# Metodología de estudio de casos singulares de Interceptación Legal en Internet

Francisco González, Juan Pablo Viñuela

Departamento de Ingeniería de Sistemas Telemáticos
ETSIT - Universidad Politécnica de Madrid
{vidal, vinuela}@dit.upm.es

***Abstract* — Lawful Interception of the Internet can be a trying experience. It is far more difficult than traditional access network interception and represents a big challenge for service providers in general. Law Enforcement Agencies are giving special attention to Internet interception as many emerging service providers appear in the scene, offering new ways of communications over the Internet. In this paper, we explain a technique for studying special and complex cases of Lawful Interception of the Internet, through the analysis of the main actors and characterization of the services involved in the process, and how the can collaborate together in order to comply with national regulations.**

## I. Introducción

La Interceptación Legal es el proceso de interceptar comunicaciones entre dos o más usuarios, según el interés y requisitos de las agencias autorizadas por la ley para tal efecto, comúnmente llamadas LEA (Law Enforcement Agencies). Este proceso se hace mediante autorización legal y se debe realizar sin que los sujetos a interceptar puedan percibirlo, y debe cumplir una serie de requisitos referentes a la confidencialidad de la información que se obtiene producto de la interceptación. Desde el punto de vista de la seguridad de las naciones, la Interceptación Legal es una herramienta de extremada importancia y utilidad, ya que combatir los actos criminales que pongan en riesgo el orden público y la seguridad de un país. De esta forma, las compañías que son operadores o proveedores de servicios públicos de comunicaciones, se ven hoy en la obligación legal de realizar interceptación de las comunicaciones de sus servicios, ante la petición de las agencias respectivas.

Hasta hace poco tiempo atrás, los sujetos obligados a realizar la interceptación han sido las compañías de telecomunicaciones de telefonía tradicional (PSTN). Debido al crecimiento explosivo de Internet en los últimos años, hoy nos encontramos con un escenario totalmente diferente. Por un lado, el acceso a la gran red mundial ya se hace desde cibercafés, bibliotecas públicas, kioscos virtuales, universidades, y otros, y por otro lado, hay un gran número de proveedores de servicios de comunicaciones que utilizan Internet como su principal soporte. Todo esto, sin duda alguna, ha hecho reaccionar a las agencias y les ha hecho empezar a enfocar su atención en la interceptación de servicios de comunicaciones en Internet.

No es tarea fácil realizar la Interceptación Legal de servicios en Internet, y esto ha venido a representar un gran reto para los proveedores de servicios, y en general para todos los sujetos obligados a realizar interceptación. Esta tarea tendrá un mayor o menor grado de complejidad en función de la configuración de los escenarios posibles, según las distintos tipos de redes y actores involucrados. Este artículo describe algunos de los retos y dificultades que se presentan a la hora de realizar interceptación de servicios en Internet, y pretende dar a conocer una metodología de análisis de escenarios y casos singulares, la cual servirá como guía para el desarrollo de posibles soluciones a las dificultades que se presentan. El resto del documento, se estructura de la siguiente forma: La sección II muestra un modelo de referencia y dificultades que se presentan para la interceptación en Internet. La sección III hace referencia a la metodología de análisis propuesta para el estudio de casos y se expone un ejemplo concreto. Finalmente, el apartado IV presenta las conclusiones obtenidas.

## II. Modelo General de Interceptación en Internet.

A pesar que los detalles específicos de una arquitectura de Interceptación Legal varían según la normativa propia de cada país, se expondrá aquí un modelo basado en requerimientos físicos y lógicos, los cuales se desprenden de los requerimientos legales impuestos según la normativa de cada país. En el caso europeo, existe una normativa general y común para toda la comunidad, pero se ha dejado espacio para que cada país concrete esas normas de acuerdo a la realidad y situación propia. [1]

Uno de los elementos claves de la Interceptación Legal, y qué está reflejado en los requisitos legales, es que cualquier proceso de interceptación que se lleve a cabo, no debe afectar al funcionamiento normal del servicio, y más aún, debe pasar desapercibido por los sujetos que serán interceptados. Desde este punto de vista, se hace necesario contar con una clara separación entre la red pública, que puede corresponder a la red de un operador de acceso o bien a Internet, y la red que se utilizará para los procesos y distribución de toda la información que se obtenga producto de la interceptación. Las interfaces entre la red de los proveedores de servicios y las agencias de monitorización normalmente se encuentran estandarizadas dentro de las políticas de cada país, la descripción detallada de las mismas va más allá del alcance de este artículo. [2]

El proceso de interceptación debe ser capaz de extraer la información deseada de la red pública donde se realizan las comunicaciones entre los sujetos a interceptar, procesarla y luego entregarla en las instalaciones de monitorización de las agencias. La ley establece que los operadores deben entregar dos tipos de información: Información relacionada a la interceptación (IRI) y el contenido mismo de la comunicación (CC). Para entregar la información a la agencia, se hace necesario contar con una red separada, la cual debe tener acceso extremadamente restringido y altas condiciones de seguridad.

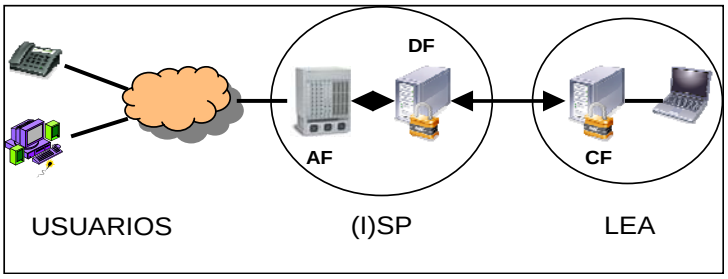


**Figura 1. Modelo Funcional de Interceptación en Internet**

Desde el punto de vista funcional, hay una serie de procesos que deben ser llevados a cabo para realizar la interceptación según las exigencias legales. La Figura 1 muestra el modelo general que se utiliza para interceptaciones en Internet, quedando claramente identificados los tres elementos básicos para realizar la Interceptación Legal:

- Función de Acceso (AF)

  La función de acceso es llevada acabo por una serie de equipos por los cuales transitará la información del sujeto que se desea interceptar. Su principal función es capturar el tráfico desde y hacia el objetivo en cuestión, para luego ser enviado al dispositivo de mediación (DF). El envío de información al DF debe ser hecho en forma segura, pero no necesariamente cifrado. Normalmente, esta función es llevada a cabo por un switch, router, PBX o algún otro dispositivo de red que sea idóneo para caso puntual que se desee interceptar.

- Función de Entrega ó Dispositivo de Mediación (DF)

  Recibe información de algún elemento de red (función de acceso) y hace correlación para determinar si se trata de información sensible a la interceptación que se esté llevando a cabo. En caso de ser información relevante, crea una copia de la ésta para que sea enviada a la LEA. Por lo general, estas funciones son llevadas a cabo en servidores, y cuentan con la inteligencia necesaria para automatizar el proceso de aprovisionamiento de la AF.

- Función de Recolección (CF)

  El proceso de recolección o recepción de información de interceptación enviados por el DF, se lleva a cabo en las instalaciones propias de las respectivas LEA's.

## III. Modelo de Referencia y Metodología de Análisis

Para poder elaborar, en forma eficaz, una metodología que permita hacer el análisis y descripción de los distintos casos singulares que se puedan presentar para la interceptación, es necesario hacer una buena definición del modelo de referencia con el que se va a trabajar, y hacer una correcta identificación de los actores involucrados y el rol que tienen dentro del proceso. La Figura 2 resume el modelo de referencia que se utiliza para este análisis y a partir de aquí, se podrán determinar algunos elementos importantes que permitirán desarrollar la metodología.

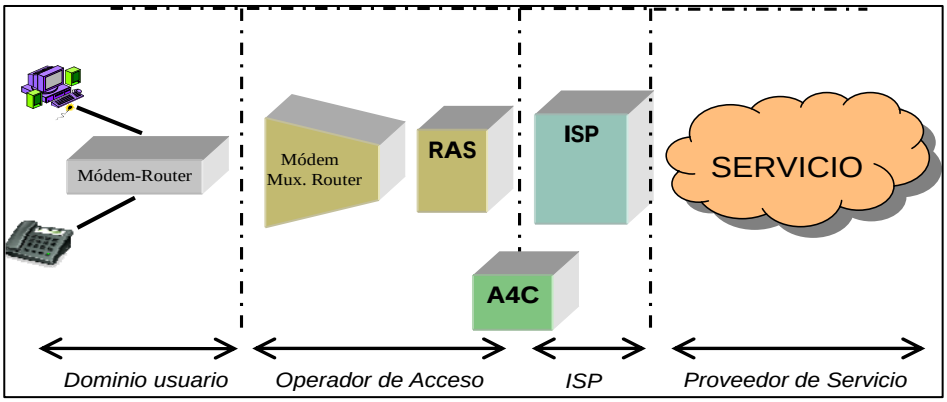


**Figura 2. Modelo de Referencia**

La metodología comienza por hacer una correcta identificación de los actores relevantes en este modelo, y determinar una serie de hipótesis respecto al grado de responsabilidad e injerencia que tienen cada uno de ellos, así como también establecer los supuestos respecto de la capacidad de interceptación que tienen, y de qué forma la colaboración de cada un o de ellos contribuye al resultado final, que es lo requerido por las agencias de interceptación. Uno de los elementos claves en el estudio, es la caracterización del servicio de comunicaciones que se desea interceptar, y según la naturaleza de éste, se irán configurando una serie de escenarios posibles en función de la topología y estructuras de la red involucrada. Por consiguiente, una componente importante de la metodología serán los elementos de investigación que se van a generar producto de los diferentes escenarios que se puedan configurar. En la Figura 3 se presenta un esquema que resume esto y muestra como a partir de las distintas configuraciones se forman los posibles escenarios. Esto finalmente se traducirá en una matriz de análisis de casos, que va a resumir la información relevante y elementos a investigar asociados a los posibles escenarios.

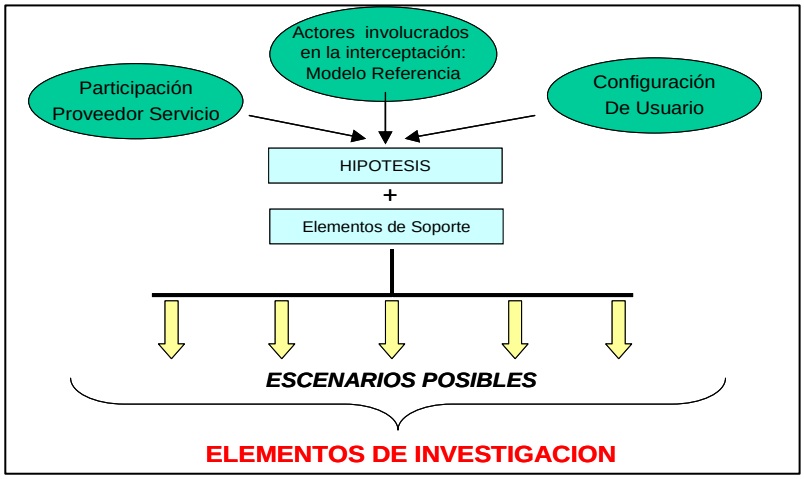


**Figura 3. Generación de Matriz de Análisis de Casos**

Un ejemplo concreto de esto, podría ser la interceptación de comunicaciones en el servicio de voz que ofrece Skype. En este caso el proveedor del servicio, dentro del modelo de referencia propuesto, se correspondería con Skype Ltd., y el resto del modelo se puede suponer que permanece igual, por lo que se podría suponer que el usuario sujeto de interceptación es un usuario residencial que se conecta a Internet por una conexión ADSL Una vez identificados los actores y las características de los servicios proporcionados por Skype, se pueden formular las hipótesis y las capacidades de interceptación de cada actor. Esta información se resume en la TABLA I.

El siguiente paso es generar una descripción de los diversos casos o escenarios que se pueden presentar teniendo en cuenta el conjunto de actores e hipótesis que se han determinado antes. Esta descripción de casos corresponderán a las distintas matrices de análisis y que determinarán los elementos de investigación. Estos casos quedarán determinados por algunos parámetros aplicables a cada uno de los actores. A modo de ejemplo, el usuario sujeto de interceptación podría estar detrás de un firewall o de un NAT, en tanto que el proveedor del servicio, podría o no colaborar con la interceptación.

Siguiendo el ejemplo de Skype que se ha propuesto, un escenario posible se daría de la siguiente forma: [3]

1. El usuario realiza el proceso de "Internet Login" con el ISP. Entre la red de acceso y el ISP se puede determinar el punto de acceso, la dirección IP y el nombre de usuario.
2. El ISP, haciendo un sniffing sobre la dirección IP fuente y destino, y apoyándose en una lista de super-nodos de skype previamente conocidos, puede detectar actividad de inicio de sesión en skype.
3. El super-nodo reenvía la información de inicio de sesión a los servidores skype
4. El servidor skype contesta con un certificado de autenticación a través del super-nodo. El ISP puede hacer sniffing del mismo para potencialmente utilizarlo en posteriores funciones de interceptación.

En el caso desarrollado aquí, se ha considerado un usuario que tiene dirección de red pública, sin estar detrás de firewall o NAT, y por otro lado, se asume que skype colabora en la interceptación. A partir de aquí se desprenderán los distintos elementos a investigar. Para este ejemplo en particular, se consideró que sería necesario tener super-nodos trucados, los cuales podrían facilitar el proceso de interceptación, ya que son los que advierten de que un usuario está ingresando al sistema, pero habría que determinar que tipo de información útil para la interceptación podrían proporcionar. Otra elemento a investigar sería la posibilidad de cambiar la dirección IP de un super-nodo trucado en forma indetectable para el usuario. Sólo se han presentado dos temas de investigación aquí por tratarse de un ejemplo, pero a partir de un escenario se podrían presentar múltiples elementos de investigación.

TABLA I.
IDENTIFICACIÓN DE ACTORES E HIPÓTESIS

| ACTORES | HIPÓTESIS | CAPACIDAD INTERC. |
|---|---|---|
| USUARIO | • No se puede intervenir equipo<br>• Cliente Skype estándar | • Identificadores varios del objetivo (IP, punto de acceso, etc) |
| OPERADOR ACCESO | • Sujeto obligado legalmente<br>• Autentica a los usuarios<br>• Transparente al servicio que se quiere interceptar | • Asocia la identidad de usuario a un punto de acceso en la red |
| ISP | • Sujeto obligado legalmente<br>• Autentica al usuario junto con el operador de acceso<br>• Transparente al servicio que se quiere interceptor | • Coopera para asociar una identidad de usuario a un punto de acceso de la red |
| SERVIDOR SKYPE | • Autentica al usuario Skype<br>• Mantiene la lista de contactos de los usuarios<br>• Proporciona certificado al usuario | • Conoce la identidad Skype del usuario<br>• Posee las claves privadas para el inicio de sesión y el certificado que usará para comunicarse con sus peers |
| SUPER-NODOS SKYPE | • Es posible convertirlos en Man in the Middle. Modificar cliente Skype | • Conoce la ID y localización del usuario destino<br>• Actúa como relay de comunicaciones cuando un usuario está detrás de NAT o FW<br>• Hace relay de login. Los usuarios no se autentican directo con el servidor skype. |

El proceso termina al determinar cuál información es relevante para efectos de la Interceptación Legal que se esté llevando a cabo, y con el consecuente envío de esta información a las instalaciones de las agencias de interceptación, que son justamente las que han solicitado esta información desde un principio.

## IV. CONCLUSIONES

En primer lugar, se ha visto que la Interceptación Legal en Internet es un proceso de alta complejidad, y en la cual intervienen un gran número de factores que hay que tener en consideración al momento de diseñar equipos y estratégicas para realizar una interceptación.

La metodología presentada aquí, permite abordar el estudio de servicios en Internet, muchos de los cuales están en fases emergentes y que presentan una serie de dificultades que no han sido abordadas hasta el presente. Al mismo tiempo, la metodología permite abordar casos singulares y complejos en los que intervienen múltiples actores y diversas situaciones referentes a los sujetos a interceptar y los actores.

El estudio presentado no da soluciones a situaciones posibles, sino es una herramienta que permite generar distintos escenarios y las líneas de investigación asociadas, los que finalmente servirán para llegar a las soluciones posibles según cada caso.

## AGRADECIMIENTOS

Este trabajo está dentro del marco del proyecto “CENIT segur@” en colaboración con Alcatel-Lucent y Telefónica Investigación y Desarrollo.

## REFERENCIAS

[1] Council of The European Union, “*Council Resolution on law enforcement operational needs with respect to public telecommunication networks and services*”, 9194/01. Brussels, 20 June 2001.

[2] European Telecommunications Standards Institute, "*Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic*," 2001.

[3] Salman A. Baset and Henning G. Schulzrinne, An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, Columbia University, New York.