BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ TEZLİ
YÜKSEK LİSANS PROGRAMI

TÜRKİYE TELEKOMÜNİKASYON SEKTÖRÜNDE SAHTECİLİK SORUNU İÇİN DÜZENLEYİCİ ÖNERİLER

HAZIRLAYAN

SÜLEYMAN BAYRAM

YÜKSEK LİSANS TEZİ

TEZ DANIŞMANI

DR. ÖĞR. ÜYESİ ESMA ERGÜNER ÖZKOÇ

ANKARA - 2022

BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

Tarih: 16 / 12 / 2021

Öğrencinin Adı, Soyadı: Süleyman BAYRAM

Öğrencinin Numarası: 21920276

Anabilim Dalı: Yönetim Bilişim Sistemleri

Programı: Yönetim Bilişim Sistemleri Tezli Yüksek Lisans

Danışmanın Unvanı/Adı, Soyadı: Dr. Öğr. Üyesi Esma ERGÜNER ÖZKOÇ

Tez Başlığı: Türkiye Telekomünikasyon Sektöründe Sahtecilik Sorunu İçin Düzenleyici Öneriler

Yukarıda başlığı belirtilen Yüksek Lisans tez çalışmamın; Giriş, Ana Bölümler ve Sonuç Bölümünden oluşan, toplam 84 sayfalık kısmına ilişkin, 08/12/2021 tarihinde tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı %3'tür. Uygulanan filtrelemeler:

1. Kaynakça hariç
2. Alıntılar hariç
3. Beş (5) kelimeden daha az örtüşme içeren metin kısımları hariç

"Başkent Üniversitesi Enstitüleri Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Usul ve Esaslarını" inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Öğrenci İmzası:

ONAY

Tarih: 16 / 12 / 2021

Öğrenci Danışmanı Unvan, Ad, Soyad, İmza:

Dr. Öğr. Üyesi Esma ERGÜNER ÖZKOÇ

TEŞEKKÜR

Çalışmam boyunca değerli yardım ve katkılarıyla beni yönlendiren danışmanım Sayın Esma ERGÜNER ÖZKOÇ'a, her türlü desteği hiçbir zaman esirgemeyen kıymetli arkadaşım Furkan ŞAVŞATLI'ya, çalışmam boyunca yol arkadaşlığı yaptığımız değerli arkadaşım Gürkan GEBİÇ'e, manevi destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli eşim Elif'e, oğlum Ilgar'a ve aileme teşekkürü bir borç bilirim.

ÖZET

Süleyman BAYRAM, Türkiye Telekomünikasyon Sektöründe Sahtecilik Sorunu İçin Düzenleyici Öneriler, Başkent Üniversitesi, Sosyal Bilimler Enstitüsü, Yönetim Bilişim Sistemleri Tezli Yüksek Lisans Programı, 2022.

Sahtecilik, insanlığın var oluşu ile birlikte sürekli yaşanan bir olgu olarak karşımıza çıkmaktadır. Günümüzde teknolojik anlamda pek çok alanda önemli gelişmeler yaşanmaktadır. Sahtecilik de bu gelişmeleri takip etmekte ve günden güne değişen ve gelişen şekillerde devam etmektedir. Özellikle telekomünikasyon sektöründe 2000'li yılların başlarından itibaren mobil teknolojilerin de gelişimiyle birlikte önemli dönüşümler yaşanmıştır. Telekomünikasyon sahteciliğinin de bu dönemde önemli oranda arttığı, çok ciddi gelir ve itibar kayıplarına yol açtığı gözlemlenmektedir. Bu bağlamda tüm sektörlerde olduğu gibi telekomünikasyon sektöründe de sahtecilikle mücadele ve sahteciliği önlenmesi önemli bir faaliyet olarak görülmektedir.

Bu çalışma kapsamında, sahteciliğe ilişkin yaklaşımlar ve telekomünikasyon sahteciliği özelinde konu detaylı şekilde ele alınmıştır. Dünyada telekomünikasyon sahteciliği konusunda yaşananlar ve sahteciliğin azaltılması ve önlenmesi kapsamında gerçekleştirilen faaliyetler incelenmiştir. Türkiye'de faaliyet göstermekte olan iki mobil operatör ile odak grup çalışması gerçekleştirilerek ülkemizdeki telekomünikasyon sahteciliğine ilişkin sektörün mevcut durumu ve beklentileri öğrenilmiştir. Edinilen tüm bu bilgiler ve yapılan tüm çalışmaların değerlendirilmesi neticesinde çalışmanın sonucunda Türkiye telekomünikasyon sektöründe sahteciliğin azaltılması ve önlenebilmesi amacıyla çeşitli düzenleyici öneriler sunulmuştur.

Anahtar Kelimeler: Sahtecilik, Telekomünikasyon, Düzenleme, CLI Manipülasyonu

ABSTRACT

Süleyman BAYRAM, Regulatory Recommendations for Fraud Problem in Turkish Telecommunication Sector, Başkent University, Institute of Social Science, Master's of Management Information Systems with Thesis, 2022.

Fraud emerges as a phenomenon that is constantly experienced with the existence of humanity. Nowadays, there are important developments in many areas in terms of technology. Fraud also follows these developments and continues in ways that change and develop day by day. Especially in the telecommunication sector, since the beginning of the 2000s, important transformations have been experienced with the development of mobile technologies. It is observed that telecommunication fraud also increased significantly in this period, causing serious income and reputation losses. In this context, as in all sectors, combating and preventing fraud is seen as an important activity in the telecommunication sector.

Within the scope of this study, approaches to fraud and in particular telecommunication fraud are discussed in detail. Experiences in telecommunication fraud and activities carried out within the scope of reducing and preventing fraud in the world have been examined. A focus group study was conducted with two mobile operators in Turkey and the current situation and expectations of the sector regarding telecommunications fraud in our country were discovered. As a result of the evaluation of all this information obtained and all the studies carried out, various regulatory proposals were presented in order to reduce and prevent fraud in the Turkish telecommunication sector.

Keywords: Fraud, Telecommunication, Regulation, CLI Spoofing

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ACFE	Sertifikalı Sahtecilik Denetleyicileri Birliği (Association of Certified Fraud Examiners)
BEREC	Elektronik Haberleşme için Avrupa Düzenleyiciler Kurumu (The Body of European Regulators for Electronic Communications)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CDR	Çağrı Detay Kaydı (Call Detail Records)
CEPT	Avrupa Posta ve Telekomünikasyon İdareleri Konferansı (The European Conference of Postal and Telecommunications Administrations)
CFCA	İletişim Sahteciliği Kontrol Birliği (Communications Fraud Control Association)
CLI	Arayan Hat Bilgisi (Calling Line Identity)
DLT	Dağıtılmış Defter Teknolojisi (Distributed Ledger Technology)
ECC	Elektronik Haberleşme Komitesi (Electronic Communications Committee)
GLF	Global Liderler Forumu (Global Leaders Forum)
HTTP	Hiper Metin Transfer Protokolü (Hyper Text Transfer Protocol)
IP	İnternet Protokolü (Internet Protocol)
IRSF	Uluslararası Gelir Paylaşım Sahteciliği (International Revenue Share Fraud)
ISDN	Bütünleştirilmiş Sayısal Şebeke Hizmetleri (Integrated Services Digital Network)
ITU	Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)
M2M	Makineler Arası İletişim (Machine-to-Machine)
PBX	Özel Telefon Santrali (Private Branch Exchange)
PSTN	Genel Aktarmalı Telefon Şebekesi (Public Switched Telephone Network)

SHAKEN	Belirteçler Kullanılarak İddia Edilen Bilgilerin İmzaya Dayalı Olarak İşlenmesi (Signature-Based Handling of Asserted Information Using Tokens)
SMS	Kısa Mesaj Servisi (Short Message Service)
SOLID	Sosyal Bağlantılı Veri (Social Linked Data)
STIR	Güvenli Telefon Kimliği Gözden Geçirilmesi (Secure Telephony Identity Revisited)
STH	Sabit Telefon Hizmeti
VoIP	İnternet Protokolü Üzerinden Ses İletimi (Voice over Internet Protocol)

1. GİRİŞ

Latince aldatma eğilimi anlamındaki "fraudem" kelimesinden gelmekte olan fraud (Tezin bundan sonraki kısımlarında "sahtecilik" olarak kullanılacaktır.) Concise Oxford Sözlüğüne göre adil olmayan kişisel kazanç için yanlış temsiller kullanan kriminal aldatma olarak tanımlanmaktadır (Bolton ve Hand, 2002; Becker vd., 2010). Sahteciliği açık veya gizli aldatma yoluyla finansal avantaj elde etmeye veya bir tarafa zarar vermeye yol açan faaliyet olarak da tanımlamak mümkündür (Rebahi vd., 2013). Sahtecilik insanlığın var oluşundan itibaren hep yaşanagelen bir olgu olarak karşımıza çıkmaktadır. Günlük hayatta pek çok alanda karşımıza çıkan bu olgu, teknolojinin gelişimiyle birlikte birçok alanda yeni teknik ve formlar kazanarak kendi serüvenine devam etmektedir (Alraouji ve Bramantoro, 2014). Genellikle finansal kazanç elde etmek için gerçekleştirilen sahtecilik, bazen de kişisel edinimler, siyasi nedenler veya başka nedenlerle de yapılabilmektedir (Becker vd., 2010). Yıllar içinde telekomünikasyon, finans, sağlık, akademik süreçler vb. birçok alanda çeşitli sahtecilik yöntemleri geliştirilmiş olsa da bunların çoğunun temeldeki ortak noktaları, masum bir tarafa karşı meşru bir girişim gibi göstererek sahtekâr şekilde bir girişimde bulunmaktır (Fanning vd., 1995; Bell ve Carcello, 2000; Lin vd., 2003; Brown, 2005; Pironet vd., 2009; Błaszczyński vd., 2020; ACFE, 2020;).

Sahteciliğin pek çok hedefi, yöntemi ve tekniği bulunmaktadır. Bunlardan her biri için çeşitli çalışmalar ve araştırmalar yapılmaktadır. Bu çalışma kapsamında telekomünikasyon sahteciliği sorunu araştırılarak Türkiye açısından çeşitli değerlendirme ve önerilere yer verilecektir. Telekomünikasyon sahteciliği 1950'li yıllardan itibaren görülmekte şebekeleri, kullanıcıları, şirketleri ve diğer paydaşları da zaman zaman hedef almaktadır. İlk dönemlerde analog şebekelerde bulunan güvenlik açıkları hedef alınmaktayken zaman içerisinde gelişen sayısal teknolojiler ile birlikte sahtecilik de değişmiş ve gelişmiştir. Özellikle 90'lı ve 2000'li yıllardan itibaren mobil ve hücresel şebekelerde yaşanan önemli değişim ve gelişimler sonrası sahtecilik yöntemleri ve girişimleri de önemli ölçüde artmıştır (Becker vd., 2010; Pourhabibi vd., 2020).

Sahtecilik hem sabit hem de mobil telekomünikasyon şebekelerinde yoğun şekilde uygulanmaktadır. Mobil tarafta genellikle ön ödemeli veya faturalı kullanıcılara yönelik

sahtecilik yöntemleri uygulanmakta iken sabit tarafta ise genellikle operatörlere yönelik yöntemler uygulanmaktadır. Bununla birlikte, her iki tarafta da temel amaç çağrıları ve servisleri illegal şekilde ele geçirmek ve bu sayede kazanç elde etmektir (Perols, 2011; Abdallah vd., 2016). Sahtecilik dolayısıyla telekomünikasyon operatörlerinin yıllık kazancının yaklaşık %5'i kaybolmakta ve bu oran her geçen yıl artış göstermektedir (Rebahi vd., 2013). 2019 yılında dünya çapında telekomünikasyon sektöründe yaşanan sahtecilik vakaları nedeniyle yaklaşık 28,3 milyar dolar gelir kaybı olduğu ölçülmüştür (CFCA, 2019). Sahtecilik ile sadece gelir kaybı değil, müşteri memnuniyetsizliği ve kayıpları, itibar kayıpları ve çeşitli başka kayıplar da yaşanabilmektedir. Sahteciliğin bu yönleriyle sadece operatörleri değil doğrudan kullanıcıları da hedef almakta olduğu ve telekomünikasyon sektöründeki kullanıcı sayılarının yüksek oluşu da dikkate alındığında sahtecilik açısından en önemli ve önlem alınması gerek sektörlerden birinin telekomünikasyon sektörü olduğu değerlendirilmektedir (Brown, 2005; Alraouji ve Bramantoro, 2014; Weiss, 2014; Abdallah vd., 2016).

Telekomünikasyon sahteciliği tüm dünyada olduğu gibi Türkiye'de de yaşanmakta ve çeşitli kayıplara neden olmaktadır. Türkiye'de telekomünikasyon sahteciliğinin boyutlarını daha iyi anlamak açısından sektörün durumuna bakmakta fayda olduğu düşünülmektedir. Türkiye telekomünikasyon sektörünün en önemli aktörleri ve sektörün büyük paydaşları olarak karşımıza mobil işletmeciler (tezin bundan sonraki kısımlarında "işletmeci" yerine "operatör" ifadesi kullanılacaktır) çıkmaktadır. Mobil operatörlerin toplam abone sayısı yaklaşık 85 milyon ve yıllık net satış gelirleri toplamı yaklaşık olarak 50 milyar TL civarındadır (BTK, 2021). Ayrıca, pazar payları çok büyük olmamakla birlikte Sabit Telefon Hizmeti (STH) operatörleri de çağrı trafiğinde önemli roller oynamakta ve sektörün önemli paydaşları olarak karşımıza çıkmaktadır. Türkiye'de telekomünikasyon sektörünün düzenleyici ve denetleyici kurumu olan Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yetkilendirilmiş ve hâlihazırda faaliyet göstermekte olan 3 adet mobil operatör ve 141 adet de STH operatörü bulunmaktadır. Çağrı trafiği anlamında ise mobil kaynaklı çağrılar tüm çağrı trafiğinin yaklaşık %98'ine tekabül etmektedir (BTK, 2021). BTK tarafından yetkilendirilmiş başka operatörler ve yetkilendirme türleri bulunmakla birlikte, sektörde sahtecilik konusunda yaşanan ve BTK'ya en yoğun şekilde iletilen şikâyetler ses çağrı trafiğinde yaşandığı için bu çalışmada mobil ve STH operatörlerine ilişkin sahtecilik konularına odaklanılacaktır.

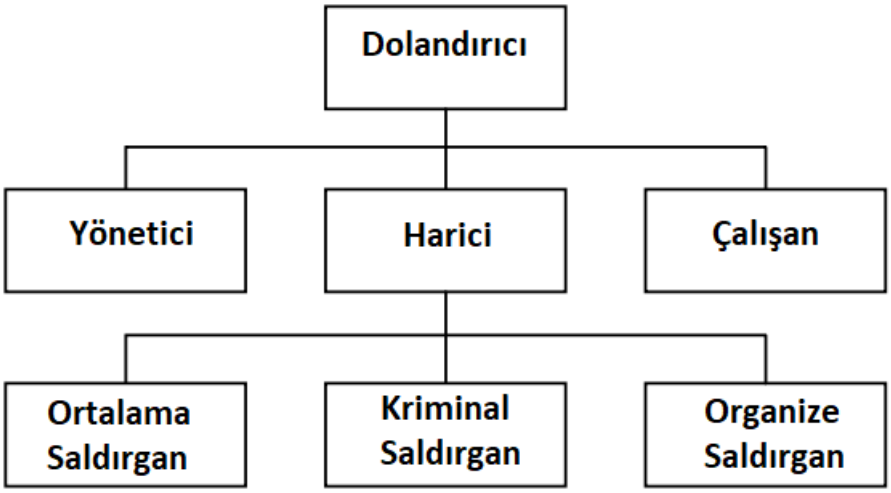
Bu tez çalışması kapsamında, öncelikle sahtecilik ve sonrasında ise telekomünikasyon sahteciliği konularında literatür araştırması yapılacaktır. Türkiye ve dünyada yaşanan telekomünikasyon sahtecilik sorunları ele alınarak olası tedbirlerden bahsedilecektir. Üçüncü bölümde, Türkiye'de faaliyet gösteren ve toplam pazar payları toplamı yaklaşık %70 olan iki mobil operatör ile odak grup şeklinde gerçekleştirilen yarı yapılandırılmış görüşmelere ve bunların detay ve analizlerine yer verilmiştir. Bir sonraki bölümde ise, dünyada bu sorun için yapılanlar ve önerilen çözümler ile Türkiye'deki operatörler ile gerçekleştirilen görüşmeler birlikte değerlendirilerek ülkemizde telekomünikasyon sahteciliği sorununa karşı alınabilecek önlemler ve yapılabilecek düzenlemeler için öneriler sunulmuştur.

2. LİTERATÜR ARAŞTIRMASI

2.1. Genel Sahtecilik Yaklaşımı

Sahtecilik faaliyetlerinin birden çok tanımı bulunmaktadır. ACFE (Sertifikalı Sahtecilik Denetleyicileri Birliği - Association of Certified Fraud Examiners; sahtecilik karşıtı uygulama ve eğitimler sunan, dünyanın en büyük sahtecilik karşıtı organizasyonlarından birisidir) tarafından, işveren kuruluşun kaynaklarının veya varlıklarının bilerek kötüye kullanılması sayesinde kişinin mesleğinin kişisel zenginleşme için kullanılması olarak tanımlanmıştır (ACFE, 2002). Bir başka tanıma göre, doğrudan yasal sonuçlara yol açmadan bir kâr kuruluşunun sisteminin kötüye kullanılması anlamına gelmekte ve rekabetçi bir ortamda, sahtecilik çok yaygınsa ve önleme prosedürleri soruna karşı yeterince güvenli değilse, bu durum kritik bir sorun haline gelebilmektedir (Phua vd., 2005).

Sahteciliği dâhili ve harici olarak iki türe ayırmak da mümkündür. Dâhili sahtecilik, bir çalışan şirketine karşı bir girişim yaptığında meydana gelir, çalışanın yetkisine göre de düşük veya yüksek seviyeli olarak tanımlanabilir (Green ve Choi, 1997; Beneish, 1997; Summers ve Sweeney, 1997; Phua vd., 2005). Harici sahtecilik ise müşterileri, üreticileri, üçüncü taraf hırsızları ve daha birçok tarafı içerebilen daha geniş bir yelpazede olabilmektedir (S. Chen ve Gangopadhyay, 2013). Bunun yanında, daha riskli harici sahtecilik unsurları ise, bireysel suçlular ve/veya organize suçlular olabilmektedir. Örneğin dâhili ve sigorta sahteciliğinin genellikle ortalama saldırganlar tarafından yapılması ve kredi kartı veya telekomünikasyon sahteciliğinin ise, profesyonel ve organize saldırganlar tarafından gerçekleştirilmesi daha olasıdır. Milyonlarca harici tarafla etkileşimi olan birçok şirket için, harici tarafların çoğunun kimliklerini ve etkinliklerini kontrol edebilmek hem maliyet olarak hem de teknik açıdan oldukça zor bir durumdur (Phua vd., 2005). Dâhili ve harici sahtecilik unsurlarının hiyerarşik durumuna Şekil 2.1'de yer verilmektedir.



Kaynak: (Phua vd., 2005)

Şekil 2.1 Dâhili ve harici sahtecilik unsurlarının hiyerarşik durumu

Sahteciliğin altında yatan temel motivasyon, yasadışı yollarla haksız kazanç elde etmek olduğundan bunun ekonomik, hukuki ve ahlaki değerler üzerinde de ciddi bir etkisi bulunmaktadır (Alexopoulos vd., 2007). Yirminci yüzyılda, işlem ve etkileşim gerektiren sektörlerde sahtecilik oldukça artmıştır. Telekomünikasyon şebekeleri, mobil iletişim, bankacılık, e ticaret vb. birçok teknolojik sistemde sahtecilik faaliyetleri önemli ölçüde artış göstermekte ve iş hayatında önemli kayıplara yol açmaktadır. Sahtecilik kapsamında bazen bir yöntem sadece araç olarak kullanılabilmekte esas hedef ise farklı bir sektör olabilmektedir. Yani birbirine girift şekilde sahtecilik vakaları da yaşanabilmektedir. Örneğin kredi kartı veya bankacılık sahteciliği gerçekleştirmek isteyen sahtekârlar, ilgili kişiye kısa mesaj gönderebilir veya arama yapabilirler. Bu durumda, telekomünikasyon araçları kullanılmış olduğundan burada hem telekomünikasyon sahteciliği hem de bankacılık sahteciliği bulunmakta olduğu söylenebilmektedir (Becker vd., 2010).

Sahteciliğin ilk dönemlerinde dolandırıcılar şirketlere milyarlarca dolarlık zarar verecek düzeye kadar ulaşmıştır. Zaman ilerledikçe şirketler sahtecilik ile mücadele için pek çok yöntem denemiş ve bunlarda kısmen başarılı da olabilmişlerdir. Dolandırıcılar ve etkilenen şirketler arasında günümüze kadar devam eden öne geçme savaşı da bu yolla başlamış ve ilerlemiştir (Becker vd., 2010).

Sahteciliği tespit etmek, önlemek ve engellemek için sahtecilik tespit ve sahtecilik yönetim sistemleri karşımıza çıkmaktadır (Kou vd., 2004). Sahteciliği önleme, sahteciliği, gerçekleştiği ilk aşamada durdurmayı tanımlamakta olduğundan bunun gerçek hayatta yüzde yüz şekilde başarılması pek mümkün değildir (Bolton ve Hand, 2002). Sahtecilik tespiti ise, sahtecilik önlemenin başarısız olduğu durumlarda, gerçekleşir gerçekleşmez sahteciliğin belirlenmesi ve tanımlanması olarak düşünülebilir. Sahtecilik tespitini anlık bir durum olarak değil sürekli gelişen ve devam eden bir süreç olarak düşünmek önem arz etmektedir. Çünkü bir yöntem tespit edilince karşı taraf başka bir yöntem geliştirecek ve bu döngü böylece devam edecektir (Cortes vd., 2001; Bolton ve Hand, 2002). Sahtecilik tespitinin temel amacı doğru tahmini maksimize etmek ve yanlış tahmini sürdürülebilir seviyede tutmaktır (SAS, 1996; Kou vd., 2004).

2.2. Telekomünikasyon Sahtecilik Yaklaşımı

Analog telekomünikasyon şebekeleri ilk kullanılmaya başlandığında çeşitli güvenlik ve şifreleme açıklıkları bulunmaktaydı ve bunlar sosyal mühendislik vb. basit sahtecilik yöntemlerine yol açmaktaydı. Örneğin erken dönemlerin ünlü dolandırıcılarından olan Joe Engressia, 1957 yılında dolandırıcılık dünyasına girdiğinde telekomünikasyon sahteciliği için yeni bir dönemi ve kültürü ortaya çıkarmış ve belirli frekanslarda ıslık çaldığında, otomatik çağrı yönlendirmelerini kontrol edebildiğini fark etmiştir. Engressia ile başlayan bu süreçte başka dolandırıcılar da benzer bilgileri kullanarak telefon sistemlerine sızmak için cihazlar oluşturmuş ve maliyeti tamamen operatörlere yükleyerek kullanıcılar için ücretsiz hizmet sağlayabilmişlerdir (Becker vd., 2010). Daha sonrasında analog teknolojiler yerini sayısal teknolojilere bırakmış ve bu değişimle birlikte sahteciliğin de doğası değişmek durumunda kalmıştır (Pourhabibi vd., 2020). Büyük telekomünikasyon şirketlerinin şebekeleri PBX (Özel Telefon Santrali - Private Branch Exchange; bir organizasyonun içindeki dâhili görüşmeleri ve organizasyonun dış dünya ile harici görüşmelerini anahtarlayan ve yönlendiren sistemlerdir (Karel, 2021)), hücresel iletişim ve sanal özel ağlar gibi sahtecilik senaryolarına karşı korunması gereken yeni teknolojilere kavuşmuştur. Bu değişimle birlikte pek çok sahtecilik yöntemi de ortaya çıkmış ve telekomünikasyon endüstrisi için ciddi gelir kayıpları yaşanmaya başlamıştır. Bu da yukarıda da bahsedildiği üzere telekomünikasyon sektöründe de sahtecilik tespit ve önleme yöntem ve sistemlerini vazgeçilmez kılmıştır (Rosset vd., 1999; Gossett ve Hyland, 1999; Galeotti vd., 2020).

Telekomünikasyon şebekelerinin tasarımları gereği çok güvenli olmaması, bir başka ifadeyle bu şebekelerin her zaman operatör ve ekosistemdeki diğer oyuncular arasındaki ilişkilere bağlı olması sahtecilik senaryolarına da zemin hazırlamaktadır (TRI, 2021). Telekomünikasyondaki en temel sahtecilik, telefon kullanımı için ücret ödememektir. Ancak bu niyette olan kişiler ile normal bir kullanıcı arasındaki farkı tam olarak belirleyebilmek de oldukça zordur. Her sahtecilik yöntemini tespit etmek ve engellemek için kendine özgü yöntemler kullanmak gerekebilmektedir. Pek çok sahtecilik yöntemi bulunmakla birlikte bunlardan bazıları da birkaç yöntemin bir araya gelişiyle oluşan sofistike yöntemlerdir. Teknoloji statik olmadığı için dolayı sahtecilik yöntemleri de statik kalmamakta ve formunu değiştirmektedir ve sektörün doğası gereği potansiyel olarak milyonlarca kişiyi etkileyebilecek düzeye gelebilmektedir (Becker vd., 2010; Kabari vd., 2015).

Pek çok sahtecilik yöntem ve senaryosundan bahsetmek mümkün olsa da telekomünikasyon sahteciliği 4 kategoride gruplanabilmektedir. Sözleşmesel (contractual) sahtecilik; ücret ödemeden hizmetlerden faydalanmayı amaçlamakta, korsan (hacking) sahtecilik; telekomünikasyon şebeke ve servislerinin illegal şekilde ele geçirilmesini amaçlamakta, teknik (technical) sahtecilik; mobil sistem teknolojilerindeki zayıflıklardan yararlanmayı amaçlamakta ve yüksek teknik kapasite gerektirmekte ve prosedürel (procedural) sahtecilik; sahtecilik risklerine karşı sistemlerde uygulanan prosedürlere karşı illegal girişim yapmayı amaçlamaktadır (Gossett ve Hyland, 1999; Sahin, 2017). Bir diğer yaklaşımda ise, telekomünikasyon sahteciliğinin çok karmaşık ve operatör yapısına göre değişken olduğu ve bu nedenle sahtecilik fenomeninin 3M yaklaşımı ile sınıflandırılabileceği belirtilmiştir: Motivasyon (motive), sahteciliğin arkasındaki gerçek nedeni (gelir elde etmek veya etmemek), Araç (means), motivasyonu yerine getirmek için kullanılan sahteciliğin doğası ve formunu ve Metod (methods), sahteciliği uygulamak için kullanılan yöntemleri temsil etmektedir (Cortesão vd., 2005; Abdallah vd., 2016). Telekomünikasyon sahteciliğinin neden sonuç ilişkileri üzerinden ele alarak sınıflandıran ve analizi bu katmanlar üzerinden yapan bir başka çalışma da bulunmaktadır. Buna göre sahtecilik, bir teknik kullanarak yasal olmayan fayda sağlamak olarak tanımlanmakta ve bu teknikler sistemdeki kök nedenlerden kaynaklanan zayıflıklar nedeniyle mümkün olabilmektedir. Bu tanım çerçevesinde bazı kavramlar telekomünikasyon sahteciliğini anlama noktasında birbirlerine bağlı olan önemli özellikler olarak görülmektedir (Sahin, 2017). Kök neden; telekomünikasyon şebekelerinin, standartlarının ve ekosisteminin

zayıflığa neden olabilecek doğal bir özelliğidir. Bunlara örnek olarak; eski sistemlerin güvenlik mantığıyla ele alınmamış olması ve güncellemenin oldukça maliyetli olacak olması, arabağlantı teknolojilerinin ve sistemlerinin genellikle belirsiz ve birbirine bağlı sistemler olması nedeniyle, tüm paydaşların sahteciliğe karşı aynı düzeyde olmaması (Johnson, 2012) ve sektörün liberalleşmesi ile çok fazla sayıda ve çeşitli ölçeklerde operatörün markette bulunması verilebilir. Zayıflık; istenmeyen yollarla manipüle edilebilecek zafiyet veya sistem özelliğidir. Zayıflık 4 kategoride incelenebilmektedir. Bunlar, protokoller (Pastor vd., 2015) ve şebekeler (Langlois, 2012), düzenlemeler, faturalama (Johnson, 2012) ve insan kaynaklı (Collier ve Endler, 2013) faktörlerdir. Teknik; bir telefon sistemindeki zayıflığı kötüye kullanmak ve bu yolla sahtecilik gerçekleştirmek için kullanılan yasal veya yasal olmayan mekanizmalardır. Operatörler düzeyindeki sahtecilik tekniklerine numara aralığını ele geçirme (Vervier vd., 2015), çağrı yönlendirme manipülasyonu, çağrı sinyalleşmesinin manipülasyonu ve fiyatlandırma karışıklığı örnek verilebilir. Bunun dışında sanal trafik oluşturma (TransNexus, 2013), birden fazla eşzamanlı arama (TransNexus, 2015), katma değerli hizmet numaraları (I3Forum, 2014), VoIP (İnternet Protokolü Üzerinden Ses İletimi - Voice over Internet Protocol) atakları (Keromytis, 2012), CLI (Arayan Hat Bilgisi – Calling Line Identity) manipülasyonu (Mustafa vd., 2014), Simbox (Reaves vd., 2015), IRSF (International Revenue Share Fraud) (Sahin ve Francillon, 2021) ve sosyal mühendislik (Collier ve Endler, 2013; Castillo, 2017) gibi birçok teknik de bulunmaktadır. Sahtecilik şemaları; bir sistemi kötüye kullanmak için teknikleri kullanarak, yasal olmayan şekilde menfaat elde etmek için kullanılan yöntemlerdir. Fayda ise; maddi veya yarışma avantajı, saygı, düzenlemeleri aşmak gibi hususları elde etmek için sahtecilik şemalarından elde edilmektedir (Tu vd., 2016; Sahin, 2017).

Bu sınıflandırmalar genel yaklaşımı ele almakta olup telekomünikasyon endüstrisinde bu sınıflandırmaların altına giren 200'den fazla sahtecilik çeşidi bulunmaktadır. Bunlardan en önemlileri; abonelik (subscription), birleştirilmiş (superimposed), özel tarifeli sistem (Premium rate), dolaşım (roaming) ve Simbox sahteciliği olarak sıralanabilmektedir (Cortesão vd., 2005; Kuşaksızoğlu, 2006; Farvaresh ve Sepehri, 2011; Mohd Yusoff vd., 2013; Abdallah vd., 2016).

Avrupa Posta ve Telekomünikasyon İdareleri Konferansı (CEPT) ülkeleri arasında telekomünikasyon sahteciliği önemli bir sorun olarak görülmektedir. CEPT'e bağlı olarak faaliyetlerini yürüten Elektronik Haberleşme Komitesi (ECC), E.164 (Uluslararası bir numaralandırma standardı) numaralarının elektronik haberleşme hizmetlerinde uluslararası sahtecilik amacıyla kötüye kullanımına yönelik kapsamlı bir rapor yayımlamıştır. Pek çok yöntemi olduğundan daha önce bahsedilen sahtecilik için CEPT ülkeleri bünyesinde bir analiz yapıldığında en çok karşılaşılan yöntemler şunlardır (ECC, 2018);

- CLI Manipülasyonu (CLI Spoofing); CLI çağrılarda yer alan arayan tarafın numara bilgisidir. Bu manipülasyon da arayan tarafın, aranan tarafa çağrının başka bir kişiden/numaradan geldiğini düşündürtecek şekilde CLI'da manipülasyon yapması olarak tanımlanmaktadır.
- Trafiğin santralde manipüle edilmesi; Sahtekârlar tarafından çağrının A numarasının (çağrının başladığı numara) değiştirilmesi ve manipüle etmesi yolu ile gerçekleştirilmektedir.
- Wangiri çağrıları; Kısaca çaldır kapat yöntemi olarak bilinmektedir. Bu yöntemle, çağrı bırakılan tarafın geri araması sağlanarak yüksek trafik miktarı elde edilmekte ve önemli miktarda sonlandırma ücretleri elde edilmektedir. Özellikle yüksek sonlandırma ücretleri olan katma değerli hizmet numaralarına doğru yapılan çağrılarda aboneler de mağdur olabilmektedir.
- PBX hesapların ele geçirilmesi; Sahtekârların abonelerin telefon hesaplarını veya şirketlerin PBX'lerini ele geçirerek yüksek tarifeli hatlara doğru suni trafik oluşturması ile gerçekleştirilmektedir.
- Roaming (uluslararası dolaşım) sahteciliği; Sim kutuları (Simbox) veya başka cihazlar vasıtasıyla, yurt dışında dolaşımda olan abonelerin sim kartları ele geçirilerek yüksek tarifeli numaralara doğru suni trafik oluşturulması olarak bilinmektedir.
- Çağrı ele geçirme (hijacking); Çağrıyı transit olarak teslim alan operatörün çağrıyı kendi şebekesinde sonlandırması olarak bilinmektedir.
- Abonelik sahteciliği; Sahte veya çalıntı kimlik bilgileri ile abone olarak herhangi bir ücret olmadan hizmet almayı amaçlamaktadır. Genellikle bayiler aracılığıyla yapılan işlemlerde karşılaşıldığı için zaman zaman bayi sahteciliği olarak da adlandırılmaktadır.

Yukarıda yer verilen sahtecilik türlerinden CLI manipülasyonu ile, özellikle ülkemizde de çok ciddi şekilde karşılaşılmakta ve ciddi sorunlara ve gelir kayıplarına neden olabilmektedir. Temel olarak, yüksek seviyedeki sonlandırma ücretlerinden kaçınmak için CLI'da manipülasyon yapılarak çağrının orijini farklı olarak gösterilmektedir. Bu sayede çok daha düşük sonlandırma ücretleri ödenebilmektedir. Tabi bu durum pek çok operatör için önemli gelir kayıplarına neden olmaktadır. Amerika Birleşik Devletleri (ABD) ve Avrupa'daki düzenleyici kurumlarca bu konuya yönelik pek çok düzenleme bulunmakta ve çeşitli yaptırımlar uygulanmaktadır. Bu düzenlemeler ülkeden ülkeye önemli ölçüde farklılıklar içerdiği için uluslararası trafik anlamında bu farklı çözümlerin birlikte çalışabilirliği de önemli bir zorluk içermektedir. Bu konuda özellikle uluslararası anlamda tüm paydaşların işbirliği son derece önem arz etmektedir (I3Forum, 2020).

Telekomünikasyon sahteciliğini tam anlamıyla anlayabilmek oldukça zor bir husustur. Şöyle ki, birinin bu sahteciliği tam anlayabilmesi için telekomünikasyon ekosistemine, tarihine, teknolojilerine, düzenlemelerine ve uluslararası anlaşmalara da tam anlamıyla hâkim olması gerekmektedir. Sektördeki aktörlerden, operatörler, üçüncü taraf servis sağlayıcıları, müşteriler, çalışanlar ve herhangi bir diğer taraf tarafından sahtecilik gerçekleştirilebilmektedir. Sahteciliği anlama noktasındaki zorluklardan bazıları; ekosistem çeşitliliği, tutarsız terminoloji, kısıtlı erişim, eksik bakış açısı ve bilgi eksikliği olarak sıralanabilmektedir (Sahin, 2017).

Yukarıda da bahsedildiği üzere telekomünikasyon sahteciliğinin pek çok türü ve yönü bulunmaktadır. Bununla birlikte, hem yurt dışında hem de Türkiye'de öne çıkan farklı farklı başlıklar ve konular bulunmakta olup Türkiye'de ve dünyada sahtecilik sorunu başlıkları altında bu husus daha detaylı şekilde açıklanacaktır. Teknoloji geliştikçe telekomünikasyon sahteciliği ve kötüye kullanımı giderek daha fazla sorun haline gelmektedir. IP (İnternet Protokolü) tabanlı ağların, VoIP hizmetlerinin ve akıllı son kullanıcı cihazlarının yaygınlaşması, birçok temel konuyu ağların kontrolünden çıkararak son kullanıcıların çok daha fazla erişim ve kontrol sahibi olmalarına neden olmuştur. Bu durum, uygulamalara ve hizmetlere seçim ve erişim açısından son kullanıcıların büyük çoğunluğu için memnuniyetle karşılanan bir gelişme olmakla birlikte, sahteciliği çok daha kolay hale getirmesi nedeniyle artık küresel bir sorun haline gelmiştir (ECC, 2018; ECC, 2022).

Bu dönüşüm ile, daha sofistike son kullanıcı cihazları ve uygulamaları ortaya çıktığından, son kullanıcıların ülkemizde ve dünyada yaygın şekilde yaşanan sorunlardan biri olan CLI'ı manipüle etme yeteneği artmış ve böylece sahtecilik dünyasına geleneksel oyuncuların yanında yeni aktörler de girmiştir. Aynı zamanda, CLI kavramına daha az aşina olan ve IP tabanlı ses ve mesajlaşma hizmetleri de sunan birçok yeni ve genellikle daha küçük operatörün de piyasaya çıktığı görülmüştür. Ülkemiz için STH operatörleri bu duruma örnek olarak verilebilmektedir. Bu durum dolayısıyla çağrı zincirinde gerçekleşen uzama ve yeni aktörlerin çağrı zincirine dâhil olması CLI'ın bütünlüğünü korumayı da oldukça zorlaştırmaktadır (ECC, 2022).

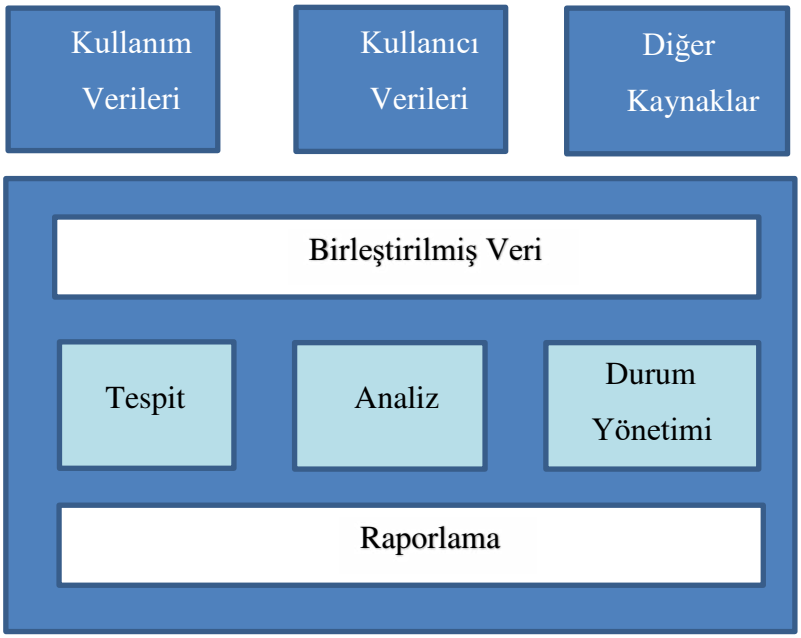
Teknolojik gelişmeler elektronik haberleşme sektörü için sınırsız bir ekosistemi mümkün kılmış ve bu durum yine son kullanıcılar için faydalı olmakla birlikte yargısal sorunları da beraberinde getirmiştir. Bir ülkedeki mağdurlara başka bir ülkeden dolandırıcılık yapanları tespit edebilmek için uluslararası işbirliği girişimleri daha önce ITU (Uluslararası Telekomünikasyon Birliği - International Telecommunication Union) düzeyinde uygulanmıştır, ancak dolandırıcılık ve kötüye kullanımla mücadele için daha sağlam düzenlemeler ve küresel tekniklerin kullanılması gerekmekte olup aksi halde bu sorunlar yaşanmaya devam edecektir (ECC, 2018).

Sahtecilik tespit yöntemlerinin esnek ve hızlı reaksiyon alacak yapıda olması gerekmektedir. Bu konuda tek bir basit kural olmasa da en temel kural olarak para neredeyse saldırganın da oraya yönelmesi düşünülebilir. Bu açıdan en yüksek ücretler uluslararası çağrılarda olduğundan sahteciliğin de en çok buraya yönelmesi çok olasıdır. Bir operatör sahteciliğe karşı iyi önlemler alırsa dolandırıcıların daha zayıf olan başka operatöre yönlenmesi beklenebilecek bir durumdur (Becker vd., 2010; Sahin, 2017).

Telekomünikasyon sahteciliğinin tespiti için en önemli kaynak çağrı detay kayıtları (Call Detail Records - CDR), müşteri veri ve davranışları, sunucu kayıtları (log) ve olası diğer verilerdir. Bununla birlikte, CDR analizi önemli bir uzmanlık gerektirmektedir. Teste tabi tutulan çağrılar çok yüksek hacimde olabildiğinden profil örneği çıkarmanın zorlaşması ve sahteciliği gerçekleştirenlerin yakalanmaktan kaçınmak için davranışlarını sıklıkla değiştirmesi de bu modelin etkinliğini yer yer azaltabilmektedir. Bu nedenle, sahtecilik

yönetim sistemleri önemli bir sorunun çözümüne karşılık gelebilmektedir (Becker vd., 2010; Rebahi vd., 2011; Sahin, 2017). Müşteri faturaları ve çağrı davranışları için anomali incelemesi yapılarak müşteriler normal veya sahteciliğe meyilli olarak kategorilere ayırılır ve şüpheli müşteriler üzerinde yapılacak detaylı incelemelerle sahtecilik tespiti yapılabilir (Farvaresh ve Sepehri, 2011). Ulusal ve uluslararası CDR'lar ve karşılık gelen fatura bilgileri incelenerek burada da sahtecilik yapılan kayıtlar, müşteriler ve operatörler tespit edilebilmektedir (Alraouji ve Bramantoro, 2014; Kabari vd., 2015).

Sahtecilik tespiti yapılırken verilerin toplanması ve analizi aşamasında pek çok makine öğrenmesi, veri madenciliği ve yapay zekâ tekniği kullanılmaktadır. Bunlardan bazıları şunlardır; karar ağaçları (decision tree), nöral ağlar (neural networks), destek vektör makineleri (support vector machines), mantıksal regresyon (logic regression), bayes sınıflandırması (bayesian classification) (Rosset vd., 1999; Bishop, 2005; Chen vd., 2006; Coussement ve Poel, 2008; Farvaresh ve Sepehri, 2011; Abdallah vd., 2016; Xie vd., 2019; Mawgoud ve Ali, 2020; Nguyen vd., 2020). Sahtecilik yönetim sistemleri pek çok kaynak ve formda veriyi toplayıp, bunları yukarıda verilen yöntemler ile analiz ederek raporlama yapabilmektedir. Şekil 2.2'de sahtecilik yönetim sistemlerine ilişkin genel bir tasarıma yer verilmektedir.



Kaynak: (Cortesão vd., 2005)

Şekil 2.2 Sahtecilik Yönetim Sistem Mimarisi

Bu mimari yapısında, merkezi bir sahtecilik yönetim sistemi bulunmaktadır. Kullanıcılarda, çeşitli kullanımlardan ve olası bütün diğer kaynaklardan birden çok formatta toplanan veriler sisteme aktarılmakta, belirli algoritmalar ile birleştirilmekte ve iç veri formatına uygun hale getirilmektedir. Bu aşamada farklı veri kaynakları ile çapraz ilişki içerisinde olarak veri geliştirme sağlanabilmektedir. Sonrasında ise, analistler tarafından yakından inceleme gerektirdiği düşünülen durumlar hakkında uyarılar oluşturulması için yapay zeka, profil çıkarma ve akıllı öğrenme teknikleri de kullanılarak tespit süreçleri uygulanmaktadır. Tespit sonrasında, ilgili tüm bilgiler ile birlikte bir vaka tanımlaması yapılarak ilgili vaka yöneticisine iletilir. Sürecin sonunda ise tüm hususları detayları ile içeren raporlama araçları sağlanarak, ilgililerin erişimi sağlanmaktadır (Cortesão vd., 2005).

2.3. Türkiye'de Sahtecilik Sorunu

Tüm dünyada olduğu gibi ülkemizde de telekomünikasyon sektörü hızla gelişmekte ve her geçen gün yeni alanlara açılmaktadır. Tüm dünyada olduğu gibi ülkemizde de sahtecilik kaynaklı gelir ve prestij kaybı yaşanmakta ve bu durum ciddi sorunlara yol açmaktadır. Sahtecilik yöntemlerine ilişkin yukarıda yer verilen bilgilerin pek çoğu birebir aynı ve/veya benzer formlarda ülkemizde de yaşanmakta ve Türkiye'de faaliyet göstermekte olan başta mobil olmak üzere elektronik haberleşme sektöründe yer alan operatörler açısından önemli ölçüde prestij, güç, zaman ve en önemlisi gelir kaybına neden olmaktadır. BTK'nın 2021 yılı 3.çeyrek pazar verileri raporuna göre Türkiye'de elektronik haberleşme sektöründe faaliyet gösteren tüm operatörlerin yıllık net satış gelirleri toplamı yaklaşık olarak 75-80 milyar TL olup bu sektörün oldukça yüksek hacimli bir sektör olduğu görülmektedir. Bu durumun sektörde yaşanacak gelir kayıplarının da ne derece önemli ve yüksek miktarlarda olabileceği açısından önemli bir gösterge olduğu düşünülmektedir (BTK, 2021).

Türkiye'de elektronik haberleşme sektörünün düzenlenmesi ve denetlenmesi konusunda yetkili olan kurum BTK'dır. Sektörde hizmet veren operatörler BTK tarafından yetkilendirilmektedir. Operatörler, hizmet sunumu, hizmet sunumu esnasında karşılaşılan sorunlar vb. hususlarda BTK'ya karşı sorumlu durumdadır ve BTK tarafından yürütülen ve denetlenen ilgili mevzuat hükümlerine uymakla yükümlü bulunmaktadır.

Yukarıda da belirtildiği üzere telekomünikasyon sahteciliğinin pek çok yöntemi bulunmaktadır. Türkiye'de sahtecilik yöntemleri olarak; rıza dışı numara taşıma ve abonelik tesis etme, CLI manipülasyonu, uluslararası çağrı sahteciliği, katma değerli hizmet sahteciliği, bahis/kumar/reklam vb. istenmeyen mesajlar ve suni trafik oluşturma hususlarının yakalanabildiği bilinmektedir. Bu hususlara yönelik olarak pek çok düzenleme bulunmakta, sektörde duyulan ihtiyaçlara göre düzenlemeler güncellenmekte ve gerekli durumda denetimler gerçekleştirilmektedir. Ancak, sahtecilik çok geniş kapsamlı bir olgu olduğundan sadece mevzuat, denetim ve kamu gücüyle bu sorunu çözmek çok kolay görünmemektedir. Bu açıdan bakıldığında hem BTK'nın hem de sektörde faaliyet gösteren operatörlerin ortaklaşa çalışması, teknolojinin sunduğu imkânların da bu kapsamda olumlu yönde kullanılmasının faydalı olabileceği düşünülmektedir.

BTK'nın sektörde oldukça önemli görevleri ve rolü bulunmaktadır. Bu yönüyle Türkiye'de telekomünikasyon sektöründe yaşanan sahtecilik sorununu BTK'dan bağımsız olarak ele almak mümkün görünmemekle birlikte sorunların çözümünü sadece kamu otoritesine ve düzenlemelere bırakmanın da günümüz teknolojisinde ve şartlarında makul bir durum olmayacağı aşikârdır. Yukarıda da ifade edildiği üzere sektördeki her bir paydaşın sahteciliğin bir parçası olabileceği de göz önüne alındığında her bir paydaşın çözüm için üzerine düşen sorumluluğu alması gerektiği kaçınılmaz bir durum olarak görünmektedir.

BTK tarafından hazırlanan Arayan Hat Bilgisi (CLI) Kullanımına İlişkin Usul ve Esaslar düzenlemesi ile de elektronik haberleşme hizmeti sunan operatörlerin CLI kullanımlarına ilişkin usul ve esaslar belirlenmiştir. Buna göre operatörler; çağrılarda yer alan CLI'ın operatöre tahsisli numara olmasını ve karşı taraftaki kullanıcıya bu numaranın gösterilmesini, CLI'ın hem CDR hem de sinyalleşme içerisinde "90+Alan Kodu+7 Haneli Abone Numarası" formatında olmasını, CLI'ın boş, eksik veya yanıltıcı biçimde oluşturulmamasını, oluşturulan CLI'ın kullanıcılar tarafından değiştirilmemesini, yurt dışı kaynaklı çağrılarda ülkemiz numaralandırma planında yer alan numara formatlarının bulunmamasını sağlamakla yükümlü olup bu hususlara aykırı şekildeki çağrıları da engellemeleri gerekmektedir. Bu düzenleme ile esasen CLI manipülasyonu kapsamındaki sahtecilik senaryolarının mevzuat çerçevesinde engellenmesi amaçlanmış olup halen aktif şekilde uygulaması devam etmektedir. Bununla birlikte zaman içerisinde pek çok düzenleme de yürürlüğe girmekte ve çeşitli önlemlerin de alındığı bilinmektedir. Ancak, sahtecilik

sorunları da halen yaşanmaya devam etmekte ve çeşitli kayıplar yaşatmaktadır. Bu noktada ülkemiz mevzuatı kapsamında yapılan incelemede operatörlerin sahteciliğe karşı alması gereken önlemlere ilişkin olarak özel başka bir düzenleme bulunmadığı ve konuya genel olarak yaklaşıldığı görülmüş olup bu alanda bir düzenleme açığı bulunduğu düşünülmektedir.

Önceki bölümlerde yer verildiği üzere, Türkiye'de de sahtecilik senaryoları dünya ile benzerlik göstermektedir. Abonelik (bayi) sahtecilikleri, CLI manipülasyonu, uluslararası çağrı sahteciliği, katma değerli hizmet sahteciliği, bahis/kumar/reklam vb. istenmeyen mesajlar ve suni trafik oluşturma vb. hususlar en çok karşılaşılan sahtecilik türleridir. Bununla birlikte, bu çalışmada genel olarak telekomünikasyon sahteciliği ve pek çok senaryo ele alınmış olsa da esas olarak CLI manipülasyonu hususu noktasında yaşanan sorun ve çözüm önerilerine yer verilecektir. Çünkü bu sorun ses çağrı trafiğindeki sahtecilik sorunlarından biri olmakla birlikte, hem dünyada hem de ülkemizde son zamanlarda artmakta ve önemli gelir kayıplarına yol açmaktadır. Özellikle ülkemizde bu alanda sektörde yer alan operatörler arasında da anlaşmazlıklar yaşanmakta ve hâlihazırda uygulanan anlamlı ve faydalı bir çözüm bulunmamaktadır.

CLI manipülasyonlarının genellikle, yurt dışı sonlandırma ücretleri ödemek yerine ülke veya Avrupa Birliği (AB) içi sonlandırma ücretlerinden yararlanmak amacıyla yapıldığı bilinmekte olup burada kuralların daha belirgin olmasına ihtiyaç olduğu aşikârdır. Son kullanıcıları yanıltmak amacıyla bilinçli olarak CLI'ı manipüle eden sektör aktörlerini caydırmak için mevcut durumdaki tedbirler yeterli görünmemektedir. Uluslararası çağrı sistemlerinin geldiği karmaşık durum nedeniyle, bu aktörleri ve manipülasyonu gerçekleştirenleri tespit etmek ve yaptırım uygulamak oldukça zor olduğundan buna yönelik ek önlemlerin düşünülmesi gerekmektedir. Ortalama bir kullanıcının gelen çağrıda CLI'ın manipüle edilip edilmediğini anlaması beklenemez ve bu durum için mutlaka daha üst noktadan bir önlem alınması gerekmektedir (ECC, 2016; ECC, 2022).

Ülkemizde yaşanan CLI manipülasyonu senaryoları da genellikle benzer şekilde yurt dışı kaynaklı çağrıların CLI'ının değiştirilerek yurt içi çağrıymış gibi gösterilmesi yoluyla çağrı sonlandırma ücretlerinin çok daha düşük ödenmesi şeklinde gerçekleşmektedir. Yurt dışı bir çağrı transit bir STH operatörü tarafından sonlandıran operatöre teslim edildiğinde

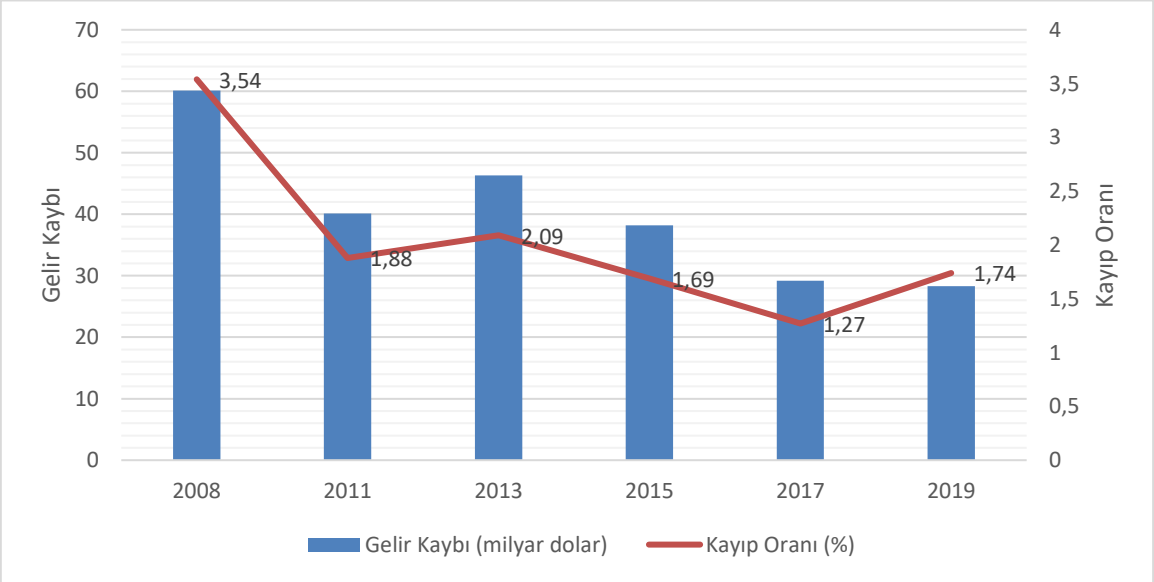
yaklaşık olarak 0,11 Euro ücret ödenmektedir. Bununla birlikte, yurt içi çağrı sonlandırma ücretleri için ise sonlandıran operatörlere yaklaşık 5 kuruş ücret ödenmektedir. Bu nedenle bir çağrıda CLI manipülasyonu gerçekleştiği durumlarda sonlandıran operatör ancak 20'de bir oranında ücret alabilmektedir. Sektördeki çağrı trafiğinin yaklaşık %98'inin mobil operatörler kaynaklı (BTK, 2021) olması nedeniyle bu durumdan en çok etkilenen taraf da mobil operatörler olarak görünmektedir.

Bu noktada, temel sorunlardan biri sahteciliğin kim tarafından gerçekleştiğinin kesin olarak bilinememesi veya tespit edilememesidir. Mobil operatörler, kendi teknik imkânlarıyla CLI manipülasyonu yapıldığını tespit ettiğinde veya bu yönde ciddi şüphe oluştuğunda öncelikle çağrıyı teslim eden STH operatörlerine durumu iletmekte ve numaranın hizmete kapatılması vb. talepler iletmektedirler. STH operatörlerince zaman zaman bu numaralar kapatılmakta ve abone tarafından CLI manipülasyonunun yapıldığının anlaşıldığı belirtilmekle beraber zaman zaman da durum kabul edilmeyerek abone tarafından bu manipülasyon yapılmış olsa dahi kendilerinin haberinin olmadığı ve bu noktada yapabilecekleri bir işlemin olmadığı belirtilmekte ve ayrıca sektörde faaliyet gösteren operatörler arasında (mobil ve sabit) ilgili mevzuata göre bir ayrım bulunmadığı ve alt üst ilişkisi olmadığı bu nedenle kendilerine iletilen manipülasyon çerçevesindeki taleplerin bir başka operatörden değil kamu otoritesi tarafından iletilmesi gerektiği ifade edilmektedir. Bunun yanında, benzer durumların yoğun şekilde yaşanması ve belirli STH operatörlerinden gelen çağrılarda daha çok gerçekleşmesi halinde ise mobil operatörler konuyu BTK'ya ilettiği ve durumun araştırılmasını ve bu kapsamda gerekli tedbirlerin alınmasını talep ettiği bilinmektedir.

Hem önceki kısımlarda hem de bu kısımdan sonra anlatılacağı üzere CLI manipülasyonunun tespiti için bazı yöntemler bulunmaktadır. Ülkemizde faaliyet gösteren mobil operatörlerce bu yöntemlerin kullanıldığı da bilinmektedir. Bununla birlikte, bu tespitlerin sektördeki bir operatör tarafından tespit ediliyor olması yasal anlamda fazla bir anlam ifade etmemekte ve bu tespitler kapsamında yaptırım uygulamak mümkün görünmemektedir. Bu nedenle, sektörde yer alan aktörlerin tecrübeleri ile kamu otoritesinin idari, teknik ve yasal gücünün bir araya gelmesi, sorunun çözümü noktasında elzem görünmektedir.

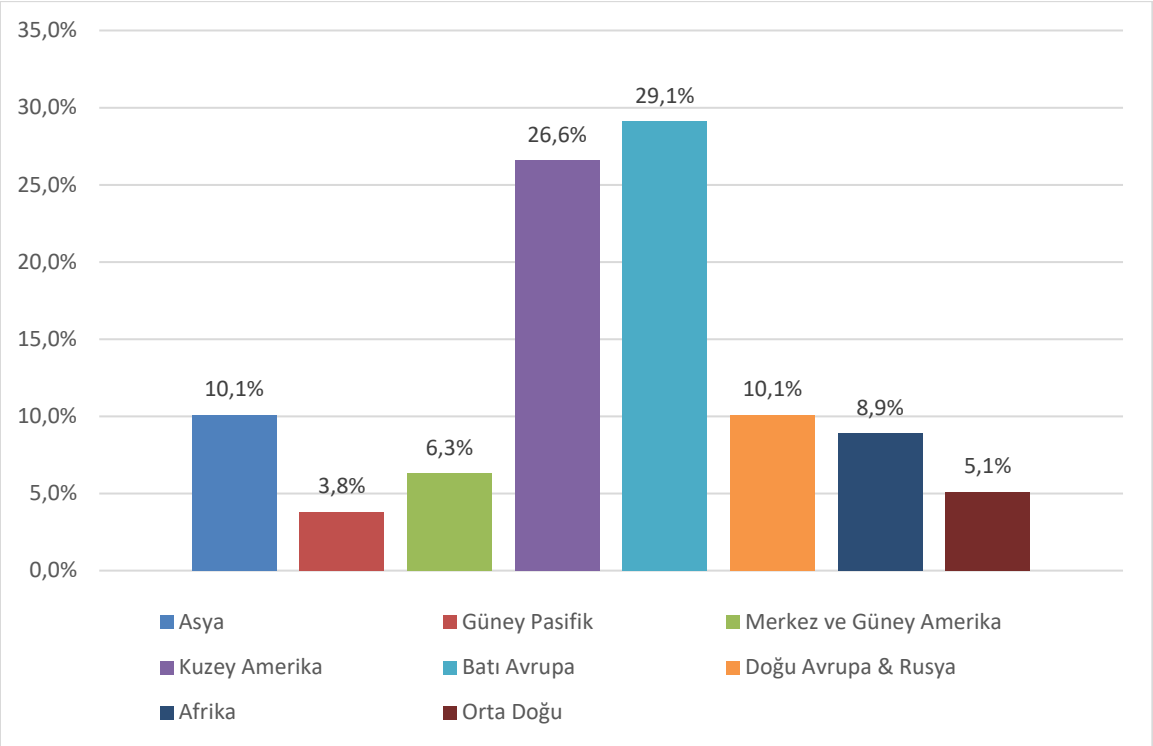
2.4. Dünyada Sahtecilik Sorunu

İletişim Sahteciliği Kontrol Birliği (CFCA) tarafından 2019 yılında yayımlanan global telekomünikasyon anketine göre, dünya çapında telekomünikasyon sektörünün sahtecilik nedeniyle gelir kaybı 2017 yılında 29,2 milyar dolarken 2019 yılında 28,3 milyar dolar olarak tüm sektör gelirlerinin %1,74'ü olarak ölçülmüştür. Ankete tüm kıta ve bölgelerden katılım gerçekleşmiş olup katılımın ekseri çoğunluğu Avrupa ve Kuzey Amerika'dan olmuştur. Şekil 2.3'te 2008 yılından 2019 yılına kadar sahtecilik kaynaklı gelir kayıplarının değişimine ve Şekil 2.4'te ise ankete katılanların bölgelere göre dağılımına yer verilmiştir (CFCA, 2019). Bu kayıplardan 6.8 milyar doları ise sadece servis sağlayıcı operatörlerin kaybı olarak belirtilmektedir (TRI, 2021). Gelir kayıplarında yıllar içerisinde bir düşüş gözlemlense de halen ciddi miktar ve oranda kaybın olduğu da gözlenmektedir. Global Liderler Forumunun (GLF), 2018'de yayımladığı sahteciliğe karşı alınacak aksiyonlar raporunda da sahtecilik bulunan çağrı trafiğinin uluslararası toptan transit çağrı (Telekomünikasyon çağrılarında, çağrının başlatıldığı nokta ile sonlandığı nokta arasında birden çok taşıyıcı nokta ve operatör olabilmektedir. Çağrıları başlatmayan veya sonlandırmayan ve sadece taşıyan bu operatörlere transit operatör, bu tarz çağrılara da transit çağrı denmektedir) sektörüne yıllık yaklaşık 17 milyar dolara mal olduğu ve bu transit operatörlerden %85'inin sahtecilik sorununun şirketleri ve sektör için birincil öncelikli problem olduğu belirtilmiştir (GLF, 2018).



Kaynak: (CFCA, 2019)

Şekil 2.3 Yıllara Göre Sahtecilik Kaynaklı Gelir Kayıpları ve Oranları



Kaynak: (CFCA, 2019)

Şekil 2.4 Gelir Kaybı Anketine Katılımın Bölgesel Dağılımı

Öte yandan, 2016 yılında Amerika Federal Ticaret Komisyonu verilerine göre ABD'de sahtecilikten etkilenen müşteri şikâyetlerinin ayda ortalama 400 bin civarında olduğu belirtilmektedir (FTC, 2016).

BEREC (Elektronik Haberleşme için Avrupa Düzenleyiciler Kurumu - The Body of European Regulators for Electronic Communications) tarafından 2019 yılında E.164 numara bloklarında sahtecilik (CLI manipülasyonu, Simbox, Wangiri vb.) ve kötüye kullanım kapsamında bir çalışma gerçekleştirilmiş ve sonuçları bir rapor ile yayımlanmıştır (BEREC, 2019). Bu çalışmada öncelikle, BEREC üyesi tüm ülkelerin de katılımıyla bir anket düzenlenmiş ve sahtecilik konusunda ülkelerin durumları özetlenmiştir. Anket ülkelerin telekomünikasyon sektöründeki kamu otoriteleri ile gerçekleştirilmiş ve aralarında Türkiye'nin bulunmadığı 15 ülke ankete katılım sağlamıştır. Ankete ilişkin bilgilere aşağıda yer verilmektedir.

Sahtecilik gerçekleşen durumlarda servislere veya numaralara erişimin engellenmesi ya da ilgili transit operatörlere arabağlantı ücreti ödenmemesine yönelik olarak düzenlenmiş

bir prosedür bulunup bulunmadığına ilişkin soruya 8 ülke evet, 7 ülke ise hayır şeklinde cevap vermiştir. Ülkedeki operatörler arasındaki sahtecilik sorunlarına yönelik olarak uyuşmazlık sürecinin işletilip işletilmediğine ilişkin soruya 7'şer ülke evet ve hayır cevabı vermiştir.

Meydana gelen sahtecilik ve kötüye kullanım durumlarını önleyebilmek amacıyla uygulanan bir prosedürleri olup olmadığına ilişkin soruya 4 ülke evet ve 11 ülke hayır cevabı vermiştir. Sahtecilik vakalarının son kullanıcılar üzerindeki etkilerini durdurmak ve azaltmak için bir prosedürleri olup olmadığına ilişkin soruya 6 ülke evet 8 ülke ise hayır cevabı vermiştir. Evet cevabı veren ülkelerden bazılarında sahteciliğin belirlenen kriterlere uygun şekilde tespit edilmesi halinde operatörlere trafiği durdurma ve sonlandırma ücretini ödememe noktasında ilgili otoriteye başvurduğu ve otoritenin 2 gün içinde onay vermesi halinde süreci işletebildiği, bazı ülkelerde ulusal polis ve operatörlerle birlikte seminerler düzenlendiği ve prosedürlerin bu çalışmalar sonucunda oluşturulmak istendiği, bazı ülkelerde ise bu çalışmaların sonucu olarak operatörlerce birlikte hareket edildiği ve ülkede faaliyet gösteren en büyük 10 operatörün ülke otoritesi vasıtasıyla bilgi ve tecrübelerini ve engellenen numara bloklarının bilgisini birbirleriyle ve tüm kamuoyu paylaştığı ve bu sayede son kullanıcıların da faydalanabildiği bir ekosistem oluşturulduğu ve ayrıca güvenilir olmayan CLI'a sahip bir çağrı ülkeye girdiğinde çağrıya eklenen yeni bir numara aralığı belirlendiği ve bu sayede bu tip çağrıların daha kolay izlenebildiği belirtilmiştir. Ülkeler arası (sınır dışı) düzenleyici otoriteleri ile iş birliği yapılıp yapılmadığına ilişkin soruya ise 3 ülke evet 8 ülke ise hayır cevabı vermiştir.

Ülkenizdeki operatörlerin bağımsız olarak sahtecilik vakalarını azaltmak için uyguladığı önlemlerden haberdar olunup olunmadığına ilişkin soruya 11 ülke evet ve 3 ülke hayır cevabı vermiştir. Ülkelerden bazıları bu farkındalığın bilgi paylaşımı gerçekleştirilen ulusal platformlar vasıtasıyla yapıldığını, bazı ülkelerde operatörlerin sahtecilik gerçekleşen numaraları yayımladığı ve bazılarında ise operatörlerin önlemleri önce kendileriyle paylaştığını belirtmişlerdir.

Ülke düzenleyici otoriteleri arasında ortak bir iletişim bilgileri veri tabanı oluşturmanın ve sahtecilik vakalarının raporlandığı ve kaydedildiği ortak bir veri tabanı oluşturmanın sahteciliğe karşı ülkeler arasındaki iş birliğini arttırıp arttırmayacağına ilişkin

soruya ise ülkelerin tamamı evet cevabı vermiştir. Engellenen numara bloklarının ve sahtecilik gerçekleştiren operatörlerin yayımlanmasının faydalı olup olmayacağına ilişkin soruya ise ülkelerin yarısı evet cevabı vermiştir.

Raporda anket çalışması dışında gerçekleştirilen toplantı ve seminer sonuçları da paylaşılmıştır. Europol'de (Avrupa Polis Teşkilatı) görevli bir çalışan tarafından, polisin AB ülkelerinin düzenleyici otoriteleri ile iş birliği içinde olduğu ve ülkeler arası iş birliğinin de geliştirilmesi gerektiği ifade edilmiştir. Sahtecilik çözümleri sunan özel bir şirketin yetkili temsilcisi tarafından CLI manipülasyonu hususunda brifing verilmiş ve yine benzer şekilde transit ve diğer operatörler ile düzenleyici otoriteler ve diğer sektör temsilcilerinin iş birliği halinde olması gerektiği belirtilmiştir.

Toplantı sonunda bazı hususlara dikkat çekilmiş ve sahteciliğe karşı mücadele noktasında faydalı olabilecek hususlara yer verilmiştir. Düzenleyici otoritelerin hantal mekanizmaları, bilgi paylaşımındaki otomasyon eksiklikleri ve dolandırıcıların kullandıkları teknolojilere erişim noktasında yaşanan eksiklikler bulunduğu belirtilmiş sahteciliğe karşı BEREC olarak çerçeve bir anlaşma yapılmasının ve sektörün olası tüm paydaşlarının yaklaşımlarında birlik sağlanmasının faydalı olacağının düşünüldüğü ifade edilmiştir (BEREC, 2019).

2022 yılında ise ECC tarafından, CLI manipülasyonu ile mücadele edebilme noktasında farklı teknikler ve çeşitli düzenleyici otoritelerin perspektifinde mevcut düzenleyici uygulamaları gözden geçirmek için bir rapor yayımlanmıştır (ECC, 2022). Kısa vadeli bazı çözümlerin hâlihazırda kullanıldığı ancak bunların genellikle gerçek zamanlı bir çözüm olmadığı belirtilmiştir. Hem ulusal hem de uluslararası düzeyde CEPT ülkelerinin düzenleyici otoriteleri ile ITU ve BEREC gibi organizasyonların da CLI manipülasyonu ile mücadelede bilgi paylaşımı ve trafik analizi gibi konularda endüstri gruplarını teşvik etmeleri gerektiği savunulmuştur. Ayrıca düzenleyici hususların, kullanıcılara sağlanan CLI'ın geçerli olup olmadığının çağrıyı başlatan operatör tarafından sağlanması noktasında yeterli olması gerektiği ifade edilmiştir. Ayrıca daha sonra detaylarına yer verilecek olan STIR (Secure Telephony Identity Revisited)/SHAKEN (Signature-based Handling of Asserted Information Using Tokens) benzeri işe yaradığı onaylanmış tekniklerin bu bağlamda kullanılmasının uzun vadeli çözümlerden olabileceğine yer verilmiştir. Ancak bu

tür tekniklerin tamamen IP ortamını gerektirebileceği ve bu nedenle kısa vadede uygulanabilmesinin de zor olabileceği belirtilmiştir.

Aşağıdaki bölümde bazı AB ülkeleri ile ABD'nin sahtecilik sorunları kapsamındaki yaklaşımlarına yer verilecektir (ECC, 2022).

2.4.1. Belçika

Belçika düzenleyici otoritesi tarafından 2020 yılı içerisinde yayımladığı yönerge ile, sahteciliği azaltmak, CLI kullanımı noktasında çağrının başlatıldığı andan tamamlandığı ana kadar daha fazla netlik sağlamayı ve CLI güvenilirliğini arttırmayı amaçlamakta olup bu noktada dört ilke ortaya koymuştur.

İlk ilke, her aramanın bir şebeke numarası ile ilişkilendirilmesi gerektiğidir. Bu şebeke numarası aramanın kaynağını temsil etmekte ve kullanıcı ile kamu elektronik iletişim şebekesi arasındaki bağlantıya karşılık gelmektedir. Kullanıcı tarafından üretilen CLI arayanı tanımlayacak, isteğe bağlı olacak ve şebeke numarası ile aynı olacaktır.

İkinci ilke, şebeke numarasının arayan bağlantıyı benzersiz şekilde tanımladığını belirtir. Numara, aramayı yapan operatör tarafından arayana atandığından, arayan kişi bu numarayı kullanmak durumunda olmalıdır.

Üçüncü ilke, son kullanıcıya gösterilen numaranın mutlaka aranabilir bir numara olmasıdır. Böylece son kullanıcı gördüğü CLI ile, bu numarayı çevirerek bir çağrıyı tam anlamıyla gerçekleştirebilecektir.

Dördüncü ilke, şebeke ve gösterilen numaranın geçerli olmasıdır. Geçerli numaradan kasıt ITU numaralandırma planlarına ve Belçika numaralandırma planına uygun olması ve bir son kullanıcıya tahsis edilmiş olmasıdır.

Bu ilkelerin yanı sıra Belçika'da kara liste uygulaması da bulunmaktadır. Bazı coğrafi numaraların CLI manipülasyonuna karşı özellikle hassas olduğu belirtilmiştir. Yurt dışından gelen CLI manipülasyonlarına karşı, sahtecilik şüphesi bulunan coğrafi numaralara yönelik

olarak bir kara liste hazırlanmış ve devam ettirilmektedir. Son kullanıcılar bu listede bulunmayı talep edebilmektedirler. Belçika'daki çoğu operatör bu tarz yurt dışı kaynaklı CLI'a sahip çağrıları engelleyebilmek için bu tür bir kara liste kullanmaktadır. Bu hususstaki detaylar Belçika'daki sektör temsilcilerinin oluşturduğu sahteciliğe karşı mücadele çalışma grubunda ele alınmaktadır.

2.4.2. Fransa

Fransa düzenleyici otoritesi tarafından yıllar içerisinde CLI manipülasyonuna yönelik olarak pek çok karar alınmıştır. Bu düzenlemelere şu örnekler verilebilmektedir. 2012 yılında katma değerli hizmet numaralarından gelen Wangiri çağrılarından korunmak için bu numaraların CLI olarak kullanılması yasaklanmıştır. 2018 ve 2019 yıllarında yapılan çalışma ile sahte CLI kullanılarak gerçekleştirilen sahtecilik çağrılarının azaltılması için birtakım önerilerde bulunulmuştur. Bu öneriler;

- Fransa'daki numaralara doğru uluslararası arabağlantılardan gelen ses ve SMS (Kısa Mesaj Servisi – Short Message Service) çağrıları için operatörlerin yönlendirmeleri engelleme hakkı olduğu,
- Otomatik sistemlerden gelen çağrılarda 2019 yılında mobil numaraların CLI olarak kullanılmasının yasaklanması ve bu yasağın 2021 yılında sabit numaralar için de genişletilmesi,
- CLI olarak kullanılan numaraların operatörlere tahsis edilen numara bloklarında yer alıyor olması, operatörler tarafından abonelere ikincil tahsisinin yapılmış olması ve bu tahsis süresince bu numara ve CLI ile sadece ilgili abone ile iletişim kurulabilmesi

şeklinde sıralanabilmektedir. Yine aynı çalışmada (ECC, 2022), 2018 yılından itibaren mobil ve coğrafi olmayan yeni numaralar için alt tahsisi yasaklamış ve her yıl alt tahsisi yapılmış olan numara listesinin operatörlerden alınması kararlaştırılmıştır. Bu karar ve tavsiyelerin uygulamasını kontrol etmek amacıyla operatörlerden düzenli şekilde engellenen çağrı sayıları ve nereden geldiklerine ilişkin bilgi alınmakta olup örneğin 2019 yılının Eylül – Kasım döneminde ülkede faaliyet gösteren büyük çaplı bir operatör tarafından sadece 111 milyon çağrının engellendiği bilinmektedir. 2019'da yapılan bu düzenlemeler ile uzun vadede STIR/SHAKEN (ilerleyen bölümlerde detaylı şekilde açıklanacaktır) modeline

benzer çözümlere yol açmaktadır. Bu ve benzeri çözümlerin konuşulup tartışılabilmesi amacıyla operatörlerle çeşitli çalıştaylar düzenlenmektedir. STIR/SHAKEN modelinin yalnızca IP arabağlantılar ile çalışması dolayısıyla eski nesil şebekelerin de dönüşmesi gerekeceğinden uzun vadeli bir mekanizma üzerinde çalışmanın faydalı olacağı değerlendirilmektedir. Bu noktada Fransa'da yakın bir gelecekte PSTN (Genel Aktarmalı Telefon Şebekesi – Public Switched Telephone Network) ve ISDN (Bütünleştirilmiş Sayısal Şebeke Hizmetleri – Integrated Services Digital Network) gibi daha eski nesil şebekelerin sona ereceği planlanmaktadır.

2.4.3. Almanya

Almanya düzenleyici otoritesi tarafından yapılan düzenlemelerde, gerçekleşen çağrılarda yer alan numaralara ilişkin birtakım hususlar bulunmaktadır. 2021 yılı sonunda bu düzenlemelerde bazı değişiklik ve iyileştirmelerin yapılacağı yeni bir telekomünikasyon yasasının yürürlüğe gireceği açıklanmıştır. CLI'a yönelik hususlarda Almanya'da bazı yaklaşım ve prensipler belirlenmiştir. Çağrının başlatıldığı operatör arayan numara olarak tam anlamlı bir ulusal numaranın iletilmesini ve bu numaranın aboneye tahsisli olmasını sağlamalıdır. Numara tahsisi aramanın ilgili olduğu servis için aboneye atanmalıdır. Rehber sorgulama, toplu arama, sesli kısa kod ve yüksek tarifeli hizmetler için Almanya ulusal numaralandırma planında yer alan numaralar arayan tarafın numarası olarak iletilememesi gerekmektedir. Çağrı akışında bulunan diğer operatörler tarafından iletilen numaraların değiştirilememesi gerekmektedir. Abonelerin sadece kullanım hakları olan numaraları kullanma ve şebekeye çağrı iletme hakları bulunmaktadır. Çağrılarda bu hükümlere aykırı şekilde bir numara iletimi bulunması halinde bu çağrıda CLI manipülasyonunun bulunduğu kabul edilmektedir. Bu durumlarda da düzenleyici otorite tarafından 100.000 Euro'ya kadar idari para cezası ve çeşitli yaptırımlar uygulanmaktadır.

2.4.4. Norveç

Norveç'te 2013 yılından beri yürürlükte olan düzenlemeye göre, teknik olarak mümkün olan ve ekonomik olarak da uygun olan durumlarda operatörlere son kullanıcıların kullanma hakkına sahip olmadığı arayan numaralarla başlayan çağrıları engelleme hakkı verilmiştir. Norveç düzenleyici otoritesi tarafından, müşterilerin zararlarını ve mali

kayıplarını önlemek için çağrıları engelleme hakkını açıklayan paydaşlara yasal rehberlik hizmeti sunulmaktadır. Ayrıca düzenleyici otoritenin girişimleri ile oluşturulan Numaralandırma Çalışma Grubu paydaşlarıyla iş birliği halinde CLI hususlarına yönelik bir kılavuz oluşturulmuştur. Bu çalışma grubunca çağrı trafiğini izleme, sahtecilik mağdurları için özel çözümler üretme ve SMS dolandırıcılığını önlemek gibi çabalar sarf edilirken bütüncül sürece yönelik başkaca çalışmalar da devam etmektedir.

2.4.5. Litvanya

Norveç'e benzer şekilde, arayan numaranın manipüle edildiği ve son kullanıcının ilgili numarayı kullanma hakkının bulunmadığı durumlar için operatörlere çağrıları engellemek üzere yasal hak tanınmıştır. Arayan numaranın kısmen veya tamamen değiştirilmesi de dâhil olmak üzere CLI manipülasyonu, Letonya'da sahtecilik ve numaranın kötüye kullanımı olarak görülmektedir. Letonya'da numaralar kullanılarak gerçekleştirilen sahteciliklerin ortadan kaldırılmasına yönelik olarak bir prosedür geliştirilmiştir. Buna göre, numara kullanılarak yapılan sahtecilik vakalarında ve numaraların kötüye kullanımı tespit edildiğinde, operatörlerin çağrıların yönlendirilmesini ve ilgili numaralara erişimi derhal engellemesi öngörülmektedir. Ayrıca operatörlerin sahtecilik ve numaraların kötüye kullanımı durumlarında, arabağlantı sözleşmelerinde yer alan ödeme prosedürleri ve diğer hususlara yönelik olarak önlemler alabileceği öngörülmüştür. Ayrıca Letonya'daki elektronik haberleşme kanunu uyarınca düzenleyici otoritenin sahtecilik gerçekleştirdiği tespit edilen operatörlere numara tahsis etmeme, yetkilendirmesini iptal etme vb. yaptırımlar uygulama hakkı bulunmaktadır.

2.4.6. Birleşik Krallık (İngiltere)

CLI verilerinin doğruluğunu sağlamak ve böylece tüketici çıkarlarını koruyarak güveni arttırmak için çeşitli önlemler alınmakta ve yasal düzenlemeler yapılmakta ve ayrıca bilgi paylaşımını ve paydaşlar arasındaki iş birliğini arttırmaya yönelik çeşitli girişimler üzerinde de çalışılmaktadır. IP teknolojilerinde yaşanan gelişim ile kolaylaşan CLI bilgilerinin değişimi hususunda daha fazla çaba harcamak gerektiği ve operatörlerin son kullanıcılara doğru CLI verisinin sunulmasını sağlama noktasında önemli bir rolü olduğu belirtilmektedir.

2.4.6.1. CLI yükümlülükleri ve kılavuzlar

Birleşik Krallık düzenleyici otoritesi CLI verilerinin arayanı benzersiz şekilde tanımlayan geçerli ve çevrilebilir bir telefon numarası içermesini şart koşmaktadır. Ayrıca;

- Arayan numaranın geçerli olabilmesi için Ulusal Numaralandırma Planında yer almalı ve düzenleyici otorite tarafından bir operatöre tahsis edilmiş olmalıdır.
- Çevrilebilir numara, hizmette olan, geri aranabilen ve sonraki aramalarda da kullanılan bir numara olmalıdır.
- Numara, kullanıcının kullanma izni bulunacak ve kullanma yetkisine sahip olacak şekilde arayan tarafı benzersiz şekilde tanımlamalıdır.

Düzenleyici otorite tarafından ayrıca CLI'ın geçerliliğini ve bütünlüğünü koruyacak ilkeleri ortaya koyan ve operatörlerin yükümlülüklerini belirleyen bir yasal düzenleme yapmıştır. Buna göre çağrı akışındaki farklı operatörlerin farklı yükümlülükleri bulunmaktadır. Çağrıyı başlatan operatörler CLI verilerinin sağlanmasından sorumludur ve transit ve sonlandıran operatörler ise söz konusu numaranın geçerli bir numara bloğundan olup olmadığını kontrol etmekle yükümlüdürler. Ayrıca, tüm aramalar aramanın kaynağını tanımlayan bir şebeke numarası ile ilişkilendirilmelidir. Bununla birlikte gösterilen numara (CLI) zaman zaman yasal yollarla değiştirilip farklı numara bloklarından kullanılabilmektedir. Ancak, bu gösterilen numara yüksek ücretli numara bloklarından olamamaktadır. Düzenlemenin esasında CLI'ın güvenilirliğinin sağlanmasının çağrı akışındaki tüm operatörlerin iş birliğine bağlı olduğu ve bu kapsamda tüm paydaşların doğru davranışı sergilemek durumunda olacağı şartların sağlanması gerektiği düşüncesi ile oluşturulmuştur.

2.4.6.2. CLI'ın geçersiz olduğu durumlardaki operatör aksiyonları

Bir operatörün bir çağrıdaki CLI'ın geçersiz olduğunu teknik olarak mümkün olacak şekilde tespit etmesi veya anlaması durumunda, bu çağrılar operatör tarafından filtrelenebilmekte veya engellenebilmektedir. Yurt dışı kaynaklı çağrıların ülkeye ilk girdiği noktada operatörler öncelikle CLI'ın geçerli bir şekilde doldurulmuş olduğunu kontrol

etmektedirler. Eğer geçerli değilse, düzenleyici otorite tarafından belirlenmiş olan "08979" ile başlayan 10 haneli bir numara CLI kısmına yazılarak bu tarz durumların ayrıştırılabilmesi için kolaylık sağlanmış olur.

2.4.6.3. Düzenleyici ve sektör koordinasyonu

Düzenleyici otorite güvenilir bir CLI olmayan çağrıların engellenmesi konusunda operatörlerle;

- Sahtecilik ve kötüye kullanım durumlarında engellenen numara listesinin düzenleyici aracılığıyla paylaşabilecekleri platformun sağlanması,
- Düzenleyici otorite tarafından numaralandırma planında tanımlanmamış ve geçerli olmayan numaraların listesini sağlaması ve operatörlerin de çağrıları engellerken bu listeyi referans alması,
- Yanlış numaraların geri aranması amacıyla iletilen kısa mesaj dolandırıcılığına karşı yenilikçi çözümler üretilebilmesi için mobil şebeke operatörleri ve polis kuvvetleri ile birlikte çalışılması

hususlarını içeren iş birliği çalışmaları yürütmektedir.

2.4.7. Amerika Birleşik Devletleri

ABD düzenleyici otoritesi tarafından CLI manipülasyonu ve genel olarak sahteciliğe karşı pek çok teknik yöntem uygulanmakta ve düzenlemeler yapılmaktadır. 2009 tarihli bir yasa uyarınca, CLI'ın dolandırıcılık, zarar verme ve haksız şekilde herhangi bir şey edinme amaçları ile yanlış ve yanıltıcı olacak biçimde iletilmesi yasaklanmıştır. Herhangi bir zarar amaçlanmadıysa veya gerçekleşmediyse bu faaliyet illegal olarak değerlendirilmemektedir. Ayrıca bu dolandırıcılığı gerçekleştiren herkes 10.000 Amerikan Dolarına kadar para cezasına çarptırılabilmektedir. 2011 yılında ise, bu hususların daha da sıkılaştırılması gerektiği üzerine bir düzenleme daha ortaya çıkmıştır. Buna göre, söz konusu dolandırıcılık faaliyetlerinin kapsamı genişletilerek, ülke dışındaki kişiler, IP tabanlı ses hizmetleri ve SMS hizmetleri de kapsama dâhil edilmiştir.

Özellikle istenmeyen aramalar (robocalls and telemarketing calls) ile ilgili önemli çalışmalar bulunmaktadır. Bu noktada düzenleyici otorite tarafından operatörler kullanıcılara daha fazla etkinlik vermesi için teşvik edilmektedir. Aramayı engelleme ve başkalarına tahsis edilen numaraları kullanarak insanları dolandıranları belirlemek çözümün temel taşlarıdır. Bu çerçevede üç temel durumdan oluşan bir eylem planı belirlenmiştir.

1) Kaynağı tanımlama: E.164 numaralarını taklit etmek ve kimliğini gizlemek kolay bir yöntemdir. Böylece yasa dışı otomatik aramalar ve pazarlama aramaları artabilmektedir. Oluşturulan bir çalışma grubu bünyesinde, IP tabanlı çağrılarda arayanın kimliğini doğrulamak ve bu anlamda standartlar geliştirmek için çalışmalar başlatılmıştır. Bu standartlar STIR ve SHAKEN olarak bilinmektedir. Temel olarak bir çağrının ve çağrıya ilişkin numaraların yetkili bir şekilde çağrı oluşturulurken şifrelenmesi ve imzalanması ile çağrı sonlandırılırken doğrulanması üzerine kurgulanmıştır. Böylece IP tabanlı çağrı ekosisteminde uçtan uca güvenilir bir hat oluşturulmuş olmaktadır.

2) Şebeke ve tüketici için engelleme araçları: Bu noktada temel amaç, kullanıcıların iletişimlerini daha sağlıklı şekilde kontrol edebilecekleri yetkilerinin olmasıdır. Tüketiciler doğrulanmış arayan kimliği bilgilerini görebilecek ve gelen aramalar için gerçek zamanlı olarak karar verebilecektir. Bu anlamda, standardizasyon çalışmaları da devam etmektedir.

3) Tespit, değerlendirme, geriye dönük izleme ve azaltma: Geçmiş veriler üzerinde çeşitli çalışmalar yapılarak hiçbir şekilde trafik oluşturmaması gereken numaralara yönelik bir liste oluşturulmuştur. Geriye dönük izleme çalışmaları yapılarak öğrenilen bilgilerde yer alan istenmeyen ve yasa dışı trafik bilgileri kullanıcılar ile paylaşılarak bu anlamda bir iyileşme sağlanmıştır.

Ayrıca, düzenleyici otorite tarafından sadece operatörlerin SHAKEN sertifikası alabilmesi noktasında bir mekanizma tanımlanmış ve bu sertifikanın dolandırıcıların eline geçmemesi için gerekli tedbirler alınmıştır. 2023 yılında tamamlanacak bir çalışma ile tüm operatörlerin bu sertifikaları edinmesi ve bu yöntemleri uygulaması planlanmaktadır.

2.5. Telekomünikasyon Sahteciliğine Yönelik Önleyici Tedbirler

Yapay zekâ yöntemleri ile sahteciliğe yönelik pek çok çözüm sunulmaktadır. Yukarı kısımlarda bu hususlara yer verilmiştir. Bu yöntemlerin pek çoğu çağrı sonrası oluşan kayıtlar üzerinde yapılan analizler ile gerçekleştirilmektedir. Bununla birlikte, CLI manipülasyonu ile mücadeleye yönelik bazı uzun vadeli başka çözümler de bulunmaktadır (ECC, 2022). Bunlardan bazılarına bu kısımda yer verilecektir.

2.5.1. STIR/SHAKEN

Yukarı bölümlerde kısaca bahsedildiği üzere, bu yöntemler ABD'de yönetim yapısı da dâhil olmak üzere çeşitli katmanlarda uygulanmaktadır. Eski şebeke yapısında CLI çağrıyı başlatan operatör tarafından arayan numara olarak sinyalleşmeye eklenmekte ve sonlandıran operatörde doğru bir şekilde görülmekte idi. Günümüz IP teknolojisinde ise CLI herhangi bir numara olarak girilebilmektedir. Ayrıca çağrı zincirindeki operatörler tarafından da müdahaleye karşı zayıf durumdadır (ECC, 2022).

SHAKEN protokolünde esas olan her zaman çağrıyı başlatan operatörün arama hakkında bilgisi bulunduğudur. Bu bilgiler, CLI'daki numara, müşterinin başka bir CLI kullanımına verdiği izin ve kendi şebekesine giriş yapılan nokta olabilmektedir. SHAKEN, çağrıyı başlatan operatörün bu bilgileri sonlandıran operatöre güvenli bir mekanizma ile iletmesini sağlamaktadır. Çağrıyı başlatan operatör yukarıda yer verilen bilgilere dayalı olarak çağrı için bir dijital imza oluşturur ve bunu sonlandıran operatöre iletilecek sinyalleşme bilgisinin içerisine ekler. Sonlandıran operatör dijital imzayı doğrular ve bu sayede CLI'ın değiştirilmemiş olduğu güvence altına alınmış olur. Gerçekleşecek bir değişiklik durumunda ise imza değişmiş olacağından bu durumun farkına varılabilecektir (McEachern ve Burger, 2019; Azad vd., 2020). Her çağrı başlangıcında "origid" adı verilen çağrıyı benzersiz şekilde tanımlayan özel bir numara tanımlanmakta ve bu numara üzerinden bilgilerin takibi yapılabilmektedir. SHAKEN, uçtan uca bir mekanizma olarak tasarlanmış olan STIR protokolüne dayanmaktadır. Hem çağrıyı gönderen hem de sonlandıran tarafın telefonunda STIR istemcisi bulunmalıdır. İmzayı oluşturma ve doğrulama çağrıya katılan kullanıcılar tarafından gerçekleştirildiğinden operatörlerin süreçte son derece şeffaf olması gerekmektedir. SHAKEN, STIR'e dayalı olduğundan sertifika yönetim sistemlerine ihtiyaç duymakta ve bu süreçler operatör düzeyinde gerçekleştirilmektedir. Bu yöntemle çağrılar

doğrudan engellenmemekte ve çağrıyı alan tarafın kullanacağı bir uygulamaya, çağrının iyi, şüpheli veya muhtemelen sahte olduğuna ilişkin uyarı verildiği ve son kullanıcının arama bazında karar verebildiği bilinmektedir. Özetle bu sayede, sadece operatörlere çağrıyı imzalama ve doğrulama sağlanmakla kalınmaz, aynı zamanda son kullanıcılara aramaya güvenip güvenemeyecekleri hususunda da güvence sağlanmış olur (ECC, 2022).

STIR/SHAKEN'a dayalı yöntem merkezi bir mimariden oluşmaktadır ve başlangıçta sadece ABD için tasarlanmıştır. Sonrasında Kanada ile bir anlaşmaya varılmış ve model iki ülkeye genişletilmiştir. Ancak, iki ülkede aynı organizasyon ve ülke kodu kullanıldığından bunu tam anlamıyla iki ülke modeli görmek de pek mümkün değildir. Yakın bir gelecekte bu yöntemin Avrupa çapında bir modele veya başka yerlerde gerçekleşecek modellere dönüşmesi de beklenmektedir. Çok sayıda ikili anlaşma gerektirmesi ve tüm ülkelerin bu anlaşmaları kabul etmesi gerektiği gibi hususlar ise bu noktada yaşanabilecek zorluklar olarak görünmektedir (I3Forum, 2019).

2.5.2. SOLID

SOLID (Social Linked Data – Sosyal Bağlantılı Veri), bağlantılı veri ilkelerine dayanan merkezi olmayan uygulamalar oluşturmak için önerilen bir dizi sözleşmeler ve araçlar bütünüdür. SOLID bireysel varlıkların verilerini, özel veri depolarında veya "Pod"larda (kişisel veriler için güvenli web servisleri) kullanılan sistem ve uygulamalardan ayırmasına olanak tanımaktadır. Her bir varlık kendi Pod'undaki verileri kontrol etmekte ve bu verileri hangi varlıklarla paylaşacağını seçmektedir. Bu standart HTTP (Hiper Metin Transfer Protokolü – Hyper Text Transfer Protocol) üzerine kurulmuştur. SOLID'in, merkezi olmayan yapısı, sağladığı yetkilendirme ve şifreleme sayesinde telekomünikasyon ekosisteminde arayan numaranın doğrulaması amacıyla kullanılabileceği değerlendirilmektedir. SOLID uluslararası çağrı sahteciliğini azaltma anlamında STIR ile birlikte değerlendirilmiş ve aynı kişiler arasında esnek ve güvenli iletişim için kullanılabileceği düşünülmüştür. Bu teorik yaklaşım ile, çağrı akışındaki tüm paydaşlarda herhangi bir kesinti olmaksızın sahtecilik ele alınabilecektir. Bu yaklaşımda, her şebeke bir SOLID Pod'a sahip olacaktır. Farklı katılımcılar başlatılan her çağrı için, başlatan şebeke kendi Pod'unda sadece hedef şebekenin erişim yetkisi olan alanda bir çağrı kaydı oluşturur ve bu çağrıya arama başlatma zamanı, arayan numara, aranan numara ve arama durumu gibi

önemli bilgileri kaydeder. Bilgileri anonimleştirerek iletir ve sonlandıran şebekede bu bilgiler edinilerek kayıtlar güncellenir. Arayanı doğrulamak ve akışın bütünlüğünü sağlamak için STIR protokolü kullanılmaktadır. Hâlihazırda herhangi bir operatör tarafından uygulamaya geçirilmemiş olsa da teoride faydalı olabileceği düşünülmektedir (Sambra vd., 2016; I3Forum, 2019).

2.5.3. Blok zinciri (blockchain)

DLT (Distributed Ledger Technology – Dağıtılmış Defter Teknolojisi), birden çok noktada birden çok katılımcı tarafından merkezi olmayan veri tabanı yönetimine olanak sağlayan bir protokoldür (Yli-Huumo vd., 2016; Yaga vd., 2019). DLT'de bulunan; süreçlerde güvence sağlama, güvenli değişmez varlıklar oluşturma ve akıllı sözleşmeler sunma özellikleri sayesinde numara veri tabanları oluşturma anlamında çok uygun olacağı düşünülmektedir. Blockchain ise bir tür DLT'dir. Art arda büyüyen blok zincirleri olarak düzenlenmiş ve dijital olarak kaydedilmiş verilerden oluşmaktadır. Her bir blok şifrelenerek bağlanmaktadır ve değiştirilmeye karşı sağlamdır. Numaralandırma yönetimi için uygulanması halinde telefon numaralarının dijital varlık olarak kullanılabilir, bu yönetime katılan tüm taraflar için işlevsellik sağlanmış olur ve sadece bazı eylemlerin izin verilen katılımcılar tarafından gerçekleştirilmesi sağlanabilir ve veriler güvenli ve şeffaf bir şekilde değiştirilebilir (ECC, 2022).

Blockchain iki taraf arasındaki işlemleri verimli, doğrulanabilir ve kalıcı bir şekilde kaydedebilen dağıtılmış bir defterdir. Opeatörlerin abonelerin kimlik bilgilerini ve sertifikaları hakkında bilgi paylaştığı kullanım durumu, yurt içi ve yurt dışı operatörler arasında oluşturulabilecek blockchain ekosistemi ve kullanıcı kimliğini doğrulamak için ortak anahtar sertifikalarının paylaşılması blockchainin bu sektörde uygulanabilmesi açısından önemli özelliklerdir. Ayrıca, ITU vb. kuruluşlar tarafından DLT'nin telekomünikasyon uygulamalarında kullanılması için çeşitli çalışmalar yürütülmektedir (ITU-T, 2019).

2.5.4. AB el sıkışması (AB handshake)

AB Handshake, operatörler arasındaki iş birliğine dayalı olarak gerçek zamanlı olarak sahteciliği tespit etmek ve şebekeler arasındaki trafiği doğrulayarak operatörler gurubu içindeki sahteciliği ortadan kaldırmak için kullanılan bir yöntemdir. Belirli bir ülke veya yönetmelikle doğrudan bağlantısı bulunmamaktadır ve bağımsız bir çözüm olarak ortaya çıkmıştır. Farklı coğrafi alanlarda bulunan operatörlerce canlı trafik doğrulaması için kullanılmakta ve operatörler aynı ülkedeki diğer operatörlerden bağımsız olarak bireysel şekilde hizmete bağlanabilmektedir. Çağrıyı başlatan taraf, çağrı bilgilerini kendi çağrı kayıt merkezine iletir ve HTTP vasıtasıyla sonlandıran tarafın çağrı kayıt merkezine doğru bir doğrulama isteği iletilir. Sonlandıran taraf çağrıyı aldıktan sonra çağrı bilgilerini kendi kayıt merkezine iletir. Bu kayıt, tahsisli numara veri tabanından kontrol edilerek arayan numaranın tahsisli olduğu operatöre doğrulama talebi ile gönderilir. Eğer bu numara sahteyse çağrı tamamlanmaz ve engellenir. Arayan tarafa çağrının sonlanan tarafa farklı bir CLI ile gitmiş olduğu bilgisi iletilir. Bu sayede çağrının sahte olduğu gerçek zamanlı olarak anlaşılabilir ve bu tür çağrılar engellenebilir. Arayan numaranın sahte olmaması durumunda arayan tarafa çağrının tamamlandığı bilgisi iletilir. Her iki taraftan da bilgilendirme gelmezse çağrı kesintisiz şekilde devam eder. Bu yöntem özel bir ticari girişim tarafından sunulmaktadır. Hem IP tabanlı hem de eski sistemlerde uygulanabilmekte ve şebekeleri ve çağrı akışlarını etkilemeden kullanılabilmektedir. Bu yöntemin uygulanabilmesi için numaralandırma planlarının paylaşılması ihtiyacı bulunduğundan, ilgili düzenleyici otoriteler ile entegrasyon ve koordinasyon kurulması gerekmektedir (GSMA, 2021).

3. ARAŞTIRMA YÖNTEMİ

Bu bölümde araştırma kapsamında verilerin nasıl ve ne şekilde toplandığı ve sonrasında bu verilerin hangi teknikler vasıtasıyla değerlendirildiği anlatılacak ve ilgili analizlere yer verilecektir.

3.1. Veri Toplama Yöntemi

Tezin önceki bölümlerinde yapılan araştırmalar ve edinilen bilgiler çerçevesinde hareket edilerek veri toplama tekniği olarak yarı yapılandırılmış görüşme tekniği kullanılmış ve ilgili taraflarla odak grup görüşmeleri gerçekleştirilmiştir.

3.1.1. Görüşme tekniği

Görüşme, sözel iletişim vasıtalarıyla insanları ve ilişkileri anlamaya olanak tanıyan veri toplama tekniklerinden birisidir. Görüşmeler; yapılandırılmış, yapılandırılmamış ve yarı yapılandırılmış görüşme olmak üzere üç başlıkta ifade edilebilmektedir. Araştırmacının görüşme öncesi bir takım sorular hazırlaması, bu soruların rehberliğinde görüşmeyi gerçekleştirirken bir yandan da ihtiyaç duyulduğunda daha derin şekilde konunun incelenebilmesi bakımından önceden hazırlanan sorular dışındaki konulara da değinilmesi ve bu sayede verilerin elde edilmesi yöntemi yarı yapılandırılmış görüşme olarak adlandırılmaktadır (Patton, 2002; Bernard, 2006; Gürbüz ve Şahin, 2018). Tez çalışmasının bu bölümünde yarı yapılandırılmış görüşme tekniği kullanılmıştır.

3.1.2. Görüşülen taraflara ilişkin bilgiler

Türkiye'de faaliyet göstermekte olan 3 adet mobil operatör bulunmaktadır. Tez çalışması kapsamında bu operatörlerden 2 tanesiyle görüşme gerçekleştirilmiştir. Görüşme gerçekleştirilemeyen operatörün ilgili temsilcileri ile irtibata geçilmiş görüşme soruları kendilerine iletilmiştir. Bununla birlikte, operatör Şirketlerinin gizlilik politikaları gereği görüşmeye katılmaktan imtina etmiştir.

Görüşme gerçekleştirilen operatörlerden bundan sonra “X” ve “Y” operatörü olarak bahsedilecektir. Her iki operatör de sektörde 2000’li yılların başlarından beri hizmet vermekte olup hem ülkemiz hem de dünya telekomünikasyon sektörü açısından önemli tecrübeleri bulunmaktadır. BTK tarafından yayımlanan son pazar verilerine göre X ve Y operatörleri mobil pazarın yaklaşık %70’ini temsil etmektedirler. Sabit ve mobil pazar birlikte düşünüldüğünde ise, tüm çağrı trafiğinin yaklaşık %98’ini mobil kaynaklı çağrılar oluşturmaktadır (BTK, 2021). Bu açıdan bakıldığında yapılan görüşmeler ile hedeflenen kesimin büyük oranda görüşlerinin alınmış olduğu değerlendirilmektedir.

X operatörü ile 16.06.2021 tarihinde ve Y operatörü ile de 30.06.2021 tarihinde görüşme gerçekleştirilmiştir. Görüşmeler bahse konu operatörlerin sahtecilik ekip yöneticisi ve sahtecilik ekibinin tecrübeli personellerinin de katılımıyla 3’er kişilik ekiplerden oluşan odak gruplar ile çevrimiçi olarak gerçekleştirilmiştir. Katılımcıların tamamı, en az 10 yıldır bu sektörde ve sahtecilik hususlarında çalışan ve hem alanlarında son derece yetkin hem de oldukça tecrübeli kişilerdir. Görüşmelere katılan personel sayısı ilgili şirketlerin kendi tasarrufları neticesinde şekillenmiştir.

Odak grubu, araştırma konusunu kişisel deneyimlerden yola çıkarak tartışmak ve yorum yapmak için araştırmacılar tarafından seçilen ve bir araya getirilen bir grup birey olarak ifade etmek mümkündür (Powell ve Single, 1996). Odak grup araştırmasının temel amacı, katılımcıların tutumlarını, duygularını ve deneyimlerini verimli şekilde gözlemleyebilmektir. Bu yolla daha kısa sürede daha fazla bilgi elde edinilebilmektedir (Morgan ve Krueger, 1993). Bir başka tanımda ise, odak grup görüşmelerinin önceden belirlenen bir konu için belirli katılımcıların düşüncelerini anlama yöntemi olarak ifade edilmektedir. Ayrıca görüşmelerde açık uçlu olacak şekilde ve yorum yapmaya müsait sorular ile sohbet ortamında bir tarz bulunmasının faydalı olacağı ifade edilmiştir (Krueger ve Casey, 2000; Arlı, 2013).

3.2. Görüşme Notları ve Değerlendirme

Görüşmelerde kullanılmak üzere hazırlanan ve aşağıda yer alan sorular için uzman kişilerden görüş alınmıştır. Görüşmede söz konusu sorular üzerinden ilerlenmiş ancak

zaman zaman ilgili olabilecek çeşitli konulara da değinilmiştir. Görüşmelerde kullanılan sorular şu şekildedir:

"1-Sektörde hangi sahtecilik (fraud) türleri ile karşılaşılmaktadır?
2-Son 5 yılda hangi sahtecilik tipleri yoğun olarak görülmektedir? Şirketinizce buna yönelik tutulan bir istatistik var mıdır?
3-Özel olarak ses çağrı trafiğine yönelik ne tür sahtecilikler / manipülasyonlar (CLI manipülasyonu vb.) yaşanmaktadır? Bu husus özelinde ne tür önlemler almaktasınız? Çözüm önerileriniz nelerdir? CLI manipülasyonu özelinde, manipülasyonun tam olarak hangi operatörde ve/veya hangi noktada yapıldığını nasıl tespit ediyorsunuz?
4- Sahteciliği önlemek için özel sistemler kullanıyor musunuz? Kullandığınız sistemler nelerdir? Kullanılan bu sistemlerin maliyeti ne kadardır ve bu sistemlerin güvenilirliği ve doğruluk oranı ne kadardır?
5-Son 5 yılda sahtecilik kaynaklı gelir kaybınız tahmini ne kadardır? (Yıllık bazda)
6-Önümüzdeki zamanlarda hangi sahtecilik senaryoları ile daha çok karşılaşılacağını öngörüyorsunuz?
7-Sahteciliğin önlenmesi noktasında, yapay zekâ, makine öğrenmesi vb. araçlar kullanarak insan faktörünün etkisini azaltmayı planlıyor musunuz / nasıl?
8-Sahtecilik sonrası ne tür kayıplar yaşamaktasınız? Bu kayıpları azaltmak için ne gibi aksiyonlar alıyorsunuz?
9-Sahteciliğin önlenmesi için BTK tarafından teknik, idari ve yasal olarak neler yapılması gerektiğini düşünüyorsunuz / beklentileriniz nelerdir?
10-Şirketinizce sahtecilik hususunda düzenlenmiş rapor / yayın bulunmakta mıdır?"

Görüşme soruları için operatörler yazılı olarak da geri dönüş yapmışlardır. Bu yazılı metinlere ilaveten görüşme esnasında tutulan notlar ve görüşme kayıtları da kullanılarak her bir soru ve konu için operatör görüşlerini temsil eden metinler oluşturulmuştur. Bu görüşme kayıtları, nitel araştırma analizlerinde kullanılan Nvivo programı vasıtasıyla analiz ve değerlendirmeye tabi tutulmuş olup değerlendirmelerde kullanılan kodlar; operatör cevapları, literatür araştırması bölümünde yer verilen genel çerçeve ve bunların birlikte değerlendirilmesi neticesinde oluşturulmuştur. Bu kodlar; *"CLI manipülasyonu, Simbox, STH, yurt dışı çağrı, yurt içi çağrı, CDR analizi, test çağrıları, mevzuat, Wangiri, IRSF, A numarası, B numarası, makine öğrenmesi, fraud sistemleri, büyük veri, yapay zeka,*

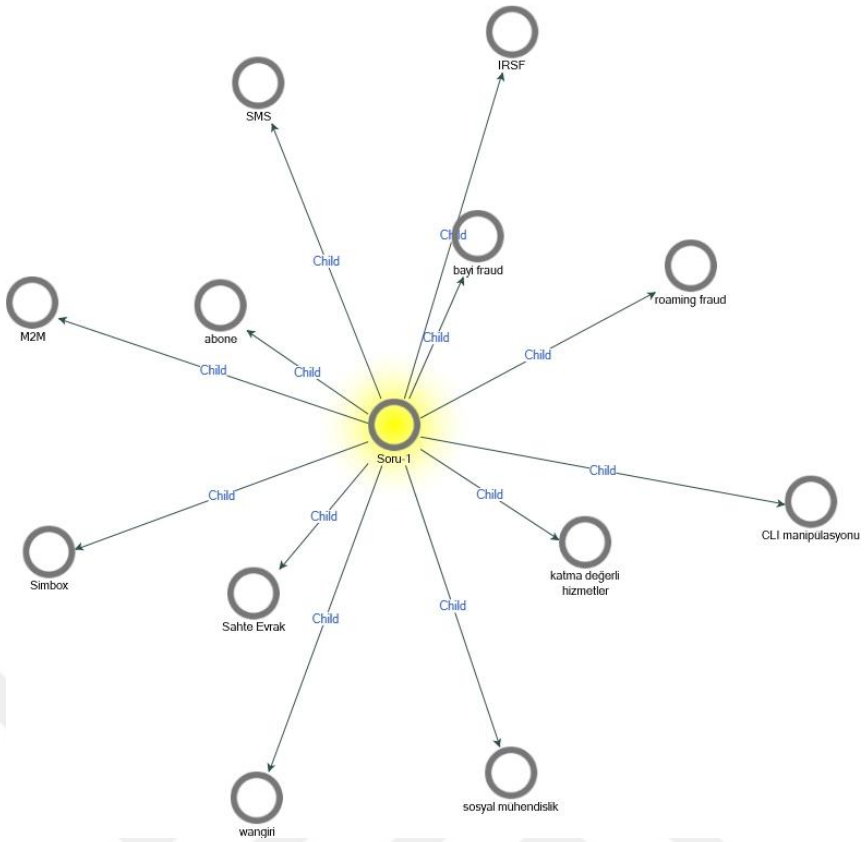
otomasyon, insan gücü, bayi fraud, abone, sahte evrak, SMS, M2M, bypass fraud, yüksek gelir, suni trafik, birlikte çalışılabilirlik, denetim, yasal düzenleme, ortak zemin, gelir kaybı, sosyal mühendislik, roaming fraud, simswap fraud" şeklindedir.

Görüşmelere ilişkin analiz ve değerlendirmelere aşağıda yer verilmektedir.

3.2.1. Sektörde hangi sahtecilik türleri ile karşılaşıldığına ilişkin soru

Operatörlerin verdikleri cevaplar hem birbirleri ile hem de dünyadaki durum ile örtüşmektedir. X operatörü tarafından iletilen; *"... sahtecilik vakalarının yaklaşık olarak %95'inin sabit ve mobil tarafta gerçekleştiği ..."* ifadesi ile, genişbant internet pazarında yaşanan sahteciliğin oldukça az olduğu ve sahtecilik noktasında harcanacak emeğin yoğun olarak mobil ve sabit pazara yöneltilmesinin daha anlamlı olacağı düşünülmektedir. Yine X operatörünün; *"... vatandaşa dokunan en net noktaların bayiler olması nedeniyle ..."* ifadesi kapsamında bayilerin sektörde önemli bir yer tuttuğu ve doğrudan tüketiciler ile iletişimleri olması nedeniyle hem sahtecilik açısından birincil kaynak olabildikleri hem de tam tersi güven anlamında önemli katkı sağlayabilecekleri ve bu anlamda sahteciliğin önlenmesi noktasında önemli yer tutabilecekleri düşünülmektedir. Bununla birlikte, Y operatörü ise ilettiği; *"... CLI'ın yanlış ve yanıltıcı şekilde değiştirilmesi suretiyle yurt dışından gelen çağrıların yurt içi çağrı olarak gösterilmesi ..."* ifadesi ile, CLI manipülasyonu konusunda sorunlar yaşadıklarını ifade etmiş olup bu çerçevede bu tip çağrılar ile manipülasyon yapılmasının önüne geçilmesi için çaba harcanması gerektiği değerlendirilmektedir. Ayrıca, yine Y operatörü tarafından iletilen *"... sabit telefon hizmeti sunan operatöre çağrı sonlandırma ücreti kazandırmak için geçerli olmayan hatlara yapılan yoğun aramalar sebebiyle oluşan suni trafik ..."* ifadesiyle Wangiri sahteciliğine dikkat çekilmiş ve bu sahtecilik yönteminin de önemli ölçüde karşılaşılan sorunlardan olduğu ve çözümü için adımlar atılmasının faydalı olacağı belirtilmiştir.

Bu soruya operatörlerce verilen cevapların özet durumuna Şekil 3.1'de yer verilmektedir.



Şekil 3.1 Sektörde yoğun karşılaşılan sahtecilik türleri

Yukarıda görüldüğü üzere X ve Y operatörlerinin verdikleri cevaplara göre yapılan kodlamalarda en sık karşılaşılan sahtecilik türleri bu şekilde sıralanmaktadır. Burada merkeze en yakın sahtecilik çeşidi (bayi ve abone sahteciliği) görüşme notlarında en sık şekilde adı geçen sahtecilik türü olarak belirtilmektedir. Merkeze en yakın olan ifadeler en sıklıkla değinilen ifadeler olarak karşımıza çıkmaktadır. Operatörlerce belirtilen bu sahtecilik türlerinden (veya kodlardan) bazılarının birbirleriyle ilişkisi bulunmaktadır. Örneğin, sahte evrak sahteciliğinin en çok bayiler üzerinden gerçekleştiği ve bayi sahteciliğinin bir alt dalı olarak da kabul edilebileceği değerlendirilmektedir. İki operatörün de öne çıkardığı sahtecilik türleri incelendiğinde, uluslararası anlamda da kabul gören durumla Türkiye'deki sahtecilik senaryoları arasında önemli derecede benzerlik ve paralellik olduğu görülmektedir. CLI manipülasyonu, Simbox, Wangiri, IRSF ve abone sahtecilikleri bunların önemli örnekleridir. Bunun yanında, katma değerli hizmetler, M2M (Machine-to-Machine) ve sosyal mühendislik konularında da çok yoğun olmamakla birlikte sahtecilik yaşandığı görülmektedir. Her iki operatör tarafından da yoğun şekilde öne çıkarılan sahteciliklere detaylı bakıldığında ise, diğer sahtecilik hususlarında hem

teknolojide yaşanan gelişmeler hem operatör yatırımları hem de BTK düzenlemeleri ile önlem noktasında önemli gelişim yaşandığı belirtilmekte ancak özellikle CLI manipülasyonu konusunda ciddi sorunlar yaşandığı ve bunun çözümü noktasında gelişme kaydetmekte zorlanıldığı ifade edilmektedir.

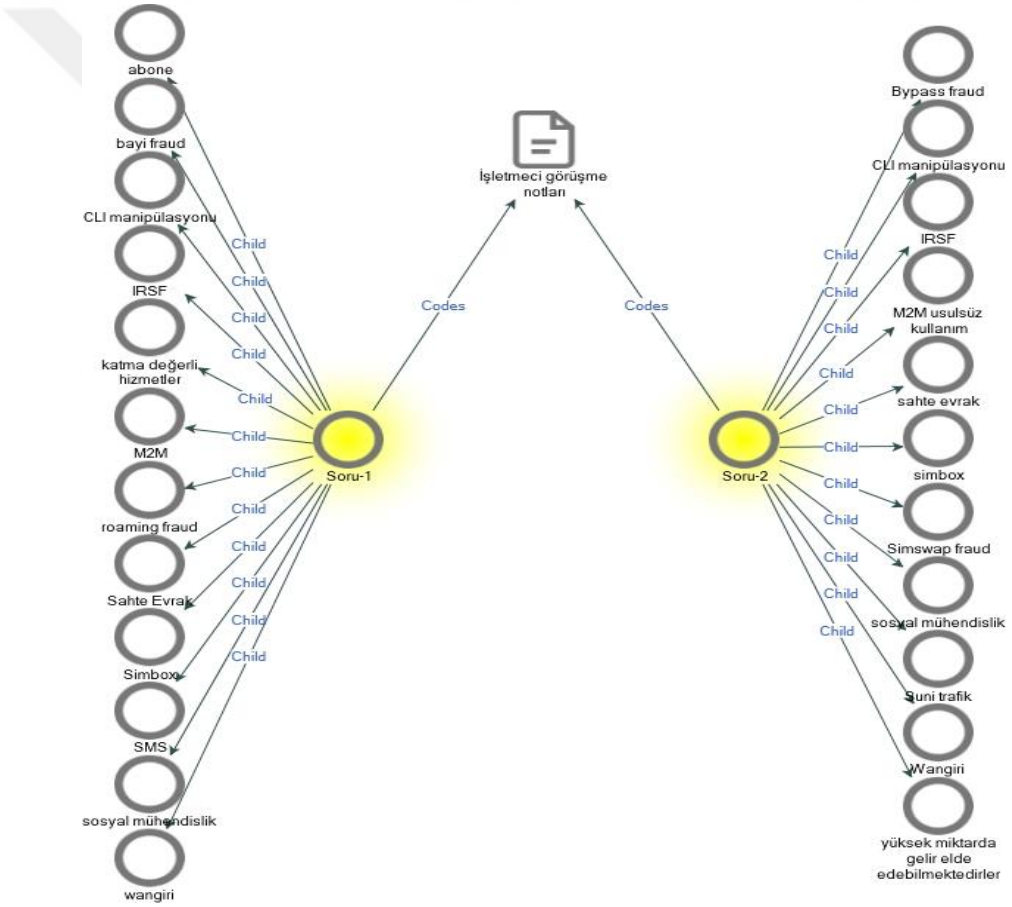
3.2.2. Son 5 yıldaki sahtecilik türlerine ilişkin soru

Bu kısımda operatörlerin cevapları da bir önceki soru ile benzeşmekte ancak son dönemde değişmekte olan durumları da yansıtmaktadır. Örneğin X operatörünün; *"... bypass sahteciliği ise her zaman benzer yoğunlukta devam etmektedir ..."* ifadesi ile Simbox ve CLI manipülasyonu gibi sahteciliklerin her zaman yoğun şekilde yaşandığı ve bir azalma olmadığı belirtilirken, *"... Wangiri sahteciliği son 1,5-2 yılda önemli ölçüde artmış ..."* ifadesi ile bu tip sahteciliğin son dönemlerde arttığı ve *"... Simswap sahteciliği diye yeni bir yöntem ..."* ifadesi ile de hem dünyada hem de ülkemizde daha önce gerçekleşmeyen bir sahtecilik yönteminin yeni yeni uygulanmaya başladığı ifade edilmiştir. Y operatörü tarafından ise; *"... bu sahtecilik tipleri içerisinden en yoğun karşılaşılan sahtecilik tipi ise sahte evrak düzenlenmesi usulüyle ..."* ifadesi öne çıkarılmış ve bayiler üzerinden gerçekleştirilen abonelikler noktasında çok fazla sayıda sahte evrak işlemi yaşanmaya başladığı belirtilmiştir. Bu kapsamda bakıldığında öne çıkmaya başlayan ve yeni yeni ortaya çıkan sahtecilik hususlarının da önemle incelenmesi ve dikkate alınması gerektiği düşünülmektedir.

Bu soruya verilen cevapların kodlanması ile elde edilen sonuçlar incelendiğinde bir önceki sorudaki cevaplarla önemli benzerlikler olduğu görülmektedir. Örneğin, bayi sahteciliği ve sahte evrak sahtecilikleri her iki soruda da en yoğun şekilde karşımıza çıkmaktadır. Yine Simbox ve CLI manipülasyonunun da yoğun şekilde karşılaşılan sahteciliklerden olduğu görülmektedir. Bununla birlikte, bazı farklılıklar da göze çarpmaktadır. Örneğin sosyal mühendislik vakalarının ve usulsüz M2M kullanımının artmaya başladığı anlaşılmaktadır. Sahte evrak sahteciliklerinin yoğun şekilde yaşanmasının temel nedeninin bayiler üzerinden yapılıyor olması olduğu değerlendirilmektedir. Tüm Türkiye'ye yayılmış geniş bayi ağı olan X ve Y operatörlerinin tüm bayilerde kontrolü aynı şekilde sağlaması oldukça zor olduğundan ve bayilerin prim sistemi ile çalışması nedeni ile daha fazla gelir elde etmeye eğilimi olmasından dolayı bu sahtecilik türü her zaman yoğun

şekilde yaşanmaktadır. Bununla birlikte, son dönemlerde yaşanan dijital dönüşüm ve benzeri gelişmelerle birlikte, BTK tarafından yapılan ve elektronik ortamda kimlik doğrulamasına imkân tanıyan bu kapsamdaki Elektronik Haberleşme Sektöründe Başvuru Sahibinin Kimliğinin Doğrulanma Süreci Hakkında Yönetmelik ve benzeri bazı düzenlemelerin de katkısıyla elektronik ortamda yapılan işlemlerin önemli ölçüde artmasıyla bu sorunun önemli ölçüde azalacağı görüşünün her iki operatöre de hâkim olduğu gözlemlenmektedir.

İlk iki soru arasındaki benzerlik, Nvivo programı ile yapılan kodlamaların karşılaştırılması üzerinden oluşturulan ve aşağıda yer verilen Şekil 3.2'deki görsel ile de desteklenmektedir.



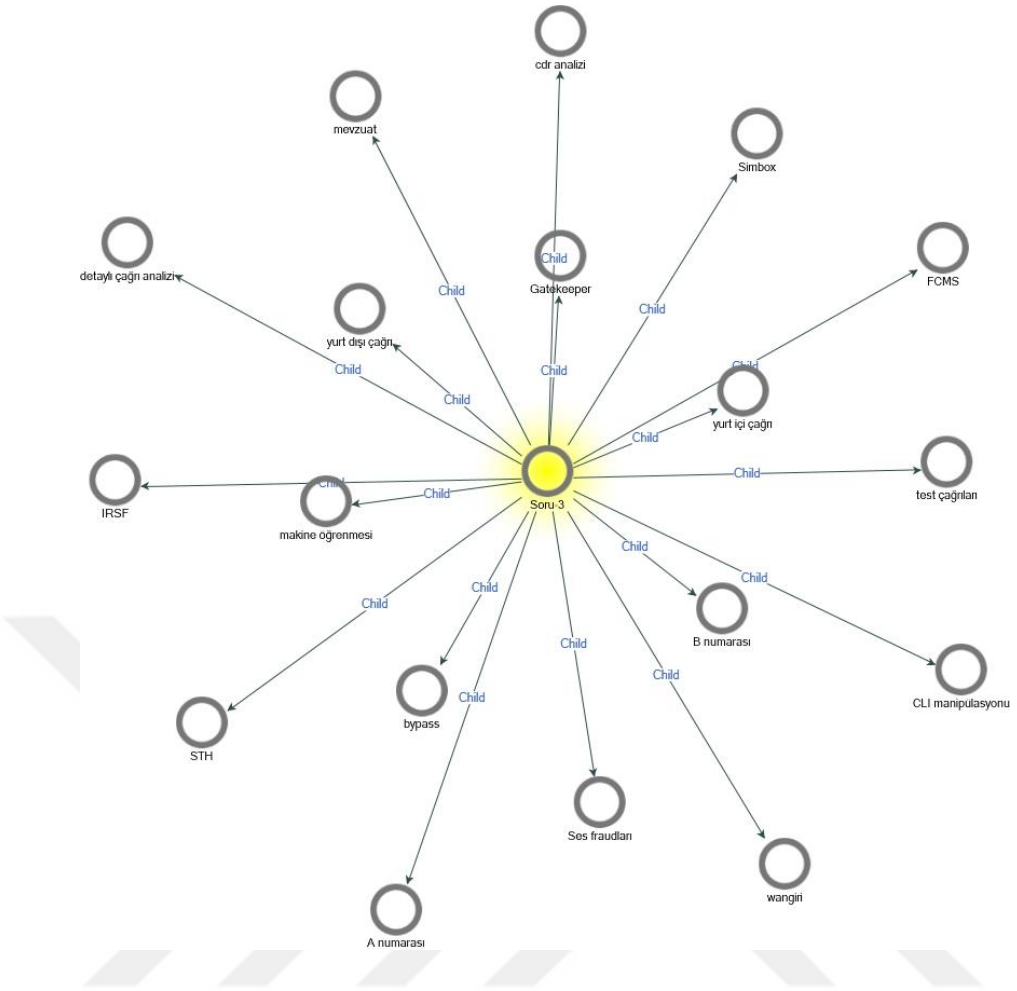
Şekil 3.2 İlk iki soru karşılaştırması

Şekilden de görüleceği üzere genel olarak karşılaşılan sahtecilik türlerinin pek çoğunun son dönemde de yaşanmaya devam ettiği her iki soruya yönelik cevaplarla oluşturulan kodlardan anlaşılabilmektedir. Bunun yanında, Simswap sahteciliği gibi yeni

ortaya çıkmaya başlayan bazı sahtecilik türlerinin de olduğu görülmektedir. Simswap sahteciliği ile sadece kişinin sim kartı değil pek çok kimlik bilgisi ele geçirilerek genellikle bankacılık sahtecilikleri gerçekleştirilmektedir (The Guardian, 2020). Bununla birlikte, X operatörü tarafından ülkemizde sim kart değişikliği sonrası bankalarca uygulanan bloke işleminin bu soruna karşı etkili bir çözüm yöntemi olduğu belirtilmiştir.

3.2.3. Ses çağrı trafiği ve CLI manipülasyonuna ilişkin soru

Bu soruda ise özel olarak ses çağrı trafiğine yönelik ne tür sahtecilik ve manipülasyonların yaşandığı ve bu husus özelinde ne tür önlemler alındığı sorulmuştur. İlaveten bu konuya yönelik çözüm önerileri ile yukarıda da yoğun şekilde yaşandığı ve çözüm noktasında sorun yaşandığı belirtilen CLI manipülasyonu özelinde, manipülasyonun tam olarak hangi operatörde ve/veya hangi noktada yapıldığının nasıl tespit edildiği sorulmuştur. X operatörü tarafından; *"... ses sahtecilikleri, Wangiri, bypass (Simbox ve CLI manipülasyonu), IRSF ... bypass sahteciliklerinde tespit için iki temel yöntem bulunmaktadır; test çağrıları ve CDR analizi ..."* ifadeleri kullanılmıştır. Bu kapsamda, CLI manipülasyonu özelinde test çağrıları ve CDR analizi yöntemlerinin etkili çözümlerden olduğu anlaşılmakta, ancak *"... ilgili STH operatörünün bu sahtecilikten benim haberim yok abonem yapmış olabilir dediği durumlarda ilgili mevzuat açısından ve yaptırımın uygulanacağı taraf bakımından çıkmaz sokağa girilebilmektedir ..."* ifadelerinden ise bu tespitler ve çözümler noktasında operatörün yasal düzenleme ve yaptırım noktasında desteğe ihtiyacı olduğu anlaşılmakta ve kamu otoritesinin bu anlamda çalışma ve düzenleme yapmasının faydalı ve anlamlı olabileceği değerlendirilmektedir. Y operatörü tarafından ise; *"... bazı şirketler üzerinden taşınan çağrılarda manipülasyonların yoğunlaşması ise bu şirketlerin detaylı olarak incelenmesine ihtiyaç olduğu ... Şirketimiz tarafından (ve CLI manipülasyonuna maruz kalan diğer mobil operatörler tarafından) manipülasyon yaptığı tespit edilen numaralara ait trace log (izleme günlüğü) kayıtlarının BTK tarafından ilgili operatörlerden temin edilmesinin ve incelenmesinin faydalı olacağı ..."* hususları ifade edilmiş ve yine X operatörüne benzer şekilde kamu gücünün desteğine ihtiyaç duyulduğu ve şüpheli davranışları bulunan operatörlere yönelik denetimlerin sıklaştırılmasının faydalı olacağı belirtilmiştir. Bu soruya verilen cevapların Nvivo ile kodlanması ile oluşturulan görsele Şekil 3.3'te yer verilmektedir.



Şekil 3.3 Ses çağrısı sahtecilikleri, çözüm önerileri ve CLI manipülasyonu

Operatör görüşleri ve kodların analiz edilmesi sonucunda, ilgili soruda ses çağrılarında ne tür sahtecilikler bulunduğu sorulmuş olup şekle bakıldığında CLI manipülasyonu, Simbox, IRSF ve Wangiri sahteciliklerinin belirli oranlarda dile getirildiği görülmektedir. Bu bölümde en çok değinilen sahtecilik CLI manipülasyonu olarak görülmektedir. Bu açıdan bakıldığında, ses çağrısı sahteciliklerinde CLI manipülasyonunun önemli bir yer tuttuğu sonucu çıkarılabilmektedir. Bu yöntemin özellikle yurt dışı çağrıların sanki yurt içinden başlatılıyormuş gibi gösterilmesi yoluyla yapıldığı belirtilmiş ve bu sayede sonlandırma ücretlerinin düşük ödendiği ifade edilmiştir. Yine şekilden görüldüğü üzere STH operatörlerinin de çoğu zaman bu yöntemin önemli bir unsuru olduğu anlaşılmaktadır. CLI manipülasyonunun yaşandığı çağrıların genellikle STH operatörlerinde başlayıp (çoğunlukla yurt dışında başlamasına rağmen CLI manipüle edildiği için bu çağrılar yurt içinde başlamış gibi görünmektedir) mobil operatörlerde sonlanmaktadır. İlgili çağrı olması gerektiği gibi yurt dışı çağrı olarak kayıtlara geçerse STH operatörünün mobil operatöre 0,11

Euro civarında bir sonlandırma ücreti ödemesi gerekmektedir. Ancak ilgili çağrı yurt içi çağrısı olursa bu ücret 5 kuruş civarında olmaktadır. Bu çerçeveden bakıldığında CLI manipülasyonu yapılarak önemli bir gelir kaybının mobil operatörlerde yaşanmakta olduğu ve STH operatörüne de haksız kazanç olarak yansıdığı anlaşılmaktadır. Dolayısıyla bu problemin çözümünün önemli oranda bir haksızlığı ve gelir kaybını gidereceği anlaşılmakta ve değerlendirilmektedir.

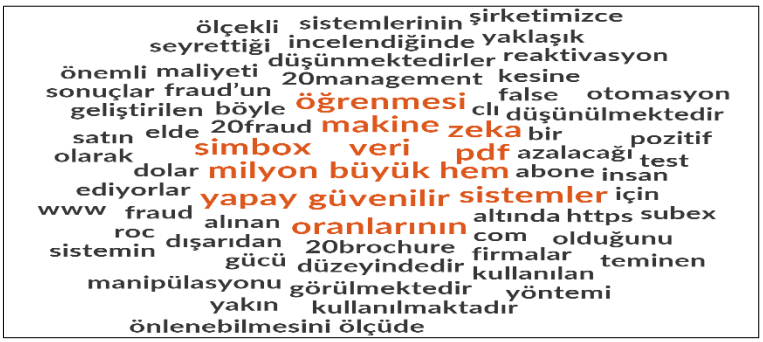
Önlemler noktasında operatörlerin yaptıklarına bakıldığında, çağrıların detaylı şekilde analiz edilmesi, benzer şekilde CDR analizlerinin yapılması ve test çağrısı yapılması yöntemlerinin öne çıktığı gözlemlenmiştir. Bu yöntemlerden kısaca bahsedilmesi gerekirse, detaylı analizlerde belirli bir dönem veya çok uzun dönemde elde edilen CDR verileri üzerinden yapılan incelemelerde ve algoritmik analizlerde belirli tip çağrılarda ve belirli STH operatörlerinden başlayan çağrılarda CLI manipülasyonu yapıldığının tespit edilebildiği görülmektedir. İlgili çağrıların hem arayan (A numarası) hem de aranan (B numarası) numaraları üzerinden çağrı profilleri oluşturularak bu çağrı profilindeki çağrıların zaman zaman yurt dışından bazen de yurt içinden geldiğinin gözlendiği ve bu sayede de manipülasyonun tespit edilebildiği ifade edilmiştir. Bu tespitlerin ilgili STH operatörleri ile paylaşıldığı ancak zaman içerisinde numaraların son hanelerinin vb. değiştirilerek benzer profildeki çağrı akışlarının yinelediğinin görüldüğü iletilmiştir. Operatörlerce, bu durumun bazı STH operatörlerinde zaman zaman önemli ölçüde yoğunlaştığı ve bu STH operatörlerinin bu yolla mevzuatı ihlal ettiğinin değerlendirildiği ifade edilmiş ve BTK tarafından bu operatörler nezdinde detaylı incelemeler yapılmasının faydalı olacağı belirtilmiş ancak bunun da tam anlamıyla sorunu ortadan kaldırmayabileceğinin düşünüldüğü iletilmiştir. Bir diğer yöntem olan test çağrılarında ise bazı şirketlerden hizmet alımı yapıldığı, gerçek numaralar vasıtasıyla yurt dışından belirli B numaralarına doğru test çağrılarının gerçekleştirildiği, çağrının abonenin telefonunda çalmadan sonlandırıldığı ancak CDR verisinin oluşturulduğu ve sonrasında da bu CDR verisi üzerinden CLI manipülasyonu kontrolünün sağlandığı ifade edilmiştir.

Operatörlerin çözüme yönelik görüşleri ise şu şekilde ifade edilmektedir. Sorunun temel olarak operatör ekosistemindeki aktörler arasında yaşanan bir durum olduğu, bu anlamda BTK'nın çözüm açısından rolünün önemli olacağı, hem sorunun yaşandığı operatörler özelinde detaylı denetim ve incelemelerin yapılmasının hem de yukarıda ifade

edilen tespit ve analiz yöntemlerinin BTK bünyesinde veya BTK'nın dâhil olacağı ve herkese eşit mesafede olacak bir mekanizma ile sorunun aşılabileceği belirtilmiştir. Ayrıca, ilgili mevzuatın da güncellenmesi ve sahtecilik gerçekleştiren operatörün ve diğer tüm operatörlerin gerekli tedbirleri alması, abonelerinin sahtecilik gerçekleştirmesi halinde aboneliği sonlandırması ve tekraren ihlal halinde daha ağır yaptırımların uygulanması hususunun da faydalı olacağına değinilmiştir.

3.2.4. Sahteciliği önlemek için kullanılan sistemlere ilişkin soru

Sahteciliği önlemek için özel sistemlerin kullanılıp kullanılmadığına ve yaklaşık maliyetlerine ilişkin soruya yönelik olarak operatörlerce sahtecilik tespiti ve önlenmesi için pek çok sistem kullanıldığı, bunların bazılarının iç kaynak bazılarının ise yurt dışından satın alınan sistemler olduğu, bu sistemlerin bir ekosistem şeklinde birlikte çalışabildiği ve kullanılan akıllı sistemler ve elde edilen büyük veri sayesinde de tespitlerin kesine yakın şekilde gerçekleştirildiği belirtilmiştir. X operatörü tarafından yurt dışı menşeili yeni bir sisteme geçilmesi üzerinde çalışmaların devam ettiği belirtilmiş, Y operatörü tarafından ise sistemlerin çoğunluğun iç kaynaklarla sağlandığı ve ayrıca CLI manipülasyonu, Simbox vb. gibi çeşitli yöntemler için farklılaşmış ve özelleştirilmiş sistemlerin kullanıldığı belirtilmiştir. Her iki operatör tarafından da sistemlerin kullanılan yapay zekâ vb. akıllı sistemler sayesinde önemli derecede güvenilir olduğu ifade edilmiştir. Ayrıca X operatörü tarafından Türkiye'deki mobil operatörler ölçeğindeki bir operatörün kuracağı sistemin maliyetinin resmi bir değer olmamakla birlikte yaklaşık olarak 2-3 milyon dolar olduğu belirtilmiştir. Operatörlerin bu soru kapsamında verdikleri cevaplar neticesinde oluşturulan kelime bulutu görseline Şekil 3.4'te yer verilmektedir.



Şekil 3.4 Sahtecilik sistemlerine ilişkin kelime bulutu

3.2.5. Son 5 yıldaki sahtecilik kaynaklı gelir kaybına ilişkin soru

Her iki operatör tarafından da hem şirket politikası olarak hem de keskin şekilde böyle bir hesaplama yapılmasının tam mümkün olmaması nedeniyle resmi ve kesin bir tutar bilgisi iletilememiştir. Bununla birlikte, X operatörü tarafından ülkemizdeki mobil operatörlerin ölçeğindeki bir operatörün sahtecilik kaynaklı yıllık gelir kaybının 10 milyon TL'den az olmayacağı belirtilmiştir. Y operatörü tarafından ise yılda 60-100 milyon TL aralığında oluşabilecek sahtecilik kaynaklı gelir kayıplarının Şirketlerince önlendiği ve ayrıca abonelik ve sahte evrak kaynaklı yıllık gelir kayıplarının da tahmini olarak 20-30 milyon TL civarında olduğunun düşünüldüğü ifade edilmiştir.

3.2.6. Sahteciliğe yönelik olarak öngörülere ilişkin soru

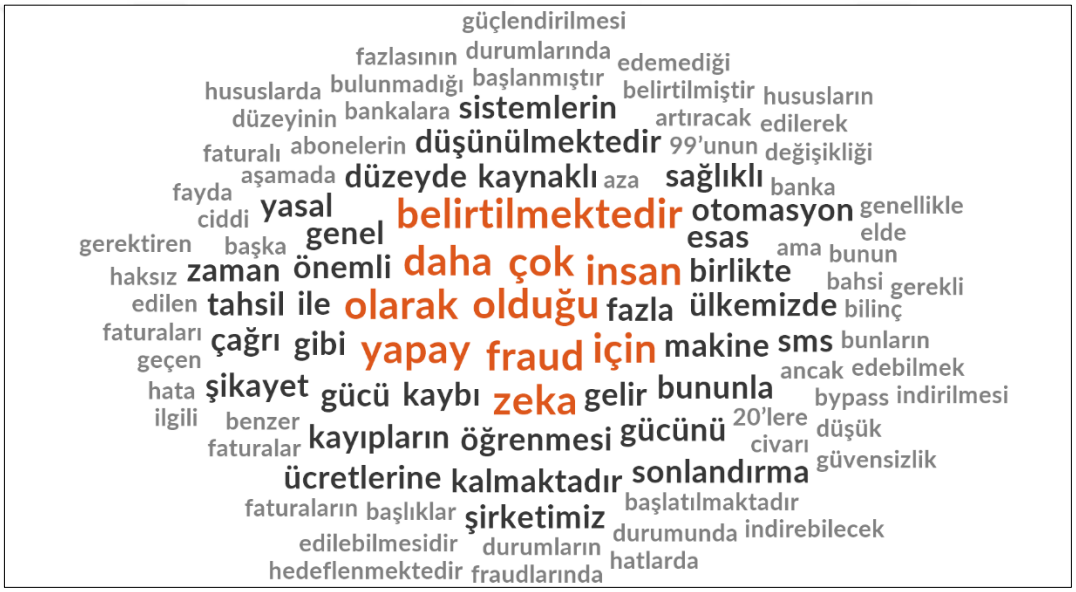
Her iki operatör de sosyal mühendislik kaynaklı sahtecilik vakalarının ilerleyen dönemlerde daha çok artmasının beklendiğini ifade etmiştir. X operatörü tarafından ilaveten SMS oltalama (phishing) yöntemlerinin, Y operatörü tarafından ise CLI manipülasyonu, Simbox ve akıllı telefonlar üzerinden gerçekleştirilen malware (zararlı yazılım) ataklarının önümüzdeki dönemde artabileceği belirtilmiştir.

3.2.7. Yapay zeka vb. yöntemlerin kullanımına ilişkin soru

Her iki operatör tarafından da sahteciliğin önlenmesi noktasında yapay zekâ, makine öğrenmesi vb. yöntemlerin önemli ölçüde kullanıldığı, bunun yanında robotik otomasyon süreçlerinin önemli ölçüde arttırılarak insan gücünden maksimum verim alınmaya çalışıldığı belirtilmiştir. X operatörü tarafından yapay zekâ kullanımının hâlihazırda %5 civarında olduğu ve bunun ilerleyen dönemlerde %20 civarına çıkarılmasının planlandığı ancak temel hedefin teknoloji kullanımından maksimum verim almak ve sahtecilik yönetimini kendi ekiplerinin kontrolünde devam ettirmek olduğu ifade edilmiştir. Y operatörü tarafından ise bazı sahtecilik türlerine özel yapay zekâ çözümlerini geliştirildiği ve yapay zekâ kullanımının ilerleyen dönemlerde arttırılmasının planlandığı belirtilmiştir.

3.2.8. Sahtecilik sonrası yaşanan kayıplara ilişkin soru

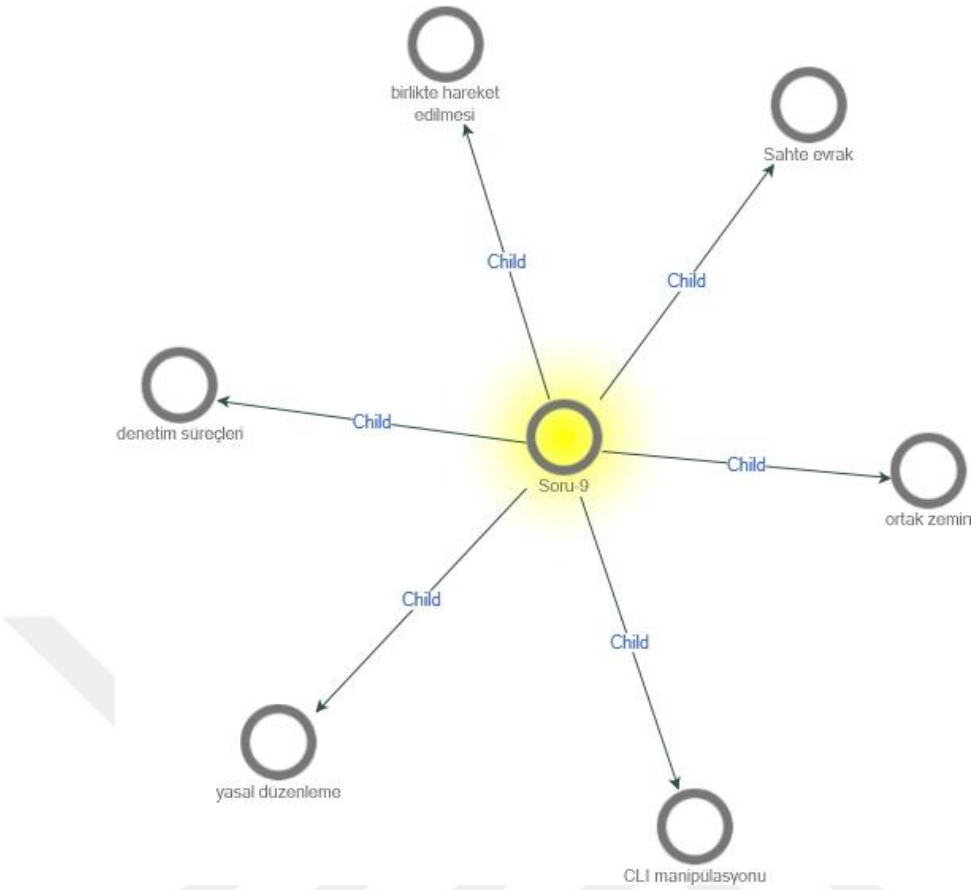
Sahtecilik sonrası ne tür kayıplar yaşandığı ve bu kayıpların azaltılması için ne gibi önlemler alındığına ilişkin olarak her iki operatör de sahtecilik sonrası yaşanan en önemli kaybın gelir kaybı olduğunu belirtmiştir. Bununla birlikte, X operatörü tarafından ülkemizde sahteciliğe ilişkin farkındalık düzeyinin az olduğu sadece banka kaynaklı gelir kayıplarında şikâyetçi olunduğu ve ayrıca sahtecilik kaynaklı kayıpların %99'unun gelir kaybı olduğu belirtilmiştir. Y operatörü tarafından ise fatura tahsisli, CLI manipülasyonu, Simbox vb. yöntemlerin tamamında gelir kaybı yaşandığını ve kayıpları azaltmak için yapay zekâ kullanımının arttırılmasının planlandığını ifade etmiştir. Bu soruya verilen cevaplar çerçevesinde oluşturulan kelime bulutu görseline Şekil 3.5'te yer verilmektedir.



Şekil 3.5 Sahtecilik kayıplarına ilişkin kelime bulutu

3.2.9. Teknik, idari ve yasal beklentilere ilişkin soru

Sahteciliğin önlenmesi için BTK tarafından teknik, idari ve yasal olarak neler yapılması gerektiğini düşündükleri ve beklentilerine ilişkin soruya verilen cevapların özet durumuna Şekil 3.6'da yer verilmektedir.



Şekil 3.6 BTK'nın yapması gerekenler ve beklentiler

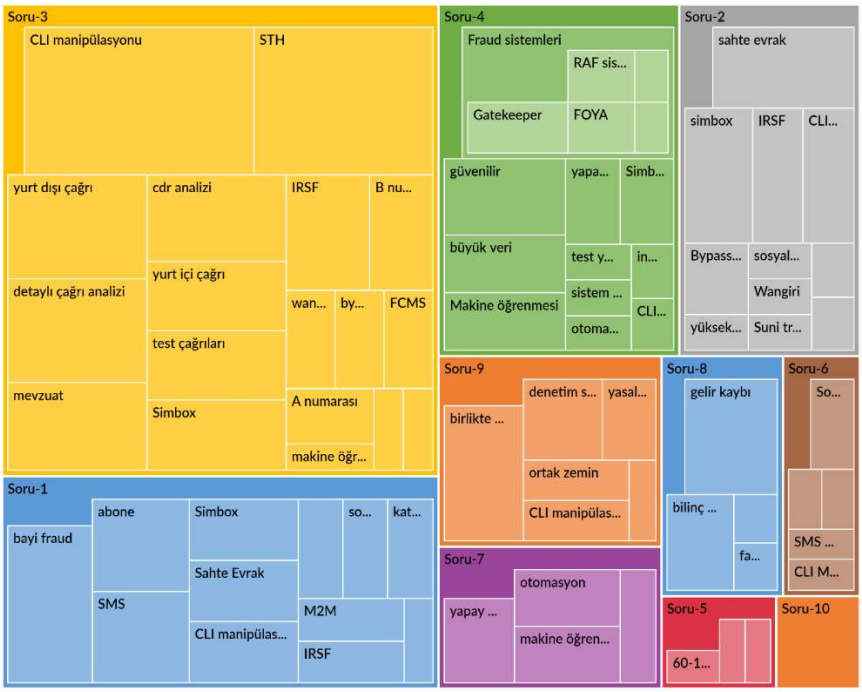
Her iki operatör tarafından da ortak olarak dile getirilen hususlar, özellikle CLI manipülasyonu için STH operatörlerine yönelik denetimlerin arttırılması, sahteciliğe neden olan ya da gerçekleştiren STH operatörlerine karşı ağır yaptırımların uygulanması, operatörlerin ve BTK'nın birlikte hareket edebileceği ortak bir zemin oluşturulması, gerekli yasal düzenlemelerin yapılması ve sahtecilik ile bu sayede birlikte mücadele edilmesi olarak görülmektedir. Ayrıca her iki operatör de sahteciliğe karşı pek çok önlem almalarına rağmen tamamen önüne geçmenin mümkün olmadığı ama ekosistem olarak birlikte hareket edilmesi halinde önemli ölçüde önlenebileceğini ifade etmişlerdir. İlaveten Y operatörü tarafından kimlik doğrulama, adres kontrolü vb. hususlarda dijitalleşmenin önünün açılması ve süreçlerin hızlandırılması gerektiği belirtilmiştir.

3.2.10. Düzenlenen raporlara ilişkin soru

Sahtecilik hususunda düzenlenmiş rapor veya yayın bulunup bulunmadığına ilişkin soruya ise her iki operatör de resmi olarak böyle bir rapor veya yayın bulunmadığı şeklinde cevap iletmiştir.

3.3. Görüşmelerin özeti

Gerçekleştirilen görüşmeler oldukça verimli geçmiştir. Hem sorulan sorular çerçevesinde hem de genel olarak sahteciliğe yönelik hususlarda sektör temsilcilerinin bakış açıları detaylı şekilde alınmış ve değerlendirmeler ile birlikte teze aktarılmıştır. Operatörler tarafından aktarılan hususların detaylarına yukarı kısımlarda yer verilmiştir. Bununla birlikte, bazı hususların öne çıktığı görülmektedir. Özellikle CLI manipülasyonu konusunda yaşanan sorun konusunda önemli bir çözüm beklentisi bulunduğu düşünülmektedir. Bu noktada sektörün tüm paydaşlarının yer aldığı ortak bir çözümün ise elzem olduğu değerlendirilmektedir. Bununla birlikte diğer alanlarda da çözüm beklentileri, düşünceler ve çözüme ilerleme noktasında olası öneriler de dile getirilmiştir. Gerçekleştirilen yarı yapılandırılmış görüşmelere ilişkin kayıtlar ve oluşturulan kodlar çerçevesinde Nvivo programında oluşturulan genel özet görsele Şekil 3.7'de yer verilmektedir.



Şekil 3.7 Görüşme özet durumu

Bu görselde de en büyük alanı kaplayan kısım en çok dile getirilen ve kodlara en çok karşılık gelen alanları işaret etmektedir. Şekilden görüldüğü ve yukarıda da ifade edildiği üzere 3'üncü soruda yer alan CLI manipülasyonu hususu operatörlerin de en çok değindiği ve sorun yaşadığı alanlardan olduğu anlaşılmaktadır. Bunun yanında, ilk iki soruda yer alan genel sahtecilik türlerinin de sıklıkla ifade edildiği görülmüştür. Ayrıca kamu otoritesinden beklentilere ilişkin 9'uncu sorunun da genel olarak önemli bir yer tuttuğu ve bu noktada bir düzenleme, çalışma ve/veya sektörü bir araya getirebilecek her türlü hususun faydalı olacağının ifade edildiği görülmüştür. Ayrıca görüşme kapsamında operatörlerce verilen cevaplar ışığında oluşturulan ve hem cevapları hem de kodları simgeleyen kelime bulutu görseline Şekil 3.8'de yer verilmektedir.

Şekil 3.8 Görüşmelere ilişkin kelime bulutu

4. DEĞERLENDİRME/TARTIŞMA VE ÖNERİLER

Bu bölümde, tez çalışmasının daha önceki kısımlarında gerçekleştirilen çalışmalar ve yapılan araştırmalar ve görüşmeler ışığında çeşitli değerlendirmeler ve tartışmalar yapılarak çeşitli öneriler sunulmaya çalışılacaktır.

4.1. Sahteciliğin Kaynağı ve Nedenleri

Sahtecilik çok büyük oranda haksız şekilde gelir veya kazanç elde etmek için gerçekleştirilmekte, bununla birlikte zaman zaman da başka zararlar vermek veya edinimler elde edebilmek için de yapılabilmektedir. Bu bağlamda, telekomünikasyon sahtecilik sorunu özelinde konuya yaklaşılınca daha önce de bahsedildiği üzere pek çok sahtecilik türü ve vakası bulunmaktadır. En yaygın şekilde karşılaşılanlar ise; Simbox, CLI manipülasyonu, IRSF, Wangiri, abone sahteciliği, PBX ele geçirme olarak görünmektedir. Bu bakımdan, ülkemizde, dünyada ve literatürde yer alan sahtecilikler açısından önemli bir benzerlik ve uyum görünmektedir. Bu çerçeveden bakıldığında, coğrafya bazlı çeşitli ayrımlar olabilmekle beraber sahteciliğe ilişkin hususlarda tüm dünyaya yaygın modeller ortaya koymanın pek çok açıdan sağlıklı ve anlamlı olacağı değerlendirilmektedir.

Telekomünikasyon sahteciliğinin arkasında da farklı nedenler yatabilmektedir. Operatörlerle gerçekleştirilen görüşmeler ele alındığında, örneğin CLI manipülasyonunun arkasında yurt dışı kaynaklı çağrılar için yüksek sonlandırma ücreti ödemek yerine yurt içi çağrı gibi gösterip düşük sonlandırma ücreti ödeme motivasyonu yatmaktadır. Yine yukarıdaki bölümlerde yer verilen dünya ülkelerinin yaşadığı CLI manipülasyonu vakalarına bakıldığında çağrı ekosisteminde yer alan bir operatörün bile kontrol altında veya iş birliği içinde olmamasının bu tür vakalar açısından son derece kritik olduğu ve çağrıların başlatıldığı andan sonlandığı ana kadar bir bütünlük ve netlik içerisinde ilerlemesi gerektiği pek çok ülke tarafından belirtilmiş ve buna yönelik çeşitli uygulamalar geliştirilmiştir. Bu sahteciliğin kaynağı genellikle çağrıyı başlatan operatörler olarak görülmektedir. Ancak zaman zaman da olsa, operatör görüşmelerinde de özellikle vurgulandığı üzere söz konusu operatörler tarafından sahteciliğin kendileri tarafından gerçekleştirilmediğini ve abonelerinin çağrı şebekeye girmeden önce kendi kurdukları sistemler ile CLI'ı değiştirmiş

olabilecekleri zaman zaman belirtilebilmektedir. Bu bağlamda, CLI manipülasyonunun kaynağının hem operatörler hem de aboneler olabileceği anlaşılmakta olup sahteciliğin önlenmesi noktasında tüm ekosistemi içerisine alacak şekilde geniş kapsamlı bir yapıya ihtiyaç olacağı öngörülmektedir.

Bir diğer yöntem olan Wangiri çağrılarına bakıldığında ise bu sefer kök neden yine benzer gibi görünmekle birlikte, uygulanan yöntemler ve sahteciliğin kaynağı oldukça farklılaşmaktadır. Bu yöntem hem yurt içinden hem de yurt dışından uygulanabilmektedir. Buradaki temel amaç pek çok numaraya doğru çaldırıp kapatılacak şekilde çağrı bırakılması ve bu numaralardan geri dönüş aramaları alınmaya çalışılmasıdır. İki farklı durum burada karşımıza çıkabilmektedir. Çağrı bırakılan numaranın normal tarifeli bir hat olması durumunda temel amaç çok fazla suni trafik üreterek çağrı sonlandırma ücreti gelirlerini arttırmak olacaktır. Örneğin aylık çağrı sonlandırması yaklaşık 100 bin dakika olan bir operatörden bu şekilde bir saldırı yapıldığını ele alırsak, toplamda 100 bin numaraya doğru eş zamanlı çağrılar bırakıldığından bunların bir kısmının da geri dönüş araması yaptığı öngörüldüğünde ilgili operatörün aylık çağrı sonlandırması 200-300 bin dakikalara çıkabilecek ve bu yolla operatörün bu anlamdaki gelirleri de en az 2-3 katına çıkabilecektir. Çağrı bırakılan numaranın katma değerli hizmet numarası veya yüksek tarifeli başka bir numara olması durumunda ise, konu biraz daha farklılaşmaktadır. Bu sefer geri aramayı gerçekleştiren taraf görüşmenin devam ettiği dakika başına yüksek ücretler ödemek durumunda kalacak ve yüksek fatura dolayısıyla şikâyetçi olabilecektir. Karşı taraf ise yüksek tarifeli aramalar ile önemli ölçüde haksız gelir elde edebilecektir. Her iki şekilde de temel gayenin gelir elde etmek olduğu açıkken, yüksek tarifeli hatlarda önemli ölçüde tüketici şikâyeti ve abonesi olduğu operatör bakımından da prestij ve müşteri memnuniyeti açısından kayıplar olabilmektedir. Bu tür sahtecilikte kaynak hem aboneler hem de operatörler olabilmektedir. Yüksek tarifeli hatlarla yapılan saldırılarda hattın sahibi kendi kazancını arttırmak amaçlı bunu gerçekleştirmek isteyebilecekken, normal tarifeli hatlarda ise çağrı sonlandırma ücretini arttırmak isteyen operatör kaynak olabilecektir.

Bir başka yöntem olan abone sahteciliğinde ise edinimler farklılaşabilmektedir. Sahte evrak veya kimlik hırsızlıkları ile farklı kişiler adına abonelikler yapılması ve bu yolla suç işlenmesi vb. kötüye kullanımlar yapılması yöntemi olarak bilinmektedir. Burada abonelik hizmetini hiçbir ücret ödemeden temin etmek de amaçlardan olabilmektedir. Abonelik

işlemleri yaygın olarak bayiler üzerinden gerçekleştirildiğinden ve bayiler yaptıkları her işlem karşılığında operatörlerden belirli primler aldığından bayilerin de zaman zaman bu geliri elde etmek amacıyla bu tarz sahteciliklerin içine girmesi mümkündür. Bu çerçevede bakıldığında, işlenecek suçlar veya yapılacak çeşitli kötüye kullanımlar için başkası adına abonelik gerçekleştirme, ücret ödemeksizin abonelik imkânlarından faydalanma ve bayi primlerinden yüksek gelir elde etme gibi amaçlarla ve hem bayiler hem de genel olarak sahtekârlar tarafından gerçekleştirilebilmektedir.

Sahteciliğin kaynağını ve nedenlerini anlamanın sorunun tespiti ve çözümü noktasında çok önemli yer tutacağı düşünülmektedir. Her bir sahtecilik vakasının kendine özgü nedenleri olabileceğini unutmamak gerekmektedir. Bunun yanında, sahteciliğe karşı oluşturulacak yapılarda ve alınacak tedbirlerde mutlaka bu farklılıkların bir arada ve birbirine katkı sağlayacağı şekilde ele alınması gerektiği düşünülmektedir.

4.2. Sahteciliğin Tespiti ve Önlenmesi

Her vakada her hastalıkta veya her sorunda olabileceği gibi sahtecilikte de en önemli adımlardan birisi tespiti doğru yapabilmektir. Daha önce anlatıldığı üzere pek çok akıllı öğrenme ve yapay zekâ sistemlerini kullanan sahtecilik yönetim sistemleri bu yönde kullanılmaktadır. Çok geniş kapsamlı uygulamalar kullanılmakta ve pek çok derin analizler gerçekleştirilmektedir. Alınan tüm önlem ve tedbirlere rağmen sahteciliğin zaman zaman azalarak zaman zaman artarak ve bazen de form değiştirerek devam edebildiği de gözlemlenebilmektedir.

Telekomünikasyon sahteciliği noktasında ele alınabilecek pek çok farklı husus bulunmaktadır. Bunlara yönelik pek çok tespit ve önlem mekanizmaları da geliştirilmektedir. Bu çalışma kapsamında da farklı farklı türler çeşitli yönlerden ele alınmış ve bazı detaylar aktarılmıştır. Bununla birlikte, bu tez çalışmasında esas olarak odaklanılmak istenen alan CLI manipülasyonu ve çözümü hususudur. Bu kapsamda, öncelikle ve özellikle CLI manipülasyonuna yönelik hususlar değerlendirilecek ve öneriler sunulacaktır. Ancak, genel olarak telekomünikasyon sahteciliği noktasında tez çalışması kapsamında edinilen bilgiler ışığında da çeşitli tespit, değerlendirme ve önerilere de yer verilecektir.

4.2.1. Operatör görüşmeleri kapsamında CLI manipülasyonu

Öncelikle üçüncü bölümde yer verilen operatör görüşmeleri kapsamında konuya yaklaşılacaktır.

CLI manipülasyonunun tespiti noktasında ülkemiz uygulamalarında iki yöntemin öne çıkmakta olduğu görülmektedir. Öncelikle bu yöntemlerin önleme işlemi değil vaka gerçekleştikten sonra yapılan bir tespit olduğunu unutmamak gerekmektedir. Buna göre; belirli algoritmalara göre test çağrıları yapılarak yurt dışından gelen normal bir çağrının yurt içi çağrısı olarak görünecek şekilde CLI'ının değiştirilmiş olduğu gözlenebilmektedir. Burada önemli olan manipülasyon bulunan çağrı akışı ile aynı akışta olacak bir test çağrısı oluşturabilmektir. Bu noktada bu hizmeti sağlayan pek çok uluslararası şirket bulunduğu ve yetkin şekilde bu testlerin gerçekleştirilebildiği bilinmektedir. Diğer yaygın yöntem ise, detaylı çağrı ve CDR analizi yapılmasıdır. Uzun dönemlerde oluşan çağrı verileri üzerinden yapılan çeşitli incelemeler ve algoritmik analizler vasıtasıyla belirli operatörlerden ve belirli numaralardan benzer tipte çağrı profillerinin oluştuğu gözlenebilmekte ve manipülasyon tespitleri yapılabilmektedir.

Önleme noktasında ise, operatörlerin hâlihazırda yaptıkları tespitler çerçevesinde ilgili taraflarla iletişime geçerek bu tarz çağrı ve numaraların engellenmesini talep etmektedirler. Kamu otoritesi tarafından da zaman zaman denetimler gerçekleştirildiği ve idari yaptırımlar uygulandığı bilinmektedir. Bununla birlikte, soruna yönelik keskin bir önlem hâlihazırda alınamamış operatörlerce yapılan tespitlerin yasal noktada dayanağının tam olarak oluşturulamamış olduğu düşünülmektedir. Bu kapsamdaki, ihtiyaç duyulanlara ve yapılması gerekenlere ilişkin hususlara ilerleyen kısımlarda yer verilecektir.

4.2.2. Dünya uygulamaları kapsamında CLI manipülasyonu

CLI manipülasyonu ülkemizde olduğu gibi çeşitli ülke ve coğrafyalarda da önemli bir sorun olarak görülmekte ve bu çerçevede çeşitli yaklaşımlar sunulmaktadır. Genel olarak kısa vadeli çözümlerin uygulandığı ancak bunların gerçek zamanlı bir çözüm sağlamadığının ifade edildiği görülmüştür. Birbirlerine benzer veya farklı olan pek çok önlem alındığı da görülmektedir. Bu önlem ve yaklaşımlar yukarıda ülke bazlı olarak detaylıca anlatılmıştır.

Bu kısımda bu hususlara genel olarak yer verilecek ve ülkemiz açısından durum değerlendirmesi yapılacaktır.

Bu önlemlerden kısaca bahsetmek gerekirse, kullanıcılara gösterilen CLI'ın mutlaka ilgili ülke numaralandırma planına göre geçerli bir numara olması, aranabilir bir numara olması ve bu numaranın bir operatöre tahsisli olması noktasındaki önlemin genel olarak uygulandığı ve anlamlı bir önlem olduğu düşünülmektedir. Ülkemizde CLI'ın ulusal numaralandırma planında yer alan bir numara olması zorunluluğu bulunmaktayken, operatörlere tahsisli bir numara olması noktasında herhangi bir kontrol bulunmamaktadır. Bu bağlamda, ülkemizde de bu yönde bir uygulama yapılmasının faydalı olabileceği düşünülmektedir.

Bazı ülkelerde şüpheli numaralara ilişkin kara listeler oluşturulduğu ve bu kara liste kullanılarak operatörlerin gelen çağrıları kontrol edebilmesi ve çağrıları engelleyebilmesi olanağı sağlanmaktadır. Yine bu uygulama da hâlihazırda ülkemizde uygulanmamaktadır. Bu uygulama sayesinde hem operatörler hem de son kullanıcılar şüpheli numaralara ilişkin bilgi sahibi olabilmekte, çağrı geldiği zaman bunu kabul etmeme ve engelleme hakkına sahip olacağından bu uygulamanın da manipülasyonu azaltma noktasında önemli katkısı olabileceği ve ülkemizde de uygulanabileceği düşünülmektedir.

Bazı ülkelerde, o ülkede faaliyet gösteren operatörlerden her yılın sonunda engellenen çağrılara ilişkin detaylı bilgi istendiği ve bu bilgilerin ortak bir veri tabanına aktarıldığı görülmektedir. Bu uygulama ile de yukarıda anlatılan kara liste benzeri bir faaliyet yürütülmüş olmakta ve sonraki süreçte gelecek çağrılara yönelik aksiyonlar alınması noktasında operatörlerin eli güçlenebilmektedir.

Çağrı oluşturulurken eklenen CLI bilgisinin transit ve sonlandıran operatörler tarafından değiştirilmemesi gerektiği yükümlüğü ülkemizde olduğu gibi bazı ülkelerde de uygulanmaktadır. Bunun yanında, CLI'ın sadece abonelik hizmeti amacıyla tahsis edilen numara gruplarından olması ve rehberlik, kısa numara ve yüksek tarifeli numaralarının CLI olarak kullanılamaması da ülkemizde olmamakla birlikte bazı ülkelerde uygulanan yaklaşımlardandır. Bu uygulama ile arkasında abone olmayan bir çağrının gelmesi engellenebilecek olmakla birlikte zaman zaman rehberlik numaralarından veya 112, 155 vb.

kısa numaralardan geri dönüş amacıyla yapılacak çağrılar açısından da sorun oluşturabileceği düşünülmekte olduğundan ülkemizde uygulanması açısından sakıncalar bulunduğu düşünülmektedir.

Çağrı trafiğinin detaylı izlenmesi ve analizi gibi ülkemiz operatörlerince uygulanmakta olan yöntemlerin de yine pek çok ülkede uygulandığı görülmüş olup bu yöntemin de yaygınlığı dolayısıyla önemli ve faydalı olduğu kanaati oluşmuştur.

Bazı ülkelerde uygulandığı görülen, operatörlerce CLI manipülasyonu veya numaraların kötüye kullanımının tespiti durumunda çağrıları engelleme ve numaraya erişimi durdurma hakkı bulunması hususu önemli bir önlem olarak karşımıza çıkmaktadır. Yine aynı durumlarda, operatörlere diğer operatörler ile aralarında bulunan arabağlantı sözleşmeleri kapsamında ödemeleri gerçekleştirmeme vb. hususlarda çeşitli kararlar alma hakkı tanınmıştır. Bu uygulama özelindeki durum ülkemizdeki sorun ile uyumlu görünmektedir. Operatör görüşmelerinde de önemle vurgulandığı üzere operatörlerin kendi sistemleri ve yöntemleri vasıtasıyla yaptıkları tespitlerin yasal olarak sağlam bir zemine oturmaması ve eşit iki erkin arasında üstünlük oluşturma durumu olduğundan bu anlamda bu örnekten yola çıkılarak ülkemiz uygulamaları açısından referans veya örnek alınabilecek bir uygulama karşımıza çıkmaktadır. Bunun yanında ülke düzenleyici otoritesi tarafından sahtecilik gerçekleştiren operatörlere numara tahsis etmeme, yetkilendirmesini iptal etme gibi yaptırımlar uygulandığı görülmüş olup bu tarz caydırıcı önlemlerin de sahteciliği önleme noktasında önemli faydaları olacağı değerlendirilmektedir.

Bazı ülke uygulamalarında gözlendiği üzere bir operatör CLI'ın geçersiz olduğunu teknik olarak mümkün olacak şekilde ve ispatlanabilir biçimde tespit ederse ilgili çağrıyı sonlandırma hakkına sahip olacaktır. Bunun yanında, esas olarak CLI'ın güvenilirliğinin sağlanması noktasında çağrı akışının başından sonuna yer alan tüm operatörlere yönelik yükümlülükler getirilmiştir. Bu noktada en önemli görünen yükümlülüklerden biri de CLI'ın çevrilebilir/aranabilir bir numara olması zorunluluğudur. Çevrilebilir numaradan kasıt ise hizmette olan, geri aranabilen ve sonraki aramalarda da kullanılabilen bir numaradır. Bu bağlamda, bu yükümlülükler ile CLI'ın güvenilirliği noktasında ciddi adımlar atılmış olduğu görünmekte ve bu yükümlülüklerin manipülasyonu azaltma noktasında ülkemize de ışık tutabileceği düşünülmektedir.

CLI manipülasyonu noktasında ilginç bazı yaklaşımlar da bulunmaktadır. Buna göre, CLI'ın dolandırıcılık, zarar verme ve haksız şekilde herhangi bir edinim sağlama amacıyla yanlış ve yanıltıcı biçimde oluşturulması ve iletilmesi yasaklanmış, bununla birlikte herhangi bir zarar amaçlanmadıysa ve/veya gerçekleşmediyse bu işlem illegal olarak değerlendirilmemektedir. Bu uygulama ile iyi niyet yaklaşımı sergilenmiş olmakla birlikte, ülkemiz dinamiklerinde bunun kontrolünün ve denetiminin sağlanmasının pek kolay olmayacağı ve bu tarz bir uygulamanın ülkemizde uygulanmasının anlamlı olmayacağı değerlendirilmektedir.

Hem ITU, BEREC ve ECC gibi organizasyonlar tarafından hem de bu çalışmada yer verilen ülkelerin tamamına yakını tarafından en çok öne çıkarılan hususlar ise sektörün, tüm ekosistemi içerecek şekilde iş birliği içerisinde olması, bilgi paylaşımının arttırılması ve bu hususta oluşturulacak çalışma grupları vasıtasıyla çalışmaların aktif şekilde yürütülmesi gerektiğidir. Ülkemizdeki durumu ele almak gerekirse, bu anlamda bazı eksiklikler olduğu düşünülmektedir. Özellikle kamu gücü ile sektörde faaliyet gösteren şirketlerin (operatörler) arasında genellikle var olan kurallar ve denetimler üzerinden kurulu ilişkinin bu konu çerçevesinde bir miktar daha değiştirilmesi ve iş birliklerinin arttırılmasının çok önemli olacağı düşünülmektedir. İş birliğinden kasıt sadece toplantılar, çalıştaylar vb. değil somut olarak düzenleme de yapılarak üzerinde mutabık kalınan bir çerçeve oluşturmak ve tüm tarafların bu çerçeve doğrultusunda sahteciliğin önlenmesi noktasında üzerine düşeni tam anlamıyla yerine getirmesidir. Elbette ki kanunlarla ilgili tarafa verilmiş olan yetkilerin çerçevesinden çıkmamak gerekmektedir, ancak bu çerçeveler içerisinde oluşturulacak sağlam iş birlikleri ile sektörde yer alan ve sahteciliğe meyilli tarafların da zaman içerisinde oluşan ekosisteme uyum sağlayacakları ve sahteciliğin önemli ölçüde azalacağı ve belki de sona erebileceği değerlendirilmektedir.

4.2.3. Dünyada uygulanan veya uygulanabileceği düşünülen tedbirlerin değerlendirilmesi

Bu bölümde çeşitli ülkelerde ve bölgelerde uygulanan veya uygulanmasının faydalı olduğunun düşünüldüğünün belirtildiği tedbirlerin ülkemiz açısından uygunluğu veya uygulanabilirliğine yönelik değerlendirmelere yer verilecektir.

ABD'de uygulanmakta olan ve yukarı bölümlerde detaylarına yer verilen STIR/SHAKEN yöntemi vasıtasıyla CLI'ın güvenilirliği ve sahteciliğin önlenmesi noktasında önemli faydalar görüldüğü anlaşılmaktadır. Öncelikle bu yöntemin tamamen IP ekosistemindeki çağrılar için uygulanabilir olduğunun hatırlatılmasında fayda görülmektedir. Bu yöntem ile uçtan uca doğrulanmış ve imzalanmış bir çağrı akışı sağlanmakta ve bu sayede hem CLI'ın tam anlamıyla güvenilirliği sağlanmakta hem de operatör ve kullanıcılar/abonelerin güvenli şekilde çağrıları iletmeleri ve karşılamaları sağlanmış olmaktadır. Bu yöntemin ABD özelinde oluşturulmuş olması ve Kanada harici henüz hiçbir ülkede denenmemiş olması önemli bir dezavantaj olarak karşımıza çıkmaktadır. Uygulanması noktasında homojen bir yapı bulunması gerekmektedir. Bu da şu anlama gelmektedir; örneğin ülkemizde bu yapı kurulur ve ülke içindeki tüm çağrılar doğrulanmış şekilde iletilse dahi yurt dışında bu uygulamanın bulunmadığı veya ülkemiz ile bu uygulama noktasında anlaşma yapmamış bir ülkeden bir çağrı geldiğinde yine doğrulama gerçekleştirilememiş olacağından bu noktada yaşanan sıkıntıların önlenemeyebileceği düşünülmektedir. Ayrıca, CLI manipülasyonu yapma niyetindeki bir operatör şu anda izlemekte olduğu yöntem gibi yurt dışından IP vasıtasıyla gelen bir çağrıyı kendi şebekelerinde sıfırdan başlıyormuş gibi gösterip bu aşamada da çağrıyı doğruladığında ve ekosisteme aktardığında yine manipülasyonun önüne geçilemeyebileceği düşünülmektedir. Elbette ki bu yöntem uygulanırsa pek çok sahtecilik vakasının engelleneceği ve önemli ölçüde azalma yaşanacağı öngörülebilmektedir. Bununla birlikte, hem yukarıda yer verilen gerekçeler hem de bu yöntemin tamamen IP ortamındaki çağrı ekosisteminde uygulanabilir olması ve ülkemizde halen eski nesil (IP tabanlı olmayan) şebekelerin yaşamına devam ediyor olması nedeniyle şu aşamada ülkemizde doğrudan uygulanmaya başlanmasının kısa vadede önemli bir fayda sağlamayabileceği düşünülmektedir. Bununla birlikte, uzun vadeli olarak çağrı ekosisteminin tamamen IP tabanlı olacak şekilde dönüşme durumu, AB ülkeleri içerisinde bu anlamda yapılacak düzenlemeler ve olası diğer etmenlerin izlenerek ilerleyen dönemlerde bu yöntemin ülkemizde de uygulanabileceği düşünülmektedir.

SOLID yönteminin henüz teori aşamasında olması ve herhangi bir uygulamasının olmaması nedeniyle ülkemiz açısından şu aşamada bir anlam ifade etmediği, zaman içerisinde uygulamalarının izlenerek edinilen tecrübeler ışığında yeniden değerlendirilebileceği düşünülmektedir.

Blockchain teknolojisinin de STIR/SHAKEN yönteminde olduğu gibi, tamamen doğrulanmış bir çağrı ekosistemi ve numara veri tabanı oluşturma anlamında önemli özelliklerinin olduğu görülmektedir. Burada da önemli olanın doğru bir ekosistem kurmak olduğu düşünülmektedir. Tüm operatörlerin dâhil olduğu blockchain tabanlı bir numara ve çağrı yapısı oluşturulduğu durumda, CLI güvenilirliğinin sağlanabileceği, operatör ve kullanıcıların daha güvenli şekilde iletişim kurabilecekleri bir ekosistem oluşabileceği ve bunun da sahteciliklerin azaltılması noktasında son derece faydalı olabileceği düşünülmektedir.

AB El Sıkışması gibi özel girişimler ise genellikle belirli operatörler arasındaki iş birliği ve ikili veya daha çok taraflı anlaşmalar ile sağlandığından ve tüm ekosisteme yönelik bir çözüm olmadığından ülkemiz düzenlemeleri açısından çok net bir anlam ifade etmeyeceği düşünülmektedir. Bununla birlikte, birbiri ile anlaşma sağlayan operatörler arasındaki trafiğin güvenilir bir şekilde gerçek zamanlı olarak doğrulanması anlamında önemli ve faydalı bir yöntem olduğu değerlendirilmektedir. Bu bakımdan, düzenlemelerin uygun olması halinde ülkemizde faaliyet gösteren operatörler açısından faydalı bir çözüm olabileceği düşünülmektedir.

4.2.4. CLI manipülasyonu dışında kalan bazı sahteciliklere ilişkin değerlendirmeler

Özellikle operatör görüşmeleri çerçevesinde öne çıkan hususlardan biri olan abone (bayi) sahteciliklerinin de sektörde önemli bir yer işgal ettiği ve bu hususa yönelik çeşitli önlemlerin de alınması gerektiği düşünülmektedir. Bu sahtecilik türünde bayilerin tüketicilere dokunan en önemli nokta olması nedeniyle öne çıktığı görülmektedir. Bayilerde yaşanan sorunların operatörlerce daha kapsamlı incelenmesi, bu noktada bir düzenleme ihtiyacı varsa bunun daha somut olarak belirlenmesinin önemli olduğu görülmektedir. Abonelik süreçlerinde insan faktörünün azaltılması noktası da son derece önem arz etmektedir. Ülkemiz düzenlemeleri açısından dijitalleşmeye dönük belirli adımlar olduğu görülmekle birlikte, aboneliklerin veya numara taşıma taleplerinin E-devlet vb. platformlar üzerinden daha güvenilir şekilde yapılabilmesinin sahteciliğin azaltılması noktasında faydalı olacağı düşünülmektedir.

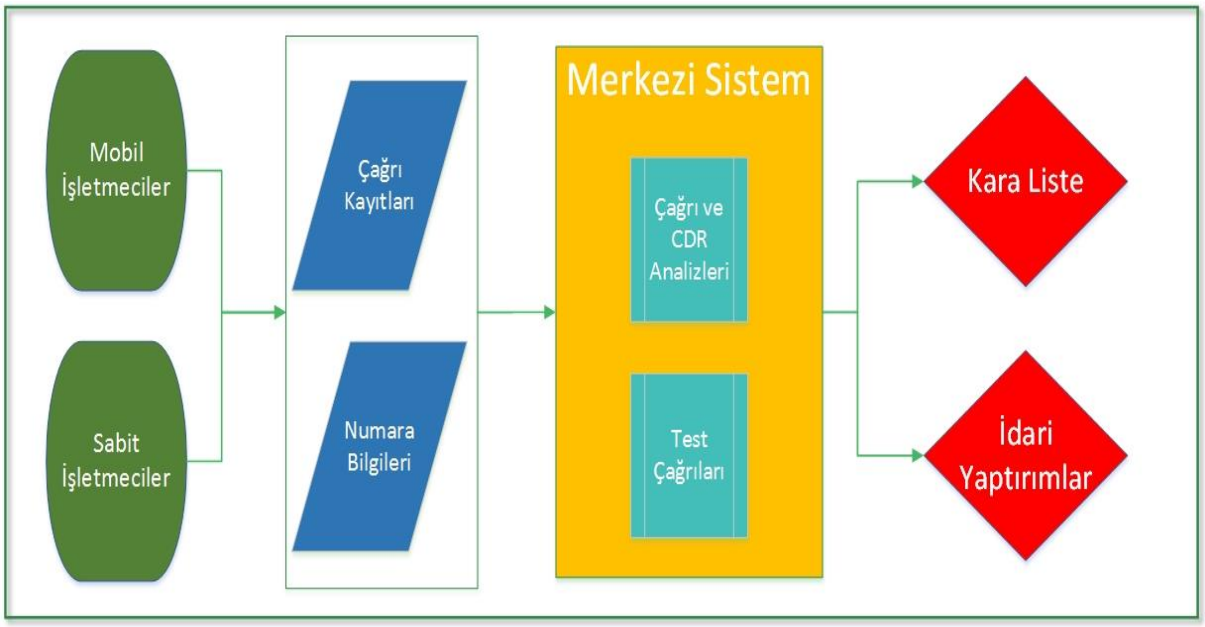
Yine öne çıkan sahteciliklerden biri olan Wangiri noktasında ise, operatör düzeyinde çeşitli önlemlerin alınabileceği düşünülmektedir. Bu sahteciliklerde tek bir numaradan birçok numaraya doğru eş zamanlı çağrıların yapıldığı bilinmekte olup şebekeye gelen bu tip eş zamanlı çağrılar için belirli kurallar oluşturulabileceği düşünülmektedir. Yüksek tarifeli hatlardan gelen çağrılar açısından ise, ülkemiz içindeki bu tip hatlara doğru yapılan çağrılar noktasında çeşitli önlemler alındığı bilinmektedir. Örneğin; Katma Değerli Elektronik Haberleşme Hizmetlerinin Sunumuna İlişkin Usul ve Esaslar ile, tüketicilerin yüksek tarifeli bu hatlara yönelik olarak korunması, mobil telefon numaralarının bu hatlara doğru aramalara istenildiği zaman kapatılabilmesi vb. bazı hususlar düzenlenmiş ve söz konusu düzenlemede geçen *"... Bu usul ve esaslar kapsamında KDH'ye ilişkin; ... olası sahtecilik (fraud) yöntemlerine karşı gerekli teknolojik önlemleri almak/aldırmak ... işletmecinin sorumluluğudur ..."* hükümleri ile sadece bu çerçevede olsa bile operatörlere sahteciliği önleme noktasında bir yükümlülük getirilmiştir. Bu tarz parça parça önlemlerin mutlaka anlamlı olduğu ancak daha genel çerçeveli ve kapsayıcı düzenlemeler yapılmasının sahteciliği azaltma noktasında daha faydalı olacağı düşünülmektedir. Ayrıca, yurt dışı kaynaklı Wangiri aramalarına yönelik olarak kullanıcı hatları çerçevesinde bazı önlemlerin alınmasının faydalı olabileceği düşünülmektedir.

4.3. Öneriler

Bu kısımda, tez çalışmasının önceki tüm bölümlerinde edinilen bilgiler ve yukarıda yer verilen değerlendirmeler neticesinde, ülkemiz telekomünikasyon sektörü açısından sahteciliğin azaltılması noktasında çeşitli öneriler sunulacaktır.

CLI manipülasyonu konusunda ülkemizde yaşanan sorunlara detaylı şekilde yer verilmiştir. Görüşme gerçekleştirilen operatörlerin kendi sistemlerinde yaptıkları tespitler ve önlemler ışığında bakıldığında, bu noktadaki temel problemin operatörlerin kendi aralarında yaşanan sorunu birbirleri arasında çözmeye çalıştıkları olduğu düşünüldüğünden çözüm bu noktasında öncelikle bu hususa bakmakta fayda olacaktır. Bu itibarla, sektörün düzenleyici kamu otoritesi bünyesinde, CLI manipülasyonu ve olası diğer sahtecilikler özelinde bir sahtecilik yönetim sisteminin kurulması, kurulacak bu sistemde sektörde faaliyet gösteren operatörlerin de yer alması ve bu sistemin oluşturulacak yasal düzenlemeler ile sahteciliğe karşı çalışması önemli bir kazanım olacaktır. Bu sistemin nasıl olması gerektiğine ilişkin

bazı çerçeve hususlara değinmek gerekirse, sisteme bağlı olan tüm operatörlerin çağrı verileri sürekli şekilde bu sisteme aktarılacak ve burada gerçekleştirilen detaylı analizler neticesinde sahtecilik bulunan çağrı ve numaralar tespit edilecektir. Yine halihazırda operatörlerce uygulanmakta olan test çağrısı yönteminin de bu sistem üzerinde kurulan yapılarla otomasyon yapılmış şekilde gerçekleştirilmesi ve bu testler sonucu manipülasyon yapılan çağrı, numara ve operatör akışlarının tespit edilmesi sağlanmalıdır. Tespitlerin yapılması sonrasında ise ilgili paydaşlar ile paylaşım yapılması ve bu sonuçlar neticesinde uygulanacak yaptırımlar öne çıkacaktır. Bu noktada, sistemin paydaşı olan her bir operatöre karşı şeffaf olması, işletilen süreçlerin ve yapılan tespitlerin şeffaf şekilde tüm paydaşlara sunulması, yine yapılan tespitler sonucu oluşturulacak şüpheli numaralar listesinin ortak şekilde paylaşılması ve bu numaraların bulunduğu çağrıların engellenebilmesinin sağlanması önemli hususlar olarak karşımıza çıkacaktır. Operatörler sisteme hem veri aktaran hem de bu sistemin çıktıları ile sahteciliğe karşı korunan ve güvenilir çağrı kurma noktasında da fayda gören taraflar olacaklardır. Bununla birlikte, sistemin yönetimini sağlayan kamu tarafı da hem düzenleyici otorite görevini sağlıklı şekilde yürütebilecek hem de sahtecilik faaliyeti yürütenlere yönelik işlemlerini daha sağlıklı ve hızlı şekilde gerçekleştirebilecektir. Sistemde yürütülen faaliyetler neticesinde sahtecilik gerçekleştirdiği anlaşılan operatörlere ilgili mevzuatta belirtilmek üzere çeşitli idari yaptırımlar uygulanmalı ve sahteciliğin boyutu veya tekrarı halinde ilgili operatörün yetkilendirmesinin iptaline kadar giden önlemler alınmalıdır. Ülkemiz kanun ve düzenlemelerinde haberleşmenin gizliliği esastır. Bu hükme aykırı bir süreç yaşanmaması açısından, söz konusu sisteme iletilen tüm bilgi ve verilerin anonimleştirilmesi, kişisel bilgilerden tamamen arınması ve toplu analizler yapılması noktasındaki bütünün bir parçası olması gerekmektedir. Sistemin yasal olarak altyapısının sağlanması için yukarıda yer verilen tüm hususları içerecek şekilde ve sistem mimarisi ile tüm paydaşların rollerini açık şekilde belirtecek bir düzenlemenin Bilgi Teknolojileri ve İletişim Kurulu tarafından hayata geçirilmesi gerektiği değerlendirilmektedir. Kurulacak bu yapı sayesinde, uluslararası organizasyonların, çeşitli ülkelerin ve görüşme gerçekleştirilen operatörlerin de önemle vurgulamış olduğu şekilde iş birliği ve birlikte çalışılabilen bir ekosistem oluşturulması gerektiği görüşleri de gerçek anlamda hayata geçirilebilmiş olacaktır. Bu sistemin yapısını ve paydaşlarını özetleyen mimari yapısına Şekil 4.1'de yer verilmektedir.



Şekil 4.1 Merkezi Sahtecilik Tespit Sistemi Mimarisi

Yukarıdaki şekilden de görülebileceği üzere, mobil ve sabit operatörler bu sistem için girdi sağlayan en temel unsurlardır. Bu operatörlerin şebekelerindeki çağrılar dolayısıyla oluşan çağrı kayıtları ve numara bilgileri ile yine bu operatörlerin kendi tecrübe ve çalışmaları ile elde ettikleri bilgi ve veriler sisteme aktarılacaktır. Bu sistemde yukarıda da detaylarına yer verildiği üzere detaylı çağrı ve CDR analizleri yapılacak, ayrıca ihtiyaç durumlarında da test çağrıları yapılarak sahtecilik tespitleri yapılacaktır. Bu sistemde yapılan tespitler ışığında aşağıda yer verildiği şekilde kara liste oluşturulması ve sahteciliğe karışan taraflara yönelik olarak çeşitli idari yaptırımların uygulanması mümkün olabilecektir.

Bazı ülkelerde uygulaması bulunan numara kara listeleri oluşturulması hususu çerçevesinde, yukarıda yer verilen sistem içerisinde veya başka bir platform üzerinden ülkemiz ulusal numaralandırma planında yer alan ve operatörlere tahsis edilmiş numaraların listesinin yayımlanması ve operatörlerin çağrıları başlatırken veya sonlandırırken bu liste üzerinden kontrollerini gerçekleştirerek aslen olmaması gereken çağrıları engellemesi sahteciliğin önlenmesi noktasında kritik olacaktır. Bu kara liste yukarıda yer verilen sistem ile uyumlu şekilde çalışarak sistem çıktıları ışığında sürekli güncelliği sağlanabilecektir. Hâlihazırdaki ülkemiz düzenlemelerinde operatörlerin böyle bir liste üzerinden CLI vb. numara kontrolü yapmak gibi bir yükümlülükleri bulunmamaktadır. Dolayısıyla böyle bir uygulamaya başlanması için Bilgi Teknolojileri ve İletişim Kurulu tarafından hem kara

listenin oluşturulması ve güncel şekilde tutulmasının ne şekilde ve hangi platform üzerinden yapılacağına ilişkin ve hem de operatörlere bu listeyi referans alarak gerçek zamanlı olarak tüm çağrılarda CLI kontrolü yapması yönünde yükümlülük getirilmesine ilişkin bir düzenleme yapılması gerektiği düşünülmektedir. Bu düzenlemenin genel çerçevesinin şu şekilde olması gerekmektedir; kara listenin tutulacağı platformun düzenleyici otorite tarafından sağlanması, yine liste içeriğinin düzenleyici otorite uhdesinde olması ve operatörler ve olası diğer paydaşlarca liste içeriğine katkı yapılmasının sağlanması, kara listede yer alan bilgilerin ne sıklıkta güncellenmesi gerektiği hususunun belirlenmesi (örneğin saat başı veya her gün belirli bir saatte), operatörlere getirilecek yükümlülüklerin teknik olarak uygulanabilir olduğundan emin olunması ve operatörlerce yükümlülüğe uyulmaması halinde ne tür yaptırımlar uygulanacağının açık şekilde belirlenmesi gerekmektedir.

Yukarıda yer verilen sistemden bağımsız olarak değerlendirilmek ve ele alınmak üzere, Letonya örneğinde detayları anlatılan, operatörlere çağrı engelleme vb. bazı hususlarda çeşitli yetkiler verme ve hak tanıma gibi bazı düzenlemelerin de hayata geçirilebileceği düşünülmektedir. Operatör görüşmelerinde sıklıkla belirtildiği üzere, operatörler kendi sistemleri vasıtasıyla yaptıkları sahtecilik tespitlerinde yeterli aksiyonu alamadıklarını belirtmiş olduğundan bu noktada özellikle mobil operatörlerin ellerinin güçlenmesinin sağlanabileceği değerlendirilmektedir. Şebekelerine gelen çağrılarda CLI manipülasyonu tespit etmeleri halinde mobil (veya tüm) operatörlere söz konusu çağrıyı engelleme ve ilgili numaraya erişimi engelleme hakkı tanınabileceği, ayrıca operatörlerin bu tip çağrıları kendilerine ileten veya çağrıyı başlatan operatörlere aralarındaki arabağlantı sözleşmelerine de çeşitli ilaveler yapılmak suretiyle sonlandırma ücreti ödememe veya vakaların tekrarı halinde arabağlantı sözleşmesini feshetme gibi haklar tanınabileceği düşünülmektedir. Bununla birlikte, böyle bir durumun Elektronik Haberleşme Kanunu'nda yer alan ayrım gözetmeme ve rekabetin önlenmemesi gerektiği gibi hususlarla çelişeceği öngörülmektedir. Dolayısıyla böyle bir düzenleme yapılacaksa bile bunun sınırlarının iyi çizilmesi ve suistimal edilmesinin önüne geçilmesi gerektiği düşünülmektedir. Birleşik Krallık örneğinde yer aldığı üzere, operatörlerin yapacakları tespitlerin teknik olarak mümkün ve ispatlanabilir olması beklenmelidir. Ayrıca yukarıda yer verilen sistemin hayata geçirilmesi halinde böyle bir düzenlemeye de ihtiyaç kalmayacağı düşünülmektedir.

CLI manipülasyonunun önlenmesine yönelik olarak bahsedilen STIR/SHAKEN ve SOLID yöntemlerinin, tamamen IP ekosistemi gerektirmesi, henüz somut olarak uygulamalarının bulunmaması ve faydalarının çok net şekilde ölçülememiş olması nedenleriyle hâlihazırda ülkemizde somut şekilde uygulamaya geçirilebilir düzeyde olmadığı düşünüldüğünden bu yönde bir aksiyon alınmasına gerek olmadığı ancak bu ve benzeri yöntemlerin ilgili operatörler ve düzenleyici otorite tarafından takip edilerek ilerleyen dönemlerde ülkemizde uygulanmasının önünün açılmasına yönelik çalışmalar yapılmasının önemli olduğu düşünülmektedir.

Blockchain teknolojisi kullanılması vasıtasıyla doğrulanmış bir çağrı ekosistemi oluşturulması ve yine blockchain tabanlı olacak şekilde numara veri tabanı oluşturulması ve çağrıların buna göre kurulması noktasında bir çalışma yapılmasının faydalı olacağı düşünülmektedir. Bu tarz bir sistem kurulması halinde, sistemin kurulumu ve yürütülmesinin yine kamu otoritesi uhdesinde olması yasal olarak ve işleyiş olarak çok önemlidir. Bu sistemin de operatörleri de hem kullanıcı hem de katkı sağlayan olarak içine alması ve sürece dâhil etmesi gerekmektedir. Bu tarz bir sistemin hayata geçirilebilmesi için de bir düzenlemeye ihtiyaç bulunduğu değerlendirilmektedir. Bu düzenleme ile hem kurulan sistem yasal olarak güvence altına alınmalı hem de operatörlere getirilecek yükümlülükler ile sitemin sağlıklı şekilde yürümesi güvence altına alınmalıdır.

Ülkemizde faaliyet gösteren operatörlerin, AB El Sıkışması vb. yöntemleri uygulama noktasında teşvik edilmesi gerektiği düşünülmektedir. Bu noktada yapılacak bir düzenleme ile bu tarz sistemleri kullanan operatörlere yönelik olarak belirli kolaylıklar sağlanabileceği ve çağrı ekosisteminin daha sağlıklı olması noktasında fayda elde edilebileceği düşünülmektedir.

Abone sahteciliklerine ilişkin olarak ise; abonelik işlemlerinin yoğun olarak gerçekleştirildiği kanal olan bayiler üzerindeki denetimlerin arttırılmasının sağlanması, operatörlerce merkezi yetkilerin arttırılarak bayilerin müşteri toplamak ve sisteme aktarmak noktasındaki yetkilerinin bırakılması ve bu yolla suistimal ihtimalinin azaltılması ve çeşitli dönemlerde bayilerin operatörlerce eğitimlere tabi tutulmasının faydalı olabileceği değerlendirilmektedir.

Ayrıca, abonelik, numara taşıma vb. fiziksel evrak süreçlerini ihtiva eden tüm işlemlerin dijital ortamlarda da yapılabilmesi gerektiği ve bu sayede kimlik sahteciliği vb. hususların ciddi oranda önüne geçileceği düşünülmektedir. Bu çerçevede, E-devlet üzerinden abonelik başvurusu alınabilmesine yönelik başlandığı bilinen çalışmaların bir an önce tamamlanması ve numara taşınabilirliği başvurularının da yine aynı kanal üzerinden yapılabilmesinin sağlanması için gerekli çalışmaların yapılması ve bu süreçlerin yasal zemininin de hazırlanması gerekmektedir. Bu noktada başta Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği ve Numara Taşınabilirliği Yönetmeliği olmak üzere ilgili mevzuatta yapılması gereken değişikliklerin de bu yönde yapılması gerekmektedir.

Son olarak, mevcut düzenleme ve uygulamalarda sahteciliğe ilişkin belirli önlemler ve yükümlülükler bulunmakta iken genel olarak sahteciliğe ilişkin düzenlenmiş özel bir düzenleme bulunmamaktadır. Bu çerçevede, "Sahteciliğe Karşı Alınması Gereken Önlemler" başlıklı bir Usul ve Esaslar'ın Bilgi Teknolojileri ve İletişim Kurulu tarafından hayata geçirilmesinin önem arz ettiği düşünülmektedir. Bu Usul ve Esaslar'da yer alması gerektiği değerlendirilen başlıca hususlar şu şekildedir:

- Elektronik haberleşme hizmeti sunan tüm operatörler sahteciliğe karşı şebekelerinde ve aboneyi koruma noktasında gerekli tedbirleri almalıdır.
- Opeatörler sahteciliğe uğrayan abonelerinin, kendilerine ulaşması noktasında tüm kolaylıkları sağlamalı ve mağduriyetlerin giderilmesi noktasında azami hassasiyet göstermelidir.
- Operatörler bayilerince gerçekleştirilebilecek sahteciliklere karşı düzenli aralıklarla bayilerini denetlemeli ve sahteciliğe karşı alınacak önlemler konusunda eğitime tabi tutmalıdır.
- Abone sayısı on binin üzerinde olan operatörler, alanında uzman en az 3 kişiden oluşan sahtecilik ekibi kurmalıdır.
- Ses çağrısı hizmeti sunan operatörler, tek numaraya doğru eş zamanlı çok fazla çağrı yapılması, tek numaradan çok yöne doğru eş zamanlı çağrı yapılması, belirli numaralarda oluşan yoğun trafik vb. hususlar çerçevesinde şebekesinde gerekli önlemleri almalı ve bu tür çağrıları engellemelidir.

5. SONUÇ

Sahtecilik insanlığın varlığıyla beraber sürdürmekte olduğu varlığını halen pek çok yapı ve form altında sürdürmektedir. İnsanlık tarihi boyunca sahtecilik vakaları yaşanmış ve bunun karşılığı olarak çeşitli önlemler ve tedbirler alınmış ya da alınmaya çalışılmıştır. Bu döngü bazen kısır bir şekilde bazen de bir tarafın daha üstün olduğu şekilde devam etmiş olsa da gelinen noktada birinden birinin sona ermiş olduğunu söylemek mümkün görünmemektedir. İnsanlık tarihi kadar eski olmayan telekomünikasyon sektöründe de bu mücadele her zaman yaşanmış ve halen de yaşanmaktadır. Bu çalışmada sahteciliğin telekomünikasyon sektöründeki serüveni ele alınmış ve genel yaklaşım bu şekilde oluşmuştur.

Çalışma kapsamında yapılan literatür araştırması çerçevesinde, telekomünikasyon sahteciliğinin pek çok çeşidi, tekniği ve yöntemi olduğu ve aynı zamanda birden çok motivasyon kaynağı olabileceği anlaşılmıştır. Bu yöntemlerden pek çoğu belirli oranlarda yaşanmakla birlikte bir kısmının çok daha yaygın şekilde yaşandığı ve bunların farklı bölge ve coğrafyalarda belirli bir kesişimle ortaklaşmaya ve benzeşmeye başladığı görülmüştür. Yani en temel ve yoğun olarak karşılaşılan sahtecilik yöntemleri dünyanın pek çok yerinde birbirine benzerlik göstermektedir. Bununla birlikte hem ülkemizde hem farklı yerlerde o bölgenin dinamiklerine göre öne çıkan çeşitli sahtecilikler olduğu da görülmüştür.

Sahtecilik için gelir elde etme, itibar kazanma/kaybettirme, hizmetlerden ücretsiz yararlanma vb. pek çok motivasyon kaynağı olsa da çok büyük oranda gelir elde etmek için gerçekleştirildiği görülmektedir. Bu kapsamda, en yüksek gelir kazancı neredeyse sahteciliğin de orada bulunması doğal karşılanmakta ve ilerleyiş de buna uygun şekilde gerçekleşmektedir. Dünya telekomünikasyon sektöründe sahtecilik kaynaklı yıllık gelir kaybının yaklaşık 30 milyar dolar (CFCA, 2019) olduğu düşünüldüğünde, bu anlamda sahtecilik senaryolarının amaçlarına belirli oranlarda ulaştığı ve sahteciliğe maruz kalan tarafların ise yeterli düzeyde önlem alamamış oldukları değerlendirilmektedir.

Hem pek çok ülkede hem de ülkemizde telekomünikasyon sahteciliğini önlenmesi için önemli çabalar harcanmakta ve birçok önlem ve tedbir alınmaktadır. Bunun yanında önemli

uluslararası kuruluşlar da bu yönde çalışmalar yapmakta ve çabalar harcamaktadır. Tüm bu çalışmalar ve yaşanan her şey hem bugüne hem de geleceğe ışık tutmaktadır. Sahtecilik ile mücadele noktasında sürekli var olanın üstüne koymanın ve yaşanan tecrübelerden edinilen bilgiler ile daha iyisini yapmaya çalışmanın çok önemli olduğu düşünülmektedir. Bu çalışma kapsamında da esas yaklaşımın bu olduğu ve bundan sonrası için yapılan değerlendirme ve oluşturulan önerilerin mevcut ve geçmiş durumun geleceğe bakan perspektifi ile sentezlenmesinin sonucu olduğu değerlendirilmektedir.

Bu çalışmanın temel amacı, ülkemiz telekomünikasyon sektöründeki sahtecilik vakalarının incelenmesi ve sahteciliğin azaltılabilmesi amacıyla alınabilecek önlemlere katkı sağlanmasıdır. Bu amaçla, literatür araştırması yapılarak konunun pek çok önemli yönü ortaya konmuş, ülkemizde faaliyet gösteren ve sektördeki pazar payları yaklaşık %70 olan iki mobil operatör ile görüşmeler gerçekleştirilmiş, dünyada sahtecilik kapsamında yapılanlara ve alınan önlemlere yer verilmiş ve nihai olarak tüm bu bilgiler ışığında gerekli tartışma ve değerlendirmeler yapılarak ülkemiz açısından telekomünikasyon sahteciliğinin azaltılması anlamında çeşitli öneriler sunulmuştur.

Türkiye telekomünikasyon sektörünün yaklaşık %70'ini temsil eden iki mobil operatör ile gerçekleştirilen yarı yapılandırılmış odak grup görüşmeleri ile sektörde mevcut durumda yapılanlar, gelecekte yapılması planlananlar, beklentiler vb. hususlarda derinlemesine bilgiler elde edilmiştir. Elde edilen bu bilgiler ışığında, Türkiye telekomünikasyon sektöründe yaşanan sahteciliğe ilişkin mevcut durum ortaya konulabilmiştir. Bunun yanında yaşanan sorunlar ve ihtiyaçlar da birinci ağızdan dile getirilmiştir. Tüm bu hususların kapsamlı şekilde analizi ve incelenmesi ile yapılan değerlendirmeler ortaya konularak oluşturulan önerilere şekil verilmiştir. Ayrıca, dünyada sahtecilik alanında neler yapıldığı, ne tür önlemler alındığı ve hangi yöntemlerin kullanıldığına ilişkin olarak çeşitli AB ülkeleri ile ABD'deki durum ve sahteciliği önlemeye yönelik bazı teknik tedbirler incelenmiş olup bu hususlarda önerilerde değerlendirmeye alınmıştır.

Yapılan tüm inceleme ve değerlendirmeler neticesinde, CLI manipülasyonunun önlenmesine yönelik olarak sektördeki tüm paydaşların katılım sağlayacağı merkezi sahtecilik yönetim sistemi önerisi geliştirilmiş ve bu sistemin detayları aktarılmıştır. Bu sayede, bu alanda yaşanan sahtecilik vakalarının önemli ölçüde azalacağı düşünülmektedir.

Ayrıca, sahteciliğe yönelik olarak çeşitli düzenlemelerde bazı yükümlülükler bulunmasına rağmen, sahtecilik özelinde bir düzenleme bulunmadığından bu anlamda bir düzenleme yapılması gerektiği belirtilerek söz konusu düzenlemenin temel çerçevesi çizilmiştir. Bu sayede hem operatör düzeyinde hem de abone düzeyinde koruyucu genel bir çerçeve çizilmiş olacağı ve sahtecilik vakalarının azalmasına katkı sağlanabileceği düşünülmektedir.

Bu çalışmada elde edilen bilgiler, yapılan inceleme ve değerlendirmeler ve netice olarak oluşturulan öneriler açısından telekomünikasyon sektöründe yaşanan sahtecilik sorununun azaltılması ve önlenmesi noktasında bu çalışmanın oldukça faydalı olacağı, bundan sonra bu alanda yapılacak çalışmalar için önemli bir kaynak olabileceği ve telekomünikasyon sahteciliği alanında geleceğe bir ışık tutabileceği değerlendirilmektedir.

KAYNAKLAR

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, *68*, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007

ACFE. (2002). *Occupational Fraud And Abuse*.

ACFE. (2020). *Global Study on Occupational Fraud and Abuse*.

Alexopoulos, P., Kafentzis, K., Benetou, X., Tagaris, T., & Georgolios, P. (2007). Towards a generic fraud ontology in e-government. *ICE-B 2007 - Proceedings of the 2nd International Conference on e-Business*, *February 2015*, 269–276.

Alraouji, Y., & Bramantoro, A. (2014). International call fraud detection systems and techniques. *MEDES 2014 - 6th International Conference on Management of Emergent Digital EcoSystems, Proceedings*, *November*, 159–166. https://doi.org/10.1145/2668260.2668272

Arlı, E. (2013). Barınma Yerinin Üniversite Öğrencilerinin Kişisel ve Sosyal Gelişim ve Akademik Başarı Üzerindeki Etkilerinin Odak Grup Görüşmesi İle İncelenmesi. *Journal of Higher Education and Science*, *3*(2), 173. https://doi.org/10.5961/jhes.2013.073

Azad, M. A., Alazab, M., Riaz, F., Arshad, J., & Abullah, T. (2020). *Socioscope: I know who you are, a robo, human caller or service number*.

Becker, R. A., Volinsky, C., & Wilks, A. R. (2010). Fraud detection in telecommunications: History and lessons learned. *Technometrics*, *52*(1), 20–33. https://doi.org/10.1198/TECH.2009.08136

Bell, T. B., & Carcello, J. V. (2000). *A Decision Aid for Assessing the Likelihood of Fraudulent Financial Reporting*.

Beneish, M. D. (1997). *Detecting GAAP violation: implications for assessing earnings management among firms with extreme financial performance*.

BEREC. (2019). *BEREC summary report on the Workshop on Fraud & Misuse of the E . 164 number range*. *December*.

Bernard, H. R. (2006). *Research methods in anthropology: qualitative and quantitative approaches* (4.Edition).

Bishop, C. M. (2005). *Neural Networks For Pattern Recognition*.

Błaszczyński, J., de Almeida Filho, A. T., Matuszyk, A., Szeląg, M., & Słowiński, R. (2020). Auto loan fraud detection using dominance-based rough set approach versus machine learning methods. *Expert Systems with Applications*, *163*. https://doi.org/10.1016/j.eswa.2020.113740

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, *17*(3), 235–255. https://doi.org/10.1214/ss/1042727940

Brown, S. (2005). *Telecommunication Fraud Management*.

BTK. (2021). *Elektronik Haberleşme Sektörü - 3 Aylık Pazar Verileri Raporu - 2021 3.Ç*.

Castillo, C. (2017). *Trojanized Photo App on Google Play Signs Up Users for Premium Services*. McAfee. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/trojanized-photo-app-on-google-play-signs-up-users-for-premium-services/

CFCA. (2019). *Communications Fraud Control Association Announces Results of 2019 Global Telecom Fraud Survey*. www.cfca.org.

Chen, C. T., Lin, C. T., & Huang, S. F. (2006). A fuzzy approach for supplier evaluation and selection in supply chain management. *International Journal of Production Economics*, *102*(2), 289–301. https://doi.org/10.1016/j.ijpe.2005.03.009

Chen, S., & Gangopadhyay, A. (2013). *A Novel Approach to Uncover Health Care Frauds Through Spectral Analysis*.

Collier, M., & Endler, D. (2013). *Hacking Exposed Unified Communications & VoIP Security Secrets & Solutions* (Second Edi).

Cortes, C., Pregibon, D., & Volinsky, C. (2001). Communities of interest. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *2189*(October), 105–114. https://doi.org/10.1007/3-540-44816-0_11

Cortesão, L., Martins, F., Rosa, A., & Carvalho, P. (2005). Fraud Management Systems in Telecommunications : a practical approach. *Proceeding of ICT*, *July 2016*.

Coussement, K., & Poel, D. Van Den. (2008). Churn Prediction in Subscriber Services. *Expert Systems with Applications*, *34*(1), 313–327. www.crm.UGent.be

ECC. (2016). *Evolution in CLI usage – decoupling of rights of use of numbers from service provision*. *April*.

ECC. (2018). *The role of E.164 numbers in international fraud and misuse of electronic communications services*. *May*.

ECC. (2022). *CLI Spoofing*.

Fanning, K., Cogger, K. O., & Srivastava, R. (1995). Detection of management fraud: A neural network approach. *Proceedings the 11th Conference on Artificial Intelligence for Applications, CAIA 1995*, *March*, 220–223. https://doi.org/10.1109/CAIA.1995.378820

Farvaresh, H., & Sepehri, M. M. (2011). A data mining framework for detecting subscription fraud in telecommunication. *Engineering Applications of Artificial Intelligence*, *24*(1), 182–194. https://doi.org/10.1016/j.engappai.2010.05.009

FTC. (2016). *National Do Not Call Registry Data Book*.

Galeotti, M., Rabitti, G., & Vannucci, E. (2020). An evolutionary approach to fraud management. *European Journal of Operational Research*, *284*(3), 1167–1177. https://doi.org/10.1016/j.ejor.2020.01.017

GLF. (2018). *Taking Action Against Fraud*.

Gossett, P., & Hyland, M. (1999). Classification , Detection and Prosecution of Fraud on Mobile Networks. *Proceedings of ACTS mobile summit, Sorrento*, *1*, 2–4.

Green, B. P., & Choi, J. H. (1997). Assessing the risk of management fraud through neural network technology. *Auditing*, *16*(1), 25–28.

GSMA. (2021). *AB Handshake Global Solution for Call Validation*.

Gürbüz, S., & Şahin, F. (2018). *Sosyal Bilimlerde Araştırma Yöntemleri* (5.Baskı).

I3Forum. (2014). *Fraud classification and recommendations on dispute handling within the wholesale telecom industry*. *May*, 1–32.

I3Forum. (2019). *OBC and A-Number validation*.

I3Forum. (2020). *Technical Report Calling Line Identification (CLI) spoofing*. *October*, 1–38.

ITU-T. (2019). *Technical Specification FG DLT D1.1: Distributed ledger technology terms and definitions*.

Johnson, M. (2012). *Demystifying Communications Risk: A Guide to Revenue Risk Management in the Communications Sector*.

Kabari, L. G., Nuka Nanwin, D., & Uduak Nquoh, E. (2015). Telecmmunications Subscription Fraud Detection Using Artificial Nueral Networks. *Transactions on Machine Learning and Artificial Intelligence*, *3*(6). https://doi.org/10.14738/tmlai.36.1695

Karel. (2021). *PBX nedir?* https://www.karel.com.tr/bilgi/pbx-terimler-sozlugu-nedir-acilimi-nedir-ne-demek

Keromytis, A. D. (2012). *A Comprehensive Survey of Voice over IP Security Research*.

Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P. (2004). Survey of fraud detection techniques. *Conference Proceeding - IEEE International Conference on Networking, Sensing and Control*, *2*(September 2014), 749–754. https://doi.org/10.1109/icnsc.2004.1297040

Krueger, R. A., & Casey, M. A. (2000). *Focus Group: A Practical Guide for Applied Research*.

Kuşaksızoğlu, B. (2006). *Fraud detection in mobile communication networks using data mining*.

Langlois, P. (2012). SCCP hacking, attacking the SS7 & SIGTRAN applications. *26th Chaos Communication Congress*.

Lin, J. W., Hwang, M. I., & Becker, J. D. (2003). A fuzzy neural network for assessing the risk of fraudulent financial reporting. *Managerial Auditing Journal*, *18*(8), 657–665. https://doi.org/10.1108/02686900310495151

Mawgoud, A. A., & Ali, I. (2020). *Statistical Insights and Fraud Techniques for Telecommunications Sector in Egypt*.

McEachern, J., & Burger, E. (2019). How to shut down robocallers: The STIR/SHAKEN protocol will stop scammers from exploiting a caller ID loophole. *IEEE*.

Mohd Yusoff, M. I., Mohamed, I., & Abu Bakar, M. R. (2013). Improved expectation maximization algorithm for gaussian mixed model using the kernel method. *Mathematical Problems in Engineering*, *2013*. https://doi.org/10.1155/2013/757240

Morgan, D. L., & Krueger, R. A. (1993). *When to use focus groups and why*.

Mustafa, H., Xu, W., Sadeghi, A. R., & Schulz, S. (2014). You can call but you can't hide: Detecting caller ID spoofing attacks. *Proceedings of the International Conference on Dependable Systems and Networks*, *April 2016*, 168–179. https://doi.org/10.1109/DSN.2014.102

Nguyen, C. T., Nguyen, D. N., Hoang, D. T., & Pham, H. (2020). *BlockRoam : Blockchain-based Roaming Management System for Future Mobile Networks*. 1–14.

Pastor, J., Tuexen, M., & Loughney, J. (2015). *Security Considerations for Signaling Transport (SIGTRAN) Protocols*.

Patton, M. Q. (2002). *Qualitative research and evaluation methods*.

Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing*, *30*(2), 19–50. https://doi.org/10.2308/ajpt-50009

Phua, C., Lee, V., Smith, K., & Gayler, R. (2005). *A Comprehensive Survey of Data Mining-based Fraud Detection Research*. https://doi.org/10.1016/j.chb.2012.01.002

Pironet, M., Antunes, C., Moura, P., & Gomes, J. (2009). Classification for Fraud Detection with Social Network Analysis. *Masters Degree Dissertation, Engenharia Informática e de Computadores*, 1–64.

Pourhabibi, T., Ong, K. L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*, *133*(August 2019), 113303. https://doi.org/10.1016/j.dss.2020.113303

Powell, R. A., & Single, M. (1996). *Focus Groups*.

Reaves, B., Shernan, E., Bates, A., Carter, H., & Traynor, P. (2015). Boxed out: Blocking cellular interconnect bypass fraud at the network edge. *Proceedings of the 24th USENIX Security Symposium*, 833–848.

Rebahi, Y., Nassar, M., Magedanz, T., & Festor, O. (2011). A survey on fraud and service misuse in voice over IP (VoIP) networks. *Information Security Technical Report*, *16*(1), 12–19. https://doi.org/10.1016/j.istr.2010.10.012

Rebahi, Y., Thanh, T. Q., Busse, R., & Lorenz, P. (2013). On the Use of Unsupervised Techniques for Fraud Detection in VoIP Networks. Içinde *Emerging Trends in ICT Security*. Elsevier Inc. https://doi.org/10.1016/B978-0-12-411474-6.00022-0

Rosset, S., Murad, U., Neumann, E., Idan, Y., & Pinkas, G. (1999). *Discovery of fraud rules for telecommunications---challenges and solutions*. *July 2014*, 409–413. https://doi.org/10.1145/312129.312303

Sahin, M. (2017). *Understanding Telephony Fraud as an Essential Step to Better Fight it*. 207.

Sahin, M., & Francillon, A. (2021). Understanding and Detecting International Revenue Share Fraud. *Proceedings 2021 Network and Distributed System Security Symposium*, *February*. https://www.ndss-symposium.org/wp-content/uploads/ndss2021_4C-2_24051_paper.pdf

Sambra, A. V., Mansour, E., Hawke, S., Zereba, M., Greco, N., Ghanem, A., Zagidulin, D., Aboulnaga, A., & Berners-Lee, T. (2016). Solid: A Platform for Decentralized Social Applications Based on Linked Data. *MIT CSAIL & Qatar Computing Research Institute, Tech. Rep.* http://emansour.com/research/lusail/solid_protocols.pdf

SAS. (1996). *Using Data Mining Techniques for Fraud Detection: A Best Practices Approach to Government Technology Solutions*. http://www.sas.com

Summers, S. L., & Sweeney, J. T. (1997). *Fraudulently Misstated Financial Statements and Insider Trading: An Empirical Analysis*.

The Guardian. (2020). *Sim-swap fraud is on the rise. How can you stop it happening to you?* https://www.theguardian.com/money/2020/sep/13/sim-swap-is-on-the-rise-how-can-you-stop-it-happening-to-you

TransNexus. (2013). *The Face of Traffic Pumping*. https://transnexus.com/blog/2013/the-face-of-traffic-pumping/

TransNexus. (2015). *Phone App Traffic Pumping Fraud*. https://transnexus.com/blog/2015/phone-app-traffic-pumping-fraud/

TRI. (2021). *The 2021 State of Communications-Related Fraud, Identity Theft & Consumer Protection in the USA*. 1–49.

Tu, H., Doupé, A., Zhao, Z., & Ahn, G.-J. (2016). *SoK: Everyone Hates Robocalls: A Survey of Techniques Against Telephone Spam*.

Vervier, P.-A., Thonnard, O., & Dacier, M. (2015). *Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks*. *February*, 8–11. https://doi.org/10.14722/ndss.2015.23035

Weiss, G. M. (2014). *DATA MINING IN TELECOMMUNICATIONS*. *June*, 0–13. https://doi.org/10.1007/0-387-25465-X

Xie, Y., Liu, G., Cao, R., Li, Z., Yan, C., & Jiang, C. (2019). A Feature Extraction Method for Credit Card Fraud Detection. *Proceedings - 2019 2nd International Conference on Intelligent Autonomous Systems, ICoIAS 2019*, *August*, 70–75. https://doi.org/10.1109/ICoIAS.2019.00019

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain Technology Overview*.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). *Where Is Current Research on Blockchain Technology?—A Systematic Review*.