# E-POSTALARDA SPAM SORUNU VE ÇÖZÜM ÖNERİLERİ

Özgür ÖZTÜRK

UZMANLIK TEZİ

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

Temmuz 2009

ANKARA

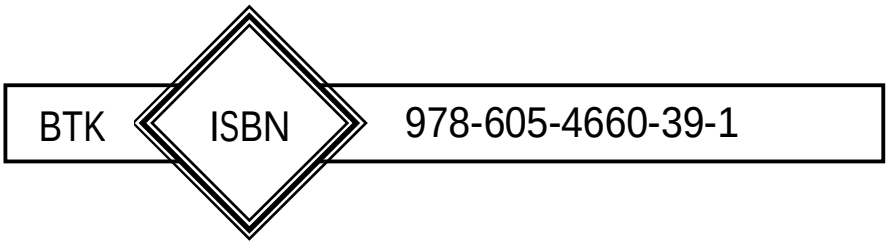
©Bu eserin tüm telif hakları

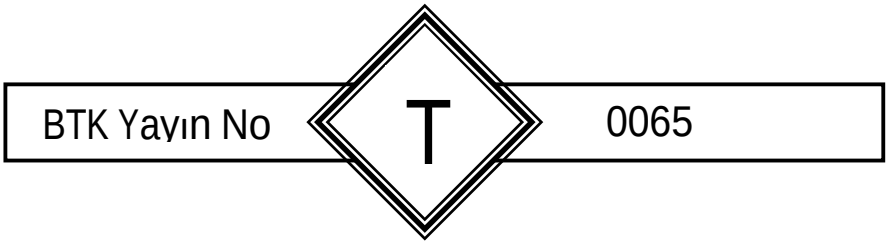
Bilgi Teknolojileri ve İletişim Kurumuna aittir.

Kaynak gösterilmeden alıntı yapılamaz.


Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.



Özgür ÖZTÜRK tarafından hazırlanan "E-POSTALARDA SPAM SORUNU VE ÇÖZÜM ÖNERİLERİ" adlı bu tezin Uzmanlık Tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Mustafa ALKAN
Tez Yöneticisi

Bu çalışma, jürimiz tarafından Uzmanlık Tezi olarak kabul edilmiştir.

| | | |
|---|---|---|
| Başkan | : | Ahmet Hamdi ATALAY |
| Üye | : | Doç. Dr. Mustafa ALKAN |
| Üye | : | Mustafa ÜNVER |
| Üye | : | Ejder ORUÇ |
| Üye | : | Osman Nihat ŞEN |
| Üye | : | Kemal Sacid SARIKAYA |
| Üye | : | Prof. Dr. Şeref SAĞIROĞLU |

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

## İÇİNDEKİLER

# E-POSTALARDA SPAM SORUNU VE ÇÖZÜM ÖNERİLERİ

**(Bilişim Uzmanlık Tezi)**

**Özgür ÖZTÜRK**

**BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU**

**Nisan 2009**

## ÖZET

Elektronik haberleşmenin önemli hizmetlerinden birisi de elektronik posta kullanımıdır. İnternetin ortaya çıkışı ve yaygınlaşmasıyla birlikte en çok kullanılan haberleşme araçlarından biri haline gelen elektronik posta hizmetinde yaşanan gelişmeler, birtakım sorunları da beraberinde getirmiştir. Bu sorunlardan birisi de "spam" mesajların e-postalar üzerinden yayılmasıdır. Gün geçtikçe daha kritik bir sorun halini alan spam mesajlar, e-posta hizmetlerinin güvenliğini ve güvenilirliğini tehdit etmekte ve bu da kullanıcıların tedirginliğine yol açmaktadır. Ortaya çıkan bu tehdit karşısında dünya genelinde teknik ve yasal önlemler alınmakta ve sorunla mücadele edilmeye çalışılmaktadır. Bu çalışmada, spam mesajların e-posta hizmetleri üzerindeki olumsuz etkileri incelenmiş, sorunla mücadele kapsamında uluslararası kuruluşların çalışmaları ve farklı ülke uygulamaları değerlendirilmiş ve geliştirilen teknik ve yasal çözümler üzerinde durulmuştur. Bu çerçevede, ülkemizdeki mevcut durum değerlendirilmiş ve bu değerlendirmeler doğrultusunda Türkiye için çözüm önerileri geliştirilmiştir.

Anahtar Kelimeler : Elektronik haberleşme, elektronik posta, spam
Sayfa Adedi : XIV + 139
Tez Yöneticisi : Doç. Dr. Mustafa ALKAN

**SPAM PROBLEM IN E-MAIL SERVICE AND SOLUTION PROPOSALS**

**(ICT Expertise Thesis)**

**Özgür ÖZTÜRK**

**INFORMATION AND COMMUNICATION TECHNOLOGIES AUTHORITY**

**April 2009**

## ABSTRACT

One of the important services of electronic communications is the use of e-mail. Development of e-mail services that have become one of the most used communication instruments along with the emergence and widespread use of internet, has brought some problems. One of these problems is the spread of spams via e- mail. Spam, which is seen as a more serious problem daily, have become security and reliability threats and this has been leading to the anxiety of users. Against this emerging threat, technical and legal measures are taken around the world and are being tried to combat the problem. In this study, negative impacts of spam on e- mail services have been evaluated. In the context of struggling with the problem, the works of international organisations and different countries' experiences have been assessed and technical and legal solutions have been evaluated. In this context, current situation in our country have been considered and in accordance with the considerations, solutions have been developed for Turkey.

Keywords : Electronic communication, electronic mail, spam
Number of Pages : XIV + 139
Advisor : Assoc. Prof. Dr. Mustafa ALKAN

## TEŞEKKÜR

Tez çalışmam boyunca değerli katkı ve görüşlerinden dolayı tez danışmanım Sayın Doç. Dr. Mustafa ALKAN'a,

Bilgi ve tecrübeleriyle beni yönlendiren Daire Başkanım Sayın Mustafa ÜNVER'e,

Yardımlarından dolayı çok değerli mesai arkadaşlarıma, desteğini her zaman yanımda hissettiğim eşim Çiğdem'e ve manevi desteklerini esirgemeyen anne ve babama teşekkürü borç bilirim.

# ÇİZELGELERİN LİSTESİ

# ŞEKİLLERİN LİSTESİ

## KISALTMALAR

| | |
|---|---|
| AB | Avrupa Birliği |
| ABD | Amerika Birleşik Devletleri |
| ACCC | Avustralya Rekabet ve Tüketici Komisyonu (Australian Competition and Consumer Commission) |
| ACMA | Avustralya Telekomünikasyon ve Medya Otoritesi (Australian Communications and Media Authority) |
| ARPANET | Gelişmiş Araştırma Projeleri Ajansı Şebekesi (Advanced Research Projects Agency Network) |
| BİT | Bilgi ve İletişim Teknolojileri |
| BM | Birleşmiş Milletler |
| CTSS | Uyumlu Zaman Paylaşımlı Sistem (Compatible Time-Sharing System) |
| DKIM | Etki Alanı Anahtarları Tanımlanmış Posta (Domain Keys Identified Mail) |
| DMA | Avustralya Doğrudan Pazarlama Birliği (Australian Direct Marketing Association) |
| DNS | Alan Adı Sistemi (Domain Name System) |
| DNSBL | DNS Kara Listeleri (DNS Black Lists) |
| DNSWL | DNS Beyaz Listeleri (DNS White Lists) |
| DoS | Hizmet Engellenmesi (Denial Of Service) |
| ENISA | Avrupa Şebeke ve Bilgi Güvenliği Kurumu (Europa Network and Information Security Agency) |
| E-posta | Elektronik Posta |
| EPS | E-posta Servis Sağlayıcı |

| | |
|---|---|
| FTC | Federal Ticaret Komisyonu<br>(Federal Trade Commission) |
| IETF | İnternet Mühendisliği Görev Gücü<br>(Internet Engineering Task Force) |
| IMAP | İnternet Mesaj Erişim Protokolü<br>(Internet Message Access Protocol) |
| IP | İnternet Protokolü<br>(Internet Protocol) |
| ITU | Uluslararası Telekomünikasyon Birliği<br>(International Telecommunication Union) |
| İSS | İnternet Servis Sağlayıcı |
| İK | İnternet Kurulu |
| MDA | Posta Teslim Aracı<br>(Mail Delivery Agent) |
| MHS | Posta İşleme Servisi<br>(Mail Handling Service) |
| MIME | Çok Amaçlı İnternet Posta Uzantıları<br>(Multipurpose İnternet Mail Extensions) |
| MMS | Çoklu Ortam Mesaj Hizmeti<br>(Multimedia Messaging Service) |
| MS | Mesaj Deposu<br>(Message Store) |
| MSA | Posta Sunum Aracı<br>(Mail Submission Agent) |
| MTA | Posta Aktarım Aracı<br>(Mail Transfer Agent) |
| MUA | Posta Kullanıcı Aracı<br>(Mail User Agent) |
| MX | Posta Değişim<br>(Mail Exchange) |

| | |
|---|---|
| OECD | Ekonomik İşbirliği ve Kalkınma Teşkilatı<br>(Organization for Economic Cooperation and Development ) |
| PGP | Oldukça İyi Gizlilik<br>(Pretty Good Privacy) |
| POP | Posta Ofis Protokol<br>(Post Office Protocol) |
| RBL | Gerçek Zamanlı Kara Listeleri<br>(Real Time Black Lists) |
| RFC | Yorum Talepleri<br>(Request For Comments) |
| SMS | Kısa Mesaj Hizmeti<br>(Short Message Service) |
| SMTP | Basit Posta Aktarım Protokolü<br>(Simple Mail Transfer Protocol) |
| SPF | Gönderici Yetkilendirme Dizgesi<br>(Sender Policy Framework – Sender Permitted From) |
| SSL | Güvenli Yuva Katmanı<br>(Secure Socket Layer) |
| STK | Sivil Toplum Kuruluşu |
| S/MIME | Güvenli/Çok Amaçlı İnternet Posta Uzantıları<br>(Secure/Multipurpose Internet Mail Extensions) |
| TASO | Türk Anti-Spam Organizasyonu |
| TCK | Türk Ceza Kanunu |
| TCP | İletim Denetim Protokolü<br>(Transmission Control Protokol) |
| TKK | Tüketicinin Korunması Kanunu |
| TLS | Taşıma Katmanı Güvenliği<br>(Transport Layer Security) |
| TMK | Türk Medeni Kanunu |
| TTK | Türk Ticaret Kanunu |

| | |
|---|---|
| VoIP | IP Üzerinden Ses İletimi<br>(Voice Over IP) |
| WSIS | Dünya Bilgi Toplumu Zirvesi<br>(World Summit on the Information Society) |
| WTSA | Dünya Telekomünikasyon Standardizasyon Genel Kurulu<br>(World Telecommunication Standardization Assembly) |
| | |

# 1 GİRİŞ

Elektronik posta (e-posta), günümüzde dünya üzerinde milyonlarca insanın iletişim kurmasını sağlayan en önemli ve yaygın iletişim araçlarından bir tanesidir. İnternetin ortaya çıkışı ve yaygınlaşması, bilgi ve iletişim teknolojilerinin gelişerek hayatımızın önemli bir parçası haline gelmesi ve hemen hemen her alanda kullanılmaya başlaması e-posta hizmetlerinin gelişimine ve yaygınlaşmasına olumlu yönde katkı yapmıştır.

Bilgi toplumu kavramının ön plana çıktığı, bilginin en hızlı şekilde paylaşımının son derece önemli olduğu bir dönemde kişiler arasındaki iletişimi anlık seviyelere indirmesi, kolay kullanılabilirlik özelliği sunması ve düşük maliyetli bir hizmet olması e-posta hizmetinin bu denli etkili ve önemli bir unsur haline gelmesini ve geleneksel posta hizmetlerinin yerini almasını sağlamıştır.

E-posta hizmetinin günlük hayatın vazgeçilmez bir parçası haline gelmesi ve yaşanan teknolojik gelişmeler birtakım sorunları da beraberinde getirmiştir. İnternet'in ilk hizmetlerinden birisi olmasından dolayı, şu anda İnternet hizmetleri söz konusu olduğunda şiddetle ihtiyaç duyulan güvenlik ve kimlik denetimi gibi gereklilikler göz önünde bulundurulmamıştır. Bu yüzden, e-posta hizmeti günümüzde İnternet'in en büyük problemlerine yataklık etmekte ve bunların başında da spam mesajlar gelmektedir.

E-posta hizmetinde büyük bir sorun olarak karşımızda duran spam mesaj oranı gün geçtikçe daha da artmakta ve tehlikeli bir hal almaktadır. E-posta hizmetlerinin düşük maliyetli olması özellikle reklam ve pazarlama faaliyetlerinde spam göndermenin en önemli nedenlerinden biri olmuştur. Bu kapsamdaki spam e-postalar her ne kadar kullanıcıya zarar vermek amaçlı gönderilmeseler de bunların kontrol edilmesi ve ayıklanması kullanıcıya ciddi bir zaman kaybı yaşatmakta, aynı zamanda sistem kaynaklarını gereksiz

yere meşgul etmektedir. Spam e-postalar dolandırıcılık, sahtecilik ve kötü niyetli yazılımların (virüs, solucan, truva atı ve casus yazılımlar) yayılmasına da neden olmaktadır. Gerek kişisel ve kurumsal güvenliği, gerekse ulusal güvenliği tehdit eden bu tür mesajlar maddi ve manevi anlamda çok büyük zararların ortaya çıkmasına neden olmaktadır.

E-posta hizmetinin geleceğini tehdit eden ve güvenilirliği konusunda kuşkular oluşturan bu durum karşısında gerekli teknik ve yasal önlemlerin alınması kaçınılmaz hale gelmiştir. İnternetin doğasında bulunan küresellik, spam e-postalar ile mücadelenin tüm dünyada topyekün sürdürülmesini zorunlu kılmaktadır. Nitekim, birçok ülke bu kapsamında gerekli önlemleri almış ya da bu yönde çalışmalara başlamıştır.

Bu çalışmanın amacı, tüm dünyada olduğu gibi ülkemizde de yaygın bir sorun haline gelen spam e-posta konusunu teknik ve yasal anlamda ele alarak dünyada yapılan uygulamaları incelemek, Türkiye'nin spam ile mücadelede nerede olduğunu belirlemek ve ülkemiz için çözümleyici bir yaklaşım oluşturmaktır.

Giriş bölümünü takiben tezin ikinci bölümünde, e-posta hizmetinin ortaya çıkışı ve tarihsel süreç içerisindeki gelişimi, e-posta hizmetinin işleyişi ve servis bileşenleri, kullanılan haberleşme protokolleri ve e-postanın yapısı anlatılmıştır.

Üçüncü bölümde, spam tanımı yapılarak karakteristik özellikleri ortaya konmuş ve tarihsel gelişimine ilişkin bilgiler verilmiştir. Ayrıca spam mesajların, kullanıldıkları haberleşme teknolojilerine göre çeşitlerine, içerik ve amaç bakımından sınıflandırmasına ve ortaya çıkardığı maliyete ilişkin bilgilere yer verilmiştir.

Dördüncü bölümde, e-posta hizmetinde yaşanan spam sorununun çözümüne yönelik en yaygın kullanım alanına sahip olan ve en etkili çözümler sunan teknolojik yöntemler ele alınmış, güçlü ve zayıf yönleri incelenmiştir.

Beşinci bölümde, Ekonomik İşbirliği ve Kalkınma Teşkilatı (Organization for Economic Cooperation and Development – OECD), Uluslararası Telekomünikasyon Birliği (International Telecommunication Union – ITU) ve Avrupa Birliği (AB) gibi uluslararası yapıların spam ile mücadele konusundaki değerlendirmeleri, çalışmaları ve önerileri ile ilgili bilgiler sunulmuştur.

Altıncı bölümde, ülke örnekleri olarak Avustralya ve Amerika Birleşik Devletleri (ABD) incelenmiştir. Söz konusu ülkelerin seçilmelerinin nedeni, bu ülkelerin spam ile mücadele kapsamında oluşturdukları yasal düzenlemelerde farklı yöntemleri benimsemiş olmalarıdır.

Yedinci bölümde, Türkiye'de spam ile mücadele hususunda yapılan çalışmalar ve mevcut hukuki durum incelenerek bunlara ilişkin değerlendirmeler yapılmıştır.

Sekizinci ve son bölümde ise e-posta hizmetlerinde spam ile mücadele konusunda Türkiye'de yapılması gerekli olan çalışmalar konusunda önerilerde bulunulmuştur.

# 2 E-POSTA HİZMETİ

Elektronik haberleşme ağları üzerinden her türlü verinin (resim, ses, video, html dökümanları, çalışabilir programlar vb), kişiler arasındaki iletişimi sağlamak amacıyla iki uç nokta arasında taşınması işlemine e-posta hizmeti, taşınan mesaja da e-posta iletisi denir [1]. Bu bölümde e-postanın tarihçesi, hizmetin işleyişi, temel bileşenleri, kullanılan protokoller ile e-postanın yapısı ele alınacaktır.

## 2.1 E-postanın Tarihçesi

Günümüzde e-posta hizmeti, kişilerin internet üzerinden haberleşmesi olarak algılansa da, ortaya çıkışı internetten çok daha eskiye dayanmaktadır. 1961 yılında MIT bünyesinde geliştirilen *Uyumlu Zaman Paylaşımlı Sistem (Compatible Time-Sharing System - CTSS)*[1] ile birlikte ilk olarak telaffuz edilmeye başlanmıştır [2]. CTSS'de ortaya konulan dosya paylaşım sistemi, kullanıcıları yeni yöntemlerle bilgi paylaşımı sağlama konusunda yüreklendirmiş ve yeni arayışlara itmiştir.

CTSS kullanıcıları ilk olarak kendi aralarında mesajlaşmak amacıyla mesaj dosyaları oluşturarak, bu dosyaları tüm kullanıcıların erişim izni olan bir dizin içerisine koymakla başlamışlardır. Oluşturulan bu mesaj dosyalarına, mesajın gideceği kullanıcının ismi (*"TO JOHN"* gibi) verilerek mesajı hangi kullanıcının alacağı da bir anlamda belirtilmiştir. Kullanıcılar sisteme giriş yaptıklarında bu dizine girerek kendilerine gelen mesaj dosyalarını okuyabilmekte ve çıktı alabilmekteydiler. Ancak, oluşturulan dosyalar herkese açık bir dizinde bulunduğundan haberleşme güvenliği mevcut değildi. Bir başka ifadeyle gönderilen mesajın herkes tarafından okunması riski bulunmaktaydı.

---

[1] CTSS: Çok kullanıcılı bir dosya paylaşım sistemidir. Kullanıcılar çevirmeli bağlantı ile terminaller sayesinde sisteme bağlanmaktadır.

1964 yılına gelindiğinde ise bir yazılı belge ile mesaj gönderme konusunda sistemli bir çalışma yapılması kararlaştırılmıştır. Bu amaçla, CTSS projesinde hazırlanan *Programlama Grup Notları 49 (Programming Staff Note 49 - PSN)* ile e-posta hizmetinin çıkışına zemin hazırlanmıştır [3].

PSN'de belirtilen işlevleri yerine getirmek amacıyla Noel Morris ve Tom Van Vleck, CTSS projesinde görevli personelin haberleşmesini sağlamak üzere kullanıcıların birbirlerine mesaj gönderebilecekleri bir yapı tasarlamışlar ve 1965 yılında çalışmalarını bitirmişlerdir [2].

Yapılan çalışmalar neticesinde günümüz e-posta hizmeti ile benzer çalışma prensibine sahip bir sistem ortaya çıkmıştır. Her kullanıcının kendisine ait posta kutusunu oluşturan bir dosyası bulunmakta ve gelen mesajlar bu dosyaya yazılmaktadır. Kullanıcılara ait bu dosyalara erişim sadece ilgili kullanıcı tarafından gerçekleştirilebilecek şekilde tasarlanmıştır. Bu sayede alıcıya gönderilen mesajların başkaları tarafından görülmesi riski de ortadan kaldırılmıştır.

Ancak yaşanan bu gelişmelerin temeli aynı bilgisayar üzerinde mesajlaşma üzerine kuruluydu. İlk olarak 1971 yılında *Gelişmiş Araştırma Projeleri Ajansı Şebekesi (Advanced Research Projects Agency Network – ARPANET)* bünyesinde Ray Tomlison tarafından iki farklı bilgisayar arasında mesaj gönderme işlemi gerçekleştirilmiştir. Günümüzde e-posta adreslemesinde kullanılan '@' işareti de ilk olarak bu tarihte kullanılmıştır [4].

E-posta hizmeti, ortaya çıkışından günümüze gelinceye kadar çok büyük ölçüde değişim göstermiş ve karmaşıklaşmıştır. Kullanım alanlarının ve kullanıcı kitlesinin genişlemesi, servis sağlayıcılarının sayısındaki artışla birlikte hizmet veren altyapı ve ortam çeşitliliklerinin ortaya çıkması ve geliştirilen ürünlerin çeşitlilik göstermesi e-posta himzetinde standardizasyona gidilmesini zorunlu kılmıştır. Zaman içerisinde evrimleşen

e-posta hizmeti günümüzde belli kurallar dahilinde internet üzerinden işleyen bir servis halini almıştır.

İnternetin yaygınlaşmasına paralel olarak da e-posta hizmetini kullanan kişi sayısında çok hızlı bir artış görülmüş ve günümüzün en önemli iletişim araçlarından biri haline gelmiştir.

## 2.2 E-posta Adresi ve Mesaj Yapısı

### 2.2.1 E-posta adresi

E-posta adresi @ işareti ile iki kısma ayrılmaktadır. Bu işaretin solunda kalan kısım yerel bir kimlik ifade ederken, sağında kalan kısım ise global bir kimlik ifade etmektedir (*yerel_kisim@global_kisim)* [5].

Yerel kısım kullanıcının e-posta hesabı alırken belirlediği alandır ve her bir hizmet sağlayıcı bünyesinde kullanıcıya özel, tek bir kimlik bilgisi yer almaktadır. Bir başka deyişle e-posta sunucusu üzerindeki posta kutusunu ifade etmektedir.

Global kısım ise e-posta servis sağlayıcısını ifade etmektedir. Bu alan internet dünyasında tektir ve bu nedenle belirleyici bir özellik taşımaktadır. Alan adlarının DNS'te kayıtlı olması sayesinde, gönderilen e-postaların alıcılarına ulaşması için gerekli bilgiler buradan alınır ve internet üzerinden taşınarak teslim edilirler.

### 2.2.2 E-posta mesajının yapısı

E-posta mesajı RFC-2822 ile tanımlanmıştır. Buna göre bir e-posta mesajında *mesaj başlığı* ve *mesaj içeriği* olmak üzere iki kısım bulunmaktadır [6].

### 2.2.2.1 Mesaj başlığı

Mesaj başlığı e-postaya ilişkin temel bilgiler içeren kısımdır. Bu bilgiler ile mesajın alıcısına taşınması sağlanmaktadır. Mesaj başlığındaki bilgilerin her biri satır başından başlamak üzere alan etiketi ile bu alana karşılık gelen bilgiden oluşmaktadır (Örn: "*From: yerel_kisim@global_kisim*").

Mesaj başlığında bulunan temel bilgiler aşağıda açıklanmıştır [6].

- **Geri Dönüş Yolu (Return-Path):** Bu alan, mesajın taşınması sırasında oluşan hataların ve bilgilendirme mesajlarının iletileceği e-posta adresini içermektedir.
- **Alındı (Recieved):** Mesajın alıcısına kadar taşınmasında görev yapan sunucu bilgilerini tutmaktadır. Başka bir deyişle gönderenden alıcıya kadar olan yol üzerindeki MTA'ların bilgilerini tutmaktadır.
- **Tarih (Date):** Mesajın gönderildiği tarih tutulmaktadır.
- **Gönderen (From):** Mesajı gönderen e-posta adresini içermektedir.
- **Konu (Subject):** Mesajın konusu tutulmaktadır.
- **Alıcı (To):** Mesajı alacak olan e-posta adresini/adreslerini içermektedir.
- **Mesaj Numarası (Message-ID):** E-postanın gönderildiği sistem tarafından mesaja verilen tek ve özel bir numaradır.

Mesaj başlığında zorunlu olarak bulunması gereken bilgiler *tarih bilgisi (date)*, *mesajın gönderildiği e-posta adresi (from)* ve *alıcı e-posta adresi (to)* olup, bunların dışındaki bilgiler zorunlu değildir [6].

### 2.2.2.2 Mesaj içeriği

Mesaj içeriği mesajın kendisini ifade etmektedir ve tamamıyla alıcıya özel bilgidir. İçeriği standart olarak ASCII karakter dizisinden oluşmaktadır.

Dolayısı ile farklı türdeki verilerin taşınması için yetersiz kalmaktadır. Bu nedenle, mesaj içeriğinde ses, resim veya video verilerinin karışık bir biçimde taşınması amacıyla *Çok Amaçlı Internet Posta Uzantıları (Multipurpose Internet Mail Extensions - MIME)* geliştirilmiştir.

### 2.2.3 MIME

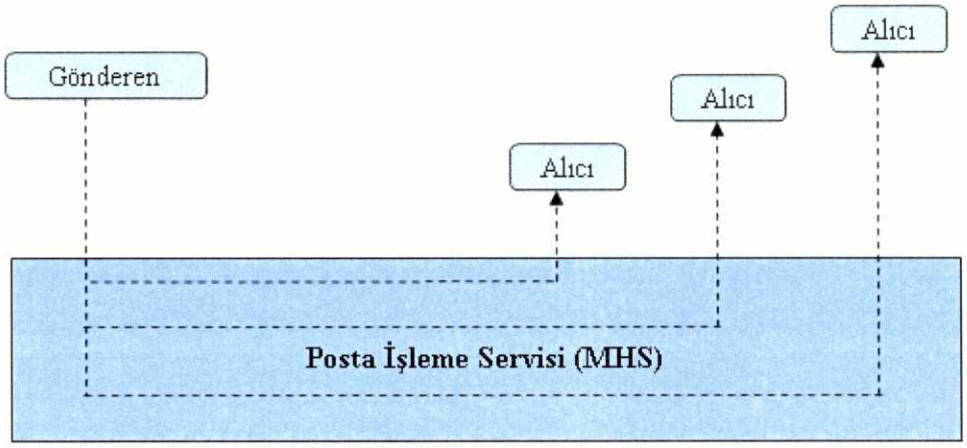
MIME ile e-posta içeriklerinde gönderilen veri türleri çoğaltılmış, her boyutta ve her türde içerik ya da dosyanın taşınması sağlanmıştır. Böylece, mesaj içeriğinde ASCII dışındaki karakter setlerinin kullanılmasına olanak sağlanmıştır. Mesaj içeriğinin birden fazla türde (ses, resim, görüntü vs.) dosya ya da veri türünden oluşturulabilme özelliği de MIME'ın getirmiş olduğu önemli bir yeniliktir [7].

MIME ile birlikte e-posta mesaj başlığında da bir takım yeni özelliklerin tanımlanması gerekmiştir. E-posta mesajının oluşturulması sırasında eklenen bu bilgiler sayesinde alıcının mesaj içeriğindeki veriyi, gönderildiği formatla tekrar biçimlendirmesi sağlanmaktadır. Mesaj başlığına eklenmesi zorunlu olan MIME bilgileri aşağıda listelenmiştir [6].

- **MIME Versiyonu (MIME-Version):** Bu alan kullanılan MIME versiyonu bilgisini tutmaktadır.
- **İçerik Tipi (Content-Type):** Mesaj içeriğinde taşınan verinin türünü ve alt türünü ifade etmektedir. Örneğin "gif" uzantılı bir resim dosyası için **"image/gif"** şeklinde belirtilmektedir.
- **İçerik Aktarım Şifreleme (Content-Transfer-Encoding):** Mesaj içeriğinin hangi gösterim biçimiyle (Örn: binary, base64, 8 bit vb.) oluşturulduğunu belirtmektedir.

## 2.3 E-posta Hizmetinin Bileşenleri

### 2.3.1 Posta işleme servisi




Şekil 2.1 Posta İşleme Servisinin Rolü

Posta İşleme Servisi (Mail Handling Service - MHS), e-posta iletisinin göndericiden alıcıya kadar ulaşmasını sağlayan ve bu süreci yöneten servistir. Bu süreçte, e-posta iletisinin alıcıya kadar taşınmasında ve işlenmesinde Şekil 2.2'de görüleceği gibi farklı işlevleri gerçekleştiren birimler bulunmaktadır. MHS bu fotoğrafın tamamını kapsayan ve yöneten servistir [8].

### 2.3.2 Posta kullanıcı aracı

Posta Kullanım Aracı (Mail User Agent - MUA), e-posta göndermek ve almak için kullanılan MS - Outlook, Mozilla - Thunderbird gibi yazılımlardır. Sağladığı arayüz ile e-posta hizmetinin son kullanıcıya dönük bileşenidir [9].

### 2.3.3 Mesaj deposu

Gelen ve gönderilen e-posta iletilerini depolayan bileşen Mesaj Deposu (Message Store - MS)'dur. Posta Teslim Aracı (Mail Delivery Agent - MDA) ile gelen e-postaları saklayarak kullanıcının talep ettiği zamanlarda depoladığı bu iletilerin MUA aracılığıyla yine kullanıcılara iletilmesini sağlar. MUA ve MDA ile aynı makinede bulunabileceği gibi uzak bir sunucuda da bulunabilir.

### 2.3.4 Posta sunum aracı

Kullanıcı tarafından MUA aracılığıyla hazırlanarak gönderilen e-posta iletileri yine MUA aracılığıyla Posta Sunum Aracı'na (Mail Submission Agent - MSA) iletilmektedir. MSA kendisine gelen iletilerin e-posta hizmeti kurallarına göre oluşturulup oluşturulmadığı kontrolünü yapan bileşendir. Yapılan kontroller iki aşamalı gerçekleşmektedir. İlk kontrolde, iletinin e-posta hizmet sağlayıcının koyduğu kurallara uygunluğu denetlenmektedir (konu kısmının doldurulup doldurulmadığı, mesaj boyutunun belirlenen limiti geçip geçmediği vb.). İkinci aşamada ise mesaj formatının (mesaj başlık yapısı, alıcı ve gönderici bilgileri vb.) internet e-posta standartlarına uygunluğu denetlenmektedir. Yapılan iki aşamalı kontroller neticesinde e-posta iletisinde yapısal bir sorun tespit edilmesi halinde gönderme işlemi yarıda kesilmekte, iletinin uygunluğu durumunda ise MSA, e-posta iletisini Posta Aktarım Aracı'na (Mail Transfer Agent - MTA) ileterek aktarım işlemini başlatmaktadır [8].

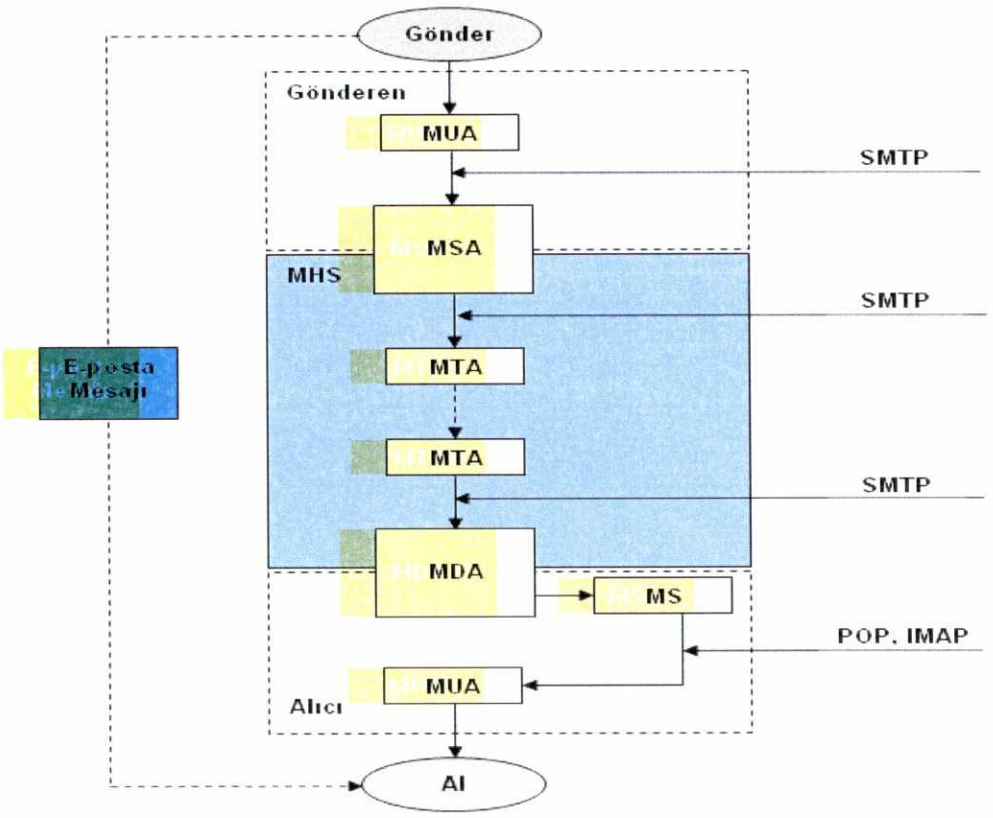
### 2.3.5 Posta aktarım aracı

MHS içerisindeki en önemli bileşendir. Mesajın alıcısına iletilmek üzere internet üzerinde taşınmasından sorumludur. Mesajı MSA'dan alarak alıcıya giden yolda bir başka MTA'ya nakletmekte ya da alıcının MDA'sına direk

bağlantı kurabiliyorsa buraya teslim etmektedir. Mesajın alıcıya iletilmesi için takip etmesi gereken yol bu bileşen tarafından belirlenmektedir. En çok kullanılan MTA yazılımlarına örnek olarak MS Exchange, Sendmail ve qmail verilebilir [9].

### 2.3.6 Posta teslim aracı

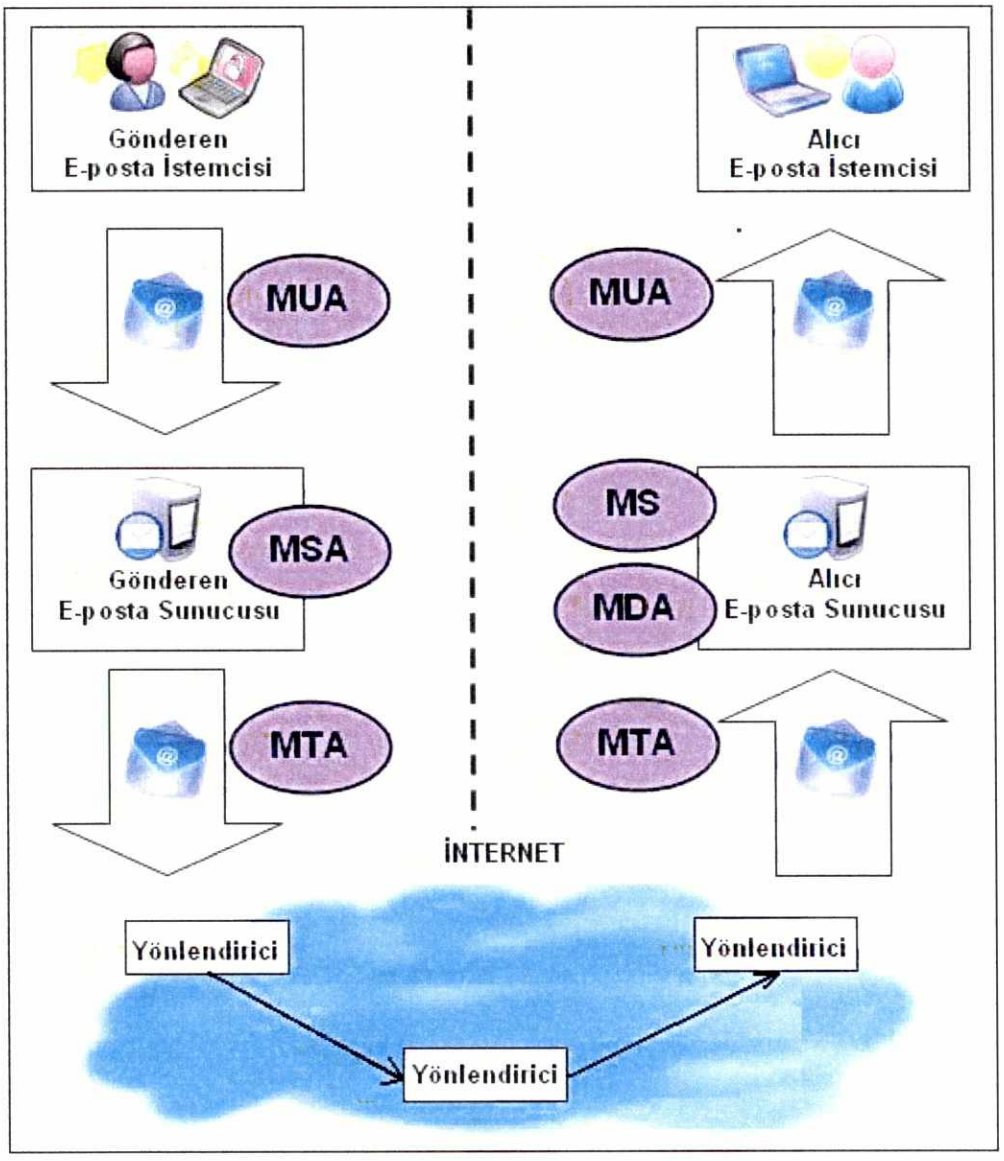
Mesajın alıcıya ulaştığı noktadır. MTA tarafından taşınan e-posta iletisi alıcının MDA'sına teslim edilmektedir. MDA kendisine gelen iletiyi kullanıcının görüntüleyebilmesi ve işleyebilmesi için MS'ye ileterek saklanmasını sağlamaktadır. En yaygın kullanılan MDA'lara örnek olarak Sendmail'i vermek mümkündür [10].




Şekil 2.2 E-posta Hizmetinin Bileşenleri [8]

## 2.4 E-posta Hizmetinin İşleyişi

E-posta hizmeti, yukarıda bahsedilen bileşenlerin belli kurallar dahilinde birlikte çalışmasıyla ortaya çıkmaktadır.




Şekil 2.3 E-posta Hizmetinin İşleyişi

E-posta iletisi, gönderici tarafından bir MUA uygulaması (outlook, mozilla vb.) kullanılarak oluşturulmakta (mesaj içeriği, mesaj başlığı, alıcı listesi vb.) ve yine bu uygulamayla gönderme işlemi başlatılmaktadır. E-posta istemcisi üzerindeki MUA, *Basit Posta Aktarım Protokolü (Simple Mail Transfer Protocol - SMTP)* standartlarını kullanarak iletiyi e-posta servis sağlayıcısındaki e-posta sunucu üzerinde bulunan MSA'ya iletmektedir [11].

Bu noktadan itibaren iletinin alıcısına/alıcılarına teslim edilmesi işleminin kontrolü sunucu üzerinde ve MHS tarafından gerçekleşmektedir. Sunucu üzerindeki işlemler sırasıyla;

- Mesaj kontrol işlemi
- Alıcı e-posta sunucularının tanımlanması ve
- Mesajın taşınması

şeklinde gerçekleşmektedir.

MSA kendisine gelen iletiyi öncelikle servis sağlayıcının yerel kontrollerine uygunluğu açısından ve formatının internet mesaj standartlarına uygunluğunu açısından denetlemektedir. Yapılan kontrollerden başarıyla geçen ileti SMTP standartları kullanılarak taşıma işlemini gerçekleştirecek olan MTA'ya gönderilmektedir.

E-postanın alıcısına ulaştırılması için öncelikle alıcıya ilişkin bilgilerin öğrenilmesi gerekmektedir. Bu amaçla MTA, Alan Adı Sistemi'nden (Domain Name System - DNS[1]) alıcının Posta Değişim (Mail Exchange - MX[2]) bilgilerini öğrenerek işe başlar [12].

---

[1] DNS: Okunması ve akılda tutulması kolay olan ve genelde aranan adres sahipleri ile ilişkilendirilebilen simgesel isimlerle yapılan adreslemede, karşılığı olan internet protokolü numarasını bulan ve kullanıcıya veren sistemi [13].

[2] MX Kaydı: DNS üzerinde tutulmakta olup e-posta sunucusuna ait Alan Adı ve adres bilgisini içeren kayıttır. E-postaların alıcılarına ulaşabilmesi için gerekli bilgiler DNS'ten sorgulanarak öğrenilmektedir [14].

E-posta iletilerinin gönderen ile alıcı arasındaki yola bağlı olarak varış noktasına kadar geçen yolculuğunda bir veya daha fazla sayıda MTA görev alabilir. Alcının MX bilgilerine göre MTA tarafından mesajın izleyeceği yolun belirlenmesi gerekir. Bu nedenle MTA'nın mesajı alıcısına ulaştırmak için bir sonraki varış noktasını bilmesi ve sıradaki MTA'ya mesajı iletmesi gerekmektedir. Mesajın internet üzerindeki bu yolculuğu alıcının MDA'sına ulaşıncaya kadar bir MTA'dan diğerine taşınarak gerçekleştirilmekte ve bu taşınma işlemi sırasında SMTP kuralları uygulanmaktadır.

MTA alıcının MDA'sı ile bağlantı kurarak SMTP kuralları çerçevesinde mesajı teslim eder. MDA, mesajı teslim alma esnasında servis sağlayıcı tarafından belirlenen bir takım kontroller yapar. Bu kontroller, gelen mesajın güvenlik kriterlerine uygun olup olmadığı, virüs veya solucan gibi tehlike içeren bir durum olup olmadığı ile ilgilidir.

MDA, aldığı e-postanın saklanması ve daha sonra kullanıcıya gösterilmesi için MS'deki posta kutusuna gönderir. Kullanıcı, sunucu üzerindeki posta kutusunda bulunan e-postalarını MUA işlevselliğinde bir istemci program ile görüntüleyebimekte, üzerinde işlem yapabilmektedir. Teslim edilen e-postanın MS ile MUA arasında taşınması *Posta Ofis Protokolü (Post Office Protocol - POP)* veya *İnternet Mesaj Erişim Protokolü (Internet Message Access Protocol - IMAP)* ile gerçekleştirilmektedir [11].

## 2.5 E-posta Protokolleri

Bilgisayarlar arasındaki veri iletişimi ve haberleşmesi, tanımlanmış ve standartlaştırılmış birtakım kurallar dizisiyle gerçekleştirilmekte ve yönetilmektedir. Bu kurallar bütününe protokol adı verilmektedir. Protokolleri oluşturan kurallar ve standartların amacı farklı ortamların ve ürünlerin birbiriyle uyum halinde çalışabilmesini sağlamaktır.

Değişik e-posta uygulamalarının birlikte çalışabilmesi, e-posta hizmetinin güvenilirliğinin sağlanabilmesi ve ortak bir standart oluşturulabilmesi için de e-posta protokolleri geliştirilmiştir. Bu protokoller şunlardır:

- Basit Posta Transfer Protokolü (SMTP)
- Posta Ofis Protokolü (POP)
- İnternet Mesaj Erişim Protokolü (IMAP)

### 2.5.1 SMTP

SMTP bir e-posta gönderim protokolüdür. IP tabanlı iletişim ağlarında e-posta gönderimine bu protokol ile birtakım kurallar ve standartlar getirilmiştir. Böylece birbirinden farklı işleyiş ve özellikler gösteren MTA'ların, e-postanın taşınması sırasında iletişim kurması ve veri iletişimini gerçekleştirmesi sağlamıştır.

Bu protokol 1982 yılında Jon Postel tarafından geliştirilmiş ve İnternet Mühendisliği Görev Gücü[1] (Internet Engineering Task Force - IETF) tarafından yayınlanan RFC[2]-2821 ile tanımlanmıştır [7]. Protokol çalışmaları ile e-postaların gönderenden alıcıya kadar iletişim ağları üzerinde MTA'lar tarafından daha güvenli ve daha verimli olarak taşınması amaçlanmıştır.

#### 2.5.1.1 SMTP komutları

İki MTA arasındaki veri iletişimi Çizelge 2.1'de listelenen SMTP komutları ile gerçekleştirilmektedir. İstemciden sunucuya gönderilen komutlar ve sunucunun bu komutlara verdiği cevaplar ile iletişim yönetilmekte ve süreç işletilmektedir.

---

[1] IETF: İnternet dünyasında tanımlı protokolleri geliştiren ve standartlaştıran bir gruptur.
[2] RFC (Request For Comments): İnternet ile ilgili her türlü bilginin standartlaştırılarak anlatıldığı dokümanlardır [5].

Çizelge 2.1 SMTP Komutları [7]

| KOMUT | KULLANILIŞI | AÇIKLAMASI |
|---|---|---|
| EHLO (HELO) | *EHLO <alan adı>* | SMTP sunucusuna SMTP istemcisini tanıtmak için kullanılmakta ve argüman alanı, SMTP istemcisinin alan adından oluşmaktadır. |
| MAIL | *MAIL FROM:<gönderen e-posta adresi>* | Mesajı gönderen e-posta adresini sunucuya bildirir. |
| RCPT | *RCPT TO:<gönderen e-posta adresi>* | Mesajı alacak e-posta adresini sunucuya bildirir. |
| DATA | *DATA* | E-posta içeriğini oluşturacak mesajın sunucuya gönderme işleminin başlatılacağı bilgisini sunucuya bildirir. |
| RSET | *RSET* | Sunucu bağlantısını yeniden başlatır. |
| VRFY | *VRFY <kullanıcı>* | Belirtilen kullanıcının alıcı sunucu tarafından doğrulamasını ister. |
| EXPN | *VRFY <dağıtım listesi>* | Belirtilen dağıtım listesinin alıcı sunucu tarafından doğrulamasını ister. |
| HELP | *HELP [yardım konusu]* | Belirtilen konuyla ilgili yardım bilgisinin alınmasını sağlar. |
| NOOP | *NOOP* | Bu komut, bağlantının kurulduğu karşı tarafın bağlantıya cevap verip vermediğinin kontrol edilmesini sağlar. Alıcının OK yanıtı göndermesi dışında hiçbir faaliyet belirtmez. |
| QUIT | *QUIT* | Sunucuyla kurulan bağlantının sonlandırılmasını sağlar. |

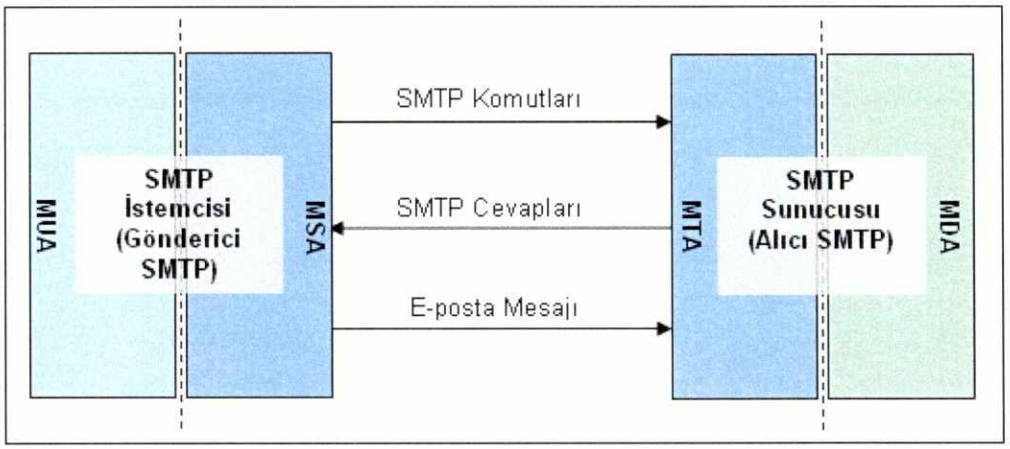
Sunucu kendisine gelen taleplere üç basamaklı rakamlardan oluşan kodlarla cevap vermektedir. Bu kodların ilk basamağı sunucu tarafından verilen cevabın olumlu veya olumsuz olma koşuluna göre sınıflandırmayı ifade ederken ikinci basamak verilen cevaplara ilişkin daha detay bilgileri ifade etmektedir. Son basamak ise ikinci basamakta verilen açıklayıcı bilginin ayrıntısını içeren kodlamadır. Bu gruplandırma Çizelge 2.2'de listelenmiştir.

Çizelge 2.2 SMTP Sunucu Cevapları [15]

| KOD GRUBU | AÇIKLAMA |
|---|---|
| 1XX | Komutun kabul edildiğini ifade etmektedir ancak komutla istemci tarafından talep edilen işlemin geçici olarak askıya alındığını belirtmektedir. |
| 2XX | Talep edilen işlemin başarıyla gerçekleştiğini ifade etmektedir. |
| 3XX | Komutun kabul edildiğini ifade etmektedir ancak komutun tamamlanabilmesi için istemciden gerekli bilgilerin gelmesi beklendiğini ifade etmektedir. |
| 4XX | İstemci tarafından gönderilen komutun geçici bir problemden dolayı kabul edilmediğini ancak bu komutun istemci tarafından daha sonra tekrar gönderildiği takdirde olumlu sonuç dönebileceğini ifade etmektedir. |
| 5XX | İstemci tarafından gönderilen komutun kabul edilmediğini ve bu problemin kalıcı olduğunu ifade etmektedir. |
| X0X | Komutlarla ilgili sözdizimsel hataları ifade etmektedir. |
| X1X | Komutlara ilişkin bilgi içeren ifadelerdir. |
| X2X | Sunucu ile istemci arasındaki bağlantıya ilişkin açıklamalardır. |
| X3X | Belirtilmemiştir |
| X4X | Belirtilmemiştir |
| X5X | Veri iletişiminde istemci tarafından talep edilen işleme ilişkin sunucunun durumunu ifade etmektedir. |

#### 2.5.1.2 SMTP işleyişi

E-posta iletileri SMTP protokolü ile sunucular arasında taşınarak alıcılarına ulaştırılırlar. Bu iletişimde gönderen ve alıcı olarak görev yapan iki MTA bulunmaktadır. Bu MTA'lardan gönderme işini yapan sunucu SMTP istemcisi, alıcı olarak görev yapan sunucu ise SMTP sunucusu olarak rol almaktadır. SMTP iletişiminde TCP port 25 kullanılmaktadır. SMTP sunucusu bu portu sürekli dinleyerek bir istek olup olmadığını kontrol etmekte ve bir bağlantı isteği algıladığında gerekli kontrolleri yaparak istemciye cevap göndermektedir.




Şekil 2.4 SMTP İşleyişi

SMTP iletişimi istemciden sunucuya gönderilen komutlar ve sunucudan gelen nümerik cevap kodları ve açıklamaları ile yürütülmektedir. İki MTA arasında gerçekleşecek olan veri transferi SMTP istemcisi ile SMTP sunucusu arasındaki bağlantının kurulmasıyla başlamaktadır.

TCP port 25'ten IP tabanlı bağlantının kurulmasının ardından sunucu ve istemci arasında bir oturum başlatılması gerekmektedir. Kurulan bağlantı üzerindeki oturum talebi, istemcinin *EHLO* komutu ile sunucuya kendisini tanıtması ile başlamaktadır. Sunucu kendisine komut parametresi olarak gelen istemcinin alan adı ile TCP bağlantısındaki Ip bilgilerini karşılaştırarak kimlik doğrulamasına ilişkin kontrolleri gerçekleştirmektedir. Doğrulamanın gerçekleşmesi durumunda oturum talebine olumlu yanıt vermekte, aksi durumda ise talebi reddetmektedir.

Oturumun başlatılmasının ardından, istemci tarafından *MAIL* komutu ile e-posta gönderen adres bilgisi sunucuya iletilmektedir. Ardından e-posta alıcı bilgileri *RCPT* komutu ile bildirilmektedir. Bir e-posta dağıtım listesinde birden fazla alıcı bilgisi bulunması durumunda *RCPT* komutu her defasında bir alıcı adresini göndermek üzere alıcı sayısı kadar işletilmektedir.

*DATA* komutu ile de istemci tarafından e-posta içeriğinin gönderilmeye başlatılacağının sunucuya bildirilmesi sağlanmaktadır. Sunucu bu komuta vereceği cevap ile mesaj gönderiminin başlatılabileceğine ilişkin onayın yanında, mesaj içeriğinin hangi karakter dizisi ile sonlandırılması gerektiği bilgisini de göndermektedir. İstemci tarafından mesaj içeriği sonuna sunucudan gelen sonlandırma karakter dizisi de eklenerek mesaj verisi gönderme işleminin sonlandırılması sağlanmaktadır.

İstemci tarafında gönderilmeyi bekleyen başka e-posta mesajı bulunması durumunda mesaj gönderme işlemi tekrar edilmekte, kuyrukta bekleyen bir mesaj bulunmadığı durumda ise istemciden gönderilecek *QUIT* komutu ile sunucudan alınacak onay cevabının ardından bağlantı sonlandırılmaktadır [16, 17].


Şekil 2.5 Sunucu–İstemci Arasındaki SMTP Haberleşmesi (E-posta Gönderimi) [17]

### 2.5.2 POP

E-posta sunucusu üzerinde bulunan ve alıcının posta kutusunda saklanan iletilerin kullanıcıya gösterilmek üzere MUA tarafından istemciye kopyalanması için gerekli iletişim ve veri alışverişini düzenleyen standart ve kuralları içeren protokoldür. Bu protokol ilk olarak 1984 yılında geliştirilmiş olup, günümüzde üçüncü versiyonu olan POP3 kullanılmaktadır [7].

#### 2.5.2.1 POP komutları

E-posta sunucusu üzerinde bir kullanıcıya ait posta kutusundaki mesajların görüntülenebilmesi için sunucu ile istemci arasındaki iletişim Çizelge 2.3'te listelenen komutlar ile gerçekleşmektedir. İstemciden sunucuya gönderilen komutlar ve sunucunun bu komutlara verdiği cevaplar ile iletişim yönetilmekte ve süreç işletilmektedir.

Çizelge 2.3 POP Komutları [7]

| KOMUT | KULLANILIŞI | AÇIKLAMASI |
|---|---|---|
| USER | *USER <kullanıcı adı>* | Kullanıcı adı sunucuya gönderilmektedir. |
| PASS | *PASS <şifre>* | Kullanıcıya ait şifreyi bildirir. |
| STAT | *STAT* | Sunucu üzerindeki posta kutusunun durumunu ve posta kutusundaki ileti sayısını sunucudan talep eder. |
| LIST | *LIST [mesaj numarası]* | Posta kutusundaki komut parametresi ile belirtilen e-postanın listelenmesini sağlar, parametre verilmezse tüm listeyi getirir. |
| RETR | *RETR <mesaj numarası>* | Posta kutusundaki komut parametresi ile belirtilen mesaj içeriğinin istemciye kopyalanmasını sağlar. |
| DELE | *DELE <mesaj numarası>* | Posta kutusundaki komut parametresi ile belirtilen e-postanın sunucudan silinmesini sağlar. |
| RSET | *RSET* | Sunucu üzerinde ilgili posta kutusundaki silinmiş olarak işaretlenen e-postaların silinmemiş olarak işaretlenmesini sağlar. |
| NOOP | *NOOP* | Bu komut, sunucunun bağlantıya cevap verip vermediğinin kontrol edilmesini sağlar. Alıcının OK yanıtı göndermesi dışında hiçbir faaliyet belirtmez. |
| QUIT | *QUIT* | Sunucuyla kurulan bağlantının sonlandırılmasını sağlar. |
| TOP | *TOP <mesaj numarası> <satır sayısı>* | Mesaj numarası belirtilen e-postanın komutta belirtilen sayıda satırının kopyalanmasını sağlar. |
| UIDL | *UIDL [mesaj numarası]* | Mesaj numarası belirtilen e-posta için rakam ve harflerden oluşan tek ve benzersiz bir kimlik bilgisinin sunucudan öğrenilmesini sağlar. |
| APOP | *APOP <kullanıcı adı> <güvenli şifre>* | Posta kutusuna bağlantıyı sağlamak için şifrenin açık bir şekilde gönderilmesi yerine güvenli bir şekilde gönderilmesini sağlar. |

### 2.5.2.2 POP işleyişi

E-posta iletileri POP protokolü ile sunucudan istemciye taşınarak kullanıcılara MUA'lar aracılığıyla ulaştırılmaktadır. İletişimin TCP port 110 üzerinden gerçekleştirilmektedir. POP sunucusu bu portu sürekli dinleyerek bir istek olup olmadığını kontrol etmekte ve bağlantı isteği algıladığında gerekli kontrolleri yaparak istemciye cevap göndermektedir [16].

POP protokolünün son sürümü POP3 olarak adlandırılmaktadır. POP3 sunucusu ve istemcisi arasındaki iletişim üç aşamada gerçekleşmektedir. Bu aşamaları belirten durumlar şu şekilde sıralanmaktadır [18]:

- Yetkilendirme Durumu
- İşlem Durumu
- Güncelleştirme Durumu

*Yetkilendirme Durumu*, sunucu üzerindeki posta kutusuna bağlanmak üzere oturum açma işlemini kapsamaktadır. Oturumun açılabilmesi için istemci tarafından iletilen kullanıcı adı ve şifre bilgilerinin sunucu tarafından doğrulanması gerekmektedir. POP protokolünün ilk ortaya çıktığı dönemlerde şifre bilgisi istemciden sunucuya gönderilirken açık olarak gönderilmekte, herhangi bir güvenlik önlemi bulunmamaktaydı. Bir güvenlik açığı oluşturması nedeniyle daha sonra geliştirilen yöntemlerle şifrenin taşınması güvenli bir hale getirilmiştir. POP3 sunucusu tarafından kimlik doğrulamasına olumlu cevap verilmesiyle birlikte posta kutusuna bağlantı sağlanmakta ve oturum açıma işlemi tamamlanmaktadır. Oturumun açılmasıyla birlikte posta kutusundaki e-postalar üzerinde işlem yapıldığı sırada yeni bir iletinin posta kutusuna eklenmesi, işlemlerde karışıklığa neden olabileceğinden sunucu posta kutusunu kilitlemektedir. Posta kutusunun kilitli kaldığı bu süre içerisinde kullanıcıya gelen e-postalar sunucu üzerinde önbellekte tutulmakta ve posta kutusu üzerindeki kilit kaldırıldığında buraya eklenmektedir.

*İşlem Durumu* ise sunucu üzerinde bulunan posta kutusundaki iletiler üzerinde Çizelge 2.3'te verilen komutlar yardımıyla istenilen işlemlerin gerçekleştirilmesini kapsamaktadır. Posta kutusu üzerinde yapılacak işlemlerin tamamlanmasının ardından oturumun kapatılması amacıyla istemciden sunucuya *QUIT* komutu gönderilmektedir. Bu komutla birlikte *İşlem Durumu* sona erdirilerek *Güncelleme Durumu* başlatılmaktadır.

QUIT komutunun sunucuya ulaşması ile birlikte *Güncelleme Durumu*'na girilerek, istemci tarafından posta kutusu üzerinde *DELE* komutuyla *silindi* olarak işaretlenen iletilerin silinme işlemi gerçekleştirilmektedir. Bu işlemle birlikte oturum sonlandırılmakta ve sunucu ile istemci arasındaki TCP bağlantısı kapatılmaktadır.

### 2.5.3 IMAP

POP protokolü gibi e-posta sunucusu üzerinde bulunan ve alıcının posta kutusunda saklanan iletilerin kullanıcı tarafından yönetilmesi için gerekli iletişimi düzenleyen standart ve kuralları içeren protokoldür. Bu protokol ilk olarak 1988 yılında geliştirilmiş olup, günümüzde dördüncü versiyonu olan IMAP4 kullanılmaktadır [7].

IMAP protokolünün POP protokolüne göre bazı avantajları bulunmaktadır. POP protokolü sunucu üzerindeki e-postaların kopyasını istemci üzerine indirdikten sonra tüm işlemlerin yerel disk üzerinde yapılması gibi bir kısıtlama getirmektedir. Buna karşın IMAP, e-postaları istemci üzerine indirmek yerine sunucu üzerinde kalmasını temin ederek MUA tarafından yapılan tüm işlemlerin sunucu üzerinde gerçekleşmesini sağlamaktadır. Bu olanakla birlikte kullanıcı istemci bilgisayarı kullanarak, sunucu üzerinde mesaj silme, okuma, gönderme, gönderilen iletinin kopyası saklama gibi işlemler ile posta kutusunu yönetebilmektedir. Böylece, kullanıcıya e-postalarına farklı bilgisayarlardan ve farklı lokasyonlardan erişibilme olanağı getirilmiştir [18].

#### 2.5.3.1 Temel IMAP komutları

IMAP protokolünün temel komutları Çizelge 2.4'de listelenmiştir. Bu listenin dışında kalan komutlarla birlikte toplam komut sayısı 25'i bulmaktadır. Komut

sayısının çeşitliliği kullanıcıya daha esnek yönetim olanağı sağlamaktadır. Bu açıdan da POP protokolüne göre daha çok seçenek sunmaktadır.

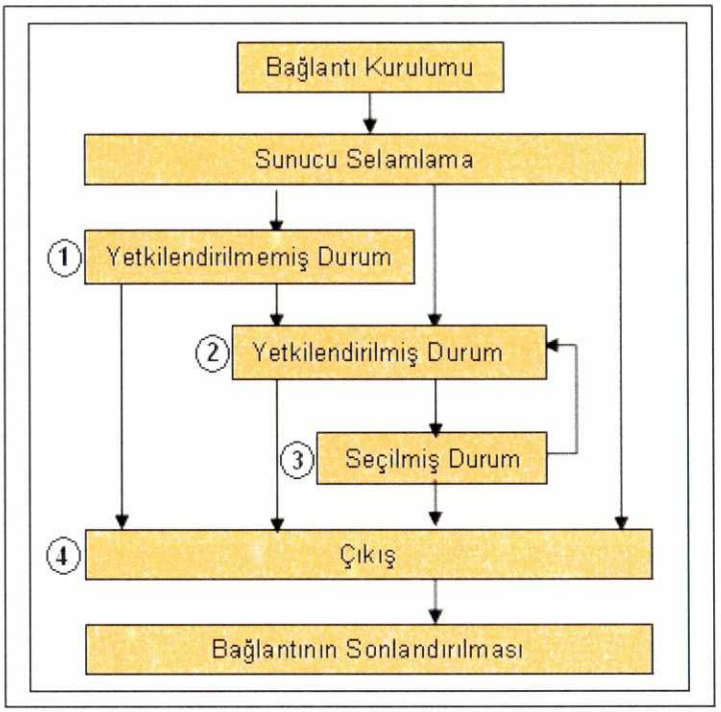
Çizelge 2.4 Temel IMAP Komutları [7]

| KOMUT | KULLANILIŞI | AÇIKLAMASI |
|---|---|---|
| CAPABILITY | *CAPABILITY* | Sunucu tarafından desteklenen özelliklerin listelenmesini sağlar. kullanıcı adını gönderir. |
| NOOP | *NOOP* | Bu komut, sunucunun bağlantıya cevap verip vermediğinin kontrol edilmesini sağlar. Alıcının OK yanıtı göndermesi dışında hiçbir faaliyet belirtmez. |
| LOGOUT | *LOGOUT* | Sunucuyla kurulan bağlantının sonlandırılmasını sağlar. |
| AUTHENTICATE | *AUTHENTICATE <kimlik doğrulama metodu>* | Seçilen kimlik doğrulama metodunu belirtir. |
| LOGIN | *LOGIN <kullanıcı adı> <şifre>* | Kullanıcı adı ve şifre ile sunucuya bağlanmayı sağlar. |
| SELECT | *SELECT <posta kutusu>* | Belirtilen posta kutusuna bağlanmayı sağlar. |
| EXAMINE | *EXAMINE <posta kutusu>* | Belirtilen posta kutusuna sadece okuma izinli bağlantı sağlar. |
| CREATE | *CREATE <posta kutusu>* | Belirtilen isimle bir posta kutusu oluşturulmasını sağlar. |
| DELETE | *DELETE <posta kutusu>* | Belirtilen posta kutusunun silinmesini sağlar. |
| RENAME | *RENAME <posta kutusu> <yeni posta kutusu>* | Bir posta kutusunun isminin değiştirilmesini sağlar. |

### 2.5.3.2 IMAP işleyişi

IMAP protokolü iletişimde TCP port 143'ü kullanmaktadır [16]. IMAP sunucusu bu portu sürekli dinleyerek bir istek olup olmadığını kontrol etmekte ve bağlantı isteği algıladığında gerekli kontrolleri yaparak istemciye cevap göndermektedir.

IMAP protokolünün son sürümü IMAP4 olarak adlandırılmaktadır. IMAP4 ile sunucu ve istemci arasındaki iletişim Şekil 2.6'da görüldüğü gibi dört farklı durumda gerçekleşmektedir.




Şekil 2.6 IMAP Protokolü Durum Geçiş Diyagramı [19]

İlk olarak sunucu ile sitemci arasındaki TCP tabanlı bağlantının kurulması gerekmektedir. Bağlantının kurulmasıyla birlikte ilk durum olan *Yetkilendirilmemiş Durum* ortaya çıkmaktadır. Herhangi bir kimlik doğrulaması ve yetkilendirme işlemi yapılmadığından komutların işlevselliği bulunmamaktadır.

İstemciden sunucuya ilgili komutlarla gönderilecek kullanıcı adı ve şifre bilgileri ile kimlik doğrulamasının yapılmasının ardından *Yetkilendirilmiş Durum*'a geçilmektedir.

Üçüncü durum ise hangi posta kutusuna erişim sağlanacağının belirlenmesiyle geçilen *Seçilmiş Durum*'dur. Bu duruma geçilmesiyle birlikte seçilen posta kutusunda istenilen işlemler (mesaj okuma, silme, listeleme, gönderme vb.) gerçekleştirilebilmektedir.

Son durum ise *Çıkış Durumu*'dur. Herhangi bir durumdan bu duruma geçiş yapılabilmektedir. Sunucu ile istemci arasındaki bağlantının sonlandırıldığı aşamadır [16].

# 3 E-POSTA HİZMETİNDE SPAM

İstek dışı haberleşme (spam) sayısal ekonomi üzerinde çok olumsuz bir etki yapmakta, ekonomik ve sosyal anlamda önemli bir maliyet oluşturmaktadır.

Günümüzde elektronik haberleşme araçlarında görülen spam oranındaki artışın çok hızlı bir şekilde sürmesi ve özellikle de bu tür mesajların verdiği zararların gerek kişisel anlamda ve gerekse ticari anlamda ciddi boyutlara ulaşmış olması söz konusu araçlara olan güvenilirliğini zedelemektedir.

Bu bölümde, öncelikle spam tanımı yapılarak karakteristik özellikleri ortaya konacak ve tarihsel gelişimine ilişkin bilgi verilecektir. Ayrıca spam mesajların kullanıldıkları haberleşme teknolojilerine göre çeşitlerine, içerik ve amaç bakımından sınıflandırmasına ve ortaya çıkardığı maliyete ilişkin bilgilere yer verilecektir.

## 3.1 Spam Nedir?

Uluslararası alanda kesin kabul görmüş, üzerinde mutakabat sağlanmış ve çerçevesi tam olarak belirlenmiş bir spam tanımı bulunmamaktadır. Bununla birlikte, aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere zorlayıcı nitelikte gönderilmesine spam denmektedir. İstek dışı haberleşme olarak da adlandırılmaktadır [21].

Spam mesajların her ne kadar kabul gören ortak bir tanımı bulunmasa da bu tür mesajların bazı karakteristik özelliklerinden bahsetmek mümkündür [22].

- **Elektronik Mesaj:** Spam mesajlar elektronik verilerdir. Mobil hizmetler (SMS, MMS vb.) ile IP üzerinden ses iletimi (VoIP) hizmetinde de spam

mesaj sorunu bulunmaktadır, ancak e-posta hizmetinde bu sorun çok ciddi boyutlara ulaşmıştır.

- **Toplu Gönderim ve Tekrarlanma:** Spam mesajlar alıcının adresi dışında herhangi bir bilgi olmaksızın rastgele ve yığın ileti olarak tekrarlı bir şekilde gönderilmektedir.

- **Gizli / Yanlış Mesaj Kaynağı:** Spam mesajların oluşturulması genellikle e-posta mesajının başlık bölümünde bulunan gönderen bilgisinin gizlenmesi veya yanlış bir bilgiyle değiştirilmesi şeklinde olmaktadır. Spam üreticileri çoğunlukla yetkilendirilmemiş üçüncü parti e-posta sunucularını kullanmaktadırlar.

- **Zorlayıcı Nitelik:** Kullanıcılara dağıtım listesinden çıkma ve bir sonraki mesajı almama seçeneği sunmadıklarından zorlayıcı bir nitelik taşımaktadır.

- **Yasadışı / Saldırgan İçerik:** Spam mesajlar genellikle sahtecilik faaliyetlerinde kullanılmakta ve aldatıcı içerik (virüs, solucan vb.) taşıyarak tehdit unsuru olmaktadır. Bunun dışında cinsel içerikli veya terör propagandası gibi yasadışı sayılabilecek içerikli mesajlar da bulunmaktadır.

- **İzinsiz Adres Kullanımı:** Spam üreticileri sahibinin izni olmaksızın toplanan e-posta adreslerini kullanmaktadırlar. E-posta adreslerinin toplanması genellikle internet sitelerindeki casus yazılımlar sayesinde yapılabildiği gibi sözlük yöntemiyle (deneme yoluyla harf dizelerinden anlamlı adresler üretilmesi) de yapılabilmektedir.

## 3.2 Spam Sorununun Gelişimi

İlk spam e-posta 03 Mayıs 1978 tarihinde internetin ortaya çıkışından önce görülmüş olup o tarihte geliştirilmekte olan ARPANET projesinde kullanılmıştır [23]. Gary Thuerk adında bir mühendis tarafından bir ürünün tanıtımında kullanılmıştır. ARPANET üzerinden gönderilen bu mesaj proje yöneticileri tarafından şiddetli bir tepki görmüştür [24].

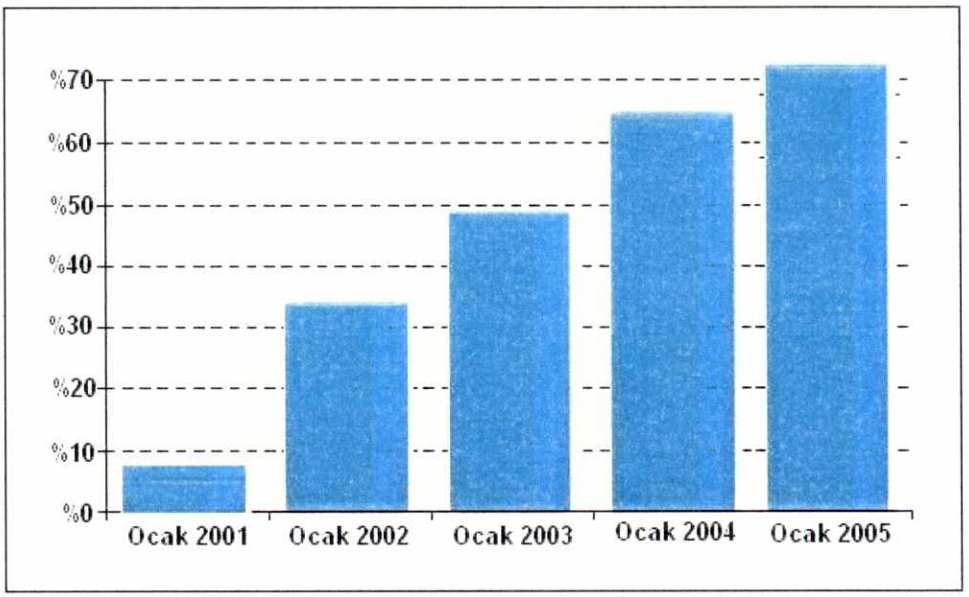
Nisan 1994 tarihine kadar henüz *spam* terimi kullanılmaya başlamamışken Phoenix firmasının Canter ve Siegel isimli iki avukat tarafından internet haber gruplarına reklam amaçlı e-postalar gönderilmiştir [25]. Bu tarihten sonra spam e-posta oranının giderek artan oranlarda seyretmesine rağmen 1997 yılına gelindiğinde henüz kontrol dışına çıkmadığı görülmektedir. Ancak bu yılın sonunda, bir önceki yıla göre katlanarak arttığı görülmüştür. Öyle ki, yılın ikinci yarısında spam e-postalarda 10 katlık bir artış görülmüş, 200 milyon adet e-posta adresi bu yıl içinde spam üreticileri tarafından ücret karşılığında dağıtılmıştır [23].

1997 yılından sonraki üç yıllık periyotta spam sorunu ciddi boyutlara ulaşmış ve tehlike unsuru olmaya başlamıştır. Spam üreten yeni firmaların ortaya çıkışı ve spam tekniklerinin gelişimi bu dönemde spam sorunuyla mücadele etmeyi zorunlu hale getirmiştir. 1998-1999 yıllarında spam oranındaki artış azalmış ancak yine de 3 ile 4 kat arasında bir artış göstermiştir. 2000 yılına gelindiğinde ise artış oranının yine yükselerek devam ettiği görülmüştür.

2001 yılında üssel bir artış gösteren spam, 2002 yılı sonuna gelindiğinde altı yıl önceki oranın yaklaşık 60 katına çıkmıştır [23]. Bu tarihten sonra ise spam sorunu tamamıyla kontrolden çıkmış ve üstesinden gelinmesi çok zor bir hal almıştır. Spam e-posta oranında görülen artış karşısında servis sağlayıcılar sorunun üstesinden gelmek adına yeni yöntemler üretmek zorunda

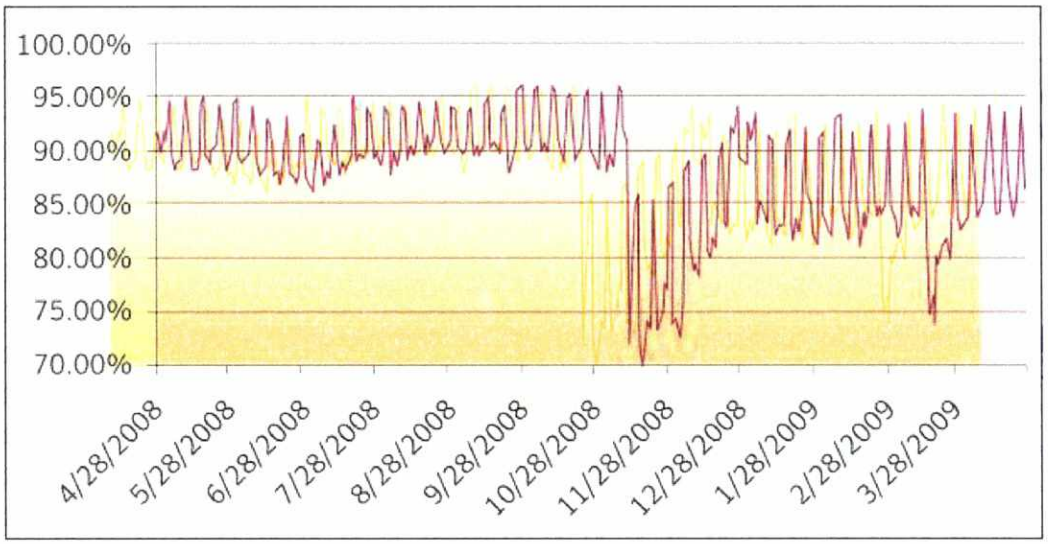
kalmışlardır. Çeşitli filtreleme teknikleri geliştirilmiş, spam oluşturan kaynakların listeleri yayınlanmaya başlamıştır.

Şekil 3.1'de görüldüğü gibi 2003 yılı Ocak ayında tüm e-posta trafiği içinde %50'ye yaklaşan spam e-posta oranının aradan iki yıl geçmesiyle birlikte, 2005 yılı Ocak ayında %70'e çıktığı görülmektedir [26, 27].



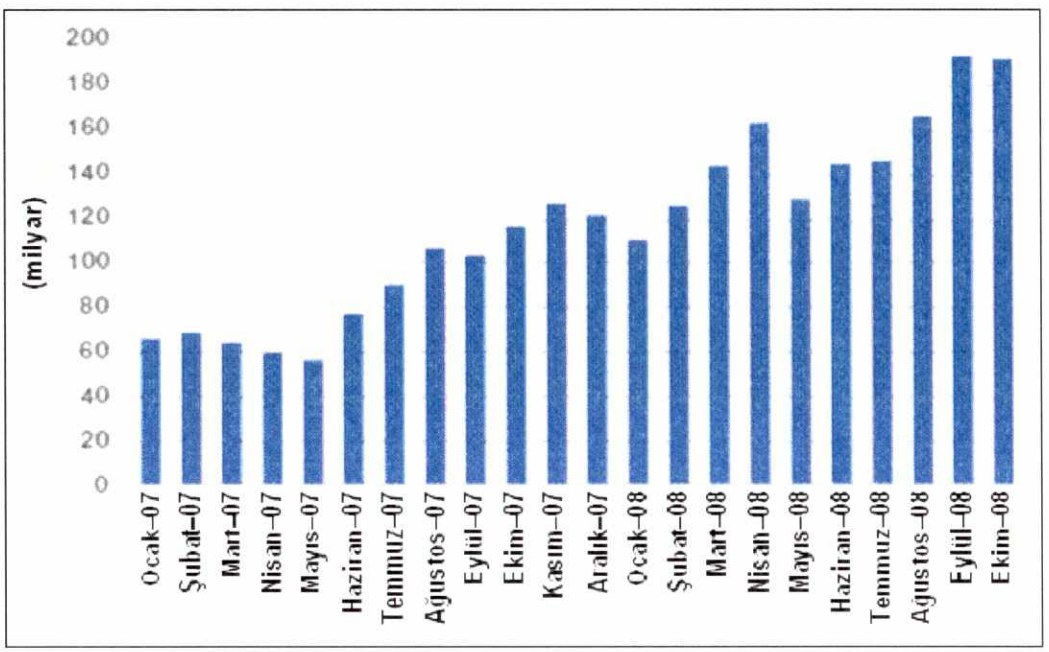

Şekil 3.1 Ocak 2001-2005 Dönemindeki Spam E-posta Oranı

Spam sorunu günümüzde de artarak devam etmekte ve internetin yaygınlaşmasıyla doğru orantılı bir şekilde artış gösterdiği açıkça görülmektedir. Öyle ki, Şekil 3.2'de görüldüğü üzere Nisan 2008 – Mart 2009 arasındaki bir yıllık dönemde spam e-posta oranının toplam e-posta trafiği içerisindeki payı %70'in altına hiç düşmemiş, hatta dönem dönem %95'in üzerine dahi çıkmış olup ortalama %85-%90 arasında seyretmiştir [28].




Şekil 3.2 Nisan 2008 – Mart 2009 Dönemi Spam E-posta Oranı

Bir başka araştırma ise, 2007 yılının Ocak ayında üretilen toplam spam e-posta sayısının 60 milyar civarında olduğunu ancak bu rakamın 2008 yılının Ekim ayında yaklaşık üç kat artarak 180 milyarı geçtiğini göstermektedir (Şekil 3.3) [29].




Şekil 3.3 Ocak 2007 – Ekim 2008 Dönemi Aylık Spam E-posta Sayıları

## 3.3 Spam Çeşitleri

Spam göndermenin maliyetinin düşük olması ve çok geniş kitlelere çok kısa sürelerde ulaşmayı sağlaması başlangıçta e-posta hizmetinde ortaya çıkan bu sorunun giderek diğer elektronik haberleşme araçlarına da sıçramasına zemin hazırlamıştır.

### 3.3.1 E-posta spam

Spam mesajlar ilk olarak e-posta hizmetinde ortaya çıkmış ve zamanla bu alandaki en önemli sorun halini almıştır. Günümüzde de yine en çok spam kullanılan elektronik haberleşme aracı e-posta hizmetidir. Bu alanda spam sorununun ortaya çıkması spam üreticilerinin bu servisin işleyişindeki açık noktaları keşfetmeleri ile çok büyük boyutlara ulaşmıştır. SMTP protokolünün spam karşısında açık oluşturan iki unsurunu şu şekilde saymak mümkündür [22];

- Kimlik doğrulama işleminin zorunlu kılınmaması, kullanıcılara kimliklerini gizleyerek e-posta gönderme imkanı sağlamıştır. Bu da spam üreticileri için bir gizlenme mekanizması oluşturmuştur.
- E-posta mesajlarındaki başlık bilgisi ve mesaj içeriği de dahil olmak üzere her türlü verinin değiştirilebilir olması alıcıların yanıltılmasına neden olmaktadır. Öyle ki e-posta alıcısının, güvendiği bir kişiden geldiğini sandığı mesaj aslında sahtecilik içerebilme riski taşımaktadır.

### 3.3.2 Mobil spam

Mobil telefonlarda karşılaşılan spam sorunu diğer alanlara göre daha düşük bir oranda seyretmektedir. Çünkü, mobil telefonlarda spam gönderimi SMS

veya MMS ile gerçekleşmektedir ve bu işlemler her ne kadar tek bir mesaj için az bir ücret karşılığında yapılabiliyor olsa da gönderilen mesaj sayısındaki artışın maliyete etkisi doğru orantılı olduğundan daha az tercih edilmesine neden olmaktadır.

Ancak, üçüncü nesil mobil hizmetleriyle birlikte mobil telefonlarla internet bağlantısı yapmak ve e-postalara ulaşmak mümkün olduğundan e-posta yoluyla gelen spam mesajlar mobil telefonlar için de bir sorun teşkil etmektedir [22].

### 3.3.3 VoIP spam

IP üzerinden ses iletimi sağlayan VoIP teknolojisinin dünyanın bir ucundan diğer ucundaki kullanıcılara çok düşük maliyetlerle ulaşmayı sağlaması spam üreticilerinin dikkatini bu alana çekmektedir. Saniyeler içerisinde çok büyük miktarlarda sesli mesajı dünyanın dört bir tarafına göndermek mümkündür. Bu açıdan bakıldığında spam mesaj sorunu VoIP için de mücadele edilmesi gereken bir sorun olma niteliği taşımaktadır [22].

### 3.3.4 Arama motoru spam

Çok büyük bir hızla genişleyen internet ortamında, kayıtlı internet sitesi sayısı her geçen gün artarak devam etmektedir. Bu kadar büyük bir ortamda kullanıcıların aradıkları bilgiyi barındıran sitelere ulaşabilmelerini sağlamak amacıyla arama motorları ortaya çıkmıştır.

E-posta hizmetinde olduğu gibi yeni hizmetler ve uygulamalar, spam üreticileri açısından amaçlarını gerçekleştirebilecekleri yeni fırsatlar olarak değerlendirilmektedir. Arama motorlarındaki spam sorunu da her ne aranırsa aransın, belirli internet sitelerinin (cinsel içerikli siteler, çeşitli ürün tanıtım

siteleri vb.) arama sonuçlarının en üst sıralarında listelenmesini sağlamak şeklinde görülmektedir [22].

### 3.3.5 Blog spam

Kişilerin bir konu üzerinde fikirlerini ve düşüncelerini ortaya koyduğu sanal tartışma platformları olan (weblog-web günlüğü vb.) web uygulamalarında da spam sorunu giderek artmaktadır.

Blog'ların yorum sayfalarında web sitelerinin reklamlarının yapılması şeklinde gerçekleşmektedir. Bir web günlüğü barındırma servisi olan *Blogger* tarafından 2005 yılının Ekim ayında bir hafta içerisinde 13 bin adet blog spam tespit edildiği ifade edilmiştir [22].

Blog spam sorununun artarak devam etmesi hem Blog'ların işlevselliğine zarar vermekte hem de internette yayınlanan bilgiler üzerindeki güvenilirliği zedelemektedir.

### 3.3.6 Spam ve sazan avlama (phishing)

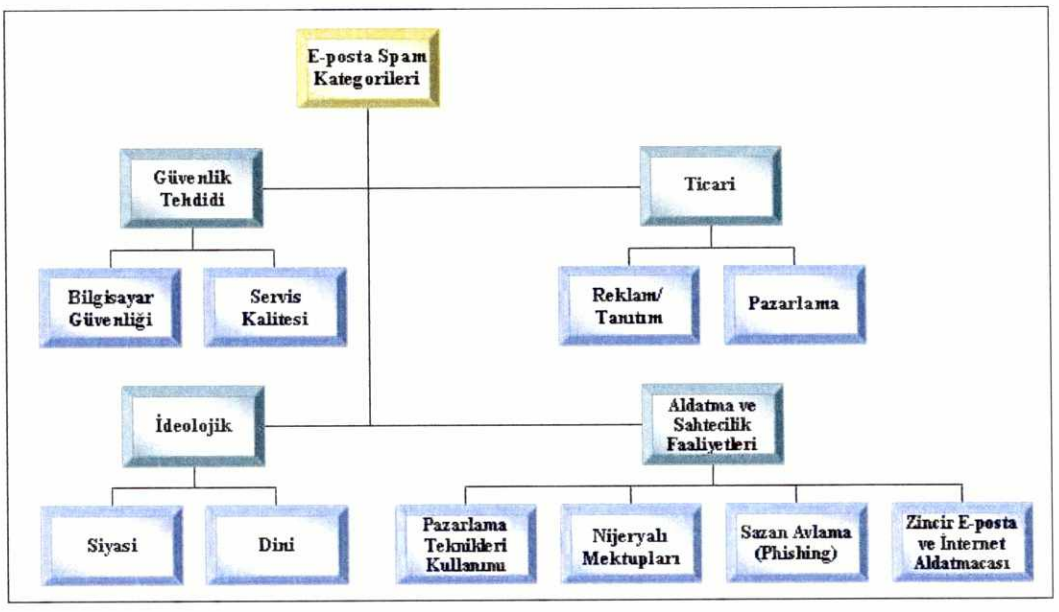
*Sazan Avlama*, sahtecilik ve dolandırıcılık amaçlı bir faaliyettir. Genellikle bir kurum ya da kuruluşun ismi kullanılarak yasal bir işlem yapılıyormuş gibi gösterip kullanıcıların kişisel bilgilerini (kredi kartı numarası, şifre vb.) elde etmek şeklinde ortaya çıkmaktadır. Kullanıcılarla sağlanan irtibat iki yöntemle gerçekleşmektedir. Bunlardan bir tanesi e-posta veya SMS mesajları ile kullanıcıyla iletişimin sağlanması ve kişisel bilgilerinin elde edilmesidir. Diğer yöntem ise hedef alınan kurum ya da kuruluşun web sitesinin birebir sahtesinin oluşturularak yayınlanması ve kullanıcıların bu sayfa üzerinden işlem yapmasını sağlamak şeklinde gerçekleşmektedir.

Sazan Avlama ataklarında en çok kullanılan araç e-posta hizmetidir. Kötü niyetli kişiler, gönderdikleri e-postaların mesaj içeriğinde kullanıcı nezdinde inandırıcılıklarını artırmak adına kuruluşun logosunu taklit etmek ve şirketin internet sitesinde bulunan bilgileri sunmak yolunu izlemektedirler.

Sazan Avlama atakları fark edilme ve açığa çıkma riski nedeniyle kısa süren ataklardır. Amaç bu kısa süre içerisinde hedef kitleye ulaşmak ve casus yazılımların kullanıcıya ilişkin kişisel verileri toplayarak bu bilgileri dolandırıcılık faaliyetini yürüten kaynağa göndermesini sağlamaktadır. Ele geçirilen bu bilgilerle banka hesaplarına ulaşmak veya kullanıcıların adına yeni banka hesapları ve kredi kartı hesapları açtırmak suretiyle dolandırıcılık suçları işlenmektedir [22].

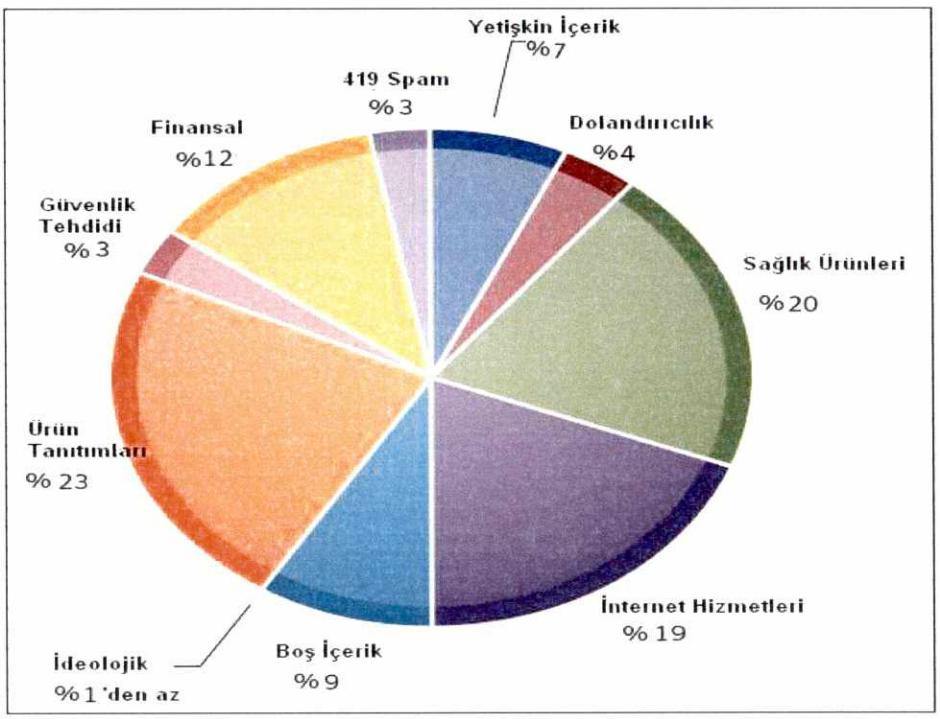
## 3.4 Spam E-posta Kategorileri

E-posta spam mesajlarını, içerik ve amaçlarına göre belli kategorilere ayırmak mümkündür (Şekil 3.4).




Şekil 3.4 Spam E-posta Kategorileri

Spam e-posta kategorileri içerisinde en büyük oran ticari bir ürün ya da hizmetin pazarlanmasını amaçlayan mesajlara aittir. Bu kategorideki spam e-postalar, Şekil 3.5'te görüldüğü gibi tüm spam e-posta kategorileri içerisinde **%81**'lik *(%23-Çeşitli Ürün Tanıtımları + %20-Sağlık Ürünleri + %19-İnternet Hizmetleri + %12-Finansal Konular + %7-Yetişkin İçerik)* bir orana sahiptir. Suç teşkil eden aldatma ve sahtecilik faaliyetleri ise **%7**'lik *(%4-Dolandırıcılık + %3-Nijeryalı Mektupları ya da 419 Spam)* bir oranla ikinci sırada yer almaktadır. Üçüncü sırada, **%3**'lük bir oranla virüs, solucan, truva atı gibi kötü niyetli yazılımların dağıtılması suretiyle güvenlik tehdidi oluşturmayı amaçlayan spam e-postalar bulunmaktadır. En son sırada ise oldukça düşük bir orana sahip **(%1'den daha küçük)** olan ve siyasi, dini ya da kültürel bir düşünceyi yaymayı amaçlayan, ideolojik içerikli spam e-postalar bulunmaktadır [30].




Şekil 3.5 Kategorilerine Göre Spam E-posta Oranları (2009 Şubat)

### 3.4.1 Ticari amaçlı spam e-posta

Doğrudan pazarlama amacı güden spam e-postalar ve bir ürün ya da hizmetin tanıtımını yapmak suretiyle dolaylı olarak pazarlama amacı güden spam e-postalar olmak üzere iki gruba ayrılmaktadır.

#### 3.4.1.1 Reklam ve tanıtım amaçlı spam e-posta

Reklam ve tanıtım amacıyla gönderilen ve doğrudan bir pazarlama faaliyeti içermeyen spam e-postalar kullanıcılara zarar verici özellik taşımamaktadır. Buradaki amaç en kısa sürede geniş kitlelere ucuz ve kısa yoldan ulaşarak tanıtım yapmaktır. Ancak, bu tür mesajların sayıları spam olmayan mesajlara göre çok daha fazladır ve her geçen gün kullanıcılar e-posta kutularının daha fazla spam mesaj ile dolmaya başladığını görmektedir. Söz konusu durum nedeniyle spam mesaj ile spam olmayan mesajların kontrol edilmesi ve ayırt edilmesi ciddi bir zaman kaybı yaşanmasına ve kimi önemli e-postaların gözden kaçmasına neden olmaktadır. Ayrıca, servis sağlayıcıların kaynaklarının bu şekilde meşgul edilmesi de hizmet kalitesinin düşmesine neden olmakta ve önemli bir maliyet oluşturmaktadır.

#### 3.4.1.2 Pazarlama amaçlı spam e-posta

Direk olarak pazarlama amacı güden spam mesajlardır. Şirketler adına geniş kitlelere ulaşmanın kolay ve ucuz bir yoludur. Genellikle şirketlerin direk olarak yürüttüğü bir süreç olmayıp, spam üreticileri ile yapılan anlaşmalar neticesinde bu kaynakların şirketler adına yürüttüğü süreçlerdir.

Bu türdeki e-postalar genelde mortgage, sağlık ürünleri, cinsel içerikli yayınlar ve diyet ürünlerinin tanıtımını amaçlamaktadır. Her ne kadar bu yöntemle yapılan pazarlama sonucunda çok düşük oranlarda satış

yapılmakta ise de e-posta göndermenin maliyetinin çok düşük olması cazibe merkezi haline gelmesine neden olmaktadır.

### 3.4.2 İdeolojik spam e-posta

Bir görüş ya da düşüncenin yayılması amacını güden spam e-postalardır. Siyasi, dini veya kültürel konulardaki fikirleri kitlelere ulaştırmak ve taraftar bulmak üzere gönderilmektedir.

### 3.4.3 Aldatma ve sahtecilik faaliyetlerini içeren spam e-posta

Bu tür spam e-postalar aldatma, sahtecilik ve dolandırıcılık amacı taşımakta ve suç teşkil etmektedir.

#### 3.4.3.1 Pazarlama tekniklerini kullanan sahtecilik

Dolandırıcılık amaçlı kullanılmakta olup normal bir reklam veya pazarlama mesajları olarak gönderilmektedir. Amaç, yapılan işlemin pazarlama amaçlı olduğu konusunda kullanıcıyı ikna etmek ve güven duygusu oluşturmaktır. Ancak söz konusu mesajda bahsedilen ürün ya da servis aslında tamamen sahtecilik faaliyeti olarak kullanılmaktadır. Ürünü satın alan kullanıcı çoğu zaman sahte bir ürünle karşılaşmakta ya da üründen beklediği özellikleri bulamamaktadır. Geri kalan durumlarda ise ödemesini yapmasına rağmen ürün hiçbir zaman kullanıcıya ulaşmamaktadır. Dolandırıcılık faaliyeti kullanıcılar tarafından fark edildiğinde sorumlulara ulaşmak mümkün olmamakta, sorumlular iz bırakmadan ortadan kolayca kaybolmaktadır. Kaybedilen paraların geri iadesi ise böyle durumlarda çoğunlukla mümkün olmamaktadır.

### 3.4.3.2 Nijeryalı mektupları

*Nijeryalı mektupları* ya da *419 dolandırıcılığı* olarak adlandırılmaktadır. Kullanıcı çoğu zaman duygusal olarak sömürülmekte ve uydurma hikayelerle yardım talep edilmektedir. Dolandırıcılık olayına bahse konu hikayede zor durumda bulunan kişi ya da kişiler adına yardım kampanyaları düzenlendiği belirtilmektedir. Kullanıcıların bu sahte durum karşısında duyarlılıkları kullanılarak maddi yardım talep edilmektedir.

Bir başka yöntemi ise sözde bir ticari faaliyete az miktarda bir maddi destek ile ortak olma fırsatı tanınmasıdır. Az miktarda bir para karşılığında çok para kazanma vaatleri, kullanıcıları etkilemekte ve dolandırıcıların ağına düşürmektedir [31].

### 3.4.3.3 Sazan avlama (phishing)

Sahtecilik faaliyetine konu olan spam e-postaların bir kısmı da kullanıcıların banka hesapları, şifreleri, kredi kartı numaraları gibi kişisel bilgilerinin elde edilmesini amaçlamaktadır. Tanınmış şirket ya da kuruluşların ismi kullanılarak gönderilen e-postalar ile kullanıcıdan bir takım kişisel bilgiler istenmektedir. Dolandırıcıların, amaçlarına alet ettikleri firmanın saygınlığı nedeniyle güven duyan kullanıcı, gönderilen e-postanın sahte olduğunun farkına dahi varmadan kendisinden talep edilen bilgileri cevaplamaktadır. Ancak, kötü amaçlı kullanılan bu bilgiler ile çok sayıda insan maddi ve manevi açıdan zarar görmektedir [31].

### 3.4.3.4 Zincir e-posta ve internet aldatmacası (hoax)

Zincir e-postalar birçok kişinin birbirine gönderdiği ve insanların çok fazla ilgisini çekebilecek çoğunlukla da mistik bir hava taşıyan, dini sömürü içeren iletileri ya da duygusal sömürü içerikli e-postaları alıcının listesindeki diğer

kişilerle paylaşmasını isteyen (*"bu mesajı listendeki herkese ilettiğin takdirde tüm problemlerin çözüme kavuşacak ve mutlu olacaksın"* vb.) iletilerdir [31].

İnternet aldatmacası ise bir kurum, kuruluş ya da tanınmış bir kişi hakkında uydurma hikaye ve haberler üreterek zarara uğratmak, kişisel ya da ulusal güvenliği tehdit edecek durum olduğu havası oluşturarak panik havası estirmek şeklinde ortaya çıkmaktadır. Bu tür e-postalar bilinen ve güvenilir olan bir kaynaktan geliyormuş gibi gönderilmekte ve alıcının mesajı listesindeki tüm kişilerle paylaşması istenmektedir [31].

Zincir e-postalar ve internet aldatmacalarının temel amacı mesajların mümkün olduğu kadar çok kişiye ulaşmasını sağlayarak e-posta adreslerinin toplanması sağlamaktır. Bu şekilde ele geçirilen e-posta adresleri üçüncü kişilere bir ücret karşılığında satılmakta ya da spam göndermede kullanılmaktadır. Bu tür mesajların bir başka amacı da e-posta sunucuları üzerinde yoğun bir trafik oluşturmak suretiyle dar boğaz yaratmak ve sunucunun hizmet vermesini engelemek olarak ortaya çıkmaktadır [31].

### 3.4.4 Güvenlik tehditi oluşturan spam e-posta

Bilgisayar sistemleri üzerinde güvenlik açığı oluşturmak veya servis kalitesini düşürmek amacıyla kullanılan iletilerdir. Bilgisayar güvenliği ve servis güvenliği şeklinde iki ayrı başlık olarak ele alınmaktadır.

#### 3.4.4.1 Bilgisayar güvenliği

Virüs, solucan, truva atı ve casus programlar gibi kötü niyetli yazılımlar, bilgisayar sistemlerine sızmak ya da zarar vermek amacıyla üretilmektedir. Bu tür yazılımlar e-posta eklentisi olarak gönderilmektedir. Kullanıcının

dosyayı açmasıyla birlikte kötü niyetli yazılım kurulumunu bilgisayar üzerinde gerçekleştirmektedir.

Spam e-postalar ile kötü niyetli yazılımlar arasında iki yönlü bir bağımlılık söz konusudur. Spam e-postalar bu tür yazılımları yayarken, casus yazılımlar da bilgisayarı kontrol altına alarak spam e-posta üretmesine neden olmaktadır. Spam yayan bu bilgisayara ***zombi***, oluşturdukları topluluğa ise ***robot ağ (botnet)*** denilmektedir. Kullanıcısının bilgisi dışında gerçekleşen bu işlem ile birlikte bilgisayar zararlı bir faaliyetin bir parçası haline gelmektedir.

Kötü niyetli yazılımların bir kısmı da (virüs, solucan truva atı vb.) direk olarak bilgisayarı çalışamaz hale getirmektedir. Kimi durumlarda kontrol altına aldığı bilgisayar üzerinden aynı ağ üzerindeki diğer bilgisayarlara da bulaşarak sistemin tamamına zarar verme noktasına gelmektedir.

Casus yazılımlar ise bilgisayar kullanıcısının yaptığı işlemleri izlemek üzere kullanılmaktadır. Kullanıcının bilgisi dışında faaliyet gösteren bu tür yazılımlar şifre ve kullanıcı adı gibi kişisel verilerin başkaları tarafından öğrenilmesine yol açmakta ve bu bilgiler çoğu zaman suç teşkil eden işlerde kullanılmaktadır.

#### 3.4.4.2 Servis kalitesi

Servis kalitesini ve kullanılabilirliğini olumsuz yönde etkileme amacı gütmektedir. Bu tür ataklar, e-posta sunucusu üzerinde darboğaz yaratacak şekilde trafik oluşturma biçiminde gerçekleşmektedir. Çoğu zaman sunucu, kendisine gelen trafiği yönetemeyecek duruma gelmekte ve servis verememektedir. Kullanıcıların e-posta gönderme ve alma isteğine yanıt veremediğinden servis sağlayıcı açısından bir prestij kaybı oluşturmaktadır.

Bu tür ataklara genel olarak DoS[1] (Denial of Service) atakları da denmektedir.

## 3.5 E-posta Hizmetinde Spam Maliyeti

Spam maliyetinin değerlendirilmesi iki farklı açıdan ele alınmalıdır. Spam üreticileri için maliyeti ayrı olarak değerlendirilmeli, spam e-postalardan zarar gören ya da görmesi muhtemel kişi ya da kuruluşlar açısından ayrıca ele alınmalıdır. Spam göndermek maliyet açısından çok ucuz bir yöntemdir. Geleneksel pazarlama teknikleriyle karşılaştırıldığında maliyeti çok önemli ölçüde daha düşüktür ve bu nedenle çok fazla tercih edilen bir yöntem durumuna gelmiştir. Ancak, spam mesajlar nedeniyle zarar görmesi muhtemel olanlar için önemli ölçüde maliyet oluşturmaktadır.

### 3.5.1 Spam oluşturma maliyeti

*SpamCon Foundation* tarafından hazırlanan bir rapora göre bir adet spam e-postanın maliyeti gönderen için *0,001 sent* kadarken spam alan biri için bu maliyet *10 sent*'tir [33].

Spam göndermenin maliyetini oluşturan unsurlar şunlardır;

- **İnternet Bağlantısı:** Bir spam e-posta oluşturmak için gerekli olan ilk şey bir internet bağlantısıdır. Günümüzde servis sağlayıcıların sunduğu çok çeşitli uygun seçenekler bulunmaktadır. Aylık ortalama 10 dolarlık ücret karşılığında herhangi bir servis sağlayıcıdan bir internet bağlantısı tedarik etmek mümkündür.

[1] DoS: Bir sistemin hizmet vermesini engellemeye ya da aksatmaya yönelik bir saldırı çeşitidir. Hedef bilgisayara ya da sisteme ait tüm kaynakların tüketimi amaçlanarak işlemez duruma getirilmeye çalışılmaktadır [32].

- **Yazılım:** Spam göndermek için zorunlu unsurlardan biri de yazılımdır. Spam göndermek için tasarlanmış özel yazılımlar mevcuttur ve bu yazılımları edinmenin maliyeti yaklaşık 1000 dolar civarındadır.
- **E-posta Adres Listesi:** Çoğu spam üreticisinin kendi oluşturduğu bir adres listesi mevcuttur. Spam üreten kişi ya da şirketler, içerisinde milyonlarca adres bulunan bu listeleri bir ücret karşılığında dağıtmaktadırlar. Bu listeleri yaklaşık olarak 50 dolar bir maliyetle tedarik etmek mümkündür.

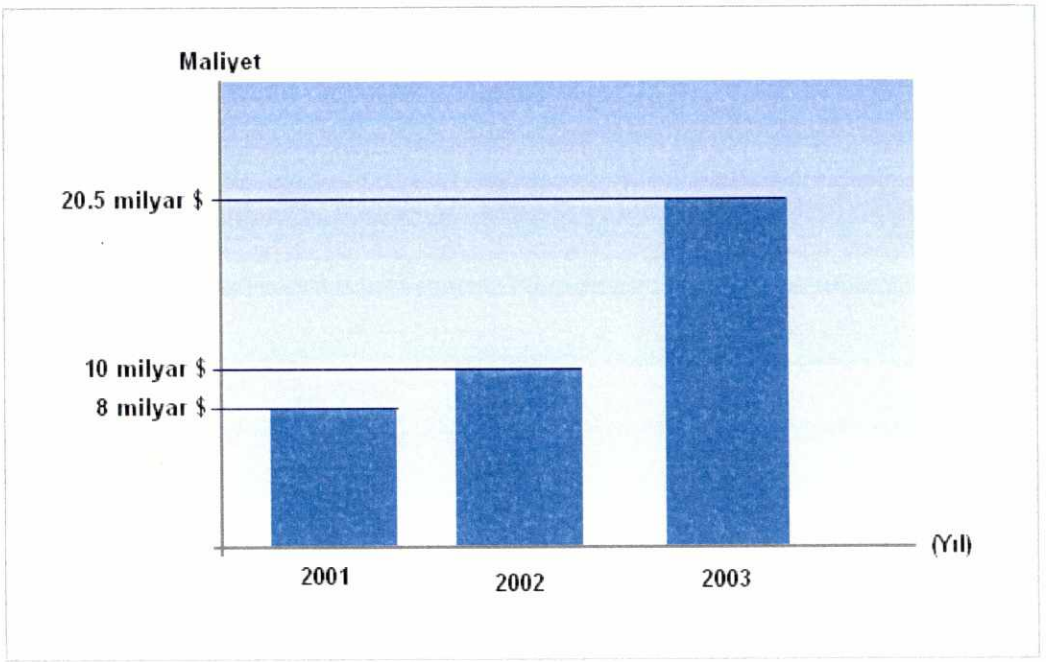
Bütün gereksinimlerin maliyetleri üst üste eklendiğinde çok küçük sayılabilecek bir harcamayla birkaç saat içerisinde on binlerce spam e-posta gönderebilme kapasitesine sahip olmak mümkündür. Bu da spam göndericiler için oldukça avantajlı bir durum oluşturmaktadır [33].

### 3.5.2 Spam e-postanın alıcılara maliyeti

Spam e-postalar internet kullanıcılarını kişisel anlamda direk olarak etkilemektedir. Gelen e-postaların spam olup olmadığının incelenmesi ve istenmeyen e-postaların silinmesi için harcanan zamanın dışında, e-posta hizmetine olan güvenin zedelenmesi de negatif bir sonuç olarak ortaya çıkmaktadır. Spam e-postaların yanıltıcı ya da aldatıcı mesajlar içermesi, virüs ve/veya solucan gibi zararlı etkilere neden olan uygulamalar içermesi ve sahte ürün ya da servis pazarlaması gibi etkileri bu güven bunalımının ortaya çıkmasına neden olan başlıca faktörlerdir.

Avrupa Birliği (AB) tarafından 2001 yılında yapılan bir araştırma sonucuna göre spam mesajların tüketicilere, ticari işletmelere ve servis sağlayıcılara yaklaşık maliyetinin 8 milyar dolar olduğu ifade edilmiştir [33]. 2002 yılında üretilen spam mesajların spam üreticilerine toplam maliyeti 270 milyon dolar seviyesinde iken bu rakam dünyanın geri kalanı için yaklaşık maliyet 10 milyar dolar olarak ortaya çıkmıştır. 2003 yılına gelindiğinde bu rakamın

yaklaşık 20.5 milyar dolara çıktığı görülmektedir. Bu maliyetin bir kısmı üretimin durması ve zaman kaybı olarak ortaya çıkarken bir kısmı da spam nedeniyle üretim için gerekli hammaddelerin tedarikçilerinde oluşan sorunların dolaylı yollardan yansıması şeklinde gerçekleşmektedir.




Şekil 3.6 Spam E-postaların Neden Olduğu Maliyet (2001 - 2003)

İş dünyasında spam maliyetinin yansıması bir çalışan başına yıllık ortalama 600 dolar ile 1000 dolar arasında bir rakam şeklinde gerçekleşmektedir [33]. 100 çalışanı bulunan bir işletme açısından ele alındığında bu maliyetin toplamı yıllık 60.000 ile 100.000 dolar arasında gerçekleşecektir. Spam e-postaların getirmiş olduğu sorunlar nedeniyle ortaya çıkan maliyeti oluşturan unsurları;

- Zaman kaybının ortaya çıması ve bu süre içerisinde üretimin durması ya da yavaşlaması,
- Ağ trafiğinin sürekli meşgul edilerek iletişimin işlemez hale getirilmesi,
- Disk alanlarının doldurularak kullanılamaz hale getirilmesi,

- Sistem kaynaklarının (yazıcı, işlemci, RAM, disk vb.) sürekli meşgul edilerek işlemez hale getirilmesi,
- Üretim araçlarının (fabrikalarda üretim, paketleme yapan makineler vb.) işlemez hale getirilmesi,

şeklinde sıralamak mümkündür.

Bütün bu riskler ve spam sorununun günümüzde ulaştığı boyut göz önüne alındığında koruma kalkanı oluşturmanın kaçınılmaz bir zorunluluk olarak ortaya çıktığı açıkça görülmektedir. Spam e-postalara karşı bir önlem almamış olmak hem ticari ve kişisel riskleri beraberinde getirecek hem de bir sorun oluştuğunda üstesinden gelmek zaman alıcı ve zahmetli bir iş olacaktır.

Bu nedenle İSS ve EPS'ler tüketicilerine verdiği hizmet kalitesini artırmak ve tüketicinin güven duygusunu pekiştirmek adına teknik çözümler üretmekte, spam filtreleme yazılımları kullanmaktadırlar. Yine yerel ağı bulunan kurum ve kuruluşlar e-posta sunucularına gelebilecek spam mesajların olası zararları karşısında sistemlerini ve kullanıcılarını korumak adına teknik çözümlere yatırım yapmaktadırlar.

# 4 SPAM ÖNLEME TEKNİKLERİ

E-posta hizmetinde büyük bir sorun olarak karşımızda duran spam mesaj oranı gün geçtikçe daha da artmakta ve tehlikeli bir hal almaktadır. E-posta hizmetini ciddi anlamda tehdit eden bu durum karşısında bir koruma kalkanı oluşturmak kaçınılmaz olmuştur. Bu amaçla çeşitli teknik çözümler geliştirilmiş son kullanıcıların ve servis sağlayıcıların daha güvenilir bir ortamda çalışmaları amaçlanmıştır.

Bu bölümde, e-posta hizmetinde yaşanan spam sorununun çözümüne yönelik en yaygın kullanım alanına sahip olan ve en etkili çözümler sunan tekonolojik yöntemler ele alınacak, güçlü ve zayıf yönleri açıklanacaktır. Spam sorunuyla etkili bir mücadele yürütmek bu yöntemlerden sadece birini tercih edip uygulamakla mümkün değildir. Etkili sonuçlar elde etmek için söz konusu yöntemlerin en az birkaç tanesinin birlikte ve bütünlük içerisinde çalışması gerekmektedir.

Bu bölümde, spam sorununun teknik anlamda çözümü temelde üç açıdan ele alınacaktır:

- Giden e-posta spam sorununun çözümleri
- Gelen e-posta spam sorununun çözümleri
- Diğer yöntemler

## 4.1 Giden E-posta Spam Çözümleri

Spam sorununa karşı etkili bir mücadele göstermenin ilk adımı servis sağlayıcıların kendi iletişim altyapılarından üretilip dağıtılan spam e-posta sorununa yönelik çözüm üretmeleridir. Günümüzde spam e-posta dağıtım kaynağı olan bir servis sağlayıcı kolaylıkla deşifre edilmekte ve internet dünyasının bilgisine sunulmaktadır. Bunun bir sonucu olarak da çoğu zaman

diğer servis sağlayıcılar tarafından, spam dağıttığı tespit edilmiş kaynaklardan gelen e-posta iletişimi kapatılmaktadır. Bu anlamda spam dağıtan bir şebeke durumuna düşmek servis sağlayacılar adına hem prestij kaybı oluşturmakta hem de kullanıcılarına sunulan e-posta hizmetinin kalitesinde düşüş yaşanmasına neden olmaktadır. Söz konusu soruna çözüm oluşturan yöntemler aşağıda açıklanmıştır.

### 4.1.1 Port 25'in kapatılması

SMTP bağlantılarında otomatik olarak port 25 kullanılmaktadır ve bu port aracılığıyla yapılan iletişimde kimlik doğrulama zorunluluğu bulunmamaktadır. Bu nedenle robot ağlar korumasız SMTP anahtarlamasını kullanmak suretiyle 25 nci porttan spam yaymakta ve bilgisayarları kontrol altına alarak robot ağa dahil etmektedir. Araştırmalar spam oluşturan etkenlerin başında zombi bilgisayarların geldiğini göstermektedir. Öyleki bu oranın toplam spam e-posta içerisinde %80 oranında olduğu ifade edilmektedir [34]. Spam yayan zombi bilgisayarların çok büyük bir oranda dinamik IP kullanan bilgisayarlar aracılığıyla yayılıyor olması İSS'lerin bunları tek tek deşifre ederek engellemesini olanaksız kılmaktadır.

Bir İSS'nin şebekesinden dağıtılan spam e-postaların çok büyük bir oranda zombi bilgisayarlar aracılığıyla port 25'nin kimlik doğrulama zorunluluğu bulunmamasını kullanarak üretiliyor olması bu konuda önlem alınmasını zaruri kılmaktadır. Bu kapsamda, İSS'lerin şebekelerinden spam e-posta dağıtımını önlemelerinin en etkili yöntemlerinden birinin dinamik IP'li kullanıcılar için SMTP bağlantısında 25 nci portun kullanımının iptal edilerek yerine daha güvenilir olan 465 nci ya da 587 nci portun kullanılması olacağı değerlendirilmektedir. Böylece İSS'ler şebekelerinden çıkacak olan SMTP trafiğine izin vermeden önce kullanıcının hizmet aldığı e-posta sunucusundan gerekli bilgilerin doğrulanmadığı durumlarda spam e-posta trafiğini deşifre

etmiş olacak ve bu trafiği engelleme olanağına sahip olacaktır. Birçok İSS, spam ile mücadelede bu yöntemi kullanmaktadır [26,34].

**Dezavantajı:**
Dinamik IP'li kullanıcılar için Port 25'in kapatılarak 465 inci ya da 587 nci portların kullanımı, evde ya da işte kişisel amaçlı olarak e-posta sunucusu barındırmayı olanaksız kılacaktır.

### 4.1.2 SMTP trafik sınırlaması

İSS tarafından SMTP trafiğine bir sınırlama getirilmektedir. Bu sınırlama ile belirli bir kaynaktan yapılan SMTP trafiği limit değerlerin dışına çıktığı takdirde zombi bilgisayar olacağı düşünülmekte ve bu kaynaktan gelen trafik engellenmektedir. Bu yöntemle, İSS'ler kendi servisleri aracılığıyla spam e-posta yayan zombi bilgisayarların deşifre edilmesini sağlamaktadır.

Uygulanması oldukça kolay ve giden e-posta spam önlemede etkili bir yöntemdir. Ancak SMTP trafiğine getirilecek limit değerin belirlenmesine dikkat edilmelidir. Bu değerin çok yüksek belirlenmesi zombi bilgisayarların deşifre edilmesindeki etkinliğin azalmasına, çok düşük belirlenmesi ise zombi olmayan bilgisayar kullanıcılarının trafiğinin kesilmesine neden olacaktır. Bu nedenle söz konusu yöntemin uygulanabilmesi için e-posta kullanıcılarının SMTP trafiği üretim miktarı birbirine yakın değerler olmalı, en azından çok büyük farklılıklar göstermiyor olmalıdır. Bu açıdan, İSS'lerin kullanıcılarını davranışlarına göre gruplandırarak uygulaması gereken bir yöntem olduğu mütalaa edilmektedir. Aksi takdirde hatalı çıkarım üretme riski taşımaktadır.

**Dezavantajı:**
Spam göndericilerinin limit trafik değerini belli sınamalar sonucunca öğrenmesi olasılığı mevcuttur. Bu nedenle bu değerin altında üretilen SMTP trafiğinin deşifre edilmesi mümkün değildir.

### 4.1.3 Gönderici kimlik tanımlaması

Kullanıcıların EPS'ler tarafından kimlik tanımlarının yapıldığı ve e-posta gönderme hizmetinden faydalanmadan önce kimlik doğrulama işleminin zorunlu kılındığı yöntemdir. Bu özellik sayesinde kimlik doğrulaması yapılmamış kaynakların e-posta hizmetinden yararlanması engellenmekte ve sunucuların açık anahtarlama (open relay) şeklinde çalışmasının önüne geçilmektedir. Tüm EPS'lerin, giden e-postalarda spam ile mücadelede kullanıcı kimlik tanımlama yöntemlerini kullanmalarının elzem olduğu değerlendirilmektedir [35].

Kullanıcı doğrulama yöntemlerinden bir tanesi de *SMTP-AUTH (Simple Mail Transfer Protocol - Authentication)* mekanizmasının kullanılmasıdır. *AUTH* bir SMTP eklentisidir ve 1999 yılında RFC-2554 ile tanımlanmıştır. E-posta hizmeti ve SMTP protokolünün geliştirildiği dönemde olası güvenlik açıklarının ileride kötü amaçlı kullanılabileceği öngörülememiştir. Bu nedenle e-posta göndericisinin kimlik tespitine ilişkin herhangi bir kontrol mekanizması geliştirilmemiştir. Bu da spam göndericilerinin e-posta sunucularının açık anahtarlama şeklinde kullanılması sorununu ortaya çıkarmıştır. Bu sorunun ortaya çıkışıyla birlikte sunucu ile istemci arasında mesaj transferinden önce gerçekleşen ve *kimlik doğrulama* adımı olarak işleyen SMTP-AUTH geliştirilmiştir. Böylece kullanıcı adı ve şifre üzerinden kişilerin kimlik kontrolünü yapmak olanaklı hale gelmiştir. Bu adımın gerçekleşmesiyle birlikte istemci ile sunucu arasındaki bağlantı süresince kullanıcı doğrulanmış sayılmakta ve e-posta gönderimine izin verilmektedir [36].

**Dezavantajları**

- SMTP-AUTH metodu yetkisiz kişilerin e-posta hizmeti kullanmasının engellenmesini sağlamaktadır. Ancak, kullanıcıya ilişkin şifre bilgisinin spam göndericileri tarafından ele geçirilmesi durumunda bir çözüm

oluşturmamaktadır. Alternatif yöntemlerle beraber kullanılmadığında ele geçen şifreyle doğrulanmış bir oturum açılarak istenilen sayıda spam e-posta gönderilebilmektedir [31].

- Bu yöntemin bir başka dezavantajı da bütün sunucuların SMTP-AUTH özelliğini desteklemiyor olmasıdır.

### 4.1.4 Gönderilen e-posta sayısının sınırlandırılması

E-posta servis sağlayıcıları tarafından uygulanan bir yöntemdir. Belli bir zaman dilimi içerisinde aynı kaynaktan gönderilen e-posta sayısına bir kısıtlama getirmektedir. Söz konusu kaynaktan gönderilen e-posta sayısı belirli bir limiti (örn: bir saat içerisinde gönderilen mesaj sayısı) aştığında bundan sonra gönderilecek olan mesajlar geçici bir süre için engellenmektedir. Bu yöntemle EPS'ler kendi servisleri aracılığıyla spam e-posta yayan zombi bilgisayarların deşifre edilmesini sağlamaktadır.

Uygulanması oldukça kolay ve giden e-posta spam önlemede etkili bir yöntemdir. Bu yöntemin kullanılması durumunda dikkat edilmesi gereken en önemli nokta eşik değerin belirlenmesidir. Bu nedenle söz konusu yöntemin uygulanabilmesi için kullanıcı davranışlarının homojen özellikler gösteriyor olması gerektiği değerlendirilmektedir. Bu açıdan, EPS'lerin kullanıcılarını davranışlarına göre gruplandırarak eşik değer ataması yapmak suretiyle uygulayabileceği bir yöntem olduğu mütalaa edilmektedir. Aksi takdirde hatalı çıkarım üretme riski taşımaktadır. Çünkü her kullanıcının gün içerisinde e-posta gönderme oranı farklıdır. Bu değer düşük bir seviyede belirlenirse spam olmayan e-postaların da engellenmesi sorununu ortaya çıkaracaktır. Aynı şekilde çok yüksek bir seviyede belirlenirse de spam e-postaların gözden kaçmasına neden olacağından etkinliği ve verimliliği büyük oranda azalacaktır.

**Dezavantajı:**
Spam göndericilerinin eşik değeri belli sınamalar sonucunca öğrenmesi olasılığı mevcuttur. Bu nedenle bu değerin altında üretilen spam mesajların deşifre edilmesi mümkün değildir.

## 4.2 Gelen E-posta Spam Çözümleri

Gelen e-postaların incelenerek spam olup olmadıkları konusunda bir çıkarım yapan yöntemlerle sorundan kaçınmak mümkündür. Başlıca spam önleme yöntemleri aşağıda açıklanmıştır.

### 4.2.1 Kara listeleme

Kara liste yöntemi oldukça kullanışlı ve tercih edilen bir spam önleme ve filtreleme yöntemdir. Gerçekleştirilmesi ve yönetilmesi oldukça kolaydır. Kara liste yöntemi bilinen spam e-posta kaynaklarını içeren bir veritabanıdır. Bu yöntemde veritabanı, IP adresi ve alan adları gibi bilgiler bazında tutulabileceği gibi e-posta adresleri bazında da tutulabilmektedir. Bu sayede spam oluşturan kaynağın tümüyle engellenmesinin yanında belli e-posta adreslerinin engellenmesi şeklinde de kullanılabilmektedir. Kara listede yer alan kaynaklardan gelen e-postalar engellenmekte, silinmekte veya işaretlenmektedir. Söz konusu listenin dışında bir kaynaktan gelen e-postalar ise kabul edilmektedir.

Kara liste yöntemi iki şekilde uygulanmaktadır:

- Yerel Kara Listeleme
- Gerçek Zamanlı Kara Listeleme (Real Time Black Lists - RBL)

#### 4.2.1.1 Yerel kara listeleme

Servis sağlayıcıların ya da son kullanıcıların kendi kara listelerini oluşturdukları yöntemdir. Bilinen spam e-posta kaynaklarının IP adresleri, alan adları ve kullanıcı e-posta adresleri bazında tutulmaktadır. Altyapıyı oluşturması kolay bir yöntem olmakla birlikte listenin oluşturulması ve güncellenmesi bakımından zahmetlidir. Etkin olarak kullanılması açısından listenin güncel tutulması zorunludur. Bu anlamda, bu yöntemin yerel olarak uygulanması zaman alıcı ve uğraştırıcı bir yöntemdir.

#### 4.2.1.2 Gerçek zamanlı kara listeleme

Servis sağlayıcılar bu yöntemde kara listelerini kendileri yönetmezler ya da oluşturmazlar. Bunun yerine listeleri oluşturan kuruluşlardan satın alırlar. Bu sayede servis sağlayıcı açısından bakıldığında liste yönetimi aşamasında harcanan emek ve zamandan tasarruf edilmekte ve liste güncelliği kolayca sağlanmaktadır.

Bu listeler DNS üzerinden gerçek zamanlı olarak servis edilmektedir. DNS tabanlı bu listeler *DNS Kara Listeleri (DNS Black Lists - DNSBL)* olarak da ifade edilmektedir. Listelerin gerçek zamanlı tutulması bu yöntemin en dikkat çekici ve etkili noktasıdır. Çünkü spam üreticileri sık sık spam e-posta gönderdikleri IP adreslerini değiştirmektedir. Bu nedenle Kara Liste yönteminin etkinliğini artırmak ve hızlı reaksiyon göstermek adına gerçek zamanlı liste güncellenmesi önemli ve bir o kadar da gerekli bir durumdur [31].

RBL'ler, spam e-posta ürettiği tespit edilen bir kaynağın IP adresi listeye eklendiği andan itibaren listeyi kullanan servis sağlayıcılarının bu değişikliği de kapsayacak şekilde hizmet almalarına olanak sağlamaktadır. Servis

sağlayıcı, her gelen e-posta için gönderilen kaynak[1] bazlı olarak kara listede olup olmadığını DNS üzerinden kontrol etmektedir. Yapılan kontrollerde gönderen kaynak bilgisi kara listede mevcutsa e-posta spam olarak değerlendirilmekte ve engellenmektedir [37].

Bir servis sağlayıcı tarafından kara liste yönteminin kullanımına karar verildiğinde, üzerinde dikkatle durulması gereken nokta hangi liste sağlayıcıdan bu hizmetin alınacağına karar verilmesidir. Listeleme hizmeti alınırken dikkat edilmesi gereken noktalar şunlardır [22]:

- Profesyonel bir yönetim anlayışı taşıyan liste sağlayıcılar tercih edilmelidir.
- Listeleme yöntem ve ilkeleri açıklanmış olmalıdır.
- Listeden çıkarma prosedürü iyi tasarlanmış, açık, basit ve kolay uygulanabilir olmalıdır.
- Listeleme kriterleri birden fazla özelliği (ip adresi, alan adı vb.) içermelidir.
- Liste sağlayıcının iletişim bilgileri açık bir şekilde yayınlanmalıdır.
- Listeleme işlemindeki değerlendirme tek bir mesaj üzerinden yapılmamalıdır.
- Kara liste verileri sıklıkla güncellenmelidir.

**Dezavantajları:**

Kara liste kullanmanın bir takım dezavantajları bulunmaktadır. Bunları şu şekilde sıralamak mümkündür [38];

- Kara liste yönteminin en önemli eksilerinden bir tanesi genelleme üzerine kurulu olmasıdır. Örneğin, bir servis sağlayıcı üzerinden spam e-posta üretildiğinde bu kaynak kara listeye alınmaktadır. Ancak bu durum, servis sağlayıcıdan hizmet alan diğer kullanıcıların da mağdur olması anlamını taşımaktadır. Bu açıdan bakıldığında bütün bir servis

[1] Çoğunlukla IP adresidir ancak zaman zaman alan adı bilgisi de kullanılmaktadır.

sağlayıcının hizmet vermesini engellemek oldukça büyük bir dezavantaj teşkil etmektedir.

- Meydana gelen değişikliklerin hızlı bir şekilde işlenmesi ve kara listenin güncel tutulması oldukça zor ve sürekli takip edilmesi gerekliliği açısından zaman alıcı bir işlemdir.
- Zaman zaman spam üreticileri, kişi ya da kuruluşların güvenlik açıklarını kullanarak buralardan spam e-posta üretmektedirler. Bu nedenle kara listelere girenler bu açıklarını kapattıktan sonra engelleme listelerinden çıkmak amacıyla bu listelerin yöneticilerini ikna etmek durumunda kalmakta ve kimi zaman bu prosedür oldukça zor ve zaman alıcı bir süreç olmaktadır.
- DNS tabanlı siyah listeler internet trafiğinin artmasına yol açmakta ve DNS'i daha kritik bir kaynak haline dönüştürmektedir. Bu da DNS'in bütünlüğünü ve orjinalliğini tehdit eden DNS sınamaları olarak ortaya çıkmaktadır.

### 4.2.2 Beyaz listeleme

Beyaz listeleme, sadece listede bulunan kaynaklardan gelen e-postaların kabul edildiği yöntemdir. Liste dışında kalan kaynaklardan gelen tüm e-posta mesajları reddedilmektedir. Gerçekleştirilmesi ve yönetilmesi kolaydır. Kara listeler gibi yerel olarak ya da erişime açık genel listeler şeklinde yönetilebilmektedir. DNS üzerinden yayın yaptıklarında Alan Adı Sistemi Beyaz Listeleri (Domain Name System Whitelists - DNSWLs) olarak adlandırılmaktadır. Ancak, genellikle yerel olarak tutulmaktadır ve servis sağlayıcıların kendilerinin oluşturduğu, yönettiği listelerdir.

Kara listelerden farklı olarak beyaz liste verilerinin güncelliğinin sağlanması daha az kritik bir gereklilik taşımaktadır. Kara listenin tam tersi olan bu yöntemin tek başına uygulanması çok faydalı değildir. Çünkü kullanıcılara sadece listede kayıtlı adreslerden e-posta almakla kısıtlı bir servis

sunulmaktadır. Bu kısıtlama, beyaz liste yönteminin en önemli dezavantajını oluşturmaktadır. Ancak yine bu yöntemde, kullanıcıların spam e-posta alma oranı oldukça düşüktür. Çünkü, e-posta iletisi kabul edilen kaynaklar listede bulunan güvenilir kaynaklardan oluşmaktadır.

Beyaz liste yöntemi tek başına yaygın olarak kullanılan bir yöntem değildir. Diğer spam e-posta önleme teknikleriyle tamamlayıcı olarak birlikte kullanıldığında daha anlamlı hale gelmektedir. Birlikte kullanıldığında ilk kontrol basamağını oluşturmaktadır ve beyaz listede bulunan bir kaynaktan gelen e-posta iletileri diğer filtreleme teknikleriyle değerlendirilmeden kabul edilmektedir. Bir anlamda, diğer filtreleme ve önleme tekniklerinin kontrollerine tabi tutulmayan geçmeyen istisnai listeyi oluşturmaktadır [31].

**Dezavantajları:**

Beyaz liste kullanmanın bir takım dezavantajları bulunmaktadır. Bunları şu şekilde sıralamak mümkündür [23, 31];

- Bu yöntem tek başına kullanıldığında, listenin dışında kalan kaynaklardan e-posta alımı engellenmektedir. Bu da kullanıcılara verilen hizmetin sadece bu listelerle kısıtlı olmasına neden olmakta ve hizmet kalitesini oldukça düşürmektedir.
- Beyaz listede yer alan verilerin koşulsuz olarak güvenilir kabul edilmesi, bu kaynaklardan gelebilecek olası spam e-postaların zararları konusunda servis sağlayıcıları ve kullanıcıları savunmasız bırakmaktadır.

### 4.2.3 Gri listeleme

Spam üreticileri tarafından kullanılan yazılımların, alıcı tarafından reddedilen spam e-posta mesajlarını aynı alıcıya tekrar göndermediği varsayımı üzerine kurulmuştur. Bu yöntemde servis sağlayıcı tarafından, bilinmeyen bir kaynaktan geldiği tespit edilen e-posta mesajı ilk aşamada 4XX SMTP hata

koduyla[1] reddedilmektedir. Bu cevapla birlikte reddedilen kaynak bilgisi servis sağlayıcı tarafından veritabanına kaydedilmektedir. Aynı e-posta mesajı ikinci defa gönderildiğinde alıcı tarafından tanımlanabildiğinden ileti kabul edilerek alıcısına ulaştırılmaktadır [22].

Gri listenin işleyişinde ilk olarak gönderen SMTP sunucusu e-posta transfer işlemini başlatmaktadır. Alıcı SMTP sunucusu öncelikle gönderen kaynağın tanımlı olup olmadığını kontrol etmektedir. Alıcı tarafındaki sunucu, gönderen ile ilgili bir bilgi bulamadığı mesajı SMTP *geçici hata* (4XX) koduyla reddetmekte, aksi takdirde ise kabul etmektedir [39].

E-posta mesajı, tanımlı olmayan bir kaynaktan geliyorsa bu kaynağa ilişkin üç bilgi alıcı tarafında tutulan veritabanına kaydedilmektedir. Bu üç bilgi,

- Gönderen ip adresi bilgisi
- Gönderenin e-posta adresi ve
- Alıcının e-posta adresidir.

Alıcı tarafında gerçekleşen tanımlama işleminden sonra belirlenen süre içerisinde aynı göndericinin e-posta mesajını tekrarlaması gerekmektedir. Aksi takdirde, tanımlaması yapılmasına rağmen, servis sağlayıcı tarafından belirlenen süre içerisinde mesaj göndermediği belirlenen kayıtlar iptal edilmektedir. İptal işleminin ardından gelecek e-posta mesajları için bu prosedür tekrar başa dönerek işlemeye başlamaktadır.

Gri listelemenin uygulanması oldukça kolay ve yönetimi oldukça basittir. Gri liste metodu bir defa kurularak işletilmeye başladığında artık kullanıcı veya servis sağlayıcı tarafından herhangi bir veri güncellemesi ya da yönetim anlamında bir müdahale gerektirmemektedir. Sistemin işleyişi ve yönetimi tamamıyla otomatik olarak gerçekleşmektedir.

---

[1] Alıcı e-posta sunucusu tarafında geçici bir hata olduğunu ifade eden, daha sonra tekrar denenebileceğini belirten hata mesajıdır.

**Dezavantajları:**

Kolay uygulanabilir ve yönetilebilir olmasına rağmen birtakım zayıf yönleri de bulunmaktadır. Bunları şu şekilde sıralamak mümkündür [39, 40];

- Kayıtlı olmayan bir kaynaktan gelen ilk e-posta mesajının iki defa gönderiliyor olması;
    - fazladan bir trafik oluşturmaktadır.
    - alıcısına ulaşma süresini artmaktadır.
- Tekrar edilmeyen ilk e-posta mesajları alıcılarına ulaşmayacağından kaybolmaktadır.
- Gri liste yöntemi spam üreticileri tarafından mesajın tekrarlanması yoluyla kolaylıkla aşılabilen bir sistem üzerine kurulmuştur. Bu anlamda karşı önlem alınarak etkinliği azaltılabildiğinden çok etkili bir yöntem olduğunu söylemek pek mümkün değildir. Günümüzde demode bir yöntem halini aldığından uygulanma oranı oldukça düşüktür.

### 4.2.4 DNS üzerinde MX kaydı sorgulaması

Oldukça basit bir yöntemdir. E-posta gönderen adresinin doğruluğunun sınanması üzerine dayalıdır. Spam e-posta göndericilerinin kullandığı yöntemlerden biri de sahte gönderici e-posta adresleri kullanmaktadır. Temel hedef, arkalarında kendilerini deşifre edecek iz bırakmamaktır.

Gönderilen e-posta mesajlarında gönderen adresi (*"From"*) zaman zaman uydurma adresleri içermektedir. Hiç var olmayan, tamamen hayali etki alanı içeren adres kullanımı yapılmaktadır. Buradan yola çıkılarak gönderici adresinin geçerli olup olmadığını belirlemek için, adres formatı içerisinde bulunan ve @ işaretinden sonra gelen ilk kısım olan etki alanı bilgisi ile DNS üzerinde kayıtlı bir MX sorgusu yapılmaktadır. Sorgu sonucunda geçerli bir MX kaydı bulunamamışsa söz konusu e-posta spam olarak etiketlenmektedir [22].

**Dezavantajı:**

Günümüzde spam e-posta göndericileri, kolayca deşifre edilmesinden dolayı var olmayan etki alanına sahip e-posta adresleri kullanmayı tercih etmemektedir. Bu nedenle spam ile mücadelede başvurulan en basit yöntemlerden biri olmasına rağmen günümüzde çok etkin olduğunu söylemek pek mümkün değildir.

### 4.2.5 Gönderici yetkilendirme dizgesi

Günümüzde kötü niyetli e-posta mesajlarının çoğu üçüncü şahısların e-posta adresleri kullanılarak gönderilmektedir. Bu nedenle sadece söz konusu kötü niyetli e-postayı alan kişiler değil, e-posta adresleri bu kötü amaç için izinsiz olarak kullanılan kişiler de zarar görmektedir.

Gönderici Yetkilendirme Dizgesi (*Sender Policy Framework* veya *Sender Permitted From - SPF*) kötü niyetli e-posta gönderiminde kullanılan adres sahtekarlığının önlenmesi adına geliştirilmiş bir tekniktir. Bu yöntemde, etki alanı sahipleri DNS üzerinde bir SPF kaydı yayınlamaktadır. Söz konusu kayıt içerisinde ilgili etki alanının kullandığı e-posta sunucu bilgileri yer almaktadır. Bir mesajın alıcısına teslim edileceği esnada alıcı tarafından e-postanın geldiği kaynağın doğrulanması için bu bilgilere ihtiyaç duyulmaktadır. DNS üzerinden yapılacak sorgulama ile, ilgili SPF kaydına ulaşılmakta ve gelen e-posta başlığındaki bilgilerle karşılaştırılmaktadır. Yapılan kontrollerde e-postanın SPF kaydında belirtilmeyen bir sunucusundan gönderildiği tespit edildiğinde mesaj reddedilmekte, doğruluğu teyit edilmiş mesaj ise kabul edilerek alıcısına ulaştırılmaktadır. SPF yöntemi adres yanıltmalarına karşı oldukça etkili bir çözüm sunmaktadır. Ancak henüz kullanımı çok yaygın bir teknik değildir [41, 42].

**Dezavantajları:**

- Sadece DNS üzerinde SPF kaydı yayınlamış olan kaynaklardan gelen e-posta mesajlarının kabul edilme zorunluluğu ortaya çıkmaktadır. Bu da SPF kaydı bulunmayan kaynaklardan gelen mesajların alıcılarına ulaşamaması anlamı taşımaktadır.
- Bu yöntem sadece gönderen ve alıcı taraflardaki e-posta sunucuları arasındaki iletişimi doğrulamada etkilidir. Ancak, güvenilir bir etki alanı içerisinden herhangi bir kullanıcının bilerek ya da bilmeyerek gönderdiği spam e-posta sorununa alıcı tarafında bir çözüm getirmemektedir.

### 4.2.6 Etki alanı anahtarları tanımlanmış posta

Etki Alanı Anahtarları Tanımlanmış Posta (Domain Keys Identified Mail - DKIM), adres sahtekarlığına karşı geliştirilmiş bir yöntemdir ve mesajın geldiği ifade edilen kaynağın doğruluğunun kontrol edilmesi şeklinde işlemektedir. IETF tarafından geliştirilen bu teknik, elektronik imza teknolojisi kullanmakta ve bu yöntemle doğrulama yapmaktadır [43]. Verilerin imzalanması için bir gizli anahtar ve bir açık anahtar bulunmaktadır. Gizli anahtar bilgisi sadece etki alanı sahibinde bulunmaktadır. Açık anahtarlar ise DNS üzerinde tutulmaktadır ve erişime açık bilgilerdir.

E-posta mesajındaki kritik veriler (mesaj başlığındaki bazı alanlar ve mesaj içeriği) gönderici etki alanı tarafından gizli anahtar ile sayısal olarak imzalanmaktadır. Alıcı tarafında ise imzalanan veri, DNS üzerinden elde edilecek gönderen etki alanının açık anahtarı ile doğrulanmaktadır. Doğrulama işlemi gerçekleştiğinde mesaj kabul edilmekte, aksi takdirde ise reddedilmektedir.

DKIM, gönderici kimliği doğrulama fonksiyonu sayesinde spam e-posta gönderiminde başvurulan adres sahteciliği sorununu çözmektedir. Henüz

kullanımı çok yaygın olmamakla birlikte ileride daha popüler olacağı, daha yaygın bir şekilde kullanılacağı tahmin edilmektedir.

**Dezavantajları:**

- Kullanılabilmesi için hem gönderen hem de alıcı taraflarca desteklenmesi zorunludur. DKIM yöntemini kullanan bir alıcı tarafından olaya bakıldığında bu durum, DKIM desteklemeyen kaynaklardan gelen e-postaların tümünün reddedilmesi anlamını taşımaktadır. Bu yöntemin henüz gelişme aşamasında olduğu ve günümüzde kullanım oranının oldukça düşük olduğu göz önüne alındığında, reddedilen e-posta oranının çok ciddi boyutlara ulaşacağı değerlendirilmektedir.
- Bu yöntem sadece gönderen ve alıcı taraflardaki e-posta sunucuları arasındaki iletişimi güvenilir kılmada etkilidir. Ancak, güvenilir bir etki alanı içerisinden herhangi bir kullanıcının bilerek ya da bilmeyerek gönderdiği spam e-posta sorununa alıcı tarafında bir çözüm getirmemektedir.
- Alıcı taraftaki e-posta sunucusu DKIM yöntemini desteklemediği takdirde imzalanmış veriyi çözümleyemeyecek ve anlamsız ifadeler şeklinde görüntüleyecektir. Bu da e-posta mesajının alıcısına doğru bir şekilde ulaştırılamamasına neden olacaktır [44].

### 4.2.7 Filtreleme yöntemleri

Filtreleme yöntemi en çok kullanılan spam önleme tekniği olup ***hem giden e-postalar için hem de gelen e-postalar*** *için* uygulanabilmektdir. Filtreleme tekniğinin tercih edilmesinin nedenleri kolay uygulanabilir olması ve kullanıcılara esnek bir yönetim olanağı sunmasıdır. Filtreleme metodları e-posta servis sağlayıcıları seviyesinde kullanılabileceği gibi son kullanıcı seviyesinde de kullanılabilmektedir. Bu yöntemle kullanıcılar, hangi

mesajların spam olarak değerlendirilmesi gerektiğine karar verebilmekte, bu kriterleri kendisi belirleyebilmektedir [22].

Filtreleme metotları birbirinden farklı yöntem ve algoritmalar kullanarak işlemektedir. Bu yöntemler kimi zaman mesaj içeriğinin analiz edilmesi şeklinde gerçekleşirken, kimi zaman da gelen mesajların bilinen spam e-posta mesajları ile yapısal benzerlikleri üzerinde yapılan değerlendirmeler şeklinde gerçekleşmektedir. Bazı filtrelemeler sadece e-posta başlığı üzerinde ya da sadece mesaj içeriği üzerinde inceleme yaparken bazıları her iki veriyi de değerlendirerek inceleme yapmaktadır. Çoğu zaman birden fazla filtreleme tekniği birlikte kullanılmaktadır. Böylece e-postalar farklı açılardan incelendiğinden spam e-posta ile mücadelede daha etkin ve verimli sonuçlar elde edilmektedir.

Kullanılan filtreleme yöntemlerinin spam ile mücadelede etkinliğini sürekli koruyabilmesi için iki önemli kriter mevcuttur. Bunları şu şekilde sıralamak mümkündür [31];

1- Filtreleme sistemleri sürekli olarak kendini geliştirebilir, öğrenebilir olmak zorundadır. Çünkü spam göndericileri kullandıkları teknikleri ve mesaj içeriklerini değiştirmek ve yeni yöntemler üretmektedir. Buna karşın filtreleme sistemleri de elde ettikleri verileri değerlendirebilen bir işlevle çalışarak değişen spam tekniklerini deşifre etmelidir.

2- Filtrelemeler kullanıldıkları organizasyonun karakteristik özelliklerine göre geliştirilmeli ve buna göre adapte edilmelidir. Çünkü organizasyonun yapısı ve görevleri itibariyle spam e-postaya bakış açıları da değişkenlik göstermektedir. Örneğin bir doktor ya da hastaneye göre tıbbi ürünlerin pazarlamasını veya tanıtımını içeren e-postalar spam olarak değerlendirilmezken, bir finans kuruluşu için bu kapsamdaki mesajlar istenmeyen e-posta olarak işlem görmektedir. Bu nedenle, hatalı çıkarım sorunundan kaçınmak için filtreleme yönteminin uygulanacağı kullanıcı

profili gruplandırılmalı ve bu gruplara farklı filtreleme kriterleri uygulanmalıdır.

Filtreleme metodları tek başına kullanıldığında bazı dezavantajları da beraberinde getirmektedir [31].

- Tam ve düzgün olarak planlanmadığında hatalı çıkarım oranının yüksek seviyelere çıkarma riski taşımaktadır.
- Filtreleme metodları, özellikle e-posta mesaj içeriğinin incelenmesi esnasında sistem kaynaklarını oldukça yüksek oranda kullanmaktadır. Günlük gelen e-posta sayısının yüksek miktarlarda olduğu düşünüldüğünde sistem kaynaklarının filtreler tarafından meşgul edilmesinin genel işleyişi olumsuz yönde etkileme riski bulunmaktadır.
- Gelişmiş filtreleme uygulamaları genellikle oldukça pahalı sistemlerdir.

#### 4.2.7.1 Kelime filtreleme

Kelime filtreleme yöntemi halen en yaygın kullanılan metodlardan biridir. Tercih edilmesinin birincil nedeni oldukça basit bir uygulama olmasıdır. Son kullanıcıdan servis sağlayıcıya kadar herkes tarafından kolayca yönetilebilme avantajı taşımaktadır.

Temel işleyişi e-posta mesajlarının başlık veya içerik bölümünde önceden belirlenen kelimelerin taramasının yapılmasına dayanmaktadır. Örnegin istenmeyen elektronik postada yaygın olarak bulunan *"viagra"* gibi daha önceden tanımlanmış belli anahtar kelimelerin gelen mesaj içeriğinde taraması yapılmaktadır. Yapılan değerlendirmede anahtar kelime içerdiği tespit edilen e-postanın kötü niyetli olduğu varsayımı işlemekte ve engellenmektedir [22].

**Dezavantajları**

- Spam göndericiler filtrelerden geçmek adına bazı taktikler geliştirmektedir. Bunlardan biri de filtrelere takılan kelimelerin yazılışında bazı harfleri değiştirerek kullanmaktır. Örneğin **"viagra"** kelimesi yerine **"v1agra"** kullanılarak filtreler devre dışı bırakılmaktadır. Bu nedenle kelime filtreleri, düzenli olarak anahtar kelimelerin varyasyonları ile güncellenmelidir. Aksi takdirde kolayca aşılabilen bir yöntem durumuna düşeceğinden etkinliği oldukça azalacaktır.
- Bu yöntemin bir başka önemli dezavantajı da hatalı çıkarım yapma oranının oldukça yüksek olmasıdır. Filtrelemede kullanılan kelimelerin geçtiği tüm e-postaların spam olduğu varsayımı her zaman geçerli olmayabilir. Bu durumda yanlış bir değerlendirmeye neden olabileceğindan kötü niyetli olmayan e-postalar da alıcısına ulaşamayacaktır [22].

#### 4.2.7.2 Bayes filtreleri

*Bayes Teoreminin* olasılık ilkeleri üzerine geliştirilen istatistiksel filtreler, günümüzde spam e-posta ile mücadele konusunda oldukça popüler hale gelmiş ve geniş bir kullanım oranına ulaşmıştır [45].

Bir elektronik postanın spam e-posta olma olasılığını belirlemek için daha önce elde edilen sayısal verilerden yararlanılmaktadır. E-posta içerisinde geçen kelime veya ifadelerden yola çıkılarak, daha önce alınan toplam e-posta sayısı (normal ve istenmeyen), spam olarak tespit edilen e-posta sayısı, normal e-posta sayısı gibi sayılar kullanılarak elde edilen bir olasılık hesaplamasına dayanmaktadır. Bayes analizi sonucunda elde edilen rakam e-postanın spam olma olasılığını göstermektedir. Bayes filtreleri kendi kendini geliştirebilen ve öğrenebilen sistemlerdir. Gerektiğinde istenmeyen

elektronik postadaki değişikliklere otomatik olarak uyum sağlayabilmektedir [22].

Bayes filtreleri mesaj içeriğindeki kelimeler üzerinden hesaplamalar yaptığından iletişim davranışları homojen olan ve küçük gruplardan oluşan organizasyonlar için kullanıldığında daha güvenilir sonuçlar üretmektedir. Örneğin, üniversitede bir bölüm bünyesinde aynı etki alanı içerisinde çalışan ve benzer kelimeleri kullanan bir grup için oldukça etkili çıktılar üretecektir. Çünkü böyle bir ortamda hangi kelimeler üzerinden incelemelerin yapılacağını belirlemek daha kolaydır. Aynı zamanda bu kelimelerin kullanım amacı ve sıklığı da benzer özellikler taşıyacaktır. Oysa heterojen iletişim davranışına sahip bir grup için bu durum tam tersi olacaktır. Öyle bir durumda çok farklı davranış özellikleri olacağından filtrelenecek kelimeler de çeşitlilik gösterecektir. Dolayısı ile farklı davranış biçimlerinin aynı analiz içinde kullanılması hata payını artıracak bir unsur olacaktır.

Bayes yöntemi her ne kadar gruplar için de potansiyel bir çözüm oluştursa da kişisel kullanıcılar için en yüksek verimle çalışmaktadır. Ayrıca uygun filtreleme kriterleri ile programlanıp tek başına kullanıldığında bile büyük oranda başarı sağlayan birkaç yöntemden biridir [22].

**Dezavantajları**

Büyük e-posta servis sağlayıcıları için uygun bir çözüm değildir. Farklı kullanıcı davranış biçimlerinin aynı analiz içinde kullanılması hata payını artıracak bir unsur olarak değerlendirilmektedir. Bu nedenle heterojen bir kullanıcı profiline uygulandığında verimliliği düşmektedir.

#### 4.2.7.3 Heuristic filtreler

Heuristic filtreleri spam e-postaların karakteristik özelliklerinden yola çıkarak gelen e-postaları rakamsal olarak değerlendirmektedir. Mesaj içeriğinde yer

alan kötü niyetli bağlantılar, şüpheli kelimeler veya ifadeler, mesaj ekinde gelen dosya türleri potansiyel spam e-postaları belirtmekte kullanılan etkenlerdir. Bu yöntemde e-postanın, spam olabilecek her özelliği belli bir puan ifade etmektedir. E-postanın incelenmesi yapılırken diğer spam önleme teknikleri de puanlamaya dahil edilebilmektedir. Örneğin DKIM yöntemi ile yapılan değerlendirmede adres doğrulaması yapılamamışsa toplam puanın artmasına neden olacak, doğrulama yapılmışsa puanın azalmasına neden olacaktır. Mesajın herhangi bir teknik ile kontrolden geçerek olumlu sonuç dönmesi halinde yine toplam puan etkilenmekte, ancak bu defa azalmaktadır. Filtreleme sonunda toplanan puanlar o mesaja ilişkin kararın verilmesinde kullanılmaktadır. Ortaya çıkan puan belirlenen limiti aşıyorsa mesaj spam olarak değerlendirilerek işaretlenmekte veya silinmektedir [23].

Heuristic filtrelemede kullanılan puanlamaya, tabi tutulan özellikler ne kadar iyi belirlenirse o derece etkili sonuç almak mümkündür. Hem doğru özellikler belirlenmeli hem de belirlenen özelliklerin sayısı mümkün olduğu kadar çoğaltılmalıdır. Kullanılan yöntemler zaman içerisinde spam göndericileri tarafından öğrenilmekte yeni yöntemler geliştirilerek filtreleme aşılmaktadır. Bu nedenle filtrelemede kullanılan özelliklerin sürekli olarak güncellenmesi gerekmektedir [22].

Heuristic filtrelerin kurulumu kullanıcılar için oldukça kolaydır, yöneticiler için de az bir çalışmayla yüksek dereceli bir filtreleme sunmaktadır. Filtreler denetlenmeli, potansiyel hatalı çıkarımlar izlenmeli ve filtreleme kriterleri iyileştirilmelidir.

**Dezavantajları**

- Kuralları ve filtreleme özellikleri iyi belirlenmediği takdirde hatalı çıkarım oranı artacaktır [46].
- Gelişmiş özelliklere sahip Heuristic filtreleri oldukça pahalı yöntemlerdir.

### 4.2.8 Davet etme/cevap verme sistemleri (challenge/response systems)

Buradaki temel felsefe spam e-postaların otomatik sistemler tarafından gönderildiği düşüncesine dayanmaktadır. C/R sistemleri herhangi bir kaynaktan gelen ilk e-postalar için, gönderen tarafından teyit isteyen bir yöntem kullanmaktadır. E-postayı gönderen kullanıcıyla karşılıklı bir etkileşim oluşturmak suretiyle mesajın gerçek bir kullanıcı tarafından oluşturulduğunun kontrolüne yapılmaktadır. Gelen ilk e-posta, alıcı sistem tarafında kullanıcıya ulaştırılmadan geçici olarak saklanmaktadır. Bunun ardından e-postayı gönderen kullanıcıya bir e-posta ile cevap verilmektedir. Cevap e-postasında genellikle bir web adresi ya da bir kod gönderilmektedir. Karşıdaki kullanıcıdan belirtilen adrese bağlanması ya da gönderilen kodu e-postadaki boş kutucuğa yazarak cevaplaması istenmektedir. Eğer gönderen bu e-postaya istenilen şekilde cevap verirse, gönderdiği mesaj alıcısına ulaştırılmakta ve sistem tarafından izin verilmiş kullanıcılar listesine eklenmektedir [47, 48].

**Dezavantajları**

- Her bir kaynaktan gelen ilk e-postalar için kontrol mesajları oluşturmak fazladan bir veri akışına neden olmakta ve sistem kaynaklarının meşgul edilmesine neden olmaktadır. Özellikle büyük servis sağlayıcılar için düşünüldüğünde bu durum ciddi bir sorun oluşturmaktadır.
- İlk e-postaların alıcısına ulaşma süresini uzatmaktadır. Ayrıca kontrol e-postaları ve istenen teyit işlemi kimi zaman kullanıcılar üzerinde can sıkıcı bir etki bıraktığından bu mesajlara cevap vermemeyi tercih etmektedirler.

### 4.2.9 Balküpü kullanımı

Balküpü (Honeypot) yöntemi genelde büyük ölçekli servis sağlayıcılar, istatistik firmaları ve liste (Beyaz, Kara) sağlayıcıları tarafından kullanılan bir yöntemdir. Temel amaç korunmasız bir e-posta ortamı oluşturarak spam üreticilerinin buralara saldırmasını sağlamaktır. Böylece kurulan tuzak sonucunda spam kaynaklarının deşifre edilmesi sağlanarak bunlara karşı önlem alınmaktadır [49].

### 4.2.10 E-posta sayısı eşik değer sınırlaması

Spam e-postaların deşifre edilme süreleri gittikçe kısalmaktadır. Bu nedenle spam göndericileri mümkün olduğu kadar kısa süre içerisinde maksimum sayıda kullanıcıya ulaşmak üzere planlama yapmaktadır. Bu yöntem de bu varsayım üzerinden yola çıkılarak geliştirilmiştir.

Belli bir zaman dilimi içerisinde aynı kaynaktan gelen e-posta sayısına bir kısıtlama getirmektedir. Söz konusu e-posta sayısı belirlenen eşik değere ulaşıncaya kadar bütün iletiler kabul edilmektedir. Ancak, eşik değer aşıldığında sunucu tarafından kısa bir süre için bu kaynaktan gelen mesajların reddedilmesi üzerine dayalı bir yöntemdir. Önceden tanımlanmış olan kısıtlama süresi dolduğunda ise, bu kaynaktan gelen e-posta mesajları yine serbest bırakılarak kabul edilmektedir.

Bu yöntemin kullanılması durumunda dikkat edilmesi gereken en önemli nokta eşik değerin belirlenmesidir. Bu değer düşük bir seviyede belirlenirse spam olmayan e-postaların da engellenmesi sorununa neden olacaktır. Aynı şekilde çok yüksek bir seviyede belirlenirse de spam e-postaların gözden kaçmasına neden olacağından etkinliği ve verimliliği büyük oranda azalacaktır.

**Dezavantajları:**

- Aynı kaynaktan seyrek aralıklarla gönderilen ya da farklı kaynaklar kullanılarak gönderilen spam e-postaların deşifre edilerek engellenmesinde yetersiz kalmaktadır.
- Sistem izleme ve denetleme uygulamaları tarafından üretilen bilgilendirme e-postaları çoğu zaman otomatikleştirilmiş olarak ve sık aralıklarla gönderilmektedir. Bu anlamda söz konusu e-postaların sayısının belirlenen eşik değerin üzerine çıkma olasılığı bulunmaktadır. Dolayısı ile spam olmayan e-postaların da engellenmesi sorunu ortaya çıkmaktadır. Bu sorunun giderilmesi adına bilinen kaynaklar için farklı eşik değerler belirlenebileceği gibi beyaz liste yöntemiyle birlikte kullanıldığında bu kaynakların listeye eklenmesiyle de çözülebilmektedir.

## 4.3 Diğer Yöntemler

Spam sorununun çözümüne yönelik geliştirilen yöntemlerden bazıları gerek kullanıcı bazında bilinçli davranış oluşturma ve gerekse sistem yöneticileri bazında erken uyarı sistemlerinin kullanılması şeklinde ortaya çıkmıştır. Bir kısmı ise hizmet sağlayıcılar seviyesinde e-posta iletilerinin güvenliğinin sağlanmasına yönelik geliştirilen yöntemlerden oluşmaktadır.

### 4.3.1 E-posta hizmeti performansı izleme

Spam e-posta mesajları zaman zaman servis sağlayıcıların vermiş olduğu hizmetin kalitesini önemli ölçüde düşürecek boyuta ulaşmaktadır. Servis sağlayıcılar tarafından verilen e-posta hizmet kalitesinin, sistem performansının ve fonksiyonelitesinin ölçümü ve izlenmesi bu açıdan oldukça önemlidir. Sistem raporlaması yapan uygulamalar aracılığıyla spam e-posta mesajlarının yol açabileceği durumlara ilişkin isatistiki veriler elde edilerek

ortaya çıkan ani değişimler sistem yöneticilerine rapor edilmektedir. Bir anlamda erken uyarı sistemleri olarak işlev görmektedir [50].

#### 4.3.1.1 E-posta kuyruk denetimi

E-posta sunucularında gelen ve giden e-posta mesajlarının sunucu tarafından işlenme sırası kuyruk mantığıyla gerçekleşmektedir. Sunucu meşgul durumdayken işlenmeyi bekleyen mesajlar bu kuyruğa dahil edilmektedir. Kuyrukta bekleyen mesaj sayısı, gelen ve giden e-posta trafiğinin yoğunluğuna göre zaman zaman değişiklik göstermektedir. Normal şartlarda kuyruk boyutunun bir üst sınırı mevcuttur. Ancak bu üst sınırın ani bir şekilde aşılması donanım kaynaklı bir sorun olmadığı durumlarda giden ya da gelen e-posta hizmetinde problem olduğunu göstermektedir. Böyle bir durumun oluşması da servis sağlayıcının verdiği servis kalitesinin düşmesi anlamını taşımaktadır.

Kuyruk izleme sistemleri sayesinde e-posta kuyruk boyutu sürekli izlenerek ani değişimler karşısında bilgi edinilmekte ve bu sayede spam e-posta trafiği tespit edilerek engellenmektedir. Bu uygulamayla birlikte servis sağlayıcı hem kendi bünyesinden gönderilebilecek spam e-posta trafiğini önleyebilmekte hem de dışarıdan gelebilecek ataklara karşı kendini koruyabilmektedir.

#### 4.3.1.2 Mesaj işleme gecikmesinin ölçümü

E-posta mesajlarındaki gecikmenin ölçümü mesajların işlenme süreleri ile kuyrukta bekleme süreleri üzerinden yapılmaktadır. Bu sürelerden herhangi biri için uygulanabileceği gibi her ikisi için de uygulanabilmektedir.

Zaman zaman spam e-posta mesajları çok büyük boyutlarda üretilmekte ve e-posta hizmetinin sürekli bu mesajları işlemekle meşgul edilmesini sağlayarak hizmet vermesini engellemeyi amaçlamaktadır. Bu nedenle gelen

ve giden e-posta mesajlarının boyutuna bir sınırlama getirmek gerekir. Buna rağmen spam üreticileri bu sınırı çeşitli denemelerle çözebileceğinden bu sınıra çok yakın boyutlarda çok sayıda mesaj ile sistemi meşgul etme yoluna da başvurmaktadır. Bundan dolayı uzun süreli mesaj işleme gecikmeleri yaşandığı durumları izleyen ve sistem yöneticilerini bu gibi durumlar karşısında uyaran çözümlerin kullanılması gerekmektedir. Bu tür çözümler oldukça etkili bir uyarı sistemi oluşturmaktadır ve böylece sisteme müdahale etmek ve gelen ya da giden spam mesajları engellemek mümkün olmaktadır.

### 4.3.2 E-posta adres hırsızlığından kaçınma

Spam göndericileri çeşitli yöntemlerle e-posta adreslerini toplamaktadırlar. Bu nedenle spam sorunundan kaçınmak için alınması gereken birincil önlem e-posta adresinin korunmasıdır.

#### 4.3.2.1 E-posta adresi gizleme

Adres gizleme tekniği e-posta adreslerinin gizlenmesi suretiyle spam göndericilerinin eline geçmesini engellemek ve kötü amaçlı kullanımlarının önüne geçmeyi amaçlamaktadır. Spam üreticileri bir takım casus yazılımlar kullanarak web sayfaları, sohbet siteleri, haber grupları, e-posta dağıtım listeleri, web formları gibi haberleşme platformlarında yayınlanan e-posta adreslerini kullanıcıların farkında olmadan toplamaktadır.

Kullanıcıların e-posta adreslerini spam göndericilerinden korumak için adres toplama yöntemine karşı bir takım önlemler almaları kaçınılmazdır. Alınacak önlemler esasında oldukça basittir. Öncelikle ve en etkili yol olarak çok gerekmedikçe güvenilir olduğu bilinmeyen ortamlarda e-posta adresi yayınlanmamalıdır. Ayrıca e-posta adreslerini internet üzerinde yayınlarken açık bir şekilde yazmak yerine bazı ifade ya da işaretleri kullanmak yoluyla

casus yazılımlara karşı önlem almak mümkündür. Örneğin @ işaretini **[et]** şeklinde kullanmak ya da e-posta adresi içinde geçen "." işareti yerine yazıyla **"nokta"** yazmak (ad.soyad@etkialani.com e-posta adresinin **"ad nokta soyad [et] etkialani nokta com"** şeklinde ifade edilmesi) gibi basit ancak etkili önlemler ile e-posta adres hırsızlığına karşı mücadele etmek bir zorunluluk halini almıştır [51].

#### 4.3.2.2 Adres sınamalarının engellenmesi

Adres toplama yöntemlerinden bir tanesi de e-posta sunucularına gönderilen sınama mesajlarıdır. Aynı etki alanına değişik e-posta adresleri üretilerek gönderilen bu mesajlar sayesinde deneme yanılma yoluyla e-posta adreslerinin elde edilmesi amaçlanmaktadır [35]. Söz konusu ataklar servis sağlayıcıları tarafından kolaylıkla tespit edilebilmektedir. Bu amaçla, belirli bir zaman diliminde aynı kaynaktan hatalı alıcı adresleri ile gelen e-posta sayısının, belirlenen limiti aşması halinde, söz konusu kaynağın spam üreticisi olduğu değerlendirilmektedir. Bu değerlendirmeden yola çıkılarak tespit edilen olası spam kaynaklarından gelen SMTP taleplerine verilecek cevaplar için bir gecikme süresi uygulanmaktadır. Limit aşıldığında ise kaynaktan gelen talepler tümüyle reddedilmektedir.

**Dezavantajı:**
Adres sınamaları belli bir zaman diliminde sürekli yapılmak yerine belli aralıklarla yapıldığında ya da tek bir kaynaktan yapılması yerine farklı kaynaklardan yapıldığında atakların tespit edilmesi mümkün değildir.

### 4.3.3 Virüs koruma programları

Spam e-postaların bir kısmı virüs ve solucan gibi zararlı yazılımlar ile alıcının bilgisayarına ya da e-posta hizmet sağlayıcının sistemine zarar vermek

amacı gütmektedir. Bu tür spam e-postaların zararlı etkilerinden kaçınmak ve daha güvenli bir e-posta ortamı oluşturmak adına son kullanıcıdan sistem yönetcisine kadar her aşamada virüs koruma programlarının kullanılması gereklidir. Burada dikkat edilmesi gereken en önemli nokta kullanılan virüs koruma programlarının sürekli güncel tutulması gerektiğidir. Çünkü spam göndericileri her geçen gün bu tür koruma yöntemlerinden kaçınmak adına yeni yöntemler denemektedir. Güncellenmemiş bir virüs programı yeni yöntemlerle gönderilmiş spam e-postaları çözemeyeceğinden etkisiz kalacak ve saldırılara karşı güvenlik açığı oluşacaktır.

### 4.3.4 Güvenlik mekanizmaları

Bilgisayarlar arasında güvenli bağlantılar oluşturmak ve gönderilen verinin alıcısı dışındakiler tarafından okunmasını önlemek amacıyla geliştirilmiş yöntemlerdir.

E-posta hizmetinin güvenliği, kurulan haberleşme bağlantısının güvenliğiyle doğru orantılıdır. *"Taşıma Katmanı Güvenliği (Transport Layer Security – TLS)"* ve *"Güvenli Yuva Katmanı (Secure Socket Layer - SSL)"* güvenli iletişimde kullanılan yöntemlerdir. Bu protokoller sayesinde veri iletişimi daha sağlıklı ve güvenli bir şekilde gerçekleştirilmektedir.

E-posta mesajının güvenliği ise veri içeriğinin korunması ve kimlik doğrulama sağlayan şifreleme mekanizmaları ile sağlanmaktadır. En çok kullanılan yöntemler *"Oldukça İyi Gizlilik (Pretty Good Privacy - PGP)"* ve *"Güvenli/Çok Amaçlı İnternet Posta Uzantıları (Secure/Multipurpose Internet Mail Extensions – S/MIME)"*dır. Bu yöntemlerin kullanılabilmesi için, gönderici ve alıcı tarafların her ikisinin de yöntemleri desteklemesi gerekmektedir. Aksi takdirde alıcı taraf mesaj içeriğini göremez.

#### 4.3.4.1 Taşıma katmanı güvenliği

TLS, IP tabanlı iletişimde güvenli veri alış verişini sağlayan protokoldür. SSL protokolü temel alınarak geliştirilmiştir. Veri iletişimi sırasında, bilgilerin şifrelenerek gönderilip alınmasını sağlamaktadır [52].

TLS, istemci ve sunucu arasında çift yönlü bir el sıkışma ile gerçekleşen bağlantıdır. Söz konusu bağlantıda veriler şifrelenerek gönderilmektedir. Verinin şifrelenmesinde bir çift anahtar kullanılmaktadır. Bu anahtarların biri gönderen tarafından verinin imzalanması için kullanılan açık anahtar, diğeri ise alıcının veriyi çözebileceği gizli anahtardır. Gizli anahtar sadece alıcı tarafından bilinmektedir. Açık anahtar ise, gönderen tarafından verinin şifrelenerek gönderilmesi için kullanılmaktadır.

TLS bağlantısının kurulması için istemci, sunucuya güvenli bir bağlantı başlatması için talepte bulunmaktadır. Sunucu gelen isteği kabul eder ve isteğe karşılık kendi sertifikasını istemciye gönderir. Bu sertifika içerisinde sunucuya ait açık anahtarı bulunmaktadır. İstemci, gelen sertifika içerisinde bulunan imzaya bakarak, bu sertifikanın güvenilir olup olmadığını, sertifikanın geçerlilik süresini ve sertifikanın gerçekten istekte bulunulan sunucunun sertifikası olup olmadığını kontrol eder. Sertifika güvenilirliği doğrulandıktan sonra kabul edilerek sonraki aşamaya geçilir. İstemci, sunucunun göndermiş olduğu sertifikanın içerisindeki açık anahtarı kullanarak örnek bir veriyi şifreleyip sunucuya gönderir. Sunucu şifrelenmiş veriyi, gizli anahtarını kullanarak çözer.

Bu şekilde istemci ve sunucu arasında güvenli ve şifreli bir iletişim kurulmuş bulunmaktadır. Bundan sonraki aşamada sunucu ve istemci arasındaki gidip gelen bütün veriler şifreli olarak TLS bağlantısı üzerinden taşınmaktadır. TLS tabanlı bağlantıda veriler şifrelendiğinden ve yalnızca alıcı tarafından çözümlenebileceğinden, veri paketleri başkalarının eline geçse dahi mesaj içeriğine ulaşmaları mümkün değildir.

TLS bağlantısının kurulabilmesi için veri iletişimi yapacak tarafların her ikisinin de bu özelliği desteklemesi gerekmektedir. Ayrıca TLS kullanımına karar verildiğinde ayarlarının doğru olarak yapılandırılması çok önemlidir, aksi takdirde sunucular üzerinde ciddi güvenlik riskleri oluşturmaktadır [53].

#### 4.3.4.2 Güvenli yuva katmanı

SSL, TCP/IP tabanlı bir güvenlik protokoldür ve istemci ile sunucu arasında gönderilen veya alınan bilgiyi şifreleyerek güvenli bir iletişim olanağı sunmaktadır [54]. 1993 yılında Netscape tarafından geliştirilmiş olup daha sonra IETF tarafından TSL standardı olarak RFC-2246 ile yayınlanmıştır [55].

1996 yılında 3.0 versiyonunun çıkarılmasıyla hemen bütün İnternet tarayıcılarının (Microsoft Explorer, Netscape Navigator vb.) desteklediği bir standart haline gelmiş ve çok geniş uygulama alanları bulmuştur.

Açık Anahtarlama altyapısını kullanan SSL, gönderilen bilginin kesinlikle ve sadece doğru adreste deşifre edilebilmesini sağlar. Bilgi gönderilmeden önce otomatik olarak şifrelenir ve sadece doğru alıcı tarafından deşifre edilebilir. Çünkü şifrelenen veriyi çözebilecek anahtar sadece alıcı tarafından bilinmektedir. Her iki tarafta da doğrulama yapılarak işlemin ve bilginin gizliliği ve bütünlüğü korunmaktadır [55].

#### 4.3.4.3 Oldukça iyi gizlilik

PGP, temel olarak e-posta haberleşmesinde verilerin korunması amacıyla ortaya çıkmıştır. Phillip Zimmermann tarafından geliştirilen PGP, dünyada en yaygın olarak kullanılan e-posta şifreleme ve sayısal imzalama yazılımıdır. Açık anahtar altyapısı kullanıldığından herkesin bir gizli, bir de açık anahtarı

bulunmaktadır. Gizli anahtar sadece sahibi tarafından bilinirken açık anahtar herkese erişimine açık bir bilgidir ve açık bir biçimde yayınlanmaktadır [56].

PGP yönteminde iki farklı güvenlik işlemektedir [57]:

- Veri şifreleme
- Mesaj imzalama

Veri şifreleme e-posta içeriğinin şifrelenerek sadece alıcı tarafından okunmasını sağlamaktadır. Gönderici tarafından alıcının açık anahtarı ile şifrelenen veri, ancak alıcıya ait gizli anahtar ile çözülebilmektedir. Mesaj başkaları tarafından ele geçirilse dahi çözümlenmesi mümkün değildir.

Mesaj imzalama ise, gönderilen mesajın imzalanması suretiyle alıcı tarafından gönderen kimliğinin doğrulanmasına olanak sağlamaktadır. Gönderilen veri, göndericinin gizli anahtarı ile imzalanmaktadır. Alıcı tarafta ise imzanın doğruluğu göndericinin açık anahtarı ile kontrol edilmektedir.

#### 4.3.4.4 Güvenli/Çok amaçlı internet posta uzantıları

S/MIME, IETF tarafından geliştirilen MIME standardının devamı niteliğinde olan ve ona güvenli e-posta eklentileri getiren bir standarttır [58].

S/MIME bildiğimiz e-posta formatına açık anahtar altyapısı kullanarak sayısal imza ve şifreleme özelliklerini eklemiştir. Veri şifreleme, e-posta içeriğinin şifrelenerek sadece alıcı tarafından okunmasını sağlamaktadır. Mesaj imzalama ise, gönderilen mesajın imzalanması suretiyle alıcı tarafından gönderen kimliğinin doğrulanmasına olanak sağlamaktadır [59].

# 5 ULUSLARARASI ALANDA YAPILAN ÇALIŞMALAR

Spam sorunu özellikle son 10 yıldır ele alınmakta ve bu soruna idari, teknik ve hukuki çözümler geliştirilmeye çalışılmaktadır. Geçen süre zarfında ITU, OECD ve AB tarafından konu ile ilgili çalışmalar yapılmış, tavsiyelerde bulunulmuş ve üye ülkelerin bu konuda gerekli düzenlemeleri gerçekleştirmeleri yönünde değerlendirmeler yapılmıştır.

## 5.1 Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD)

OECD, ekonomik ve sosyal konularda fikir paylaşımı ortamı sağlayan; çevre, sağlık, eğitim, tarım, bilgi teknolojileri ve enerji gibi pek çok alanda çalışmalar ve araştırmalar yapan, hükümetlere söz konusu alanlarda politika üretme ve vizyon geliştirme konularında yardımcı olan, uluslararası alanda kabul görmüş kararlar ve tavsiyeler yayımlayan bir kuruluştur.

OECD'nin spam konusundaki çalışmaları 2003 yılından beri yoğunlaşarak devam etmektedir. Bu kapsamda OECD, üye ülkelerin hükümetleri ve özel sektörüne, küresel bir sorun haline gelen spam ile mücadelede gerekli işbirliğini sağlamalarını ve gerekli önlemleri almalarını tavsiye etmektedir.

Spam sorununun tehlikeli boyutlara ulaştığı ve hem tüketiciler hem de iş dünyası üzerinde ciddi oranda maliyet oluşturduğu vurgulanmaktadır. Verimliliği olumsuz yönde etkilediği, ağlara zarar verdiği ve virüs yayılımına neden olduğu ifade edilmektedir. OECD, üye ülke hükümetlerine ulusal spam önleme politikalarını oluşturmaları ve yasaların icrasını yürütecek kurumlara yeterli güç ve kaynağı tahsis etmeleri konusunda çağrı yapmakta ve kamu ile özel sektör arasında oluşturulacak koordinasyon ve işbirliğinin önemini vurgulamaktadır [60].

Eğitim faaliyetlerinin önemine de dikkat çekilerek kullanıcıların spam sorunu karşısındaki farkındalıklarının artırılması ve bilinç düzeylerinin geliştirilmesi gerektiği belirtilmektedir. Bu amaçla hükümetlerin ve sektör aktörlerinin eğitici kampanyalar düzenlemesi gerektiği vurgulanmaktadır. Ayrıca okullarda okutulacak bilgisayar derslerinin içeriğinin spam ile mücadeleyi de içerecek şekilde revize edilmesi tavsiye edilmektedir.

OECD, spam ile mücadelede uluslararası işbirliğinin anahtar rol oynadığını ifade etmektedir. Bu nedenle üye ülkelere uluslararası işbirliğini geliştirmelerini ve bilgi paylaşımında bulunmalarını tavsiye etmektedir. OECD bünyesinde, uluslararası işbirliğini geliştirmek, uyumlu politika altyapıları oluşturmak ve tecrübe paylaşımını artırmak amacıyla geniş katılımlı çalıştaylar düzenlenmiştir. Ayrıca kuruluş bünyesinde spam ile mücadele konusundaki çalışmaları yürütmekle görevli Spam Görev Gücü (OECD Task Force on Spam ) grubu oluşturulmuş ve bu konudaki çalışmaların tek elden daha etkili ve verimli bir şekilde yürütülmesi sağlanmıştır.

### 5.1.1 Spam görev gücü

OECD üyesi 30 ülke, Avrupa Komisyonu, OECD Ticaret ve Danışma Kurulu ve sivil toplum kuruluşlarından (STK) katılımcıların bulunduğu OECD Spam Görev Gücü, spam ile mücadele konusundaki çalışmaları yürütmekle görevlendirilmiştir [61].

Oluşturulan grup, spam e-posta problemi karşısında kapsamlı bir bakış açısıyla hükümetlerin, iş dünyasının ve STK'ların çabalarına kılavuzluk etmek ve günün şartlarına göre en hızlı stratejiyi geliştirmek amacıyla çalışmalarını sürdürmektedir [62].

Görev grubu, spam sorunu ile mücadele kapsamında iki adet uluslararası katılımlı çalıştay düzenleyerek bilgi alış verişinde bulunulmasını sağlamış,

tecrübe paylaşımını gerçekleştirmiş ve yapılan çalışmaların gözden geçirilerek devamında izlenecek stratejilerin belirlenmesini sağlamıştır. Ayrıca, mevcut spam önleme stratejilerini inceleyerek bu konuda gerek teknolojik anlamda ve gerekse yasal düzenlemeler anlamında yol gösterici bir kılavuz hazırlamıştır. Grup, kılavuzun hazırlanması aşamasında OECD üyesi olmayan ülkelerin de sürece katılmalarını sağlayarak küresel boyutta bir çalışma ortaya çıkarmıştır.

### 5.1.2 Brüksel çalıştayı – Şubat 2004

02-03 Şubat 2004 tarihlerinde Brüksel'de düzenlenen çalıştayda giderek daha kritik bir hal alan spam sorunu uluslararası boyutta ele alınmıştır. İki gün süren oturumlarda,

- Spam mesajların karakteristik özellikleri tanımlanmış,
- Spam sorununun kaynağı ve konuya ilişkin istatistikler değerlendirilmiş,
- Spam ile mücadele konusunda ortaya çıkan yaklaşımlar görüşülmüş,
- Söz konusu yöntemlerin ne ölçüde başarı sağlayabileceği incelenmiş ve
- Uluslararası işbirliğini artırmanın yolları araştırılmıştır [63].

### 5.1.3 Busan çalıştayı – Eylül 2004

OECD spam görev gücü tarafından 08-09 Eylül 2004 tarihlerinde Güney Kore'nin Busan şehrinde düzenlenmiştir. Brüksel'de düzenlenen çalıştayın devamı niteliğini taşımakta olup hükümetlerden, iş dünyasından, sivil toplum kuruluşlarından ve akademik çevrelerden temsilcilerin katılımıyla gerçekleştirilmiştir. İki gün süren çalıştay süresince,

- OECD Anti-Spam kılavuzu çalışmalarında gelinen nokta değerlendirilmiş ve bundan sonra atılacak adımlar üzerinde durulmuş,

- Spam önlemede kullanılan ağ yönetim çözümleri tartışılmış,
- Sorunla mücadelede kullanılan teknik araçlar ve kimlik doğrulama kullanımı incelenmiş ve

Asya-Pasifik Ekonomik İşbirliği ekonomileri ve OECD üyesi olmayan ülkelerle işbirliği çalışmalarının artırılması konularında çalışmalar yapılmıştır [64].

### 5.1.4 Anti-spam kılavuzu

Kılavuz, OECD Spam Görev Gücü tarafından yürütülen çalışmalar sonucunda 2006 yılında tamamlanarak yayınlanmıştır. Güvenilir bir e-posta hizmetine kavuşmak amacıyla çalışmalar yapan hükümetler, kamu kurumları ve düzenleyici kurumlar, İSS ve EPS'ler, iş dünyası ve STK'lar gibi birçok aktöre, geniş kapsamlı insiyatif üretme konsunda yardımcı olmak amacıyla ortaya çıkarılmış bir üründür [65].

Spam Görev Gücü başkanı Tom Dale, kılavuzun oluşturulmasındaki amacı şu sözlerle özetlemiştir [66]:
*"Teknoloji spam göndermeyi daha zor bir pozisyona iterken, spam mesajlar çevrimiçi ortamlar için gittikçe daha kötü niyetli bir hal almakta ve zararlı hale gelmektedir. Spam mesajlar günümüzde en çok yasa dışı amaçlarla kullanılmaktadır ve amacımız spam göndericilere karşı sınır ötesi uygulamaların gelişimini desteklemektir. Kılavuz oluşturma çalışmaları bu konuya katkı yapacak bir stratejinin ürünüdür ".*

Kılavuz birbiriyle ilişkili sekiz bölümden oluşmaktadır [22]:

1- **Düzenleyici Yaklaşımlar:** Bu bölümde spam ve ilişkili problemlerin üstesinden gelen spam önleyici yasaların gelişimi temel alınmaktadır. Güçlü bir yasal mevzuatın nasıl oluşturulacağı konusunda bilgiler içermektedir. Yasalarda, izin verilen ve yasaklanan kuralların açık ve net bir şekilde tanımlanması gerekliliği vurgulanmaktadır.
2- **Yasaların İcrası:** Yasal düzenlemeleri oluşturan kanunların icrası temel alınmakta ve bu sürecin en verimli şekilde nasıl işletilebileceği

konusunda bilgiler verilmektedir. Spam sorunu ile etkili bir mücadele yürütmek için yasaların icrasının mümkün olduğunca hızlı reaksiyon gösterebilir mekanizmalar çerçevesinde yürütülmesi gerektiği vurgulanmaktadır. Çevrimiçi dijital dünyada kanunların icrasında yaşanacak gecikmelerin suçla mücadeledeki başarı oranını olumsuz yönde etkileyeceği ifade edilmektedir.

3- **Özel Sektör İnisiyatifleri:** Spam ile etkin bir mücadele yürütebilmek için yasal düzenlemelerin oluşturulması aşamasına özel sektörün de katılımını sağlamak gerektiğine vurgu yapılmaktadır. Bu süreçte sektör temsilcilerinin üzerine düşen rol incelenmektedir.
4- **Teknik Çözümler:** Bu bölümde spam ile mücadelede kullanılan teknik yöntemler, altyapılar ve araçlar incelenmektedir.
5- **Eğitim ve Bilinç:** Son kullanıcının spam ile mücadele konusunda bilinçlendirilmesi ve eğitilmesi gerektiği vurgulanmakta ve bu konuda uygulanması gereken stratejilerden bahsedilmektedir.
6- **Spam ile Mücadelede Ortak İşbirliği:** Spam ile mücadelede kamu ve özel sektör işbirliğinin gerekliliği belrtilmektedir. Söz konusu işbirliğinin sağlanması ve geliştirilmesine ilişkin stratejileri içermektedir.
7- **Spam Ölçütleri:** Spam ile mücadelede alınan yöntemlerin etkilerinin ölçülmesi konusunda ipuçları verilmektedir.
8- **Küresel İşbirliği:** Spam sorununun küresel bir sorun olduğuna vurgu yapılmaktadır. Söz konusu sorunla mücadelede başarılı olmanın temel kriterlerinden birinin uluslararası işbirliğini geliştirmek olduğu ifade edilmekte ve bu konudaki yol haritası bulunmaktadır.

### 5.1.5 Sınır ötesi işbirliği üzerine OECD önerileri

OECD'nin, 13 Nisan 2006 tarihli 1133 üncü Konsey oturumunda spam ile mücadele konusu görüşülmüş ve bu kapsamda üye ülkelere tavsiye kararları alınmıştır. Alınan kararlar aşağıda açıklanmıştır [66]:

- Üye ülkelerin spam ile mücadele kapsamında gerekli yasaları oluşturmaları ve yasaların icrası noktasında etkili çözümler üretmeleri tavsiye edilmektedir.
- Üye ülkelerin diğer ülkelerle işbirliği içinde olmaları ve spam sorununa karşı organize bir mücadelenin yürütülmesi tavsiye edilmektedir.
- Spam ile ilgili düzenleme altyapılarının oluşturulması ve kanunların icrası aşamasında başta ilgili kamu kurumları ve düzenleyici kurumlar olmak üzere, İSS'ler, iş dünyası ve STK'lar gibi birçok aktörün dayanışma ve işbirliğinde bulunmaları tavsiye edilmektedir.
- Spam ile mücadelenin başarılı olabilmesi için hukuki ve teknik alanda yapılacak çalışmaların ve düzenlemelerin yanı sıra eğitim ve bilinçlendirme çalışmalarının da bu konuda büyük yarar sağlayacağı vurgulanmaktadır.
- Ayrıca tavsiye kararları kapsamında yapılacak sınır ötesi işbirliği konusundaki gelişmelerin OECD'nin ilgili birimleri tarafından 3 yıl boyunca izlenmesi kararlaştırılmıştır.

## 5.2 Uluslararası Telekomünikasyon Birliği (ITU)

ITU spam sorununa oldukça önemle yaklaşmış ve bu sorunun çözümlenmesi yönünde adımlar atılması gerektiğini vurgulamıştır. E-posta yoluyla yayılan spam mesajların günümüz dijital dünyasının en önemli sorunu olduğu dile getirilmiştir. Başlangıçta küçük bir sorun olarak algılanan spam mesajların günümüzde servis sağlayıcılar, iş dünyası ve son kullanıcılar açısından değerlendirildiğinde önemli bir maliyet oluşturduğu ve verimlilik kayıplarına neden olduğuna dikkat çekilmiştir [67].

Uygun yasal düzenlemeler ve etkin uygulamaların sorunla mücadelede iki temel öğe olduğu vurgulanmıştır. Her ne kadar ulusal çözümler ve yasal düzenlemeler üretilmiş olsa da spam göndericilerinin internetin uluslararası doğasını kullandıkları ifade edilmektedir. Bu nedenle sınır ötesi işbirliği

yapılmasının bu konuda yapılacak yeni yasalar ile bu yasaların icrasının gerçekleştirilmesinde ve detaylandırılmasında son derece önemli olduğu değerlendirilmektedir. Uluslararası işbirliğinin temelde iki amacı olduğu vurgulanmıştır. Bunlar,

- Henüz yasal düzenleme yapmamış ülkelerde uyumlu ve uygun spam önleme yasaları çıkarılması ve
- Yasal düzenlemelerin etkili bir şekilde icrasını sağlanmak ve spam sorununa kapsamlı bir çözüm getirmek için ülkeler arası işbirliğinin teşvik edilmesi şeklinde açıklanmıştır.

Tüketici birlikleri ile bilgi ve tecrübe paylaşımının önemi vurgulanmış ve yapılacak işbirliği çalışmaları ile kullanıcıların elektronik haberleşme konusundaki alışkanlıklarını geliştirilebileceği ifade edilmiştir. Bunun sonucunda da kullanıcıların spam mesajlara karşı kendilerini daha iyi koruyabilecek bilinç düzeyine ulaşabilecekleri belirtilmiştir.

ITU spam ile mücadelede uluslararası işbirliğini destekelemek, uyumlu politika altyapıları oluşturmak ve bu konuda ülkeler arasındaki bilgi ve tecrübe paylaşımını artırmak amacıyla gerek bölgesel ve gerekse uluslararası kapsamda çeşitli organizasyonlar düzenlemiştir. Gerçekleştirilen organizasyonlarda ve çalışmalarda spam sorununun çözümüne yönelik teknik ve yasal düzenlemelere ilişkin değerlendirmelerde bulunulmuştur. Bu anlamda gerçekleştirilen çalışmalardan bazıları aşağıda açıklanmıştır.

### 5.2.1 Dünya bilgi toplumu zirvesi (World summit on the information society – WSIS)

Dünya Bilgi Toplumu Zirvesi (World Suımmit on the Information Society – WSIS), Birleşmiş Milletler (BM) ve ITU tarafından, iki aşamalı olarak düzenlenen Bilgi Toplumu konulu bir dünya zirvesidir. İlk aşaması 10-12 Aralık 2003 tarihleri arasında Cenevre'de, ikinci aşaması ise 16-18 Kasım

2005 tarihleri arasında Tunus'ta düzenlenmiştir. Zirvenin düzenlenmesindeki temel amaç, hükümetlerin, uluslararası kuruluşların, özel sektör temsilcilerinin ve STK'ların katılımıyla bilgi toplumu için ortak bir vizyon ve anlayışın geliştirilmesidir [68].

#### 5.2.1.1 Cenevre 2003

Bu aşamanın sonunda *"İlkeler Bildirgesi"* ve *"Eylem Planı"* kabul edilmiştir. Zirvenin bu aşamasında spam sorunu, internet ve e-posta teknolojisinde potansiyel bir tehdit olarak tanımlanmıştır.

İlkeler Bildirgesinde spam mesajların, kullanıcılar, bilgisayar ağları ve internetin tümü için ciddi boyutlara ulaşan ve giderek büyüyen bir sorun olduğu ifade edilmiştir. Ayrıca, izinsiz ticari e-posta mesajlarının e-posta hizmetinin güvenliğini ve verimliliğini tehdit eder duruma geldiği, kullanıcıların elektronik haberleşme teknolojilerine karşı güvenlerini azaltıcı bir unsur olduğu değerlendirilmiştir. Spam sorununun uygun ulusal ve uluslararası zeminlerde ele alınması gerektiği belirtilmiştir [69].

Zirve sonunda Eylem Planının 5 numaralı ana başlığının *(Bilgi ve İletişim Teknolojilerinin Kullanımında Güven ve Güvenlik)* (d) maddesinde spam konusunda ulusal ve uluslararası seviyede gerekli çalışmaların yapılması ve uygun tedbirlerin alınması gerektiği ifade edilmiştir [70].

#### 5.2.1.2 Tunus 2005

Zirvenin Tunus aşamasında, Cenevre'de imzalanan "İlkeler Bildirgesi" ve "Eylem Planı" çerçevesinde kat edilen gelişmeler ele alınmıştır. Artık alınan kararların uygulamasına geçme zamanının geldiği ifade edilerek Cenevre'de yapılan taahhütler yinelenmiştir. Bu Zirvenin sonunda *"Bilgi Toplumu İçin*

*Tunus Gündemi (Tunus Agenda For The Informaiton Society)"* kabul edilerek yayınlanmıştır [71].

Zirve sonunda yayınlanan Tunus Gündemi dökümanının 41 inci ve 42 nci maddelerinde spam sorununa değinilerek büyüyen ve önemli bir sorun olarak ortaya çıkan spam için gerekli tedbirlerin alınması kararlaştırılmıştır.

41 inci maddede, ciddi ve büyüyen bir problem kaynağı olan spam e-postalarla etkili bir şekilde mücadele etmeye kararlı olunduğu belirtilmiştir. Spam e-posta sorununun çözümü için bölgesel ve uluslararası işbirliğine yönelik mevcut çok taraflı ve çok paydaşlı yapılara önem verildiği ifade edilerek uluslararası alanda işbirliğinin gerekliliği vurgulanmıştır. Spam e-posta sorununa karşı diğer tedbirlerin yanı sıra gerekli yasal düzenlemelerin yapılarak, icra otoriteleri ve araçların oluşturulması, teknik çözümlerin geliştirilmesine devam edilmesi, tüketici ve iş dünyasının eğitilmesi ve uluslararası işbirliği gibi faaliyetleri içeren çok yönlü bir mücadele yürütülmesi gerektiği belirtilmiştir.

42 nci maddede ise spam e-postalarla mücadele için alınan önlemlerin, kişisel mahremiyet ve ifade özgürlüğünü gözetmesi gerektiği ve buna göre şekillendirilmesi gerektiği ifade edilmiştir.

Zirve sonucunda Cenevre-Tunus Zirve kararlarının uygulanması ve takip edilmesi yönünde karar alınmış ve bu konuda hedeflere ulaşmada yaşanacak ilerlemenin sürdürülebilir olması için ulusal, bölgesel ve uluslararası seviyede, uygulama ve takip mekanizmaları kurulmasına karar verilmiştir. Buna göre, ITU'nun spam konusunda alınan kararların uygulamasında önderlik yapması gerektiği ve bu konuda yapılacak çalışmaları tertip etmesi gerektiği değerlendirilmiştir.

### 5.2.1.3 WSIS - Spam ile mücadele tematik toplantısı – Temmuz 2004

ITU tarafından gerçekleştirilen WSIS I. aşamasında açıklanan *İlkeler Bildirgesi* ve *Eylem Planı'nda* alınan kararlar çerçevesinde 07 - 09 Temmuz tarihleri arasında Cenevre'de spam ile mücadele konulu bir toplantı düzenlemiştir. Bu toplantı aynı zamanda Tunus'ta yapılan II. aşamaya da bir hazırlık niteliği taşımaktadır [72].

Sayıları 200 civarında olan katılımcıların profili oldukça geniş bir yelpazeyi kapsamakta olup ülke temsilcileri, uluslararası organizasyonların temsilcileri, tüketici grupları, İSS temsilcileri, Bilgi ve İletişim Teknolojileri (BİT) şirketleri, akademisyenler ve STK'ların temsilcilerinden oluşmaktadır.

Bu toplantılarda;

- Spam sorununun ulaştığı boyut ve verdiği zarar bir kez daha vurgulanmış ve problemin çözümü konusunda mutlak surette önlemler alınması gerektiği ifade edilmiş,
- Spam tanımı yapılmış ve sorunun çerçevesi çizilmiş,
- Teknolojik anlamda spam önleme teknikleri görüşülmüş,
- Yasal anlamda spam sorununa karşı kanunlarını ve icrasını tamamlamış ülke örnekleri incelenmiş,
- Bu konuda yasal düzenlemelerini henüz tamamlamamış ülkeler için model oluşturacak araştırmalar üzerinde durulmuş ve
- Uluslararası işbirliğinin önemine dikkat çekilerek ülkelerin ve organizasyonların bu konuda neler yapmaları gerektiği incelenmiştir.

Yapılan çalışmalar sonucunda elde edilen veriler bir rapor haline getirilerek yayınlanmıştır. Söz konusu raporda spam sorununa karşı çok yönlü ve kapsamlı bir mücadelenin beş ana maddeyi içerdiği vurgulanmıştır. Bu maddeler;

- Güçlü yasaların oluşturulması,
- Teknik önlemlerin geliştirilmesi,

- Sektörde faaliyet gösteren aktörlerin çözüm ortaklığı amacıyla işbirlikleri oluşturması,
- İnternet güvenliği ve spam önleme yöntemleri konularında tüketicilerin ve özel sektör oyuncularının eğitimi ve
- Hükümetler, sektör temsilcileri, tüketiciler, STK'lar ve uluslararası organizasyonların katılımıyla oluşturulacak uluslararası seviyede işbirliği ve çalışmalar neticesinde spam sorununa küresel boyutta bir yaklaşım getirilmesi

şeklinde sıralanmaktadır.

#### 5.2.1.4 WSIS - Siber güvenlik tematik toplantısı – Haziran 2005

ITU 07 – 09 Haziran tarihleri arasında Cenevre'de spam konulu bir toplantı düzenlemiştir. Toplantının ilk günü 2004 yılında düzenlenen *WSIS - Spam İle Mücadele* toplantısının devamı niteliğini taşımış ve spam ile mücadele konusunda küresel anlamda yapılan çalışmalar değerlendirilmiştir.

### 5.2.2 Dünya telekomünikasyon standardizasyon genel kurulu

21 – 30 Ekim 2008 tarihleri arasında *Johannesburg*'da gerçekleştirilen Dünya Telekomünikasyon Standardizasyon Genel Kurulu'nda (World Telecommunication Standardization Assembly - WTSA), spam konusunda bir adet çözüm kararı almıştır [73].

#### 5.2.2.1 Çözüm kararı 52 - spam ile mücadele

WSIS I. aşamasında açıklanan *İlkeler Bildirgesi* ve *Eylem Planı*'nın spam ile ilgili maddelerine ve *"Spam İle Mücadele"* konulu ITU WSIS toplantısı sonucunda açıklanan raporda ortaya konulan kapsamlı çalışmalara dikkat çekilmiş ve spam ile mücadelenin gerekliliğine vurgu yapılmıştır [74].

Bu kararda;

- Spam sorunun giderek yaygınlaşan bir problem olduğuna ve sektörde gelir kayıpları yaşanmasına neden olduğuna,
- Spam ile mücadele konulu ITU WSIS toplantısı sonunda hazırlanan raporun bu konuda yapılacak mücadeleye ilişkin kapsamlı ve çok yönlü bir yaklaşım ortaya koyduğuna,
- Spam mesajların global bir sorun olduğu ifade edilerek bu konudaki çözümlerin uluslararası işbirliği çerçevesinde geliştirilmesi gerektiğine,
- Spam yönteminin birçok kez aldatıcı faaliyetler, sahtecilik ve suç içeren faaliyetlerde kullanıldığına,
- Elektronik haberleşme ağlarındaki güvenliği tehdit ettiğine ve
- Özellikle az gelişmiş ülkelere ve küçük ada ülkelerine spam ile mücadele konusunda destek verilmesi gerektiğine

dikkat çekilmiştir [74].

Spam ile mücadele kapsamında ITU bünyesinde sürdürülen çalışmaların desteklenmesi, bu çalışmaların geliştirilerek devam ettirilmesi ve elde edilen sonuçların kamuoyu ile paylaşılması kararlaştırılmıştır. Ayrıca spam konusunda teknik çalışmalar yapan ve çözüm önerileri üreten İETF ve diğer gruplarla işbirliği içerisinde olunması ve düzenlenen organizayonlara katılım (çalıştay, konferans vb.) sağlanması gerektiği belirtilmiştir.

## 5.3 Avrupa Birliği

Avrupa Birliği spam ile mücadele konusunda önemli adımlar atmış ve üye ülkelere yasal düzenlemelerini yapma yükümlülüğü getirmiştir. Başlangıçta küçük bir sorun olarak algılanan spam mesajların günümüzde servis sağlayıcılar, iş dünyası ve son kullanıcılar açısından değerlendirildiğinde önemli bir maliyet oluşturduğuna dikkat çekilmiştir. Sık sık üye üyelerinin katılımıyla çalıştaylar düzenlenmiş ve alınacak önlemler üzerinde inceleme

ve değerlendirmeler yapılmıştır. Ayrıca bu çalışmalara zaman zaman üçüncü tarafların da katılımı sağlanarak uluslararası işbirliğinin artırılması hedeflenmiştir. Bu anlamda, OECD ve ITU gibi diğer uluslararası kuruluşların organize ettiği çalışmalara da katılım sağlanmış ve gelişmeler yakından takip edilmiştir.

### 5.3.1 Elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve mahremiyetin korunmasına ilişkin 2002/58/EC sayılı direktif

12 Temmuz 2002 tarihinde kabul edilen 2002/58/EC sayılı Direktif, özünde 97/66/EC sayılı "*Kişisel verilerin işlenmesi ve bu bilgilerin serbestçe dolaşımı hususunda bireylerin korunmasına ilişkin direktif*" ile aynı olmakla beraber internet ve multimedya teknolojilerinin yaygın olarak kullanıma girmesi ve teknolojide yaşanan gelişmelerle beraber eski direktifte bulunmayan ve aralarında spam e-posta konusunun da bulunduğu yeni kavram ve tanımları ele almıştır [75].

Söz konusu Direktifte spam ile ilgili olarak:

- Pazarlama amacıyla kullanılan ve otomatize edilmiş sistemler tarafından gönderilen faks, e-posta, SMS ya da MMS gibi her türlü mesajın, kullanıcıların önceden izninin alınmadan gönderilmesi yasaklanmış ve bu tür mesajların ancak önceden izni alınan kullanıcılara gönderilebileceği hükme bağlanmıştır. Böylece kapsam içi (opt-in)[1] yöntem tercih edilmiştir.
- Müşterilerinin e-posta adreslerini alan gerçek ya da tüzel kişilerin, müşterilerine kendi benzer ürünleriyle ilgili olarak doğrudan reklam amaçlı iletiler göndermesine izin verilmiştir.

[1] Opt-in: Ticari amaçlı ve toplu olarak e-posta gönderiminde öncelikle kişinin rızası ve onayının alınması zorunlu kılınmaktadır. Kişinin izni olmadan bu tür mesajların gönderilmesi yasaklanmaktadır.

- Müşterilerine pazarlama ve reklam amaçlı e-posta gönderecek olan firmaların mesaja konu ve açıklayıcı başlık koyması zorunluluğu getirilmiştir.
- Reklam e-postası gönderenlerin, kullanıcılara e-posta dağıtım listesinden çıkma ve bir daha bu tarz mesajları almama seçeneği sunmaları bir yükümlülük olarak getirilmiştir. Ayrıca, kullanıcıların dağıtım listelerinden çıkmalarını kolaylaştıracak yöntemleri, kolay ve ücretsiz bir yolla sunma zorunluluğu getirilmiştir.
- Her türlü reklam ve pazarlama faaliyetlerinde gönderilecek e-posta mesajlarında, mesajı gönderen tarafın kimliğini gizlemesi veya yanlış bilgi vermesi ya da yanlış e-posta adresi kullanımı (kullanıcıların taleplerini iletebilecekleri ya da e-posta dağıtım listesinden çıkmak için talepte bulunacakları e-posta adresi) yasaklanmıştır.
- Direktif, spam konusunda üye ülkelerin kurallar koyması gerekliğini vurgulamış ve oluşturulacak yasal düzenlemenin temelinde kapsam içi (opt-in) yöntemin tercih edilmesi gerektiğini belirtmiştir. Böylece, kapsam dışı (opt-out)[1] yöntemi temel alan düzenlemelerin uygulanması direktif kapsamında reddedilmiştir.
- Direktifin yayınlanmasının ardından üye ülkelerin spam konusunda gerekli yasal düzenlemelerini bu Direktif çerçevesinde tamamlamaları konusunda 31 Ekim 2003 tarihine kadar süre tanınmıştır.

Genel itibariyle Direktifte bulunan maddeler incelendiğinde süreçlerin detaylandırılmadığı, daha çok temel konulara yer verildiği görülmektedir. Örneğin, kapsam içi yöntemi gereği tüketicilere e-posta göndermek üzere alınması gerekli iznin ne şekilde yapılacağı konusu belirtilmemiştir. Ayrıca, satıcıların daha evvel kendilerinden alışveriş yapmış alıcılara benzer ürünler hakkında satış amaçlı e-posta gönderebileceği hükmü yer almasına rağmen

[1] Opt-out: Ticari ve toplu mesaj gönderiminde ön koşul olarak kişinin izninin alınması gerekli değildir. Ancak, kişinin bir daha mesajı almak istememesi durumunda mesaj dağıtım listesinden çıkışını kolaylaştıran bir yöntemin olması zorunlu kılınmaktadır. Başka bir deyişle mesaj almak istemediklerini belirten kişiler dışındakilere mesajın gönderilmesi serbest bırakılmaktadır.

benzer üründen kastedilenin ne olduğu açıkça belirtilmemiştir. Bununla birlikte, Direktifte e-posta göndericilerin uyması gereken şartlar belirtilmiş olmasına rağmen bu şartlara uymayan bir durum olduğunda ne gibi yaptırımlar uygulanacağına yer verilmemiştir.

### 5.3.2 Spam çalıştayları

AB tarafından çeşitli tarihlerde spam konulu çalıştaylar düzenlenmiştir. Bunlardan üçü de 16 Ekim 2003, 22 Ocak 2004 ve 15 Kasım 2004 tarihlerinde Brüksel'de gerçekleştirilmiştir. Söz konusu çalışmalarda spam ile mücadele kapsamında:

- AB direktifleri çerçevesinde üye ülkeler tarafından gerçekleştirilmesi gereken yasal düzenleme platformları,
- Teknolojik çözüm yolları,
- Kullanıcıların bilinç düzeyi ve eğitim seviyelerinin artırılmasına yönelik çalışmalar ve
- Uluslararası işbirliği çalışmaları konularında bilgi alış verişi gerçekleştirilmiş ve incelemelerde bulunulmuştur.

### 5.3.3 Konsey kararları

#### 5.3.3.1 2568 inci konsey toplantısında alınan kararlar

AB Konseyi tarafından 08 Mart 2004 tarihinde gerçekleştirilen 2568 inci toplantıda spam konusu da gündem maddelerinden birini oluşturmuş ve bir takım tavsiye kararları alınmıştır [76]. Üye ülkelere verilen tavsiye kararları;

- Spam ile mücadele kapsamında ikili ve çoklu seviyedeki uluslararası işbirliklerinin geliştirilerek sürdürülmesi,

- Spam konusunda çözüm oluşturacak teknik çözümlerin değerlendirilmesi,
- Kullanıcı bilinçlendirme ve eğitim kampanyalarının desteklenmesi,
- Gerek kanunların icrasını gerçekleştiren kurumların ve gerekse özel sektör tarafından spam önleme konusunda gerçekleştirilecek işbirliği faaliyetlerinin özendirilmesi ve
- Birlik üyeleri arasında spam ile mücadele kanunlarının icrası konusundaki tecrübe ve bilgi paylaşımının sağlanması şeklindedir.

Komisyonun amaçları ise;

- Spam ile mücadelede atılan adımların verimliliğinin ve soruna etkisinin izlenerek alınması gereken ek önlemler olup olmadığının belirlenmesi,
- Birlik içerisinde ya da üçüncü taraflarla yapılacak ortaklıkların etkili sonuçlar ortaya koymasını sağlayacak şartların belirlenmesi ve
- Birlik üyelerinin ulusal düzenlemeleri ve çalışmalarının takip edilerek güncel bilgilerin yayınlanması şeklinde belirlenmiştir.

#### 5.3.3.2 2629 uncu konsey toplantısında alınan kararlar

AB Konseyi tarafından 09-10 Aralık 2004 tarihinde gerçekleştirilen 2629 uncu toplantıda spam konusunda bir takım tavsiye kararları alınmıştır [77]. Üye ülkelere verilen tavsiye kararları;

- Spam ile mücadele kapsamında kullanıcı bilinçlendirme kampanyaları konusunda bilgi paylaşımı ve
- İkili ve çoklu işbirliklerinin geliştirilmesi şeklinde olmuştur.

Komisyonun amaçları ise;

- Spam ile mücadelede konusundaki AB direktifleri uyarınca hazırlanan ulusal altyapılar arasında farklılıklar olup olmadığının incelenmesi,

- Uluslararası çalışmaların devamının sağlanması ve
- Birlik içerisinde ya da üçüncü tarafların da katılımıyla gerçekleşecek çalışmalarda aktif rol oynamak şeklinde sıralanmıştır.

### 5.3.4 Avrupa Şebeke ve Bilgi Güvenliği Kurumu

İletişim şebekeleri ve bilgi sistemleri günümüzde bir toplumun gelişmesini sağlayan temel faktörlerdir. Dijital dünyada güvenli şebekeler her geçen gün su gibi elektrik gibi hayatımızın vazgeçilmez öğeleri arasında yerini almaktadır. Bu nedenle iletişim şebekeleri ve bilgi sistemlerinin güvenliğinin sağlanması son derece kritik ve önemli bir konu halini almıştır. Bu ihtiyaçtan yola çıkılarak AB bünyesindeki üye ülkelerde yüksek dereceli güvenlik seviyesini elde etmek amacıyla tek bir çatı altında bu konudaki çalışmaları yönlendirecek bir organizasyon oluşturulması amaçlanmıştır. Bu bağlamda bilgi güvenliği konusunda Avrupa koordinasyonunu kurmak ve geliştirmek amacıyla, 13.3.2004 tarih ve 460/2004/EC sayılı Tüzük ile merkezi Yunanistan'da bulunan Avrupa Şebeke ve Bilgi Güvenliği Kurumu (Europa Network and Information Security Agency - ENISA) kurulmuştur.

ENISA, bilgi ve iletişim güvenliği konusunda temel güvenlik ihtiyaçlarını karşılamak üzere Komisyona ve üye devletlere gerekli her türlü katkıyı ve desteği sağlamakla görevlendirilmiştir. Kurum, bilgi güvenliği ile ilgili tüm taraflar ve aktörler arasında uluslararası işbirliğinin kurulması ve geliştirilmesine katkıda bulunmak üzere faaliyetlerini sürdürmektedir. ENISA ayrıca, AB dışındaki diğer ülkelerle de şebeke ve bilgi güvenliği konusunda işbirliği kurmak ve geliştirmek üzerine çalışmalarda bulunmaktadır.

ENISA'nın çalışma yaptığı alanlardan bir tanesi de spam ile mücadele konusudur. Bu kapsamda, 2006 ve 2007 yılında iki ayrı çalışma yapılmış ve elde edilen bilgiler rapor haline getirilerek kamuoyu ile paylaşılmıştır.

## 5.4 Londra Eylem Planı

11 Ekim 2004 yılında 27 ülkeden hükümet temsilcileri, bilgi güvenliği kurumları, telekomünikasyon sektör temsilcileri ve tüketici koruma birliklerinin katılımıyla gerçekleştirilen görüşmeler sonucunda kabul edilmiştir [78].

Eylem Planında yer alan temel konulardan bazıları şunlardır;

- Spam ile mücadele konusunda uluslararası alanda bilgi ve tecrübe paylaşımı.
- Belli peryotlarda, katılımcılar arasında görüş alışverişinde bulunmak üzere konferanslar düzenlenmesi.
- Kamu ve özel sektör temsilcilerinin spam ile mücadelede yeni stratejiler geliştirmek üzere diyalog içinde olması.
- Az gelişmiş ülkelerin çeşitli işbirliği çalışmaları ile desteklenmesi.
- Özel sektör temsilcilerinin teknolojik gelişmeleri takip etmeleri bu konuda diğer sektör temsilcileri ile bilgi paylaşımında bulunması.

# 6 ÜLKE ÖRNEKLERİNİN İNCELENMESİ

Bu bölümde spam konusunda gerekli yasal düzenlemelerini tamamlamış ülkelerden örnekler incelenmiştir.

## 6.1 Bazı Avrupa Birliği Ülkelerinin Değerlendirilmesi

AB'nin 2002/58/EC sayılı direktifiyle birlikte spam konusunda üye ülkelerin yasal düzenlemelerini oluşturmaları zorunlu kılınmıştır. Bu kapsamda aralarında Avusturya, Belçika, Danimarka, Finlandiya, Fransa, İngiltere İrlanda, İspanya, İsveç, İtalya ve Portekiz'in bulunduğu 11 ülkenin spam konusundaki düzenleme alt yapılarının çeşitli yönlerden değerledirilmesi Çizelge 6.1'de ele alınmıştır [79]. Buna göre, söz konusu 11 ülkenin yasası, spam kavramının kapsamını belirlerken doğrudan ya da dolaylı olarak pazarlama amacı içeren mesajları ele almıştır. Bunun dışında sadece Avusturya'da toplu olarak gönderilen mesajlar da ele alınmış ve bir mesajın spam olarak değerlendirilmesinin bir koşulu da toplu gönderim olarak belirlenmiştir. Buna göre, dağıtım listesinde 50'den fazla alıcı adresi bulunan mesajlar yasa kapsamına dahil edilmiştir. Teknolojik açıdan kapsamın belirlenmesi kısmında ise Belçika, İspanya, Fransa ve İsveç'in sadece e-posta hizmetini ele aldıkları görülmekte, diğer ülkelerin ise SMS, MMS ve faks mesajları gibi teknolojik çerçeveyi daha geniş bir kapsamda ele aldıkları görülmektedir.

AB'nin 2002/58/EC sayılı direktifi gereğince tüm ülkelerin mesaj gönderiminde alıcının izninin alınmasını şart koşan kapsam içi (opt-in) yöntemi tercih ettiği görülmektedir. Bu yöntemde şart koşulan alıcının rızasının alınması işleminin açık bir şekilde kullanıcıya sunulması zorunlu kılınmakta ancak bu zorunluluğu ortadan kaldıran bazı istisnai durumlar bulunmaktadır. Bu yasalara göre, gönderici ve alıcı arasında önceden var

olan ilişkilerde (işveren-çalışan, satıcı-alıcı, dernek-üye vb.) kullanıcıdan açık izin alma zorunluluğu bulunmamaktadır.

Gerçekleştirilen yasal düzenlemelerin birçoğunda yasa kapsamına alınan her türlü mesajda, mesajı gönderen tarafın kimliğini açık, doğru ve eksiksiz bir şekilde belirtmesini zorunlu kılan hükümlere yer verilmiştir. Yine mesajı gönderenin, e-posta adresini doğru bir şekilde belirtmesi ve kullanıcıların ilgili mesajı bir daha almamak üzere dağıtım listesinden çıkma taleplerinin de ücretsiz ve kolay bir yolla sağlanması değerlendirmeye tutulan 11 ülkenin tamamında zorunlu kılınmıştır. Ayrıca e-posta adreslerinin izinsiz toplanması, adres toplayan yazılımların kullanılması, bu adreslerin mesaj gönderiminde kullanılması veya başka kişi ya da kuruluşlarla paylaşılması da yasaklanmıştır.

Çizelge 6.1 Bazı Avrupa Birliği Ülkelerinin Değerlendirmesi [79]

| | *Avusturya* | *Belçika* | *Danimarka* | *İspanya* | *Finlandiya* | *Fransa* | *İngiltere* | *İrlanda* | *İtalya* | *Portekiz* | *İsveç* |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Spamın kapsamının belirlenmesi** | | | | | | | | | | | |
| Ticari Nitelik | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Tekonolojik Kapsam | ■ | | ■ | | ■ | | ■ | ■ | ■ | ■ | |
| Alıcı Sayısı | ■ | | | | | | | | | | |
| **Mesaj Gönderim İzni** | | | | | | | | | | | |
| Ön İzin Şartı | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| **Mesaj Gönderme Şartları** | | | | | | | | | | | |
| Gönderenin Kimlik Bilgisi | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | ■ | | |
| Dağıtım Listesinden Çıkma | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |

## 6.2 Avustralya

Avustralya'da spam mesajlar ile ilgili yasal çerçeve "Spam Kanunu" ile belirlenmiş ve bu kanun 10 Nisan 2004 tarihinde yürürlüğe girmiştir [80].

### 6.2.1 Kanunun içeriği

Kanuna göre spam mesajlar, *"alıcısının izni olmadan gönderilen ticari elektronik mesajlar"* şeklinde tanımlanmaktadır. Ticari elektronik mesajların kapsamı ise yine bu kanun ile belirlenmiştir [81]. Buna göre;

- Bir ürüne ya da hizmete ilişkin pazarlama veya reklam faaliyetleri içeren,
- Ticari yatırım fırsatlarının reklamına ilişkin faaliyetleri içeren,
- Mesaj alıcılarını bir ürün ya da hizmetin satışının veya reklamının yapıldığı bir konuma yönlendiren veya
- Bir kişiye gayri meşru yollardan mülk edinme, mali kazanç sağlama ya da bir başka kişi üzerinden kazanç sağlama faaliyetleri içeren mesajlar,

ticari elektronik mesaj kapsamında ele alınmaktadır.

Ticari elektronik mesajların teknolojik bazlı kapsamı ise elektronik posta hizmeti, SMS, MMS ve anlık mesajlaşma olarak belirlenmiştir. Telefon yoluyla yapılan ses iletişimi ve faks yoluyla gönderilen mesajlar kanun kapsamı dışında bırakılmıştır. Kanun ile belirlenen yükümlülükler ve gereklilikler toplu ya da kişisel olarak gönderilen mesajlar da dahil olmak üzere tüm ticari mesajları içermektedir [78].

Kanuna göre ticari elektronik mesaj gönderme faaliyetlerinin beş temel şartı yerine getirmesi gerekmektedir [80, 81, 82].

1- Kanun ile ticari elektronik mesaj gönderme sürecinde kapsam içi yöntem (opt-in) tercih edilmiştir. Buna göre, mesajlar sadece izin veren alıcılara gönderilebilmektedir. Alıcının iznini almak öncelikli bir şart durumundadır.
2- Tüm ticari elektronik mesajlar göndericisi ile ilgili tanımlayıcı bilgi içermelidir ve söz konusu bilgi, mesajın gönderildiği tarihten sonra 30 gün için geçerliliğini korumalıdır.
3- Mesaj alıcılarına bir daha mesajı almak istememeleri durumunda dağıtım listesinden çıkabilme seçeneği sunulması zorunlu kılınmıştır. Herhangi bir kullanıcıdan gelecek böyle bir talebin 5 iş günü içerisinde sonuçlandırılarak kişinin mesajı tekrar almaması sağlanmalıdır. Kullanıcılara mesajı tekrar almama seçeneğini ortaya koyan yöntemin, mesajın gönderildiği tarihten sonra 30 gün için geçerliliğini koruması gerekmektedir.
4- Elektronik adreslerin izinsiz toplanması, adres toplayan yazılımların kullanılması ya da izinsiz ele geçirilmiş adres listelerinin mesaj gönderiminde kullanılması yasaklanmıştır.
5- Kanuna aykırı hareket edenlere yardım etmek ya da işin bir parçası olmak suç teşkil eden durumlar arasında değerlendirilmiş ve yasaklanmıştır.

Kanun kapsamı dışında bırakılan bazı elektronik mesajlar bulunmaktadır. Bu kapsamda değerlendirilen mesajlar kamu yararına faaliyet gösteren bazı yapılar tarafından gönderilen mesajları kapsamaktadır [82]. Bu yapılar:

- Hükümet Organları
- Tescilli Siyasi Partiler
- Yardım Kuruluşları
- Dini Organizasyonlar
- Eğitim Kuruluşları

Kapsam dışında kalan elektronik mesajlar için alıcının izninin olması zorunluluğu bulunmamaktadır. Ancak gönderilen mesajda, gönderen

organizasyonun ya da organizasyon adına yetkilendirilmiş kişinin kendisini tanımlayıcı bilgilerin yer alması zorunlu kılınmıştır.

### 6.2.2 Kanunun uygulanması

Avustrulya'da Spam Kanunu'nun uygulama yetkisi ACMA'ya (Avustralya Telekomünikasyon ve Medya Otoritesi-Australian Communications and Media Authority) verilmiştir. Buna göre ACMA, kanuna aykırı durumlara ilişkin incelemeleri yapmakta ve soruşturmayı yönetmektedir. Bu kapsamda ACMA tarafından yürütülen bazı faaliyetler aşağıda belirtilmiştir [83].

- Gelen ihbarları almak ve değerlendirmek için bir şikayet merkezi ve internet sayfası oluşturulmuştur.
- Çeşitli eğitim ve bilinçlendirme kampanyaları düzenlenerek kullanıcıların spam konusunda bilgilenmeleri sağlanmıştır.
- Özel sektör aktörleri ile işbirliği yapılmış ve kanun uygulamasının etkin bir şekilde yürütülmesi sağlanmıştır.
- Spam ile mücadele konusundaki teknolojik gelişmeler takip edilmiştir. Spam mesajları ACMA'ya rapor edebilen bir raporlama aracı geliştirilmiş ve kullanıcıların hizmetine sunulmuştur.
- Uluslararası işbirliğine önem verilmiş ve bu alanda çeşitli çalışmalar yapılmıştır.

Bunun yanı sıra ACMA, spam ile mücadele konusunda;

- Avustralya Rekabet ve Tüketici Komisyonu (Australian Competition and Consumer Commission - ACCC),
- İnternet Endüstrisi Birliği (Internet Industry Association),
- Avustralya Güvenlik ve Yatırım Komisyonu (Australian Securities and Investments Commission),
- Doğrudan Pazarlama Birliği (Direct Marketing Association - ADMA) ve
- Avustralya Federal Polisi

ile yakın işbirliği içinde bulunmaktadır.

### 6.2.3 Uluslararası işbirliği çalışmaları

Spam konusunun küresel bir problem olduğuna dikkat çekilmiş ve Avustralya'da dolaşan spam mesajların %99 oranında ülke dışındaki kaynaklardan geldiği belirtilmiştir [84]. Bu kapsamda, Avustralya'nın diğer ülkelerle yaptığı işbirliği çalışmaları aşağıda verilmektedir;

- Tayvan ile İkili Mutabakat Zaptı
- Çin, Hong Kong, Japonya, Kore, Malezya, Yeni Zelanda, Filipinler, Tayland ve Tayvan ile spam ile mücadele konulu Çoklu Mutabakat Zaptı (Seul-Melbourne Anti-spam Anlaşması)
- Kore ile ikili Mutabakat Zaptı
- İngiltere ve ABD ile üçlü Mutabakat Zaptı
- Londra Eylem Planı

## 6.3 Amerika Birleşik Devletleri

ABD'de spam ile mücadele 1997 yılından itibaren yürütülmektedir. İlk olarak bu yıl yetkililerin dikkatini çeken spam sorununa ilişkin önlem alıcı çalışmalar aynı yıl içerisinde başlatılmıştır. Bu kapsamda aynı yılın Haziran ayında Federal Ticaret Komisyonu (Federal Trade Commission - FTC) bir çalıştay düzenlemiş ve spam konusunu ele almıştır. Spam ile ilgili ilk yasal düzenleme önerisi de aynı yıl içerisinde Kongre'ye ve 5 eyaletin yasama meclisine sunulmuş fakat kabul görmemiştir [85].

1997 yılında başlayan çalışmalar her geçen yıl giderek artan bir önem ve dikkat çerçevesinde ele alınmış ve 2003 yılına gelindiğinde 36 eyalette spam e-postaları yasaklayan çeşitli yasalar çıkarılmıştır. Bu yasaların kapsamı

değişiklik göstermekle birlikte çoğu, reklam içerikli e-postalar üzerinde bir düzenleme içermekteydi. Yapılan yasal düzenlemelerin birçoğu kapsam dışı yöntemi tercih ederken sadece iki eyalette çıkarılan yasalar kapsam içi yöntemin uygulanmasını zorunlu kılmıştır.

2003 yılına gelindiğinde spam ile mücadele kapsamında federal bir yasa çıkarılmamış her eyalet kendi yasasını oluşturmaya çalışmıştır. Ancak, eyaletlerin yasal düzenlemeleri birbirinden farklılık arz ettiğinden ve uygulama kapsamında bazı zorluklar ortaya çıktığından yasaların spam ile mücadelede etkin bir sonuç üretmesi mümkün olmamıştır. Eyaletler arasındaki kanunların farklılığı, kanunlara göre suç sayılan durumların çeşitliliği nedeniyle iki farklı eyaleti birden ilgilendiren (spam e-posta göndericisi ile alıcısının farklı eyaletlere mensup olması) spam olaylarında hangi kanunun gereklerinin yerine getirileceği konusunda sıkıntılar ortaya çıkmıştır. Ortaya çıkan bu durum ABD'de federal bir yasanın çıkarılmasını zorunlu kılmış ve 16 Aralık 2003 tarihinde federal bir yasa olan "İstenmeyen Pornografinin ve Pazarlamanın Denetlenmesi Kanunu - The Controlling the Assault of Non-Solicited Pornography and Marketing Act" Kongre'de kabul edilmiştir. "Can Spam Act" olarak da bilinen bu kanun 01 Ocak 2004 tarihinde yürürlüğe girmiş ve mevcut eyalet yasalarını geçersiz kılmıştır.

### 6.3.1 Kanunun içeriği

Çıkarılan yasa esas itibariyle ticari nitelik taşıyan e-postaları kapsamaktadır. Ticari nitelik taşıyan e-postalar kanunda, ticari reklam, ya da ticari bir ürün veya hizmetin reklamı ya da promosyonu olan e-postalar şeklinde tanımlanmıştır. Ticari nitelik taşıyan e-postaların niteliğinin gizlenmesi söz konusu kanunda yasaklanmıştır. Bu anlamda, bu tür e-postaların ticari nitelikte olduğunun alıcı tarafından açık ve kolay anlaşılır şekilde gönderilmesi gerekmektedir. Başka bir deyişle alıcının, adresine gelen e-

postanın ticari nitelikte bir içerik taşıdığını e-postanın konu kısmından açıkça anlayabilmesine olanak sağlayacak şekilde gönderilmesi gerekmektedir. Ancak, önceden izin alınmış kişilere gönderilecek ticari e-postalar istisna bir durum olarak ele alınmış ve bu kapsamdaki e-postaların ticari nitelik taşıdığının belirtilmesi zorunlu kılınmamıştır [86].

ABD spam yasasında e-posta göndericisi ve alıcısı arasındaki mevcut ticari ilişkilerin gereği olarak gönderilen mesajlar, kanun kapsamı dışında tutulmuştur. Buna göre,

- Tarafların önceden üzerinde anlaştığı bir ticari işlemi onaylayan veya doğrulayan,
- Bir ürünün iade koşullarını, kullanım bilgilerini ve garanti koşullarını içeren,
- Abonelik veya üyelik gibi ticari ilişkilerin koşul ve niteliklerindeki değişiklikleri bildiren ve
- Ürün güncellemelerini içeren e-postalar kanun kapsamı dışında bırakılmıştır.

ABD spam yasasının temelinde kapsam dışı (opt-out) yöntem kabul görmüştür. Buna göre, e-posta göndericileri alıcılarından izin almaksızın ticari e-posta gönderme hakkına sahiptir. Kapsam dışı yöntemin tercih edilmesi ABD'de bazı çevreler tarafından şiddetle eleştirilmiş ve bu yöntemin spam gönderimini bir nevi serbest bıraktığı yönünde bir anlayış oluşturmuştur. Bir defa dahi olsa spam gönderiminin serbest bırakıldığı ifade edilmiş ve kanunun spam ile mücadelede etkin sonuçlar vereceği noktasında kuşkular oluşmasına neden olmuştur. Bir başka eleştiri noktası da bir gün içerisinde bir kişiye gelen spam e-posta sayısının oldukça fazla olmasından yola çıkılarak kişinin her bir e-postayla ilgili dağıtım listesinden çıkma talebi yapmasının ciddi bir zaman kaybı olacağı konusudur. Spam kanununun 2003 yılında çıkarılmasına rağmen, ABD'nin halen en çok spam üreten ülkelerin başında gelmesi yapılan eleştirileri bir nevi haklı çıkarmaktadır [87, 88].

Yasaya göre,

- E-posta göndericisinin mesaj içeriğinde kendisini tanımlayıcı bir bilgi bulundurması,
- Alıcının mesajı bir daha almak istememesi durumunda, mesajın tekrar gönderilmemesine imkan tanıyan bir yöntemin alıcıya sunulması,
- Alıcının e-postayı gelecekte almayı reddetme hakkını kullanması durumunda göndericinin söz konusu talebi on iş günü içerisinde yerine getirmesi

zorunlu kılınmış olup,

- Göndericinin kendisini tanımlama konusunda aldatıcı ya da yanlış bilgiler vermesi,
- Gönderen e-posta adresinin sahte, geçersiz ya da yanlış bilgi içermesi,
- Reddedilen göndericinin başka bir gönderici aracılığıyla e-posta göndermeye devam etmesi,
- E-posta alıcısının adresinin başka göndericilerle paylaşılması ya da bu adreslerin satılması,
- E-posta adreslerinin izinsiz bir şekilde toplanması,
- İzin verilmemiş bir e-posta sistemini kullanmak suretiyle ticari amaçlı e-postalar gönderilmesi

yasaklanmıştır [86, 89].

### 6.3.2 Kanunun uygulanması

ABD'de "Can Spam Act" in uygulama yetkisi FTC'ye verilmiştir. Buna göre FTC, kanuna aykırı durumların oluşup oluşmadığına ilişkin incelemeleri yürütmektedir. Bu kapsamda FTC tarafından yürütülen bazı faaliyetler aşağıda belirtilmiştir [89].

- Gelen ihbarları almak ve değerlendirmek için şikayet merkezleri oluşturulmuştur.

- Kişi ve kurumların spam e-posta ile mücadele konusunda bilgi edinebilecekleri, Kanun'a ve uygulamasına ilişkin kamuoyunu bilgilendirici değerlendirmelerin yayınlandığı internet sayfası oluşturulmuştur.
- Çeşitli eğitim ve bilinçlendirme kampanyaları düzenlenerek kullanıcıların spam konusunda bilgilenmeleri sağlanmıştır.
- Özel sektör aktörleri ile işbirliği yapılmış ve kanun uygulamasının etkin bir şekilde yürütülmesi sağlanmıştır.
- Spam ile mücadele konusundaki teknolojik gelişmeler takip edilmiştir.
- Uluslararası işbirliğine önem verilmiş ve bu alanda çeşitli çalışmalar yapılmıştır.

Ayrıca, DMA ticari nitelikte e-posta almak istemeyen kişilerin başvurularını alarak bu kişilerin e-posta adreslerini bir liste şeklinde tutmaktadır. Söz konusu listede bulunan e-posta adreslerine ticari e-posta mesajlarının gönderimi yasaklanmıştır. Böylece kullanıcılar, her bir ticari e-posta için dağıtım listesinden çıkma talepleri ile uğraşmak zorunluluğundan kurtarılmış olmaktadır [90].

İSS'ler de bu kapsamda teknik ve idari önlemler almak durumunda kalmışlardır. Kullanıcıları ile yaptıkları abonelik sözleşmelerinde e-posta ile spam gönderemeyeceklerine dair taahhüt yer almakta, aksi takdirde zararı kullanıcıların kendilerinin gidermek zorunda kalacakları maddesi bulunmaktadır.

ABD'de spam kanununun uygulaması neticesinde yasalara aykırı hareket eden kişi ya da kurumlara çok ciddi para cezaları verilmiş, hatta hapis cezalarına kadar varan durumlar olmuştur. Örneğin, 1,2 milyon kullanıcıya ticari ürün reklamlarını içeren milyonlarca spam e-posta gönderen Todd Moeller, New York'ta görülen davada 27 ay hapis cezasına çarptırılmış, bunun yanı sıra 180 bin dolar da para cezası verilmiştir [91]. Bir başka örnek

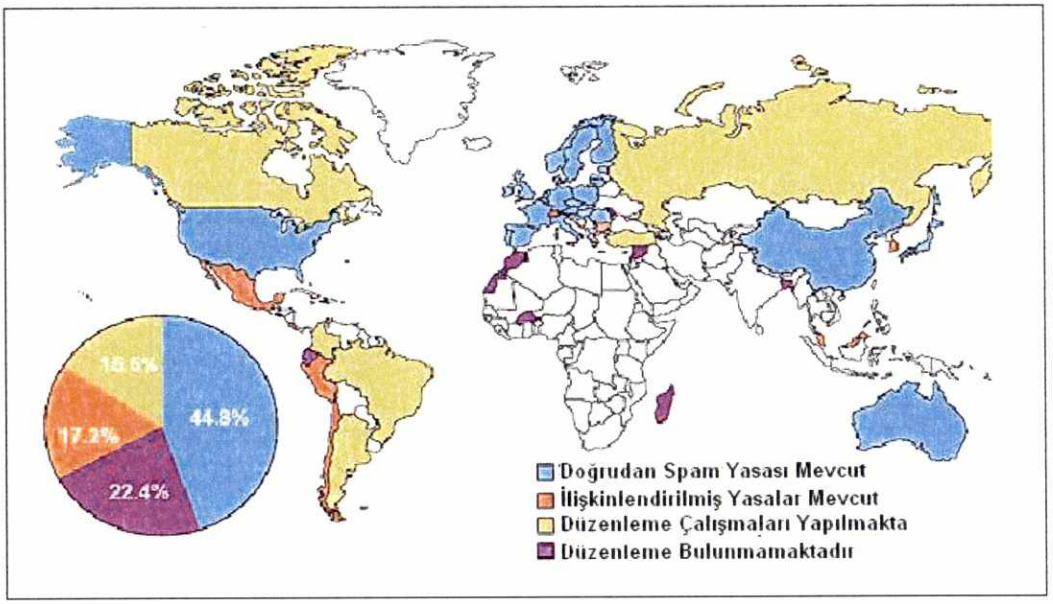
ise Iowa eyaletinde görülen davalar sonucunda verilen cezalar olmuştur. Buna göre AMP Dollar Savings şirketine 720 milyon dolar, Cash Link Systems şirketine 360 milyon dolar ve TEI Marketing Group'a da 140 bin dolar para cezası verilmiştir [92].

### 6.3.3 Uluslararası işbirliği çalışmaları

Spam konusunun küresel bir problem olduğu gerçeğinden yola çıkılarak uluslararası kuruluşların organize ettiği çalışma ve toplantılara katılım sağlanmış ve destek verilmiştir. Ayrıca, bu konuda uluslararası ilişkilere önem veren İngiltere ve Avustralya ile üçlü Mutabakat Zaptı imzalamıştır.

## 6.4 Diğer Ülkelerde Durum

ITU tarafından 2005 yılında 58 ülkeyi kapsayan ve bu ülkelerdeki spam ile ilgili düzenlemeleri konu alan bir araştırma, aralarında Avustralya, ABD ve Japonya'nın da bulunduğu birçok ülkenin spam konusunda özel yasa çıkardığını ortaya koymuştur. Şekil 6.1'de görüldüğü gibi bu kapsamda değerlendirilen ülkelerin oranı %44.8 olarak belirtilmiştir. Meksika, Malezya, Peru gibi doğrudan spam yasası olmamakla birlikte Tüketicinin Korunması Kanunu, Verilerin Korunması Kanunu ve Telekomünikasyon Kanunu gibi çeşitli kanunlarla spam problemini adreslemiş ülkelerin oranı ise %17.2 olarak belirtilmiştir. Araştırmanın yapıldığı tarih itibariyle Sinagapur ve Yeni Zelanda gibi ülkelerin ise spam konusunda yasal düzenleme çalışmalarına başladığı görülmüştür. Bu ülkelerin oranı ise yapılan araştırmada %15.5 olarak ifade edilmiştir. Spam konusunda herhangi bir düzenlemesi bulunmayan ülkelerin (Burkina Faso, Lübnan vb.) oranı ise %22.4 olarak tespit edilmiştir [93].




Şekil 6.1 Çeşitli Ülkelerin Spam Konusundaki Düzenlemeleri

Çizelge 6.1'de spam konusunda yasal düzenleme yapmış çeşitli ülkelere ilişkin bazı bilgiler yer almaktadır. Bu ülkelerin birçoğunun kapsam içi yöntemi benimsediği görülmektedir. Ayrıca, kapsam içi yöntemi benimseyen söz konusu ülkelerin genellikle, e-posta göndericisi ile alıcısı arasında bir ilişkinin var olması durumunda, kapsam içi yöntemin temelinde yatan e-posta alıcısının izninin alınması ön şartından muaf tutan bir düzenleme gerçekleştirdikleri görülmektedir.

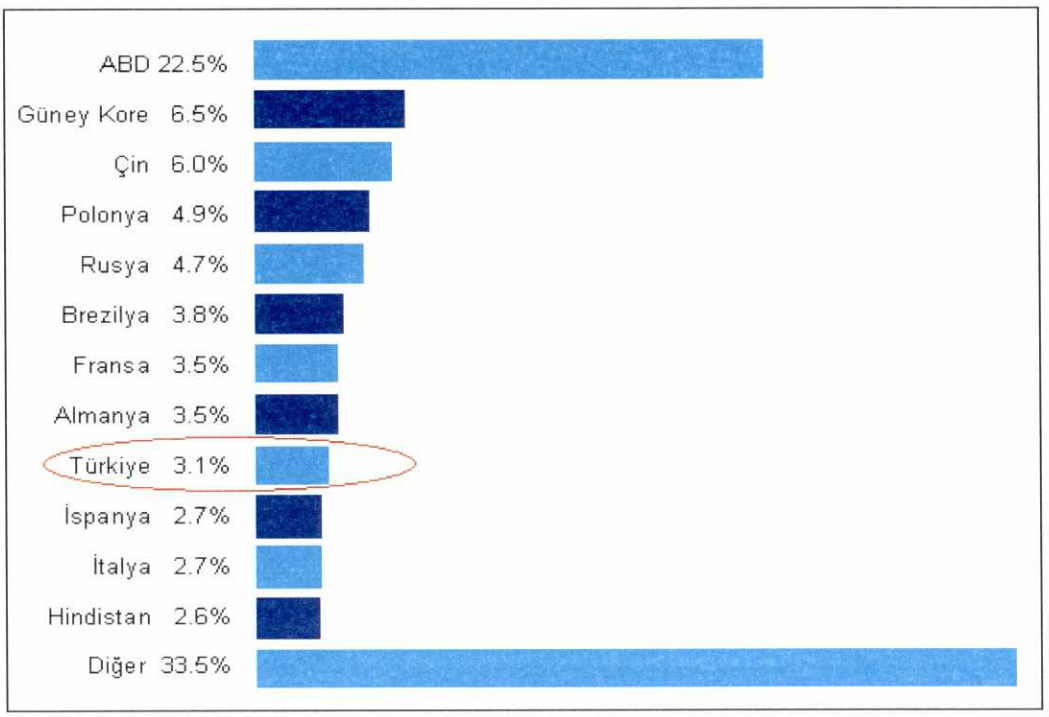
Çizelge 6.2 Spam Konusunun Diğer Ülkelerdeki Durumu [94]

| | MEVZUAT | MEVZUATIN İSMİ VE YÜRÜRLÜK TARİHİ | KAPSAM İÇİ/KAPSAM DIŞI | KAPSAM İÇİ/KAPSAM DIŞI YÖNTEMİNDE İSTİSNA |
|---|---|---|---|---|
| ABD | Can-Spam Kanunu | 1.1.2004 | Kapsam dışı | |
| Almanya | Mevcut kanun olan haksız rekabet kanunu | | Kapsam içi | Önceden var olan ilişkide kapsam dışı |
| Avustralya | Spam kanunu | 2.12.2003 | Kapsam içi | Kamu kurumları, siyasi partiler, dini kuruluşlar, yardım kuruluşları, eğitim kurumları |
| Avusturya | Telekomünikasyon düzenlemeleri kanunu | 2003 | Kapsam içi | |
| Belçika | Elektronik ticaret kanunu | 11.3.2003 | Kapsam içi | Tüzel kişi, önceden var olan ilişki |
| Çek Cumhuriyeti | Mevcut kanun olan reklamların düzenlenmesi kanunu | 1995 | Kapsam içi | |
| Danimarka | Pazarlama faaliyetleri kanunu | | Kapsam içi | Önceden var olan ilişki |
| Finlandiya | Telekomünikasyonda veri güvenliği ve mahremiyetin korunması kanunu | 1999 | Kapsam içi | Tüzel kişi |
| Fransa | Sayısal ekonomiye güven | | Kapsam içi | Önceden var olan ilişki, tüzel kişi |
| İngiltere | Mahremiyet ve elektronik haberleşme düzenlemeleri | 11.12.2003 | Kapsam içi | Mevcut müşteri ilişkileri için kapsam dışı istisnası uygulanmaktadır. Tüzel kişiler, yeni e-posta kapsam içi kuralları gereğince kapsanmamaktadır. |
| İrlanda | Elektronik haberleşme şebekeleri ve hizmetleri | 2003 | Kapsam içi | Önceden var olan ilişki |
| İspanya | Bilgi toplumu hizmetleri kanunu, | Haziran 2002 | Kapsam içi | Önceden var olan ilişki |

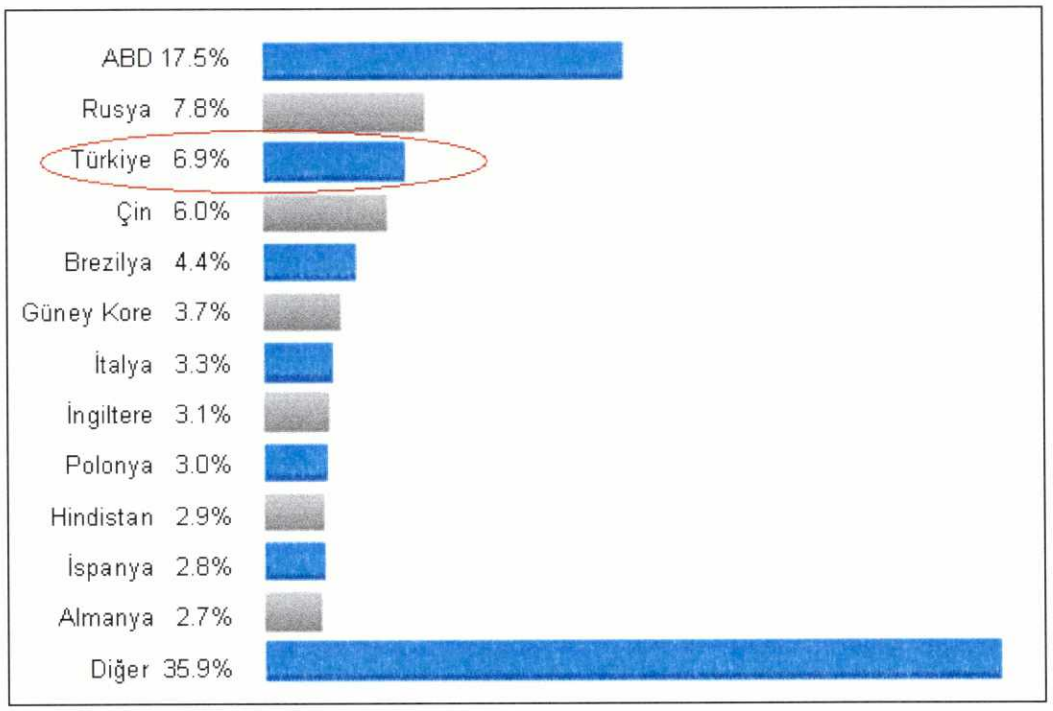
| | | | | |
|---|---|---|---|---|
| | telekomünikasyon kanunu | Kasım 2003 | | |
| İsviçre | Telekomünikasyon Kanunu<br><br>Haksız Rekabete ilişkin Kanun | | Kapsam içi | Önceden var olan ilişki |
| Japonya | Özel e-postaların iletilmesi konusundaki kanun, özel ticari işlemler konusundaki kanun | Temmuz 2002 | Kapsam dışı | |
| Kanada | Mevcut kanun olan elektronik doküman kanunu | Ocak 2001 | Kapsam içi | |
| Kore | Bilgi şebekesi ve korunması kanunu | Temmuz 2001 | Kapsam dışı | |
| Macaristan | Uzaktan satış konusundaki tebliğ | 1999 | Kapsam dışı | |

# 7 TÜRKİYE İNCELEMESİ

Spam e-posta konusu tüm dünyada olduğu gibi ülkemizde de önemli bir sorun haline gelmiştir. Ülkemizde spam ile mücadele konusundaki yasal hükümlerde sorunun geniş çerçevede ve tüm detaylarıyla ele alınmamış olması ve dolayısı ile yetersiz kalması, ülkemizin e-posta ortamını tam bir spam cennetine dönüştürmüş durumdadır. Özellikle son yıllarda en çok spam üreten ülkeler sıralamasında Türkiye en başlarda yer almaktadır. Şekil 7.1 ve Şekil 7.2'de görüldüğü üzere 2007 yılı istatistiklerine göre Türkiye %3.1'lik bir oranla en çok spam üreten dokuzuncu ülke konumundayken, 2008 yılında bu oran %6.9'a çıkmış ve en çok spam üreten üçüncü ülke konumuna gelmiştir. Bir yıl içerisinde ülkemiz kaynaklı spam oranındaki artışının %100'den fazla olduğu görülmektedir. Bu durum ülkemiz adına ciddi bir prestij kaybı oluşturduğu gibi giderek artan bir sorunun varlığını açıkça ortaya koymakta ve gerekli önlemlerin bir an önce alınması konusundaki aciliyeti de gözler önüne sermektedir.




Şekil 7.1 2007 Yılında En Çok Spam Üreten Ülkeler [87]




Şekil 7.2 2008 Yılında En Çok Spam Üreten Ülkeler [88]

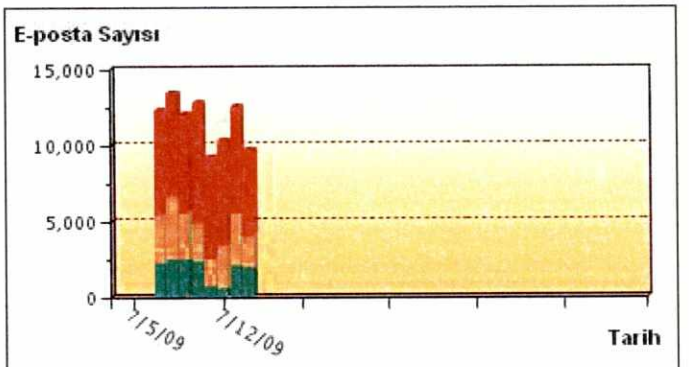
## 7.1 Bilgi Teknolojileri ve İletişim Kurumu (BTK) İncelemesi

BTK, bünyesinde görev yapan personele e-posta hizmetini kendi içerisinde sağlamaktadır. Söz konusu hizmetin verilebilmesi amacıyla e-posta sunucusu barındırmakta ve bu hizmetin yönetimini de yine kendi bünyesinde görevli çalışanları ile yürütmektedir.

Tüm dünyada olduğu gibi spam e-posta sorunu BTK için de mücadele edilmesi ve önlem alınması gereken bir konudur. Bu amaçla, kurumsal bilgi teknolojileri altyapısını spam e-postalar aracılığıyla gelebilecek saldırılara karşı korumak, verilen hizmetin kalitesini ve güvenilirliğini artırmak, görev yapan personelin e-posta kullanımı kapsamında kişisel güvenliğini sağlamak

ve kullanıcıların zamanının spam mesajlar yüzünden boşa gitmesini önlemek adına spam mesajların deşifre edilmesini sağlayan ürünler kullanılmaktadır.

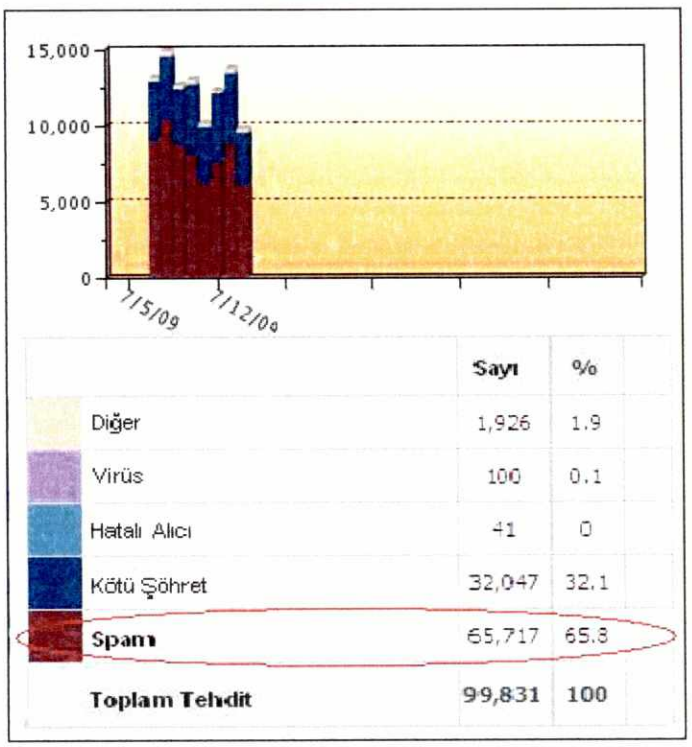
Spam e-posta mesajlarının BTK üzerindeki etkisinin görülebilmesini teminen; Kurum sistemlerinde 07-14 Temmuz 2009 tarihleri arasını kapsayan bir inceleme yapılmıştır. İnceleme neticesinde, sekiz gün sonunda gelen toplam e-posta sayısının 92.172 adet olduğu görülmüştür. Şekil 7.3'de görüldüğü gibi bu e-postaların 76.713 tanesini kapsayan %83.2'lik dilim tehdit içerdiği tespit edilerek engellenmiştir. Engellenen bu e-postalardan %58.3'ünde (53.732 adet) spam, virüs, yanlış alıcı bilgisi gibi nedenlerin sadece bir tanesi tespit edilirken %24.9'unda (22.981 adet) bu tehditlerden en az iki tanesinin bulunduğu görülmüştür.




| | Sayı | % |
|---|---|---|
| Bir Tehdit İçeren E-posta | 53,732 | 58.3 |
| Çoklu Tehdit İçeren E-posta | 22,981 | 24.9 |
| **Tehdit İçeren Toplam E-posta** | **76,713** | **83.2** |
| Temiz E-posta | 15,459 | 16.8 |
| **Toplam E-posta** | **92,172** | **100** |

Şekil 7.3 BTK E-posta İstatistikleri (07-14 Temmuz 2009 Tarihleri Arası)

Şekil 7.4'de belirtildiği gibi engellenen 76.713 adet e-posta mesajında toplam 99.831 adet tehdit ya da sakınca tespit edilmiştir. Söz konusu tehditler içerisinde en fazla oran %65.8 ile (65.717) spam mesajlara aittir. İkinci sırada ise %32.1'lik oranla (32.047) daha önce spam, virüs vb. tehditleri yaydığı tespit edilmiş sakıncalı kaynaklardan gelen e-posta mesajları bulunmaktadır. Virüs ve hatalı kullanıcı adresi nedeniyle engellenen mesaj sayısı ise sadece 141 adet olarak ifade edilmektedir.




| | Sayı | % |
|---|---|---|
| Diğer | 1,926 | 1.9 |
| Virüs | 100 | 0.1 |
| Hatalı Alıcı | 41 | 0 |
| Kötü Şöhret | 32,047 | 32.1 |
| Spam | 65,717 | 65.8 |
| **Toplam Tehdit** | **99,831** | **100** |

Şekil 7.4 BTK E-posta Spam Oranı (07-14 Temmuz 2009 Tarihleri Arası)

Yapılan araştırma sonucunda, kurumsal e-posta adreslerine gelen 92.172 adet mesajın 65.717'sinin spam olduğu tespit edilmiştir. Bu rakamlar üzerinden hesaplandığında BTK'ya gelen toplam e-posta trafiğinin %71.3'ünün spam e-posta olduğu görülmektedir. Sekiz gün sonunda elde edilen toplam rakamların günlük ortalaması alındığında bir günde yaklaşık 8.215 adet spam e-postanın engellendiği görülmektedir. Kurumun 656

çalışanı olduğu göz önüne alındığında ise kişi başına günlük gelen spam e-posta sayısı 12,5'dir.

Kurum, aldığı önlemler neticesinde spam mesajları ve diğer tehdit içeren unsurları (virüs, casus yazılım vb.) kullanıcılarına ulaşmadan e-posta sunucusu üzerinde tespit ederek çalışanlarının her gün spam e-postalar ile boşa zaman harcamasını önlemekte ve bilgi sistemleri alt yapısını bu tür tehditlere karşı korumaktadır.

## 7.2 Mevzuat Durumu

Dünyada birçok ülke gerekli yasal ve teknik önlemleri almasına karşın Türkiye'de spam e-posta konusu yeterli seviyede ele alınmamıştır. Konu İSS ve EPS'ler tarafından bir takım teknik önlemler alınarak çözümlenmeye çalışılmaktadır. Sadece teknik önlemler ile çözüme kavuşturulamayacak olan spam e-postaları önleme konusunda Türk mevzuatı içinde sorunu tüm detaylarıyla ele alan bir düzenleme bulunmamakta, mevcut düzenlemeler ile sorunla mücadele edilmeye çalışılmaktadır. Mevcut yasalar nezdinde ve yürütülen çalışmalar kapsamında konunun incelenmesi aşağıda yapılmaktadır.

### 7.2.1 5809 Sayılı Elektronik Haberleşme Kanunu

10 Kasım 2008 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren Kanun'un 50 nci maddesinde spam konusu da ele alınmıştır. Böylece spam konusu ilk olarak doğrudan bir yasa kapsamında ele alınmıştır. Söz konusu kanunun spam ile ilgili hükmünde *"Abonenin önceden izni alınmadan otomatik arama makineleri, fakslar, elektronik posta, kısa mesaj gibi elektronik haberleşme vasıtalarının kullanılması suretiyle doğrudan pazarlama, siyasi propaganda veya cinsel içerik iletimi gibi maksatlarla istek*

*dışı haberleşme yapılması halinde, abone ve kullanıcılara gelen her bir mesajı bundan sonrası için almayı reddetme hakkı kolay bir yolla ve ücretsiz olarak sağlanır."* denilmektedir.

Kanun'un, spam konusunun ilk olarak bir yasa ile ele alınması açısından son derece önemli olduğu düşünülmekle birlikte birçok açıdan eksik bir düzenleme olduğu görülmektedir. Özellikle, AB'nin 2002/58/EC sayılı direktifinde spam konusundaki düzenlemelerin temelinde kapsam içi (opt-in) yöntemin tercih edilmiş olmasına rağmen Kanun hükümlerinde kapsam dışı (opt-out) yöntem temel alınmıştır. Bu açıdan Kanun'un AB direktifleri ile uyumlu olarak hazırlanmadığı görülmektedir.

Ayrıca;

- Elektronik mesaj göndericisinin kimliğini gizlemesi ya da yanlış adres belirtmesi durumlarının yasaklanarak gönderici kimliğinin açıkça belirtilmesini zorunlu kılan,
- Dolaylı yoldan pazarlama içeren haberleşmeleri yasaklayan,
- Reddedilen göndericinin başka bir gönderici aracılığıyla e-posta göndermeye devam etmesini yasaklayan,
- E-posta adresleri, telefon numaraları gibi iletişim bilgilerini taşıyan kişisel bilgilerin izinsiz toplanmasını ve dağıtılmasını yasaklayan,
- Sahte ürün pazarlamasını ve aldatıcı ya da yanlış bilgiler içeren mesajların gönderilmesini yasaklayan ve
- Ahlaka ve kamu düzenine aykırılık teşkil eden, kişisel ve kurumsal güvenliği tehdit eden mesajların gönderilmesini yasaklayan hususlara ilişkin bir düzenleme yapılmadığı görülmektedir.

Yapılan değerlendirmeler sonucunda Kanun'un spam ile ilgili hükümlerinin AB direktifleri de dikkate alınarak daha geniş bir çerçevede ve tüm detaylarıyla ele alınarak yeniden düzenlenmesi gerektiği sonucuna ulaşılmıştır.

### 7.2.2 Türk Medeni Kanunu

Türk Medeni Kanunu'nun (TMK) 24 üncü maddesinde *"Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır"* denmektedir.

Buna göre ticari içerikli olsun ya da olmasın, kişilik haklarına aykırı kabul edilebilecek bir içerikle gönderilen e-postalarla yukarıda belirtilen hükümler çerçevesinde mücadele etmek mümkündür. Ayrıca İnternet Kurulu (İK)[1], e-posta adreslerinin kişisel bilgi olduğu ve bu bilgilerin izin alınmaksızın ticarete konu edilmesinin kişilik haklarına açık bir saldırı niteliği taşıdığı görüşündedir. Bu görüşten yola çıkılarak kişisel veri niteliği taşıyan e-posta adreslerinin yasal olmayan yollardan elde edilmesinin TMK'nın 24 üncü maddesi kapsamında ele alınabileceği ve kişilik haklarına aykırı bir unsur olarak görülebileceği değerlendirilmektedir [95].

### 7.2.3 Tüketicinin Korunması Kanunu

Tüketicinin Korunması Kanunu'nda (TKK) ticari reklam ve ilanlara ilişkin hükümlerin yer aldığı 16 ncı maddede *"Ticari reklam ve ilanların kanunlara, Reklam Kurulunca belirlenen ilkelere, genel ahlaka, kamu düzenine, kişilik haklarına uygun, dürüst ve doğru olmaları esastır. Tüketiciyi aldatıcı, yanıltıcı veya onun tecrübe ve bilgi noksanlıklarını istismar edici, tüketicinin can ve*

[1] İK: Çeşitli Kamu kurumlarının temsilcileri, özel sektör temsilcileri ve STK temsilcilerinin katılımıyla oluşturulmuştur. Kurul, Bilgi Toplumu oluşumuna katkıda bulunmak üzere, Bilgi ve İletişim Teknolojilerinin sağlıklı gelişmesi ve bu kapsamda Türkiye'de internetin toplumsal faydasının en üst düzeye çıkarılması için temel öneriler oluşturmak amacını taşımaktadır.

*mal güvenliğini tehlikeye düşürücü, şiddet hareketlerini ve suç işlemeyi özendirici, kamu sağlığını bozucu, hastaları, yaşlıları, çocukları ve özürlüleri istismar edici reklam ve ilanlar ve örtülü reklam yapılamaz. Aynı ihtiyaçları karşılayan ya da aynı amaca yönelik rakip mal ve hizmetlerin karşılaştırmalı reklamları yapılabilir. Reklam veren, ticari reklam veya ilânda yer alan somut iddiaları ispatla yükümlüdür. Reklam verenler, reklamcılar ve mecra kuruluşları bu madde hükümlerine uymakla yükümlüdürler.*" denmektedir.

TKK'nın bu maddesinden hareketle e-posta yoluyla doğruluk ve dürüstlük kuralına aykırı olarak yapılan reklam ve pazarlama faaliyetleri hukuka aykırı sayılabilir. Buna göre tüketicilere gelen reklam veya pazarlama içerikli e-postanın bir daha alınmak istenmemesinin belirtilmesine rağmen söz konusu e-posta gönderiminin devam etmesi TKK'nın 16 ncı maddesinde belirtilen doğruluk ve dürüstlük ilkelerinin açık bir ihlali olarak değerlendirilebilmektedir [86].

### 7.2.4 Türk Ceza Kanunu

Türk Ceza Kanunu'nun (TCK) bilişim alanındaki suçları kapsayan,

- 243 üncü maddesinde *"Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir. Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir. Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur"*
- 244 üncü maddesinde *"Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır. Bu fiillerin*

*bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur"*

denilmektedir.

Bilişim sistemlerine zarar verici unsur içeren spam e-postalar ile mücadele TCK'nın yukarıda belirtilen hükümleri doğrultusunda yürütülmektedir. Spam e-posta yoluyla yayılan kötü niyetli yazılımların (virüs, solucan, truva atı vb.) bilişim sistemlerine zarar vermesi nedeniyle bu hükümlerin açıkça ihlal edildiği görülmektedir.

### 7.2.5 Türk Ticaret Kanunu

Türk Ticaret Kanunu (TTK) 56 ncı maddesinde haksız rekabetin tanımı şu şekilde yapılmaktadır: *"Haksız rekabet, aldatıcı hareket veya hüsnüniyet kaidelerine aykırı sair suretlerle iktisadi rekabetin her türlü suistimalidir"*. Yine aynı Kanunun 57, 58, 59, 60, 61, 62 ve 63 üncü maddelerinde ise zarar gören kimselerin hukuki boyutta hakları tanımlanmıştır. TTK'nın devam eden 64 ve 65 inci maddelerde ise haksız rekabette bulunan kimselere verilecek cezai müeyyideler yer almaktadır.

Buna göre reklam amaçlı gönderilen e-postaların özellikle aldatıcı içerikte olması durumunda bu maddelerden yararlanmanın mümkün olabileceği değerlendirilmektedir.

### 7.2.6 5197 Sayılı Kanun

"Gıdaların Üretimi, Tüketimi ve Denetlenmesine Dair Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun"un tüketici haklarının korunmasına ilişkin hükümlerinin yer aldığı 22 nci maddede *"Gıda maddeleri ile ilgili olarak tüketiciler yanıltılamaz ve yanlış yönlendirilemez"* denmektedir.

Bilindiği üzere spam e-postaların zararlı sonuçlarından biri de sahte ürün pazarlama ve satışı olarak karşımıza çıkmaktadır. 5197 sayılı kanunun yukarıda belirtilen hükümlerinden hareketle sahte gıda maddesi pazarlanmasında ya da aldatıcı ifadeler içeren reklam faaliyetlerinde kullanılan spam e-postaların hukuka aykırılık taşıdığı görülmektedir.

### 7.2.7 Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik

Türkiye'de spam konusuyla en yakından ilgili hükmün, BTK tarafından hazırlanan ve Resmi Gazete'nin 6 Şubat 2004 tarihli sayısında yayımlanarak yürürlüğe giren "*Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik*"te bulunduğunu söylemek mümkündür. Söz konusu yönetmeliğin *"İstek Dışı Haberleşme"* başlığını taşıyan 20 nci maddesinde *"İşletmeciler kişi müdahalesi olmadan çalışan fakslar, elektronik posta, kısa mesaj gibi otomatik arama sistemlerini, abonenin önceden izni olmadan siyasi propaganda amacıyla kullanamazlar. Söz konusu otomatik arama sistemlerinin doğrudan pazarlama amacıyla kullanılması halinde kullanıcılara gelen her bir mesajı bundan sonrası için almayı reddetme hakkı ücretsiz ve kolay bir yolla sağlanır. Doğrudan pazarlama amacıyla gönderilen ve kimin adına haberleşme yapıldığı hususunda göndericinin kimliğini saklayan veya alıcının bu iletişimin sonlandırılması konusunda talepte bulunacağı bir adres bulunmayan*

*elektronik mektupların gönderilmesi abonenin bu yöndeki talebi halinde engellenir"* denilerek spam konusu düzenlenmeye çalışılmıştır.

Bu yönetmelik ile e-postalar konusunda iki farklı yaklaşım benimsenmiştir. Siyasi propaganda içeren e-postalar ve doğrudan pazarlama amacı güden e-postalar ayrı ayrı ele alınmıştır. Siyasi propaganda içeren e-postalar için kapsam içi (opt-in) yöntemi benimsenmiştir. Bu yaklaşıma göre siyasi içerikli e-posta gönderebilmek için kişilerin önceden izninin alınması zorunlu hale getirilmiştir. Doğrudan pazarlama amacı güden e-postalar için ise kapsam dışı (opt-out) yöntem benimsenmiştir. Buna göre pazarlama içerikli e-posta gönderimi serbest bırakılmış ancak kullanıcılara bu tarz e-postaları bir daha almayı reddetme hakkı tanınmış ve göndericilere de bu yönde gelen talepleri ücretsiz ve kolay yoldan sağlamaları yükümlülüğü getirilmiştir.

Her ne kadar bu yönetmelik ile ilk olarak spam konusu düzenleme açısından doğrudan ele alınmış olsa da birçok açıdan eksik olduğu değerlendirilmektedir. Buna göre;

- Yönetmeliğin istem dışı haberleşme konusundaki maddesinde belirtilen gerekliliklerin sağlanmaması durumunda ne gibi yaptırımlar uygulanacağı, verilecek cezai müeyyidelerin neler olacağı belirtilmemiş,
- Yönetmelikte belirtilen hükümlere aykırı durumlarda hangi Kurum ya da Kuruluşun gerekli incelemeyi yürüteceğine değinilmemiş,
- E-posta göndericisinin kimliğini gizlemesi ya da yanlış adres belirtmesi durumlarının yasaklanarak gönderici kimliğinin açıkça belirtilmesini zorunlu kılan bir hüküm getirilmemiş,
- Doğrudan pazarlama kapsamında ele alınacak durumlar detaylarıyla açıklanmamış,
- Dolaylı yoldan pazarlama içeren e-postalara bir hüküm getirilmemiş,
- Siyasi içerikli e-postaların gönderilebilmesi için kullanıcıdan alınacak izinin ne şekilde gerçekleştirileceği belirtilmemiş,

- Pazarlama içerikli e-postaların bir daha alınmamak üzere reddedilmesine yer verilirken siyasi içerik taşıyan e-postaların alınmasına ilişkin tüketicinin verdiği izni iptal ederek dağıtım listesinden çıkmak istemesi durumunda ne gibi bir yol takip edileceği açıklanmamış ve
- Sahte ürün pazarlamasının yasaklanmasına ilişkin bir hüküm getirilmemiştir.

Ayrıca söz konusu yönetmelik 5809 sayılı Kanun'un çıkmasının ardından Kanun ile çelişen maddeler ve uygulamalar içermektedir. Bu açıdan, gerek Kanun'un ilgili hükümlerinin gerekse yönetmeliğin AB direktifleri ile uyumlu olacak şekilde yeniden düzenlenmesinin gerektiği değerlendirilmektedir.

## 7.3 Farkındalık Çalışmaları ve Sivil İnisiyatifler

### 7.3.1 İnternet Kurulu

İK, spam ile mücadele konusunda kamuoyunu bilgilendirmek ve yürütülen mücadeleye destek vermek amacıyla 2000 yılının Temmuz ayında bir bildiri yayınlamıştır. Söz konusu bildiride, spam mesajların sakıncalarına değinilmiş ve toplumlar adına giderek artan bir sorun olduğu ifade edilmiştir. Kurul, spam mesajların bir kamu suçu oluşturduğunun düşünüldüğünü ifade etmiş ve spam kaynaklı oluşan sakıncaların en aza indirgenmesi gerektiğine vurgu yapmıştır. Gelişmekte olan internet kültürüne bu konuda bir etik değer kazandırmak için yapılmakta olan ve yapılacak çalışmaların İK tarafından desteklendiği deklare edilmiş ve spam nedeniyle oluşan en temel sakıncalar şu şekilde sıralanmıştır.

- Kişi ve kuruluşların e-posta adresleri, cep telefon numaralarında olduğu gibi kişisel bilgileridir. Bu gibi bilgilerin kişisel izin olmaksızın ticarete konu olması kişilik haklarına açık bir saldırıdır.

- Spam iletileri bireysel İnternet kullanıcıları için en azından ek maliyet anlamına gelmektedir. Oluşan toplam kayıp ise ciddi bir ulusal kaynak israfına işaret etmektedir.
- Spam iletileri yeni gelişmekte olan İSS'lerin kaynaklarını da israf etmekte, kullanıcılarına daha iyi servis vermelerini engellemektedir.
- Spam yasadışı ürün ve servislerin tanıtımı için de kullanılabilmektedir.

Yapılan bildiride internetin oluşturduğu özgür iletişim ortamına zarar vermeden, bu özgürlüklerin kişilere zarar vermesini de engelleyecek yöntemlerin geliştirilmesi gerektiği ifade edilmiş ve bu doğrultuda kısa ve uzun vadede bir takım önlemler alınması önerilmiştir.

Kısa vadede alınması önerilen önlemler,

- Elektronik adres veri tabanı ticaretinin engellenmesi kapsamında yasal sürecin başlatılması ve
- İstek dışı haberleşme eylemlerinin engellenmesi kapsamında İSS'lerin ve kurumsal kullanıcıların teknik işbirliği yapmaları şeklinde açıklanmıştır.

Orta ve uzun vadede alınması önerilen önlemler ise,

- E-posta kullanarak reklam ve bilgilendirme yapmak isteyen kuruluşlara yönelik düzenlemelerin yapılması ve
- Kullanıcı kitlesinin bilinçlendirilmesi ve örgütlenme çalışmalarının yapılması şeklinde açıklanmıştır.

### 7.3.2 Türk Anti-Spam Organizasyonu (TASO)

TASO, 1999 yılında sanal bir çalışma grubu olarak kurulmuş olup Türkiye'de spam ile mücadele etmeyi amaçlamaktadır. Kullanıcıları spam konusunda bilgilendiren ve bilinçlendiren grup aynı zamanda Türkiye'de spam e-postalara karşı alınabilecek teknik çözümlere ilişkin bilgiler vermektedir.

TASO aynı zamanda spam ile mücadele konusunda kendi bünyesinde teknik çözümler üretip bunları kamuoyu ile paylaşmaktadır. Çeşitli kamu kurum ve kuruluşları ile üniversiteler tarafından da desteklenen söz konusu grup çalışmalarını www.spam.org.tr internet adresinden yayınlamaktadır.

# 8 SONUÇ VE ÖNERİLER

Bu bölümde, çalışma kapsamında yapılan tespitler ve değerlendirmeler ile elde edilen sonuçlar alt başlıklarda özet olarak verilmiştir.

## 8.1 Sonuçlar

E-posta hizmeti, kolay kullanım olanağı sunması, hızlı, esnek ve ucuz bir iletişim şekli olması sebebiyle günlük hayatın önemli bir parçası haline gelmiştir. Kullanıcıya sunduğu bu avantajlar sayesinde haberleşme yöntemleri arasında önemli bir unsur olmuş ve geleneksel posta yönteminin yerini almaya başlamıştır.

E-posta hizmeti, iletilerin gönderenden alıcısına ulaşıncaya kadar taşınmasını sağlayan bileşenlerin oluşturduğu bir yapıdır. İnternet üzerinden işleyen bir servis olması ve internetin yaygın kullanım alanı bulmasıyla birlikte e-posta hizmetinin kullanım oranı giderek artmış ve günümüzde en çok tercih edilen iletişim araçlarından biri haline gelmiştir. E-posta hizmetinin tarihi, internetten daha eskiye dayanmasına rağmen internetin ortaya çıkışıyla birlikte standartlaştırma çalışmalarının da ağırlık kazandığı görülmüştür. Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler e-posta hizmetinde farklı ortamların ve ürünlerin ortaya çıkmasını sağlamış ve uygulamalardaki çeşitliliği artırmıştır. Bu ürünlerin birbirleriyle uyum halinde çalışabilmelerini sağlamak ve verilen hizmetin güvenilirliğini artırmak amacıyla e-posta hizmetinin iletişim kurallarını tanımlayan protokoller (SMTP, POP, IMAP) geliştirilmiş, farklı veri türlerinin taşınmasını sağlayan MIME kullanılmaya başlanmış ve standart bir yapının ortaya çıkması hedeflenmiştir. Bu sayede e-posta hizmetini oluşturan bileşenlerin bir bütün içerisinde ve birlikte çalışabilmeleri sağlanmıştır.

İnternet'in ilk hizmetlerinden birisi olmasından dolayı, e-posta hizmetinin ortaya çıkışında, günümüzde şiddetle ihtiyaç duyulan güvenlik ve kimlik denetimi gibi gereklilikler göz önünde bulundurulmamıştır. Bu yüzden, e-posta altyapısı günümüzde İnternet'in en büyük problemlerine yataklık etmekte ve bunların başında da spam mesajlar gelmektedir.

E-posta hizmetinin düşük maliyetli olması ve çok kısa sürede çok geniş kitlelere ulaşım sağlaması spam sorununun ortaya çıkışındaki en önemli nedenleri oluşturmaktadır. Çoğunlukla reklam/pazarlama faaliyetleri için gönderilen spam mesajlar, siyasi ve dini ideolojilerin yayılması, sahte ürün pazarlaması, güvenliğin tehdit edilmesi (virüs, solucan, trojan ve casus yazılımlar vb.) gibi amaçlar taşımaktadır. Gönderilen spam e-postaların verdiği zararlar arasında;

- Gelen e-posta mesajlarının kontrol edilerek ayıklanması için geçen zaman kaybı,
- Yüksek band genişliği ihtiyacı,
- Posta kutusunun dolması sonucunda gerekli e-postaların alınamaması,
- Zaman, para ve itibar kayıplarının oluşması,
- Spam mesajların arasında önemli e-postaların gözden kaçması,
- Sahte ürün satışlarıyla kullanıcıların dolandırılması,
- Terör amaçlı propaganda faaliyetlerinde kullanılması,
- Sistem kaynaklarının gereksiz yere meşgul edilerek hizmet veremez duruma getirilmesi,
- Bilgisayar ve sistem güvenliği için tehdit oluşturması,
- Casus yazılımlar sayesinde kişisel bilgilerin toplanarak yasa dışı olaylarda kullanılması,

sayılabilir. Gerek kişisel gerekse kurumsal güvenliği tehdit eden bu tür mesajlar, maddi anlamda milyarlarca dolarlık zarara neden olurken kullanıcı nezdinde e-posta hizmetine olan güveni de ciddi oranda zedelemektedir.

Bütün bu riskler ve spam sorununun günümüzde ulaştığı boyut göz önüne alındığında önleyici tedbirler almanın bir zorunluluk olarak ortaya çıktığı açıkça görülmektedir. Spam ile mücadele konusunda İSS ve EPS'lerin hizmet verdikleri altyapılarından yayılan spam mesajlara yönelik önlemler almalarının yanında dışarıdan gelebilecek spam tehdidine yönelik de önlemler almaları gerektiği değerlendirilmektedir. Bu amaçla bir takım teknik önlemler geliştirilmiştir. Bunlardan en yaygın kullanılan ve etkili sonuçlar üreten yöntemler;

- Giden e-posta
  - Port 25'in kapatılması
  - SMTP trafik sınırlaması
  - Gönderici kimlik tanımlaması
  - Gönderilen e-posta sayısının sınırlandırılması
- Gelen e-posta
  - Listeleme yöntemleri (Kara, Beyaz ve Gri liste)
  - Kimlik doğrulama yöntemleri (DNS MX sorgulaması, SPF, DKIM)
  - Filtreleme yöntemleri
  - Meydan okuma/cevap verme sistemleri
  - E-posta sayısı eşik değer sınırlaması
  - Balküpü sistemleri
- Diğer
  - Virüs taraması
  - E-posta hizmeti performansının izlenmesi
  - E-posta adres sınamalarının engellenmesi
  - Güvenlik mekanizmalarının kullanımı

şeklinde sıralanmaktadır.

E-postalarda yaşanan spam sorununun her geçen yıl daha büyük boyutlara ulaşması uluslararası kuruluşların da dikkatini çekmiş ve bu konuda önemli çalışmalar yapılmıştır. ITU, OECD ve AB gibi kuruluşlar konunun önemine

dikkat çekmiş ve üye ülkelere sorunun çözümü konusunda gerekli yasal düzenlemeleri gerçekleştirmeleri yönünde tavsiyelerde bulunmuşlardır.

AB'nin 2002/58/EC sayılı Direktifi ile spam ile mücadele hususunda gerekli düzenlemeler ele alınmıştır. Söz konusu direktif ile tüm üye ülkelerin spam sorununu çözüme kavuşturacak yasal tedbirleri almaları zorunlu kılınmıştır.

Gelinen nokta itibariyle AB üye ülkelerinin spam konusunda yasal düzenlemelerini tamamladığı görülmektedir. AB üyesi ülkeler de dahil olmak üzere spam ile ilgili yasal düzenleme yapan ülkelerin çoğunun kapsam içi (opt-in) yöntemi tercih ettikleri görülmektedir. Buna rağmen aralarında ABD'nin de bulunduğu az sayıda ülke kapsam dışı (opt-out) yöntemi uygulamaktadır. Her iki yöntem karşılaştırıldığında kapsam içi yöntemi temel alan yaklaşımın, e-posta göndermeden önce alıcının iznini gerektirmesi nedeniyle soruna daha etkili bir çözüm getirdiği düşünülmektedir. Nitekim, ABD'de kapsam dışı tabanlı spam yasasının çıkarılmasına karşın en çok spam üreten ülkelerin başında geldiği görülmektedir. Kapsam dışı yönteminde izin olmaksızın e-posta gönderebilme esnekliği spam mesaj gönderimini ilk etapta serbest bırakmaktadır. Kullanıcı kendisine gelen ilk mesajdan sonra tekrar almak istemediğini belirterek ancak sorundan kurtulabilmektedir. Spam e-posta oranının ulaştığı boyut göz önüne alındığında kullanıcıların gelen her bir mesaja cevap vermesi oldukça zahmetli ve kullanıcıyı zorlayıcı bir eylem olarak değerlendirilmektedir.

Ülkemizde ise spam konusundaki doğrudan ya da dolaylı olarak ilişkili yasa maddeleri sorunu geniş bir çerçeveyle ve tüm detaylarıyla ele almadığı gibi spam konusuyla doğrudan ilişkili yasa maddesi de AB direktifleri ile uyumlu olarak oluşturulmamıştır. Yasal düzenlemelerin oldukça yetersiz kalması ve İSS/EPS'ler tarafından alınan teknik tedbirlerin konuya etkili bir çözüm getirememiş olması ülkemizin spam üreten ülkeler sıralamasında en üst basamaklarda yer almasına neden olmaktadır. Bu açıdan, spam ile mücadele konusundaki yasal düzenlemelerin bir an önce detaylı bir şekilde yeniden

düzenlenmesi ve alınan teknik tedbirlerin artırılması gerektiği düşünülmektedir.

## 8.2 Öneriler

E-posta hizmetinin geleceğini tehdit eden ve güvenilirliği konusunda kuşkular oluşturan spam sorununun geldiği nokta itibariyle gerekli teknik ve yasal önlemlerin alınması kaçınılmaz hale gelmiştir. Bu kapsamda, son kullanıcıların, İSS ve EPS'lerin ve düzenleyici kurumların üzerine düşen görev ve sorumluluk çerçevesinde gerekli önlemleri almaları gerekmektedir.

Servis sağlayıcılar, kullanıcılarına güvenli bir iletişim olanağı sunmakla yükümlüdür. Bu amaçla, İSS ve EPS'lerin tüketicilerine verdiği hizmet kalitesini artırmak ve tüketicinin güven duygusunu pekiştirmek adına spam ile mücadele kapsamında, mevcut teknik yöntemleri değerlendirerek *organizasyon ve sistem altyapısına en uygun çözümleri* uygulaması gerekmektedir. İSS'ler baz alındığında özellikle port 25 kullanımının dinamik IP'li kullanıcılar için yasaklanmasının ve bunun yerine daha güvenli olan 465 veya 587 nci portların kullanılmasının, spam e-postaların çoğunun dinamik IP kullanan zombi bilgisayarlar aracılığıyla üretildiği düşünüldüğünde faydalı olacağı değerlendirilmektedir. EPS'ler açısından bakıldığında ise Gönderici Kimlik Tanımlaması yönteminin kullanılmasının elzem olduğu değerlendirilmektedir. Ayrıca e-posta hizmetini güvenli iletişim protokolleri (TLS, SSL) üzerinden gerçekleştirmelerinin ve veri şifreleme metotlarını (S/MIME, PGP) kullanmalarının faydalı olacağı düşünülmektedir. Alınan tedbirler ve sonuçları raporlanmalı, teknolojik gelişmeler yakından takip edilmeli ve belli peryotlarla tedbirler gözden geçirilerek iyileştirme çalışmaları yapılmalıdır.

İSS ve EPS'lerin, kullanıcıları ile yaptıkları abonelik sözleşmelerinde e-posta ile spam gönderemeyeceklerine dair taahhüte yer vermeleri, aksi takdirde

zararı kullanıcıların kendilerinin gidermek zorunda kalacakları maddesinin yer alması gerektiği değerlendirilmektedir. Böylece kullanıcıların spam sorunu konusunda daha güncel kalmaları ve farkındalıklarının artırılması sağlanmış olacaktır.

Bireysel kullanıcıların, anti virüs yazılımları ve spam filtreleme programları kullanmaları, e-posta adreslerini güvenilir olduğundan emin olmadıkları kişi ya da internet siteleri ile paylaşmamaları, e-posta kullanımında mutlaka kolay tahmin edilemeyecek parola kullanmaları ve bu parolaları sık sık güncellemeleri, şüpheli gördükleri e-postaları açmamaları, sistem ve ağlarındaki diğer kullanıcılara karşı sorumlu olduklarının bilincinde olmaları gereklidir. Ayrıca, spam olarak tespit ettikleri e-posta iletilerine ilişkin bilgileri servis sağlayıcıları ile paylaşmalarının kullanıcıların spam ile mücadelede alması gerekli önlemler olduğu değerlendirilmektedir. Kullanıcıların, bu önlemler ışığında hareket etmeyi alışkanlık haline getirmeleri sayesinde e-posta kullanım kültürünün yerleşeceği düşünülmektedir.

Spam sorununun geldiği boyut değerlendirildiğinde, önlem alınmadığı takdirde kişilerin en temel haklarından biri olan haberleşme özgürlüğünü kısıtlayacak seviyelere çıkabileceği değerlendirilmektedir. Bu açıdan BTK, spam ile mücadele konusundaki mevcut yasal düzenlemelerin, konunun tüm detaylarıyla ele alınacak şekilde, güncellenmesi için çalışmalara bir an önce başlamalıdır. Bu kapsamda, spam mesajlara ilişkin düzenlemenin gerekliliği hükümet temsilcileri ile yapılacak çalışmalar nezdinde ifade edilmeli ve 5809 sayılı Elektronik Haberleşme Kanunu'ndaki spam mesajları yasaklayan maddelerin AB direktifleri ile uyumlu olacak şekilde yeniden düzenlenmesi hususunda görüş bildirilmelidir. Kurum, yasal mevzuatın hazırlanması aşamasında ilgili kamu kurumları, özel sektör temsilcileri ve STK'lar ile görüş alışverişinde bulunmalı ve tüm aktörlerin sürece dahil edilmesi sağlanmalıdır. Oluşturulacak yasal düzenlemeyle sorumluluklar ve yaptırımlar açık olarak belirlenmeli ve cezalar caydırıcı nitelikte olmalıdır. Yasal düzenlemelerin temelinde bir ürün ya da servise ilişkin her türlü reklam, dolaylı ya da direk

pazarlama amacı güden e-postalar ile gönderici ve alıcı arasında önceden herhangi bir ilişki bulunmadığı durumlarda gönderilen çoklu e-postalar alınmalı ve kapsam içi yöntem tercih edilerek alıcının izninin alınması e-posta gönderiminde ön şart olarak getirilmelidir. Ayrıca yasa kapsamı dışında tutulacak istinai durumların da açıkça belirlenmesi gerekmektedir. Örneğin, acil durumlarda (doğal afetler, güvenlik tehdidi oluşturan durumlar vb.) kamu kurum ve kuruluşlarının görev ve sorumlulukları çerçevesinde mesaj göndermesi tamamıyla kapsam dışında tutularak toplu e-posta gönderimi serbest bırakılmalıdır. Gönderici ile alıcı arasında önceden var olan ticari ilişkilerde ve bir ürün ya da servis hakkında tüketicilerin sağlığını tehdit edici bir unsur oluşması gibi durumlarda önceden izin alınması zorunlu tutulmamalı, bu kapsamda yer alan durumlar için kapsam dışı yöntem uygulanmalıdır. Yine, Kamu yararına faaliyet gösteren organizasyonların, faaliyet alanları ile ilgili olmak şartıyla gönderecekleri e-postalar için kapsam dışı yöntem uygulanmalıdır. Ancak, bu tür e-postaların gönderilebileceği e-posta adresleri önceden belirlenerek ilgili taraflarca Kuruma bildirilmiş olmalı ve bu adresler dışındaki herhangi bir adresin kullanımı yasaklanmalıdır.

Mesaj göndericilerinin hatalı ya da yanlış e-posta adresi kullanmaları, aldatıcı ya da yanlış bilgiler içeren konu başlığı ve mesaj içeriği kullanmaları önlenmeli ve yasa kapsamında bulunan her türlü e-postanın içeriğinde mesajı gönderenin açık bir şekilde belirtilmesi zorunlu kılınmalıdır. Ahlaka ve kamu düzenine aykırılık teşkil eden, kişisel ve kurumsal güvenliğe zarar veren kötü niyetli yazılımları (virüs, solucan, Truva atı, casus yazılımlar vb.) içeren e-postaların gönderilmesi yasaklanmalıdır. Yasa kapsamında bulunan her türlü e-postanın içeriğinde mesajı gönderenin açık bir şekilde belirtilmesi ve alıcının mesajı tekrar almak istememesi durumunda ücretsiz ve kolay bir yolla reddedebilme imkanının tanınması zorunlu kılınmalıdır.

E-posta adresleri kişisel veri kapsamında değerlendirilmeli, izinsiz e-posta adresi toplanması, kullanılması, paylaşılması ve satılması yasaklanmalıdır.

Oluşturulacak yasa, sadece e-posta hizmetiyle sınırlandırılmamalı, bunun yanında spam sorunun görüldüğü SMS, MMS, telefon ve faks hizmetlerini de kapsamalıdır.

Kurum tarafından oluşturulacak ikincil düzenlemeler ile, alıcının talebi üzerine listeden çıkarma işleminin talepten sonra en geç kaç gün içinde yapılması gerektiği, kapsam içi yönteminin temelinde yatan ön izin alınması işleminin ne şekilde yapılacağı, tüketicilerden gelen şikayetlerin hangi süreçler dahilinde değerlendirileceği gibi detay konular açık ve net bir biçimde tanımlamalıdır. Aynı zamanda, İSS ve EPS'lerin spam ile mücadele kapsamında gerekli teknik tedbirleri almaları hususunda yükümlü oldukları hükmüne yer verilmesinin gerektiği değerlendirilmektedir.

Kurum tarafından, yasadan kısmen ya da tamamen muaf tutulan koşulları sağlayan *(izinli)* e-posta adreslerini içeren Beyaz Liste ve spam gönderdiği tespit edilen *(yasaklı)* e-posta adreslerini içeren Kara Liste oluşturulmalıdır. Beyaz ve kara listelerin oluşturulması ve İSS/EPS'ler ile paylaşılması için gerekli sistem Kurum tarafından kurulmalı ya da kurdurulmalıdır.

Kurum bünyesinde bulunan Çağrı Merkezi spam e-postalar konusunda gelecek ihbarların alınabileceği şekilde yeniden yapılandırılmalı ve tüketicilerden gelen ihbar ve talepler incelenmek üzere kayıt altına alınmalıdır.

Kamuoyunu bilgilendirici ve bilinçlendirici bilgiler içeren bir internet sayfası hazırlanmalı ve güncel bilgiler buradan kamuoyu ile paylaşılmalıdır. Kullanıcıların spam konusunda bilinçlerini artırıcı ve eğitici nitelikte kampanyalar düzenlenmeli ve spam ile mücadele kapsamında faaliyet gösteren STK'lar ile organizasyonlar desteklenmeli ve işbirliği yapılmalıdır.

Kurum önderliğinde konuyla ilgili kamu, özel sektör ve STK'ların katılımıyla bir çalışma grubu oluşturulmalıdır. Bu çalışma grubu belirli aralıklarla

toplanarak dünyada ve Türkiye'de yaşanan gelişmeleri değerlendirmeli ve ileriye dönük stratejiler belirlemelidir. Kurum tarafından, çalışma grubunun yaptığı değerlendirmeleri kamuoyu ile paylaşmak ve görüş alışverişinde bulunmak amacıyla forumlar düzenlenmelidir.

Spam sorunu ile mücadelede uluslararası işbirliğinin önemli olması nedeniyle Kurumun bu konuda yapılan çalışmaları takip ederek aktif katılım sağlaması gereklidir. Diğer ülkelerin konuyla ilgili kuruluşları ile görüş alışverişinde bulunulmalı ve işbirliği anlaşmaları hayata geçirilmelidir.

İnternetin doğasında bulunan küresellik, spam e-postalar ile mücadelenin tüm dünyada topyekün sürdürülmesini zorunlu kılmaktadır. Yasal düzenlemelerini tamamlamış ülkelerin mevzuatlarının farklılık göstermesi ve halen düzenleme yapmamış ve spam mesajları suç saymamış ülkelerin mevcut olması spam ile mücadelede dünya genelinde etkin sonuçlar alınmasına engel teşkil etmektedir. Bu açıdan, soruna yapısal bir çözüm bulmanın, ancak uluslararası alanda kabul görecek bir yasal düzenlemenin varlığı ile mümkün olabileceği düşünülmektedir. Bu nedenle ITU'nun girişimiyle uluslararası kuruluşların bir araya gelerek spam sorununa yasal çözüm getirecek bir düzenleme üzerinde uzlaşmaları ve bu düzenlemenin üye ülkeler nezdinde yürürlüğe girmesinin zorunlu tutulmasının sorunun üstesinden gelmede hayati bir unsur olacağı değerlendirilmektedir.

## KAYNAKLAR


**[1]** Baker, G., Bowen, T., 2003, First Byte: Using Information and Communication Technology, Oxford University Press, 5th Ed., s. 127, İngiltere

**[2]** Van Vleck, T., 2001, The history of electronic mail, http://www.multicians.org/thvv/mail-history.html, 09.12.2008

**[3]** Chisnall, D., Electronic Messaging, http://hocc.swan.ac.uk/?q=node/91, 13.12.2008

**[4]** Tomlinson, R., The first network email, http://www.bbn.com/resources/pdf/firstemail04.01.05.pdf, 17.12.2008

**[5]** Dent, K., 2004, Postfix: The Definitive Guide, O'Reilly Media, s. 12, 14

**[6]** Resnick, P., Nisan 2001, Internet Message Format (RFC 2822), http://www.tools.ietf.org/html/rfc2822, 02.01.2009

**[7]** Tracy, M., Jansen, W., Scarfone, K., Butterfield, J., Şubat 2007, Guidelines on Electronic Mail Security, National Institute of Standards and Technology - U .S. Department of Commerce, s. 18 – 24

**[8]** Crocker, D., Mayıs 2004, Internet Mail Architecture, s. 10-13, 30 http://tools.ietf.org/html/draft-crocker-email-arch-12, 23.12.2008

**[9]** Collings, T., Wall, K., 2005, Red Hat Linux Networking and System Administration, Wiley Publishing, 3rd Ed., s. 468 - 469

**[10]** Blum, R., 2002, Open Source E-mail Security, Sams Publishing, s. 11 - 12

**[11]** How e-mail Works, http://en.kioskea.net/contents/courrier-electronique/fonctionnement-mta-mua.php3, 23.12.2008

**[12]** How email really works, https://support.kavi.com/khelp/kmlm/user_help/html/how_email_works.html, 20.12.2008

**[13]** 5809 sayılı Elektronik Haberleşme Kanunu, http://rega.basbakanlik.gov.tr/main.aspx?home=http://rega.basbakanlik.gov.tr/eskiler/2008/11/20081110m1.htm&main=http://rega.basbakanlik.gov.tr/eskiler/2008/11/20081110m1.htm, 16.07.2009

**[14]** http://en.wikipedia.org/wiki/MX_record, 12.01.2008

**[15]** Kozierok, C., 2005, The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference, No Starch Press, s. 1281, 1282, 1283

**[16]** Zurawski, R., 2004, The Industrial Information Technology Handbook, CRC Press, s. 29-2, 29-3, 29-4, 29-8, 29-9, 29-10

**[17]** Comer, D., 2006, Internetworking With TCP/IP: Principles, Protocols, and Architecture, Prentice Hall, s. 476, 477, 478

**[18]** Ogletree, T. W., Mueller, S., 2003, Upgrading and Repairing Networks, QUE Publishing, 4th Ed., s. 439, 440, 441

**[19]** Comer, D., 2008, Computer Networks and Internets, Prentice Hall, s. 650

**[20]** Okin, J. R., 2005, The Internet Revolution: The Not-For-Dummies Guide to the History, Technology and Use of the Internet, Ironbound Press, s. 235, 236, 237

**[21]** Spam nedir?, http://www.spam.org.tr/nedir.html, 06.01.2009

**[22]** OECD, 2006, OECD Anti-Spam Toolkit of Recommended Policies and Measures, s. 21 – 25, 61 – 63, http://books.google.com.tr/books?id=E0RqRQ-RnQ8C&dq=OECD+Anti-Spam+Toolkit+of+Recommended+Policies+and+Measures&printsec=frontcover&source=bl&ots=1RnTVcnFoW&sig=sWYT0b4YYwaC3Z5r2_Bg1vI0Htk&hl=tr&ei=W1dnSv6DKZ2CmwOGppTGDQ&sa=X&oi=book_result&ct=result&resnum=5, 16.07.2009

**[23]** Zdziarski, J., 2005, Ending Spam: Bayesian Content Filtering and The Art of Statistical Language Calssification, No Starch Press, s. 4 – 23, 29, 30, 31, 32, 33

**[24]** Templeton, B., Reflections on the 25th anniversary of spam, http://www.templetons.com/brad/spam/spam25.html, 23.12.2008

**[25]** Templeton, B., Origin of the term "spam" to mean net abuse, http://www.templetons.com/brad/spamterm.html, 23.12.2008

**[26]** ITU, 2004, ITU WSIS thematic meeting – countering spam, s. 14, 56

**[27]** Alataş, Ş., SMTP sorununa yeni bir yaklaşım: Sistemin yeniden inşası, http://ab.org.tr/ab06/bildiri/120.doc, 27.12.2008

**[28]** Symantec, State of spam – a monthly report (Report #29), http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_05-2009.en-us.pdf, 15.04.2009

**[29]** Cisco, Cisco 2008 – Annual security report, http://cisco.com/en/US/prod/collateral/vpndevc/securityreview12-2.pdf, 16.07.2009

**[30]** Symantec, State of spam – a monthly report (February 2009), http://www.datamanager.it/systemFiles/files/SpamReport_Feb09.pdf, 23.03.2009

**[31]** Schryen, G., 2007, Anti-Spam Measures: Analysis and Design, Springer Science+Business Media, s. 13, 16, 62, 63, 64, 66, 67, 72

**[32]** Krause, M., Tipton, H., 2007, Information Security Management Handbook, CRC Press, 6th Ed., s. 2883

**[33]** McDonald, A., 2004, SpamAssassin: A Practical Guide to Integration and Configuration, Packt Publishing Ltd., s 7,8

**[34]** MAAWG, Managing port 25 for residential or dynamic IP space benefits of adoption and risks of inaction, http://www.maawg.org/port25/MAAWG_Port25rec0511.pdf, 25.12.2008

**[35]** Slettnes, T., Bugüner, N.B., Kasım 2005, Eposta Alıcısında (MX'te) Spam Engelleme, s. 18, 20, http://pdf.belgeler.org/howto/spam-filtering.pdf, 16.07.2009

**[36]** Myers, J., Mart 1999, SMTP Server Extension for Authentication (RFC 2554), http://www.tools.ietf.org/html/rfc2554, 16.07.2009

**[37]** Cook, D., Hartnett, J., Manderson, K., Scanlan, J., Kasım 2005, Catching Spam before it arrives: Domain specific dynamic blacklist, School of Computing University of Tasmania, Avustralya, s. 2,3, http://crpit.com/confpapers/CRPITV54Cook.pdf, 16.07.2009

**[38]** Goodman, J., Kasım 2003, Spam: Technologies and Policies, s. 3,4, http://research.microsoft.com/en-us/um/people/joshuago/spamtech.pdf 16.07.2009

**[39]** Puniskis, D., Lauritis, R., 2008, Artificial intelligence for greylisting anti-spam, Kaunas University of Technology, Litvanya, http://www.ee.ktu.lt/journal/2008/5/12_ISSN_1392-1215_Artificial%20Intelligence%20for%20Greylisting%20Anti-Spam.pdf, 16.07.2009

**[40]** Levine, J.R., Experiences with greylisting, Trumansburg-New York, USA, http://www.taugh.com/greylist.pdf, 17.06.2009

**[41]** Wiehes, A., 2005, Comparing anti spam methods, Yüksek lisans tezi, Gjøvik University College, Norveç, http://hig.no/content/download/3316/70510/file/Wiehes%20-%20Comparing%20anti%20spam%20methods.pdf, 16.07.2009

**[42]** Lim Aik Yong Amanda, Lim Lay Yee, Ong Hui Ying Cheryl, Authentication: users & systems, National University of Singapur

**[43]** Wiehe, A., Hjelmas, E., Wolthusen, D., 2006, Quantitative analysis of effcient antispam techniques, Bilgi Güvenliği Çalıştayı, ABD Askeri Akademisi

**[44]** Leiba, B., Fenton, J., Haziran 2006, DKIM: Using digital signatures for domain verification, IBM Araştırma Raporu, http://www.ceas.cc/2007/papers/paper-78.pdf, 16.07.2009

**[45]** Schwartz, A., 2004, SpamAssassin, O'Relly Press, 3rd Ed.

**[46]** Zelkowitz, M., 2008, Advances in Computers: Software Development, Academic Pres, s. 62

**[47]** Wyatt, A., 2006, Cleaning Windows Vista For Dummies, Wiley Publishing, s. 125,126

**[48]** Cormack, G., 2008, Email Spam Filtering: A Systematic Review, Now Publishers Inc., s. 33

**[49]** Altunyaprak, C., 2006, Bayes Yöntemi Kullanarak İstenmeyen Elektronik Postaların Filtrelenmesi, Yüksek Lisans Tezi, Muğla Üniversitesi, s. 24, Muğla

**[50]** Sullivan, D., 2005, The Definitive Guide to Controlling Malware, Spyware, Phishing and Spam, Realtimepublisher.com, s. 160, 161, 162

**[51]** Willard, W., 2006, HTML: A Beginner's Guide, McGraw-Hill Professional, 3rd Ed., s. 114, 115

**[52]** http://belgeler.magmalinux.org/ssl/ssl002.html, 22.02.2009

**[53]** Russel, R., Walshaw, R.,Krause, 2001, Hack Proofing Your E-Commerce Site, Elsevier, s. 355, 356

**[54]** TÜBİTAK UEKAE, Açık anahtar altyapısı eğitim kitabı - SSL/TLS, http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/teknik/aaa/index.html?ssltls.html, 22.02.2009

**[55]** Chapman, B., Cooper, S., Zwicky, E., 2000, Building Internet Firewalls, O'Reilly, 2nd Ed., s. 368, 369

**[56]** Çağlayan, M. U., Levi, A., Elektronik posta güvenliği için PGP kullanımı, Boğaziçi Üniversitesi, İstanbul, http://people.sabanciuniv.edu/levi/as97.htm, 16.07.2009

**[57]** Çağlayan, M. U., Kurtuldu, N., Levi, A., Elektronik posta güvenliği ve açık anahtar sunucuları, Boğaziçi Üniversitesi, İstanbul, http://people.sabanciuniv.edu/levi/blsm97.pdf, 16.07.2009

**[58]** Levi, A., Nasıl bir e-posta güvenliği, Sabancı Üniversitesi, İstanbul, http://people.sabanciuniv.edu/levi/bilisimguvenlik1.pdf, 16.07.2009

**[59]** TÜBİTAK UEKAE, Açık anahtar altyapısı eğitim kitabı – S/MIME, http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/teknik/aaa/index.html?5.html, 25.02.2009

**[60]** OECD, OECD urges governments and industry to do more to tackle spam, http://www.oecd.org/document/62/0,2340,en_2649_201185_36488702_1_1_1_1,00.html, 27.02.2009

**[61]** OECD, OECD launches anti-spam toolkit and invites public contributions, http://www.oecd.org/document/50/0,3343,en_2649_201185_33732274_1_1_1_1,00.html, 27.02.2009

**[62]** OECD, OECD task force to coordinate fight against spam, http://www.oecd.org/document/7/0,2340,en_2649_22555297_33656711_1_1_1_1,00.html, 27.02.2009

**[63]** OECD, OECD calls on governments to step up their fight against spam, http://www.oecd.org/document/37/0,2340,en_2649_34487_25676581_1_1_1_1,00.html, 27.02.2009

**[64]** OECD, OECD launches anti-spam toolkit and invites public contributions, http://www.oecd.org/document/50/0,3343,en_2649_34487_33732274_1_1_1_1,00.html, 27.02.2009

**[65]** OECD, OECD launches fight against spam with Brussels workshop, http://www.oecd.org/document/38/0,3343,en_2649_34487_26198225_1_1_1_1,00.html, 27.02.2009

**[66]** OECD, Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, http://www.oecd.org/dataoecd/43/28/38770483.pdf

**[67]** ITU, ITU activities on counterin spam, http://www.itu.int/osg/spu/spam/, 13.02.2009

**[68]** ITU, http://www.itu.int/wsis/index.html, 13.02.2009

**[69]** ITU, 2003, WSIS – Cenevre İlkeler Bildirgesi, http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf, 16.07.2009

**[70]** ITU, 2003, WSIS – Cenevre Eylem Planı, http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-E.pdf, 16.07.2009

**[71]** ITU, 2005, WSIS – Tunus Agenda For The Informaiton Society, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html, 16.07.2009

**[72]** ITU, 2004, WSIS Thematic Meeting on Countering Spam, http://www.itu.int/osg/spu/spam/background.html, 15.02.2009

**[73]** World Telecommunication Standardization Assembly (WTSA-08), http://www.itu.int/ITU-T/wtsa-08/, 15.02.2009

**[74]** ITU, 2008, WTSA – Resolution 52, http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf, 16.07.2009

**[75]** EU, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, http://www.dataprotection.ie/documents/legal/directive2002_58.pdf

**[76]** http://www.consilium.europa.eu/pressData/en/trans/79353.pdf, 02.02.2009

**[77]** http://www.eu2004.nl/default.asp?CMS_TCP=tcpAsset&id=B44C0E30C17A46DA81E62332EA6C2B7AX1X51359X3, 02.02.2009

**[78]** THE LONDON ACTION PLAN On International Spam Enforcement Cooperation, http://www.londonactionplan.com/, 16.07.2009

**[79]** OECD, 2005, Anti-Spam Regulation, http://www.oecd.org/dataoecd/29/12/35670414.pdf, 21.07.2009

**[80]** ACA, Spam Act 2003: A practical guide for business, http://www.acma.gov.au/webwr/consumer_info/frequently_asked_questions/spam_business_practical_guide.pdf, 16.07.2009

**[81]** Relf, P., 2005, A look at Australia's anti-spam legislation, http://www.law.mq.edu.au/html/MqJBL/vol2/vol2_4.pdf, 16.07.2009

**[82]** Main features of the spam act, http://www.dbcde.gov.au/__data/assets/pdf_file/0015/34431/Main_Features_of_the_spam_act.pdf, 16.02.2009

**[83]** ACMA, How ACMA is fighting spam, http://www.acma.gov.au/WEB/STANDARD/pc=PC_310308, 16.02.2009

**[84]** ACMA, International Cooperation, http://www.acma.gov.au/WEB/STANDARD/pc=PC_310313, 16.02.2009

**[85]** Sorkin, D. E., Spam legislation in the United States, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1061301, 16.07.2009

**[86]** Başar, M. S., İkizler, M., Spam'in zararları ve spam ile hukuki mücadele: ABD örneği ve Türk ve Avrupa Birliği hukukları karşılaştırılması, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 8, Sayı: 2, 2006, s.91-114, http://web.deu.edu.tr/hukuk/dergiler/DergiMiz8-2/pdf/mikizler.pdf, 16.07.2009

**[87]** Sophos, 2008, Security threat report: 2008, https://secure.sophos.com/sophos/docs/eng/marketing_material/sophos-security-report-08.pdf, 16.07.2009

**[88]** Sophos, 2009, Security threat report: 2009, http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf, 16.07.2009

**[89]** http://www.ftc.gov/bcp/conline/edcams/spam/rules.htm, 17.02.2009

**[90]** ITU News, Haziran 2004, Spam: A Threat to the Information Society, s.5, http://www.itu.int/osg/spu/spam/, 16.07.2009

**[91]** Spam mail'e ABD'de 2 yıl 3 ay hapis cezası,

http://www.turkhukuksitesi.com/showthread.php?t=21502, 03.03.2009

**[92]** ABD'de spam'e milyar dolarlık ceza, http://arsiv.ntvmsnbc.com/news/301662.asp, 03.03.2009

**[93]** ITU, ITU survey on anti-spam legislation worldwide, http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf, 22.02.2009

**[94]** Çelebioğlu, D., Şubat 2005, Türkiye'de Bilgi ve İletişim Teknolojilerinde Bilgi Güvenliği, Uzmanlık Tezi, Ankara

**[95]** Memiş, T., Hukuki açıdan kitlelere e-posta gönderilmesi, http://www.hukukcu.com/bilimsel/kitaplar/spamming.htm, 16.07.2009

# ÖZGEÇMİŞ

1978 yılında Tokat'ın Niksar ilçesinde doğdu. İlkokulu Niksar'da, ortaokulu Tokat'ta ve liseyi İstanbul'da bitirdi. 2003 yılında Dokuz Eylül Üniversitesi Bilgisayar Mühendisliği Bölümü'nden mezun oldu. Evlidir. 2006 yılından bu yana Bilgi Teknolojileri ve İletişim Kurumu, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı'nda Bilişim Uzman Yardımcısı olarak görev yapmaktadır.