Al Juzgado de Guardia de Madrid

Miguel Ángel Gallardo Ortiz, con DNI 7212602-D, criminólogo e ingeniero especializado en seguridad informática-telemática y criptografía, en su propio nombre y derecho, y también como representante y presidente de la Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (**APEDANICA**) y administrador único de la mercantil Cooperación Internacional en Tecnologías Avanzadas (**CITA**), SLU, con teléfono 914743809, móvil 619776475 y domicilio para notificaciones en calle Fernando Poo, 16 Piso 6ºB, 28045 de Madrid, como mejor proceda comparece y presenta **DENUNCIA PENAL** por presuntos **delitos perseguibles de oficio** en base a los siguientes **HECHOS**:

PRIMERO.- Con fecha 11/06/2010 la edición digital del periódico **PÚBLICO**, con la firma de la periodista **BLANCA SALVATIERRA**, publica el titular "**Una ONG acusa a Google de "intención delictiva**" y las siguientes afirmaciones que consideramos extremadamente relevantes

Privacy International sostiene que los coches de Street View han infringido la ley en casi 30 países

*La organización Privacy International ha reaccionado con dureza al conocer el mecanismo con el que los coches Street View de Google captaban datos de las redes WiFi abiertas que encontraban en su camino. "**El estudio establece, más allá de la duda razonable, que Google tiene la intención de interceptar y almacenar sistemáticamente el contenido de las comunicaciones**", explica la ONG en un comunicado. La organización alega que, en consecuencia, **la compañía podría verse envuelta en enjuiciamientos penales en casi la totalidad de los 30 países en los que ha utilizado el sistema**.*

*Los detalles sobre la forma de captar los datos se han conocido a través de una auditoría externa encargada y hecha pública por la propia Google. En ella se detalla que el programa utilizado en los coches de Street View, que en apariencia sólo tomaban imágenes a pie de calle para ilustrar los mapas de la compañía, recogía el contenido que circulaba por las redes WiFi no protegidas y procedía a su almacenaje. **"La auditoría revela intención delictiva por parte de la compañía [...] Es el equivalente a colocar una grabadora en un teléfono sin consentimiento**", responde PI.*

La Agencia Española de Protección de Datos (AEPD) ha bloqueado los datos que captaron los coches de Google en España y los está analizando. Si su investigación administrativa demostrase que Google ha violado la ley, la Agencia impondría una sanción a la compañía. Las investigaciones que se están llevando a cabo analizan, entre otros aspectos, los procedimientos y métodos por los que han sido captados y almacenados los datos, así como su tipología y la finalidad para la que han sido recabados.

*"Si preparas una aplicación para la interceptación de datos, parece clara cuál es la intención. Es prácticamente imposible que Google no captara información de carácter personal", explica el abogado especializado en protección de datos Samuel Parra. Además de las sanciones que pudieran derivarse de la investigación de la AEPD, Parra establece una vía alternativa que hace referencia al **artículo 197 del Código Penal**. Este detalla penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses para aquel que "intercepte las telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o [...] de cualquier otra señal de comunicación". El abogado explica que cualquier ciudadano podría iniciar este procedimiento. **La fiscalía, por su parte, también podría actuar de oficio contra Google en el caso de hallar indicios de delito**.*

Importancia de la intención

*Para PI, aunque algunas legislaciones establecen un margen para captación de datos por error, la intención que supone haber creado este tipo de software es clara. **La organización añade que la interceptación de las comunicaciones sólo puede realizarse con una orden judicial. "Todo lo demás se considera ilegal", añade**.*

*Google siempre ha argumentado para defenderse que no había intención de delinquir, ya que ni siquiera tenía conocimiento de estos hechos. Según la compañía, un ingeniero introdujo sin permiso las instrucciones de recopilación de datos en el software de los coches, una situación incomprensible para el director de la AEPD, Artemi Rallo. "**Google no puede alegar un error tecnológico cuando es la principal empresa de tecnología del mundo**", declaraba días después de que el escándalo se hiciera público. Privacy International también duda de esta explicación, afirmando que **la captación de datos "va más allá del error individual que promueve Google"**.*

Mediante un escueto comunicado en su blog oficial, Google insiste en que la recopilación de datos se debió a un error y que continúan trabajando con las autoridades para dar respuesta a sus preocupaciones.

SEGUNDO.- Para profundizar en nuestro estudio crítico y pericial mediante la comprobación de las fuentes de la anterior noticia también hemos buscado en la Web www.privacyinternational.org encontrando en http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-566346

Google Wi-Fi audit reveals criminal intent by the company 09/06/2010

Google today published an audit on its blog of the code used to collect Wi-Fi data as part of the company's global Street View operation. The report asserts that the system had intent to identify and store all unencrypted Wi-Fi content. This analysis establishes that Google did, beyond reasonable doubt, have intent to systematically intercept and record the content of communications and thus places the company at risk of criminal prosecution in almost all the 30 jurisdictions in which the system was used.

The independent audit of the Google system shows that the system used for the Wi-Fi collection intentionally separated out unencrypted content (payload data) of communications and systematically wrote this data to hard drives. ***This is equivalent to placing a hard tap and a digital recorder onto a phone wire without consent or authorisation****.*

The report states: "While running in memory, gslite permanently drops the bodies of all data traffic transmitted over encrypted wireless networks. The gslite program does write to a hard drive the bodies of wireless data packets from unencrypted networks."

This means the code was written in such a way that encrypted data was separated out and dumped, leaving vulnerable unencrypted data to be stored on the Google hard drives. This action goes well beyond the "mistake" promoted by Google. ***It is a criminal act commissioned with intent to breach the privacy of communications****. The communications law of nearly all countries permits the interception and recording of content of communications only if a police or judicial warrant is issued. All other interception is deemed unlawful.*

Some jurisdictions provide leeway for "incidental" or "accidental" interception. However where intent to intercept is established, a violation of criminal law is inevitably created.

This action by Google cannot be blamed on the alleged "single engineer" who wrote the code. It goes to the heart of a systematic failure of management and of duty of care.

TERCERO.- Más relevante aún es el documento de 23 páginas en formato PDF publicado en http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//googleblogs/pdfs/friedberg_sourcecode_analysis_060910.pdf titulado "Source Code Analysis of gstumbler. Prepared for Google and Perkins Coie. Prepared by STROZ FRIEDBERG. June 3, 2010" por el que otros expertos en la materia, ya pueden llegar a la concluir que, en efecto, **sí pueden haberse cometido presuntos delitos tipificados por el artículo 197 del Código Penal en España**.

Por lo expuesto, al Juzgado de Instrucción se proponen las siguientes **DILIGENCIAS PREVIAS**:

PRIMERA.- Se requiera al Director de la **Agencia Española de Protección de Datos (AEPD)**, con sede en C/ Jorge Juan, 6. 28001 Madrid, Teléfono: 901100099 y 913996301 Fax: 914455699, toda la documentación e informaciones sobre los presuntos delitos que puedan haberse cometido, y que desde la misma notificación **mantenga puntual e inmediatamente informado al juzgado** de cuantos hechos relevantes vaya conociendo en relación a los presuntos delitos aquí denunciados.

SEGUNDA.- Que para auxiliar al juzgado instructor, se designen peritos funcionarios de oficio que queden a la disposición del juzgado tanto para interpretar la documentación requerida en la anterior, como para realizar cuantas otras diligencias el juzgado disponga, recomendando aquí a:

a) **Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI)** en Internet www.ccn.cni.es con sede en la Avenida Padre Huidobro s/n, 28071 Madrid, Tel. 913725000

b) **BRIGADA DE INVESTIGACIÓN TECNOLOGICA** de la C**OMISARIA GENERAL DE POLICIA JUDICIAL** del **CUERPO NACIONAL DE POLICIA** en C/ Julián González Segador s/n 28043 Madrid, Tel. 915822752 Fax. 915822756

c) **GRUPO DE DELITOS TELEMÁTICOS DE LA GUARDIA CIVIL** en C/ Guzmán el Bueno, 110. 28003 Madrid, Tel. 915146400. Fax. 915146402

d) **Departamento de Tratamiento de la Información y Codificación del Instituto de Física Aplicada del Consejo Superior de Investigaciones Científicas (CSIC)** en calle Serrano, 144. 28006 Madrid, Tel. 915618806. Fax: 914117651

así como en cualquier otra entidad de derecho público en la que funcionarios públicos tengan formación, experiencia y criterio para asumir responsabilidades periciales de oficio emitiendo opinión motivada sobre los hechos anteriormente expuestos y sobre cuanta documentación pueda tener acceso el juzgado en relación a posibles delitos cometidos por personal contratado por GOOGLE en España o por quienes tienen la función pública de vigilar, impedir y sancionar faltas, o de **poner en conocimiento de la autoridad judicial indicios racionales de criminalidad**.

Entendemos que **esta denuncia contiene datos y referencias suficientes** como para que los peritos funcionarios más expertos en la materia puedan pronunciarse o precisar qué más requieren para ello sin perjuicio de que se produzcan nuevas noticias sobre los hechos denunciados de notoria relevancia internacional, creciente interés general e incluso **ALARMA SOCIAL en varios países**.

y **TERCERA**.- **Que se cite en calidad de imputado, para la mejor defensa y garantía de sus propios derechos, al representante legal de la mercantil GOOGLE ESPAÑA con domicilio en Plaza Pablo Ruiz Picasso 1, C.P. 28020 Madrid, Tel.: 917486400, requiriéndole antes toda la documentación de que disponga sobre los presuntos delitos aquí denunciados.**

Por último, el denunciante y todos los recursos al alcance de las dos entidades a las que representa están permanente e incondicionalmente a la disposición del juzgado instructor, ofreciéndose para **ratificar esta denuncia con todas las explicaciones** que como técnico con amplia experiencia en conflictos tecnológicos e incluso como director de un curso de formación continuada en la Escuela Judicial del CGPJ (véase el Cuaderno de Derecho Judicial XI "**Ámbito Jurídico de las Tecnologías de la Información**" editado por el CGPJ en 1996, muy en especial por el prólogo e "**Informatoscopia y Tecnología Forense**"), también como profesor invitado en cursos de formación y perfeccionamiento de la Escuela Superior de Policía en Ávila (véase el artículo titulado "**Métodos de inspección legal de ordenadores e introducción a la informática policial**" publicado por la revista Ciencia Policial del Ministerio del Interior) y coautor del libro "**Seguridad en Unix. Sistemas Abiertos e Internet**" (Editorial Paraninfo 1996) y como autor de varias docenas de informes y dictámenes periciales presentados y ratificados en juzgados y tribunales.

Por lo expuesto, solicito al juzgado que, teniendo por presentado este escrito, se digne admitirlo y abra las diligencias previas propuestas así como cuantas otras más también considere oportunas.

Por ser de Justicia que pido en Madrid, a 13 de junio de 2010.

Miguel Ángel Gallardo Ortiz, con DNI 7212602-D, criminólogo e ingeniero especializado en seguridad informática-telemática y criptografía, en su propio nombre y derecho, y también como representante y presidente de la Asociación Para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (**APEDANICA**) y administrador único de la mercantil Cooperación Internacional en Tecnologías Avanzadas (**CITA**), SLU, con teléfono 914743809, móvil 619776475 y domicilio para notificaciones en calle Fernando Poo, 16 Piso 6ºB, 28045 de Madrid, y en Internet www.miguelgallardo.es www.cita.es/apedanica

Al Juzgado de Guardia de Madrid