INVESTIGACIÓN DE LOS METADATOS

Por Francisco Javier Pérez-olleros Sánchez-Bordona

Noviembre de 2014

Hoy en día es frecuente que en la investigación policial o instrucción de los delitos de violencia de género sea fundamental indagar en las comunicaciones de los sospechosos y de las denunciantes.

Es decir, investigar la fase preparatoria del delito y su ejecución a través del flujo de llamadas recibidas y emitidas, mensajes, geolocalización de los terminales mediante sus coordenadas GPS o mediante los nodos, correos electrónicos, entradas en servicios de internet, etc.

Por ejemplo para probar las injurias o calumnias que la expareja puede realizar mediante medios telemáticos o en medios de comunicación amparados en el anonimato que pueden otorgar las tecnologías de informática y comunicación, que permiten incluso el uso de un nombre supuesto o la suplantación de la personalidad de otra persona.

También podemos citar para ver la importancia de la huella digital en los delitos de violencia de género, a los delitos de acoso criminal, que además pueden ir dirigidos no sólo a la expareja, sino también a su familia, su nueva pareja y amigos, o compañeros de trabajo, y en los que es común que el acosador efectúe amenazas muy graves o inquietantes.

Estos delitos cometidos con medios informáticos o telemáticos, por la complejidad que conlleva la prueba electrónica y el aseguramiento en la cadena de custodia (que pasa por la realización de una copia exacta, o copia espejo, en presencia de un fedatario público, como puede ser un notario o el secretario judicial), requieren de una intervención temprana.

Así, en el supuesto del "acosador rechazado" o "resentido" que puede llegar a ser muy persistente, el acoso per se significa un modo de continuar la relación con la víctima, en la que está atrapado por la rabia o frustración que siente.

A lo anterior se puede añadir que muchos acosadores rechazados o resentidos se caracterizan por padecer anomalías de personalidad, y a menudo también, por ser individuos dependientes, narcisistas, con signos de sufrir paranoia y/o con algún problema de dependencia a substancias tóxicas.

El acoso cibernético y telefónico en la esfera social y personal de su víctima, ataca directa y en primer término la libertad y seguridad de la expareja, ya sea mediante actos que, aisladamente considerados no alcanzan relevancia penal, pero que, contemplados globalmente, afectan al desarrollo vital de la acosada, generándola desasosiego o miedo, pues en esa situación de incertidumbre, no se sabe qué es lo siguiente que puede o va a sucederle, pudiendo llegar a alterar su salud mental, y a la perdida incluso de su trabajo, o nueva relación afectiva, y puede desencadenar reacciones impredecibles en la misma.

En muchas ocasiones el problema para la víctima se encuentra en poder probar el acoso realizado por los citados medios telemáticos y su autoría. Un claro ejemplo de ello sería poder demostrar quién es el autor que colgó la foto de la víctima en Internet.

Esta prueba del delito y la autoría del mismo, requiere muchas veces la cesión de datos de las operadoras sobre las llamadas recibidas por la propia víctima en su teléfono, o la identificación de la IP desde la cual se produjo la entrada en el servicio de internet, o del correo electrónico.

En cuanto a las llamadas y mensajes recibidos por la propia víctima en su teléfono fijo o móvil, si los solicita a su operadora, le será denegada esta información, pues la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal –LOPD-, en el artículo 3 i), define la cesión o comunicación de datos como "toda revelación de datos realizada a una persona distinta del interesado", y

conforme al artículo 11.1 de la misma LOPD esos datos sólo pueden ser cedidos con el consentimiento del interesado, salvo en los supuesto del artículo 11.2 de la misma Ley 15/99, como sería que se recabaran mediante resolución judicial para un procedimiento judicial (Informe 0176/2012 de la Agencia Española de Protección de Datos, entre otros).

Por lo tanto, la prueba de la coacción, vejación, injuria o calumnia de violencia de género cometidas con tecnologías de información o comunicación, requiere a menudo que el juez solicite a la operadora la cesión del listado de llamadas recibidas por la víctima y mensajes SMS, hora en que se recibieron, desde qué teléfono, duración de la comunicación, e incluso geolocalización de la misma, y que esta entregue tales datos en formato electrónico al agente de la policía judicial autorizado para la causa penal.

O bien, que se recabe al operador de servicios informáticos en la red, la IP de la conexión en una hora y día determinado, en la web, foro, red social o blog, o diario electrónico, en el cual se produjo el comentario calumnioso o injurioso, o se colgó la foto íntima de la víctima, por ejemplo.

Expuesto lo anterior, nos encontramos con el segundo problema, pues aunque la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, en su artículo 42 relativo a la conservación y cesión de datos de las comunicaciones electrónicas, señala que las operadoras de telefonía y prestadores de servicios de internet, que operan en España, tienen la obligación de conservar dichos datos, y cederlos a los agentes facultados a través de la correspondiente autorización judicial, determina también que sólo cabe la cesión con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en leyes especiales.

Estos datos periféricos al contenido de la llamada o “metadatos”, quedan protegidos por el secreto de las comunicaciones del artículo 18.3 de la Constitución Española, y de ahí, que su cesión requiera autorización judicial.

Estamos hablando de la cesión de los datos del tráfico, no del contenido de la comunicación en sí misma, cuya obtención se sigue regulando por el artículo 579 de la ley de Enjuiciamiento Criminal, y que también requiere de autorización judicial.

El problema se encuentra en qué se entiende por delito grave a los efectos de la Ley 25/2007, que obliga preventivamente que las operadoras de telecomunicaciones y servicios en la red monitoricen

los datos del tráfico de las comunicaciones, independientemente de que posteriormente los mismos luego sirvan o no para una investigación criminal, pues pasado el tiempo que la ley determina deben ser eliminados.

Recordemos que la Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, que es la que transpone la Ley 25/2007, nace a raíz de los atentados terroristas en los trenes de Atocha en Madrid y de los posteriores atentados de Londres. En el caso español, la localización del locutorio telefónico en el que se vendieron las tarjetas prepago de los móviles que activaron las bombas de los trenes, se logró gracias a que una de las compañías telefónicas conservó los datos de aquellas comunicaciones.

Hay que señalar que no existe unidad de criterio en la judicatura, ni entre la Fiscalía y Jueces, sobre qué se entiende a estos efectos por delitos graves, y menos tras la Sentencia del Tribunal de Justicia de la unión Europea de 8 abril de 2014 (Gran Sala), que anuló la Directiva 2006/24/CE.

El Tribunal de Justicia de la Unión Europea –TJUE- no declara ilegal la retención o conservación de datos de las comunicaciones, sino que anula la Directiva 2006/24 por falta de proporcionalidad y suficientes garantías en la limitación de los derechos fundamentales al secreto de las comunicaciones, privacidad, y al tratamiento de los datos personales, señalando además que debe existir un estricto control en la cesión de los datos.

Con arreglo al artículo 52.1 de la Carta de Derechos Fundamentales de la Unión Europea, que desde la entrada en vigor del Tratado de Lisboa (2009) tiene carácter vinculante, cualquier limitación del ejercicio de los derechos y libertades reconocidos por ésta deberá ser establecida por la ley, respetar su contenido esencial y, dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones a dichos derechos y libertades cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión Europea, o a la necesidad de protección de los derechos y libertades de los demás.

El TJUE determina en la citada sentencia que el conjunto de los datos que se obliga a conservar a los operadores permitiría obtener datos relativos a circunstancias de la vida privada de las personas (hábitos, lugares de residencia, relaciones sociales, etc), supone efectivamente

una intrusión en dicha vida privada. Y concluye que, aunque los fines que persigue la Directiva son de interés general, el legislador excedió los límites del principio de proporcionalidad sin que haya medidas ni garantías suficientes en la Directiva que permitan controlar que la intromisión se limite a lo estrictamente necesario.

La sentencia basa su conclusión en los siguientes motivos:

En primer lugar, la Directiva abarca de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves.

En segundo lugar, la Directiva no fija ningún criterio objetivo que permita garantizar que las autoridades nacionales competentes únicamente tendrán acceso a los datos y podrán utilizarlos para prevenir, detectar o reprimir penalmente delitos que, por la magnitud y la gravedad de la injerencia en los derechos fundamentales en cuestión, puedan considerarse suficientemente graves para justificar tal injerencia. Por el contrario, la Directiva se limita a remitir de manera general a los “delitos graves” definidos por cada Estado miembro en su ordenamiento jurídico interno. Además, la Directiva no define las condiciones materiales y procesales en las que las autoridades nacionales competentes pueden tener acceso a los datos y utilizarlos posteriormente. En particular, el acceso a los datos no se supedita al control previo de un órgano jurisdiccional o de un organismo administrativo autónomo.

En tercer lugar, en lo relativo al período de conservación de los datos, la Directiva prescribe un período mínimo de seis meses sin establecer ninguna distinción entre las categorías de datos en función de las personas afectadas, o de la posible utilidad de los mismos con respecto al objetivo perseguido. Además, este período oscila entre seis meses como mínimo y veinticuatro meses como máximo, sin que la Directiva precise los criterios objetivos con arreglo a los que debe determinarse el período de conservación para garantizar que se limite a lo estrictamente necesario.

Asimismo el Tribunal de Justicia considera que la Directiva no contiene garantías suficientes que permitan asegurar una protección eficaz de los datos contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos de los datos. En particular, señala que la Directiva autoriza a los proveedores de servicios a tener en cuenta consideraciones económicas al determinar el nivel de seguridad que aplican (especialmente en lo que respecta a los costes de aplicación

de las medidas de seguridad), y no garantiza la destrucción definitiva de los datos al término de su período de conservación.

Por último, el Tribunal de Justicia censura que la Directiva no obliga a que los datos se conserven en el territorio de la Unión Europea. Por lo tanto, la Directiva no garantiza plenamente el control del cumplimiento de los requisitos de protección y de seguridad por una autoridad independiente, como se exige expresamente en la Carta. Dicho control, efectuado sobre la base del Derecho de la Unión, constituye un elemento esencial del respeto a la protección de las personas en lo que respecta al tratamiento de datos personales.

La Ley 25/2007 que traspuso la Directiva 2006/24 a nuestro ordenamiento interno establece más garantías para los derechos fundamentales a la privacidad y al tratamiento de los datos personales que la Directiva. Y es respetuosa con el derecho al secreto de las comunicaciones, pues en primer lugar, los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

Por lo tanto, la Ley 25/2007 española no queda anulada por la STJUE de 8 de abril de 2014, de hecho, la vigente Ley 9/2014, General de Telecomunicaciones se publica el 10 de mayo de 2014 y se remite a ella, y a la vez, en su disposición final cuarta, reforma los artículos 6 y 7 de la Ley 25/2007, para señalar que la cesión se realizará en formato electrónico y exclusivamente a los agentes facultados (Policía Judicial, Vigilancia Aduanera y CNI), en el plazo de 7 días desde que se reciba la orden, sino se establece otro plazo en la resolución judicial.

Pero entiendo que es urgente realizar en la Ley 25/2007 algunos cambios, partiendo de que tanto la ley General de Telecomunicaciones como la ley 25/2007 son leyes ordinarias, y conforme al artículo 81 de la Constitución Española, afectando la segunda a los derechos fundamentales del artículo 18 CE, debería haberse traspuesto la Directiva hoy anulada por Ley Orgánica.

Al menos, el legislador debería aclarar cuanto antes **qué se entiende por delito grave** a los efectos de la Ley 25/2007, dado que actualmente esta indefinición está causando gran controversia

jurídica, inseguridad, y lo que es más grave impunidad y victimización procesal innecesaria.

Y digo victimización secundaria innecesaria porque de nada vale que el juez instructor lleve a cabo la investigación judicial con el apoyo de los metadatos cedidos del tráfico de las comunicaciones, si posteriormente la Audiencia Provincial, por lo dispuesto en el artículo 11.2 de la ley Orgánica del Poder Judicial, y artículos 1 y 6 de la ley 25/2007, declara nula dicha prueba y por lo tanto las restantes pruebas obtenidas a raíz del conocimiento de dichos datos del tráfico de las comunicaciones.

Ante el silencio de la Ley 25/2007 sobre qué debe entenderse por delito grave cuya investigación justifique la autorización judicial ordenando la cesión de los datos a las operadoras, cabe interpretar que la gravedad del delito viene determinada por el propio Código Penal.

El Código Penal define como delito grave el que lleva aparejada pena privativa de libertad superior a 5 años (artículos 13 y 33 Código Penal).

Pero también cabe una interpretación no penológica sobre la gravedad del delito, como la que realiza la Circular 1/2013 de la Fiscalía General del Estado, que se fija no en la pena objetiva del hecho que se investiga, sino en las circunstancias de tal hecho, el bien jurídico protegido, la relevancia social y la jurisprudencia aplicable al caso.

En otras injerencias aún más graves, como en la prisión preventiva regulada en el artículo 503 de la ley de Enjuiciamiento Criminal, el legislador no ha determinado criterios de proporcionalidad estrictamente penológicos.

También el Tribunal Constitucional en diversas resoluciones, para medir la gravedad del delito, sobre todo si éste se comete por medios informáticos, no ha tenido en cuenta el criterio penológico, sino factores o criterios como:

- el bien jurídico protegido,
- la relevancia social de los hechos,
- y la potencialidad lesiva del uso de instrumentos informáticos.

Este último criterio se basa en la posibilidad de expansión de determinados delitos por las redes de comunicaciones, y la grave

dificultad de su persecución por los medios tradicionales de investigación (STC 104/2006, de 3 de abril).

Además hay que tener en cuenta que actualmente nos relacionamos en gran medida por medios telemáticos, sustituyendo en muchas ocasiones la relación personal física por la relación a distancia a través de aplicaciones telefónicas y ordenadores personales.

Por ello, y teniendo en cuenta el Código Penal vigente, un criterio penológico estricto de delito grave, dejaría en la impunidad muchos hechos que cometidos de manera física serían punibles, pero que realizados por medios telemáticos o informáticos, sin la cesión por las operadoras y prestadores de servicios en la red de los datos externos de la comunicación (por ejemplo el flujo de las llamadas, o la determinación de la IP, que sirva al menos de prueba indiciaria), quedarían impunes.

Por otra parte, no tiene mucho sentido que no venga limitada la obtención del contenido de la comunicación a que la investigación judicial tenga por objeto hechos con penalidad en su caso superior a cinco años de prisión, y sí se límite con esta posible pena para obtener datos externos a la comunicación. Datos que además ya existen en un fichero de la operadora o prestador del servicio en la red.

La proporcionalidad de la injerencia en el secreto de las comunicaciones y en la privacidad depende de distintas circunstancias en cada caso, como por ejemplo la alarma social que causa el hecho o la conducta, la persistencia en la comisión del hecho, el anonimato que el medio informático o telemático otorga, y el sentimiento de impunidad y apoderamiento que dicha herramienta produce en el autor, las circunstancias personales del sospechoso, etc.

Por todo lo expuesto, parece lógico que al igual que para decretar la prisión preventiva, no se sigan criterios estrictamente penológico para determinar la proporcionalidad de la injerencia en los derechos fundamentales a que se refieren los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea, y el artículo 18 de la Constitución Española.

El sentido de la justicia aconseja que en gran medida se deje a la valoración judicial de la proporcionalidad en cada supuesto. Este arbitrio valorará también si la injerencia que se pretende supone una instrumentalización del procedimiento penal para obtener información privada del denunciado.

Finalizo aquí este artículo, que fundamentalmente es una reflexión y una llamada de atención sobre la importancia que para la tutela judicial efectiva tiene el tema tratado.

Amigo lector, gracias por el tiempo dedicado en la lectura del mismo, y si quiere hacerme llegar alguna aportación sobre la cuestión tratada, puede hacerlo al correo autogestionate@outlook.com