**LA PRUEBA ELECTRÓNICA EN EL PROCESO PENAL: EL CORREO ELECTRÓNICO Y EL WHATSAPP**

**ELECTRONIC EVIDENCE IN THE CRIMINAL PROCESS: EMAIL AND WHATSAPP**

Rubén López Picó

Departamento de Derecho Procesal. Universidad de Granada

**SUMARIO: I. INTRODUCCIÓN. II. PRUEBA ELECTRÓNICA.** 1. Concepto. 2. Fuentes normativas. 3. Clases de pruebas electrónicas. 4. Valoración de la prueba electrónica. 5. Problemática. 6. El clonado de la prueba electrónica por los Cuerpos y Fuerzas de Seguridad del Estado. **III. EL CORREO ELECTRÓNICO Y EL WHATSAPP COMO MEDIO DE PRUEBA EN EL PROCESO PENAL.** 1. El correo electrónico. 2. Intervención del contenido del correo electrónico. 3. La intervención del contenido de los correos electrónicos por los Cuerpos y Fuerzas de Seguridad del Estado 4. El WhatsApp. **IV. EL CORREO ELECTRÓNICO Y EL WHATSAPP EN LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES.** 1. La interceptación de comunicaciones. 2. El derecho a la intimidad. 3. El derecho al secreto de las comunicaciones. **V. CONCLUSIONES. VI. BIBLIOGRAFÍA.**

**Resumen**

A través del presente trabajo de investigación pretendemos abordar el estudio de la prueba electrónica en el proceso penal y, de forma más concreta, el empleo del correo electrónico y del WhatsApp como medios de prueba electrónica en los procesos penales. Los continuos avances en el desarrollo de las Tecnologías de la Información y de la Comunicación no van acompañados de todas las operaciones que deberían ser efectuadas por el legislador a fin de garantizar una adecuada regulación en esta materia, generándose, como resultado de su ausencia, diferentes e importantes problemas de carácter estructural y de orden práctico. Centrándonos en el estudio de la prueba electrónica en los procesos penales con relación al empleo del correo electrónico y del WhatsApp como medios de prueba electrónica en los mismos, pretendemos analizar las dificultades que existen dentro de este ámbito a raíz de la incidencia de las nuevas tecnologías sobre las comunicaciones interpersonales. Prestando especial atención al respeto por ciertos derechos fundamentales, tales como el derecho fundamental a la intimidad y el derecho fundamental al secreto de las comunicaciones, de aquellas personas que por el hecho de estar siendo investigadas pudiesen verse afectados.

**Abstract**

Through this research work we intend to address the study of electronic evidence in the criminal process and, more specifically, the use of email and WhatsApp as electronic evidence in criminal proceedings. The continuous advances in the development of Information and Communication Technologies are not accompanied by all the operations that should be carried out by the legislator in order to guarantee an adequate regulation in this matter, generating, as a result of their absence, different and important problems of a structural and practical nature. Focusing on the study of electronic evidence in criminal proceedings in relation to the use of email and WhatsApp as means of electronic evidence in them, we intend to analyze the difficulties that exist within this area as a result of the incidence of new technologies about interpersonal communications. Paying special attention to respect for certain fundamental rights, such as the fundamental right to privacy and the fundamental right to secrecy of communications, of those people who, because they are being investigated, could be affected.

**Palabras claves**

Proceso Penal, Prueba Electrónica, Correo Electrónico, WhatsApp.

**Key Words**

Criminal Process, Electronic Evidence, Email, WhatsApp.

**I. INTRODUCCIÓN**

Las Tecnologías de la Información y de la Comunicación, resultado de la revolución tecnológica digital, desempeñan un papel esencial en todos los quehaceres de nuestra vida cotidiana, sobresaliendo, de forma especial, en la esfera de las telecomunicaciones; en la transmisión e intercambio de información[[1]](#footnote-2).

Esta nueva realidad comunicativa posee incidencia directa sobre las relaciones sociales, donde los profundos cambios y transformaciones -promovidos por múltiples factores como la globalización, pero de manera especial por el desarrollo de las nuevas Tecnologías de la Información y de la Comunicación, a la que antes hemos hecho referencia[[2]](#footnote-3)-, han dado paso a lo que actualmente conocemos como la sociedad de la información.

La instantaneidad y la desaparición de las fronteras físicas se presentan como las características esenciales de este nuevo modelo comunicativo, de ahí que el número de personas que participan en él sea cada vez mayor, lo que a su vez se traduce en un mayor control de esas mismas personas dado el volumen de información que se puede obtener y registrar a través de su uso[[3]](#footnote-4).

El carácter positivo del empleo de las nuevas tecnologías en el ámbito de las comunicaciones, no impide que su uso pueda orientarse a la consecución de fines delictivos. Pues como señala MAGRO SERVET[[4]](#footnote-5), “nos encontramos ante un modelo de delincuencia cada vez más violenta, pero, sobre todo, más sofisticada en cuanto al empleo de los medios y técnicas a utilizar para la comisión de los hechos delictivos”. Aprovechan el carácter anónimo y descentralizado de la red, y los recursos técnicos - resultado del desarrollo de las nuevas Tecnologías de la Información y de la Comunicación-, para, de forma rápida, masiva y continuada, operar a nivel nacional e internacional.

Esta nueva realidad delictiva choca de frente con la realidad legislativa vigente, originando la necesidad de desarrollar nuevas técnicas de investigación y de adaptar las normas aplicables en materia de persecución y represión a estas nuevas formas de delincuencia, con el objetivo de tratar de obtener los medios de prueba necesarios con los que posteriormente enjuiciar esas conductas delictivas, sobre la base del respeto a los principios básicos del Derecho Penal, del proceso debido y de los Derechos Fundamentales.

**II. LA PRUEBA ELECTRÓNICA**

**1. Concepto**

Desde la perspectiva Doctrinal, a la hora de establecer que debemos entender por prueba electrónica, fijamos como punto de partida el hecho de que como resultado del desarrollo de las nuevas Tecnologías de la Información y de la Comunicación y su incidencia en todos los ámbitos de nuestra vida cotidiana, incluido el jurídico, existen múltiples conceptos para hacer referencia a la prueba electrónica: prueba por soportes informáticos, prueba por medios reproductivos, prueba por documentos electrónicos, prueba tecnológica o prueba documental electrónica, entre otros muchos[[5]](#footnote-6).

Frente a la perspectiva Doctrinal, el legislador español abordó inicialmente la cuestión relativa al concepto de prueba electrónica por medio del art.3.5 de la Ley 59/2003, de 19 de Diciembre, de Firma Electrónica, modificado, más tarde, por la Ley 56/2007, de 28 de Diciembre, de Medidas de Impulso de la Sociedad de la Información. Tras la modificación, la definición de documento electrónico contenida en ese art.3.5 de la Ley 59/2003 se amplió hasta quedar redactado de la siguiente forma: “*se considera documento electrónico a la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado*”.

Tal y como afirma GARRIDO CARRILLO[[6]](#footnote-7), al promulgarse la Ley 59/2003, de 19 de Diciembre, de Firma Electrónica, la regulación de la Ley de Enjuiciamiento Civil 1/2000 -LEC- quedó absolutamente superada y obsoleta. Pues conforme a lo dispuesto en el art.3.8 de la Ley 59/2003 -“*el soporte en que se hallen los datos firmados electrónicamente serán admisible como prueba documental en juicio*”-, “podríamos entender que los documentos electrónicos quedan situados dentro de la prueba documental como una modalidad de la misma, sin ser, por tanto, de aplicación a los mismos, la regulación prevista en los arts. 382 a 384 LEC, relativos a la reproducción de la palabra, el sonido y la imagen, y los instrumentos que permiten archivar y conocer datos relevantes para el proceso penal”.

La Decisión 2002/630/JAI del Consejo, de 22 de Julio del 2002, de Cooperación Policial y Judicial en Materia Penal, fue la encargada de hacer referencia y definir por primera vez el concepto de prueba electrónica -“la información obtenida a partir de un dispositivo electrónico o medio digital el cual sirve para adquirir convencimiento de la certeza de un hecho”- y el concepto de medios de prueba electrónica -“los soportes técnicos que recogen la prueba electrónica”-.

Tras lo expuesto, nos decantamos por la definición de prueba electrónica defendida por DELGADO MARTÍN[[7]](#footnote-8) y SANCHÍS CRESPO[[8]](#footnote-9), conforme a la cual, la prueba electrónica se concibe como “toda aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal”.

**2. Fuentes normativas**

Ante la ausencia de normas nacionales, comunitarias e internacionales reguladoras del empelo de la prueba electrónica en el proceso penal, ésta última encuentra su regulación en la Ley Orgánica del Poder Judicial -arts.299.3 y 230-, la Ley de Enjuiciamiento Civil -arts.299.2, 300.1.5º, 326.3, y 382 a 384- y la Ley de Enjuiciamiento Criminal -arts.448, 707, 731.bis, 743 y 788.6-.

**3. Clases de pruebas electrónicas**

Como resultado del concepto, tan amplio, de prueba electrónica al que antes hemos hecho referencia, cuando hablamos de clases de prueba electrónica, estamos haciendo referencia a las pruebas creadas por la informática -correo electrónico y WhatsApp-, las pruebas procedentes de otros instrumentos electrónicos -vídeo-, las pruebas que se alojan en dispositivos electrónicos externos -pendrive-, y las pruebas de carácter tradicional que entran en contacto con las nuevas Tecnología de la Información y de la Comunicación -declaración de un testigo a través de videoconferencia-[[9]](#footnote-10).

**4. Valoración de la prueba electrónica**

La valoración de la prueba electrónica requiere la superación por ésta del denominado “test de admisibilidad”: la integridad -el soporte que se presenta no ha sido alterado-, la autenticidad -constatación de la realidad del sujeto al que se atribuye y del contenido que refleja- y la licitud -obtención con respeto a los derechos y libertades fundamentales-[[10]](#footnote-11).

Con respecto a la concurrencia de pruebas clásicas y electrónicas, éstas últimas no representan en sí y frente a las pruebas clásicas una superioridad probatoria, sino que requieren del complemento o refuerzo de otras pruebas de carácter “tradicional” para, en un ejercicio de valoración global, acceder a un resultado determinado. Relacionado con ésta misma cuestión, debemos hacer referencia al denominado conocimiento privado el Juez, conforme al cual, afirmamos que no puede conducir a un trato desigual para el litigante y, por consiguiente, para la tutela judicial prestada a éste, el que el Juez predeterminado por la Ley posea un mayor o menor conocimiento de las nuevas tecnologías.

La valoración de la prueba electrónica, al no ser una excepción al sistema de libre valoración -configurado éste último a partir de los arts.9 y 120.3 de la Constitución Española[[11]](#footnote-12)- ni a los principios que cada orden jurisdiccional recoge, gira alrededor de la idea de su racionalidad. De este modo, la valoración de la prueba electrónica, como resultado de la exigencia de que todas las resoluciones judiciales deben estar motivadas, no puede tener lugar de manera subjetiva o arbitraria. Las particulares de la prueba electrónica exigen que, en multitud de ocasiones, para efectuar la valoración de la misma, el Juez precise del auxilio de peritos informáticos expertos en la materia.

**5. Problemática**

El estudio de la prueba electrónica pone de manifiesto la existencia de ciertas problemáticas en torno a su figura. Pudiendo destacar[[12]](#footnote-13):

1. La manipulación de la prueba electrónica. La posibilidad de poder llegar a manipular la prueba electrónica objeto del proceso penal exige la necesidad del desarrollo de un proceso basado en el contenido del art.230.2 Ley Orgánica del Poder Judicial: la necesidad de asegurar la autenticidad y la integridad de la prueba electrónica objeto del proceso penal.
2. La dificultad para distinguir los documentos originales de las copias. La distinción de los documentos originales respecto de las copias cuando éstos se aportan al proceso penal en formato electrónico se complica debido al hecho de que cuando hablamos de prueba electrónica, ésta tiene que entenderse y tratarse como la original. Pese a ello, los continuos avances y mejoras en las Tecnologías de la Información y Comunicación han permitido desarrollar las herramientas y técnicas necesarias para salvar esta cuestión y poder afirmar con total rotundidad si los documentos en formato electrónico incorporados al proceso penal son los originales o las copias de ellos, y si han sido, o no, manipulados.

**6. El clonado de la prueba electrónica por los Cuerpos y Fuerzas de Seguridad del Estado**

Con el objetivo de evitar la posible manipulación de la prueba electrónica y, como resultado, poder asegurar la autenticidad e integridad de la misma -art.230.2 LOPJ-, los Cuerpos y Fuerzas de Seguridad del Estado ponen en marcha un proceso basado en el empleo de ciertos conocimientos, un protocolo de actuación técnico y un conjunto de herramientas de hardware denominadas clonadoras. Conforme a este proceso, una vez incautado el dispositivo electrónico con toda la información que se pretende incorporar al proceso penal como medio de prueba electrónica, se procede a su protección para evitar que pueda ser manipulado y trabajar sobre él en sede judicial.

Tras la incautación del dispositivo electrónico que contiene toda la información que se quiere incorporar al proceso penal como medio de prueba electrónica, se precinta hasta que en sede judicial y en presencia del Letrado de la Administración de Justicia, el especialista proceda a su clonado mediante el empleo de ciertas herramientas de hardware que copian íntegramente el contenido del disco duro del dispositivo electrónico de origen. Se obtienen, así, dos discos duros con exactamente el mismo contenido: el original y el clonado, de lo que dará fe el Letrado de la Administración de Justicia. En todos los supuestos de clonado, el original queda bajo la custodia del Juzgado, utilizándose la copia para el resto de actuaciones, tales como la investigación o la aportación de pruebas.

A través de la técnica del clonado, se consigue solventar, o al menos en parte, el problema relativo a la posible manipulación de los dispositivos electrónicos que contienen toda la información que se pretende aportar al proceso penal como medio de prueba electrónica; siempre y cuando, se actué conforme al correcto proceso de cadena de custodia previsto por la Ley. Así como, el relativo a la distinción entre los documentos electrónicos originales y sus copias, ya que la técnica del clonado, permite obtener del original tantas copias como sea necesario para poder alcanzar los fines de la investigación y sin que el original sufra ningún tipo de daño, al quedar desde el momento posterior a su incautación a disposición Judicial.

**III. EL CORREO ELECTRÓNICO Y EL WHATSAPP COMO MEDIO DE PRUEBA EN EL PROCESO PENAL**

**1. El correo electrónico**

Tal y como ya hemos afirmado antes, la prueba electrónica es admitida en el proceso penal, una vez superado el denominado “test de admisibilidad”, es decir, cuando se pueda garantizar que se ha respetado su integridad -el soporte en el que se presenta no ha sido alterado-, y la autenticidad -constatación de la realidad del sujeto al que se atribuye y del contenido que refleja- y licitud del soporte electrónico -obtención con respecto a los derechos y libertades fundamentales-[[13]](#footnote-14).

Cuando hablamos de correo electrónico, tomamos como punto de referencia el concepto recogido en el art. 2.h) de la Directiva 2002/58/CE, de 12 de Julio de 2002,del Parlamento y del Consejo de Europa, sobre privacidad y comunicaciones electrónicas, según el cual por correo electrónico debe entenderse “*todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo. Siendo necesario para ello una dirección electrónica IP y un software de gestión de correos*”[[14]](#footnote-15).

El correo electrónico es uno de los medios de prueba electrónica que más dificultades presenta, sobre todo porque su manipulación no resulta difícil y sin embargo es casi imposible de detectar. Además, su tratamiento jurídico varía en función de si fue enviado y recibido, pero no leído, y recibido y, además, leído por su destinatario.

**2. Intervención del contenido del correo electrónico**

Pese a no existir una regulación específica al respecto, en el caso del correo electrónico, como en el caso de todos los operadores que prestan servicios de comunicación electrónica a nivel estatal, existe la obligación de actuar conforme al Real Decreto 424/2005, de 15 de Abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, encargada de regular las intervenciones electrónicas -RLSCE-. Delimitado por el art.579 de la Ley de Enjuiciamiento Criminal y por la Ley 2/2002, de 6 de Mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia (LCNI)[[15]](#footnote-16).

Siguiendo a MAGRO SERVET[[16]](#footnote-17), el empleo del correo electrónico como medio de prueba electrónica en el proceso penal, requiere realizar algunas precisiones:

1. La intervención de una dirección de correo electrónico se configura como un acto de intervención de la correspondencia privada de una persona. Por ello, conforme al art.579 y ss. Ley de Enjuiciamiento Criminal, la intervención de la dirección de correo electrónico será practicada por las Fuerzas y Cuerpos de Seguridad. Quiénes, de forma previa a su intervención, tendrán la obligación de presentar el correspondiente oficio motivado ante el Juez de guardia o instructor -dependiendo de si ya se han, o no, abierto las diligencias de investigación-, para que a la vista de la existencia de suficiente motivación del oficio antes presentado, éste pueda dictar el auto de intervención judicial sobre la dirección electrónica de la persona en torno a la que gira la investigación judicial. No se podrá intervenir otro tipo de comunicación electrónica que no sea la que se incorpore en la resolución judicial -ex. art. 87 RLSCE-.
2. La necesidad de que exista un control judicial relativo a las intervenciones del contenido de los correos electrónicos similar al que existe para el caso de las intervenciones telefónicas.
3. En la intervención del contenido del correo electrónico, es de aplicación la medida de prórroga de la misma. Según lo dispuesto por el art.579.3 Ley de Enjuiciamiento Criminal, el Juez fijará el periodo de duración máxima de esta medida, pudiendo prorrogarlo cuando exista una causa que la motive y justifique, generalmente cuando así sea solicitado por las Fuerzas y Cuerpos de Seguridad del Estado. Si en la orden de intervención del contenido del correo electrónico, el Juez olvida fijarlo, la orden deberá ser ejecutada antes de las doce horas del siguiente día hábil respecto de aquél en que efectivamente se recibió -art. 99 RLSCE-.
4. Las Fuerzas y Cuerpos de Seguridad del Estado trasladarán al Juez todo aquello que se hubiese obtenido de la práctica de la intervención del contenido de los correos electrónicos siempre que sea de interés para la causa que está siendo investigada.
5. La adopción de la medida relativa a la intervención del contenido del correo electrónico es perfectamente compatible con el decreto de secreto de sumario.

**3. La intervención del contenido de los correos electrónicos por los Cuerpos y Fuerzas de Seguridad del Estado**

Cuando hacemos referencia a la intervención de las cuentas de correo electrónico por parte de los Cuerpos y Fuerzas de Seguridad del Estado, debemos comenzar señalando la diferencia de tratamiento que existe entre los supuestos en los que se trata de acceder a una cuenta de correo electrónico disponiendo, previamente, del dispositivo electrónico desde el que se envió o que al que se recibió dicho correo electrónico, y aquellos supuestos en los que no se disponen de ellos, pretendiendo acceder, en estos casos, al contenido del correo electrónico en cuestión a través del acceso al mismo concedido por el servidor de correo electrónico que corresponda. En cualquiera de los dos casos, el acceso al contenido del correo electrónico exige estar en posesión de la correspondiente autorización judicial previa.

Con respecto al segundo de los supuestos antes referidos, señalar que la colaboración o cooperación de los servidores de correo electrónico para que los Cuerpos y Fuerzas de Seguridad del Estado accedan al contenido de ciertos correos electrónicos de ciudadanos que están siendo investigados es nula. Se trata de empresas cuyos servidores están situados en el extranjero, que al acogerse a la normativa de estos países, blindan de protección a sus usuarios. Al no existir una normativa comunitaria, ni tampoco internacional relacionada con esta mima cuestión, acaba dificultando la labor de investigación.

Así mismo, esa falta de cooperación de los servidores de correos electrónicos en el desarrollo de las investigaciones policiales y judiciales, pero sobre todo en el acceso de los Cuerpos y Fuerzas de Seguridad del Estado al contenido de los correos electrónicos de aquellas personas que están siendo investigadas dificulta la labor en la determinación de si éstos han podido ser, o no, manipulados. Pues los servidores de correos electrónicos custodian el acceso al servidor y el tráfico de datos entre los clientes y el propio servidor, siendo, por tanto, los únicos que pueden determinar si el contenido del correo electrónico ha sido manipulado. Para este tipo de situaciones, sería ideal contar con la colaboración y cooperación no solo de los diferentes servidores de correos electrónicos, sino también de los propios usuarios.

**4. El WhatsApp**

Sin lugar a dudas, el WhatsApp, resultado del avance y el progreso en las nuevas Tecnologías de la Información y de la Comunicación, es el medio de comunicación a distancia, que en la actualidad, más se utiliza para el envío de mensajería instantánea a través de Internet.

En el supuesto del WhatsApp, los problemas que se plantean y la actuación de los Cuerpos y Fuerzas de Seguridad del Estado respecto a su empleo, se asemejan en gran medida, pero con ciertos matices, a la situación antes descrita para el caso del correo electrónico. De ahí, que, con algunas salvedades, lo expuesto anteriormente para el caso del correo electrónico sirva ahora de aplicación para el caso del WhatsApp.

La posible intervención del contenido de los WhatsApp, además de caracterizarse por la prohibición de poder intervenir cualquier otro tipo de comunicación diferente a la indicada en la resolución judicial -ex. Art.87 RLSCE-, también lo hace por el hecho de asemejarse a la intervención que, a través del sistema SITEL, se aplica sobre el contenido de las comunicaciones telefónicas, con el matiz de que las intervenciones sobre el contenido de los WhatsApp no se realizan por medio de escuchas, sino a través de diferentes dispositivos informáticos y de la cesión datos por las diferentes compañías telefónicas[[17]](#footnote-18).

Así, notificada a la compañía telefónica la orden judicial por la que se acuerda la intervención del contenido de las comunicaciones electrónicas, éstas actuando en condición de sujetos obligados -art.86 RLSCE-, transmiten la información interceptada a los centros de recepción de interceptaciones -art.95 RLSCE-; y de ahí, al agente facultado -Policía Judicial o Centro Nacional de Inteligencia-, por la autoridad judicial, para materializar este tipo de intercepciones -art.84.e RLSCE-. De este modo, se garantiza la autenticidad, confidencialidad e integridad de la información interceptada -art.97 RLSCE-.[[18]](#footnote-19)

En otro orden de cosas, la manipulación del contenido de los menajes de WhatsApp solo es posible a través de la intervención, y posterior edición o modificación, de la comunicación efectuada entre el dispositivo desde el que se envía el mensaje y el servidor, o entre el servidor y el dispositivo de destino. Para poder determina si el mensaje de WhatsApp enviado ha podido ser interceptado y, por tanto, manipulado antes de llegar a su destinatario, se comparan las bases de datos de la parte emisora y receptora del mensaje de WhatsApp que se ha enviado.

El tratamiento procesal otorgado al WhatsApp como medio de prueba en el proceso penal se basa en extrapolar las actuaciones que se llevan a cabo con respecto a la intervención de las comunicaciones telefónicas, pues lo que en esencia se pretende proteger es la comunicación en sí misma. Pero siendo, al mismo tiempo, conscientes que a diferencia de lo que ocurre con las intervenciones telefónicas, nuestra legislación, con respecto a la materia que nos ocupa es muy deficiente. Dificultando la puesta en marcha de esta medida con una cobertura legal adecuada.

Como muestra de la deficiencia legislativa a la que acabamos de hacer referencia, la Ley 25/2007, de 18 de Octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones[[19]](#footnote-20) señala que “*las compañías telefónicas no están obligadas a guardar el contenido de las comunicaciones electrónicas, sino, únicamente a conservar los datos generados por dichas comunicaciones electrónicas durante un tiempo determinado*” -art.3 Ley 25/2007-. La Directiva 2006/24/CE establece que el tiempo mínimo de conservación de los datos generados por las comunicaciones electrónicas no podrá ser inferior a seis meses ni superior a dos años. Dentro de estos límites temporales, el legislador español ha fijado un plazo general de conservación de doce meses, a contar desde el momento en el que la comunicación se hubiese establecido -art.5.1 Ley 25/2007-. En atención de los fines e intereses de la investigación, detección y enjuiciamiento del delito, dicho plazo temporal podrá reducirse a seis meses o ampliarse hasta los dos años.

La revelación del contenido de las comunicaciones que derivan del uso del WhatsApp exige la concesión de la previa autorización judicial, pues de lo contrario, los derechos fundamentales -a la intimidad y al secreto de las comunicaciones (art.18 de la Constitución Española, en ambos casos)- de los ciudadanos, que intervienen en ellas, se verían vulnerados. No es hasta la entrega de la correspondiente autorización judicial a los operadores de comunicaciones electrónicas, cuando se inicia, dentro de los límites fijados por la autoridad Judicial, la Ley y el respeto a los derechos fundamentales, el sistema de intervención del las comunicaciones electrónicas -SITEL-, que persigue como finalidad esencial la de interceptar y revelar el contenido de las mismas.

**IV. EL CORREO ELECTRÓNICO Y EL WHATSAPP EN LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES**

**1. La intercepción de las comunicaciones**

La aportación, al proceso penal como medio de prueba electrónica, del contenido de las comunicaciones efectuadas a través del correo electrónico y el WhatsApp, requiere de la superación previa del denominado “test de admisibilidad” -al que antes ya hemos hecho referencia- y, como resultado, la necesidad de respetar los derechos y las libertades fundamentales de todos los ciudadanos, especialmente de aquellos que estén siendo investigados, a través del justo equilibrio y respeto entre todos esos derechos y libertades fundamentales -de modo un tanto especial, el derecho fundamental a la intimidad y al secreto a las comunicaciones-, las garantías procesales y las nuevas técnicas de investigación de carácter tecnológico[[20]](#footnote-21).

La intercepción del contenido de las comunicaciones efectuadas entre ciudadanos que están siendo investigados se alza como uno de los medios de prueba más habituales dentro de los procesos penales. Las sociedades democráticas disponen de preceptos legales que, bajo ciertos parámetros predeterminados por la Ley, permiten intervenir esas comunicaciones y, posteriormente, revelar su contenido dentro de los procesos penales de forma legal. Sin embargo, en la actual sociedad tecnológica en la que vivimos, los avances tecnológicos permiten interceptar el contenido de esas comunicaciones de forma simple, rápida y sencilla, que al hacerse fuera de los parámetros a los que antes nos hemos referidos, acaban por vulnerar el derecho fundamental a la intimidad y al secreto de las comunicaciones de todos los ciudadanos, con independencia de que estén, o no, siendo investigados policial o judicialmente[[21]](#footnote-22).

**2. El derecho a la intimidad**

Cuando abordamos la cuestión relativa a la intercepción del contenido de las comunicaciones efectuadas entre ciudadanos que están siendo investigados policial o judicialmente a través del empleo del correo electrónico y del WhatsApp, debemos hacer referencia a la incidencia que la intercepción del contenido de estas comunicaciones tenga sobre el derecho fundamental a la intimidad de las personas que son titulares de dichas comunicaciones. En caso de producirse, la intensidad de dicha incidencia se determina por medio de la aplicación de la teoría de las esferas de HUBMANN[[22]](#footnote-23) y SEIDEL[[23]](#footnote-24), utilizada, posteriormente, por BERNING PRIETO[[24]](#footnote-25) a la hora de afirmar que el concepto de intimidad del art.18 de la Constitución Española “abarca tres esferas concéntricas: la íntima, la privada y la pública”.

Estos autores, HUBMANN y SEIDEL, entendieron por:

1. Esfera íntima “aquella que integra toda la información relativa a las relaciones familiares, afectivas, sexuales, médicas o religiosas en la que participa un tercero de confianza de su titular”. Por ello, cualquier intromisión en ella, debe responder a las exigencias de los principios de proporcionalidad, legalidad, jurisdiccionalidad y necesidad.
2. Esfera privada “la que está formada por datos o informaciones no íntimos, pero que el individuo sólo desea que sean conocidos por una determinada persona o grupo reducido de ellas, y no quiere que sean conocidos por otros grupos más amplios”. Su protección es de carácter formal, pues se protege el proceso de comunicación entre los emisores y receptores frente a una intromisión de terceros. A diferencia de la esfera íntima, su titularidad puede recaer tanto sobre personas físicas como jurídicas.
3. Esfera pública “aquella que comprende las noticias respecto a las cuales el titular de las mismas autoriza expresamente su difusión a extensos grupos de personas o a toda la sociedad, independientemente de que el contenido de dichas noticias pertenezca a la esfera íntima o privada”.

**3. El derecho al secreto de las comunicaciones**

El derecho fundamental al secreto de las comunicaciones, amparado por el art.18.3 de la Constitución Española, acoge bajo su rúbrica las comunicaciones de tipo postal, telegráficas y telefónicas. Entendiendo, como resultado, la Doctrina que las comunicaciones efectuadas a través del uso del correo electrónico y del WhatsApp constituyen una modalidad de comunicación privada, que al ser equiparada al resto de modalidades de comunicación interpersonal protegidas por el art.13 de la Constitución Española, merecedora del mismo tratamiento jurídico que el otorgado a éstas[[25]](#footnote-26).

La vulneración del derecho fundamental al secreto de las comunicaciones, únicamente se materializa cuando, sin la correspondiente autorización judicial, se accede al contenido de un correo electrónico o de un WhatsApp que ha sido enviado y recibido por su destinatario, pero aún no leído por éste. Cualquier injerencia en un momento posterior a su lectura, afectaría al derecho fundamental a la intimidad del art.18.1 de la Constitución Española, pero no al derecho fundamental al secreto de las comunicaciones del art.18.3 de la Constitución Española[[26]](#footnote-27).

De este modo, los Cuerpos y Fuerzas de Seguridad del Estado podrán investigar el contenido de los correos electrónicos y WhatsApp recibidos y leídos por la persona que está siendo investigada policial o judicialmente sin incurrir en una vulneración de su derecho fundamental al secreto de las comunicaciones, siempre que actúen respetando el principio de necesidad y de proporcionalidad de la medida adoptada por el Juez al frente de la investigación. Así mismo, en estos casos, los requisitos de validez a aplicar no serán los mismos que los existentes en las intervenciones del resto de comunicaciones, sino los que rigen el hallazgo de documentos ya en poder del destinatario.

Tras lo expuesto, podemos afirmar, con total rotundidad, que a la hora de abordar las cuestiones relativas a la vulneración del derecho fundamental al secreto de las comunicaciones recogido en el art.18.3 de la Constitución Española, resulta esencial, determinar el momento en el que la comunicación debe estimarse concluida, es decir, cuando se accede al contenido del correo electrónico o WhatsApp que previamente haya sido enviado, y no, cuando éste se haya recibido[[27]](#footnote-28).

**V. CONCLUSIONES**

La prueba electrónica en el proceso penal presenta alguna que otra problemática, sobre todo en lo relativo al uso del correo electrónico y el WhatsApp. Si bien es cierto que no se han tratado, de forma exhaustiva, todas y cada una de las diferentes cuestiones relacionadas con este medio de prueba, si lo es el hecho de que se ha pretendido dar una visión general y suficiente respecto de esta misma cuestión.

Las Tecnologías de la Información y de la Comunicación avanzan a pasos agigantados, del mismo modo que éstas avanzan, debería avanzar el Derecho. Sobre todo, con el objetivo de poder adaptarse a la realidad tecnológica del momento y, como resultado, poder regular los diferentes aspectos de las mismas con incidencia directa sobre los diferentes quehaceres cotidianos de la vida de los ciudadanos, a fin de evitar situaciones de inseguridad jurídica al tiempo que reforzar la protección de ciertos derechos fundamentales tales como la intimidad o el secreto de las comunicaciones, especialmente vulnerables al avance de las Tecnologías de la Información y de la Comunicación.

Las actuaciones operadas por el Legislador en aras de responder jurídicamente a la nueva realidad tecnológica que deriva del avance de las Tecnologías de la Información y de la Comunicación, no consistentes en la elaboración de una regulación completa sobre esta misma cuestión, sino en la realización de un conjunto de modificaciones legislativas sobre las normas legales ya existentes; nos permiten afirmar que la actual regulación estatal y comunitaria -existen algunos convenios europeos para la lucha contra la cibercriminalidad, pero insuficientes, al no existir un marco de principios generales y comunes, y tampoco las disposiciones europeas que permitan la coordinación y la acción conjunta de las autoridades de los distintos Estados en esta materia- relativa a la prueba electrónica y a su incorporación al proceso penal como medio de prueba destaca por ser insuficiente, precisándose, como resultado, una regulación estatal de la misma capaz de regular sus aspectos comunes y más básicos. Mientras tanto, la única opción pasa por la interpretación y aplicación analógica de las reglas generales en materia de prueba a la prueba electrónica y su incorporación, como medio de prueba, al proceso penal.

En otro orden de cosas, y en relación con el denominado conocimiento privado del Juez, nos vemos en la obligación de recordar la necesidad de una formación continua de los Jueces en este ámbito, a fin de evitar un trato desigual en la tutela judicial prestada por el propio Juez al litigante en función de los conocimientos tecnológicos que posee. Haciendo, además, especial hincapié en el papel tan importante que juegan los peritos informáticos en esta materia, asesorando y aportando a los Jueces la visión técnica que, en muchos de estos casos, les falta. Y es que precisamente, las dificultades prácticas que en la actualidad existe en relación a la incorporación del correo electrónico y WhatsApp, como medio de prueba electrónica, al proceso penal, se podrían eliminar con la práctica de una correcta pericial informática.

**VI. BIBLIOGRAFÍA**

ABEL LLUCH, X.”Las nuevas tecnologías y acceso al proceso, dentro de la obra La Prueba judicial”, en ABEL LLUCH, X., PICÓ I JUNOY, J. y RICHARD GONZÁLEZ, M. *Desafíos en las jurisdicciones civil, penal, laboral y contencioso-administrativa*. Ed. La Ley, Madrid, 2011.

ALZAGA VILLAAMIL, O. *Derecho político español: Según la Constitución de 1978. Volumen II: Derechos Fundamentales y órganos del Estado. 3ª Edición*. Ed. Editorial Universitaria Ramón Areces, Madrid, 2002.

BERNING PRIETO, A. D. “La intervención de las comunicaciones electrónicas”. *Revista Aranzadi Doctrinal*. Ed. Thomson-Reuters Aranzadi, Pamplona 2012.

CASTELLS, M. *La era de la información. Vol. I: La sociedad red. 2ª Edición*, Ed. Alianza, Madrid, 2000.

DELGADO MARTÍN, J. “La prueba electrónica en el proceso penal”. *Diario La Ley*. Ed. Wolters Kluwer, Madrid, 2013.

DE URBANO CASTRILLO, E. “La regulación legal de la prueba electrónica: una necesidad pendiente”. *La Ley Penal*. Ed. Wolters Kluwer, Madrid, 2011.

DOLZ LAGO, M.J. “¿Hacia una jurisprudencia electrónica? Breves reflexiones sobre SITEL”. *La Ley Penal*. Ed. Wolters Kluwer, Madrid, 2010.

GARRIDO CARRILLO, F J.: “Las nuevas tecnologías como prueba en los procesos civiles y penales”. *Actas I Congreso Internacional de la Sociedad Digital: Oportunidades y riesgos para menores y jóvenes*. Ed. Comares, Granada, 2014.

GUTIÉRREZ MALDONADO, E. *La prueba electrónica en el proceso penal: consideraciones sobre el uso del correo electrónico y del WhatsApp*. Universidad de Granada, Granada, 2015.

HUBMANN, H. “Der Zivilrechtliche Schutz der Persönlichkeit gegen Indiskretion”. *Juristenzeitung*. Ed. [Mohr Siebeck](https://dialnet.unirioja.es/revistas/editor/3202), Deutschland, 1957.

LÓPEZ-BARAJA PEREA, I. *La intervención de las comunicaciones electrónicas*. Ed. Wolters Kluwer, Madrid, 2011.

MAGRO SERVET, V. *Guía de problemas y soluciones en el juicio oral. 1ª Edición*. Ed. La Ley Actualidad, Madrid, 2006.

MAGRO SERVET, V. “Intervención policial de mensajes SMS y eficacia de las juntas provinciales de Policía judicial”. *Diario La Ley*. Ed. Wolters Kluwer, Madrid, 2007.

MIRA ROS, C. *El expediente judicial electrónico*. Ed. Dykinson, Madrid 2010.

PÉREZ GIL, J. “Los datos sobre localización geográfica en la investigación penal”, en PEDRAZ PENALVA, E. -Coord.-. *Protección de datos y proceso penal*. Ed. Wolters Kluwer, Madrid, 2010.

RODRÍGUEZ LAINZ, J.L. “SITEL: nuevas tendencias, nuevos retos”. *Diario La Ley*. Ed. Wolters Kluwer, Madrid, 2013.

ROMERO PAREJA, A. “Intervención de las comunicaciones”. *Diario La Ley*. Ed. Wolters Kluwer, Madrid, 2012.

SANCHÍS CRESPO, C. “La prueba en soporte electrónico”, en VALERO TORRIJOS, J. y GAMERO CASADO, E. -Coord.-. *Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*. Ed. Ed. Thomson Reuters Aranzadi, Pamplona, 2012.

SEIDEL, U. *Datenbanken und Persönlichkeitsrecht unter besonderer Berücksichtigung der amerikanischen Computer Privacy*. Ed. Köln Schmidt, Colonia, 1972.

1. *Vid*. LÓPEZ-BARAJA PEREA, I. *La intervención de las comunicaciones electrónicas*. Ed. Wolters Kluwer, Madrid, 2011, p.1. [↑](#footnote-ref-2)
2. *Vid*. CASTELLS, M. *La era de la información. Vol. I: La sociedad red. 2ª Edición*, Ed. Alianza, Madrid, 2000, p.27. [↑](#footnote-ref-3)
3. *Vid*. GUTIÉRREZ MALDONADO, E. La *prueba electrónica en el proceso penal: consideraciones sobre el uso del correo electrónico y del WhatsApp*. Universidad de Granada, Granada, 2015, p.9. [↑](#footnote-ref-4)
4. *Vid.* MAGRO SERVET, V. “Intervención policial de mensajes SMS y eficacia de las juntas provinciales de Policía judicial”. *Diario La Ley*. Ed. Wolters Kluwer, Madrid, 2007, p.1. [↑](#footnote-ref-5)
5. *Vid*. ABEL LLUCH, X.”Las nuevas tecnologías y acceso al proceso, dentro de la obra La Prueba judicial”, en ABEL LLUCH, X., PICÓ I JUNOY, J. y RICHARD GONZÁLEZ, M. *Desafíos en las jurisdicciones civil, penal, laboral y contencioso-administrativa*. Ed. La Ley, Madrid, 2011, pp.345-366. [↑](#footnote-ref-6)
6. *Vid*. GARRIDO CARRILLO, F J.: “Las nuevas tecnologías como prueba en los procesos civiles y penales”. *Actas I Congreso Internacional de la Sociedad Digital: Oportunidades y riesgos para menores y jóvenes*. Ed. Comares, Granada, 2014, p.274. [↑](#footnote-ref-7)
7. *Vid*. DELGADO MARTÍN, J. “La prueba electrónica en el proceso penal”. *Diario La Ley*. Ed. Wolters Kluwer, Madrid, 2013, p.1. [↑](#footnote-ref-8)
8. *Vid*. SANCHÍS CRESPO, C. “La prueba en soporte electrónico”, en VALERO TORRIJOS, J. y GAMERO CASADO, E. -Coord.-. *Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*. Ed. Ed. Thomson Reuters Aranzadi, Pamplona, 2012, p.713. [↑](#footnote-ref-9)
9. *Vid*. DE URBANO CASTRILLO, E. “La regulación legal de la prueba electrónica: una necesidad pendiente”. *La Ley Penal*. Ed. Wolters Kluwer, Madrid, 2011, p.3. [↑](#footnote-ref-10)
10. *Ibídem*. [↑](#footnote-ref-11)
11. Art.9 CE: “*1. Los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico. 2. Corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social. 3. La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos*”.

    Art.120.3 CE: “*Las sentencias serán siempre motivadas y se pronunciarán en audiencia pública*”. [↑](#footnote-ref-12)
12. *Vid*. MIRA ROS, C. *El expediente judicial electrónico*. Ed. Dykinson, Madrid 2010, p.18. [↑](#footnote-ref-13)
13. *Vid*. DE URBANO CASTRILLO, E. “La regulación legal de la prueba electrónica: una necesidad pendiente”. *Óp., Cit.,* p.3 [↑](#footnote-ref-14)
14. *Vid*. LÓPEZ-BARAJA PEREA, I. *La intervención de las comunicaciones electrónicas. Óp., Cit.,* p.13. [↑](#footnote-ref-15)
15. *Vid*. BERNING PRIETO, A. D. “La intervención de las comunicaciones electrónicas”. *Revista Aranzadi Doctrinal*. Ed. Thomson-Reuters Aranzadi, Pamplona, 2012, p.5. [↑](#footnote-ref-16)
16. *Vid.* MAGRO SERVET, V. *Guía de problemas y soluciones en el juicio oral. 1ª Edición*. Ed. La Ley Actualidad, Madrid, 2006, pp.1 y 2. [↑](#footnote-ref-17)
17. *Vid*. DOLZ LAGO, M.J. “¿Hacia una jurisprudencia electrónica? Breves reflexiones sobre SITEL”. *La Ley Penal*. Ed. Wolters Kluwer, Madrid, 2010, p.5. *Vid*. RODRÍGUEZ LAINZ, J.L. “SITEL: nuevas tendencias, nuevos retos”. *Diario La Ley*. Ed. Wolters Kluwer, Madrid, 2013, p.20. [↑](#footnote-ref-18)
18. *Vid*. BERNING PRIETO, A. D. “La intervención de las comunicaciones electrónicas”. *Óp., Cit.,* p.7. [↑](#footnote-ref-19)
19. Ley 25/2007, de 18 de Octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, dictada en trasposición de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de Marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. [↑](#footnote-ref-20)
20. *Vid.* PÉREZ GIL, J. “Los datos sobre localización geográfica en la investigación penal”, en PEDRAZ PENALVA, E. -Coord.-. *Protección de datos y proceso penal*. Ed. Wolters Kluwer, Madrid, 2010, pp.307-354. [↑](#footnote-ref-21)
21. *Vid*. ROMERO PAREJA, A. “Intervención de las comunicaciones”. *Diario La Ley*. Ed. Wolters Kluwer, Madrid, 2012, p.1. [↑](#footnote-ref-22)
22. *Vid*. HUBMANN, H. “Der Zivilrechtliche Schutz der Persönlichkeit gegen Indiskretion”. *Juristenzeitung*. Ed. [Mohr Siebeck](https://dialnet.unirioja.es/revistas/editor/3202), Deutschland, 1957, pp.521-528. [↑](#footnote-ref-23)
23. *Vid*. SEIDEL, U. *Datenbanken und Persönlichkeitsrecht unter besonderer Berücksichtigung der amerikanischen Computer Privacy*. Ed. Köln Schmidt, Colonia, 1972. [↑](#footnote-ref-24)
24. *Vid*. BERNING PRIETO, A. D. “La intervención de las comunicaciones electrónicas”. *Óp., Cit.,* p.3. [↑](#footnote-ref-25)
25. *Vid*. ALZAGA VILLAAMIL, O. *Derecho político español: Según la Constitución de 1978. Volumen II: Derechos Fundamentales y órganos del Estado. 3ª Edición*. Ed. Editorial Universitaria Ramón Areces, Madrid, 2002, p.100. [↑](#footnote-ref-26)
26. *Vid*. LÓPEZ-BARAJA PEREA, I. *La intervención de las comunicaciones electrónicas. Óp., Cit.,* p.13. [↑](#footnote-ref-27)
27. *Ibídem*, p.14. [↑](#footnote-ref-28)