INVESTIGACIÓN PENAL Y NUEVAS TECNOLOGÍAS: ALGUNOS DE LOS RETOS PENDIENTES

Julio Pérez Gil
Profesor Titular de Derecho Procesal
Universidad de Burgos [1]

La irrupción de las nuevas tecnologías en la investigación penal no debe ser convertida, consciente o inconscientemente, en causa justificativa para el mantenimiento de deficiencias del sistema penal o para erosionar garantías históricamente consolidadas. También en el nuevo entorno tecnológico toda restricción de derechos fundamentales ha de precisar de autorización judicial sobre la base de expresas habilitaciones legales, sin que pueda considerarse suficiente la invocación de las de carácter genérico. Ello reviste particular importancia poniéndolo en relación con la protección de los datos personales.

SUMARIO

1. El presente texto tiene su origen en la conferencia impartida el 17 de mayo de 2005 en las Jornadas sobre *Derecho y Nuevas Tecnologías* que, organizadas por la Fundación Universidad de Verano, se desarrollaron en la sede de las Cortes de Castilla y León. Se ha mantenido el tono de la conferencia.

1. INVESTIGACIÓN DEL DELITO EN LA «SOCIEDAD DE LA INFORMACIÓN»

1.1. PLANTEAMIENTO INICIAL

No descubriré nada nuevo diciendo que el proceso penal español, particularmente en lo referido a su fase de instrucción, está precisado de reformas globales de hondo calado. Pero esa afirmación, sostenida bajo el título que encabeza este trabajo, adquiere una dimensión particular por cuanto precisamente los avances tecnológicos son uno de los factores que han de ser puestos en primer plano a la hora de abordar esa improrrogable reforma. En lo referido a la averiguación de los delitos, y en la medida en que la búsqueda y acopio de datos sobre hechos y su presunto autor constituye el sentido de toda investigación criminal, la aplicación a ella de nuevas tecnologías de tratamiento de la información deviene un elemento clave. En este contexto habremos de plantearnos si estamos o no obligados a cambiar la forma en que hemos construido algunos de los axiomas firmemente asentados a fin de que puedan resistir los embates del vertiginoso cambio tecnológico. Corresponde cuestionarnos, por ende, si nuestro cuerpo normativo, jurisprudencial y doctrinal está anclado con la suficiente firmeza como para soportar las intensas sacudidas que vienen alentadas por la técnica o si, al menos, cuenta con la suficiente flexibilidad para que su adaptación a ellos no lo fracture inutilizándolo absolutamente.

Son evidentes las mejoras que con vistas a la instrucción de los delitos han propiciado avances técnicos inimaginables hasta hace muy poco (análisis genéticos, sistemas de localización geográfica, datos de tráfico de las comunicaciones, videocámaras, dispositivos de escucha directa, programas informáticos rastreadores, agentes encubiertos en Internet, etc.), sin perjuicio de que lo que está por llegar nos seguirá sorprendiendo *ad infi-*

nitum [2]. Desde la perspectiva inversa, observamos también que la Justicia ha de enfrentarse a esos mismos o a otros desarrollos tecnológicos del mismo calibre cuando su utilización se conecta de algún modo con las más diversas modalidades de comisión delictiva, pensando ahora tanto en las tradicionales como en las más novedosas.

La escasa relevancia cuantitativa de las investigaciones criminales que se sirven de dispositivos avanzados tecnológicamente o de la investigación sobre delitos «de alta tecnología» aparentemente no parecería justificar el despliegue y la profusión de informaciones que al respecto se pueden encontrar, tanto en los medios de comunicación como en publicaciones de interés científico-jurídico. Corresponde por tanto verificar si estamos manejando soluciones viejas a problemas verdaderamente nuevos, soluciones nuevas a problemas que ya son muy viejos, o bien, posiblemente, todo ello a la vez.

Lo dicho me pone en disposición de avanzar la idea básica que quiero plantear y que, *in nuce*, es la siguiente: la irrupción de las nuevas tecnologías en la investigación penal no debe ser convertida, consciente o inconscientemente, en excusa o en coartada para acentuar hiperestésicamente carencias y deficiencias del sistema, abriendo peligrosos portillos. La justificación de ese argumento me obligará a transitar por diversos caminos, no siempre suficientemente bien trazados ni desbrozados. Y precisamente el hecho de recorrerlos será la forma de que se vayan depurando de malezas, dicho sea con permiso de los «tecno-optimistas», un colectivo en el que por el momento no tengo el gusto de incluirme (aunque me asome a él con curiosidad).

1.2. UN APRESURADO INTENTO DE DELIMITACIÓN CONCEPTUAL

Transitar ese recorrido exige una labor preliminar de desbroce, mediante un intento de delimitación conceptual. Con ello pretendo llamar la atención sobre determinados trasvases semánticos (conscientes o inconscientes) que

2. Todo ello sin tomar ahora en cuenta la forma en que las nuevas tecnologías pueden incluso inducir cambios normativos: por ejemplo, sin la llamada agenda electrónica de señalamientos y citaciones, el nuevo procedimiento para el enjuiciamiento rápido de los delitos no estaría configurado legalmente como lo está ahora. Sobre esta cuestión me he ocupado recientemente en PÉREZ GIL, Julio, «Digitalización de la justicia y reformas procesales: un balance», en *Estudios jurídicos sobre la Sociedad de la Información y Nuevas Tecnologías. Libro conmemorativo del XX aniversario de la Facultad de Derecho de Burgos,* Burgos, 2005.

en relación con el tema que nos ocupa están a la orden del día. Argumentos de autoridad aparte hay que advertir que investigar un delito se dirige a «comprobar el delito y averiguar el delincuente» según la arraigada dicción de nuestra venerable (por vetusta) LECrim (Título V del Libro II, arts. 326-485). En la medida en que, por definición, el proceso es posterior a la comisión delictiva, la traslación a la instrucción judicial de características, requisitos y efectos de medidas de índole policial, administrativo (o incluso de las propias de los servicios de inteligencia), acarreará distorsiones.

La investigación procesal ha de ser distinguida frente a otras actividades que pueden desarrollarse con anterioridad, simultáneamente o con posterioridad a ella, sin perjuicio de que la trascendencia de tales propósitos, en muchos casos, sea mayor que la de la propia indagación. Aunque sólo sea meramente a beneficio de inventario y con el fin de observar algunos matices que no deberíamos pasar por alto, se hace imprescindible no confundir investigar con: a) impedir la reiteración delictiva; b) tutelar a la víctima; c) recopilar preventivamente todo tipo de informaciones a fin de prevenir delitos; d) asegurar fuentes de prueba para un eventual enjuiciamiento; e) practicar anticipadamente una actividad probatoria (o bien, indirectamente, atribuir valor probatorio a diligencias de investigación); o f) asegurar la efectividad de un eventual pronunciamiento jurisdiccional (tutelar cautelarmente). La equívoca amalgama conceptual a la que me refiero no es exclusivamente reconducible al ámbito de las nuevas tecnologías, sino que más bien es muestra de una tendencia que atraviesa transversalmente las últimas reformas del proceso penal. Sin embargo no me caben dudas de que el sustrato tecnológico está coadyuvando sobremanera a proporcionar espurias justificaciones al respecto, bien sea de manera explícita o bien sea subrepticiamente.

Centrémonos en uno sólo de los aspectos reseñados. En un mundo en que se han hecho comunes términos como «guerra preventiva» o «tutela anticipatoria», no debemos llegar a confundir la prevención del delito o el aseguramiento de eventuales fuentes de prueba con su persecución, o al menos no hacerlo sin reparar en las consecuencias. Quizá un ejemplo sea útil a fin de esclarecer lo que quiero decir: si una norma me obligara a dejar a disposición de la policía una copia de la llave de mi domicilio por si con ocasión de un delito fuera necesario entrar rápidamente a registrarlo, parece claro que estaríamos ante una (claramente desproporcionada) medida preventiva que podría facilitar la investigación, pero en ningún caso ante una medida de investiga-

ción. Por la misma razón, si a los operadores de comunicaciones se les obliga a archivar los datos de tráfico de éstas durante un tiempo (como requiere el art. 12 LSSI), no estamos ante una medida de investigación, sino ante una medida preventiva de aseguramiento de eventuales fuentes de prueba desligada totalmente de la existencia de indicios, la cual, en un ínfimo porcentaje de los supuestos, quizá sea útil para la investigación [3].

Al referirse la LECrim a «*comprobación del delito y averiguación del delincuente*» piensa en una respuesta a hechos ya pasados. En la actualidad, sin embargo, las técnicas policiales proactivas, esto es las relativas a la prevención del delito mediante la acumulación de todo tipo de fuentes de información, están siendo reforzadas frente a aquellas otras que proporcionan una respuesta sólo una vez que el delito ha sido cometido. Lógica e ineludiblemente ambas han de combinarse, pues la investigación de los delitos no sería hoy comprensible sin estas técnicas proactivas, en las que el acopio de datos haciendo uso de las nuevas tecnologías es un elemento esencial [4].

La praxis determina en muchas ocasiones que pueda diluirse hasta desaparecer la barrera entre actividad policial preventiva y represiva, posibilitando la potenciación y protagonismo de la primera, pero revistiéndola bajo el ropaje normativo de la segunda en ausencia de un sustento legal específico. A esa transformación de la realidad policial no son ajenas las nuevas formas de investigación sobre la base de una tecnología avanzada. La tarea en curso radica por tanto en cómo encajar todas las piezas en juego, posibilitando la prevención del delito sobre una base normativa firmemente asentada en los derechos fundamentales. Obviamente este tipo de medidas habrán de sujetarse a los límites del Estado de Derecho, particularmente en lo relativo a la satisfacción de las exigencias dimanantes del principio de propor-

---

3. Obligaciones de conservación de datos se contienen en normas de diversa naturaleza, como por ejemplo lo referido al tacógrafo en la Orden FOM/1190/2005, de 25 de abril, por la que se regula la implantación del tacógrafo digital: el art. 23 contempla el deber de conservación de los datos por parte de las empresas un mínimo de 365 días, y el 26 la obligación de cederlos en los siguientes términos: *«Toda empresa titular de vehículos dotados de tacógrafo digital deberá atender los requerimientos de petición de datos solicitados por parte de los órganos competentes en materia de transportes u otros organismos de control…»*.

4. Es claro además que en determinadas modalidades delictivas (particularmente el terrorismo y otras formas graves de criminalidad organizada) la actuación policial exitosa ha de tomar por base un minucioso trabajo de análisis de informaciones previa e idóneamente compiladas.

cionalidad. De ahí que la verificación judicial, aun en caso de urgencia, haya de erigirse en necesaria garantía, en la medida en que viene a impedir la configuración de ámbitos exentos de control. Aquél debe existir antes, durante y/o después, pero tiene que estar presente de alguna manera, de forma que se pueda autorizar judicialmente una intromisión en la esfera jurídico-fundamental sólo en presencia de indicios y con el debido respeto a la triple vertiente del principio de proporcionalidad (5).

De hecho, en ocasiones puede llegar a percibirse que determinadas medidas preventivas presentan como un guante del revés la triple faz de las exigencias del principio de proporcionalidad en su relación con el logro de los objetivos propuestos: a) podemos dudar del correcto funcionamiento de tales medidas a fin de averiguar los hechos y su presunto autor (defectos en la idoneidad); b) seguramente existan medidas menos gravosas o lesivas (defectos en la necesidad); y c) nos podrían conducir a una evidente desproporción entre los fines buscados y los medios empleados, pues el sacrificio de derechos podría ser excesivo a tenor de la intensidad o del tiempo de duración de la medida (defecto en la proporcionalidad estricta) (6).

1.3. SENSIBILIZACIÓN NECESARIA

Permanentemente nos vemos obligados a replantearnos cuál es nuestra idea de libertad, de intimidad o de seguridad, así como los respectivos entrecruzamientos entre tales conceptos para redefinir nuestras preferencias,

---

5. PEDRAZ PENALVA, E., *Derecho Procesal Penal.* Tomo I. *Principios de Derecho Procesal Penal*, pp. 149 y s. Sobre el principio de proporcionalidad son de imprescindible referencia los trabajos de este mismo autor «El principio de proporcionalidad y su configuración en la jurisprudencia del Tribunal Constitucional y literatura especializada alemanas» o «Principio de proporcionalidad y principio de oportunidad», ambos en PEDRAZ PENALVA, E., *Constitución, Jurisdicción y Proceso*, 1990.

6. Es muy interesante a este respecto el Informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo sobre la iniciativa de la República Francesa, de Irlanda, del Reino de Suecia y del Reino Unido relativa a un proyecto de Decisión marco sobre la conservación de los datos tratados y almacenados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de los datos transmitidos por redes públicas de comunicaciones, a efectos de la prevención, investigación, descubrimiento y represión de la delincuencia y las infracciones penales, con inclusión del terrorismo (A6-0174/2005, de 31-5-2005). La medida es considerada inútil por cuanto *«las personas pertenecientes al ámbito de la delincuencia organizada y el terrorismo saben cómo evitar que sus datos se rastreen»* y *«cabe dudar de la disponibilidad inmediata de los datos solicitados».*

nuestras prioridades o nuestro grado de tolerancia. Ello implica por lo que a nuestro tema respecta una necesaria sensibilización con respecto al contenido jurídico fundamental del derecho a la intimidad, entendido aquí en el sentido más lato posible. La falta de conciencia social de las repercusiones en orden a la defensa de ese derecho lleva aparejado un desconocimiento mayor o menor sobre la lesividad potencial de las nuevas herramientas de investigación. En la medida que su aceptación sea acrítica, incluso por los instructores en cuyas manos se deposita la facultad de autorizar medidas limitativas de derechos fundamentales con vistas a la investigación criminal, estaremos abriendo la puerta a su utilización desmedida. Incluso las leyes que las reconocieran expresamente, siendo imprescindibles, no serían a estos efectos suficientes porque los sentimientos no se cambian a través de ellas. Se trata de algo más, de algo que tiene que ver con una conciencia general, con la percepción que el ciudadano asigne a la cuestión, con una cultura en la que se otorgue valor a unas libertades que se han hecho tan familiares y tan necesarias como el aire que respiramos.

Puesto que la tecnología no puede ser la panacea, desde luego no podría ser cierta, por ejemplo, la identificación unívoca entre la seguridad y el control derivado de acopios masivos de datos. De ahí que no debamos caer en la frecuente trampa de contraponer seguridad a libertad, como si de vasos comunicantes se tratara, en los que de un incremento de la primera se derivase un detrimento de la otra. No sería conveniente ceder subrepticiamente libertad (aunque sea virtualmente) en pos de una promesa de mayor seguridad, puesto que ni siquiera en esas condiciones la seguridad sería absoluta y esa cesión sería muy difícil de revocar o dejar sin efecto.

Sirvámonos de otro ejemplo al respecto: salvo a los protagonistas de algunos programas de televisión, a casi nadie nos gusta ser observado y grabado de forma permanente por cámaras, aun cuando un control de ese tipo pudiera tener alguna eficacia en la lucha contra la delincuencia. Por contraposición, no siempre reparamos en el volumen de datos que sobre nosotros se acumula minuto a minuto, tanto por instancias administrativas como por particulares. La información resultante del entrecruzamiento de las bases de datos de los archivos del DNI, movimientos de tarjetas de crédito, utilización de telecomunicaciones, alojamientos hoteleros y un larguísimo etcétera hace que resultemos mucho más transparentes para quien tenga la facultad de tratarla adecuadamente que todas las videocámaras que nos pusieran por

delante. El acceso a ese cúmulo de datos puede ser esencial con el fin de perseguir el delito, pero dependerá de en manos de quién se deposite, en qué condiciones y con qué mecanismos de control. El control social no es algo exclusivo de los tiempos actuales (pensemos en la vida en una ciudad de provincias de hace cincuenta años). ¿Dónde radica entonces la preocupación por habernos convertido hoy en día en ciudadanos transparentes? Probablemente ello tenga que ver, además de con la potencia de las herramientas que se manejan actualmente, con la identidad del controlador o, mejor dicho, con el desconocimiento de quién pueda ser ese controlador y con qué cobertura actúa.

Por otro lado, el impulso que se deriva del ánimo de combatir el terrorismo y otras formas graves de criminalidad abre la puerta a la introducción de medidas que suponen un alto grado de injerencia en los derechos fundamentales. Con ello, y sin atisbo de crítica, pueden hacer su entrada en las normas procesales disposiciones de carácter excepcional habilitadas por ejemplo para la persecución de gravísimos delitos socialmente muy dañosos [7], pero que subrepticiamente podrían llegar a generalizarse para cualesquiera modalidades delictivas.

La preocupación por la seguridad, exacerbada por el miedo a amenazas criminales ciertas, nos viene a situar en una dimensión novedosa: lo que importa es recoger información, cuanta más mejor, con independencia de su origen público o privado y de que no se sepa a ciencia cierta para qué puede ser utilizada en el futuro. La extensión de medidas preventivas propiciada por la técnica determina que todos nos hayamos transformado en sospechosos, por lo que podemos ser objeto de atención en todo momento. La conservación de datos relativos al tráfico telefónico, al correo electrónico, a los accesos a Internet se encomienda a sujetos privados, pero ello se hace con fines de persecución del delito (o al menos así se justifica). Los poderes públicos se sirven con esa finalidad de quienes ya han puesto su atención sobre nosotros (bien porque hemos prestado nuestro consentimiento expreso o tácito, bien porque la ley nos obliga), requiriendo su colaboración cuando sea preciso.

---

7. Por ejemplo, el art. 2.2.c) LOPD excluye de su ámbito de aplicación «*A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada*».

2. INSUFICIENTE ENCAJE LEGAL

2.1. LA NECESARIA HABILITACIÓN LEGISLATIVA

Mientras que la investigación penal ha ido sufriendo un proceso lógico pero radical de transformación al hilo de los avances técnicos y de la articulación de eso que se ha dado en llamar la «sociedad digital», no puede decirse que ello se haya visto traducido con nitidez en la legislación procesal penal (y ni siquiera con la debida rotundidad en la jurisprudencia). Hoy por hoy nuestro ordenamiento jurídico en relación con las medidas de investigación penal en las que la tecnología ocupa un papel relevante no cumple, ni aun en la más benevolente de las interpretaciones posibles, las condiciones exigidas por el art. 8.2.º del Convenio Europeo de Derechos Humanos para las injerencias en la intimidad. Mientras la materia a regular hizo su entrada hace ya bastante tiempo en el siglo XXI, su plasmación en la norma procesal penal sigue instalada en pleno siglo XIX.

La restricción de derechos fundamentales, por supuesto previa autorización judicial, también en el nuevo entorno tecnológico precisa expresas y concretas habilitaciones legales, sin que pueda considerarse suficiente la invocación de las de carácter genérico que se vienen utilizando en la actualidad. A mi juicio ha de considerarse inaplazable, y no puede hacerse esperar hasta la elaboración de una nueva Ley de Enjuiciamiento Criminal, la introducción de normas expresas que posibiliten que los jueces autoricen concretas y novedosas medidas de investigación lesivas de la intimidad personal y familiar o del derecho a la protección de datos personales. Ello conllevará necesariamente aparejada una modificación en las conductas de las autoridades de la persecución penal en el intento de ajustarse a la norma, para arrinconar la conciencia de que en la investigación «todo vale».

Del legislador ha de ser exigible que mantenga una actitud vigilante y de diligente actualización. O dicho con palabras de una reciente sentencia del Tribunal Constitucional Federal alemán [8]: *«A causa de los cambios tecnológicos derivados de la sociedad de la información, rápidos y peligrosos para la protección de los derechos fundamentales, el legislador tiene que observar con*

8. BVerfGE de 12 de abril de 2005 – 2 BvR 581/1.

atención los desarrollos tecnológicos y, en caso de urgencia, intervenir mediante legislación complementaria corrigiéndola…». Pero en la medida en que en este preciso instante se hacen perceptibles afecciones a derechos fundamentales sin sustento legal claro, no parece que quede otro remedio que aplicar la doctrina del periodo transitorio *(Übergangszeit)*, también acuñada por el Tribunal Constitucional Federal alemán: las medidas restrictivas de derechos fundamentales carentes de una regulación legal expresa sólo pueden ser aplicadas durante un lapso temporal transitorio, en tanto el legislador acomete la tarea de su elaboración, a la cual se verá compelido por decisiones jurisprudenciales en ese sentido [9].

Por situarnos nuevamente ante un ejemplo, diremos que por definición toda investigación penal tiene por objeto la búsqueda de datos. Hoy, en plena sociedad de la información y el conocimiento, las medidas que implican tratamiento (automatizado o no) de los datos personales son uno de los pilares sobre los que se asienta cualquier indagación, con lo que también podríamos hablar de la digitalización de la instrucción. Pero nuestra normativa procesal penal no sólo se halla anclada en un mundo analógico, sino que lo está en uno superado ya por el curso de los tiempos, sin alcanzar a ver la trascendencia de la protección de datos. Ello hace que nos enfrentemos constantemente a dudas sobre cómo trasvasar los conceptos de tratamiento o de cesión de datos al proceso penal, máxime cuando se trata de datos que pueden haber sido recogidos antes de la comisión de los hechos y para finalidades absolutamente diversas.

El cuerpo humano (datos biométricos), la red de contactos y comunicaciones trabados (telefonía, Internet, etc.), la localización geográfica (mediante el teléfono móvil, GPS y dispositivos de localización como los smart tags de radiofrecuencia RIFD), las transacciones económicas, etc. son fuentes de información valiosísima en orden a la averiguación de los delitos. Pero si irremisiblemente vamos hacia la construcción de un nuevo estatuto jurídico político del ciudadano (el llamado «ciudadano transparente»), más vale que nos preparemos para ello estableciendo pautas, requisitos, barreras, impedimen-

9. Sobre la necesidad de un fundamento legal para adoptar medidas limitativas de los derechos fundamentales en la investigación penal (referida a la habilitación legislativa para la práctica de medidas de intervención corporal) vid. la reciente STC de 14 de febrero de 2005 (ponente García-Calvo), FJ 6, así como el voto particular de Casas Baamonde al que se adhiere Aragón Reyes.

tos, límites en definitiva establecidos con luz y taquígrafos y con las bendiciones que se derivan de una habilitación legal expresa y clara.

En muchas ocasiones la verdadera relevancia de los mecanismos de investigación tecnológicamente avanzados y ocultos al sujeto investigado deviene invisible mediante su transmutación y la incorporación de la información al proceso por otras vías. Parece necesario por tanto hacer visibles en la ley aquellas modalidades de investigación que, utilizándose *sotto voce*, quedan enmascaradas en los atestados policiales bajo la cauta expresión de «de las diligencias practicadas...». Otro de los retos pendientes a este respecto será por ende el engarce que establezcamos entre las fuentes de prueba tecnológicamente avanzadas y las que, por ser visibles en la ley (por estar expresamente descritas al corresponderse con concretos medios de prueba), se hacen preponderantes en la forma en que se presentan a fin de entrar en el juicio oral.

Recapitulemos ahora: 1) estamos ante afecciones a derechos fundamentales con motivo de la investigación; 2) la legislación es claramente deficiente y en algún caso, directamente inexistente: no cumple las exigencias del principio de legalidad (formal y material) según los reiterados requerimientos del TEDH en interpretación del art. 8.2 CEDH; 3) conscientes de ello, pero cautelosas ante lo que pueda pasar, las autoridades encargadas de la persecución, actuando cada uno en su papel (policía, fiscales y jueces), echan tierra encima y hacen como que no se han enterado de dónde puede proceder una información tan profusamente detallada; 4) lo averiguado sirve de fundamento para la obtención de otros elementos de cargo, estos sí, cuidadosamente fundamentados en los requerimientos legales. Si después de ello seguimos sin entender que nos hallamos ante un típico caso de ilicitud probatoria por vulneración de derechos fundamentales derivada de la ausencia de fundamento legal habilitante (la necesaria *interpositio legislatoris*) es que estaremos aplicando la teoría de la conexión de antijuridicidad con brocha gorda.

2.2. CRIMINALIDAD INFORMÁTICA: ALGUNAS SUGERENCIAS

Como en tantas ocasiones ocurre en la ciencia jurídica (así como en todo el amplio mundo de las ideas), las construcciones *ex novo* son algo extraño: normalmente aprovechamos cimientos que han demostrado su solidez o que merecen ser derribados por su endeble constitución. La digitalización de la

información nos está obligando no obstante a detectar ámbitos donde se sitúan novedades verdaderamente relevantes y, por lo que a nosotros respecta, específicamente las referidas a la persecución penal. Con ello nos vemos obligados a discernir en cada caso si lo que ha sucumbido, deviniendo inútil, insuficiente o infructuoso, son concretos preceptos que han de ser amputados del ordenamiento jurídico o si esa debacle alcanza a también a alguno de los valores y principios que entendíamos sólidamente consolidados.

Para averiguar cuál ha de ser la acogida que una futura ley procesal penal deba dar a las nuevas tecnologías podría ser conveniente tratar de hacernos una idea sobre qué debemos entender por criminalidad informática y sus repercusiones en el orden procesal. Un buen principio a tal efecto viene constituido por el art. 14 del Convenio sobre el Cibercrimen que, al establecer el ámbito de aplicación de las normas procesales en él contenidas, se refiere a todas las conductas con apariencia criminal, siempre que nos hallemos en un entorno de comisión delictiva en el que los medios informáticos hayan desempeñado un papel relevante. Se toma en cuenta por tanto la utilización de sistemas y datos informáticos en tres diferentes perspectivas: como objeto mismo sobre el que se produce el delito; como instrumento para la comisión delictiva; pero también, el que ahora nos importa, como simple soporte de información [10]. Si este último aspecto lo conectamos con las definiciones de sistema y datos informáticos establecidas por el art. 1 del mismo Convenio y reparamos en el índice de penetración que éstos tienen en la sociedad de nuestros días, fácilmente llegaremos a la conclusión de que prácticamente todos los delitos podrían entrar en la categoría de delitos informáticos.

Puesto que casi todos los delitos (valga la exageración) pueden constituir delincuencia informática, casi toda la investigación penal lo será sobre nuevas tecnologías en la medida en la que habrá sistemas o datos informáticos que sirvan de soporte a información relevante (un teléfono móvil, una agenda electrónica, la utilización de un cajero automático, etc.: todos ellos contienen sistemas informáticos). En esa tesitura lo lógico será configurar un marco legal que, debidamente encajado en el núcleo jurídico fundamental, posibilite la traducción al proceso penal de las características que definen las profundas transfor-

10. Al respecto vid. PÉREZ GIL, Julio, «Medidas de investigación y de aseguramiento de la prueba en el "Convenio sobre el Cibercrimen"», *Actualidad Penal*, núm. 36, 2003, pp. 895-933.

maciones que ha impulsado la sociedad de la información: a) desmaterialización de los bienes objeto del tráfico jurídico; b) desterritorialización e irrelevancia de fronteras o distancias geográficas; c) horizontalización, en la medida en que los mecanismos de comunicación y de intercambio de información toman por base la existencia de redes, tanto abiertas (Internet) como cerradas, y d) transparencia, dado que los actos de personas y organizaciones se hacen visibles y pueden interrelacionarse (11).

En vista de ello, el marco referenciado debería agrupar, al menos, las siguientes características:

a) Ha de establecerse una clara separación entre medidas de investigación sobre sistemas informáticos (continente) frente a medidas relativas a datos (contenido). Tratándose de estos últimos habrá de distinguirse los que sean parte de un proceso de comunicación (de contenido o de tráfico) de aquellos otros que se encuentren almacenados en un sistema. Una vez trabada esa distinción las medidas de aseguramiento de la prueba y el análisis forense se configurarán de diferente forma en uno y otro caso: mientras que en el caso de los sistemas estamos ante algo tangible (cabe por ejemplo un precinto), en el caso de los datos la información puede ser asegurada de múltiples formas (por ejemplo, mediante una simple copia). Seguir tratando a los sistemas y a los datos como «efectos del delito», «libros y papeles», etc. tal y como sigue haciendo nuestra LECrim puede ser calificado, cuando menos, de conceptualmente erróneo (12).
b) En relación con medidas ya existentes, deberían enunciarse al menos los requisitos para su adopción, satisfaciendo con ello la exigencia de habilitación legal expresa del art. 8.2 CEDH. Entre ellos ha de contarse al menos con: 1) autorización judicial en el marco de un proceso expresa y con motivación suficiente; 2) decisión basada en indicios suficientes; 3) estricta observancia del principio de proporcionalidad; 4) limitación a de-

11. NETHERLANDS ADVISORY COMMISSION ON HUMAN RIGHTS IN THE INFORMATION SOCIETY, *Human Rights in the Digital Era (Grondrechten in het digtale tijdperk)*, La Haya, 2000, pp. 22-29.

12. La regulación actual de los registros de sistemas o archivos nos obliga a una forzada traslación de la normativa sobre registro de papeles y otros efectos, de la entrada en lugar cerrado (art. 546 LECrim), del registro de libros y papeles de contabilidad (art. 573 LECrim), con recogida por el Juez y dación de fe por el secretario (art. 574). Pero ¿cómo damos audiencia al imputado (arts. 576, 569 LECrim)? o ¿dónde situamos los límites de la prohibición de inspecciones inútiles (arts. 576, 552 LECrim)?

terminadas categorías delictivas en función de su naturaleza o gravedad; 5) control judicial de su práctica; 6) supuestos en que es necesaria la presencia del acusado (o al menos proporcionarle información) cuando no perturbe el resultado de la investigación.

c) Debería contemplarse la implantación de habilitaciones legales expresas para algunas novedosas medidas de investigación tales como accesos remotos a sistemas conectados en red, instalación de programas rastreadores, dispositivos de localización geográfica, búsquedas cruzadas de datos, etc. El art. 282 LECrim no admite seguir amparando toda modalidad de investigación policial que no venga prevista en otro sitio. Las cláusulas legales en las que tales previsiones se recogieran deben estar abiertas al desarrollo tecnológico, no conteniendo opciones tecnológicas concretas. Tampoco habrán de tener un carácter demasiado minucioso (que estaría sólo al alcance de su entendimiento por unos pocos), pero sin que esa falta de precisión llegase a conminar a los cuerpos de investigación y enjuiciamiento a integrar imaginativamente su contenido.

d) Tendrá que establecerse protocolariamente la actuación armonizada de todos los implicados. Ello requerirá flexibles instrumentos de carácter infralegal, configurando mecanismos de coordinación entre policía y otros cuerpos de investigación, fiscalía, tribunales, pero también operadoras de telecomunicaciones, administradores de sistemas, etc. La genérica obligación de colaboración con la Justicia (arts. 118 CE, 17 LOPJ, 4.1 LOFCS) habrá de ser concretada.

e) Homogeneidad con la legislación procesal penal de nuestro entorno, de manera que permita una ágil cooperación judicial y policial no sólo en el ámbito de la UE, sino también en el marco de las estructuras de asistencia previstas en diversos instrumentos de Derecho Internacional (Convenio europeo de asistencia judicial de 1959 y sus protocolos, Convenio sobre el Cibercrimen, etc.). Precisamente algunos de los más graves problemas en este sentido derivan siempre de la falta de homogeneidad normativa, máxime cuando nos encontramos ante una materia para la que las distancias geográficas, las fronteras e incluso los idiomas devienen irrelevantes.

f) Deberá evitarse convertir en generales las medidas que están dotadas de un carácter de excepcionalidad: una de las peores respuestas que cabe

imaginar frente al terrorismo y otras formas graves de criminalidad sería aquella que, guiada por el pánico y la urgencia, nos deslizara subrepticiamente hacia una erosión de derechos.

2.3. INCLUSIÓN DE LA PROTECCIÓN DE DATOS PERSONALES ENTRE LAS GARANTÍAS DEL PROCESO PENAL

Nuestro sistema de organización social toma ya por base, abierta o discretamente, la disponibilidad de informaciones de todo tipo, y el volumen de datos personales que de cada uno de nosotros son coleccionados en los más diversos ámbitos probablemente desborde cualquier idea que podamos preconcebir. Esa (relativa) novedad se corresponde con la impostación de una suerte de contrapoder asignado de forma difundida a todos los sujetos particulares (si bien con intervención también de órganos públicos). Europa es el área geográfica donde la tutela de la intimidad es más alta y ello no se debe a que aquí se recojan menos datos que en otros lugares, sino a la simple razón de que al menos hemos ido ganando un poder de disposición sobre los datos que nos atañen: podemos determinar las condiciones en que información relativa a nuestra persona pasa a disposición de los demás. O en otros términos, teóricamente deberíamos podemos saber qué es lo que se sabe de nosotros. La protección de datos no alude por tanto solamente a la reserva con la que se han de tratar ciertas informaciones, sino que viene fundamentalmente caracterizada por el reconocimiento a todos los ciudadanos de un poder de control sobre sus propios datos, en todo momento y dondequiera se encuentren. Ello permite hablar de un poder de control que desde el punto de vista activo tiene un carácter individualizado, pero también difuso, y desde el punto de vista pasivo va dirigido frente a todos aquellos sujetos que disponen de datos de carácter personal [13].

Cuando se trata de los mecanismos de persecución del delito, entre los cuales incluimos al proceso penal, parece evidente que esa facultad de disposición ha de quedar debilitada, pues nos hallamos en presencia de un interés

13. De ahí que se sostenga que en el marco de la Unión Europea es posible anunciar la creación de un nuevo «modelo» que, reforzando la esfera privada, refuerza al mismo tiempo el peso de cada uno en la esfera pública, para concluir que el derecho fundamental a la protección de datos personales se transforma en un elemento básico de la nueva «ciudadanía electrónica» (RODOTÀ, Stefano, «Democracia y protección de datos», texto de la conferencia disponible en https://www.agpd.es/upload/Conferencias/DemocraciaMadrid.pdf).

mayor. El problema es si llega a anularse hasta el extremo de convertirse en quimérica o si el derecho fundamental a la protección de datos personales, novedosamente configurado por la jurisprudencia constitucional al menos desde la STC 292/2000, de 30 de noviembre, construyéndolo a partir del art. 18.4 CE (y previa su distinción con el derecho a la intimidad personal y familiar del 18.1 CE) deberá erigirse en un nuevo filtro ponderador de las medidas adoptadas en la investigación. La cuestión será entonces plantearnos en qué medida eso puede considerarse necesario en una sociedad democrática, tal y como literalmente exige el art. 8 CEDH.

Enfrentarnos cabalmente con la cuestión de la protección de datos en la investigación penal nos obliga por ende a conjugar dos elementos que, pudiendo parecer antitéticos, comparten la característica de ser factores determinantes de la aparición de relevantes implicaciones jurídicas. De la aparente lucha entre ambos, pero también de sus mutuas implicaciones, deberemos extraer algunas conclusiones que aspiran a una validez general. Tales elementos son: a) la protección de datos personales en su dimensión de autodeterminación informativa, esto es, entendida como la facultad de un sujeto de decidir qué es lo que los demás conocen de él; y b) la investigación penal entendida como búsqueda del mayor volumen posible de información sobre unos hechos (datos objetivos) y sobre su presunto autor (datos personales). El conflicto entre ambas se pone de manifiesto si se considera que hacer énfasis en la primera supondrá necesariamente un detrimento de la segunda, pues la fase de investigación del proceso penal constituye una continuada intromisión en el ámbito de tutela que propicia toda la normativa de protección de datos personales.

Creo no obstante que la confrontación entre protección de datos y proceso penal no debe llegar a generarse, puesto que se trata de ámbitos no sólo congruentes entre sí, sino que se pueden entender íntimamente imbricados. La identificación que se ha hecho en ocasiones entre «protección de datos» y «protección del delincuente» *(Datenschutz=Täterschutz)* no tendría que llegar a ponerse sobre la mesa salvo aceptando ese «derecho penal del enemigo» en el que desde algún sector se nos parece querer hacer entrar. La «protección de datos» no tiene por qué estar reñida con los fines del proceso penal, sino que ha de estar ensamblada con éstos. Hoy por hoy podemos considerar que el respeto al derecho a la protección de datos es una componente más del sismógrafo de la Constitución que, en las famosas palabras de ROXIN, constituye el debido proceso penal.

La búsqueda de la mejor de las formas que permita engastar la protección de datos entre las garantías del debido proceso ha de ser objeto de un profundo análisis que excede con mucho los límites de este trabajo. Pero una primera aproximación constructiva nos obligaría a percibir la cuestión como una confrontación entre bienes jurídico-fundamentales, si se quiere en diferentes planos y con diferentes caracteres, pero reconociendo al fin y al cabo que ya hemos superado el umbral de los derechos fundamentales. Será deber del legislador facilitar una ponderación en abstracto de esos intereses contrapuestos, algo que con el debido control judicial habrá de verificarse en lo concreto. Ello nos ofrecerá como ventaja la eventual utilización de toda una sólida jurisprudencia constitucional que nos habla de contenido esencial, límites, requisitos, condiciones, etc. y, lo que es más importante, vendría a imponer expresamente un control judicial en la ejecución de medidas que ahora de forma visible exteriorizan su carácter de limitativas de los derechos fundamentales.

El acceso a datos personales por parte de la policía, así como su tratamiento, es una actividad que integra hoy habitualmente sus funciones y constituye en la inmensa mayoría de las ocasiones una forma de actuación completamente al margen de la actividad jurisdiccional (y ni siquiera de la del Ministerio Fiscal). Su encaje legal es más que dudoso, en la medida en que carecemos de una previsión legal que configure un soporte regulador de las búsquedas entrecruzadas de datos. Cabría preguntarse lícitamente ¿podemos considerar amparado por las genéricas funciones de averiguación del delito asignadas a la policía una medida que suponga la creación de un perfil de un sujeto? Y en caso afirmativo, ¿cuáles podrían ser los patrones de búsqueda y quién está capacitado para delimitarlos? ¿Dónde estarían sus límites subjetivos, objetivos o temporales? ¿Qué hacemos con los datos inútiles? Parece claro que necesitamos algún tipo de previsión legal al respecto, tal y como contempla el ordenamiento alemán: §§ 98ay, b StPO, que regulan la *Rasterfahndung* (rastreo de pistas) [14], § 163d StPO, regulador de la *Schleppnetzfahndung* (análisis comparativo de datos personales recogidos en el caso de un control fronterizo o un control policial ruti-

14. La medida no ha recibido un tratamiento doctrinal considerable, en parte a causa de su escasa utilización en la práctica. Al respecto vid. GRAF, Walther, *Rasterfahndung und organisierte Kriminalität*, Bonn, Forum-Verlag Godesberg, 1997, así como en nuestra lengua CANO PAÑOS, Miguel Ángel, «El *Rasterfahndung* en el Derecho Procesal Penal Alemán y su aplicación práctica en la lucha antiterrorista», *Revista Electrónica de Ciencia Penal y Criminología,* mayo-junio de 2003 (http://criminet.ugr.es/recpc).

nario) y § 163e StPO, regulador de la llamada *polizeiliche Beobachtung* (observación policial).

Por otra parte, ni siquiera nuestro TS otorga la relevancia requerida a la materia que nos ocupa tal y como acredita la copiosa jurisprudencia relativa a peticiones de registros y listados de llamadas (15). Aun admitiendo que no afectan al secreto de las comunicaciones, tales listados pueden contener datos de carácter personal. Pero el alto tribunal suele considerar bastante una providencia sin motivación alguna para acordar su solicitud (16), o no delimita con la suficiente nitidez conceptos esenciales de la normativa de protección de datos que sin embargo entiende de aplicación (17). Una cosa es que no nos hallemos en el ámbito del art. 18.3 CE, pero otra muy diferente es sostener que en absoluto estemos ante un derecho fundamental a fin de excluir del monopolio jurisdiccional la adopción y control de aquellas medidas que pudieran vulnerarlo o devaluarlo.

3. DE LOS INDICIOS A LA VALORACIÓN DE LA PRUEBA: UN RECORRIDO MARCADO

Corresponde ahora reparar en algún detalle de los mecanismos mediante los que el cúmulo de información recabada con fines preventivos atraviesa la ba-

---

15. La jurisprudencia de la Sala 2.ª sobre listados de llamadas es abundantísima en los últimos tiempos: STS 23/2005, de 21 de enero (RJ 2005/1508); STS 1219/2004, de 10 de diciembre (RJ 2004/7917); STS 1167/2004, de 22 de octubre (RJ 2004/7951); STS 889/2004, de 9 de julio (RJ 2004/7664); STS 1683/2003 (Penal), de 11 de diciembre (RJ 2004/186); STS 769/2003 (Penal), de 31 de mayo (RJ 2003/4285). Acorde con el derecho fundamental a la intimidad en el supuesto de recabar listado de llamadas parece la sentencia núm. 769/2003 (Sala de lo Penal), de 31 de mayo (RJ 2003\4285, Ponente Martín Pallín) al hacer constar que *«Lo cierto es que, por sus especiales características, afectaba al derecho a la intimidad del denunciante y ofendido por el delito, por lo que la actitud inicial, observada por el Juez de Instrucción, al solicitar la entrega voluntaria de los datos, fue absolutamente correcta y respetuosa con el derecho fundamental afectado».*

16. Eso es lo que ocurre, por poner un ejemplo de en la STS 1219/2004 (Penal), de 10 de diciembre (ponente Saavedra Ruiz), FD 16.º Un dictamen de la Agencia de Protección de Datos fechado en 1999 vino a convalidar la idoneidad de las solicitudes de datos efectuadas por la Policía Judicial sin mandamiento judicial o requerimiento previo del Ministerio Fiscal, un fundamento al que todavía hoy se siguen aferrando los cuerpos policiales en sus requerimientos de aportación de datos.

17. El ejemplo nos lo proporciona la STS 1167/2004 (Sala de lo Penal), de 22 de octubre (RJ 2004\7951), Ponente Berdugo y Gómez de la Torre, en la que no se distinguen los requisitos del consentimiento para el tratamiento (art. 6.2 LOPD, innecesario cuando es tratamiento de datos personales por las administraciones) de los del consentimiento para la cesión (11.2.d, en el que se habla únicamente del Ministerio Fiscal y los Jueces o Tribunales, pero que no se refiere a la Policía).

rrera de lo virtual, para dotarla de genuina y poderosa eficacia probatoria. ¿Cómo repercute el cambio de orientación descrito en páginas anteriores, a tenor del que lo relevante no es ya tanto la represión del delito cuanto su hipotética prevención y, en todo caso, el aseguramiento de fuentes de información que puedan llegar a erigirse en fuentes de prueba? ¿Cuál es el lugar del proceso penal en todo esto, teniendo en cuenta que, por definición, éste se diseña para perseguir hechos de apariencia delictiva que ya han sucedido?

Uno de los riesgos provocados por la irrupción de nuevas tecnologías en el proceso penal es la posibilidad de facilitar el socavamiento del papel del juez, convirtiéndolo en un instrumento de mera convalidación de lo fáctico. Al configurar ámbitos especiales que *(de facto)* se detraen de su control, la pérdida del papel director de la investigación por parte de la autoridad judicial queda indisolublemente relacionada con el grado de especialización técnica requerido, algo que en la práctica ampararía su apartamiento [(18)]. Tras la merma de sus funciones en beneficio de la actividad policial, la necesidad de conocimiento del juez queda con ello diluida.

La requerida especialización para una investigación precisada de una tecnificación y grado de conocimiento exacerbado puede ser una de las vías para que la policía pueda verse liberada de controles por parte del instructor y el fiscal. La complejidad técnica en la investigación de determinados delitos o la urgencia para asegurar fuentes de prueba se han erigido en muchas ocasiones en la única motivación para delegar en la Policía Judicial funciones eminentemente ligadas a facultades judiciales instructoras [(19)]. Nos enfrentamos por ello con la no lejana amenaza advertida por PEDRAZ en otra sede de que *«de un juez decisor —imprescindible y activo protector de los derechos y libertades fundamentales— se llegara al simple homologador formal de decisiones administrativas de policía»* [(20)].

---

18. A ello hace referencia ETXEBERRÍA GURIDI, J. F., *La protección de los datos de carácter personal en el ámbito de la investigación penal*, Agencia de Protección de Datos, 1998, p. 153.

19. Vid. LÓPEZ ORTEGA, J. J., «La admisibilidad de los medios de investigación basados en registros informáticos», en *Delincuencia informática. Problemas de responsabilidad*, Consejo General del Poder Judicial, Madrid, 2002, pp. 77-111.

20. Es el caso de PEDRAZ PENALVA, Ernesto, «Reflexiones sobre el procedimiento para el enjuiciamiento rápido de determinados delitos», en *Revista Jurídica de Castilla y León*, núm. 1, septiembre de 2003, p. 42. Alude el citado autor a la escasa motivación de las resoluciones judiciales permisivas de la diligencia de entrada y registro domiciliario, lo que no impide su extrapolación a la intervención de las comunicaciones o a

Convertir la fase de investigación judicial en una suerte de sumario virtual donde todo venga prediseñado por la policía puede por tanto ser interpretado como parte de una flexibilización del proceso penal que lleva no sólo a su desfiguración sino a su deconstrucción. La preconstitución probatoria que la tecnología lleva implícita puede erigirse con ello en fuente de debilitamiento del judicial, al convertirle en mero agente de convalidación de unas decisiones que le vienen ya tomadas.

Cabría preguntarse en relación con la valoración de la prueba si la utilización de medios técnicos la compromete en algún sentido (21). La respuesta podría sorprender si se tiene en cuenta que nos encontramos con normas que, *de facto*, inducirán a una valoración tasada de la prueba: será ínfimo el margen de posibilidades de apreciación que se le presentan al juez para apartarse sin incurrir en arbitrariedad de los resultados que una determinada tecnología pone a su disposición. Puesto que sólo puede examinar superficialmente lo que se le presenta (no tiene mucho tiempo y sí mucho trabajo) podríamos encontrar fácilmente una sobrevaloración de meros indicios, elevándolos incluso al carácter de prueba cuasi-anticipada en virtud de su irrepetibilidad. Valiéndonos de un símil tecnológico podríamos entender que el juez no percibirá el producto (la prueba) con sus propios sentidos sino que, aplicando un lector óptico a un código de barras que alguien (la Policía) ha adherido sobre ese producto, obtiene un resultado que plasmará por escrito en su resolución para hacerlo propio.

Pero el problema es aún mayor, en la medida en que el juez no sólo está atado por la configuración del atestado que le venga dada por la policía judicial, sino que ni siquiera ésta se halla en disposición de controlar el resultado de la investigación hasta sus últimas consecuencias: el funcionamiento de la tecnología forense puede ser imposible de refutar por contar con zonas inaccesibles. Tratándose de investigaciones y análisis forenses que requieran la utilización de programas de código cerrado (es decir, prácticamente todos) no podemos

---

otros supuestos como el acuerdo de secreto de las actuaciones (conforme al artículo 795.3 LECrim según redacción dada por Ley 38/2002, de 24 de noviembre), al que el propio autor se refiere.

21. Un reciente estudio empírico comparado parece demostrar que la utilización de la prueba tecnológicamente avanzada no favorece tanto la exactitud en la valoración como la mera acumulación de conocimiento. Vid. JOBARD, Fabien y SCHULZE-ICKING, Niklas, *Preuves hybrids. L'administration de la preuve pénale sous l'influence des techniques (France, Allemagne, Grande Bretagne),* CESPID, 2004

conocer con plenas garantías qué es lo que realmente hace el software o si, además, despliega actividades que nos permanecen ocultas. En tales supuestos (por ejemplo en cualquier extracción de datos de un sistema informático) y en la medida en que los programas están basados en un código fuente oculto a cualquier mirada ajena a la de sus creadores, su fiabilidad conlleva la imposibilidad intrínseca de una verificación absoluta. Ésta sólo será posible a través de los llamados «test de caja negra» repetidos con cada nueva versión del programa verificado, a través de los que se analizan los resultados aportados por el software en diferentes marcos hipotéticos o en diferentes situaciones a fin de extraer consecuencias. No podemos desconocer que la valoración de la prueba ha de entenderse íntimamente relacionada con la posibilidad de verificar, y en su caso contradecir, el resultado arrojado por una determinada actividad de investigación forense. Con otras palabras: el imputado que se viera perjudicado por un dictamen forense realizado con software de código cerrado no estaría en disposición de poder realizar un contraanálisis plenamente eficaz, en tanto toparía con un área vedada a la refutación (22).

Partiendo de ello, para concluir que estamos en presencia de pruebas tasadas sobre las cuales el juez tiene necesariamente que formar su convicción no hay más que un paso: el que nos conduciría a reconocer la claudicación del derecho frente a la tecnología. El carácter no verificable en plenitud del resultado probatorio no se deriva en estos casos de lagunas en el conocimiento científico, sino de un propósito ínsito en el propio diseño de la herramienta informática. El componente humano es esencial en la técnica, pues tras todo desarrollo se puede encontrar una dimensión volitiva: alguien en algún momento ha decidido el cuándo, el quién y el para qué de la novedad. En otros términos cabría decir que alguien, solapadamente, ha dictado una norma (el código, en la conocida terminología de LESSIG) que se erige en el núcleo medular del que la ley (procesal) sólo puede aspirar a ser su recubrimiento externo (23).

---

22. Con el fin de poner coto a tales problemas, el Instituto Forense Holandés ha desarrollado y publicado un programa bajo licencia de código abierto denominado TULP2G para la lectura y decodificación de datos archivados en dispositivos electrónicos móviles (teléfonos, PDAs, etc.). Más información en http://europa.eu.int:80/idabc/en/document/3675.

23. LESSIG, Lawrence, *El Código y otras leyes del ciberespacio*, Taurus, Madrid, 2001. Edición original *Code and other laws of cyberspace*, 1999. Un ejemplo de ello sería la arquitectura de Internet, pensada sobre formas de permanente identificación entre máquinas, lo cual posibilita el seguimiento de flujos de información. El verdadero anonimato en Internet sería, por el momento, técnicamente complejo y jurídicamente ilegal.

Quizá no nos quede más remedio que reconocer que el juez se ha convertido en un árbitro entre peritos, pero no atemos a éstos las manos y dejemos al menos que cuenten con las herramientas necesarias para realizar su trabajo de expertos.

4. A MODO DE CONCLUSIÓN

La técnica se gana día a día un crédito propio basado en su utilidad. El Estado de Derecho, del que el proceso penal es un parámetro de medición esencial, necesita también realizar esa tarea y ello sólo puede derivar de acreditar permanentemente sus valores intrínsecos. Ciertamente la tecnología ha hecho que el mundo haya cambiado mil y una veces y, en la actualidad, lo hace a una velocidad de vértigo. Si la tecnología sirve para dar forma a un mundo mejor, también servirá de forma irreversible a esa ínfima parte de él que conocemos como derecho procesal. A cambio, éste deberá actuar en consecuencia: no podemos incorporar nuevas modalidades tecnológicas a la investigación penal buscando aprovecharnos sólo de sus potenciales e indiscutibles ventajas, sino que necesariamente habremos de afrontar las inflexiones y debilidades que ineludiblemente pueden generar en el sistema.

No es mi intención plantear una visión descarnadamente negativa de un sistema legal falto de adecuación a los tiempos que corren (aunque soy consciente de estar haciéndolo en alguna medida). Mi aspiración es la de llamar la atención sobre algunos de los retos pendientes que nos esperan a la vuelta de la esquina, propósito que ha de entenderse justificado si con ello podemos eludir al máximo la discordancia entre por un lado la praxis cotidiana en los órganos encargados de la investigación penal (Policía, Ministerio Fiscal y Jueces Instructores) y por otro su necesario encaje constitucional y legal.

La evidente inadecuación de la actual legislación española sobre investigación penal al grado de desarrollo tecnológico merece todo tipo de reproches. Pero escudarnos en una fatalidad que vendría constituida por una ley inaceptable no puede ser la solución, así como tampoco lo sería el delegar íntegramente la respuesta en los jueces, obligándoles a interpretaciones creativas. Viéndonos resignados a admitir temporalmente y con todas las cautelas del mundo las flagrantes carencias y deficiencias en nuestras normas procesales (con el

propósito de parchearlas con premura), lo peor vendría significado no obstante por la consolidación de tales déficit en el futuro.

Más allá de las previsiones legales, los avances tecnológicos han jugado (e irremisiblemente jugarán en el futuro) un papel catalizador en las profundas convulsiones y transformaciones que viene sufriendo la fase de investigación del proceso penal. No son el único revulsivo y posiblemente ni siquiera sean el más importante de entre los factores en juego, superados en ese extraño ranking por consideraciones de política legislativa que impulsan a transmitir a la opinión pública una imagen de seguridad y de eficiencia al margen de cualesquiera otras consideraciones. De ahí que presentar las transformaciones tecnológicas como desencadenantes en una inevitable relación causa-efecto de las reformas procesales penales podría ser, como mínimo, una simplificación del problema. Más grave sería que, además, constituyera la excusa perfecta para difundir de forma propagandística un grado de confianza en la tecnología de tal calibre que nos condujera a contemplar la lucha contra la delincuencia desde la búsqueda irreflexiva de la eficiencia o la agilidad en la respuesta estatal al delito o la defensa a ultranza de una seguridad sin precio.

La clave está en que tales mutaciones no afecten a un núcleo intangible y esencial, más allá del cual el proceso penal configurado y consolidado históricamente quedaría socavado en su estructura esencial. Los argumentos basados únicamente en valores atemporales y ahistóricos parecen poco convincentes, pero un diseño del proceso penal que confíe ciegamente en las posibilidades tecnológicas, particularmente en relación con la investigación, aportaría una imagen externa de eficiencia que, tras su deslumbrante brillo, quizá escondiera un gigante con pies de barro.