uzaktan erişim sağlamasına olanak tanır.

PEKİ NEDEN VPN KULLANILMALI?

Kişilere ve şirketlere internet bağlantısı sağlayan kurumlar olan tanımlanan "İnternet Servis Sağlayıcıları", kısaca İSS olarak adlandırılır. Genellikle bağlantınızı internete bağladığınızda ayarlar ve IP adresi üzerinden sizi takip eder. Milyonlarca kullanıcının, dünyanın farklı bölgelerinde kullandığı internet ağ trafiği İSS'nin sunucuları üzerinden yönlendirilir ve böylece internette yaptığınız her şey kayıt altına alınıp görüntülenebilir.

Her ne kadar internet servis sağlayıcınız güvenilir gibi görünse de arama geçmişiniz, veriler; yanlış bir "tıklama" veya ilginizi çekerek girdiğiniz bir reklamın firmalarıyla, polis, hükûmet ve/veya üçüncü kişilerle paylaşılabilir. Bununla birlikte İSS'ler ayrıca siber suçluların saldırılarına maruz kalabilmekte birlikte; herhangi bir siteye kaydettiğiniz kişisel veya banka vb. bilgileriniz, kişisel ve özel verileriniz tehlikeye girebilir.

Elbette her VPN kanalı veya kullanıcısı bu özel ağı tek başına güvenliğini sağlama amacıyla kullanmamaktadır. Ancak, özellikle de düzenli olarak herkese açık Wİ-Fİ ağlarına bağlanarak internet erişimi sağlayan kullanıcıların bu ihtimalleri göz önünde bulundurmaları gerekmektedir.



VPN'LERİN GÜNÜMÜZDEKİ YAYGIN KULLANIM ALANLARI NELERDİR?

2009 yılında Tom Smith tarafından kurulan ve dünya çapındaki yayıncılara, medya ajanslarına ve pazarlamacılara hedef kitle farkındalıkları sağlayan bir kitle araştırma şirketi olan GlobalWebIndex'in verilerine göre; 2016 ile 2018 yılları arasında dünyadaki VPN kullanıcısı sayısı eskisinin dört katına çıktı. İnternet kullanımının kısıtlandığı ve internetin sansürlendiği Tayland, Endonezya ve Çin gibi ülkelerde internet kullanan her beş kişiden biri VPN kullanmaktadır. ABD, Birleşik Krallık ve

Almanya da ise VPN kullanıcısı oranı %5 gibi düşük miktarlardadır ancak bu sayı giderek artmaktadır.

Ülkemizde kayıtlarda yer alan ilk internet sansür olayı, 2007 yılında hükümetin, Türkiye'nin ilk Cumhurbaşkanı Mustafa Kemal Atatürk ile alay eden bir videonun yayınlaması sonucu Youtube'un bir süre erişime kapanması şeklinde ortaya çıkmıştır.

Türkiye'de özellikle son 7 yılda olmakla birlikte, dünya genelinde de VPN alımında en önemli etkenlerden biri, kullanıcıların coğrafi olarak kısıtlandırılmış içeriklere erişim talebindeki artış olmuştur. Örneğin, Netflix veya YouTube gibi video yayını yapan hizmetler bazı videoları sadece belirli ülkelerde izlenime açmaktadır. Bu engelleme sonucunda ise kullanıcılar, ücretsiz veya bütçelerine uygun VPN uygulamaları ile IP adreslerini şifreleyerek, başka bir ülkeden internete bağlanmış gibi görünmekte ve kısıtlanan içeriklere ulaşım sağlayabilmektedirler.

VPN KULLANIMI YASAL MIDIR?

Bu sorunun ayrıntılı cevapları ülkeden ülkeye değişiklik gösterebilmekle birlikte, basit haliyle "Evet, yasal." diyebiliriz**.**

Farklı cevaplarının olmasının sebebi ise, özgürlükler ülkesi olarak adlandırılan ABD de dahil olmak üzere, birçok Avrupa ülkesinde de VPN kullanımına izin veren veya yasaklayan açık bir kanun düzenlemesinin bulunmamasıdır. Büyük VPN sağlayıcılarının neredeyse tamamı, hizmetlerini tüm Amerikan ve Batı dünyasının büyük bir bölümündeki vatandaşlarının kullanımına açık haldedir. Ancak tüm ülkelerde maalesef durum aynı değil;

- **Rusya'nın** Temmuz 2017'de çıkardığı bir kanunla VPN kullanımını yasak hale getirdiği, **Belarus'un** VPN erişimini engellediği veya kısıtladığı biliniyor. Fakat bu yasak, kurumsal VPN'leri kapsamıyor.

- **Çin ise**, Şubat 2018'den bu yana tüm telekom firmalarının ticari VPN'lere olan erişimlerinin engellenmesini talep etti. Ülkede yalnızca hükümet tarafından sağlanan VPN hizmetleri kullanılabiliyor ve bunlar, sadece sınır ötesi işlemlerle uğraşan şirketlere sunuluyor.

- VPN'lerin yasa dışı veya kısıtlı olduğu ülkeler arasında **İran, Umman, Birleşik Arap Emirlikleri, Irak, Türkmenistan** ve **Kuzey Kore** de var.

Tüm bu uygulamalarla birlikte bizleri en çok ilgilendiren soru ise, Türkiye'de VPN kullanmamız halinde herhangi bir hukuki engelle karşılaşıp karşılaşmayacağımız şeklinde. Ülkemizde VPN'lerin kullanımını engelleyen bir hukuki düzenleme bulunmaması sebebiyle, Türkiye'de VPN kullanımının yasa dışı olmadığını kabul edebiliriz. Bununla birlikte bazı VPN hizmetlerine erişimde sorun yaşandığı

bilinmektedir. Elbette ki hukukumuz, yasalarla korunmakta olup VPN kullanılarak yapılan herhangi bir yasa dışı işlemin kabulü mümkün değildir.

Son olarak,VPN kullanımı ile ilgili özet bilgiler verdiğimiz bu yazımızda, VPN bağlantısının sadece internetteki veri trafiğinizi gizlediğini ve koruduğunu ancak sizi bilgisayar korsanlarının saldırılarından, Truva Atlarından, virüslerden veya diğer kötü amaçlı yazılımlardan koruyamadığını; bu tip saldırıların önüne geçmek için antivirüs yazılımının da kullanılması gerektiğini önemle belirtmek isteriz.

.

KAYNAKÇA

- *https://surfshark.com/tr/learn/vpn-nedir*
- *https://www.kaspersky.com.tr/resource-center/definitions/what-is-a-vpn*
- *https://aws.amazon.com/tr/what-is/vpn/#:~:text=VPN%20veya%20Sanal%20%C3%96zel%20A%C4%9F,maskeleyerek%20ve%20verileri%20%C5%9Difreleyerek%20%C3%A7al%C4%B1%C5%9F%C4%B1r.*
- *https://www.webtekno.com/vpn-nasil-kullanilir-ucretsiz-vpn-indir-h71224.html*
- *https://tr.wizcase.com/blog/vpn-servisleri-turkiyede-yasal-mi-kesin-rehber/*
- *https://www.chip.com.tr/haber/vpn-kullanmak-yasal-mi_86827.html*
- ***WİKİPEDİA; İSS, GlobalWebIndex***