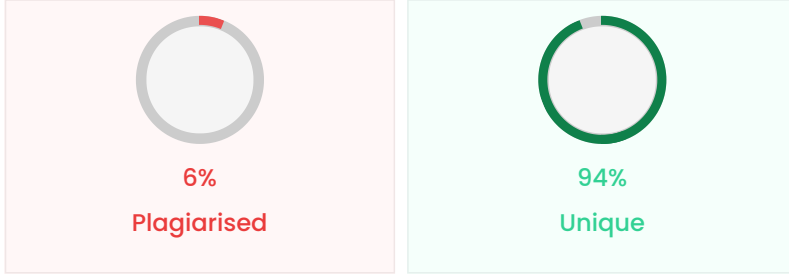


Plagiarism Scan Report



Words Statistics

Words	734
Characters	6315

Exclude URL: None

Content Checked For Plagiarism

Dijital Delillerin Hukuk Çıkamaz : İletişim Uygulamalarının Hukuki Süreçlerdeki Rolü ve Etkinliği

Günümüzde WhatsApp, Telegram, Signal, FaceTime gibi şifreli mesajlaşma ve arama uygulamalarının kullanıcı mahremiyetini koruma amacıyla başvurduğu uçtan uca şifreleme metodolojisi, iletişimin sadece gönderici ve alıcı tarafından erişilebilir olmasını temin etmekte; Böylelikle üçüncü şahısların bu iletişimi görüntülemesini engellemektedir. Ancak, bu şifreleme tekniğinin hukuki süreçlere olan etkisi, adli mekanizmalar açısından önemli zorlukları da beraberinde getirmektedir. Özellikle, soruşturma ve kovuşturma aşamalarında, delil toplama sürecinin bu teknoloji karşısındaki verimsizliği, adalete erişimde ciddi bir engel oluşturmaktadır. Uçtan uca şifreleme yöntemi, dijital iletişimin güvenliğini sağlama noktasında kritik bir rol oynar. Bu yöntemle, iletişim esnasında gönderici ile alıcı arasında aktarılan verilerin gizliliği muhafaza edilir ve sadece özel anahtar sahibi tarafından erişilebilir hale gelir. Bu özel anahtarın olmaması halinde, elde edilen veriler, anlam bütünlüğünden yoksun, çözülmesi güç bir data yığınına dönüşmektedir. Ancak, WhatsApp ve benzeri platformlar üzerinden gerçekleştirilen iletişimlerin, Türkiye'deki yargısal süreçlerde delil olarak temin edilmesi meselesi, bu platformların Türkiye ile veri paylaşımını reddetmesi ve Türkiye'de fiziki bir ofisinin bulunmaması gibi faktörler nedeniyle mümkün olmamaktadır. Bu durum, emniyet ve savcılık makamlarının söz konusu verilere erişimini engellemekte, bu da hukukun üstünlüğü ve adil yargılanma hakkının gerçekleşmesi önünde ciddi bir mani teşkil etmektedir. Şifreli mesajlaşma uygulamaları aracılığıyla gerçekleştirilen iletişimlerin, yalnızca trafiğinin tespiti mümkün olabilmektedir. Bu iletişim trafiğinin belirlenmesi, Carrier-Grade NAT (CGNAT) kayıtları üzerinden yapılabilmekle birlikte, bu kayıtların yanıltıcı ve verimsiz olabileceği önceden belirtilmiştir. Bu bağlamda, Ceza Muhakemesi Kanunu'nun ilgili maddesi, adli süreçlerde iletişimin dinlenmesi ve kaydedilmesi mekanizmalarını düzenlemektedir. Söz konusu kanun maddesi CMK m.135/1, "Bir suç bağlamında yürütülen soruşturma ve kovuşturma süreçlerinde, suçun işlendiğine dair somut delillerle desteklenen ve başka yollarla delil elde edilmesinin mümkün olmadığı durumlarda, şüpheli veya sanığın telekomünikasyon yoluyla gerçekleştirdiği iletişimin, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla

dinlenmesine, kaydedilmesine ve sinyal bilgilerinin değerlendirilmesine olanak tanımaktadır. Bu karar, Cumhuriyet savcısı tarafından hemen bir hâkime sunulmalı ve hâkim, kararını en geç yirmi dört saat içinde vermelidir. Belirtilen süre sonunda veya hâkimin aksi yönde karar vermesi halinde, alınan tedbir derhal kaldırılmalıdır." Bu düzenleme, adli makamların, belirli şartlar altında ve yasal sınırlar çerçevesinde iletişim trafiğine müdahale edebilmesine imkan sağlamaktadır. Ancak, bu denetim mekanizması sadece şebeke hattı üzerinden yapılan iletişimler için geçerlidir. Kanun koyucu, Türkiye'de iletişimin denetlenmesine ilişkin düzenlemeyi 1999 yılında 4422 sayılı kanun ile ilk kez gerçekleştirmiştir. Bu düzenleme ile iletişimin denetlenmesi, dinlenmesi ve kaydedilmesi usulleri yasal bir çerçeveye kavuşturulmuştur. Ancak, söz konusu kanunun getirdiği yetkilerin suistimal edilebileceği endişesi, toplumda güvenlik kaygılarına yol açmıştır. İletişimin denetlenmesi süreçlerinin yasal zemine oturtulması, devletin bireylerin özel hayatının gizliliğine müdahalesini düzenlerken, aynı zamanda bu yetkilerin kötüye kullanılma ihtimaline karşı endişeleri de beraberinde getirmiştir. Bu endişeler dolayısıyla bireyler özel iletişim programlarına yönelmiştir. Gemius Mobil Reytings verilerine dayanarak, Türkiye'deki en yaygın kullanılan haberleşme programı Whatsapp'ın 50 milyonu aşkın kullanıcıya sahip olduğu bilgisi paylaşılmıştır. WhatsApp, FaceTime ve benzeri uluslararası uygulamaların aksine, Türkiye'de yerli olarak geliştirilen haberleşme uygulamalarının kullanım oranı, bahsedilen verilere göre yedi kat daha azdır. Bu durumun temelinde yatan endişe, yerli iletişim uygulamalarının ve şebeke hattının görüşme içeriklerini üçüncü taraflarla paylaşma potansiyeline ve kişisel verilerin açığa çıkma riskine dairdir. Bu bağlamda, bireylerin özel hayatın gizliliğine yönelik kaygıları, onları iletişimin dinlenmesi ve kayda alınması risklerinden korunma amacıyla uluslararası platformlara yönelmeye itmektedir. Devletin, söz konusu platformlar üzerinden gerçekleştirilen haberleşmelere erişim sağlayamaması, suç faaliyetlerinin bu tür iletişim kanalları aracılığıyla organize edilmesi veya işlenmesi konusunda önemli bir sorun teşkil etmektedir. Yakın tarihte yaşadığımız en iyi örneklerden biri olan 2016 Sözde Darbe girişiminde kullanılan Bylock programının darbeden sonra tespit edilmesi ve bu program aracılığı ile yapılan konuşmaların gözden kaçması olmuştur. Ancak bireyler, günümüzde artık özel görüşmelerini şifreli haberleşme programları aracılığı ile yapmaktadır. Ancak bu şifreli haberleşme uygulamalarının yaygınlaşması ve Türkiye de ki yerli şifreli mesajlaşma uygulamalarının rağbetinin az görmesinin temel sebebi yargı ve emniyet mensuplarının bir takımı tarafından baz,hts gibi ulaştıkları verileri kişisel menfaatler doğrultusunda kullanabilme ihtimalidir. Türkiye'de faaliyet gösteren iş adamlarının müşteri bilgileri gibi hassas verilerin gizliliği, bu türden bir kötüye kullanım senaryosunda ciddi şekilde tehdit altına girebilir. Gizli bilgilerin, özellikle art niyetli emniyet veya yargı mensupları tarafından ele geçirilmesi ve bu bilgilerin kötü maksatlarla kullanılması, adalet sisteminin bütünlüğüne ve güvenilirliğine zarar verebilir. Bu, aynı zamanda FETÖ tarafından sıklıkla başvurulan bir yöntem olan, uydurma deliller üretme çabalarının da bir göstergesidir. Güvenlik ve özgürlük arasındaki bu hassas denge, yargı ve emniyet mekanizmalarının şeffaflık, hesap verebilirlik ve hukuka uygunluk ilkeleri doğrultusunda hareket etmesini gerektirir. Böylece, şifreli haberleşme teknolojilerinin hem faydalarından yararlanılabilir hem de potansiyel kötüye kullanımlarının önüne geçilebilir. Bu, bireylerin mahremiyet haklarının korunması ve adalet sistemine olan güvenin sürdürülmesi için elzemdir.

Source

13 hours ago · Ancak, bu şifreleme tekniğinin hukuki süreçlere olan etkisi,...

1.61%

13 hours ago · Ancak, bu şifreleme tekniğinin hukuki süreçlere olan etkisi, adli mekanizmalar açısından önemli zorlukları da beraberinde getirmektedir. Özellikle, soruşturma ve kovuşturma aşamalarında, delil toplama sürecinin bu teknoloji karşısındaki verimsizliği, adalete erişimde ciddi bir engel oluşturmaktadır.

<https://www.sametozdem.com/2024/02/06/dijital-delillerin-hukuki-cikmazi-iletisim-uygulamalarinin-hukuki-sureclerdeki-rolu-ve-etkinligi/>

13 hours ago · Ancak, WhatsApp ve benzeri platformlar üzerinden gerçek...

1.61%

13 hours ago · Ancak, WhatsApp ve benzeri platformlar üzerinden gerçekleştirilen iletişimlerin, Türkiye'deki yargısal süreçlerde delil olarak temin edilmesi meselesi, bu platformların Türkiye ile veri paylaşımını reddetmesi ve Türkiye'de fiziki bir

<https://www.sametozdem.com/2024/02/06/dijital-delillerin-hukuki-cikmazi-iletisim-uygulamalarinin-hukuki-sureclerdeki-rolu-ve-etkinligi/>

BİLİŞİM AĞI HİZMETLERİNİN DÜZENLENMESİ VE ...

3.23%

BİLİŞİM AĞI HİZMETLERİNİN DÜZENLENMESİ VE ...

<https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/>



[Home](#)

[Blog](#)

[Testimonials](#)

[About Us](#)

[Privacy](#)

Copyright © 2024 Plagiarism Detector. All right reserved