

**COMPARECENCIA DE LA EXPERTA EN INNOVACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN, DÑA. SALUD MARTÍNEZ MONREAL, ANTE LA PONENCIA CONJUNTA DE ESTUDIO SOBRE LOS RIESGOS DERIVADOS DEL USO DE LA RED POR PARTE DE LOS MENORES, EL DÍA 10 DE MARZO DE 2014.**

La señora **EXPERTA EN INNOVACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN** (Martínez Monreal): Buenas tardes; muchísimas gracias, señor presidente. Antes que nada, quiero agradecer a todos los miembros de la ponencia la oportunidad que me dan para explicar una solución al problema que en esta ponencia y en todo el mundo se viene planteando desde hace años. Es gratificante para mí poder explicar hoy que ya existe una solución real.

Les voy a poner una diapositiva muy concreta que va a ser el pilar – ahí la tienen– de mi ponencia. Imagínense por un momento que cualquier usuario de cualquier parte del mundo, con su terminal móvil, tableta o PC pudiera obtener una información que quedara custodiada, encriptada, que tuvieran acceso cualquier cuartel o comisaría de la policía, y que paralelamente pudiera descargar esa prueba veraz en un juzgado. Ahí tenemos unos eslabones que son fundamentales a día de hoy para el descubrimiento o el esclarecimiento de un hecho delictivo.

Ahora mismo los menores, digamos que son los reyes de los *smartphone*. Básicamente, casi todos los delitos giran en torno a un *smartphone*, a una tableta y a las redes sociales. No quiero entrar ni voy a entrar en ese tema porque ya mis predecesores anteriores les han puesto en tela de juicio, con millones de estadísticas del aumento que hay de delitos cada año.

Yo vengo a presentarles esta solución, que además contiene un algoritmo innovador, con una patente internacional, que certifica el contenido de la información que se obtiene; el contenido, que es el punto clave, el punto principal, que es lo que a un policía le interesa, a un juzgado le interesa a la hora de detectar un delito y comprobar, por supuesto, si es veraz o no lo es.

Mis predecesores en las anteriores ponencias ya les han indicado suficientes estadísticas en cuanto al incremento de delitos en la red y sus diversas tipologías. Es por ello que yo les voy a hablar de una solución con óptimas estadísticas que nos reporta la innovadora tecnología que hoy les presento. El Senado tiene la capacidad de contribuir a hacer una sociedad mejor, y es por ello que les voy a hablar de esta solución; es una solución global, una plataforma compuesta de un algoritmo, tecnología y *software* que certifica el contenido de la información que se obtiene. Porque no es manipulable por ningún usuario malintencionado. Esta información la podemos extraer a través de una web, de una fotografía, una vídeo, un audio, y nos aporta pruebas con el contenido visual y técnico. Esta es una parte muy importante y relevante, porque obtenemos pruebas técnicas (en cuanto a IP, etc., que ahora comentaremos) en una web, y la prueba visual, in situ y simultánea de lo que está ocurriendo en ese momento.

Esta tecnología, confeccionada en una plataforma transaccional que acoge la colaboración entre países para la agilización de pruebas veraces para la investigación policial y jurídica en la erradicación de todos los delitos en cualquiera de sus formas. Este *software* específico, creado con esta innovadora tecnología para usuarios particulares, para centros educativos, para las Fuerzas y Cuerpos de Seguridad del Estado y para los juzgados. *Software* que proporciona en sí mismo formación jurídica para profesores, alumnos y familias.

Internet es parte de la vida de todos los usuarios, de las empresas, de las instituciones y de los delincuentes, con la que se crea una relación entre sí de intercambio de un gran flujo de información a diario. Las redes sociales nos proporcionan una nueva forma de comunicación beneficiosa o nociva, según se utilicen, eliminando barreras temporales y geográficas.

Cuando ofrecemos información personal atentamos de forma totalmente inconsciente contra nuestra propia intimidad, por la gran desinformación en el uso de las nuevas tecnologías por parte de los usuarios. Pero tampoco podemos pretender que todos los usuarios se conviertan en expertos de las tecnologías. Pero sí es posible que adquieran unos conocimientos mínimos sobre las mismas y nuevas herramientas para su defensa, que hasta el día de hoy no las había, al menos que aportaran información veraz.

Dado que los usuarios no saben de tecnología, creé un sistema de *software* fácil, accesible y con un funcionamiento con el que se obtienen pruebas visuales y técnicas de lo que está ocurriendo en la red, con lo que el usuario puede demostrar su verdad, la policía tiene pruebas veraces para comenzar su investigación, y los juzgados tienen la carga de prueba.

La innovación de este *software* para el usuario: creadas las aplicaciones ENOCH, MOISÉS Y THOR como herramientas para los usuarios, y creados los *softwares* FCSE para las Fuerzas y Cuerpos de Seguridad del Estado, e IUS para los juzgados, con esta innovadora tecnología, a través de la que pueden ver y descargar la información (pruebas) de los usuarios que ponen su denuncia certificada y contenido veraz con esta tecnología.

Esta tecnología agiliza los trámites de investigación, de usuarios, policías, jueces, y repercute directamente en educación.

Esta tecnología está disponible a día de hoy.

La información certificada obtenida por estas herramientas: datos de prueba, desde cualquier PC, móvil o tableta, con un solo clic se obtiene la información visual y técnica del suceso. Al enviarla a su panel de administrador llegan dos documentos: uno con los datos técnicos y otro con los datos visuales.

En cuanto a los datos técnicos que obtenemos: código de denuncia, la IP de donde se ha producido el hecho, la descripción de la denuncia (fecha y hora en la que se obtiene, fecha y hora a la que se envía, fecha y hora en que se queda encriptado el archivo de la prueba capturada, que puede ser un archivo audio, foto, vídeo o web), la latitud y la longitud, los datos del usuario (DNI, nombre, etc.), entre otros datos relevantes que únicamente pueden estar al alcance de policías y juzgados que son relevantes para sus investigaciones.

Las estadísticas obtenidas de centros educativos en el año 2012-2013: hay un gran número de centros educativos que vienen todavía negando este tipo de problemas como el acoso, ciberacoso, difamación, venta de drogas, etc., y esto es un gran error porque tarde o temprano, si no se pone una solución, estos problemas acaban saliendo a la luz, como está ocurriendo a día de hoy: suicidios, abusos sexuales, etc. Y lo que se podía haber evitado, ya no tiene marcha atrás.

El foco está en los centros educativos, y es en los centros donde ha de impartirse esta herramienta de defensa para formarles en una navegación responsable pero con libertad y de forma segura. ¿Por qué? Porque por muchas prohibiciones que a día de hoy hagamos a un menor, si no será desde su casa será desde la casa del amigo o será desde la casa de quien sea, entrará a la página que quiera. Pues de este modo los alumnos aprenden a detectar, con esta herramienta, a prevenir, y en última instancia a defenderse de una conducta delictiva por parte de un usuario malintencionado, o de un delito.

La mayor problemática de incidencias radica en la gran desinformación por parte de los menores y sus tutores sobre qué es un delito en la red o lo que no lo es; y la falta de formación, y en cuanto a conocimientos mínimos para la navegación por la red.

Durante los doce años de investigación previa a la creación de este *software* observé la necesidad de proporcionar, junto con la herramienta de defensa, un material formativo adecuado para menores y sus tutores, en el cual se les indican las conductas más habituales de tipo delictivo en la red, con el fin de disminuir los casos de víctimas. Proporciona formación jurídica en nuevas tecnologías, en el uso de las redes sociales, tanto a profesores como a los alumnos y sus familias; los forma en la utilización de nuestro *software* Moisés para la obtención de las pruebas. De este modo los menores, los tutores y los padres aprenden a detectar, prevenir, y en última instancia a poder defenderse, poder denunciar con pruebas visuales y técnicas, el suceso.

El éxito que ha tenido en estos dos años esta herramienta, y en este último año 2012-2013, es el siguiente: hemos tenido a padres y alumnos informados sobre los riesgos de Internet, las penas que conllevan dichos delitos y cómo defenderse; toma de conciencia de los menores del daño psicológico que podrían estar ocasionando a los compañeros, y los riesgos a los que se exponen navegando y entrando a webs nocivas. Aprenden materia jurídica sobre los delitos en Internet, y cómo castiga la ley con su Código Civil y su Código Penal, etc., el *grooming*, el *sexting*, el *cyberbullying*, incitación al suicidio, estafas electrónicas, protección del derecho al honor, etc., propiedad intelectual, *phishing*, *pharming*, muy importantes, contratos falsos por Internet, LOPD, *spam*.

Los alumnos dados de alta en el centro encuentran asistencia psicológica, pudiendo estos entablar comunicación directa a través de su panel, el panel que les proporciona Moisés desde su administrador,

directamente con el orientador de su centro, evitando así las barreras de comunicación que se producen en la adolescencia a la hora de contar algún problema personal cara a cara.

Acuerdos entre los padres y los centros antes de llegar a una situación grave con las pruebas que le proporciona Moisés, ya que el centro en sí mismo en ocasiones no es responsable del acto, sino el alumno o tutor que lo comete.

Disminución de las incidencias por parte de los menores en las redes sociales, y una navegación más responsable, en aquellos alumnos a los que les han impartido en clase este material didáctico-jurídico.

La falta de confianza en el seno familiar es complementada por Moisés. Los menores saben que, en el momento en que se vean en algún problema, pueden obtener esta información con tan solo un clic, que pueden decidir trasladarla, si lo necesitan, a la policía, a sus padres, a sus tutores, y resolver qué van a hacer con ella.

Ha sido una gran solución también para tutores, debido a las situaciones límite que están viviendo de acoso por parte de los alumnos.

Ahora les voy a contar las soluciones policiales y jurídicas en cuanto a tecnología forense en las que se aplica este algoritmo. Hasta el día de hoy no existía ningún modelo o método capaz de obtener una prueba y conservarla sin que existiese la posibilidad de manipulación. Hasta el día de hoy los mecanismos utilizados por la tecnología forense no pueden certificar que las pruebas obtenidas de un componente electrónico son veraces y no introducidas previamente por un usuario malintencionado, entendiendo que una prueba crucial para el esclarecimiento de un hecho puede ser introducida intencionadamente culpando a un inocente.

El área pericial que abarca, entre otras: delitos informáticos, propiedad intelectual, medios de pago, pornografía infantil, autenticación de *e-mails*, técnica criminalística y obtención de pruebas en las redes TOR.

La técnica criminalística o forense se ocupa del conjunto de medios y métodos científico-técnicos que se utilizan durante la investigación de los delitos a los fines del descubrimiento, fijación, ocupación e investigación de los distintos elementos, indicios, materiales o evidencias físicas halladas en el lugar del suceso o durante la realización de la inspección o de cualquier otra acción de instrucción que conlleve la búsqueda de estos elementos.

MSM Technology ofrece la garantía del contenido de la información, prueba, obtenido durante toda la cadena desde que el usuario la obtiene hasta requerimiento judicial.

El éxito obtenido en esta cadena: primero, se obtiene información veraz; segundo, obtenemos carga de prueba visual y técnica; tercero, ahorro para la administración en tiempo y costes económicos; cuarto, que el coste emocional de las víctimas sea el menor posible, algo que paralelamente repercute en un bien mayor en toda la sociedad; cinco, un uso ejemplar y responsable de las nuevas tecnologías y la seguridad de la información, adaptadas a policía y justicia, repercutiendo directamente como ejemplo para toda la sociedad a nivel internacional; seis, refleja socialmente una toma de contacto directa sobre la conciencia de los ciudadanos en la obtención, presentación de pruebas y sus consecuencias; siete, en delitos transaccionales se obtiene la carga de prueba visual y técnica que puede ser anticipada a otros países con los que se esté en colaboración mediante acuerdo firmado.

Esta tecnología custodia las pruebas vírgenes encriptadas con las que un ciudadano de cualquier parte del mundo demuestra lo que le está ocurriendo, avisando a las fuerzas y cuerpos de seguridad, pudiendo así solicitar ayuda a su país, en el caso de estar en el extranjero, si lo necesita.

Colaboraciones mantenidas hasta el día de hoy: el usuario es el propietario en todo momento de su información. Nuestro sistema ofrece la

posibilidad de que el usuario decida compartir dicha información, colaborar, dada la situación del aumento de delitos año tras año. Por ello, pensando en la petición que tanto solicitan las Fuerzas y Cuerpos de Seguridad del Estado instando a la colaboración ciudadana y a empresas del sector, el *software* contiene un botón “Aviso” para avisar, si el usuario lo desea, sobre webs nocivas, ciberacoso, pornografía infantil, *grooming*, etc., terrorismo, ciberterrorismo..., con pruebas visuales y técnicas. En definitiva, ayuda o colaboración *online* sobre cualquier delito telemático con pruebas veraces simultáneas al suceso, contribuyendo así cada usuario a crear una red más sana y segura.

La aplicación de Moisés, conocida como Wave System S.O.S., colabora con el Grupo de Delitos Telemáticos de la Guardia Civil con el acuerdo firmado desde el 13 de febrero del año 2012; la Brigada BIT de Delitos Tecnológicos de la Policía Nacional fue informada de esta tecnología al mismo tiempo, no accediendo a dicha colaboración y servicio ciudadano.

Los resultados obtenidos por esta tecnología, la veracidad de la información obtenida, las ventajas en educación y formación, las ventajas de toma de conciencia sobre las nuevas tecnologías, las ventajas policiales, las ventajas jurídicas y las ventajas transaccionales han quedado más que demostradas.

Tras dos años de colaboración con el Grupo de Delitos Telemáticos de la Guardia Civil en la recepción de las incidencias de los usuarios, y habiendo informado a Policía Nacional, como antes he mencionado, la propia secretaría de Estado publicó el 23 de junio de 2013 en Europa Press la noticia de una herramienta llamada SIMACS, aún sin desarrollar. Con dicha aplicación, el señor Francisco Martínez Vázquez, secretario de Estado de Seguridad, desde mi punto de vista parece que pretende apropiarse de estos éxitos obtenidos durante dos años de duro trabajo, doce



años de mi investigación y mi grandísimo esfuerzo para realizar la puesta en marcha de esta innovadora tecnología como emprendedora.

La innovación que les he expuesto como solución fue presentada en la Unión Europea en el año 2009, la cual fue aprobada por todos los países miembros para su licitación en el programa SAFE, al cual no pude optar entonces por no ser empresa. Siempre he trabajado a contrarreloj para solucionar la problemática mundial en ciberdelincuencia y sabiendo que este *software* evitaría que más menores se convirtiesen en víctimas de acoso sexual, pornografía infantil, *cyberbullying*, difamación, suicidio, etc., en la red.

Lo positivo de todo esto a día de hoy es que es un hecho que existe esta solución, y ha quedado demostrado tras estos dos años la gran solución que reporta. MSM Technology dispone de toda la protección legal nacional e internacional en cuanto a su algoritmo y programas informáticos, para la obtención de dicha información, su contenido y su tráfico en cuanto a *softwares* específicos protegidos para policías y juzgados.

Tengo una petición para sus señorías, con toda mi inocencia. Y mi petición es la elaboración de una ley. Durante los doce años de mi investigación para la conclusión de este algoritmo también me quedó una visión muy precisa de la gran necesidad de la creación de una única ley global en la que –disculpen mi ignorancia–, en mi opinión, deberían sentarse los magistrados, mandatarios de todos los países que quisieran cubrir esta necesidad, recogerían todas y cada una de las leyes que castiga esta tipología de delitos de cada uno de los países participantes, y llegar a una comunión entre todas ellas –sé que no es fácil–, creando así un nuevo tratado internacional en defensa de los usuarios en Internet. Yo lo llamaría “tratado internacional Cyberlaw”.

Muchísimas gracias por escuchar mi exposición, y podemos comentar las diapositivas que he traído o pasar a preguntas.