

Secreto profesional y entrada y registro: otro desafío para la justicia digital



Ignacio de Luis Otero.

Abogado. Doctor en Derecho

Toda pregunta jurídica contemporánea encierra una sospecha: que la realidad digital ha dejado atrás las categorías con las que pretendemos explicarla. En los registros digitales y, en particular, en los accesos remotos y encubiertos a los sistemas de un despacho, ¿es posible la presencia del Decano o su delegado? ¿tendría sentido como garantía efectiva? Sin una transformación de su función hacia salvaguardas técnicas y jurisdiccionales *ex ante*, la presencia colegial corre el riesgo de convertirse en una mera quimera, incapaz de proteger el secreto profesional de terceros clientes ajenos a la causa frente a extracciones masivas y automatizadas.

La irrupción de las tecnologías digitales en la Administración de Justicia plantea desafíos extraordinarios cuando colisiona

con derechos fundamentales. La práctica del registro remoto de dispositivos electrónicos (art. 588 septies a LECrim) y su aplicación en diligencias de entrada y registro en despachos constituye una de las asignaturas pendientes más acuciantes de nuestro ordenamiento procesal.

El secreto profesional del abogado no es un privilegio gremial, sino una garantía funcional al servicio del derecho de defensa. Así lo reconoció el TEDH en *Michaud c. Francia* (2012), al señalar que la confidencialidad abogado-cliente es elemento esencial del derecho a un proceso equitativo (art. 6 CEDH) y que cualquier injerencia debe rodearse de garantías reforzadas. En el ámbito interno, diversas normas consagran este deber-derecho, cuya vulneración compromete la confianza de todo ciudadano en la posibilidad de comunicarse libremente con su defensor.

La dimensión crucial es la que atañe a los terceros clientes del despacho investigado. Cuando se practica una entrada y registro del profesional, el riesgo se extiende a todos aquellos cuyas comunicaciones, estrategias procesales y documentación confidencial obran en poder del despacho. La tutela del secreto profesional de estos terceros,

ajenos a la causa penal, constituye una exigencia ineludible que carece de un marco normativo suficientemente desarrollado en el entorno digital.

En un registro físico, la presencia del representante colegial (art. 32.2 EGAE) permite ejercer, al menos, un cierto control inmediato sobre la documentación, oponerse al acceso a expedientes de clientes ajenos a la investigación y dejar protesta de vestigios prospectivos. El registro remoto, por su naturaleza, elude por completo estas garantías: se ejecuta sin conocimiento del investigado, sin intervención colegial y sin discriminación entre datos investigados y aquellos amparados por el secreto profesional de terceros.¹

La gravedad se intensifica considerando la arquitectura actual de los sistemas informáticos de los despachos. Los servidores, plataformas de gestión, sistemas de correo y almacenamiento en la nube contienen, de forma interconectada e indivisible, información de la totalidad de clientes; dejando atrás el dispositivo físico como alojamiento. Un registro remoto potencialmente compromete el secreto profesional los clientes, de potencial interés policial para otras líneas de investigación.

La LECrim guarda un silencio preocupante sobre las garantías

¹ El artículo 588 septies a) LECrim permite la instalación de software para el examen a distancia y sin conocimiento de su titular del contenido de ordenadores, dispositivos electrónicos o sistemas informáticos. Esta medida presenta una capacidad intrusiva cualitativamente superior al registro físico tradicional.

específicas cuando el registro remoto recae sobre sistemas de un despacho de abogados. El artículo 588 septies a) establece requisitos generales de proporcionalidad, especialidad y excepcionalidad, pero no contempla la intervención del Colegio, la designación de un perito independiente que filtre la información amparada por el secreto profesional, ni mecanismo alguno de segregación previa de datos de terceros clientes.

Esta laguna contrasta con la experiencia comparada. En Francia, el *bâtonnier* desempeña un papel activo en cualquier registro que afecte a un despacho, pudiendo oponerse a la incautación y provocar un procedimiento contradictorio ante el juez de libertades. En Alemania, el parágrafo 97 StPO prohíbe expresamente la incautación de comunicaciones abogado-cliente, con independencia del soporte. Nuestro ordenamiento no ha adaptado estas garantías al entorno digital.

La CE ofrece un armazón normativo que blinda el secreto profesional en el entorno digital. El artículo 24.2 CE reconoce el derecho de defensa y la asistencia de letrado. El artículo 18 CE aporta tres ejes complementarios: la inviolabilidad del domicilio (18.2) —que alcanza el despacho profesional—, el secreto de las comunicaciones (18.3) y la protección de datos personales (18.4). En el plano legal, el art. 542.3 LOPJ consagra el deber-derecho del abogado a guardar secreto, y el EGAE aboga por la presencia decanal en los registros físicos.

El TC ha subrayado que el secreto profesional es un deber de raíz constitucional.² Esta expansión resulta crucial en el ámbito digital: las huellas electrónicas del asesoramiento (borradores, metadatos, historiales de edición) quedan igualmente amparadas y no pueden ser objeto de aprehensión indiscriminada.

La jurisprudencia ha resaltado que la intervención de comunicaciones con el letrado exige justificación reforzada, control judicial estricto y delimitación precisa, canon plenamente trasladable a la captación remota de contenidos en servidores del despacho. En el plano de la prueba ilícita, se impone la exclusión probatoria de cualquier dato extraído mediante registro remoto que alcance información amparada por el secreto profesional.

A esta arquitectura se suma la LO 5/2024, del Derecho de Defensa, que menciona expresamente la protección del secreto profesional en la entrada y registro de despachos respecto de clientes ajenos a la investigación. Aun sin desarrollo reglamentario, refuerza que la presencia colegial o mecanismos de filtrado y segregación previa son exigencias constitucionales implícitas en soportes digitales interconectados.

De la doctrina constitucional se derivan tres corolarios operativos: (i) delimitación estricta del objeto de la injerencia (dispositivos, cuentas, franjas temporales, tipos de archivo); (ii) implantación de filtros *ex ante* por un tercero independiente con

intervención colegial que excluya contenido cubierto por el secreto antes de su entrega a la policía judicial; y (iii) nulidad probatoria de lo indebidamente aprehendido y prohibición de minería de datos sin autorización judicial específica y motivada.

Ponderar adicionalmente el efecto expansivo sobre terceros ajenos obliga a articular salvaguardas técnicas y procesales específicas (piezas separadas, sellado, hash y sellado temporal, revisiones judiciales iteradas) que eviten accesos indiscriminados y respeten la confidencialidad abogado-cliente.

La digitalización multiplica los vectores de riesgo: interceptación de comunicaciones electrónicas abogado-cliente, acceso a expedientes digitales con eventuales brechas de seguridad, utilización de inteligencia artificial para el análisis masivo de datos incautados e interconexión de bases de datos judiciales y policiales. La capacidad de los algoritmos para correlacionar información convierte cualquier acceso no segregado a los sistemas de un despacho en una amenaza sistémica para la confidencialidad. La información de un cliente puede revelarse no solo por acceso directo, sino por inferencia algorítmica a partir de metadatos y patrones de comunicación que ningún filtro humano detectaría.

La salvaguarda del secreto profesional de terceros clientes exige una intervención legislativa que aborde: (i) la obligatoriedad de la intervención del Decano

² En la STC 110/1984, afirmó que no cabe imponer al letrado la revelación de datos que penetren en el núcleo de la relación profesional. En la STC 55/2004, enfatizó que el secreto “se extiende a cualquiera de las modalidades de la actuación profesional”, incluido el asesoramiento previo.

o su delegado en toda investigación tecnológica que afecte a sistemas de un despacho, incluido el registro remoto, con facultad de oposición susceptible de revisión judicial inmediata; (ii) protocolos de segregación de datos mediante peritos independientes que filtren la información amparada por el secreto antes de ponerla a disposición de los investigadores; (iii) la prohibición de herramientas de análisis masivo sin control judicial previo y específico; y (iv) un régimen de nulidad radical para pruebas obtenidas vulnerando el secreto de terceros clientes.

El modelo francés ofrece un referente operativo. La presencia del *bâtonnier* es obligatoria desde el inicio de la diligencia y puede oponerse *in situ* a la aprehensión de datos cubiertos por el secreto, determinando su precintado y remisión al juez de libertades para decisión contradictoria. En la dimensión digital, se exige filtrado previo bajo control del *bâtonnier* y del juez mediante búsquedas por palabras clave, extracción limitada por rango temporal, copias forenses con hash y sellado digital, de modo que solo se entreguen a la policía los elementos no protegidos.

Este contraste ilumina la carencia española: la intervención del Decano se prevé para el registro físico, solo a instancia de parte, sin regulación para el acceso telemático encubierto, y sin existir un procedimiento contradictorio inmediato. La transposición de estas dos piezas nucleares —presencia y oposición eficaz colegial, y decisión judicial previa con filtrado técnico-forense— quizá permitiría adaptar el estándar constitucional español al ecosistema digital.

¿Tiene sentido la presencia del Decano en la era digital? La presencia física decanal ha demostrado eficacia en registros tradicionales, donde el control humano permite separar carpetas y oponerse a incautaciones concretas. Sin embargo, en el registro remoto y automatizado la presencia colegial corre el riesgo de devenir una quimera: la medida se ejecuta sin conocimiento del titular, de forma deslocalizada; el volumen de datos es ingente y su clasificación exige capacidades técnicas (forense digital, análisis de metadatos) que exceden las funciones de un órgano deontológico pensado para la presencialidad analógica.

Incluso articulando una presencia “virtual” del Decano, su tutela efectiva estaría limitada por la opacidad técnica de las herramientas de intrusión; la interconexión sistémica de repositorios que dificulta la segregación manual; y la velocidad de los procesos de extracción, que pueden replicar conjuntos masivos antes de que exista ocasión de oponerse.

La función garantista colegial debe reconfigurarse entonces para el entorno digital, desplazando el énfasis desde la presencialidad hacia mecanismos previos, técnicos y jurisdiccionales. A título de ejemplo: órdenes judiciales con delimitación granular de objeto y ventanas temporales; filtros *ex ante* por un tercero forense independiente con participación colegial en un entorno sellado; registros de auditoría inmutables con hash y sellado temporal; prohibición de minería de datos sin autorización específica; notificación diferida y control *ex post* ante el juez instructor con posibilidad de contradicción; y protocolos

intercolegiales de clasificación por palabras clave y listas blancas de clientes ajenos.

La intervención colegial conserva sentido como garantía institucional, no por su presencia continua durante la intrusión, sino como actor que pueda proponer términos de búsqueda, validar criterios de exclusión, supervisión del perito filtrador y legitimación para impugnar ante el juez instructor. Solo ganará efectividad si se evoluciona hacia el diseño de las salvaguardas, asegurando que el procedimiento incorpore barreras efectivas para proteger el secreto de terceros clientes.

Conclusión

La irrupción de los registros remotos ha ampliado exponencialmente las facultades de injerencia estatal, pero el legislador ha olvidado acompañarlas de garantías específicas para la protección del secreto profesional de la abogacía, dejando una de las cuestiones más sensibles de la investigación digital en un preocupante vacío normativo. La protección efectiva frente a las facultades de investigación e injerencia en la era digital permanece como una asignatura pendiente, en la delicada encrucijada entre las garantías fundamentales y las posibilidades exponenciales que ofrece la investigación contemporánea. La realidad de nuestra era exige una respuesta legislativa clara y decidida, capaz de garantizar que el progreso técnico no se produzca a costa del sistema de garantías.

Sirva cuanto antecede de mero boceto.



«La inteligencia artificial acabará ayudándonos a definir qué significa realmente ejercer bien la abogacía»