Año 1999

VI Legislatura
Comisiones. Núm. 488

CORTES GENERALES

DIARIO DE SESIONES DEL

S E N A D O

COMISIÓN ESPECIAL SOBRE REDES INFORMÁTICAS

PRESIDENCIA DEL EXCMO. SR. D. ISIDRO MANUEL MARTÍNEZ OBLANCA

celebrada el jueves, 30 de septiembre de 1999

ORDEN DEL DÍA:

Comparecencias:

— **De don Anselmo del Moral Torres, Capitán de la Unidad Central Operativa del Servicio de Policía Judicial de la Guardia Civil (Número de expediente 713/000830).**

— **De don Carlos García Rodríguez, Jefe del Grupo de Delitos Informáticos de la Brigada de Delincuencia Económico-Financiera de la Unidad Central de Policía Judicial (Número de expediente 713/000831).**

Se abre la sesión a las doce horas y cinco minutos.

El señor PRESIDENTE: Señorías, se abre la sesión.

Buenos días, antes de entrar en el orden del día, quiero mostrar mi agradecimiento a los dos comparecientes por su gentileza para adaptar sus horarios a las necesidades de esta Comisión. Hay Senadores que están en esta Cámara desde el lunes y les vendrá muy bien ganar unas horas para poder desplazarse a sus lugares de origen. Por ello, quiero dar las gracias a los comparecientes y también a nuestra letrada, doña Mercedes Senén, por sus buenos oficios y por haber dado muestras —una vez más— de su eficacia y su paciencia para con todos nosotros.

Damos la bienvenida a los nuevos miembros de la Comisión y, muy especialmente, al nuevo portavoz del Grupo Parlamentario Popular, don Manuel Atencia, al que le deseamos el mayor de los éxitos en la defensa de la causa internauta.

COMPARECENCIAS:

— DE DON ANSELMO DEL MORAL TORRES, CAPITÁN DE LA UNIDAD CENTRAL OPERATIVA DEL SERVICIO DE POLICÍA JUDICIAL DE LA GUARDIA CIVIL (713/000830).

— DE DON CARLOS GARCÍA RODRÍGUEZ, JEFE DEL GRUPO DE DELITOS INFORMÁTICOS DE LA BRIGADA DE DELINCUENCIA ECONÓMICO-FINANCIERA DE LA UNIDAD CENTRAL DE POLICÍA JUDICIAL (713/000831).

El señor PRESIDENTE: Hoy nos acompañan dos responsables de las Fuerzas y Cuerpos de Seguridad del Estado relacionados con las redes informáticas. En concreto, están con nosotros dos representantes de unidades operativas que cuentan con un reconocidísimo prestigio y que son una referencia obligada entre los especialistas en la investigación de delitos informáticos de toda Europa.

Por tanto, sean bienvenidos a esta Casa para ofrecernos el testimonio sobre las actividades que realizan.

Aunque ambas unidades mantienen una sana y fructífera competencia, hemos optado por que cada uno de los dos comparecientes hagan su exposición para que, posteriormente, los portavoces y Senadores puedan formular el turno de preguntas correspondiente.

Vamos a comenzar por la comparecencia de don Anselmo del Moral, que es Capitán de la Unidad Central Operativa del Servicio de la Policía Judicial de la Guardia Civil.

Sin más preámbulos, tiene la palabra el señor Del Moral.

El señor DEL MORAL TORRES (Capitán de la Unidad Central Operativa del Servicio de Policía Judicial de la Guardia Civil): Gracias, señor Presidente.

Buenos días, en primer lugar, quería agradecer sobre todo la organización de esta Comisión, la oportunidad que me brindan de estar aquí ante todos ustedes y poder exponer básicamente lo que la Guardia Civil puede poner de manifiesto sobre los denominados delitos informáticos, que es esencialmente su experiencia en el campo real. Se trata de poder presentar ante todos ustedes cuáles son los casos en los cuales hemos participado, cuáles son nuestros problemas, en definitiva, cuál es nuestro trabajo.

Para ello voy a intentar apoyarme en una presentación en la que voy a exponer por qué existe una unidad de delitos informáticos dentro de la Guardia Civil, por qué esa unidad, que tiene una competencia nacional, se encuentra dentro de una unidad que investiga casos de delincuencia organizada, y también qué entendemos nosotros como delitos informáticos, si delitos de alta tecnología en relación con los anteriores, además de aportar una serie de estadísticas y casos más significativos para que puedan ver las dificultades con las cuales nos encontramos. *(El compareciente presenta diversos documentos apoyándose en material informático.)*

En primer lugar, las razones por las cuales existe un grupo de delitos informáticos dentro de la Guardia Civil es que aparece el Código Penal de 1995 en el que surgen un conjunto de delitos o tipos penales donde el denominador común es la utilización de una serie de medios informáticos. El bien protegido puede ser muy diverso, como podrán ver, pero lo que es muy característico es la utilización de una serie de medios informáticos.

Posteriormente, tanto el Cuerpo Nacional de Policía como la Guardia Civil forman parte de la Policía Judicial en base al Real Decreto de Policía Judicial. Por lo tanto, la Policía Nacional tiene unidades especializadas en la lucha de determinados delitos específicos y también la Guardia Civil para apoyar a sus unidades, unidades territoriales, en todo el territorio nacional.

A finales del año 1995 empezamos a recibir peticiones directas del Ministerio Fiscal y de las autoridades judiciales directamente a nuestra unidad para poder llevar a cabo una serie de investigaciones en relación con los delitos informáticos. Como consecuencia de ello, a finales de 1996 se crea un grupo de delitos informáticos. ¿Por qué dentro de una unidad, que es la Unidad Central Operativa de Policía Judicial? Esta Unidad tiene diferentes grupos de especialistas, por ejemplo, hay especialistas en delitos contra el patrimonio histórico-artístico o delitos violentos. Específicamente se ha creado un grupo denominado de delitos informáticos para apoyar en sus investigaciones a las unidades de Policía Judicial de la Guardia Civil a nivel territorial.

¿Por qué se ubica aquí esta unidad? Porque se ve claramente que los medios informáticos y tecnológicos cada vez son más utilizados por la delincuencia organizada, tanto en los medios como en los objetivos. El primer ejemplo lo tienen ustedes en los atentados que realizan las Brigadas Rojas en los años setenta contra más de 20 edificios donde se encuentran ubicados básicamente una serie de centros neurálgicos relacionados con la informática. A continuación les pongo otra serie de ejemplos en los que se han utilizado medios informáticos, el más significativo quizás es el último: grupos terroristas y usos de comunicaciones encriptadas.

Este grupo ha trabajado en colaboración con el Servicio de Información de la Guardia Civil en casos en los que antiguamente los contactos entre miembros de grupos terroristas se realizaban en el campo, a través de «zulos» donde se dejaban una serie de mensajes, pero eso ha cambiado. Existe constancia y se encuentran procedimientos judiciales abiertos donde se ha puesto de manifiesto que las comunicaciones entre miembros de grupos terroristas se efectúan, concretamente dentro de ETA, a través de Internet y mandándose fotografías o mensajes a través del correo electrónico.

¿Qué delitos perseguimos? Anteriormente al año 1995 básicamente lo único que nos llegaban eran casos de copia ilegal de programas informáticos, pero a partir de esa fecha empiezan a llegar denuncias —porque estos delitos requieren en la mayor parte de los casos de denuncia previa por parte de la víctima o de la persona afectada— revelación de secreto, concretamente relacionado con el acceso no au-

torizado a sistemas informáticos, de intrusismo informático, de interceptación ilegal de correo electrónico y de otros casos de fraude electrónico —podrán ver algún ejemplo posteriormente— o fraude en las telecomunicaciones, el denominado desde un punto de vista criminológico efecto *freeky*. La copia ilegal de *software* es un delito típico clásico dentro de esta clasificación, y finalmente la falsificación de *hardware,* porque se han encontrado en España unas corrientes que vienen del sudeste asiático y de la zona de Florida en Estados Unidos que traen a España una serie de microprocesadores remarcados, que son incorporados por empresas mayoristas a ordenadores y comercializados en más de 200 empresas dentro del territorio nacional en el ámbito local; posteriormente montan esos ordenadores con microprocesadores remarcados o fraudulentos, y finalmente los comercializan. Éste es otro delito que también se ha investigado.

Les puedo hacer una lista de todos los delitos clásicos en los que se ha trabajado y donde los medios tecnológicos aparecen como un medio de comisión, fundamentalmente para eludir la acción de la justicia. Casos como el uso por bandas organizadas, por grupos neonazis y el más reciente es la intervención de una serie de objetos arqueológicos en la zona de Sevilla, cuya subasta se realizaba a través de Internet, contrabando de obras de arte, espionaje industrial o de otro tipo.

Esta clasificación no es ni mucho menos doctrinal, está hecha más bien desde un punto de vista pragmático porque así es nuestra experiencia. Nosotros no entramos a definir los delitos informáticos de una u otra forma, sino simplemente intentamos dar una respuesta a lo que la sociedad demanda en este caso. En base a la presencia de una serie de actividades delictivas en el Código Penal, determinadas víctimas se ponen en contacto con nosotros, tramitan las oportunas denuncias y éstos son los delitos que estamos persiguiendo.

En cuanto a las estadísticas, en una comparativa de los últimos tres años en la que venimos trabajando se ve que la copia ilegal de *software* básicamente va aumentando pero de una forma progresiva, sin grandes altibajos, la falsificación de *hardware* —les comentaba un caso del año 1996— ha ido disminuyendo, y sin embargo los accesos ilegales y el fraude electrónico, sobre todo en cuanto al fraude de tarjetas de crédito a través de Internet, se ha disparado en este último año de una forma alarmante.

A continuación les contaré algunos casos y podrán ver cuál es el *modus operandi* y cómo funciona este tipo de actividades delictivas.

Otro ejemplo sería la pornografía infantil, aunque no es que se hayan producido muchos casos en lo que llevamos de año pero sí ha habido un aumento. Anteriormente sólo se podían perseguir aquellas difusiones de imágenes pornográficas de menores por las cuales se demostraba que este tipo de prácticas existía en nuestro territorio nacional. Si disponíamos de una fotografía debíamos indicar quién era el menor y conocer la ubicación donde tenían lugar estas prácticas. En la actualidad, con la modificación del Código Penal ya no es necesario porque se protege la figura del menor independientemente del origen de la fotografía, incluso desconociendo la identidad del mismo. Igualmente han aumentado los casos de terrorismo donde se utilizan medios informáticos o mensajes encriptados.

Éstas son estadísticas referidas a casos en los cuales intervienen dos o más Comunidades Autónomas. Por ejemplo, no podrán encontrar aquí estadísticas de intervenciones de una denuncia puntual en una provincia donde se comunica a la Policía Judicial o a la Guardia Civil que en una tienda determinada se está produciendo la venta de copias ilegales de programas y se actúa conforme a ello. Este tipo de casos no queda recogido en estas estadísticas, repito, sino los casos de competencia nacional donde aparecen reflejadas dos o más Comunidades Autónomas implicadas.

Voy a hablarles ahora sobre cooperaciones internacionales. Se iniciaron en el año 1996 con las solicitudes que realizábamos a otros países a través de la Comisión Rogatoria Internacional, a través de Interpol. En el año 1997 teníamos solamente solicitudes a 4 países; en el año 1998 ya fueron 8 y en el año 1999 llevamos hasta ahora 23 países; es decir, es un fenómeno donde el concepto de territorio aparece muy difuminado y donde las relaciones internacionales son esenciales.

Nuestra unidad tiene también relaciones internacionales y fundamentalmente está encuadrada en tres grupos de trabajo a nivel internacional: el primero es un grupo de trabajo de Interpol, en Lyon, también está incluido el grupo nacional de Policía. Nosotros acudimos a las reuniones que se producen cada cuatro meses, intercambiamos *modus operandi,* realizamos una labor de formación para otros países, que se concretó en la realización de un curso para miembros de policía de los países del Este y del Ministerio Fiscal con la colaboración de Interpol en Tarragona y la Universidad Rovira i Virgili. Éste es un grupo de intercambio de formación y de *modus operandi.* Los dos grupos siguientes, la IOCE y la ENFSI, son fundamentalmente de contenido forense, para analizar las evidencias dentro de ordenadores o de medios tecnológicos.

Voy a comentarles muy rápidamente algunos casos conocidos que han dado lugar a unas primeras sentencias; van a comprobar las dificultades con las que nos encontramos y ustedes mismos podrán analizar toda esta problemática.

El primer caso es el de Hispahack que si no es importante, sí es significativo porque es la primera y única sentencia que existe en nuestro país sobre acceso ilegal a un sistema informático, el caso de un *hacking.* La investigación se basa fundamentalmente en una serie de potenciales presuntos grupos de intrusos informáticos relacionados con una queja procedente de Telefónica sobre un intento de acceso a los ordenadores de la NASA en Estados Unidos conectados a Internet, así como a una tentativa de acceso a los ordenadores de la Universidad de Oxford; también se les suponía relacionados con la modificación de una página web del Congreso de los Diputados.

Con respecto a estos tres casos, como pueden ustedes imaginarse, no pudimos hacer absolutamente nada porque no existía una denuncia oficial sino que simplemente se recibió información sobre ello. Sí se produjo una denuncia sobre el robo de 2.500 palabras de paso y datos privados de

carácter reservado de un proveedor de Tarragona, con unos daños valorados en más de dos millones de pesetas. Finalmente, hubo un acceso por parte de un ordenador de la Universidad de Oviedo a 16 ordenadores de la Universidad Politécnica de Cataluña, la instalación de un programa que rastrea palabras de paso que circulan por la red y por último la información que fue capturada de forma no autorizada se salvó por un ordenador ubicado en Palma de Mallorca.

¿Cuál es el procedimiento en cuanto a la fase de investigación policial? Una entrada a través de un ordenador de la Universidad de Oviedo que llega a 16 ordenadores de la Universidad Politécnica de Cataluña, sustraen palabras de paso y datos confidenciales y los intentan almacenar en un cibercafé de Palma de Mallorca.

La primera dificultad es que la denuncia se interpone seis meses después de que ocurren los hechos, con lo cual cuando nos dirigimos a la Universidad de Oviedo para que nos dé la información, como no existe regulación en España, a diferencia de otros países, respecto a cuánto tiempo deben almacenar los ficheros *logs* de seguridad donde quedan registrados los accesos a los ordenadores, cuando llegamos a pedir esa evidencia al ordenador no se encontraba. Si hubiésemos tenido ese fichero podríamos haber llegado a identificar el teléfono desde el cual se realizó la conexión, el día y la hora en que se realizó el ataque, pero, repito, ese fichero no se encontraba, con lo cual, la única evidencia en todo este caso fue simplemente que el atacante de los dieciséis ordenadores fue borrando todas las pistas de su ataque, pero se equivocó en borrar una: en uno de los ordenadores que había atacado dejó todo el rastro de lo que había hecho, que era entrar desde la Universidad de Oviedo, hacer un salto a la Universidad Politécnica de Cataluña, instalar un *sniffer* o rastreador, que recupera todas las palabras de paso: profesores, personas que trabajan en proyectos, toda la información personal de esas personas, la volcó dentro de un ordenador de un cibercafé de Palma de Mallorca y las ubicó dentro de un fichero, de un directorio que se denominaba JFS, y para entrar en ese ordenador utilizó la palabra de paso Hispahack, que es el nombre del grupo.

Nosotros inicialmente no sabíamos lo que era ni Hispahack ni JFS. Empezamos a buscar en Internet y nos apareció una página web de un grupo de personas que, según ellos, eran intrusos informáticos que se denominaban *Mentes inquietas,* donde aparecía un artículo de diferentes personas identificándose con alias, entre ellos una persona se identificaba como JFS y que daba información de cómo atacar sistemas informáticos. Entre estos artículos figuraba el de un abogado que decía que, en caso de que los miembros de Hispahack fueran detenidos, debían ponerse en comunicación entre ellos, y como se tiene derecho a que se ponga en conocimiento de los familiares el hecho de la detención, había que aprovechar ese hecho para ponerlo en conocimiento del resto de las personas del grupo, para poder borrar determinada información. Finalmente supimos que JFS es una persona —a través de diferentes manifestaciones testificales— que trabajaba en Gibraltar, se le detuvo por estos hechos y vamos a ver a continuación la sentencia.

Esta sentencia a mí me parece ejemplar; es absolutoria, pero vamos a ver lo que dice. Indica que no existe consistencia por parte de la defensa para intentar decir que las evidencias practicadas por los medios de investigación y los medios de prueba conseguidos por la Guardia Civil son nulos; el juez dice que están bien conseguidos. El abogado de la defensa decía que nosotros habíamos vulnerado los derechos de estas personas, porque habíamos pedido, sin mandamiento judicial, a un proveedor de Internet que nos identificase, con nombres y apellidos, a un titular de un correo electrónico. El juez en esta sentencia dice —que ya digo que es la única que existe, que yo sepa— que la identificación de un titular es muy diferente a la intervención de las comunicaciones. Nosotros no intervinimos las comunicaciones de nadie, sino que pedimos datos de un titular, como si fuese el dato de un abonado telefónico, porque entre otras cosas es necesario poder contar con ese dato, porque cuando se pide a la autoridad judicial la intervención de las comunicaciones hay que decirle a quién corresponden esas comunicaciones.

El juez por primera vez —y es la primera definición, a nivel judicial, del fenómeno *hacking*— define este fenómeno diciendo que es un intrusismo informático o acceso o interferencia no autorizado a un sistema informático, y el propio juez dice que existen fundadas sospechas de la participación del detenido en los hechos porque existen cuatro indicios, y el detenido propiamente reconoce que es JFS, y que es miembro de Hispahack; que en el ordenador que fue intervenido en su casa se encuentran *sniffers* y programas para hacer este tipo de ataques; que en su ordenador se encontraron palabras de paso reservadas y *sniffers* que demuestran su acceso al ordenador de la Universidad de Oviedo, y finalmente el perito que intervino en la causa dice que la persona que instala un *sniffer* es quien lo ha utilizado, con lo cual es un indicio de que esta persona es la responsable. Pero el juez —y estoy totalmente de acuerdo— lo absuelve porque que con esa palabra de paso y con esos datos puede haber entrado cualquier otra persona; cualquier otro miembro de Hispahack puede haber hecho ese tipo de ataque y haber almacenado una información en su directorio; efectivamente es así, pero por los datos que se tienen hasta ese momento no había ningún guardia civil ni ningún policía judicial junto al atacante en el momento del ataque. Repito que estoy de acuerdo con la sentencia, pero ésos eran los datos que se tenían entonces.

Voy a relatarles rápidamente otro caso que afectó al Ministerio del Interior —y pido disculpas por la rapidez en mi exposición—, que también es novedoso. Se trata de un ataque de una persona que utiliza los recursos informáticos de diversas redes en Estados Unidos para enmascarar su ataque e intentar acceder a la red externa del Ministerio del Interior, y posteriormente a la red interna. El ataque se concreta en una instrucción de entrada por el puerto del correo del ordenador que mantiene la página web, y que lo que dice básicamente es: sustrae el fichero de palabras de paso de ese ordenador y envíalo a la cuenta «Terapia 83.@.hotmail», que se encuentra situada en Estados Unidos, es decir, sustrae información y almacénala en un lugar que está en Estados Unidos. Eso es lo que dice la orden.

Realmente no funcionó la instrucción porque el atacante se equivocó al teclear, pero si realmente llega a funcionar hubiera tenido acceso a las palabras de paso de las personas que, cuando están dentro del Ministerio del Interior y se conectan y mandan correo, están en intranet, pero finalmente cuando se intentan conectar a Internet para mandar cualquier correo, lo que hacen es que el sistema lo deposita en la página web del Ministerio del Interior. Si hubiese tenido acceso a esa palabra de paso, hubiese tenido acceso al algoritmo que transforma las palabras de paso en reales que se encuentran en el interior del sistema, y repito, hubiesen podido acceder posiblemente en alguno de los casos a correos electrónicos internos del Ministerio del Interior.

Eso no ocurrió, fue una tentativa o un delito frustrado, pero vamos a ver las dificultades. El ataque informático duró una semana, ese ataque masivo de datos de Estados Unidos para intentar difuminar de dónde procedía el ataque duró una semana, mientras que el intento de acceso, esa instrucción que les he dicho duró unos segundos, es decir, ese intento de sustraer las palabras de paso.

Intentamos pedir una Comisión Rogatoria Internacional a Estados Unidos para que nos identificase quién era la persona que había almacenado la información en la cuenta «Terapia 83.@.hotmail». Ésta es una cuenta gratuita; yo me puedo crear una cuenta *hotmail* desde España; me piden un formulario de entrada para asignarme esa cuenta de correo; yo tecleo las palabras Juan.Juan.Juan y me asignan una cuenta de correo allí, sin que nadie identifique mi nombre ni sepa quién soy. ¿Qué ocurre? Que si me dan ese dato no me sirve para nada, pero sí me sirve saber desde qué punto del mundo se han conectado al ordenador de *hotmail* para bajarse ese correo electrónico, y eso fue lo que pedimos, a través de una Comisión Rogatoria Internacional, y a los seis meses nos contestaron que la conexión que accedía a sus ordenadores en Estados Unidos para llevarse esa información procedía de un proveedor de Internet ubicado en Murcia, en España. Nos fuimos a Murcia con una orden judicial y tuvimos mucha suerte, porque después de todo ese proceso y ese tiempo el ordenador aún guardaba —y no tenía por qué— la información en su sistema informático de cuál era el usuario al que le correspondía esa conexión. Estamos hablando de siete u ocho meses después de producido el ataque.

Finalmente identifican a un usuario que es una persona que se baja ese correo y, después de comprobar que no es un cuenta comprometida, que no existe otra persona que esté utilizando esa cuenta o que esa persona haya dado su palabra de paso y su usuario a otra persona y, por tanto, sea simplemente un hombre de paja, lo que hacemos es verificar que es el propio sospechoso el que utiliza esa cuenta. Se le detuvo y estamos esperando el resultado, pero la detención se produce exactamente —además coincidió el día— un año después de producirse el ataque informático.

Otro caso —y voy muy rápido— es el intento de acceso desde una empresa que se encuentra ubicada en Madrid a ordenadores de la Universidad de Utrech, en Holanda. Es importante que lo conozcan porque se difumina en este caso el concepto de territorio. Desde España atacan a ordenadores de la Universidad de Utrech, en Holanda, y roban o intentan copiar ilegalmente —y lo hacen— un proyecto informático que está compuesto por una serie de once Cds que contienen una obra multimedia sobre los tesoros egipcios en Europa. Esa obra está valorada en más de 6 millones de euros por los contratos que tenía establecidos con todos los museos europeos, es decir, estamos hablando de cerca de mil millones de pesetas. Fue sustraída esta serie a través de Internet y hubo una solicitud por parte de las autoridades judiciales y policiales holandesas, y finalmente se identificó a una empresa en Madrid, en la que trabajaba una persona aficionada a la egiptología que utilizó el ordenador desde el cual se realizó el ataque. Como ven, es un problema legal. ¿Qué ocurre? Pues, básicamente, que el resultado de la acción se produce en Holanda, pero el origen está en España. ¿Dónde debe ser juzgado el hecho? El Código Penal es muy claro: el delito existe, tanto en Holanda como en España, pero el procedimiento penal no está claro. ¿Qué sucede? Que esta persona, al final, opta por venirse a España, interponer aquí la denuncia y nombrar un procurador en España, porque sabe que es la forma más rápida de atajar de alguna manera la difusión de este material o su venta posterior. Porque si está esperando a poner una denuncia en Holanda, y que posteriormente se tramite a través de comisión rogatoria, puede esperar unos cuantos meses.

Acabo la exposición con un caso que ha hecho que estemos totalmente desbordados en nuestra unidad con respecto a los casos de fraudes electrónicos. Les pongo un caso real.

Un señor se desplaza desde Almería, va viajando hasta Teruel, sufre una avería en su coche, va a un taller y paga con su tarjeta Visa esa avería, pero tira el papelito en el que viene la información del pago de esa cantidad. En ese papelito viene —en determinados sitios sí consta— el número de la Visa y la fecha de caducidad. Ese dato es recogido por una persona, que es un empleado del taller, que lo que hace es que se conecta a través de Internet. Su proveedor está ubicado en Valencia, y desde él accede a una tienda virtual que ofrece la venta de productos informáticos desde Vic en Barcelona. ¿Qué ocurre? Pues que a través de la pantalla puede acceder y lo que realiza es una compra de material informático por más de un millón de pesetas. ¿Cómo viaja esa transacción? Viaja desde el sur al norte, físicamente desde su casa al proveedor de Valencia, desde éste a la tienda de Barcelona, y en ésta la transacción llega al ordenador central de la entidad financiera: Visa, Master Card, o la que sea. ¿Qué comprobación se hace? ¿Es correcto el número de Visa? Vale. ¿La fecha de caducidad es correcta? Vale. ¿Existen fondos? De acuerdo. Autorizada la transacción. Automáticamente, el cargo viaja de vuelta. El proveedor de Barcelona ve que todo está correcto y automáticamente manda el material informático a Teruel. ¿Qué ocurre? Unos días más tarde se da cuenta de que existe una queja del señor de Almería de que le ha llegado un cargo, y entonces lo pone en comunicación y denuncia el caso. ¿Qué hace? Se va al cuartel de la Guardia Civil de Vic, y pone la denuncia. A nosotros nos llega el caso a través de nuestras unidades. Pero fíjense en la complejidad que tiene a veces esta investigación. ¿Qué debe-

mos hacer nosotros? Debemos verificar los hechos y entregar las diligencias en un juzgado de Vic, en Barcelona; debemos comprobar la identidad con la entidad financiera en Madrid, con Visa o con Master Card, de que realmente existe una operación fraudulenta, que ha sido un cargo en la Visa de un señor el cual no ha efectuado esa compra. ¿Qué más cosas? Debemos comprobar si realmente el señor de Almería ha puesto una denuncia, es decir, verificar si eso es cierto. Ahora hay que recorrer toda la conexión al revés. Debemos comprobar con el proveedor de Vic de dónde procede la conexión de esa compra, luego hay que identificar al proveedor de Valencia. Nos tenemos que ir allí y preguntar: ¿Qué usuario ha realizado la compra a través de Internet? Finalmente nos va a decir: Ha sido un señor de Teruel. En total creo que son cinco los partidos judiciales que intervienen, cinco demarcaciones, y el territorio, como ya le digo, queda bastante difuminado. ¿Qué ocurre? Lo señalo en la pantalla con interrogantes, pero sería muy útil la figura de una fiscalía de delitos informáticos como la que existe en Noruega, en determinados Estados de Estados Unidos y en otros países. ¿Por qué? Porque facilitaría muchísimo el trabajo. El hecho supondría un ahorro para la Administración de Justicia y para todo el procedimiento de investigación.

Hay un caso de pornografía infantil, que relato muy rápidamente. Se trata de un señor de Palma de Mallorca que tenía una página web en un proveedor de Sevilla, y lo que hacía era tener 150 enlaces con diferentes páginas, en todo el mundo, de pornografía infantil, de fotos de menores en actitudes de todo tipo: con animales, etcétera. Con lo que este señor ganaba dinero era con los logotipos publicitarios que disponía alrededor de las imágenes de los menores. Según sus propias manifestaciones, ganaba 250.000 pesetas al mes, sin salir de su casa, simplemente por el dinero que recibía por la publicidad asociada a esas imágenes pornográficas. Cada vez que una persona, desde cualquier parte del mundo, hacía clic en ese enlace o *link*, él recibía quince centavos por parte de la empresa que había hecho el contrato con él para disponer de ese logotipo.

Las fotografías, fundamentalmente, venían de Rusia, de Guatemala o de aquellos países donde la pornografía infantil está más extendida.

Finalmente les expondré —es la última diapositiva— unas conclusiones —no son propuestas mías, sino preguntas lanzadas al aire en relación con lo que yo he visto en otros países cuando hemos asistido a otras conferencias internacionales y cómo otros países han dado soluciones a este tipo de problemas—. En otros países existe una regulación sobre cuánto tiempo deben tener los proveedores de Internet los ficheros de seguridad que muestran las conexiones a Internet y que luego sirven para evidenciar o probar los hechos en un procedimiento judicial. En España, que yo sepa, no existe.

Es curiosísimo que en España, si yo pido a Telefónica o a otro proveedor de telefonía el dato —no la intervención de sus comunicaciones, que por supuesto nadie duda que hace falta un mandamiento judicial— del titular de un teléfono, si es un teléfono fijo, nos lo dan si lo solicitamos como miembros de Policía Judicial diciendo que estamos investigando un determinado caso y que tenemos unas diligencias previas abiertas con un juzgado, pero cuando pedimos los datos del titular de un teléfono móvil nos dicen que necesitamos un mandamiento judicial. No lo entiendo, porque en otros países no ocurre esto. Cuando pedimos los datos referidos al titular de una dirección de correo electrónico, resulta que Telefónica, Airtel y determinadas empresas nos dicen que nos hace falta un mandamiento judicial, mientras que el resto de los proveedores de España nos dicen que no. Nosotros siempre hacemos la petición sobre la base de un informe que ha hecho la Agencia de Protección de Datos que dice que, en interpretación del artículo 20 de la LORTAD, los miembros de la Policía Judicial están autorizados a identificar, que es muy diferente del concepto de intervenir las comunicaciones.

En cuanto a las compañías telefónicas y la identificación de los usuarios que utilizan tarjetas prepago, les digo que ahora mismo estamos investigando un caso de *freeky* o fraude en telecomunicaciones, donde lo que se utiliza es un determinado aparato que va conectado a un teléfono móvil y donde va una tarjeta prepago incorporada, así es que si una evidencia esencial es la llamada telefónica para demostrar una conexión a través de la cual se realiza un ataque informático, incluso llegando a identificar cuál es el teléfono desde el cual se ha realizado la conexión, vamos a encontrar una tarjeta prepago que no identifica al titular.

Por lo que se refiere a la identificación de los números de teléfono desde los que se han realizado las conexiones a Internet, simplemente les cuento una anécdota. Telefónica u otras compañías, en el caso que les he comentado del Ministerio del Interior, por dos veces ha contestado a la autoridad judicial que tiene almacenado el teléfono que ese día y a esa hora realizó la conexión, que es la prueba esencial para decir que desde esa casa se efectuó ese ataque, pero le dice al juez en su contestación que necesita 500.000 pesetas para poner los dispositivos oportunos para poder leer eso. Si alguien lo paga Telefónica da esa información, pero si no nada. Imagino que esto irá a costas judiciales, que es lo lógico, pero está claro que inicialmente, después de un año, estamos esperando que nos digan el teléfono.

La Ley General de Telecomunicaciones dice a los proveedores de telefonía de Internet que deben colaborar con la justicia, pero no les dice ni cómo ni en cuánto tiempo, con lo cual, ante determinadas peticiones, tardamos en recibir contestación seis meses.

En cuanto a la regulación del uso de la encriptación de las redes informáticas, se lo digo porque en otros países está regulado. Aquí simplemente lo hago constar.

Por último, sobre la figura que les comentaba anteriormente de la fiscalidad de los delitos informáticos, no sé si es la mejor solución o no, pero es cierto que en otros países está funcionando.

Muchas gracias y perdonen por haber excedido un poco el tiempo.

El señor PRESIDENTE: Muchas gracias, Capitán Del Moral, por su intervención, porque nos ha puesto de manifiesto la complejidad y la dificultad de su trabajo y de la incorporación de las nuevas tecnologías al elenco de delitos

que se pueden producir, además, desde cualquier parte del mundo.

A continuación va a comparecer don Carlos García Rodríguez, Jefe del Grupo de Delitos Informáticos de la Brigada de Delincuencia Económico-Financiera de la Unidad Central de Policía Judicial.

Posteriormente a la comparecencia de don Carlos García los portavoces y Senadores podrán hacer uso del turno correspondiente para formular preguntas o reflexiones respecto a las intervenciones de ambos comparecientes.

Tiene la palabra don Carlos García Rodríguez.

El señor GARCÍA RODRÍGUEZ (Jefe del Grupo de Delitos Informáticos de la Brigada de Delincuencia Económico-Financiera de la Unidad Central de Policía Judicial): Gracias, señor Presidente.

Agradezco de antemano la atenta invitación que ha recibido el Cuerpo Nacional de Policía para exponer sus experiencias en esta materia.

He sido citado ante esta Comisión especial para hablar del tipo y la incidencia de los delitos que conlleva la utilización de las redes telemáticas y la actuación que el Cuerpo Nacional de Policía lleva a efecto con el fin de prevenir y descubrir esa clase de conductas. Sin embargo, después de la brillante exposición del Capitán Anselmo del Moral poco o nada me queda que añadir al respecto, ya que parece que hayamos preparado esta exposición conjuntamente.

En principio pensaba que esta comparecencia se limitaba a la contestación de una serie de preguntas, pero, ya que existe la posibilidad de realizar una exposición previa, voy a explicar en líneas generales aquellos aspectos relacionados con la organización del Grupo de Delitos Informáticos, sus funciones, su trayectoria operativa, así como los problemas más destacados, para finalizar con unas conclusiones que permitan establecer un planteamiento de futuro.

El Grupo de Delitos Informáticos de la Policía se crea orgánicamente en julio de 1995 ante la demanda de los distintos sectores de la sociedad de que exista una respuesta por parte de la Policía frente a los ataques y delitos de que son víctimas. La primera actuación —quizá una de las más complejas que se ha realizado a lo largo de toda la trayectoria del Grupo— estuvo motivada por unas intrusiones en los sistemas informáticos de la Universidad Carlos III, actuación a la que posteriormente me referiré.

La ubicación orgánica del Grupo se encuentra en la Comisaría General de Policía Judicial, dentro de la Subdirección General Operativa y, a su vez, dentro de la Brigada de Delincuencia Económica y Financiera. Y se integra en dicha Brigada, como ocurre en la mayoría de los países de nuestro entorno, ya que gran parte de los delitos que se persiguen en este ámbito tienen un móvil económico.

Entre las funciones operativas, y sin citarlas de forma exhaustiva, cabe mencionar, en primer lugar, las relativas a delitos contra la propiedad intelectual por la infracción de los derechos de autor a través de la distribución no autorizada de programas de ordenador. En este aspecto tenemos un gran volumen de actuaciones. Una de ellas, que quizá haya sido pionera en España, tuvo como fin conseguir pruebas de las actividades de los autores de estos hechos. Para ello se procedió a la interceptación del correo electrónico del usuario investigado. A tal fin se colocó una máquina en Tenerife que, a través de una clave cifrada y desde un equipo remoto, nos permitió visualizar y recuperar todos los mensajes de correo electrónico entrantes y salientes del autor de los hechos para el tráfico de sus ilícitas actividades. Dicha persona tenía un voluminoso catálogo de productos en Internet, y a través de ese procedimiento recibía los encargos y enviaba los programas, que posteriormente eran recogidos por distintas personas que se encontraban en diferentes lugares del territorio nacional.

Para llevar a cabo ese procedimiento tan novedoso hubo que convencer al juzgado de distintos aspectos jurídicos, técnicos y profesionales, y con ello se aportó abundante material probatorio de este tipo de actividades.

Una segunda fase de la operación dio lugar a la detención de treinta personas en todo el territorio nacional que recibían esos programas. Pero en este caso su inculpación no se basó en la autoría de un delito contra la propiedad intelectual, sino en ser receptadores de ese material a sabiendas de su ilícita procedencia.

Por otro lado, conocemos de delitos de descubrimiento y revelación de secretos mediante la utilización de las redes de telecomunicaciones para el apoderamiento de ficheros informáticos. Éste es uno de los casos más frecuentes que tratamos en nuestra unidad, y fundamentalmente se dirige a los accesos no autorizados a los sistemas informáticos y a la alteración de esos sistemas una vez que se han introducido en la red informática.

Como ya he dicho, les voy a contar a sus señorías un caso sobre el que recientemente ha recaído una sentencia condenatoria a raíz de una denuncia interpuesta por la Universidad Carlos III. Me voy a referir a ello de forma casi enunciativa.

Se denuncia el caso y se procede a la apertura de unas diligencias previas por interceptación de telecomunicaciones. Todavía no había entrado en vigor el vigente Código Penal, pero a pesar de todo, en función de su artículo 497, referente precisamente a interceptación de telecomunicaciones, se abren unas diligencias previas, y debido a la valiosa actitud del juez al que corresponde entender del asunto, éste nos concede que llevemos a cabo las numerosas diligencias que le solicitamos, pudiéndose comprobar que hay ataques a empresas extranjeras desde máquinas de la Universidad Carlos III. Los accesos se realizan a través de los equipos módem de la Universidad, y se comprueba que están comprometidas en ello numerosas máquinas con diferentes servicios docentes de la propia institución. Se utiliza una cuenta legítima y se obtienen privilegios de administración, con lo que se produce alteración, borrado y manipulación de distintos ficheros. Se produce también apoderamiento de datos y de programas de la Universidad, y los autores, después de hacer todas esas actividades, proceden a efectuar un borrado de todas ellas y colocan en un directorio apartado de la red una serie de ficheros para evitar que puedan ser conocidas sus actividades.

Como nosotros contamos con personal en nuestras áreas técnicas de telecomunicaciones así como con la colaboración de las entidades perjudicadas, antes de que fueran borrados todos esos rastros de sus operaciones conseguimos hacer una copia de todas ellas permitiéndoles finalmente el borrado, pero de una manera tal que los autores de esos hechos no son conscientes de que nosotros almacenamos toda esa información. Se procede a un análisis de todas las comunicaciones fundamentalmente por IRC, por charlas interactivas de Internet, y se va haciendo acopio de varios volúmenes de esas actividades. A través de ese análisis la línea de investigación da un nombre. A partir de ahí hacemos distintas comprobaciones —evidentemente en la Policía Judicial resolvemos las investigaciones en muchas ocasiones por métodos tradicionales—, y a través del censo de Leganés averiguamos que este usuario aparece inscrito como residente en esa localidad. Se producen una serie de escuchas telefónicas en las que se comprueba que mantiene conversaciones con otros amigos, con otros usuarios con los que está haciendo estas actividades, y por este procedimiento vamos conociendo hasta los mínimos detalles, por ejemplo, cómo utiliza unas tarjetas bancarias de otras personas, es decir, que también están perjudicados otros titulares de tarjetas de crédito. Además, utiliza una vivienda cuyo buzón está repleto de correspondencia que no recoge su inquilino al estar fuera de Madrid, pero desde allí puede obtener las contraseñas que le envía finalmente el proveedor que le da acceso a Internet, un proveedor extranjero.

Como he dicho, se producen una serie de detenciones y un reconocimiento de los hechos, y finalmente hace poco se ha dictado una sentencia condenatoria.

Esto es descubrimiento y revelación de secretos, un delito que investigamos con frecuencia, pero también hay otra serie de ellos, por ejemplo, el de daños o estragos en sistemas informáticos o en bases de datos —es candente el tema de los virus, la transmisión de virus por distintos medios, ahora especialmente por ficheros ejecutables que se envían a través de correo electrónico—, así como las defraudaciones económicas a través de la manipulación de datos o programas para la obtención de un lucro ilícito.

Estamos —y voy a utilizar la misma palabra— desbordados por un aluvión de denuncias sobre fraudes informáticos; se trata de personas que utilizan ilícitamente las tarjetas para realizar operaciones en Internet, generalmente demandan servicios eróticos, servicios que dan conexiones para jugar en Internet, pero también se dan casos —y ya se han producido varias detenciones— por realizar compras en tiendas virtuales.

También son frecuentes las amenazas, calumnias e injurias, mediante el envío de mensajes por correo electrónico o la colocación de anuncios en diferentes servicios de Internet. Asimismo, hemos observado falsedades documentales en la comercialización de dispositivos informáticos.

Desgraciadamente, también nos enfrentamos ante un tema de tanta actualidad como es el de la pornografía infantil. Hemos realizado, antes de la entrada en vigor de la reforma del Código Penal en materia de delitos contra la libertad sexual, múltiples investigaciones. En su día se pronunciaron voces muy autorizadas anunciando la existencia de ese vacío legal, pero no llegaron a prosperar. Paralelamente, llevamos a cabo otro tipo de actuaciones que ponían en evidencia la existencia de pornografía infantil mediante la utilización de Internet para la difusión de imágenes y el establecimiento de contactos relacionados con este tipo de actividades.

Pero no termina aquí la tarea de la Unidad, a pesar de que ya es bastante teniendo en cuenta los recursos disponibles, sino que, además, se utiliza Internet para otras actividades. Si en el rastreo sistemático que hacemos de las redes encontramos información —ya sea de terrorismo, de tráfico de estupefacientes, de blanqueo de dinero o de actividades de juego ilegal— o si la recibimos a través del buzón de correo electrónico que tenemos para recibir denuncias, la cursamos a las áreas correspondientes y colaboramos con ellos en el desarrollo de la investigación.

Dicho esto, voy a exponer esquemáticamente las dificultades con que nos encontramos a la hora de perseguir este tipo de delitos.

En principio, un alto grado de incumplimiento de las normas. Si pensamos en el conjunto de delitos que se pueden englobar en esta denominación usual —y no jurídica— de delitos informáticos, podemos afirmar el elevado número de infracciones penales que se cometen en este ámbito. La escasez de denuncias que se producen, especialmente cuando afectan a entidades financieras —en ello está la salvaguarda de su propia imagen, y no quieren ver comprometida su imagen de seguridad de sus sistemas informáticos—, y la correlativa cifra negra que lleva aparejado este fenómeno, impide el conocimiento de estas actividades delictivas en toda su magnitud.

Por otra parte, hay que tener en cuenta la complejidad de las investigaciones y lo difícil que resulta la obtención de pruebas. En la mayoría de los casos —y no me quiero extender porque ya se ha hablado de ello con profusión— es necesario probar técnicamente la autoría de estos hechos, lo que da lugar a acometer continuas solicitudes a las autoridades judiciales, a los diversos operadores de red y a los proveedores de acceso a Internet.

Es patente la inexistencia de doctrina jurisprudencial en relación con estos delitos —nuestro vigente Código Penal precisa aún de asentamiento; toda norma precisa de un mayor arraigo y conocimiento—, algo que resulta necesario para vislumbrar si avanzamos correctamente en este ámbito jurídico relacionado con las nuevas tecnologías de la información.

Por último, cabe destacar el escaso rechazo social que, generalmente, produce este tipo de criminalidad asociado al uso de técnicas informáticas, al relativizarlas frente a otras que poseen un mayor arraigo histórico.

Las conclusiones a las que llego, partiendo del incremento constante de la utilización de las redes telemáticas en todos los sectores de la sociedad y la dependencia cada vez más creciente de estas nuevas tecnologías, es que debemos ser conscientes de la urgente necesidad de emplear todos los medios a nuestro alcance para afrontar con decisión las continuas violaciones legales que se producen mediante el uso de diferentes procedimientos informáticos.

Es necesaria una contribución eficaz de los poderes públicos con las misiones que tienen fijadas, es decir, completo cuadro de leyes. Si analizamos el panorama legislativo nacional podemos decir que en la actualidad, desde la entrada en vigor del nuevo Código Penal, tenemos la cobertura jurídica que nos permite perseguir este tipo de delitos en nuestro país. Sin embargo estos delitos tienen un carácter trasfronterizo —es una de sus principales características— y queda aún mucho por hacer en cuanto a la armonización de la legislación internacional.

Asimismo, ha de haber una intervención diligente de los órganos de la Administración. Los diferentes órganos administrativos relacionados con esta materia han de realizar un esfuerzo coordinado para proteger a la sociedad frente a los peligros que implica el uso delictivo de las redes de telecomunicaciones.

Se han de llevar a cabo actuaciones judiciales con procedimientos ágiles y, en la medida de lo posible, con interpretaciones uniformes. Uno de los mayores problemas que existe en la actualidad para que prosperen las investigaciones radica en cuestiones de carácter procesal; razones de competencia, con frecuentes inhibiciones, y demoras en la concesión de diligencias solicitadas pueden provocar que se perjudiquen las investigaciones. No podemos olvidar que este tipo de delitos se produce mediante acciones que se realizan con extremada rapidez, en ocasiones desde puntos muy distantes y con un elevado grado de anonimato. Para evitar la destrucción de las pruebas se requiere actuar con la máxima urgencia, y este punto siempre deberá contar con la actuación diligente de los órganos judiciales. Tal vez para agilizar estos trámites —y la verdad es que no nos habíamos puesto de acuerdo en este punto, aunque tenemos frecuentes conversaciones— e impulsar el procedimiento sería necesaria la activa intervención del Ministerio Fiscal, y así lo puse de manifiesto en unas conferencias que impartí a los miembros del Ministerio Fiscal de distintas provincias. Quizá sea interesante —y eso lo hemos hablado con frecuencia— la creación de una fiscalía especial para este tipo de delitos.

También es necesaria la colaboración de diversas instituciones públicas y privadas. Es igualmente precisa la plena colaboración de distintas instituciones, especialmente de los operadores de telefonía, de los proveedores de acceso a Internet y de las instituciones universitarias. Es la fuente donde nosotros buscamos todo ese tipo de información, esos datos que nos permitan demostrar los hechos investigados y la autoría de esos hechos. Con todos ellos se mantienen continuos contactos, pero casi más bien en una relación personal, de cordialidad, porque ellos están dispuestos a colaborar con nuestras investigaciones y siempre hay una actitud positiva al respecto, por lo que tendría que haber una norma que abordase de manera detallada las diferentes obligaciones que deben asumir todas estas instituciones, compañías telefónicas, proveedores de acceso a Internet —en nuestro país tenemos numerosos proveedores— y las universidades. Es evidente que los accesos a Internet se producen bien a través de las instituciones universitarias o bien a través de los proveedores de acceso a Internet.

No puedo evitar hablar de la urgente necesidad de emplear los medios necesarios para perseguir este tipo de delitos. Es necesario que se dote ya de estos medios a las unidades que nos dedicamos a la investigación de este tipo de delitos, porque nos enfrentamos a personas con una cualificación técnica altísima —muchos de los detenidos son ingenieros superiores de informática o de telecomunicaciones— que manejan las tecnologías más avanzadas, frente a los pocos recursos de que disponemos en estas unidades por la precaria situación administrativa. Es necesario dotar a estas unidades que se encargan de la persecución de estos delitos de los recursos necesarios humanos y tecnológicos.

En su día yo tenía puesta una gran esperanza en una proposición no de ley que se debatió el 11 de marzo de 1997, en el Pleno del Congreso, sobre actuaciones policiales a desarrollar en relación a la red informática Internet. Esta proposición no de ley, que fue aprobada, con una sola abstención, por 305 votos, instaba al Gobierno para que se reforzasen los medios a disposición de los grupos policiales que trabajan en materia de prevención y esclarecimiento de los delitos con soporte instrumental en redes informáticas, e igualmente —también se ponía de manifiesto como punto importante—, para que en el seno de la Unión Europea se prosiga impulsando la cooperación entre los distintos Estados miembros a fin de avanzar en la adopción de medidas coherentes y viables respecto de la persecución de dichas formas de delito. El procedimiento de instar al Gobierno todavía sigue conservando actualidad.

Por último, debo hablarles de la formación y cooperación internacional. En el Cuerpo Nacional de Policía se ha hecho un notable esfuerzo en cuanto a la formación. Se han realizado varios cursos sobre delincuencia informática; se han impartido numerosas conferencias sobre esta materia y se ha celebrado un Congreso sobre piratería informática, al que han asistido representantes policiales de 25 países, siendo también de gran importancia el mantenimiento de contactos internacionales. Voy a mencionar sólo lo que se está produciendo actualmente. En este momento se está desarrollando un grupo de trabajo en la sede de la Secretaría General de Interpol, en Lyon, sobre delincuencia informática y sobre temas específicos, y se está celebrando un encuentro en estos días en Viena, sobre pornografía infantil.

Con la asociación de todos estos elementos, es decir, con ese cuadro de leyes, con la actuación diligente de todos los poderes públicos, con la colaboración de las instituciones privadas, con los recursos humanos y técnicos necesarios, así como la formación y cooperación internacional, estaremos en condiciones de abordar con eficacia este creciente fenómeno de la criminalidad informática.

Nada más y muchas gracias.

El señor PRESIDENTE: Muchas gracias, señor García Rodríguez, por su intervención.

A continuación, vamos a abrir un turno de intervención para los portavoces de los diferentes grupos parlamentarios.

En primer lugar, por el Grupo Catalán en el Senado de Convergència i Unió, tiene la palabra el Senador Varela.

El señor VARELA I SERRA: Muchas gracias, señor Presidente.

En nombre de mi Grupo, debo felicitar a los dos comparecientes, señores Del Moral Torres y García Rodríguez, por sus explicaciones, que son de mucho interés para nosotros.

Sus intervenciones me han sugerido varias cuestiones. En primer lugar, en relación con la colaboración con las Autonomías, me gustaría conocer cómo funcionan los Mossos d'Esquadra.

Ha mencionado usted la colaboración con la Universidad Rovira i Virgili y me gustaría que explicase un poco más en qué consiste.

En cuanto a la colaboración internacional —no sé si está ligado a la cuestión—, me ha llegado un correo electrónico de alguien preocupado por Infopol, alegando que va a coartar las libertades, que deberíamos estar alertas, y que qué barbaridad vamos a cometer. Me gustaría conocer su opinión al respecto.

Por otra parte, en cuanto a la colaboración internacional, teniendo en cuenta que estos fenómenos implican a diversos países, me gustaría saber si se está planteando la creación de algún tribunal internacional sobre esta cuestión. De la misma forma que existe un Tribunal de Derechos Humanos, ¿en estos congresos que realizan ustedes se plantea la posibilidad de formar un tribunal internacional de delitos informáticos? ¿Consideraría interesante esa posibilidad?

Ambos comparecientes han dicho que estaban desbordados y me gustaría que precisaran el grado de desbordamiento para que tomásemos conciencia de las insuficiencias. Es decir, ¿creen ustedes que sería necesario doblar o triplicar los medios y el personal? ¿En qué aspecto debería insistir el Estado o el Gobierno?

También he tomado nota de la sugerencia de creación de una fiscalía de delitos informáticos. Es posible que ésta pudiera ser una de las conclusiones de la Comisión e incluso, dado que es un problema real, quizá fuese factible hacer una moción conjunta de todos los grupos pidiendo la creación de esta fiscalía de delitos informáticos.

El señor Del Moral ha insistido bastante en que había más legislación en otros países y el señor García Rodríguez decía que Código Penal actual no da suficiente cobertura jurídica, que tiene que adaptarse y sugiere tener en cuenta la legislación de otros países. ¿Es suficiente el Código Penal o no? ¿Hay que adaptar leyes o regulaciones de otros países?

Finalmente, el señor García Rodríguez ha mencionado que en la persecución de esos delitos había frecuentes inhibiciones en el proceso judicial. ¿Puede precisar de quién?

Nada más y muchas gracias.

El señor PRESIDENTE: Gracias, Senador Varela.

A continuación, tiene la palabra el portavoz del Grupo Parlamentario Socialista, don Josep Ramon Mòdol Pifarré.

El señor MÒDOL PIFARRÉ: Muchas gracias, señor Presidente.

También quiero dar las gracias a don Anselmo del Moral y a don Carlos García Rodríguez por sus intervenciones.

Voy a empezar diciendo que hay dos frases tópicas en España que, afortunadamente, podemos empezar a desterrar. Una de ellas es la de «pasas más hambre que un maestro», lo que afortunadamente ya no es cierto, y otra es la de «a buenas horas mangas verdes», en referencia a que, el siglo pasado, la Guardia Civil llegaba tarde a las refriegas originadas por los bandoleros, llegaba cuando los bandoleros ya estaban a salvo en la sierra.

La Guardia Civil, hace ya casi un año, en el SIMO, nos invitó a don Pedro Calvo y a mí a unas interesantísimas jornadas que auspició ella sobre estos temas. Creo recordar que fue don Fernando Igartua quien decía que los delitos de nuevas tecnologías no eran en realidad tan nuevos. Nos contó como anécdota que el primer delito informático que él recordaba —aunque es posible que los hubiese anteriores— se produjo en 1816, después de la batalla de Waterloo. El mar estaba impracticable, no se podía navegar por el Canal de la Mancha y sólo un barco, el del señor Rothschild, consiguió llegar a Londres. Inmediatamente difundió el rumor de que Napoleón había ganado estrepitosamente a los aliados y, como consecuencia, la Bolsa de Londres se hundió. El señor Rothschild compró todo lo que pudo y, al día siguiente, cuando llegaron los otros barcos se demostró que quien había perdido era Napoleón. Rothschild se hizo rico y además no entró en la cárcel. Seguramente eso hoy hubiera sido considerado un delito en toda regla.

Con esto quiero decir que tengo la impresión, y sería la primera pregunta, de que quizá desde el Parlamento deberíamos estar atentos al cambio en algún tipo de normativa, porque creo que el delito es delito, se produzca en la calle, en la red, o en el domicilio; lo que hay que hacer es adaptar las normativas para perseguir ese delito.

Abundando en la pregunta del Senador Varela, coincido con ustedes en un cosa. Recuerdo que en aquella jornada comenté que había visto por segunda o tercera vez una película que se llama «Chacal», que no sé si ustedes habrán visto, basada en un hecho real. Al hilo de esta película reflexioné que aquello era imposible, la Policía de Londres tenía que llamar a la de Roma y la de Roma a la de París; hoy en día en media hora cogían a este hombre. Quiero decir que es cierto que los delincuentes tienen más medios, pero nosotros también los tenemos para coger a los delincuentes. Por tanto, ¿qué dotación tienen en este momento, tanto humana como material, y cuál creen que debe ser la dotación óptima?

Me preocupa un tema del que han hablado los dos comparecientes, el de la utilización de las tarjetas de crédito. La verdad es que me he asustado porque tengo la costumbre de firmar la tarjeta y tirar el resguardo, aunque no lo voy a hacer más. *(Risas.)* La pregunta sería si las entidades financieras no deberían hacer una campaña de información para facilitarles el trabajo.

Estoy de acuerdo también en que seguramente el principal problema que tenemos es de procedimiento. Por

tanto, coincido plenamente con lo expresado por el señor Varela. Tomamos nota y quizás no estaría de más estudiar la posibilidad de presentar ya una moción urgente solicitando la creación de esa Fiscalía. Pero yo diría más, ¿no creen ustedes que estaría bien que además de una Fiscalía especial en España existiera otra en el marco de la Unión Europea, precisamente por la aterritorialidad de estos delitos?

El señor García Rodríguez también ha citado la necesaria colaboración con las universidades. Yo le pediría que nos dijese si hay algún tipo de colaboración entre ustedes y alguna universidad. Estoy pensando, por ejemplo, en una de las que más investiga en este campo, como es la Universidad Politécnica de Barcelona, de la que contaré como anécdota, porque hay que empezar a quitarse unos pocos tabúes de encima en los temas de seguridad, que en su afán de ser una universidad progresista y universalista, en su reglamento prohíbe la investigación para fines militares, por ejemplo. Yo estuve hablando el otro día con el Vicerrector y me decía: qué gravísimo error hemos cometido porque las principales ayudas nos podrían venir de ese campo. Quizás están estudiando en este momento quitarlo. De la misma manera que él decía esto porque es un campo magnífico, tengo la sensación de que para los investigadores en la universidad sería interesantísimo que establecieran programas de colaboración con ustedes.

Finalmente, ya sé que voy a hacerles la pregunta del millón, pero no me duelen prendas en decir que me gusta copiar lo bueno de otros lugares. Entonces, les pediría que me dijeran cuál es en su opinión el país europeo mejor dotado policialmente en estos temas, porque, al fin y al cabo, copiar de lo bueno es siempre positivo.

Por último, les agradezco nuevamente la claridad de su exposición y habernos traído aquí problemas que, sin su experiencia, seguramente no hubiéramos conocido.

Gracias.

El señor PRESIDENTE: Muchas gracias, Senador Mòdol.

Tranquilizo a los comparecientes porque el Senador Mòdol al denunciar a Rothschild de ese delito informático no tuvo la intención de incrementar el ya de por sí amplio trabajo de las unidades operativas. Es un delito prescrito y, por lo tanto, no tienen ustedes que intervenir. *(Risas.)*

A continuación, tiene la palabra el portavoz del Grupo Parlamentario Popular, el Senador Atencia Robledo.

El señor ATENCIA ROBLEDO: Muchas gracias, señor Presidente.

En primer lugar, quiero agradecerle la bienvenida a esta Comisión y hacerlo extensivo a todos porque me siento muy a gusto en esta Comisión, a la que me incorporo después de un importante trabajo que han realizado los Senadores que forman parte de la misma.

Me pongo a disposición de la Presidencia y de todos los miembros de la Comisión para colaborar, en lo que pueda ser útil, en el devenir de los trabajos de esta Comisión, que tanta trascendencia está teniendo en la vida del Senado en esta legislatura. Esperamos que con los trabajos que se están realizando se puedan llegar a conclusiones interesantes y oportunas.

En segundo lugar, quiero agradecer, como no podía ser de otra forma, la presencia en esta Comisión del capitán don Anselmo del Moral y de don Carlos García Rodríguez y especialmente su gentileza por adaptarse al calendario del Senado y de esta Comisión para que la sesión se pudiera realizar a esta hora y en comparecencia conjunta, y quiero agradecer también sus informaciones, sus reflexiones y sus opiniones, que sin duda alguna serán muy útiles para los trabajos de esta Comisión.

Por no incidir en lo que ya han planteado los anteriores portavoces, quisiera reseñar un aspecto. He escuchado las intervenciones, tanto la del Capitán Del Moral como la de don Carlos García Rodríguez y las propuestas que han dado desde el punto de vista de su experiencia profesional en la averiguación y persecución de los delitos informáticos, en el amplio sentido del término, y se me plantean una serie de interrogantes.

¿Qué adaptaciones se deberían llevar a cabo desde el punto de vista de la legislación española? En ambas intervenciones se ha hecho referencia a la adaptación de alguna normativa o legislación internacional de otros países en relación a facilitar y a poner límites o controles en la comisión de estos delitos.

¿Qué otro tipo de medidas podrían abordarse para un mejor funcionamiento de las unidades operativas, así como de la propia persecución de este tipo de delitos? He tomado nota de todas sus ideas, incluso la de la Fiscalía Especial, pero creo que sería interesante que las aportaciones que han hecho, así como las que puedan añadir se incorporen a las posibles conclusiones que en su caso tenga que plantear esta Comisión. Lógicamente, dentro del conjunto de aspectos que la Comisión tiene que abordar, sus opiniones serán de suma utilidad a la hora de incorporarlas a sus conclusiones.

Otro aspecto que han planteado los anteriores portavoces es qué tipo de medidas, no sólo en cuanto a colaboración, en la que sin duda habrá que profundizar, sino desde el punto de vista legislativo, podrían abordarse en el ámbito de la Unión Europea y en un ámbito internacional más amplio, ante la propia complejidad —destacada en ambas intervenciones— de este tipo de delitos que se producen en las redes de telecomunicación, con un escenario que no se mueve al ritmo natural de otras actividades humanas, sino mucho más rápidamente.

Insisto en agradecer sus intervenciones, y quiero felicitarles en nombre de mi Grupo por el trabajo que realizan en un cometido que cada día se hace más amplio y que requerirá muchas adaptaciones y esfuerzos de todo tipo, y agradecerles la utilidad de sus intervenciones y aportaciones para los trabajos de esta Comisión.

Nada más y muchas gracias.

El señor PRESIDENTE: Muchas gracias, Senador Atencia.

Para dar respuesta a las reflexiones y preguntas planteadas por los tres portavoces, tiene la palabra en primer lugar el Capitán Del Moral.

El señor DEL MORAL TORRES (Capitán de la Unidad Central Operativa del Servicio de Policía Judicial de la Guardia Civil): En primer lugar, al hablar de la colaboración con las Comunidades Autónomas, que es la primera pregunta planteada, tenemos constancia de que en el ámbito policial, Mossos d'Esquadra y Ertzaintza han creado ya sus propios grupos de investigación de este tipo de delitos. También es cierto que tanto con ellos como con la Policía Nacional las relaciones, por lo menos en este aspecto, son muy buenas. La informática abre un campo nuevo y todos tenemos que colaborar y poner el hombro. Ellos nos han pedido que organicemos cursos, e incluso hemos dado alguna conferencia en su academia, y últimamente han solicitado asistir a alguna reunión internacional. Cuando recibí esta petición la elevé a consulta para comprobar si podían intervenir en conferencias internacionales, porque no ocurre igual en otros países ya que a esta clase de conferencias acuden fundamentalmente unidades con competencia nacional debido al problema de territorialidad que tiene este tipo de delitos, por lo que se busca fundamentalmente a personas con un amplio espectro de respuestas ante la comisión delictiva de un hecho. Por nuestra parte la colaboración es totalmente abierta y no existe ningún tipo de problema. En este tema todos estamos empezando, y ellos quizá un poco más.

Con relación a la Universidad Rovira i Virgili ha sido para nosotros la fuente esencial, porque allí se desarrolló nuestro primer caso, con dos estudiantes que sustrajeron a través de Internet una serie de información reservada y que fueron las primeras víctimas que tuvimos en un caso más sofisticado.

Como consecuencia de ese procedimiento, hemos comprobado que una gran parte de nuestros casos se desarrolla en Cataluña. La citada Universidad Rovira i Virgili, así como otras, nos ha ofrecido cursos específicos; es decir, aparte de las clases normales, los miembros del Grupo de Delitos Informáticos de la Guardia Civil han acudido una semana para recibir por profesores de universidad cursos específicos sobre telecomunicaciones, sobre «unix», sobre paquetes de seguridad informáticos, etcétera, con los medios con los que dicha universidad cuenta. Hasta la fecha se han realizado dos cursos: uno, en el año 1997 y otro durante este año. Ha sido también nuestro referente.

Dentro de ese grupo de trabajo internacional de Interpol en Lyon que se reúne cuatro veces al año, como ya les he comentado, hay un subgrupo de formación. Nosotros propusimos que en la Guardia Civil, en colaboración con Interpol y con la mencionada Universidad Rovira i Virgili, se organizase un curso de Interpol y que tuviera lugar en España, porque hasta ahora sólo se habían realizado en Alemania, en Inglaterra, etcétera. Son cursos para miembros de la Policía Judicial, de la Policía Criminal y del Ministerio Fiscal destinados al resto de los países europeos menos desarrollados en la investigación de este tipo de delitos. Nuestra propuesta fue aceptada con fondos de Interpol y se celebró por fin un curso en España de seguridad en redes informáticas, con una parte puramente policial y otra puramente técnica al que acudieron personas de Ucrania, de Malta, de Finlandia, de Polonia, de países cuya legislación o desarrollo a nivel de investigación o estructura policial se encuentra menos avanzado, como ya he indicado.

Tengo varias preguntas relacionadas con el proyecto Infopol. Desconozco lo que es. Algunos medios de prensa me lo han preguntado incluso y les he contestado negativamente. Me han dicho que es un proyecto entre policías o miembros de agencias de inteligencia para introducirse en la red y buscar información de forma no autorizada, el espionaje a través de Internet.

Yo asisto, por suerte o por desgracia, a muchas reuniones internacionales y nunca he oído esa palabra en ningún proyecto ni en ninguna iniciativa para la creación de una organización de ese tipo, como es lógico por otra parte. Por tanto, soy el primer sorprendido. Existen conceptos como «InfoWord» y otros. Todos los servicios de inteligencia utilizan Internet como una fuente abierta. Muchas veces se obtiene más información por Internet que por los procedimientos clásicos. En lugar de acudir a una biblioteca se acude a Internet para conocer por ejemplo dónde se encuentra la Embajada de China en Prístina, en Kosovo. Por tanto, se utiliza por todos los servicios de inteligencia hasta donde conozco. Estados Unidos sobre todo es uno de los pioneros y se usa fundamentalmente como una forma de ataque hacia un determinado país para conocer las vulnerabilidades que tiene desde el punto de vista de redes informáticas. De esto se habla en las reuniones internacionales.

En cuanto a un tribunal internacional, he de decirle que a mí me gusta empezar la casa por abajo. La realidad es ésta. La legislación está ahí. Creo que el Cuerpo Nacional de Policía tiene seis miembros dedicados a esto específicamente, y nosotros somos también seis personas para todo el territorio nacional. En total, doce, dependiendo de dónde se reciba la denuncia y de dónde se tramite. Ya les he contado que nosotros siempre vamos con la maleta a cuestas. Estamos por todo el territorio nacional: hoy estamos aquí y mañana allí.

Hasta ahora no tengo ninguna queja de ningún juez; todo lo contrario. Lo único que he encontrado ha sido ayuda, pero comprendo que muchas veces es difícil entender, para cualquier persona e incluso para mí, lo que se ha producido en el mundo cibernético. Quizá esa fiscalía o alguien que conociese este tipo de delitos de una forma más especializada sería algo muy conveniente. Sé que en Noruega y en otros países existe. Es simplemente una propuesta.

¿Por qué estamos desbordados? Desde que empezamos hemos intervenido en 305 casos en todo el territorio nacional —hablamos de tres años de servicio—, en los cuales se han intervenido, no ya en un hecho que haya sucedido en una provincia, sino en hechos que tienen lugar en más de una Comunidad Autónoma, que es el ámbito de actuación de nuestra Unidad. Ahora, la Guardia Civil va a impartir un curso para cada miembro de la Policía Judicial de cada provincia. Van a asistir a un curso que nosotros vamos a dar, es decir, que vamos a llevar a cabo una formación interna de nuestros miembros, pero hasta ahora la única unidad especializada dentro de la Guardia Civil era la nuestra, con lo cual, si tiene lugar un caso en Asturias, en Palma de

Mallorca, tienes que reunir todo ese tipo de actividades e ir tanto al juez como al fiscal a contarles lo que ha ocurrido, y muchas veces, como no está claro el partido judicial donde comienza el hecho, se sufren esos retrasos y se dan esas inhibiciones en otros juzgados, y tienes que ir a otro juez a contarle el caso, e insisto en que somos doce personas para todo el territorio nacional. Estamos totalmente desbordados.

Cuando empezamos, recibíamos a través de la página web de la Guardia Civil del orden de dos o tres correos electrónicos al día de gente informando sobre casos, sobre hechos que ellos consideraban delictivos, y ahora recibimos una media de 35 ó 40 todos los días. Son 35 ó 40 mensajes que hay que canalizar, muchos de los cuales pueden ser considerados denuncias, y respecto a los que hay que hacer gestiones.

¿Haría falta más gente? Pues sí. ¿Cuánta más? No lo sé. Lo que sí quiero hacer es exponer lo que ocurre en otros países —y contesto ya a una pregunta anterior—. Para mí, Holanda es el país más desarrollado desde el punto de vista policial en este tipo de medios. ¿Cuál es su estructura policial? Ellos tienen unidades especializadas en delitos informáticos en cada región. ¿Por qué? Pues yo creo que su sociedad lo demanda. Y también es cierto que, en el terreno pericial, no existe un centro de investigación y criminalística dentro de la Policía o de cualquier otro grupo policial que coordine las actividades. Han creado un centro de peritajes tecnológicos —desde mi punto de vista, es el mejor de Europa—, dentro del Ministerio de Justicia, que es el que tiene que aportar esos peritajes, con lo cual se evita que los recursos se difuminen entre diferentes estructuras y se concentren en una organización que debe estar, entre otras cosas, para eso. Ya atienden ese tipo de casos en todo el territorio. Para mí es un ejemplo muy bueno.

Legislación. Ya he dicho que, estudiando la de otros países a la que he tenido acceso, he podido observar que hay países que optan por unas legislaciones muy específicas, creando leyes especiales, y otros que incluyen los delitos dentro del Código Penal General. España ha optado por esta última opción. A mí me parece estupendo, y no me quejo en absoluto de la legislación. Me parece que es de las más completas que he encontrado. Lo que sí creo que se queda bastante atrás es el procedimiento, las leyes procesales de colaboración, tanto a nivel nacional como internacional. Ya he mencionado la cuestión del partido judicial. El hecho de que ya un juez, que me parece muy respetable —y entiendo que en los delitos normales es esencial para el día a día—, se plantee, para un caso de este tipo, si es o no competente, y con toda la razón del mundo, me parece que sólo lleva a que, en un determinado momento, lo único que haga sea retrasar el procedimiento. Sobre todo porque lo importante es investigar, cuando no se sabe el origen del ataque o de la acción, dónde se ha producido el resultado. La mayor parte de los jueces actúan sobre el caso pensando que van a llevar el procedimiento, pero después, cuando se ubica el origen del ataque, se inhiben. Me parece muy bien, pero eso a veces plantea retrasos en el procedimiento. Me parece que hay que hacer un esfuerzo fundamental en la Ley de Enjuiciamiento Criminal, por ejemplo, o en las leyes procesales de colaboración, tanto a nivel nacional como internacional.

Sería interesantísimo un acuerdo o convenio internacional. Le voy a poner un ejemplo claro. En ese grupo de trabajo de Interpol se ha establecido un acuerdo entre los países, de tal forma que si el procedimiento normal de Interpol es que yo necesito algo de Holanda y lo mando a Interpol-Madrid, que es un servicio, Interpol-Madrid lo manda a Interpol-La Haya e Interpol-La Haya lo manda a la policía correspondiente —éste es un procedimiento muy lento—, en ese grupo de trabajo, para estos delitos, se ha establecido un procedimiento directo entre unidades. Se ha adoptado un determinado formato y nos mandamos mensajes entre nosotros. Este sistema, por supuesto, no es óbice para evitar el procedimiento habitual. Cuando hace falta recoger una prueba o que se despache un procedimiento se utiliza el habitual. En el caso concreto que les estoy comentando de Holanda, nosotros con ese fax le dijimos a la empresa que guardara esa información y que no la destruyera porque posteriormente vendría una solicitud judicial internacional sobre este tema. Para pedir eso no hace falta esperar tres meses de papeleo, sino simplemente mandar un fax. Creo que en el mundo judicial se podría hacer algo similar en el ámbito internacional. Se podría acordar un procedimiento para que en estos asuntos un juez pudiese pedir colaboración internacional a otro juez de otro país para que simplemente se reserven las evidencias y, posteriormente, se pidieran por el cauce habitual, pero por lo menos que se soliciten una serie de medidas cautelares que son esenciales en este tipo de procedimientos.

Por lo que se refiere a las tarjetas de crédito, creo que, por comentarios con personas que están dentro del mundo financiero, lo que ocurre es lo siguiente. Cuando uno va a un supermercado y paga con su tarjeta Visa, hay una señorita que le pide el carné de identidad a una persona y comprueba la firma —en el sistema informático eso se denomina terminal punto de venta—. Hay un terminal punto de venta donde se pasa la tarjeta de crédito y es un sistema nacional e internacional porque está así establecido. Lo lógico y lo ideal es que si yo tiro mi papelito no figure en él el pin o el dato concreto que solamente conozco yo. Lo que ocurre es que han incorporado ese sistema informático a Internet sin mayores medidas de seguridad. Esto quiere decir que en ese procedimiento de Internet, con una tienda virtual, no existe una señorita que le pida a uno el DNI, sino simplemente se pide Visa —u otra tarjeta— y fecha de caducidad y, si hay fondos, se autoriza la transacción.

Hay iniciativas para trabajar en sistemas de clave pública, de sistemas de encriptación que permitan que eso vaya con medidas más seguras, pero a mí me da la sensación, por comentarios que yo he oído, de que a estas empresas les resulta más rentable hacer frente a todos los problemas que surgen por reclamaciones. De hecho, el señor de Almería que yo les comentaba no pierde su dinero, porque lo recibe de Visa; la que pierde es la empresa que sirve el material informático. Visa u otras empresas pagan por ese tipo de problemas. Eso creo que les resulta más económico que modificar su sistema informático y su sistema de seguridad. Ésa es la cuestión, porque si a través de Internet

aparte de pedirme mi Visa y mi fecha de caducidad me pidiesen simplemente un código de cuatro dígitos que me han enviado en una carta reservada a mi casa se evitaría que por tirar un papelito al suelo se pudiese dar este tipo de casos. Ésa es mi opinión particular.

En cuanto a las universidades, les he comentado que la Guardia Civil celebró la primera conferencia internacional sobre delitos cibernéticos en 1996, en Barcelona; hace dos años, en Mérida, y el año pasado en Santander —este año se va a hacer otra conferencia internacional—. Se invita a miembros de la judicatura, del Ministerio Fiscal, de las universidades, y estamos en pleno contacto, porque entendemos que nuestra labor es policial. Nosotros no somos técnicos en informática, sino miembros de la Policía Judicial que llevamos a cabo investigaciones, y para ello debemos apoyarnos en un técnico que nos da información de cómo actuar y dónde podemos mostrarle al juez que han existido evidencias sobre un hecho delictivo y, por tanto, estamos haciendo cursos específicos para ello. Yo no necesito en mi unidad un guardia civil que sea ingeniero de telecomunicaciones, no me vale si no está dispuesto a viajar, si no está dispuesto a trabajar en equipo y si no tiene unos conocimientos básicos de investigación policial, porque el trabajo en Internet es un 25 por ciento y el trabajo en la calle es un 75 por ciento. Ésa es la realidad.

Colaboración con las universidades toda, porque sin ellos no hacemos absolutamente nada, porque hace falta que un profesor de universidad me diga lo que es un «sniffer» para yo explicárselo a un juez.

Por ejemplo, en el caso de las requisitorias judiciales, la Guardia Civil tiene una base de datos; la Policía Nacional, dispone de otra; la Ertzaintza, también, y tenemos que ponernos de acuerdo en los sistemas operativos, como en todo lo demás, para ver cómo podemos comunicarnos esos datos, a pesar de que esas órdenes parten de los juzgados. Por tanto, me pregunto por qué los juzgados no tienen un sistema informático que les permita dar directamente de alta y de baja las requisitorias. Y lo mismo ocurre con los delitos informáticos. En Holanda, por ejemplo, el Ministerio de Justicia tiene un departamento de peritajes tecnológicos al que acude tanto la Policía, como todos los medios e instituciones, por ser el referente nacional.

Para finalizar, insisto en que la legislación española es estupenda. Creo que en su momento el legislador hizo un trabajo magnífico, que es totalmente comparable al de otros países, porque he podido consultar otras legislaciones y eso es así. Sin embargo, como digo, en otros países se dan más competencias a los miembros de la Policía Judicial para facilitar su trabajo. Y con ello no estoy diciendo, por supuesto, que se pidan más competencias de las que nos corresponden, pero en otros países el ser miembro de la Policía Judicial tiene un determinado valor; por ejemplo, la firma de un oficial de la Policía Judicial en Francia en algunos casos —y digo en algunos— tiene más valor que mi propia firma en España.

Muchas gracias.

El señor PRESIDENTE: Gracias, Capitán Del Moral.

Aunque algunas de las preguntas ya han sido respondidas, estoy seguro de que don Carlos García podrá aportar interesantes reflexiones a las cuestiones planteadas por los portavoces.

Tiene usted la palabra.

El señor GARCÍA RODRÍGUEZ (Jefe del Grupo de Delitos Informáticos de la Brigada de Delincuencia Económico-Financiera de la Unidad Central de Policía Judicial): Gracias, señor Presidente.

Voy a centrarme en algunos detalles de las preguntas que se han formulado. Evidentemente, mantenemos una colaboración, aunque todavía escasa, con las Comunidades Autónomas, por lo que sus representantes acuden a nuestros congresos y conferencias, etcétera. Como es lógico, nosotros tenemos una experiencia acumulada de muchos años, y desean contactar con nosotros con el fin de que les aconsejemos, tanto en el terreno de la formación, como en el operativo.

Existe un proyecto en firme, denominado Falcone, que se lleva a cabo con las policías de otros países, con los Mossos d'Esquadra y con la Universitat Oberta de Catalunya. Se trata de un proceso ambicioso, para el que ya se está elaborando el material didáctico, de forma que en el futuro, y a través de Internet, se podrán impartir unos cursos de formación a escala nacional para todos los funcionarios del Cuerpo Nacional de Policía. De esa manera podremos tener esa estructura, tanto central como periférica, y en cada jefatura superior y comisaría provincial existirán funcionarios de la Policía Judicial —de hecho ya existen, porque han acudido a cursos de formación específica— que recibirán un curso más amplio para acceder a un campo virtual en Internet y seguir cursos de formación, mantener debates, plantear consultas, etcétera. Creo que será una experiencia muy positiva en la que también estarán presentes las policías de las Comunidades Autónomas.

En cuanto al proyecto Infopol, ciertamente, está rodeado de un halo de misterio y es una pregunta obligada en todas las entrevistas realizadas en los distintos medios de comunicación. La gente está alarmada con ese proyecto, pero ya he dicho en muchas ocasiones que la alarma producida por el hecho de que la policía pueda interceptar las telecomunicaciones sin una orden judicial —como algunos exponen maliciosamente en distintos foros y en conversaciones interactivas en «chat» en Internet— está muy alejada de la realidad.

Nuestra Constitución, como norma fundamental, exige que todo lo que signifique una privación de los derechos fundamentales esté autorizado y fiscalizado por los órganos judiciales. Es decir, por esa vía no se podría acceder a un entorno cerrado con el fin de averiguar una serie de datos que afectan a la privacidad. La Policía sólo trabaja en entornos abiertos, por lo que accede a Internet, como fuente de información pública que es, al igual que puede hacer cualquier otra persona.

El proyecto Infopol se basa en una Resolución de 17 de enero de 1995; se publica en el «Boletín Oficial de las Comunidades Europeas» el día 4 de diciembre de 1996. Creo

que está muy claro lo que pretende esta norma. Si su señoría quiere, le proporcionaré con mucho gusto el texto.

Hay también un borrador del proyecto Infopol del año 1998 elaborado por el Consejo de la Unión Europea y fechado en Bruselas el día 3 de septiembre, durante la Presidencia de Austria, en el que se viene a decir lo siguiente: el Consejo de la Unión Europea ha adoptado esta Resolución. El Consejo toma nota de que, debido a la continua evolución de la tecnología de las telecomunicaciones, también han cambiado los requisitos de las autoridades competentes hacia los operadores de redes y proveedores de servicios con el fin de la interceptación legal de las telecomunicaciones tal y como se describe en la Resolución de 17 de enero de 1995.

Creo que lo que se pretende con ello es tener canales ágiles de solicitud de información hacia los operadores de red y hacia los proveedores de acceso a Internet. Es decir, se pretende, ni más ni menos, que se regule de qué manera y en qué extensión estas instituciones, estas empresas privadas tienen que facilitar esa información —que a su vez conviene que se regule, ya lo hemos apuntado— puesto que no se puede actuar en el terreno personal de la buena voluntad de los operadores para que éstos proporcionen información. Es decir, se regulan de una manera bastante detallada los requisitos, las obligaciones y la conservación de los datos que deben realizar esos operadores para facilitar en su día —eso sí, con las correspondientes autorizaciones judiciales— esa información.

En cuanto a la creación de una fiscalía, me parece una idea muy positiva. Se podría avanzar mucho centralizando en ella toda la información, todas las investigaciones, todo ese contacto con las autoridades judiciales a igual nivel para hacer prosperar todo tipo de actuaciones.

Respecto de la cobertura jurídica, creo que no debo extenderme más en lo que ya he dicho. Contamos con un respaldo legal, con una cobertura para perseguir todo ese tipo de conductas en el ámbito nacional. En lo que al ámbito internacional se refiere, hay que armonizar muchas legislaciones, pero tal vez el aspecto que más interesa es el adjetivo, el aspecto procesal.

Nosotros utilizamos dos vías: el auxilio policial y el judicial. Si queremos tener información sobre un determinado usuario, sobre una determinada conexión a Internet, podemos solicitar la vía del auxilio policial a través de Interpol, pero en la mayoría de los países se nos va a solicitar una comisión rogatoria internacional. Pues bien, por esa vía adelantamos a esas empresas establecidas en el extranjero que congelen, que guarden esa información hasta que les llegue la oportuna autorización judicial. Eso lo podemos hacer por esa vía, que es más rápida, cursando más adelante la petición al juzgado competente en esos hechos para que tramite por vía diplomática —que es algo más compleja y, desde luego, más lenta— la comisión rogatoria internacional.

En cuanto a las inhibiciones de los jueces, lo he comentado porque es una realidad cotidiana en nuestra Unidad que, por tanto, entra dentro de la normalidad. En algunas ocasiones podría decirse que eso es injustificable —se trata de meras opiniones que podrían comentarse—, pero es evidente que se trata de cuestiones de competencia, de reglas de competencia.

En virtud de una denuncia, o por propia actuación de oficio, nosotros iniciamos una investigación. Pues bien, después de dar conocimiento de los hechos y de solicitar unas diligencias se nos da autorización, por ejemplo, para que un proveedor nos facilite información sobre esa conexión, pero resulta que ese usuario implicado está en otra provincia. En ese momento, ese juez ya se inhibe en favor de ese juzgado y, además, sucede que en ese trámite judicial pueden pasar meses. De momento, las investigaciones en curso están pendientes de que otro juzgado recoja las diligencias previas abiertas y conceda lo solicitado; son muchas las investigaciones que están en ese trámite.

A título anecdótico, le contaré un caso concreto. Enviamos unas diligencias a un juez de Madrid, que las remitió a otro de Barcelona —y en ese detalle no quiero entrar—; el responsable de allí estuvo hablando con el juez —yo acostumbro a hablar con los jueces para explicarles la situación, aunque comprendo que son investigaciones complejas— y éste otorgó una diligencia, pero el usuario ya estaba en Ceuta y se la ha enviado allí. Como pueden imaginar, todo ese trámite ha dado lugar a que el asunto se demore durante varios meses. Finalmente, ha llegado por otra vía a la Audiencia Nacional, que será la que recabe esa competencia. Entre tanto, el usuario está identificado y no podemos avanzar en las investigaciones ni concluir la operación a pesar de ser un delito de tanta trascendencia como es la pornografía infantil.

La dotación de recursos —como he dicho antes— tiene que hacerse de una manera decidida e inmediata. Los recursos son mínimos, ahora están aumentando en la Unidad pero todavía son insuficientes. En muchas ocasiones he expuesto un posible proyecto: la creación de una Unidad de Internet, que contaría con una unidad central y sus periféricas; estaría compuesta por una unidad operativa, encargada de hacer las labores propias de policía judicial, es decir de investigación, con el apoyo técnico de áreas de informática y telecomunicaciones y, a la vez, de ese órgano administrativo que es de gran interés para poder dar respuesta a esa servidumbre que tienen las nuevas tecnologías: reuniones internacionales, entrevistas, conferencias e intervenciones que se hacen desde un punto de vista no exclusivamente operativo. Ya se ha puesto de manifiesto la cuestión de la colaboración con las universidades. Nosotros mantenemos una buena relación con las universidades; hemos llevado a cabo investigaciones en dichas instituciones, y nuestra actuación ha sido ágil y positiva.

En cuanto a la legislación internacional, he de decir que sería necesario armonizarla, aunque entiendo que es complicado. Se pide que se pongan de acuerdo todos los países, pero estamos hablando de la soberanía nacional, de la legislación de distintos países, lo cual hace difícil llevar a la práctica dicha propuesta.

Nada más. Quedo a su disposición.

El señor PRESIDENTE: Muchas gracias, señor García Rodríguez.

¿Alguna de sus señorías desea intervenir? *(Pausa.)*

En tal caso, hemos de darles las gracias. Era imprescindible la comparecencia del Cuerpo Nacional de Policía y de la Guardia Civil en esta Comisión Especial de estudio sobre Redes Informáticas. Sin duda, las intervenciones de ambos comparecientes justifican esa necesidad.

Estoy seguro de recoger el sentir de la Comisión si animo al Cuerpo Nacional de Policía y a la Guardia Civil a proseguir en este trabajo tan difícil, pero tan necesario ante el incremento de la actividad —para bien y para mal— en el ámbito de las redes informáticas, teniendo en cuenta los problemas que conlleva la investigación de este tipo de delitos.

Nada más, gracias a todos, gracias a los servicios de la Cámara, buenos días.

Se levanta la sesión.

Eran las catorce horas.