VII.- 2. LAS NUEVAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA

Mª Belén Aige Mut

SUMARIO: 1. Introducción; 2. El agente encubierto informático; 3. La interceptación de comunicaciones telefónicas y telemáticas; 4. La captación y grabación de comunicaciones orales por dispositivos electrónicos; 5. Los dispositivos de seguimiento, localización y captación de la imagen; 6. El registro de dispositivos de almacenamiento masivo; 7. El registro remoto sobre equipos informáticos; 8. Conclusión final.

1. INTRODUCCIÓN

Con la aprobación de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, han sido aprobadas precisamente las nuevas diligencias de investigación tecnológica.

Estas diligencias suponen una novedad muy importante y un avance muy necesario que debía tomar la vetusta LECrim para adaptarse a las nuevas realidades, que afectan tanto a la forma de cometer los delitos como a los propios delitos, pero que también pueden favorecer muchísimo a la investigación de los "delitos tradicionales".

En concreto, quiero empezar haciendo referencia a la Memoria de la Fiscalía del año 2015[1] que refleja el aumento de la criminalidad informática,

1.- Dicha memoria puede consultarse en la siguiente página web: https://www.fiscal.es/memorias/memoria2015/FISCALIA_SITE/index.html

que se sitúa en un total de 20.534 delitos para el año 2014, lo que supone un incremento del 71,21% respecto del año 2013 y un incremento del 210% respecto al año 2011. En estos porcentajes el delito preponderante es el de la estafa informática que ocupa un 84% de las denuncias. En el mismo sentido, el anuario estadístico del Ministerio del Interior[2] indica que de un total de 49.966 ilícitos, 32.842 corresponden a los fraudes informáticos, constituyendo así un 65,7% del total (y siendo los más frecuentes los relativos a las estafas bancarias o con tarjeta de crédito). También es de destacar que del total de delitos, han sido esclarecidos unos 17.948, lo que constituye aproximadamente un 36% de los mismos[3].

Es por todo ello precisamente por lo que es muy importante la creación de nuevas formas de investigación y averiguación para este tipo de delitos. Estas diligencias relacionadas con las nuevas tecnologías por fin son una realidad, y aparecen recogidas en la mencionada LO 13/2015, siendo las siguientes:

1) Agente encubierto informático

2) Interceptación de comunicaciones telefónicas y telemáticas

3) Captación y grabación de comunicaciones orales por dispositivos electrónicos

4) Dispositivos de seguimiento, localización y captación de la imagen

5) Registro de dispositivos de almacenamiento masivo

6) Registro remoto sobre equipos informáticos

Menos la primera de ellas, relativa a la modalidad del nuevo agente encubierto informático, el resto están sometidas a unas disposiciones comunes, recogidas en el Art. 588 bis a), que se resumen en que todas requieren autorización judicial basada en los principios de especialidad (esto es, investigación de delitos concretos), idoneidad (definiendo el ámbito objetivo y subjetivo, así como su duración), excepcionalidad y necesidad de las medidas (solamente aplicables cuando no estén a disposición otras medidas menos gravosas y además sean realmente necesarias para la investigación),

2.- Al cual se puede acceder en la siguiente dirección: http://www.interior.gob.es/web/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas-anuarios-y-revistas-/anuario-estadistico-del-ministerio-del-interior.

3.- En este sentido, el Presidente de la Audiencia Nacional señaló en unas declaraciones en el Congreso Internacional de Derecho Procesal "Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)", celebrado en Elche los días 28 y 29 de octubre de 2015, que normalmente solo el 5,1% de los delitos cibernéticos son averiguados (esto es, uno de cada veinte).

así como la proporcionalidad a la hora de decidir adoptarlas (ponderando el sacrificio de los derechos e intereses afectados con el beneficio para el interés público y el de terceros).

Asimismo, destacar que todas estas diligencias que vamos a comentar a continuación están vigentes desde el 6 de diciembre de 2015, a tenor de la Disposición Final Cuarta de la LO 13/2015.

A continuación vamos a analizar brevemente cada una de ellas:

2. EL AGENTE ENCUBIERTO INFORMÁTICO

Esta nueva modalidad se regula en el Art. 282 bis apartados 6 y 7. A diferencia del agente encubierto tradicional, este requiere de autorización únicamente por parte del juez de instrucción, no por parte del Ministerio Fiscal, y específicamente realizada, para los delitos a que se refiere el apartado 4 del Art. 282 bis[4] o cualquiera de los recogidos en el Art. 588 ter a)[5]. Se puede observar, por tanto, que esta nueva regulación del agente encubierto informático amplía los tipos delictivos respecto a los ya existentes para el agente encubierto tradicional (es decir, aquellos relacionados con la delincuencia organizada), dando de este modo un mayor campo de actuación y superando la idea de *numerus clausus* del agente encubierto tradicional[6].

Asimismo, en el marco de esta medida el juez además podrá autorizar para la obtención de imágenes y la grabación de las conversaciones. Con ello estaríamos entrando en conexión con la diligencia de interceptación de comunicaciones, entre otras. Precisamente por ello, junto con otros motivos, se observa que esta figura supone un plus de lesividad al derecho a la

4.- Esto es, delitos relacionados con la delincuencia organizada, que serían los siguientes: delitos de obtención y tráfico de órganos, secuestro, trata de seres humanos, prostitución, delitos contra el patrimonio y orden socioeconómico, relativos a la propiedad intelectual e industrial, contra los derechos de los trabajadores y de los ciudadanos extranjeros, delitos de tráfico de especies o de flora o fauna amenazada, delitos de falsificación de moneda, tráfico de armas, terrorismo, delitos contra el patrimonio histórico.

5.- Son aquellos delitos dolosos castigados con pena con límite máximo de al menos 3 años de prisión, delitos cometidos en el seno de un grupo u organización criminal, delitos de terrorismo y delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología.

6.- Se viene a superar, de este modo, el problema de elaborar una lista tasada, problema que ya era señalado por BUENO DE MATA, F., "El agente encubierto en internet: mentiras virtuales para alcanzar la justicia", Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso de Derecho Procesal (I Internacional), A Coruña, 2 y 3 de junio de 2011 (Ana María Neira Pena, coord.), 2012, versión digital obtenida de la página web: http://ruc.udc.es/xmlui/handle/2183/9179.

intimidad y secreto de las comunicaciones que realiza el agente encubierto[7], es por ello por lo que se ha querido que la autorización en este caso fuera exclusivamente judicial y sin posibilidad de otorgarla el Ministerio Fiscal.

3. LA INTERCEPTACIÓN DE COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS

Esta diligencia se podrá adoptar a través de autorización judicial para los delitos recogidos en el Art. 579.1[8] así como aquellos delitos cometidos a través de instrumentos informáticos u otra tecnología. En este catálogo que recoge la ley, hay que destacar precisamente esta última precisión realizada en el Art. 588 ter a) *in fine* a "*delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación*", pues como señala ORTIZ PRADILLO "*la Ley utiliza terminología intencionalmente imprecisa*"[9], para dejar abierta la puerta al estado cambiante de las nuevas tecnologías que siempre van a avanzar más rápido que el proceso legislativo.

Nos llama mucho la atención de que dentro del catálogo de delitos para los cuales se incluye la medida se tiene en cuenta el factor de que para la comisión de un hecho delictivo se hayan utilizado las nuevas tecnologías. En este caso podríamos estar hablando perfectamente de delitos de escasa relevancia (de hecho, como hemos señalado en la introducción, en la mayoría de los casos los delitos informáticos son de estafa, y esta puede ser a gran escala o para casos de pequeña delincuencia), y parece un poco

7.- Como acertadamente apuntó, VALIÑO CES, A., "La actuación del agente encubierto en los delitos informáticos tras la ley orgánica 13-2015", en la comunicación realizada al *Congreso Internacional de Derecho Procesal "Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)", celebrado el 28 y 29 de octubre de 2015 en Elche*, y que puede consultarse en la página web: http://congresoexigenciasjusticia.umh.es/comunicaciones-y-ponencias/

8.- Los ya mencionados delitos dolosos castigados con pena máxima de al menos 3 años de prisión, delitos cometidos en el seno de un grupo u organización criminal y delitos de terrorismo.

9.- ORTIZ PRADILLO, J.C., "Desafíos legales de las diligencias tecnológicas de investigación", ponencia presentada en la mesa redonda *Medios de investigación tecnológica, del Congreso Internacional de Derecho Procesal "Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)", celebrado en Elche los días 28 y 29 de octubre de 2015.* En dicha ponencia señaló también que precisamente por el uso de esa terminología imprecisa, no es extraño encontrarnos en la Ley con vocablos como "dispositivos", "algoritmos", "software" que siempre se mencionan de acuerdo con el estado de la tecnología, evidentemente para cumplir con la constante evolución y salvaguardar en la medida de lo posible la continua obsolescencia legal.

chocante que se utilice una medida tan gravosa solamente por ese nexo de conexión[10].

En casos de urgencia (como por ejemplo delitos de terrorismo) cabe la autorización por el Ministro del Interior o el Secretario de Estado que deberán comunicarlo en un plazo máximo de 24 horas al juez de instrucción a fin de que este confirme o revoque la medida en el plazo de 72 horas.

Esta diligencia también podrá autorizar el acceso al contenido de la comunicación así como a los datos de tráfico, que son los que se generan como consecuencia de la conducción de una comunicación a través de la red de comunicaciones (por ejemplo el IMSI, IMEI, titular, número…). Esta posibilidad es muy importante porque en ocasiones puede ser incluso más valiosa la obtención de estos datos que del propio contenido de la comunicación.

La medida estará sometida a un control realizado mediante la transcripción de los pasajes de interés así como la entrega de las grabaciones íntegras (indicando su origen y destino), siempre asegurando su autenticidad e integridad a través de la firma electrónica avanzada (u otro sistema de sellado o adveración suficientemente fiable; por lo tanto observamos con esta última expresión que la ley vuelve a dejar la puerta abierta al avance de las tecnologías y no se pilla los dedos con definiciones demasiado excluyentes, como ya apuntábamos anteriormente).

Precisamente esta referencia legal a la firma electrónica avanzada (u otro mecanismo similar), es bastante novedosa y acertada, puesto que en leyes similares, como la LEC, tanto en el ámbito probatorio como en los mecanismos de inicio del procedimiento (por ejemplo el Art. 812 relativo al procedimiento monitorio) no se recoge la referencia a sistemas que proporcionen la autenticidad e integridad de los documentos electrónicos.

10.- En este mismo sentido se pronuncia GONZÁLEZ NAVARRO, A. para el supuesto de la diligencia de registro remoto de equipos informáticos, cuando indica que "*se equipara el hecho de que para la comisión del hecho delictivo se hayan utilizado las nuevas tecnologías con que para la investigación de los hechos (que perfectamente pueden ser de escasa relevancia, pues nada especifica el precepto en sentido contrario) se utilice una medida tan gravosa como la que aquí se estudia*", en GONZÁLEZ NAVARRO, A., "Nuevas tecnologías aplicadas a la investigación criminal: las regulaciones española y alemana", comunicación presentada en el *Congreso Internacional de Derecho Procesal "Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)", celebrado el 28 y 29 de octubre de 2015 en Elche*, que puede consultarse en la página web:
http://congresoexigenciasjusticia.umh.es/comunicaciones-y-ponencias/

Para finalizar con esta diligencia, respecto a su duración se establece por un periodo de 3 meses, prorrogables por iguales plazos hasta un máximo de 18 meses.

4. LA CAPTACIÓN Y GRABACIÓN DE COMUNICACIONES ORALES POR DISPOSITIVOS ELECTRÓNICOS

Esta medida se adopta, como todas las diligencias que estamos comentando, a través de autorización judicial. La citada diligencia se podrá completar con la obtención de imágenes si se autoriza específicamente en la resolución, conectando de esta manera con la diligencia de captación de imagen. Es más, incluso podría hablarse de que incluye a su vez una verdadera diligencia de captación de imágenes en lugar cerrado, que no se incluye dentro de la diligencia de captación de imágenes propiamente dicha, que como veremos a continuación hace referencia exclusivamente a espacios abiertos o lugares públicos.

En cuanto a su adopción, se realizará siempre que existan indicios suficientes y se cumplan los siguientes requisitos:

- que se vayan a obtener datos esenciales de relevancia probatoria, y

- que sea para la investigación de uno de los delitos siguientes: delitos dolosos con pena máxima de al menos 3 años, delitos cometidos en el seno de grupos u organizaciones criminales o delitos de terrorismo.

Respecto al control de la medida, el mismo se hará a través del control de los originales o copias, así como de la transcripción de los mismos.

5. LOS DISPOSITIVOS DE SEGUIMIENTO, LOCALIZACIÓN Y CAPTACIÓN DE LA IMAGEN

Cuando nos referimos a esta diligencia, en realidad estamos hablando de dos diligencias diferentes:

1) La grabación o captación de imágenes en lugares o espacios públicos, que la podrá realizar directamente la Policía Judicial. Observamos que no hace referencia a los espacios cerrados, para los cuales habría que acudir a la diligencia de captación y grabación de comunicaciones orales por dispositivos electrónicos.

2) La utilización de dispositivos o medios técnicos de seguimiento y localización, que requiere de nuevo autorización judicial de acuerdo con los principios de necesidad y proporcionalidad, y siempre especificando el medio técnico por el cual se va a realizar. En casos de urgencia sí podrá adoptarlo la Policía Judicial directamente, pero con la obligación de dar cuenta al juez de instrucción en el plazo máximo de 24 horas, para que confirme o revoque en el mismo plazo de 24 horas.

En este caso, por tanto, la verdadera diligencia restrictiva de derechos fundamentales sería la segunda, la colocación de dispositivos de seguimiento y localización. Con respecto a su plazo de duración será de 3 meses, prorrogables por periodos iguales hasta un máximo de 18 meses. Y en cuanto a su control, la Policía entregará el original o la copia siempre que sea solicitada por el juez durante la investigación y, en todo caso, siempre al terminar la misma.

6. EL REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO

Dicho registro podrá llevarse a cabo con motivo de un registro domiciliario o incluso fuera del mismo, requiriendo en todo caso autorización judicial específica así como una nueva autorización para el acceso a su contenido. En casos de urgencia se podrá adoptar por la Policía Judicial, que deberá comunicarlo al juez de instrucción en el plazo de 24 horas para que pueda confirmar o revocar su adopción en el plazo de 72 horas.

Esta diligencia hace referencia al registro de ordenadores, dispositivos de almacenamiento masivo, instrumentos de comunicación telefónica o telemática y acceso a repositorios telemáticos de datos. Esto es, gracias a ella podremos acceder al contenido de los USB, discos duros portátiles, ordenadores (tanto portátiles como de sobremesa) y teléfonos móviles.

Respecto a estos últimos hay que hacer una especial referencia, puesto que a día de hoy los teléfonos móviles tienen una característica particular, y es que son "inteligentes", lo que conocemos como Smartphone. Ello significa que un mismo dispositivo puede realizar multitud de funciones que realizarían también otros instrumentos independientes, por ejemplo puede servir como cámara de fotos, agenda personal, GPS, email, teléfono… lo que hace que puedan converger en el mismo varios derechos: por una parte el derecho a la intimidad (privacidad) del Art. 18.1 CE y por otra parte el derecho al secreto de las comunicaciones del Art. 18.3 CE, lo que conlleva que puedan converger también dos tipos de diligencias diferentes, la propia del registro

de dispositivos de almacenamiento masivo y la diligencia de interceptación de comunicaciones telefónicas y telemáticas (e incluso podríamos hablar también de la diligencia de seguimiento y localización).

El problema que se puede plantear al converger ambas diligencias es el de si bastaría con la adopción de una de ellas para el acceso a todo su contenido o por el contrario se requeriría la adopción de ambas. Para ello se deben comparar las previsiones de cada una para ver si son las mismas o si se incluyen unas dentro de otras.

En este sentido, en cuanto al contenido mínimo de la resolución, control de la misma… serían iguales. Evidentemente, y por la naturaleza de cada una de ellas, la duración no se contempla para el registro de dispositivos de almacenamiento masivo pero sí para la interceptación de comunicaciones, pero eso no conllevaría mayor problema. Donde sí se aprecia una discrepancia relevante es en el tema de la autorización judicial necesaria, puesto que para la interceptación de las comunicaciones únicamente se podrá adoptar para los delitos del Art. 579 así como los cometidos por soportes informáticos, mientras que para la diligencia de registro de dispositivos de almacenamiento masivo en principio se adoptaría para cualquier tipo de delito (al no contener ninguna previsión en contrario) pero además esta autorización debería ser específicamente motivada, tanto para el registro del dispositivo como para el acceso a su contenido.

Por lo tanto, se puede observar que al no coincidir la autorización judicial en ambas, una misma autorización judicial no podría sustentar la adopción de esas dos diligencias.

La solución en este supuesto dependería del contenido al cual quisiéramos acceder del Smartphone, así en el caso de contenidos que afectasen únicamente al derecho a la intimidad (como por ejemplo la agenda, las fotos, las notas…) bastaría con la adopción de la diligencia de registro de dispositivos de almacenamiento masivo, mientras que cuando se quiera acceder a contenidos que afectan al derecho al secreto de las comunicaciones (como por ejemplo los SMS, registros de llamadas, Whatsapp, emails…) deberíamos adoptar la diligencia de interceptación de comunicaciones telefónicas y telemáticas, para así en cualquier caso salvar el contenido obtenido como prueba lícita en el proceso[11].

11.- Al respecto, AIGE MUT, M.B. "El actual proceso de modernización de la Administración de Justicia: especial referencia a la nueva diligencia de registro de dispositivos de almacenamiento masivo", comunicación realizada para el *Congreso Internacional de Derecho Procesal "Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)", celebrado el 28 y 29 de octubre de 2015 en Elche*, y que puede consultarse en la página web:
http://congresoexigenciasjusticia.umh.es/comunicaciones-y-ponencias/

Encontrar una solución es muy importante, puesto que en España, de una población registrada que ronda los 47 millones de habitantes según el Anuario Estadístico del Ministerio del Interior[12], ya contamos con más de 50 millones de móviles[13]. De este modo, España se incluye en los países más relevantes en cuanto a la penetración de "smartphones" con un 81% de teléfonos inteligentes sobre el total de móviles, según informe de la Fundación Telefónica[14]. Con lo cual, podemos imaginar, al contrastar los datos anteriores, que existen a día de hoy unos 40 millones de smartphones en España[15].

Lo realmente relevante de estos datos es que en la mayoría de ocasiones la información que se contiene en los citados dispositivos es incluso mayor que la que se puede encontrar en un domicilio[16], pudiendo provocar un mayor intrusismo en la privacidad de las personas.

7. EL REGISTRO REMOTO SOBRE EQUIPOS INFORMÁTICOS

Este registro se podrá autorizar para los siguientes delitos: cometidos en el seno de organizaciones criminales, delitos de terrorismo, delitos contra menores o personas con capacidad modificada judicialmente, delitos contra

---

12.- Al cual se puede acceder, como se ha indicado anteriormente, en la siguiente dirección: http://www.interior.gob.es/web/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas-anuarios-y-revistas-/anuario-estadistico-del-ministerio-del-interior.

13.- En fecha abril de 2015 el número de líneas de telefonía móvil superaba los 50 millones, según el observatorio nacional de las telecomunicaciones y la sociedad de la información (ONTSI), datos que se pueden consultar actualizados en la siguiente dirección de internet: https://data.observatorio.es/analytics/saw.dll?Dashboard&PortalPath=/shared/Indicadores%20Destacados/_portal/Indicadores_destacados&Page=Telefon%C3%ADa%20fija%20y%20m%C3%B3vil.

14.- Datos obtenidos de la noticia "España, líder europeo en penetración de 'smartphones'", publicada por el diario El Mundo con fecha 22 de enero de 2015, a la que se puede acceder a través del siguiente enlace: http://www.elmundo.es/tecnologia/2015/01/22/54c0965c22601d656b8b456c.html Estos datos revelan el claro y rápido aumento que se ha producido con respecto a 2014, en el que los smartphones se situaban en un total de 53'7%, según indica la noticia titulada "Los teléfonos inteligentes ganan en España", publicada por el diario ABC con fecha 29 de julio de 2014, y que se puede consultar en el siguiente enlace: http://www.abc.es/tecnologia/20140729/rc-telefonos-inteligentes-ganan-espana-201407292059.html.

15.- El citado informe al que hace mención la noticia de El Mundo, revela también que en España existen 23 millones de usuarios activos de aplicaciones, y que en el año 2014 más de 21.4 millones de españoles han accedido a Internet en movilidad. Ello significa que de los 40 millones de smartphones existentes, al menos la mitad, esto es 20 millones, se utilizan con todo su potencial de conectividad online.

16.- Como ha destacado acertadamente ORTIZ PRADILLO, J.C., "Desafíos legales de las diligencias tecnológicas de investigación", Op. Cit., incidiendo en el hecho de que puede existir información en los teléfonos móviles de las personas que no se encuentra en la vida real y, por tanto, a la que no podríamos acceder con la adopción de una diligencia tradicional de entrada y registro, por ejemplo.

la Constitución, de traición y relativos a la defensa nacional o aquellos cometidos por instrumentos informáticos. La resolución autorizante deberá ser específica en cuanto a su contenido, y establecer su duración con el plazo máximo de un mes, prorrogable por periodos iguales hasta un máximo de 3 meses.

Se observa que esta nueva medida tiene un carácter muy restrictivo, tanto en cuanto a su ámbito de aplicación (delitos tasados) como a su plazo de duración (que es el más breve de los existentes para las nuevas medidas de investigación tecnológicas).

Es muy importante la incorporación de esta medida, puesto que la interceptación de las comunicaciones por internet puede en ocasiones aparecer con datos encriptados, por lo que se necesita un programa que desencripte los mismos, pero ese programa al introducirlo en el ordenador podría afectar a otros derechos fundamentales de la persona investigada porque podría actuar como un programa espía, una especie de troyano federal[17] y por eso es muy importante contar con una norma habilitante que regule esta posibilidad de acceso remoto, pero a la vez con una serie de limitaciones y restricciones importantes.

8. CONCLUSIÓN FINAL

Como conclusión a lo anteriormente expuesto, nos encontramos ante una reforma muy necesaria e importante que ayudará mucho a la investigación criminal y facilitará la correcta realización de unas diligencias de investigación restrictivas de derechos fundamentales, que posteriormente no puedan revocarse por defectos legales ante el Tribunal Constitucional. La nueva regulación no tan solo es novedosa sino también exhaustiva y muy cuidada, aunque sin embargo, y como no puede ser de otro modo al tratar estos temas tan actuales, sigue siendo ambigua en determinados aspectos. Es evidente que tendremos que esperar a la interpretación y aplicación que realicen los Tribunales para poder extraer mayores conclusiones, pero al menos podemos partir de una base que anteriormente era inexistente pero que ya devenía ineludible.

17.- Como indica GONZÁLEZ NAVARRO, A., "Nuevas tecnologías aplicadas a la investigación criminal: las regulaciones española y alemana", Op. Cit., que puede consultarse en la página web: http://congresoexigenciasjusticia.umh.es/comunicaciones-y-ponencias/