

## **Desarrollo de un sistema de gestión de disponibilidad que respete la ley como medida contra el spam sobre telefonía IP [1]**

*Fuente:*

[http://www.madrid.org/comun/datospersonales/0,3126,457237\\_458340\\_127535941\\_12489900\\_12489303,00.html](http://www.madrid.org/comun/datospersonales/0,3126,457237_458340_127535941_12489900_12489303,00.html)

Este documento explica por qué el SPIT (Spam sobre telefonía IP) es más difícil de filtrar que el spam convencional mediante correos electrónicos, indica panoramas y posibles medidas para evitarlo y presenta un prototipo para un sistema de gestión de disponibilidad para filtrar SPIT que se está desarrollando actualmente en el proyecto SPIT-AL.

**Markus Hansen, Marit Hansen, Jan Möller, Thomas Rohwer, Carsten Tolkmit, Henning Waack. Independent Centre for Data Protection (Schleswig-Holstein, Alemania).**

**Markus Hansen, Marit Hansen, Jan Möller[2],  
Thomas Rohwer, Carsten Tolkmit[3],  
Henning Waack[4]**

### ***Palabras clave:***

Spam, spot, spam sobre telefonía IP, telefonía IP, VoIP, voz sobre IP, privacidad, gestión de disponibilidad.

### **1. Introducción**

La telefonía IP se ha desarrollado hasta un nivel que permite una utilización de la tecnología VoIP con reducción de costes [Ref. Ref. 1], cumple las necesidades profesionales y no requiere un conocimiento técnico avanzado.

Se puede suponer de forma razonable que VoIP causará los mismos efectos en la telefonía que el correo electrónico produjo en la comunicación escrita. Uno de estos efectos será el de las llamadas publicitarias no solicitadas o SPIT (Spam sobre telefonía IP) [Ref. 11] [Ref. 13]. Las llamadas de SPIT pueden tener su origen tanto en humanos (ej: centros de llamadas) como en dispositivos automáticos y la legislación que prohíbe dichas llamadas es con gran frecuencia ineficaz contra las llamadas procedentes de otros países [Ref. 4]. Por lo tanto, al igual que con el correo electrónico, existirá una demanda creciente de aplicaciones para filtrar el SPIT.

El correo electrónico, como comunicación asíncrona, permite la aplicación de diversos mecanismos de filtrado al contenido completo de la comunicación antes de que ésta se presente al usuario (o se marque como SPAM o incluso se borre). Por el contrario, la telefonía es una comunicación síncrona y, por lo tanto, no proporciona mucha información antes de la transmisión del contenido, lo que la hace más difícil de filtrar y más molesta para los usuarios.

Como las telecomunicaciones (al menos en Alemania) están protegidas por diversas leyes, los ejemplos de filtrado de correos o de llamadas se enfrentan a diversas consecuencias jurídicas (por ejemplo, ingreso en prisión). Por lo tanto, resulta obligatorio no sólo elaborar mecanismos de filtrado técnico, sino también considerar las implicaciones de las normativas y las leyes de protección de la privacidad o de las telecomunicaciones [Ref. 2].

Este artículo se basa principalmente en un borrador sobre filtrado de SPIT [Ref. 12] que se ha elaborado en el proyecto SPIT-AL, cuyo objetivo es desarrollar un filtro de SPIT con código abierto que sea efectivo y que respete la ley y la privacidad. El enfoque incluye aspectos de sistemas de reputación [Ref. 8] que se aplican a un sistema de gestión de disponibilidad [Ref. 7]. El proyecto SPIT-AL está patrocinado por el Fondo Europeo de Desarrollo Regional dentro

del programa "e-Region PLUS" de Schleswig-Holstein y por fondos del Land (Estado Federal) Schleswig-Holstein.

## **2. Situaciones en las que se produce SPIT y posibles medidas para evitarlos**

Las siguientes situaciones no se limitan necesariamente a la telefonía IP pero, en un futuro próximo, probablemente se verán sobre todo en este contexto.

Los protocolos para telefonía en las plataformas modernas (por ejemplo, la telefonía IP) a menudo incluyen mecanismos para solicitar información de contexto. Por ejemplo es posible averiguar el estado de disponibilidad del usuario o enviar un mensaje corto que podría usarse para publicidad. También es posible enviar mensajes instantáneos que podrían usarse como medio para enviar publicidad no solicitada.

Por supuesto, también es posible usar la función de telefonía para transmitir mensajes de audio publicitarios o sencillamente para realizar llamadas publicitarias.

### 2.1. Situaciones en las que se produce SPIT

#### *2.1.1 Centros de llamadas*

En los centros de llamadas los agentes realizan las llamadas publicitarias. Un ordenador elige, de forma sistemática o aleatoria, a quién llamar. Si alguien contesta al número marcado la llamada se pasa a un agente disponible.

El operador de dicho centro de llamadas tiene que cubrir el coste de los empleados, del equipo informático y de las llamadas realizadas, aunque el coste de las mismas es mínimo en el contexto de la telefonía IP. El número de posibles llamadas simultáneas, y por lo tanto, el volumen de spam, depende sobre todo del número de empleados.

#### *2.1.2 Robots de llamadas*

La telefonía IP es una plataforma de comunicación que depende mucho de los ordenadores. Por lo tanto, es muy probable que, de forma sistemática o aleatoria, estos ordenadores elijan un número al que llamar y reproduzcan un mensaje publicitario una vez la llamada es aceptada.

#### *2.1.3 Spit de tonos de llamada*

Algunos teléfonos VoIP vienen configurados de fábrica para que acepten un tipo especial de información SIP llamada "Alert-Info" que podría contener un enlace a un fichero de audio grabado previamente ubicado en algún lugar de Internet. Obviamente, esto puede usarse para reproducir mensajes publicitarios mediante el tono de llamada sin que el usuario tan siquiera haya aceptado la llamada. Una correcta configuración del aparato, como por ejemplo, la imposibilidad de descargar tonos de llamada de Internet, debería resolver este problema.

#### *2.1.4 Combinaciones*

Resulta posible y probable que las situaciones descritas anteriormente se produzcan de forma combinada. El coste para el iniciador de la llamada se situará entre los costes individuales de cada situación.

### 2.2 Enfoques para medidas contra el SPIT

Dependiendo del tipo de spam, existen diferentes enfoques para contrarrestarlo. A continuación se estudiarán varias medidas.

No se prevé que el spam mediante protocolos (por ejemplo, aprovechando funciones del protocolo VoIP como las peticiones de estado de disponibilidad) genere grandes cantidades de spam, ya que el contenido del mensaje que se puede enviar está bastante limitado tanto en extensión como en opciones de presentación. Por lo tanto, su potencial como medio publicitario es limitado. Así que no tendremos en cuenta este tipo de spam en los siguientes apartados.

Ya existen medidas eficaces para evitar el spam mediante mensajería instantánea, por ejemplo, la utilización de listas de amigos. Ya que se presupone que este tipo de comunicación tendrá lugar sólo con otros usuarios calificados como "amigos", esta medida seguirá usándose en el futuro. Sin embargo, el envío de mensajes instantáneos no es directamente inherente a la telefonía y, por lo tanto, no estudiaremos este tipo de publicidad.

En estos momentos existen muy pocas medidas para evitar el SPIT y la cantidad de este tipo de spam aumentará de cara al futuro. El concepto sobre el que se reflexiona en este artículo se centra en las medidas para evitar la publicidad mediante la telefonía. Hemos encontrado los siguientes enfoques para medidas contra el SPIT. También es posible utilizar varias medidas combinadas.

### *2.2.1 Costes de la telefonía*

Una forma común de protegerse de llamadas publicitarias no deseadas es aumentar el coste de la llamada para el que la realiza. Por supuesto, esto contradice el descenso de precios que se espera en la telefonía IP. Sin embargo, esta medida puede resultar útil para permitir a un usuario desconocido establecer un contacto inicial, que de otra manera habría sido rechazado, a un coste superior al normal, por ejemplo, indicándole que usen la RTC[5] o bien pidiendo que realicen una acción (véase más adelante) para identificarse.

### *2.2.3 Listas blancas/de amigos*

Cada abonado al servicio de telefonía mantiene un listado de otros abonados de los cuales esta dispuesto a aceptar llamadas; las personas que no estén en esta lista no podrán llamar al abonado. Esto causa problemas en relación con el contacto inicial. Si bien se trata de un buen sistema para impedir las llamadas de SPIT, también rechazaría a usuarios que podrían ser bienvenidos. Si se usasen exclusivamente listas blancas, la telefonía ya no permitiría contactos iniciales. Un sistema bastante parecido podría resultar de utilidad para la elaboración del concepto SPIT-AL.

### *2.2.4 Listas blancas ampliadas con red de confianza*

El acceso a una red de confianza podría ser útil para permitir llamadas de usuarios no incluidos en la lista blanca personal. Cada abonado da su "confianza" a varios abonados y así, aprovecha sus listas blancas aceptando las llamadas de personas que figuren en esas listas. Si este sistema se extiende para incorporar las listas blancas de las personas que están en la lista blanca de las personas en las que el usuario deposita su "confianza", un número de personas significativamente superior podría llamar al abonado sin que existiesen problemas [Ref. 9]. Sin embargo, el problema de fondo para un usuario que desea llamar sigue existiendo, ya que debe figurar por lo menos en una de las listas blancas antes de poder establecer contacto.

### *2.2.5 Listas negras*

Las listas negras pueden ser individuales o pueden existir una o varias listas negras centrales. Cualquier usuario que genere SPIT se incluye en la lista negra y así se bloquean todas las llamadas provenientes de ese usuario. Entonces, el abonado sólo aceptará llamadas de las personas que no estén incluidas en ninguna de las listas negras. Este sistema se limita al rechazo de llamadas de *spammers* (personas o empresas generadores de spam) conocidos. En el caso de que los abonados tengan su propia lista y, por lo tanto, sólo puedan acceder a sus

propios datos, es muy probable que el nivel de reconocimiento de SPIT sea bajo. Una lista negra central sería más efectiva, pero tampoco puede rechazar llamadas de spammers no identificados.

#### *2.2.6 Listas negras estadísticas*

Los proveedores y operadores de telefonía pueden analizar algunos datos de tráfico y, utilizando métodos estadísticos, determinar la naturaleza de las llamadas. Por ejemplo, en caso de que el mismo usuario llame a varios cientos de números diferentes en un determinado intervalo de tiempo y las conexiones resultantes sean bastante cortas, existe cierta probabilidad de que dicho usuario sea un spammer. A continuación, se puede incluir a ese usuario en una lista negra de la que los abonados se pueden beneficiar, ya que se pueden rechazar posteriores llamadas del mismo usuario. Los registros de las listas negras estadísticas podrían tener propiedades como tiempo de eliminación, de forma que los usuarios honrados puedan "redimirse" mediante una buena conducta.

#### *2.2.7 Interacción del menú de voz*

Antes de conectar con el abonado, el usuario será dirigido a un menú de voz automático y deberá realizar una tarea, por ejemplo "Por favor, pulse 635#\* para conectar con el abonado". Sólo después de haber completado la tarea indicada se establecerá la conexión con el abonado. De esta forma, la tarea funciona como un captcha de audio.

Teniendo en cuenta que el código que se debe introducir es aleatorio, este sistema puede bloquear de forma efectiva las llamadas de SPIT procedentes de robots de llamadas, ya que la mayoría de los ordenadores no serán capaces de realizar las tareas ahora o en un futuro próximo. Los SPIT que tienen como origen centros de llamadas no se pueden bloquear, pero como un empleado de un centro de llamadas necesitará más tiempo para realizar la tarea, el centro de llamadas generará costes más altos (conexión y salario). Este sistema se puede aplicar en el prototipo SPIT-AL.

#### *2.2.8 Listas grises*

Una lista gris es un tipo de lista blanca o negra borrosa. Su comportamiento depende de las circunstancias de las llamadas: en un primer intento de llamada, el usuario recibirá una señal de "línea ocupada" y el teléfono del abonado al que llama no sonará. Sólo en caso de que el usuario intente contactar otra vez con el abonado, conseguirá la conexión con éste, ya que es probable que un humano esté realmente interesado en hablar con el abonado.

Este sistema presenta el riesgo de que los robots de llamadas adapten su funcionamiento. Aún así, se verán limitados a menos llamadas en un periodo. Las listas grises podrían ser un componente del prototipo SPIT-AL.

#### *2.2.9 Conversación simulada*

De forma similar a un menú de voz, se presenta al usuario una voz humana. Ficheros de audio previamente grabados simularán que un abonado real ha aceptado la llamada.[6] Dependiendo del silencio en la línea (por ejemplo, el usuario no está hablando y probablemente espera una respuesta), se reproducirán más ficheros de audio con contenido más o menos interrelacionado.

El objetivo de este concepto es vincular al spammer a una llamada de una duración preferiblemente larga sin éxito en relación con el propósito comercial. Se bloquean recursos del usuario y el modelo de negocio se vuelve menos rentable. Sin embargo, este sistema también bloquea recursos del abonado. No se prevé una aplicación de este modelo en el prototipo SPIT-AL.

### 2.2.10 Honeyphones

El sistema de la conversación simulada también puede utilizarse para aplicar honeyphones[7], es decir, líneas dedicadas que siempre responden de la forma descrita anteriormente. Como la línea no está vinculada a ningún abonado humano real, los usuarios tienen una mayor probabilidad de ser spammers que llaman a números aleatorios. Se pueden añadir a una lista negra central.

Todavía seguiría siendo posible que usuarios no spammers llamen accidentalmente a un honeyphone. El análisis por parte de humanos de las conversaciones grabadas podría ayudar a separar dichos casos. No está prevista una aplicación de este sistema en el prototipo SPIT-AL.

## 3. El proyecto SPIT-AL y su estructura técnica.

La siguiente estructura técnica para la implementación de una solución para evitar el SPIT, sus características, su arquitectura y el contexto en el que puede ser utilizada son el resultado de los sistemas descritos anteriormente.

### 3.1 Funcionamiento básico

SPIT-AL acepta las llamadas como intermediario para el abonado al que se llama. La llamada recibe una puntuación dependiendo de los metadatos de la llamada (origen de la llamada, identidad del usuario que la realiza y hora, si procede) y de las preferencias del abonado. No se realiza una evaluación del flujo de voz y, por lo tanto, tampoco del contenido de la comunicación, ya que las llamadas han de clasificarse rápidamente para evitar posibles molestias. Dependiendo de la puntuación de la llamada, el sistema decide cómo actuará sobre dicha llamada.

### 3.2 Arquitectura del sistema

SPIT-AL debería diseñarse de forma que pueda integrarse en una infraestructura de telecomunicaciones ya existente. Los dispositivos para conectarse a la RTC/RDSI y a la telefonía IP no se desarrollarán en este proyecto. El operador del sistema telefónico (o centralita) en el que finalizan las llamadas será responsable de reenviar las llamadas de los abonados que participan en el proyecto al sistema SPIT-AL en primer lugar. De esta manera, SPIT-AL puede usarse para varios tipos de telefonía (VoIP, RTC o incluso móviles). Algunas funciones, como el filtrado estadístico, requieren una mayor integración con la infraestructura del operador.

La arquitectura del SPIT-AL está dividida en varios subsistemas según la función que ejercen.

La *Aplicación Softswitch* se encarga de dirigir las llamadas de un componente a otro y de realizar las diversas acciones en escala. Las llamadas de los abonados que participan en el proyecto deberán dirigirse en primer lugar a este sistema.

El *Servidor de Voz* ayuda a la *Aplicación Softswitch* a realizar varias de las posibles funciones de SPIT-AL. El *Servidor de Voz* proporciona buzones para mensajes de voz, menús de voz o simples avisos.

La *Aplicación Softswitch*, por sí misma, no toma las decisiones sobre la redirección de las llamadas, sino que delega las decisiones en un *Servidor de Gestión*. Este servidor recibe de la *Aplicación Softswitch* los metadatos de las llamadas y responde con una decisión sobre a dónde redirigir la llamada. El *Servidor de Gestión* también gestiona los datos de configuración específicos de cada usuario (ajustes, preferencias) y los datos para ciertos mecanismos (véase más adelante).

El *Servidor de Gestión* almacena todos los datos relevantes para el sistema en el *Almacén de Datos*.

Un *Interfaz Web* permite a los abonados gestionar sus datos (preferencias personales, listas blancas y negras – véase más adelante – y, si procede, el contenido del buzón de voz) mediante el *Servidor de Gestión*.

El software de código abierto Asterisk[8] podría usarse como base para la aplicación softswitch y el servidor de voz.

Los subsistemas pueden implementarse en sistemas distribuidos o en un solo ordenador. De esta manera, tanto proveedores de telefonía como empresas, instituciones o pequeñas redes privadas pueden utilizar SPIT-AL.

### 3.3 Funciones y detalles del funcionamiento

Cada abonado y usuario de SPIT-AL elegirá sus preferencias personales mediante la interfaz web. Cada una de las opciones se describirá con detalle más adelante.

El servidor de gestión calcula la puntuación basándose en los metadatos conocidos de la llamada como, por ejemplo, la identidad del usuario que llama, el origen de la llamada (RTC, VoIP, o quizás el operador de la red del usuario que realiza la llamada), hora del día, etc. Las preferencias del usuario mencionadas anteriormente pueden influir en la evaluación. Para cada rango de puntos el usuario elige una acción apropiada. Por motivos de privacidad (quizás protegidos por ley) el usuario tiene que poder decidir sobre todas las posibles opciones.

#### *3.3.1 Criterios de Evaluación*

A continuación se muestra una lista de los criterios de evaluación que influyen en la clasificación de una llamada como SPIT. Algunas se aplicarán en SPIT-AL. Para calcular la puntuación antes indicada se tendrán en cuenta varios criterios, combinando los resultados (por ejemplo, sumándolos o de forma ponderada).

No todos los criterios presentados se incluirán en el prototipo de SPIT-AL. En el proyecto se aplicarán inicialmente los criterios de "lista blanca particular" y "lista negra particular".

##### 3.3.1.1 Origen de la llamada

Una llamada puede ser clasificada según su origen. Por ejemplo, si proviene de la RTC, se podría clasificar de forma positiva, ya que se puede suponer que dichas llamadas presentan costes superiores y, por lo tanto, la probabilidad de que sea un SPIT es menor.

De la misma manera, las llamadas provenientes de los principales proveedores de VoIP con una infraestructura regulada (por ejemplo, con fuertes medidas de identificación de usuario, condiciones generales de la empresa que prohíban llamadas con fines publicitarios) podrían reconocerse como tales y, por lo tanto, recibir una puntuación positiva mientras que llamadas provenientes de una conexión DSL o por módem podrían recibir una puntuación negativa.

##### 3.3.1.2 Lista blanca particular

Todos los usuarios de SPIT-AL poseen dentro de sus preferencias su propia lista de identidades de usuarios conocidos y fiables. Si la llamada proviene de un número que se encuentre en su lista blanca esa llamada recibe una puntuación positiva.

##### 3.3.1.3 Listas blancas importadas

Todos los usuarios de SPIT-AL pueden decidir hacer pública su lista blanca particular. Esta decisión se guarda con sus preferencias. Además, el usuario puede elegir de qué otros usuarios esta dispuesto a recibir listas blancas y cómo ponderar cada una de estas listas al importarlas a su lista personal. En caso de que la identidad del usuario que llama no se encuentre en la lista blanca particular del usuario, se recurriría a las listas blancas importadas. Se tendrá en cuenta el resultado junto con la ponderación de la lista importada y, como resultado se obtendrá una puntuación. Este proceso se puede efectuar de forma repetida. De esta forma, la información se envía a un contacto (marcado como fiable por el usuario) y luego (mediante un número limitado de niveles) a los contactos del contacto, y así sucesivamente.[9]

Por motivos de privacidad, es posible mejorar esta función mediante uno o varios servidores centrales en los que la persona que llama deberá explícitamente aceptar que se transfieran sus datos personales a terceros. La información sobre usuarios no contenida en estos servidores no se compartirá con otros usuarios.

#### 3.3.1.4 Listas negras particulares

Todos los usuarios de SPIT-AL tienen dentro de sus preferencias una lista de números marcados como *spammers*. Si la llamada proviene de uno de esos números, recibirá una puntuación marcadamente negativa.

#### 3.3.1.5 Listas negras importadas

Todos los usuarios de SPIT-AL pueden decidir hacer pública su lista negra particular. Esta decisión se guarda con sus preferencias. Además, el usuario puede elegir de qué usuarios (clasificados como "de confianza") quiere importar listas negras publicadas y cómo ponderar su contenido. En caso de que el número de una llamada entrante no se encuentre en la lista negra particular del usuario, se recurriría a las listas negras importadas y el resultado sería una puntuación ponderada. Este proceso se puede efectuar de forma repetida. De esta forma, la información se envía a un contacto (marcado como fiable por el usuario) y luego (mediante un número limitado de niveles) a los contactos del contacto, y así sucesivamente.

#### 3.3.1.6 Listas negras estadísticas

SPIT-AL puede recopilar datos estadísticos sobre un número en particular basados en los metadatos de todas las llamadas realizadas a través de ese número como, por ejemplo: identidad de la llamada, abonado al que se llama, hora del día, duración de la llamada, etc. Si un usuario inicia conexiones con un gran número de abonados en un plazo breve de tiempo y la mayoría de estas llamadas son relativamente cortas, se puede suponer que el usuario es un spammer. Esta información se puede publicar en una lista negra y los usuarios de SPIT-AL pueden importarla y ponderarla.

### 3.3.2 Acciones

Una vez que el servidor de gestión ha puntuado la llamada, se consultan las preferencias del abonado para decidir qué acción tomar. A continuación, se presentan varias posibles acciones. No todas se implementarán desde el principio en el prototipo de SPIT-AL. En dicho prototipo, se implementarán las acciones "aceptar", "rechazar" y "desviar a otra línea".

#### 3.3.2.1 Aceptar

Una llamada que desencadene esta acción se enviará directamente con el usuario. En caso de una puntuación positiva (por ejemplo, si la llamada proviene de un número en la lista blanca particular) la llamada se transferirá al usuario de forma inmediata.

#### 3.3.2.2 Rechazar

La persona que efectúa la llamada oír un tono de llamada (o de ocupado o de línea no disponible) pero el teléfono del abonado al que se llama no sonará. En caso de una puntuación marcadamente negativa (como, por ejemplo, si el usuario que llama figura en la lista negra particular) la llamada nunca llegará al abonado y la persona que llama nunca sabrá exactamente la disponibilidad real del usuario.

#### 3.3.2.3 Desviar a otra línea

La llamada se desvía a otra línea definida por el abonado al que se llama en las preferencias de SPIT-AL. En dicha línea el abonado puede tener un contestador o aplicar otros mecanismos.

#### 3.3.2.4 Rechazar temporalmente / Lista gris

La usuario que llama recibirá un tono de ocupado. Si llama de nuevo en un plazo breve de tiempo, conectará con el abonado. Si llama de nuevo pasado un plazo prolongado de tiempo, se actuará de forma diferente.

#### 3.3.2.5 Aviso de disponibilidad alternativa

La llamada se envía al servidor de voz, el cual comunicará a la persona que llama, mediante un mensaje pregrabado, cómo puede contactar con el usuario, por ejemplo, a través de una línea RTC más cara.

#### 3.3.2.6 Menú de voz

La llamada se transfiere al servidor de voz, donde el usuario se encontrará con un menú de voz en el que deberá escuchar un aviso (quizá un mensaje más largo) y, a continuación, realizar una tarea determinada, por ejemplo, marcar una secuencia de números en el teclado del teléfono. Una vez superada la prueba se transferirá la llamada al abonado o al buzón de voz (véase a continuación), según las preferencias del abonado.

#### 3.3.2.7 Buzón de voz

La llamada se transfiere al servidor de voz en el que el usuario que llama puede dejar un mensaje para el abonado en un buzón de voz. Si las preferencias del abonado así lo requieren, debe realizarse una acción previa a poder dejar el mensaje de voz (véase apartado anterior).

### 3.3.3 Funciones adicionales

Para permitir a los abonados usar SPIT-AL de la forma más fácil posible, se pueden implementar más funciones.

#### 3.3.3.1 Añadir los números marcados a la lista blanca automáticamente

Si un abonado llama directamente a otro, su identidad puede añadirse de forma automática a la lista blanca del abonado, ya que es razonable suponer que también estaría dispuesto a recibir llamadas de esa persona.

#### 3.3.3.2 Registro de datos de conexiones y decisiones

Si un usuario de SPIT-AL recibe una llamada, los datos de conexión como la identidad y la hora, así como la puntuación calculada por el servidor de gestión (además de una breve descripción de cómo se obtuvo la puntuación) se incluirán en un archivo de registro (o base de datos).



Mediante la interfaz web con la que el usuario gestiona sus listas blancas y negras particulares, éste puede revisar el registro de conexiones y decisiones y marcar a los usuarios que han llamado como spammers o contactos con un solo clic del ratón, añadiéndolos a su lista blanca o negra.

### 3.3.3.3 Clasificar llamadas en curso mediante tonos

Si un abonado está hablando por teléfono, puede añadir a su interlocutor a su lista blanca o negra marcando un unas secuencias de dígitos en el teclado de su teléfono.

## 3.4 Problemas técnicos básicos

### *3.4.1 Números ocultos*

La ley[10] exige que los operadores de telefonía ofrezcan la posibilidad de ocultar el número desde el cual se llama. En estos momentos también se están desarrollando mecanismos para proteger la privacidad de la persona que llama mediante telefonía IP [Ref. 10] [Ref. 14].

Por lo tanto, el abonado al que se llama no puede averiguar quien le está llamando ni decidir si quiere aceptar la llamada o no. Esto reduce de forma significativa la eficacia de las listas blancas y negras.

### *3.4.2 Comprobación de la identidad*

Hoy en día es muy fácil falsificar el origen de una llamada en la telefonía IP, ya que no existen estándares normativos ni vinculantes para la comprobación de identidades ni la autenticación de llamadas. Aunque existen mecanismos para autenticar la identidad dentro de un dominio, presentan un nivel de utilización bajo y sigue siendo barato conseguir un número casi infinito de direcciones [Ref. 13].

## **4. Aspectos jurídicos[11]**

El filtrado de llamadas telefónicas tal y como se describe anteriormente provoca una gran cantidad de problemas jurídicos que deben tenerse en cuenta al diseñar una solución técnica contra las llamadas telefónicas no deseadas. Como SPIT-AL se desarrolla en Alemania, la siguiente visión general se basa en el derecho alemán. Debería aplicarse una normativa parecida, como mínimo, en la Unión Europea [Ref. 5]. En la propuesta de SPIT-AL se puede encontrar un análisis más detallado centrado en la normativa alemana, mientras que este artículo abarca los principios básicos.

### 4.1 Fundamentos jurídicos

Diversas normas jurídicas pertenecientes a varias áreas del derecho pueden tener un efecto normativo sobre procesos que se deben utilizar en el contexto del filtrado de SPIT, como el derecho constitucional, las leyes sobre protección de datos, el derecho de las telecomunicaciones, las leyes sobre servicios a distancia, el derecho penal y posiblemente el derecho administrativo [Ref. 3] [Ref. 6]. Los distintos tipos de usuarios, por ejemplo, particulares, empresas o administraciones, se encontrarán en situaciones jurídicas ligeramente diferentes en relación con detalles debidos a las diferentes normativas aplicables, mientras que otros principios más fundamentales serán los mismos para todos los casos. Como ejemplo, un análisis del contenido de una llamada vulneraría el secreto de las telecomunicaciones y estaría sancionado con un máximo de cinco años de prisión según el derecho penal y de las telecomunicaciones de Alemania.

### 4.2 Principales requisitos jurídicos

#### *4.2.1 Filtrado controlado por el usuario*

Por razones de derecho constitucional, de protección de datos y de las telecomunicaciones, es obligatorio traspasar el control completo del qué y el cómo de un filtro de SPIT a manos del abonado, ya que así se minimizan los problemas jurídicos en relación con el secreto de las comunicaciones y la privacidad en los casos de uso privado del filtro. De esta forma, los derechos del abonado a unas telecomunicaciones no observadas y a la privacidad se encuentran en las mejores manos, las suyas.

La complejidad de los conceptos diseñados en el proyecto SPIT-AL tendrá como efecto desvelar problemas en relación con la utilización práctica, así como con la capacidad de garantizar y ejercer los propios derechos e intereses. Por lo tanto, las precauciones enumeradas a continuación pueden resultar de utilidad.

#### *4.2.2 Transparencia y control del tratamiento de datos*

Se deben explicar a los abonados los mecanismos únicos de identificación, clasificación y tratamiento de las llamadas entrantes. Esto les permitiría tomar nota del funcionamiento básico de SPIT-AL, así como de la base de datos subyacente y del objetivo de la transferencia de datos.

En caso de transferencias de datos personales pertenecientes a terceros de la esfera del abonado, es obligatorio informar a las personas afectadas sobre el objetivo, la posterior utilización y las posibilidades de ejercer los derechos del usuario. Una infraestructura central para otorgar (o retirar) el consentimiento u oponerse, así como un mecanismo de aplicación para SPIT-AL podrían ayudar a garantizar los derechos de los interesados[12].

A modo de principio, el abonado debe activar explícitamente cada mecanismo, ya que esto requiere como mínimo un conocimiento mínimo de paradigmas básicos.

#### *4.2.3 Configuraciones previamente establecidas para distintos tipos de usuarios*

Con el objetivo de facilitar el proceso de configuración y para dirigir la utilización en una dirección jurídica principal, las configuraciones previamente establecidas para algunos tipos de usuarios constituyen una opción práctica. Las configuraciones previas deben activarse en la primera utilización y se pueden cambiar posteriormente si así se desea.

Debido a las distintas situaciones jurídicas para particulares, empresas y administraciones, parece razonable establecer tres configuraciones previamente establecidas para el prototipo de SPIT-AL. Difieren entre ellas especialmente en las combinaciones de mecanismos aplicables para identificación, clasificación y tratamiento de llamadas entrantes. Asimismo, una documentación centrada en el usuario de la configuración deberá señalar las características específicas de los tipos de usuario.

### **5. Conclusión**

Este artículo explica que en el futuro se requerirán mecanismos de filtrado de SPIT. Como tienen que actuar antes de que se acepte una llamada y, por no tanto, no pueden depender del análisis del contenido (por oposición al spam de los correos electrónicos), en SPIT-AL, la identidad del usuario que llama se comprobará con listas negras y blancas dentro de un entorno distribuido, una red de confianza entre iguales. Asimismo, se podría utilizar la información de posteriores metadatos y análisis estadísticos. De acuerdo con la clasificación de una llamada y las preferencias del abonado, son posibles distintos sistemas para gestionar la llamada, por ejemplo, "aceptar", "rechazar", "desviar a un buzón de voz", "dirigir a disponibilidad alternativa", etc. El SPIT generado por ordenador se puede filtrar añadiendo mecanismos que requieran la interacción del usuario que llama como un menú de voz.

Para tener una visión general jurídica, se deben tener en cuenta distintas áreas del derecho alemán, especialmente las leyes de protección de datos y el derecho de las telecomunicaciones, pero también las leyes sobre servicios a distancia y el derecho penal y administrativo. La elaboración de listas blancas y negras centradas en la transparencia y el control por parte del usuario es de gran importancia. También se adopta el sistema de distribuir e importar listas a y de terceros.

El concepto favorecido por el proyecto SPIT-AL contiene componentes centrales así como no centrales (aplicados a ciertos usuarios). Los sistemas discutidos se depurarán más a medida que el proyecto progrese. El prototipo de SPIT-AL de código abierto cubrirá el funcionamiento básico de un sistema de gestión de disponibilidad que respete la ley como medida contra el SPIT. Posteriormente, se añadirán otros funcionamientos.

## 6. Referencias

[Ref. 1] Bundesamt für Sicherheit in der Informationstechnik: VoIPSEC – Studie zur Sicherheit von Voice over Internet Protocol, octubre de 2005,

<http://www.bsi.de/literat/studien/VoIP>

[Ref. 2] Bundesnetzagentur:

Anhörung zu Voice over IP (VoIP) – Themenweise

Auswertung der Anhörung zu Voice over IP, octubre de 2005,

<http://www.bundesnetzagentur.de/media/archive/3173.pdf>

[Ref. 3] Bundesnetzagentur:

Eckpunkte der regulatorischen Behandlung von Voice over IP (VoIP), 9 de septiembre de 2005,

<http://www.bundesnetzagentur.de/media/archive/3186.pdf>

[Ref. 4] Center for Democracy & Technology:

Spam 2005: Technology, Law and Policy, (*Centro para la Democracia y la Tecnología; Spam 2005: Tecnología, Derecho y Política*)

Washington D.C., marzo de 2005

<http://www.cdt.org/speech/spam/spam2005>

[Ref. 5] Comisión de la Unión Europea:

Commission Staff Working Document: The Treatment of Voice over Internet Protocol (VoIP) under the EU Regulatory Framework, 14 de junio de 2004 (*Documento de trabajo del personal de la comisión: El tratamiento de Voz sobre IP (VoIP) bajo el marco normativo de la U.E.*)

[http://europa.eu.int/information\\_society/policy/ecommerce/doc/information\\_centre/commission\\_serv\\_doc/406\\_14\\_voip\\_consult\\_paper\\_v2\\_1.pdf](http://europa.eu.int/information_society/policy/ecommerce/doc/information_centre/commission_serv_doc/406_14_voip_consult_paper_v2_1.pdf)

[Ref. 6] 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder:

Entschlüsselung Telefonieren mit Internettechnologie

(Voice over IP - VoIP), 28 de octubre de 2005,

<http://www.datenschutzzentrum.de/material7themen/presse/20051028-dsbk-voip.htm>

[Ref. 7] Herbert Damker, Kai Rannenber, Günter Müller:

Erreichbarkeitsmanagement und mehrseitige Sicherheit aus Benutzersicht,

Fachvorträge auf dem 4. Deutschen IT-Sicherheitskongreß des Bundesamtes für Sicherheit in der Informationstechnik, Bonn, mayo de 1995,

<http://www.wiiw.de/publikationen/Erreichbarkeitsmanagementundme.pdf>

[Ref. 8] Tobias Mahler, Thomas Olsen:

Reputation Systems and Data Protection Law, (*Sistemas de reputación y ley de protección de datos*)

Paul Cunningham, Miriam Cunningham (eds), eAdoption and the Knowledge Economy: Issues, Applications, Case Studies, IOS Press 2004, p. 180-188,

<http://www.afin.uio.no/forskning/notater/Reputation%20Systems%20and%20Data%20Protection%20Law.pdf>

[Ref. 9] Stanley Milgram:

The Small World Problem (*El problema del mundo pequeño*)

Psychology Today, mayo de 1967, p. 60-67

[Ref. 10] Jon Peterson:

A Privacy Mechanism for the Session Initiation Protocol (SIP), RFC 3323,

noviembre de 2002, (*Un mecanismo de privacidad para el Protocolo de Inicio de Sesión (SIP)*)

<http://www.jdrosen.net/papers/rfc3323.txt>

[Ref. 11] R. Pierce Reid:

Voice Spam Spam, Spamity Spam – White paper,

Julio de 2004

[http://www.qovia.com/resources/pdfs/white%20papers/qovia\\_spit\\_wpaper.doc](http://www.qovia.com/resources/pdfs/white%20papers/qovia_spit_wpaper.doc)

[Ref. 12] Thomas Rohwer, Carsten Tolkmit, Markus Hansen, Marit Hansen, Jan Möller, Henning Waack:

White Paper: Abwehr von "Spam over Internet Telephony" (SPIT-AL), marzo de 2006,

[http://www.spit-filter.com/Whitepaper\\_SPITAL\\_20060310.pdf](http://www.spit-filter.com/Whitepaper_SPITAL_20060310.pdf)

[Ref. 13] Jonathan Rosenberg, Cullen Jennings, Jon Peterson:

The Session Initiation Protocol (SIP) and Spam, draft-ietf-sipping-spam-01, SIPPING Internet-Draft, 17 de julio de 2005, (*El Protocolo de Inicio de Sesión, SIP*)

<http://www.ietf.org/internet-drafts/draft-ietf-sipping-spam-02.txt>

[Ref. 14] Jonathan Rosenberg, Cullen Jennings, Jon Peterson:

Identity Privacy in the Session Initiation Protocol (SIP), draft-rosenber-sip-identity-privacy-00, SIP Internet-draft, 11 de julio de 2005 (*Privacidad de la identidad en el Protocolo de Inicio de Sesión, SIP*)

<http://www.ietf.org/internet-drafts/draft-rosenberg-sip-identity-privacy-00.txt>

### **NOTAS A PIE DE PÁGINA**

[1] Este trabajo posee una licencia en virtud de una Licencia 2.5 CreativeCommons Attribution-NonCommercial-NoDerivs

[2] Centro Independiente para la Protección de la Privacidad, Schleswig-Holstein, Kiel, Alemania, <http://www.datenschutzzentrum.de/>

[3] TNG – The Net Generation AG. Kiel, Alemania, <http://www.tng.de/>

[4] Universidad de Tecnología de Dresde, Dresde, Alemania, <http://www.inf.tu-dresden.de/>

[5] Red Telefónica Conmutada, también conocida como Servicio Telefónico Tradicional (POTS en sus siglas en inglés)

[6] Una aplicación modelo es el Telecrapper 2000, <http://www.pagerealm.com/tc2k>

[7] Reciben este nombre por analogía con honeypots y honeynets, véase <http://project.honeynet.org/papers/honeynet/>

[8] <http://www.asterisk.org>

[9] El concepto y el diseño de la característica de listas distribuidas como un refuerzo de SPIT-AL están sujetos a un proyecto de fin de carrera de Ingeniería Informática

[10] Esto es así por lo menos en Europa, Art. 8 Dir. 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas)

[11] Se ha realizado un análisis jurídico básico para los primeros borradores de la propuesta inicial de SPIT-AL. En una posterior conceptualización del prototipo tendrá lugar un análisis con mayor profundidad.

[12] Persona cuyos datos son objeto de tratamiento, Art. 2 Dir. 2002/58/CE, Art. 2 a) Dir. 95/46/CE.