LA INTERVENCIÓN DE LAS COMUNICACIONES TELEMÁTICAS EN EL CONTEXTO DIGITAL

The interception of telematic communications in the digital context

ANTÓN FRUCTUOSO FREIRE MONTERO
Fiscal
antonfructuoso.freire@fiscal.es

Cómo citar/Citation
Freire Montero, A. F. (2024).
La intervención de las comunicaciones telemáticas en el contexto digital.
Revista Española de Derecho Constitucional, 130, 139-167.
doi: https://doi.org/10.18042/cepc/redc.130.05

Resumen

El presente trabajo pretende realizar un análisis sobre la medida de intervención de comunicaciones telemáticas y su aplicación en el ámbito de la sociedad digital. Para ello, será preciso tener en cuenta la base normativa existente tras la reforma operada en la ley procesal penal mediante la LO 13/2015, norma con la que se logra superar las anteriores situaciones de anomia existentes en nuestro país y que habían sido objeto de censura por el Tribunal Europeo de Derechos Humanos. Además, su aplicación ha de tener en cuenta la actual realidad de la comunicación a distancia, sustancialmente diversa de la existente hasta hace pocas décadas. Finalmente, estudiaremos la eficacia de esta diligencia de investigación, distinguiendo entre dos supuestos de hecho diferentes: la delincuencia en el mundo físico y la delincuencia *online*.

Palabras clave

Intervención de las comunicaciones; investigación tecnológica; secreto de las comunicaciones; protección de datos; privacidad-sociedad digital; delincuencia *online*.

Abstract

This paper aims to carry out an analysis of the measure of interception of telematic communications and its application in the field of the digital society. To do so, it will be necessary to take into account the existing regulatory basis following the reform of the criminal procedure law by LO 13/2015, a rule that overcomes the previous situations of anomie that existed in our country and which had been censured by the European Court of Human Rights. Furthermore, its application must take into account the current reality of remote communication, which is substantially different from that which existed until a few decades ago. Finally, we will study the effectiveness of this investigative diligence, distinguishing between two different factual assumptions: crime in the physical world and online crime.

Keywords

Interception of communications; technological research; communication secrecy; data protection; privacy; digital society; online crime.

SUMARIO

I. INTRODUCCIÓN: CONCEPTO Y NORMATIVA APLICABLE A LAS INTERVENCIONES TELEMÁTICAS

La intervención de comunicaciones telemáticas —también denominada «ciberintervención» (Armenta Deu, 2018: 70)— es una de las diligencias de investigación tecnológica que actualmente se hallan a disposición del órgano instructor penal y que permite la averiguación del contenido de las comunicaciones a distancia mantenidas por la persona investigada, así como la captación de los datos de tráfico anejos a estas comunicaciones. Tal actuación de indagación se caracteriza por realizarse en tiempo real y sin provocar la interrupción de la conversación afectada, pudiendo abarcar tanto las comunicaciones telefónicas —fijas y móviles— como el correo electrónico o cualquier otro tipo de comunicaciones a través de internet, *v. gr.*, en foros o chats cerrados (Cabezudo Rodríguez, 2016: 29). En un sentido negativo, quedaría fuera de este ámbito la captación de las conversaciones orales directas del investigado o «conversaciones entre presentes» (López Ortega, 2017: 36) —regulada en los arts. 588 *quater* letra a) y siguientes de la LECrim—[1]. Igualmente, se situaría extramuros de la medida la averiguación del

[1] No obstante, la medida de captación de comunicaciones orales directa puede afectar al derecho al secreto comunicativo, habiendo declarado el Tribunal Constitucional —en adelante, TC— que el derecho consagrado en el art. 18.3 de la Constitución española —en adelante, CE— ofrece cobertura también a las comunicaciones interpersonales mantenidas sin la intervención de medios o artificios técnicos destinados a hacer posible el proceso comunicativo. En esta línea se pronuncia expresamente la

contenido de las conversaciones telemáticas ya finalizadas y conservadas en un dispositivo informático —arts. 588 *sexies* letra a) y siguientes de la ley procesal penal—[2].

Aunque el legislador vigente se refiere a esta diligencia como «interceptación de las comunicaciones telefónicas y telemáticas»[3], consideramos más preciso separarnos de esta expresión en dos puntos. En primer lugar, y en la medida en que esta actividad de escrutinio estatal no interrumpe la comunicación afectada, sería preferible, siguiendo el diccionario de la Real Academia, utilizar el verbo *intervenir* —espiar, por mandato o autorización legal, una comunicación privada— frente al término *interceptar* —apoderarse de algo antes de que llegue a su destino—. Por otra parte, y como indica Sanchís Crespo (2017: 4), el empleo de la expresión *telefónicas* puede resultar ocioso, habida cuenta del amplio significado que —consultada la fuente antes referida— posee el adjetivo *telemático*: perteneciente o relativo a la *telemática*, siendo esta última la aplicación de las técnicas de la telecomunicación y de la informática a la transmisión de información computarizada.

Calificada por algunos como la «medida estrella» (Pérez Gil, 2018: 187) de la instrucción penal, la intervención de las comunicaciones telemáticas es una herramienta empleada con relativa frecuencia en el ámbito de la investigación de los delitos más graves. Sin embargo, la habitualidad en el uso de esta diligencia no puede llevarnos a obviar su «intrínseca peligrosidad potencial» (Noya Ferreiro, 2018: 87) para los derechos fundamentales de la persona investigada. El propio Tribunal Europeo de Derechos Humanos[4] —en adelante, TEDH— ha declarado recientemente que la intervención de comunicaciones telefónicas —entiéndase el uso de esta palabra como un sinónimo de telemáticas— supone una grave injerencia del Estado en el derecho a la privacidad del ciudadano, protegido por el art. 8 del Convenio Europeo de Derechos Humanos. En particular, la adopción de la medida por el órgano instructor permitirá desplazar temporalmente el derecho al secreto de las

STC 99/2021, de 10 de mayo, en su FJ 7, infiriéndose, asimismo, tal consideración de lo dispuesto en la STC 145/2014, de 22 de septiembre, FJ 7.

2 Conviene tener presente que el art. 18.3 CE protege la comunicación hasta el momento en el que el destinatario del mensaje toma conocimiento de su contenido, por lo que los mensajes ya leídos y almacenados en un dispositivo quedarían situados bajo la influencia del art. 18.1 CE —*vid.* STC 173/2011, de 7 de noviembre, FJ 3—.

3 Así se intitula el capítulo V del título VIII del libro II de la Ley de Enjuiciamiento Criminal, en la versión ofrecida por la LO 13/2015.

4 *Vid*. la STEDH *Vasil Vasilev vs Bulgaria*, de 16 de febrero de 2022, asunto 7610/15, punto 89.

comunicaciones del investigado —art. 18.3 CE—. Cabe recordar aquí, siguiendo a Jiménez Campo (1987: 36), la importancia de que se produzca un adecuado respeto de este derecho por parte de los poderes públicos democráticos, en la medida en que es un bien jurídico que actúa en favor de la autodeterminación privada y permite la constitución de un ámbito de autonomía del individuo —y de la sociedad en general— frente al Estado. Naturalmente, el derecho al secreto de las comunicaciones no es absoluto y puede ser limitado *secundum constitutionem* por las autoridades, si bien esto ha de efectuarse siempre siendo consciente de que su restricción resulta de gran trascendencia en una sociedad libre[5].

El régimen normativo de la intervención de comunicaciones a distancia se halla actualmente recogido en el capítulo V del título VIII del libro II de la LECrim —arts. 588 *ter* letra a) y siguientes—, en la versión ofrecida por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Es significativo en este sentido que, a diferencia de lo que sucede con otras modernas medidas de investigación penal —tales como la captación de conversaciones orales directas o el registro de dispositivos de almacenamiento masivo de información, antes referidas—, la LO 13/2015 no regula esta diligencia *ex novo*. Al contrario, existía ya una referencia específica sobre la intervención de conversaciones telefónicas en la versión anterior de la LECrim, aunque esta no cumplía con los estándares de calidad de la ley exigidos por el TEDH —véase la resolución recaída en el asunto *Prado Bugallo*[6]—. Anteriormente, el mismo órgano de garantías ya había censurado la total anomia que, en relación con esta materia, afectaba al ordenamiento jurídico español con carácter previo a la modificación operada por la LO 4/1988 —*vid.* la sentencia dictada en el asunto *Valenzuela Contreras*[7]—. En esta línea, Lezertua Rodríguez (1996: 88) apunta que el TEDH no es riguroso desde un punto de vista estrictamente formal, pero sí impone, en cambio, unas mayores exigencias en torno a la calidad de la norma destinada a sustentar una injerencia estatal en un derecho convencional.

---

5 En esta dirección se pronuncia la Sentencia de la Sala Segunda del Tribunal Supremo —en adelante, TS— de fecha 16 de septiembre de 2021, 699/2021, fundamento de derecho 2.º.

6 STEDH *Prado Bugallo vs España*, de 18 de febrero de 2003, asunto 58496/00, resolución que considera insuficiente la norma que contenía el 579 LECrim en la versión ofrecida por la LO 4/1988.

7 STEDH *Valenzuela Contreras vs España*, de 30 de julio de 1998, asunto 27671/95.

A la espera de una nueva ley procesal penal[8], lo cierto es que hoy en día el Estado cuenta con una «detallada»[9] regulación sobre las intervenciones telemáticas, en la que se tratan los aspectos esenciales en el desarrollo de esta diligencia. Así, además de lo recogido en la nueva Ley General de Telecomunicaciones[10], la LECrim contiene ya previsiones específicas sobre los presupuestos necesarios para la adopción de la medida —art. 588 *ter*, letra a)—, su ámbito de extensión —art. 588 *ter*, letra b)—, la posible afectación a personas diferentes del investigado —art. 588 *ter* c)—, el contenido que ha de tener la solicitud de la medida —art. 588 *ter* d)—, el deber de colaboración exigible a las empresas prestadoras de servicios de telecomunicación —art. 588 *ter* e)—, el control judicial de la medida —art. 588 *ter* f)—, la duración máxima y posible prórroga —art. 588 *ter*, letras g) y h)—, así como la forma en la que las partes pueden acceder al resultado de la diligencia y la notificación de esta a terceros afectados —art. 588 *ter*, letra i), de la LECrim—. Sin embargo, es censurable que la actual regulación no se pronuncie sobre ciertos aspectos de gran relevancia en la práctica procesal, como puede ser la forma en la que el resultado de la intervención —las grabaciones con las conversaciones orales captadas o los documentos que registren las comunicaciones por escrito— ha de incorporarse al plenario.

Dejando a un lado la regla excepcional prevista para ciertos supuestos de urgencia[11], la decisión de limitar el secreto de las comunicaciones se hará

---

8 El Anteproyecto de la nueva LECrim, aprobado en noviembre de 2020, pero cuya tramitación se halla paralizada en la actualidad, regula la intervención de las telecomunicaciones en los arts. 345 a 393; para ello, la norma se inspira en la LO 13/2015, tal y como expresamente reconoce la exposición de motivos en su punto XL.

9 Tal expresión es empleada por la Sentencia del Tribunal Supremo 660/2022, de 30 de junio, de la Sala Segunda, en su fundamento de derecho 1.º.

10 La nueva Ley General de Telecomunicaciones —Ley 11/2022, de 28 de junio— contiene previsiones de interés para la práctica de la intervención, desde el punto de vista de las empresas proveedoras de servicios de telecomunicaciones. *Vid.* en este sentido los arts. 58 —«Secreto de las comunicaciones»— y 59 —«Interceptación de las comunicaciones electrónicas por los servicios técnicos»—.

11 Art. 588 *ter*, letra d), apartado 3, de la LECrim: «En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en

siempre a través de una resolución judicial, debiendo esta decisión estar inspirada en los principios comunes a todas las diligencias de investigación tecnológica, recogidos en el art, 588 bis, letra a), de la LECrim: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. El precepto supone la «proclamación normativa»[12] de la doctrina del Tribunal Constitucional en la materia y, a nuestro parecer, su aplicación podría extenderse —*mutatis mutandis*— a todo acto estatal de investigación penal que implique una injerencia en los derechos fundamentales del ciudadano. En consecuencia, el juez que decida aplicar la medida objeto de este estudio deberá llevar a cabo una operación de ponderación —*balancing test*, en la terminología anglosajona (Suárez Robledano, 2011: 83)— de los intereses en conflicto, optando por el valor que considere preponderante en cada supuesto: bien el interés general o social subyacente en la persecución del delito en cuestión, bien los derechos fundamentales que resultarían lesionados con la práctica de la diligencia. En cualquier caso, debe tenerse presente que las intervenciones telemáticas se caracterizan por ser un medio de corroboración o agotamiento de la investigación (Magro Servet, 2013: 208) y no pueden ostentar nunca un carácter prospectivo, es decir, no pueden tender a descubrir o a localizar ilícitos penales.

Finalmente, un correcto estudio de la medida debe incluir también una referencia a aquellas actuaciones de investigación que únicamente tienen por objeto analizar los datos generados —y conservados— tras haberse producido previamente una comunicación por medios telemáticos. A pesar de que son tratadas por el legislador de forma conjunta con la intervención de comunicaciones a distancia[13], no existe una identidad total entre ambas diligencias. Es cierto que las dos actuaciones tienen una misma raíz o base, que es la existencia

que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida».

[12] La expresión es utilizada por la exposición de motivos de la LO 13/2015, en su punto IV.

[13] El legislador del año 2015 sigue una sistemática unitaria e intitula el capítulo V del título VIII del libro II: «La interceptación de las comunicaciones telefónicas y telemáticas», conteniendo en su sección 1.ª —bajo la rúbrica «Disposiciones generales»— las disposiciones relativas a la intervención de telecomunicaciones (a), y dedicando las secciones 2.ª —«Incorporación al proceso de datos electrónicos de tráfico o asociados»— y 3.ª —«Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad»— a regular (b) el análisis de los datos derivados de las telecomunicaciones.

de una comunicación realizada por medios telemáticos, pero poseen características diversas: a) la intervención se realiza a tiempo real y tiende —principalmente[14]— a permitir que los investigadores accedan al contenido de la comunicación, mientras que el análisis de datos derivados b) persigue solamente rastrear la información que es generada y conservada temporalmente[15] tras producirse una comunicación a distancia. De esta forma, se intenta sumar a los tradicionales rastros biológicos o físicos de un delito ciertos «rastros digitales» (Ortiz Pradillo, 2020: 3), los cuales permitirán vincular al autor con la víctima, con los instrumentos o efectos del crimen, o con el lugar de comisión.

No debe subestimarse la relevancia que posee la diligencia de análisis de datos de tráfico. Como apunta Huete Nogueras (2016: 65), es frecuente que el interés que atesora una conversación a distancia vaya más allá de la averiguación de su contenido. Así, los datos asociados a las comunicaciones telemáticas, a pesar de su «aparente neutralidad técnica», permiten extraer conclusiones muy valiosas para el esclarecimiento de un hecho delictivo o para la determinación de sus responsables[16]. En realidad, el Estado cuenta en este ámbito con un recurso de gran eficacia: partiendo del «principio de disponibilidad» como un paradigma en la materia (González Cano, 2019: 1335) y con sujeción a la normativa de protección de datos personales vigente[17], las autoridades tienen actualmente a su alcance una ingente cantidad de información, la cual es retenida por las operadoras y empresas del sector de las telecomunicaciones no solo por motivos de seguridad o técnicos, sino de muy diversa índole (Fernández

[14] En realidad, la intervención de telecomunicaciones permite también, con carácter accesorio, acceder a los datos de tráfico o asociados al proceso de comunicación, así como a los datos de abonado —art. 588 *ter* b), apartado 2, de la ley procesal—.

[15] *Vid.* la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, en cuyo art. 5 se ordena la conservación de esta información por un período de doce meses. No obstante, debe advertirse que la solidez de esta ley quedó afectada tras anular el Tribunal de Justicia de la Unión Europea la norma a la que trasponía la Directiva 2006/24 CE, por no adecuarse a las exigencias del principio de proporcionalidad: *vid.* la STJUE de 8/4/2014, *Digital Rights Ireland Ltd* (asunto C293/12), ECLI:EU:C:2014:238.

[16] Puede consultarse en esta línea la STS 740/2017, de 16 de noviembre, de la Sala Segunda, FD 1.º.

[17] En este ámbito ha de respetarse con carácter general la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y, con carácter específico, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Rodríguez, 2016: 102). Se ha afirmado elocuentemente en este sentido que los datos constituyen ya una nueva mercancía, una materia comparable con lo que el oro o el petróleo significaron en las revoluciones económicas anteriores, con un valor que dependerá de la utilidad que estos posean para elaborar estudios de mercado y perfiles de consumidores (Pérez de los Cobos Orihuel, 2018: 4)[18]. Tampoco ha de despreciarse la lesividad que esta diligencia puede implicar para los derechos fundamentales de los ciudadanos, especialmente cuando se trate de investigaciones prolongadas en el tiempo; en estos supuestos, ha de valorarse la posibilidad de que los órganos del Estado lleven a cabo procesos de almacenamiento de datos que permitan configurar un «perfil» o «fichero» de la persona, lo cual puede constituir una injerencia en la privacidad, tal como ha sido advertido por la jurisprudencia del TEDH[19]. A este respecto, es de interés emplear la denominada «tesis del mosaico de la privacidad» (Bellovin *et al*., 2014: 570), teoría que propugna que la injerencia en la privacidad de un individuo debe valorarse contemplando el resultado de las averiguaciones del Estado de forma conjunta, como si cada acto de investigación fuese la tesela de un mosaico.

II. NOTAS CARACTERÍSTICAS DE LA ACTUAL COMUNICACIÓN A DISTANCIA

1. UNA REVOLUCIÓN: LA APARICIÓN DE NUEVOS CANALES DE COMUNICACIÓN A DISTANCIA

Ya en los albores del siglo xx el desarrollo tecnológico provocó un impulso esencial en las capacidades de la comunicación a distancia, hablando algunos autores de cambios «dramáticos» (Waltz, 2014: 207) que otorgaban a los seres humanos la posibilidad de enviar información a través de distancias mucho mayores de lo que jamás habían imaginado. Reparemos en el trascendental avance que en este campo supuso la aparición y generalización del uso de medios de comunicación como el telégrafo, el fax o el teléfono, instrumentos

[18] A su vez, el autor cita a M. Andrejevic (2007, *Spy: Surveillance and Power in the Interactive Era*, University Press of Kansas, pp. 81 y ss.).

[19] El Tribunal de Estrasburgo ha declarado que la recogida y almacenamiento por parte de agentes del Estado con carácter sistemático de datos de un individuo —*v. gr.*, estudios, actividades políticas o antecedentes penales—, configurando un «fichero» relativo al sujeto, supone una injerencia en la privacidad de la persona (*vid.* STEDH *Rotaru vs Rumanía*, de 4 de mayo de 2000, asunto 28341/95, puntos 43 y 44).

que permitían una rápida y segura transmisión de mensajes a otras personas situadas en lugares muy distantes del remitente. Un siglo después, no parecen menos determinantes los cambios producidos por la reciente consagración de los medios de comunicación basados en las TIC —las tecnologías de la información y comunicación—, sustentados esencialmente sobre un amplísimo uso de internet[20]. Esto implica un aumento exponencial en las posibilidades que el ciudadano medio tiene para captar, comunicar, conservar e incluso procesar la información (Espín López, 2021: 45), abriendo espacios de comunicación alternativos a los medios que podríamos considerar clásicos, y cuyo uso ya se había extendido —especialmente— en la segunda mitad del siglo xx. De esta forma, nos encontramos en la actualidad con un panorama en el que las nuevas plataformas de comunicación y las redes sociales han transformado la forma en que nos comunicamos, habiéndose producido, en palabras del legislador, una «superación de las formas tradicionales de comunicación a distancia»[21]. En esta línea, la unidad de Criminalidad Informática de la Fiscalía General del Estado[22] —en adelante, FGE— considera que el concepto de «comunicaciones telemáticas» alberga modernamente al menos cuatro diferentes supuestos, en atención al sistema o mecanismo de comunicación o traslado de información utilizado: a) la mensajería instantánea, b) los mensajes SMS o MMS, c) el correo electrónico, y d) la comunicación a través de redes sociales.

Además, no puede obviarse la constante evolución que experimenta la ciencia de las telecomunicaciones, inmersa en un tránsito que provoca que lo que se reputaban técnicas novedosas pasen en poco tiempo a ser medios tradicionales o desfasados; por poner un ejemplo, los SMS se han calificado ya como «reliquias» de la comunicación (López-Barajas Perea, 2016: 18), siendo un instrumento que palidece ante la agilidad de las modernas aplicaciones de mensajería instantánea —*v. gr.*, WhatsApp—. Esta circunstancia hará necesario que para la correcta aplicación de la diligencia de intervención de

[20] En este sentido, la LO 3/2018 antes referida, en el punto IV de su exposición de motivos, señala: «Internet, por otra parte, se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad».

[21] Punto I del preámbulo de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

[22] Dictamen de la unidad de Criminalidad Informática de la FGE 1/2016, de 30 de mayo, sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportadas al proceso penal como medio de prueba de comunicaciones electrónicas, p. 3.

telecomunicaciones se lleve a cabo por el instructor un «renovado entendimiento» de sus exigencias habilitantes (Varona Jiménez, 2020: 162), considerando en todo caso que la protección constitucional del derecho al secreto de las comunicaciones se extiende a todos los medios de comunicación conocidos en el momento de promulgarse la norma fundamental, así como a los que han ido surgiendo o puedan surgir en el futuro[23].

2. NUEVAS PAUTAS DE COMUNICACIÓN

El empleo de estos nuevos medios o plataformas determina la consolidación de varios patrones de conducta comunicativa que poseen interés desde la óptica del presente estudio. En primer lugar, (1) es frecuente que el usuario de redes sociales pase a integrar «grupos» o «chats», formados por un número cerrado y plural —normalmente, tres o más— de participantes; en esta dinámica comunicativa, la persona usuaria emitirá mensajes que irán destinados a una pluralidad de receptores: los demás integrantes del grupo. En un principio, podría parecer razonable entender que la expectativa de privacidad existente en estas comunicaciones debería ser inversamente proporcional al número de personas que se incluyen en el chat de destino, si bien no siempre se cumplirá esta regla. El concepto de íntimo puede entenderse aplicable también a una información que se pretende compartir con una pluralidad determinada de personas: en esta línea, se ha afirmado desde el campo de la psicología que «la privacidad puede ser una propiedad de grupo» (Stuart *et al*., 2019: 4). En cualquier caso, el contenido de estos chats cerrados, enmarcados en lo que doctrinalmente se ha designado como «procesos de relaciones múltiples», quedaría también amparado por el derecho al secreto de las comunicaciones (Carrillo, 2016: 14). Sobre este particular, apunta Ocón García (2022: 90) que para delimitar el ámbito objetivo de protección del art. 18.3 CE, trazando una «línea divisoria entre la comunicación privada y la difusión pública», han de considerarse varios criterios: no solo i) la predeterminación de los destinatarios del mensaje, sino también ii) la conmutabilidad de roles en la relación comunicativa, y iii) la singularidad del destinatario.

Un segundo rasgo de las comunicaciones modernas realizadas a través de redes sociales sería (2) la prevalencia del carácter expresivo de los mensajes, así como la rapidez en el intercambio de información y la ausencia de reflexión (Busquet *et al*., 2011: 36). Esta circunstancia puede influir en el carácter de la información que compartimos a través de estos canales, dando a conocer a los

[23] Véase al respecto la STC 70/2002, de 3 de abril, FJ 9.

demás algunos aspectos de nuestra vida íntima que probablemente no compartiríamos si la dinámica comunicativa fuese diferente, como sucede en el envío de correos electrónicos —medio en el que el usuario suele revisar el contenido del mensaje antes de remitirlo—.

Finalmente, es también un signo característico de esta forma de comunicarse (3) la posibilidad de transmitir un contenido diverso. El vertiginoso avance de la telecomunicación arriba referido debe contemplarse también desde esta perspectiva: lejos quedan los tiempos en los que las personas nos comunicábamos interpretando una sucesión de pulsos eléctricos y el silencio que se producía entre ellos, como sucedía con el código morse. Posteriormente, los seres humanos logramos llevar a cabo la transmisión de palabras escritas, sonido y, últimamente, también de otros contenidos, tales como archivos de imagen, animación o vídeos. Todas estas formas son susceptibles de contener información relativa a nuestro ámbito íntimo y se encuentran amparadas también por el derecho plasmado en el art. 18.3 CE (Espín López, 2021: 39).

3. LA MASIVIDAD EN EL USO DE LAS TIC

El estudio de la medida de intervención de telecomunicaciones y el análisis de sus datos asociados será más completo si se comprende que la utilización de las TIC es un hecho prácticamente unánime en la actualidad. En concreto, el análisis estadístico revela que el teléfono móvil estaba presente en 2022 en el 99,5 % de hogares en nuestro país, mientras que el 96,1 % disponía de acceso a internet[24]. Estas cifras implican una verdadera democratización del uso de estas tecnologías, expandiéndose sin apenas distinciones por razones territoriales, socioeconómicas o de cualquier otra índole. Por otra parte, se produce en paralelo a esta expansión un crecimiento de las empresas dedicadas al campo de las telecomunicaciones, convirtiéndose este en uno de los sectores más florecientes y dinámicos de la economía. Contemplado desde el prisma de la investigación penal, indica Gómez Colomer (2017: 31) que el fenómeno de la «masividad en el uso» de las TIC nos convierte a una gran parte de los ciudadanos en posibles sujetos pasivos de la diligencia de intervención de comunicaciones telemáticas, al menos desde un punto de vista abstracto. No

[24] Así lo ha constatado el Instituto Nacional de Estadística, (2022). *Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación (TIC) en los Hogares Año 2022.* Nota de Prensa publicada el 29 de noviembre de 2022. Disponible para consulta en el enlace http://tinyurl.com/3t8juce8.

obstante, y como ha constatado la jurisprudencia del Tribunal Supremo[25], este uso masivo genera unos efectos más amplios en el terreno jurídico, provocando la aparición de nuevos escenarios virtuales en los que «colisionan» los derechos fundamentales de los ciudadanos.

Por otra parte, debe comprenderse también que no todo el moderno tráfico de información comprende comunicaciones entre humanos. En realidad, muchas de las comunicaciones a distancia que se producen actualmente son ya entre un humano y una máquina, o solamente *inter machinas*. Y aunque el derecho al secreto a las comunicaciones protege únicamente las producidas entre personas[26], estas transmisiones de información sí son susceptibles de comprometer el derecho a la intimidad —art. 18.1 CE— o el derecho a la protección de datos de carácter personal —art. 18.4 CE—[27].

4. USO INTENSIVO DE LAS TIC

La utilización contemporánea de las TIC —y de las redes sociales en particular— no se define solo por ser de carácter masivo, sino también intensivo. No sucedía así, *verbi gratia*, con el uso del teléfono móvil que se producía a finales del siglo pasado: por aquel entonces los seres humanos no solíamos vivir acompañados las 24 horas del día por un instrumento que nos permite comunicarnos instantáneamente con cualquier otra persona. Esta circunstancia, lógicamente, incrementa de forma muy notable la cantidad de comunicaciones a distancia que un ser humano mantiene de forma cotidiana y, por

[25] STS 593/2022, de 28 de julio, de la Sala Primera, FD 3.º.

[26] En esta dirección se pronuncia la STC 281/2006, de 9 de octubre, en su FJ 3.º: «Pues bien, si el derecho al secreto de las comunicaciones (art. 18.3 CE) constituye una plasmación singular de la dignidad de la persona y el libre desarrollo de la personalidad que son "fundamento del orden político y de la paz social" (art. 10.1 CE), las comunicaciones comprendidas en este derecho han de ser aquellas indisolublemente unidas por naturaleza a la persona, a la propia condición ».

[27] A este respecto es de interés la reflexión contenida en la Circular FGE 2/2019, de 6 de marzo, sobre interceptación de comunicaciones telefónicas y telemáticas, punto 2: «Deberá tenerse no obstante presente que existen comunicaciones entre máquinas que, puestas en relación con otros datos, sí pueden afectar a alguno de estos derechos, como el derecho a la intimidad, p. ej., la conexión entre los dispositivos móviles de comunicación, las tarjetas SIM insertadas en los mismos y las estaciones BTS. Esta conexión se produce por la mera activación del dispositivo a la red, se trata, por tanto, de una conexión entre maquinas, pero puede resultar esencial para determinar quién es el usuario de un determinado dispositivo o cuál es su localización en el espacio».

lo tanto, amplía en la práctica el ámbito objetivo o el campo de actuación de la diligencia cuyo análisis nos ocupa.

Pero más allá de lo que podría reputarse como un natural aumento del intercambio de información coherente con las modernas posibilidades comunicativas, los actuales parámetros de la telecomunicación humana están superando las expectativas. En verdad, en la actualidad seguramente no estemos ante una comunicación razonablemente potenciada por las capacidades de las TIC, sino ante una «hipercomunicación» (Ortiz Pradillo, 2020: 10). En otras palabras, es posible que los seres humanos nos estemos comunicando por encima de lo que resultaría conveniente, o al menos «más allá de lo que históricamente se ha considerado como necesario» (Marchena y González-Cuellar, 2015: 201). En opinión de Armenta Deu (2018: 68), no es infrecuente que los usuarios de las redes sociales —sobre todo las personas más jóvenes— desarrollen una relación de dependencia hacia estas aplicaciones, lo que provoca que viertan una cantidad ingente de datos personales en la red. También es significativo que los usuarios de redes sociales hayan mutado su condición o estatus, pasando de ser meros consumidores de contenidos creados por terceros a erigirse también en creadores de la información que existe en la red; en palabras del Tribunal Constitucional, tales usuarios han devenido en «sujetos colaborativos, ciudadanos que interactúan y que ponen en común en redes de confianza lo que tienen, lo que saben o lo que hacen, y que comparten con un grupo más o menos numeroso de destinatarios»[28].

5. LA EXTRATERRITORIALIDAD

Por último, el cambio en la comunicación en la era digital ha de ser interpretado desde una perspectiva espacial. En esta línea, la anteriormente referida evolución de las TIC permite al ser humano una comunicación a nivel global: en la actualidad, una gran parte de las personas —incluso aquellas que viven en las regiones menos favorecidas económicamente— poseen la capacidad de recibir y enviar ágilmente información a otras personas situadas en las zonas más alejadas del planeta.

Esta realidad ya había sido pronosticada en el pasado desde diversos ámbitos. En el terreno de la sociología, McLuhan (McLuhan y Powers, 1995: 123) refería hace más de tres décadas[29], en la explicación de los efectos prácticos que tendrían lugar en su célebre «aldea global», la siguiente posibilidad: «[…]

[28] STC 27/2020, de 24 de febrero, FJ 3.º.

[29] La edición original data de 1989.

más y más personas entrarán en el mercado de intercambio de información, perderán sus identidades privadas en el proceso, pero surgirán con la capacidad de interconectarse con cualquier persona sobre la faz de la Tierra». También desde el campo de la filosofía, Etxevarría (1994: 2) advirtió a finales del siglo pasado que se estaba conformando una nueva estructura social de escala mundial: «[…] durante el siglo xx se ha ido generando una nueva forma de organización social que tiende a expandirse por todo el planeta, transformándolo en una nueva ciudad: Telépolis». Para dicho autor, esta forma de organización social se producía no solo por la existencia de dispositivos técnicos que permitían la comunicación a distancia, sino también por la nítida voluntad de los seres humanos de asumir esta forma de contactar telemáticamente como su canal ordinario de comunicación. Hoy en día, bien entrado el siglo xxi, podemos comprobar que estas flechas teóricas han dado en la diana: quizá la mayor parte de las relaciones humanas ya no se produzcan en el mundo físico, sino en la red. Se ha dicho con acierto en este sentido que las antiguas ágoras físicas, entendidas como lugares de reunión, debate y decisión colectiva, han sido desplazadas en gran medida por ágoras digitales (Pérez-Latre, 2015: 108)[30], en donde participan personas que pueden estar ubicadas en lugares muy distantes.

III. APLICACIÓN DE LA MEDIDA FRENTE AL MODERNO PANORAMA DELICTIVO

1. EL AUGE DE LA CRIMINALIDAD *ONLINE*

Parece lógico concluir que en el tránsito de una buena parte de las relaciones humanas del mundo físico al mundo digital se incluye también un sector de las interacciones que revisten un carácter delictivo. En esta dirección, la FGE[31] destacó en el año 2021 la existencia de un progresivo aumento en el

[30] El autor reflexiona sobre esta idea: «¿Qué ha sucedido con el ágora griega? El "ágora" era un lugar de reunión, pero también era un sitio donde había personas que sólo se preocupaban de entretenerse con las últimas noticias. El recuerdo del "ágora" evoca la necesidad de no fijarnos sólo en el hecho de que estamos hablando sino también en el contenido y calidad de las conversaciones. Los nuevos espacios digitales despiertan grandes esperanzas. Gracias a ellos estamos más cerca de otros; pueden ser el ágora donde se intercambian soluciones e ideas que benefician a todos, se logra más comprensión mutua y se facilita que lleguemos a ser una comunidad».

[31] Puede consultarse, en relación con esta problemática, la Instrucción 2/2011, de 11 de octubre, sobre el fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las fiscalías (actualización de 2021), punto II.1.

número de investigaciones criminales vinculadas a la utilización de las nuevas tecnologías y, más específicamente, de internet. También la jurisprudencia constata la traslación de un gran número de delitos al ámbito digital, siendo esta una realidad especialmente alarmante en relación con determinadas tipologías criminales, en las que el empleo de las redes sociales incrementa las capacidades y el alcance de la actuación del delincuente, como sucede, *v. gr.*, con el *childgrooming* —art. 183 CP— o el *sexting* —art. 197.7 CP—. En este contexto, el TS ha declarado que bajo la expresión «lugar de comisión del delito» deben entenderse comprendidos en la actualidad no solo los lugares físicos, sino también los espacios digitales o virtuales, en los que las personas pueden también subir o volcar contenidos en el curso de una comunicación telemática[32].

Se está produciendo, por lo tanto, un auge de los llamados «delitos a distancia», es decir, aquellos en los que existe una separación espacial entre el lugar desde el que el sujeto activo lleva a cabo la acción u omisión típica y aquel en el que se produce el daño al bien jurídico protegido. La «fragmentación geográfica» (Ortiz Pradillo, 2013: 11) del *iter criminis* origina frecuentemente problemas relativos a la determinación del momento y el lugar en el que se comete el delito. Además, cuando el ilícito produce sus efectos en otro Estado nos encontraremos ante un supuesto de delincuencia transnacional, fenómeno que obliga a caminar hacia una armonización legislativa entre países (Varona Jiménez, 2020:170) con el objeto —entre otras cuestiones— de garantizar un estándar mínimo de protección de nuestros derechos en el mundo digital. Reparemos en el hecho de que, si podemos ser víctimas de delitos cometidos en otro país, nuestra privacidad también puede verse concernida por las actuaciones de investigación penal que están siendo dirigidas por las autoridades de otro Estado; así, se ha expresado desde la doctrina que «los datos no entienden de fronteras» (Pérez de los Cobos Orihuel, 2018: 5).

En referencia a esta problemática, el TS ha reflexionado recientemente sobre la admisibilidad de la investigación de un delito *online* cuando la denuncia y las primeras actuaciones de indagación se producen fuera de nuestras fronteras. El caso se origina cuando una conocida red social detecta un comportamiento delictivo —abuso sexual a menores— por parte de un usuario y decide dar parte a las autoridades extranjeras, cediendo, además, las conversaciones —ya finalizadas— que el sujeto había mantenido a través de la

[32] Véase, *ad exemplum*, la STS 547/2022, de 2 de junio, de la Sala Segunda, FD 3.º, en la que se avala la imposición de la prohibición del uso de una red social como una pena accesoria de privación del derecho a acudir a determinados lugares en que se haya cometido el delito, *ex* art. 48.1 CP.

aplicación. El TS decide validar esta cesión de datos y emplea para ello el llamado «principio de la no indagación»[33], conforme al cual la regla de la nulidad de las pruebas obtenidas con violación de los derechos fundamentales —art. 11 de la LOPJ— no debe llevar necesariamente a una exhaustiva revisión de la forma en la que las autoridades de otros países han obtenido el material probatorio, singularmente cuando se trate de Estados que se integran en nuestro entorno jurídico y comparten un mismo sistema de derechos fundamentales; en cualquier caso, este principio decaerá siempre que se atisbe una grave y flagrante violación de tales derechos.

2. LA DOBLE EFICACIA DE LA INTERVENCIÓN DE COMUNICACIONES TELEMÁTICAS

Al diseñar los «presupuestos de aplicación de la diligencia», el art. 588 *ter* a) de la LECrim dispone que «sólo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación». En nuestra opinión, puede apreciarse aquí un doble ámbito de aplicación de la intervención telemática. Por un lado, la medida se halla normativamente configurada para combatir la delincuencia —grave— perpetrada en el mundo físico; en esta línea ha de entenderse la remisión que el primer inciso del referido precepto hace al art. 579.1 de la LECrim, reservándose el uso de la diligencia para la investigación de i) delitos cometidos en el seno de un grupo u organización criminal, ii) delitos de terrorismo y iii) delitos dolosos castigados con pena con límite máximo de —al menos— tres años de prisión. La

[33] *Vid.* STS 807/2022 de la Sala Segunda, de 7 de octubre, FD 4.º. El TS valora dos circunstancias para entender legítima esta cesión: i) la previa existencia en ese caso de una aceptación por parte del usuario de las condiciones de uso de la red social —en las que se advertía de la posibilidad de denuncia a las autoridades en caso de incurrir en comportamientos delictivos—, y ii) la existencia en nuestro ordenamiento jurídico de una norma que habilita la conservación y cesión de datos en supuestos similares —en concreto, el Reglamento UE 2021/1232 del Parlamento Europeo y del Consejo, de 14 de julio de 2021, por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea—.

conveniencia de acudir a este medio de investigación es clara en los dos primeros supuestos delictivos, al tratarse en ambos casos de conductas especialmente lesivas para el interés social[34]. Más polémica nos parece la tercera premisa: no solo por permitir la aplicación de la diligencia en relación con delitos no graves en un sentido estrictamente penológico —art. 33.2, letra b), del CP—, sino porque no habilita su utilización para la investigación de ciertos ilícitos penales socialmente trascendentes[35], como pueden ser algunos delitos contra la libertad sexual —art. 182.1 del CP—.

Por otra parte, las intervenciones telemáticas también pueden emplearse para la averiguación de delitos cometidos íntegramente en el mundo digital. Esta parece ser la idea contenida en el inciso final del art. 588 *ter* a) LECrim, al referirse a ilícitos «cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación». Reparemos en que el legislador no establece ninguna mención específica a la gravedad del delito que se investiga en este ámbito, lo cual podría llevar a una utilización completamente inadecuada de la medida[36]; por ello, y dada la grave afectación de derechos fundamentales que puede ocasionar, la utilización de la diligencia requerirá en estos supuestos una especial observancia del principio de proporcionalidad[37].

En definitiva, la intervención de comunicaciones a distancia se erige como una herramienta de gran utilidad para hacer frente a varios sectores del panorama delictivo actual, estando normativamente configurada como una diligencia bidireccional o de doble eficacia: puede dirigirse al esclarecimiento de

---

[34] En relación con el terrorismo, el Consejo de Europa ha declarado que se trata de una actividad que «pone en grave peligro los derechos humanos, amenaza la democracia y pretende, en particular, desestabilizar los gobiernos legítimamente constituidos y socavar la sociedad civil pluralista». *Vid.* el art. 1 de las Directrices del Comité de Ministros del Consejo de Europa en materia de derechos humanos y de lucha contra el terrorismo (*Guidelines of the Committee of Ministers of the Council of Europe on human rights and the fight against terrorism*) adoptadas el 11 de julio de 2002.

[35] Así lo puso de manifiesto el CGPJ en su informe al Anteproyecto de la LO 13/2015, en el punto V, apartado III, número 2.

[36] Una interpretación estricta —y descontextualizada— del art. 588 *ter* a) de la ley procesal podría conducir, *verbi gratia*, a intervenir las comunicaciones telemáticas de un individuo que es investigado por un delito leve de estafa cometido por medios telemáticos.

[37] Así lo recomienda la Circular FGE 2/2019, antes citada, en su punto 3. En particular, la circular entiende que la resolución judicial habilitante deberá incluir un mayor esfuerzo argumentativo cuando el delito investigado esté sancionado con penas cuyo máximo no alcance los tres años de prisión.

hechos cometidos tanto el mundo físico como en el entorno digital. No obstante, creemos que la principal utilidad práctica de la medida sigue siendo hoy en día la de completar o ultimar la investigación de ilícitos en los que, si bien algunos de los actos preparatorios se llevan a cabo de forma telemática, terminan cometiéndose en el mundo físico. Piénsese en el supuesto prototípico o clásico en el que se emplea la intervención de comunicaciones para vigilar a un sujeto que participa en actividades relacionadas con el narcotráfico: la medida permitirá en muchas ocasiones a las autoridades conocer el lugar y el momento en el que se va a producir el traslado de las sustancias tóxicas, favoreciendo su incautación; además, el contenido de sus conversaciones telemáticas constituirá normalmente un indicio incriminatorio más, siendo un elemento de refuerzo de la tesis acusatoria durante el juicio oral.

3. PRINCIPALES INCONVENIENTES EN LA APLICACIÓN DE LA MEDIDA

El primer problema reside a nuestro juicio en el elevado impacto iusfundamental de la diligencia (a), cuestión que ha de preocupar especialmente al juez instructor como principal garante del respeto a los derechos fundamentales del investigado (López Guerra, 2018: 5). En particular, la medida compromete nítidamente el derecho al secreto de las comunicaciones, habiendo declarado el TC que este derecho ostenta un especial valor por estar conectado con otros bienes jurídicos protegidos por la Norma Fundamental[38]. Además, y dadas las características del actual contexto comunicativo, la intervención telemática posee ahora una mayor capacidad de injerencia en la intimidad, al hallarse el ciudadano medio inmerso en una dinámica en la que transmite de forma habitual y a través de las TIC una gran cantidad de información de carácter personal. De esta forma, el uso intensivo por parte del investigado del medio o terminal intervenido hará que, probablemente, sean captados un mayor número de mensajes que resultan totalmente ajenos al hecho criminal cuya averiguación justificó la injerencia. El incremento de esta «recogida de arrastre»[39] implica dos desventajas: por una parte, se lesiona en mayor medida la intimidad del investigado —y del tercero con que se comunica—, por otra,

[38] STC 123/2002, de 20 de mayo, FJ 5.º: «En una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no sólo una garantía de libertad individual, sino un instrumento de desarrollo cultural, científico y tecnológico colectivo».

[39] Así se refiere la jurisprudencia a este fenómeno, prácticamente inevitable en toda intervención telemática. *Vid.* STS 419/2013, de 14 de mayo, de la Sala Segunda, FJ 1.º.

se dificulta la labor del instructor a la hora de seleccionar o filtrar el material obtenido —art. 588 *ter*, letra i), apartado 1, de la LECrim—. Esta mayor afectación de derechos debería ser ponderada por las autoridades al adoptar la medida, con el objeto de garantizar la observancia del principio de proporcionalidad. Una opción plausible sería la de reducir con carácter general el plazo por el que se autoriza la diligencia: si bien la duración máxima inicial es de tres meses *ex* art. 588, ter g) de la LECrim, no existe ningún impedimento para que el instructor fije un plazo sensiblemente inferior; naturalmente, esto debe entenderse sin perjuicio de la posibilidad de acordar posteriormente una prórroga de ser necesaria para lograr el éxito de la investigación.

En segundo término, conviene destacar que la dimensión extraterritorial de la comunicación en la era digital provoca en ocasiones una excesiva lentitud en el desarrollo de la medida (b), sobre todo si se tiene en cuenta que las jurisdicciones de los Estados siguen inmersas en una «poco permeable dimensión territorial» (Rodríguez-Yzquierdo Serrano, 2021: 135). Así, si la persona investigada hace uso de una plataforma de comunicación que tiene sus servidores radicados fuera de nuestras fronteras, será preciso acudir a mecanismos de cooperación judicial internacional para poner en práctica la diligencia. En estos supuestos, es evidente que la emisión de una comisión rogatoria dilataría en gran medida la aplicación de la intervención telemática, convirtiéndola en una actuación ineficaz frente a muchas de las actividades delictivas para cuyo descubrimiento está normativamente diseñada: pensemos, por ejemplo, en la agilidad con la que debe sustanciarse la investigación de las organizaciones dedicadas al narcotráfico a escala internacional.

Por otra parte, la utilidad de la medida objeto de estudio decrece actualmente ante la posibilidad de que las comunicaciones a distancia sean encriptadas (c). Nos referimos aquí no solo al uso de canales de comunicación que podríamos calificar como ordinarios —*v. gr.*, las aplicaciones Telegram o WhatsApp— y que están dotados de mecanismos que dificultan el acceso a los investigadores, como es el caso del cifrado de extremo a extremo de los mensajes. Además, existen ciertas plataformas de comunicación específicamente configuradas para preservar el anonimato de sus usuarios, tales como las redes EncroChat[40] o Sky-ECC. De esta forma, si bien es cierto que el actual

[40] EncroChat era una red de comunicaciones encriptadas empleada por determinadas organizaciones criminales y dotada de numerosas cautelas dirigidas a mantener el carácter anónimo de los participantes; en particular, se empleaban en ella dispositivos que no tenían cámara, micrófono o puerto para USB o GPS, programándose, además, el borrado automático de los mensajes enviados. En relación con las actuaciones de investigación que pueden practicarse para acceder a esta clase de redes, es

estado de la técnica otorga mayores capacidades a las autoridades para intervenir las telecomunicaciones, también los delincuentes más audaces —en especial, los grupos y organizaciones criminales— suelen adoptar cautelas al respecto (Nieva Fenoll, 2016)[41].

La existencia de estos obstáculos puede llevar al órgano instructor a descartar el empleo de la intervención telemática, optando por otras técnicas de investigación introducidas en nuestra ley procesal penal a través de la citada LO 13/2015. Nos referimos, en concreto, al registro remoto sobre equipos informáticos, diligencia que se halla regulada en el art. 588 *septies*, letras a) a c), de la LECrim, y que permite a las autoridades, mediante el uso de sofisticadas técnicas, examinar a distancia al contenido de los dispositivos informáticos de la persona investigada, incluyendo el acceso a sus comunicaciones telemáticas. Dado su carácter dinámico, y a pesar de que probablemente no era esta la intención inicial del legislador (Bachmaier Winter, 2017: 15)[42], la medida posibilita en la práctica la interceptación en tiempo real de las telecomunicaciones. Por esta vía se podría evitar acudir a mecanismos de cooperación judicial internacional (b), siempre que el dispositivo objeto de examen se halle situado dentro de nuestras fronteras[43]; asimismo, el registro remoto logra

---

de interés la lectura de las conclusiones de la abogada general del Tribunal de Justicia de la Unión Europea, Capeta, sobre el caso C-670/22 (*Staatsanwaltschaft Berlin —EncroChat—*), publicadas el 26 de octubre de 2023.

41 En esta línea, Nieva Fenoll se muestra escéptico sobre la efectividad de esta medida de investigación: «La experiencia ha demostrado que esa agresión contra la privacidad sirve de muy poco a efectos investigadores. Actualmente existen canales seguros de comunicación que prestan perfecto y fácil servicio a cualquier usuario. En consecuencia, las intervenciones de comunicaciones ya sólo podrían ser útiles para perseguir a delincuentes comunes bastante descuidados en sus comunicaciones, lo que no sólo es desproporcionado, sino completamente absurdo».

42 La autora llega a la conclusión de que no sería irrazonable trazar una analogía entre el registro remoto de ordenadores y la interceptación de telecomunicaciones, tomando en consideración que el registro remoto permite acceder a los mensajes almacenados en un dispositivo, y dado que el acceso a esas comunicaciones en poco o nada se diferencia en la mayoría de los casos de su interceptación en tiempo real.

43 Coincidimos con lo sostenido por la FGE en este punto: «En estos casos, el criterio deberá ser siempre el de exigir un vínculo territorial con España; el Juez podrá autorizar el registro remoto de un sistema informático que se encuentre en España, aunque a través de él se acceda a datos ubicados en el extranjero, pero no autorizar el registro de un sistema localizado en el extranjero, sin acudir para ello a la cooperación judicial internacional». *Vid.* la Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos, punto 4.1.

salvar el obstáculo de la encriptación (c), al permitir que los investigadores tengan acceso al mensaje intervenido en las mismas condiciones que el usuario del dispositivo afectado: es decir, ya desencriptado —si es el receptor— o antes de ser cifrado y enviado —en caso de ser el emisor—. Como contrapartida, esta diligencia posee también un elevadísimo potencial de injerencia en los derechos fundamentales (a), mayor incluso que el de la genuina intervención, pues no solo lesiona la intimidad y el derecho al secreto de las comunicaciones del investigado, sino que afecta también a su «derecho al entorno virtual»[44], siendo este un bien jurídico cuya consideración como «derecho constitucional de nueva generación» es aceptable en un sentido material, pero discutible desde un punto de vista formal (Elvira Perales, 2020: 137). En nuestra opinión, es admisible utilizar el registro remoto para lograr la intervención a tiempo real de las comunicaciones telemáticas, si bien siempre que se reúnan simultáneamente los presupuestos legalmente exigidos para ambas diligencias.

Finalmente, la aplicación de cualquier diligencia de investigación sobre una comunicación telemática exige reparar en la posible actuación *in nomine alterius* de uno o de ambos interlocutores (d). Así, las modernas plataformas de comunicación poseen características que permiten la suplantación de la identidad en el entorno digital[45], siendo esta una circunstancia que no solo entorpece gravemente la identificación del verdadero responsable de un hecho delictivo, sino que puede conducir incluso al inaceptable resultado de incriminar a un inocente.

IV. *EXCURSUS*: ALGUNAS REFLEXIONES DESDE UNA ÓPTICA ANTROPOLÓGICA

Permítasenos realizar aquí algunas reflexiones que, si bien están relacionadas con la reciente evolución producida en el contexto comunicativo, trascienden el ámbito estrictamente jurídico; al fin y al cabo, el cambio del modo

[44] Tal derecho integraría, en palabras de la Sala Segunda, «toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos». Véase la STS 342/2013, de 17 de abril, FD 8.º.

[45] En relación con esta problemática, especialmente frecuente en el ámbito de las estafas *online*, puede verse la comunicación de la fiscal de Sala de Criminalidad Informática de 14 de febrero de 2022, intitulada: «Sobre la usurpación de identidad de otra persona en la planificación y ejecución de actividades de carácter defraudatorio».

en que las personas nos comunicamos no es más que una parte de una transformación mucho más profunda y que alcanza a la misma forma en que existimos, otorgándonos una suerte de «dimensión digital» (Sanchís Crespo, 2017: 2). El aspecto crucial de esta metamorfosis reside, probablemente, en el uso desmedido de los dispositivos electrónicos con conexión a internet: algunos estudios sugieren que en el actual contexto un ser humano medianamente longevo dedicará veintiocho años de su vida a navegar por la red (Meyer, 2023).

En primer lugar, la modificación de la realidad comunicativa en la era digital está íntimamente vinculada con una profunda variación experimentada en la forma en la que las personas adquirimos y transmitimos conocimientos. Son varias las notas características de este proceso (Burkle y Cobo, 2018: 84): 1) descentralización y desintermediación, 2) masividad y demanda creciente, 3) la existencia de nuevas fuentes de creación del conocimiento y, consecuentemente, 4) la aparición de nuevos medios de reconocimiento o validación del conocimiento. La mayor facilidad en la comunicación genera evidentes efectos benévolos, como potenciar la interacción y confluencia en la red entre personas que comparten —o discrepan en— ideas o intereses (Pesqueira Zamora, 2020: 421), produciendo las consiguientes sinergias. Como contrapartida, la adaptación del conocimiento al mundo digital trae consigo también algunas consecuencias injustas o indeseables, siendo un ejemplo la posible exclusión de este ámbito cognitivo de personas que carecen de habilidades para manejar los medios digitales, bien sea por motivos socioeconómicos, bien a causa de su edad. Se produce en este punto lo que algunos autores han denominado una «fractura» o «división» del conocimiento, surgiendo una diferenciación entre «nativos digitales» e «inmigrantes digitales» (Busquet *et al*., 2011: 34).

Además, y siendo un aspecto corolario de lo anterior, la sumersión del ser humano en el mundo digital tiene también su eco en la forma en que se produce nuestra percepción o análisis de la realidad. Son varias las voces que alertan sobre la cuestionable eficacia de las TIC en el proceso de interpretación de la información. Ciertamente, el hecho de disponer de ingentes cantidades de datos a golpe de un clic —como sucede en actual estado de las cosas— no garantiza que vayamos a hacer un mejor uso de estos; así, se ha indicado con acierto que el incremento de la cantidad de información no implica un aumento de los niveles de sabiduría, y ni siquiera de los de conocimiento, existiendo generalmente un déficit de contexto e interpretación (Pérez Latre, 2015: 106). Esta circunstancia tiene también sus repercusiones en el ámbito colectivo como sucede, por ejemplo, con la proliferación y expansión de noticias falsas —*fake news*—, fenómeno que se ve catapultado por el uso de las redes sociales (Flores Vivar, 2019:199).

Para algunos, la digitalización de ciertas facetas del ser humano conllevará incluso una recolocación de los marcos teóricos de nuestra civilización, comprendiendo también las más básicas adquisiciones jurídico-políticas (Lasalle, 2021). Esta recolocación terminará haciendo que sea preciso operar lo que Requejo Pagés (2020: 21) denomina una «verdadera reconstrucción intelectual del mundo». En esta línea, el autor resalta la nítida divergencia que existe entre la realidad social actual y la que imperaba en el momento de promulgarse nuestra CE, tratándose de dos mundos completamente diferentes: el mundo digital actual y el «sólidamente analógico» de 1978[46].

Por otra parte, parece que la hipercomunicación o hiperconectividad a la que más arriba hacíamos referencia no logran acabar con la sensación de soledad que muchas veces nos embarga. Los numerosos y frecuentes contactos que mantenemos con los demás usuarios de las redes sociales no impiden que sigamos experimentando sensaciones tan genuinamente humanas como la incomprensión o el abandono; de hecho, para algunos, estas nuevas aplicaciones no tienden a estrechar las relaciones humanas, sino que más bien promueven una conexión digital que ofrece «la ilusión de la compañía sin las exigencias que tiene la amistad» (Pérez Latre, 2015: 104). En verdad, puede que estemos más cerca que nunca de conformar esa «multitud solitaria» a la que Riesman (Riesman *et al.*, 1989: 307) aludía a mediados del siglo pasado.

Finalmente, debemos apuntar que la nueva realidad comunicativa puede acabar alterando la noción de privacidad, concepto cuyas bases dogmáticas tradicionales son objeto de «cambios sísmicos»[47] a medida que se incrementa el uso de las tecnologías propias de la era digital. La novación paulatina de este concepto constitucional podría dar lugar reflexiones que exceden el objeto de este estudio. Baste hacer constar aquí que, como refiere Lucas Murillo de la Cueva (2008: 45), la existencia de medios que permiten conocer y divulgar sin límites todo tipo de información, junto con otros factores contemporáneos como la urbanización y la masificación, está provocando una verdadera «redefinición» de la intimidad.

---

[46] Se explica en esta línea que «el (mundo) construido por la racionalidad occidental se ve seriamente amenazado por la racionalidad puramente inductiva que es consustancial a la gestión masiva de datos. Si aquella se fundamenta en el principio de causalidad, el de esta última lo hace en el de correlación, que permite analizar fenómenos complejos sin conocer y comprender sus causas». A su vez, el autor cita a A. Basevant y J. P. Mignard (2018, *L'empire des données*, París, Don Quichotte, p. 71).

[47] Así se expresa el juez John Roberts al emitir la opinión del Tribunal Supremo de Estados Unidos en el caso *Carpenter v. United States*, número 16-402, del 22 de junio de 2018, punto III.

V. CONCLUSIONES

La intervención de comunicaciones telemáticas es una diligencia de investigación penal que permite acceder en tiempo real al contenido de las conversaciones a distancia mantenidas por el investigado, desplazando temporalmente su derecho al secreto de las comunicaciones —art. 18.3 CE—. Si bien el legislador vigente utiliza la expresión «interceptación de comunicaciones telefónicas o telemáticas», consideramos más preciso hablar de «intervenir» —por tener el verbo una acepción que se refiere de forma específica a esta actividad de control del Estado— y de «comunicaciones telemáticas» —al englobar esta denominación también las comunicaciones a través del teléfono—.

La medida es susceptible de incluir el acceso a los datos de tráfico o asociados a la comunicación intervenida; no obstante, el acceso a tales datos puede configurarse también como una actuación de investigación diferente, teniendo por objeto únicamente el análisis de la información que es generada y conservada temporalmente tras producirse una comunicación a distancia, sin entrar a conocer el contenido de la conversación. A pesar de ser una diligencia menos conocida, el análisis de datos asociados ostenta un gran potencial para el esclarecimiento de hechos delictivos, pues posibilita seguir los rastros digitales del ilícito investigado y vincular al responsable con la víctima, con los medios empleados para cometer el delito o con el *locus criminis*. Además, esta medida podría afectar notablemente a la privacidad de los ciudadanos, especialmente en los supuestos de vigilancias que se dilatan en el tiempo, cuando los referidos vestigios digitales de un individuo se pueden almacenar y luego contemplar en perspectiva, revelando así amplias parcelas de su personalidad.

Siendo utilizada por las autoridades penales desde hace varias décadas, la intervención de comunicaciones telemáticas merece ahora un entendimiento renovado. En primer lugar, porque tras la reforma operada en la Ley de Enjuiciamiento Criminal por la LO 13/2015 existe en nuestro país una regulación que, aun siendo mejorable, contempla de forma detallada y completa los aspectos esenciales de la diligencia; se logra así superar la situación de anomia anterior, contando con una base normativa que cumple con los estándares de calidad de la ley exigidos por el Tribunal de Estrasburgo. En segundo término, porque el campo de aplicación de la medida ha variado de forma considerable. Las conclusiones que se obtenían en un mundo mayoritariamente analógico no pueden mantenerse intactas en el actual contexto digital, en el que la comunicación a distancia tiene algunos rasgos característicos propios —nuevos canales de comunicación, diferentes patrones de conducta, masividad e intensidad en el uso de las TIC, escala global…—. Debe valorarse que, en abstracto,

esta técnica de investigación tiene una mayor capacidad de injerencia en la privacidad, al haberse multiplicado la cantidad de información que los ciudadanos compartimos telemáticamente en nuestro día a día.

Debe destacarse igualmente la doble eficacia de la intervención de comunicaciones telemáticas, siendo una diligencia que puede emplearse para la investigación de delitos cometidos tanto en el mundo físico como en el mundo digital. Ante un panorama delictivo en el que la criminalidad *online* está al alza, el principal ámbito de aplicación de la medida sigue residiendo en la investigación de delitos perpetrados en el mundo físico. La normativa vigente habilita su uso en la averiguación de delitos dolosos sancionados con una pena cuyo límite máximo alcance, al menos, los tres años de prisión; sin embargo, la capacidad de injerencia de la medida hace aconsejable reservar su utilización para combatir las conductas más graves, especialmente en los supuestos de delitos de terrorismo o perpetrados por grupos u organizaciones criminales. En este contexto, existen determinadas circunstancias —*v. gr.*, la encriptación de mensajes por los criminales o la necesidad de acudir a mecanismos de cooperación judicial internacional— que disminuyen la eficacia de la medida y que pueden vadearse empleando otra novedosa técnica de investigación: el registro remoto de equipos informáticos.

En cualquier caso, la decisión de intervenir las comunicaciones a distancia del investigado ha de respetar siempre los principios que rigen todas las medidas de investigación tecnológica fijados en el art. 588 bis a) de la LECrim, señaladamente el principio de proporcionalidad. El juez que acuerde la medida deberá ponderar así los intereses en conflicto: por un lado, la represión del delito investigado, y, por otro, los derechos fundamentales que resultarían lesionados, teniendo estos un valor generalmente preponderante (Moreno Catena, 2010: 17).

Bibliografía

Armenta Deu, T. (2018). Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre. *IDP: Revista de los Estudios de Derecho y Ciencia Política*, 27, 67-78. Disponible en: http://tinyurl.com/yc45datv.

Bachmaier Winter, L. (2017). Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015. *Boletín del Ministerio de Justicia*, 81 (2195), 3-36. Disponible en http://tinyurl.com/mspfw3mn.

Bellovin, S. M., Hutchins, R. M., Jebara, T. y Zimmeck, S. (2014). When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning. *New York University Journal of Law & Liberty*, 8, 555-628. Disponible en: http://tinyurl.com/r9zeyhz2.

Burkle, M. y Cobo, C. (2018). Redefining Knowledge in the Digital Age. *Journal of New Approaches in Educational Research*, 7 (2), 84-85. Disponible en: http://tinyurl.com/jdaxfcx4.

Busquet, J., Peracaula I. y Uribe A. C. (2011). La fractura digital entre generaciones: conectados y desconectados en la nueva sociedad de la información. En *VI Congrés Internacional Comunicació i Realitat* (Barcelona, 2011) (pp. 33-41). Barcelona: Facultat de Comunicació Blanquerna – Universitat Ramón Llul, Trípodos Extra. Disponible en: http://tinyurl.com/mrfb3xff.

Cabezudo Rodríguez, N. (2016). Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. *Boletín del Ministerio de Justicia*, 70 (2186), 7-60. Disponible en http://tinyurl.com/4tkv5whf.

Carrillo, M. (2016). Los ámbitos del derecho a la intimidad en la sociedad de la comunicación. En *XX Jornadas de la Asociación de Letrados del Tribunal Constitucional. El derecho a la privacidad en un nuevo entorno tecnológico* (pp. 11-70). Madrid: Centro de Estudios Políticos y Constitucionales.

Elvira Perales, A. (2020). Derecho al secreto de las comunicaciones. En F. J. Matia Portilla y G. López de la Fuente (eds.). De la intimidad a la vida privada y familiar*: Un derecho en construcción* (pp. 115-140). Valencia: Tirant lo Blanch.

Espín López, I. (2021). Los derechos fundamentales a la vida privada afectados por la investigación tecnológica y el fenómeno del entorno virtual. *Boletín del Ministerio de Justicia*, 85 (2244), 8-67. Disponible en: http://tinyurl.com/mryuvesb.

Etxevarría, J. (1994). *Telépolis*. Barcelona: Destino.

Fernández Rodríguez, J. J. (2016). Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente. *Revista Española de Derecho Constitucional*, 108, 93-122. Disponible en: http://dx.doi.org/10.18042/cepc/redc.108.03.

Flores Vivar, J. M. (2019). Inteligencia artificial y periodismo: diluyendo el impacto de la desinformación y las noticias falsas a través de los bots. *Doxa Comunicación: revista interdisciplinar de estudios de comunicación y ciencias sociales*, 29, 197-212. Disponible en https://doi.org/10.31921/doxacom.n29a10.

Gómez Colomer, J. L. (2017). El proceso penal español a comienzos del siglo xxi. *InDret: Revista de para el análisis del derecho*, 1/2017, 3-59. Disponible en: http://tinyurl.com/2prnk83v.

González Cano, M. I. (2019). Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la directiva (UE) 2016/680. *Revista Brasileira de Direito Processual Penal*, 5 (3), 1331-1384. Disponible en: http://tinyurl.com/yp34bkc7.

Huete Nogueras, J. J. (2016). La regulación de las medidas de investigación tecnológica. Análisis de los aspectos referentes a la incorporación al proceso de datos electrónicos de tráfico o asociados. *Revista del Ministerio Fiscal*, 2 (2016), 59-75.

Jiménez Campo, J. (1987). La garantía constitucional del secreto de las comunicaciones. *Revista Española de Derecho Constitucional*, 20, 35-82.

Lasalle, J. M. (2021). Ciberleviatán. *Ethic*, 13-9-2021. Disponible en: http://tinyurl.com/3rk8byk4.

Lezertua Rodríguez, M. (1996). El derecho a la vida privada y familiar en la Jurisprudencia del TEDH. En J. J. López Ortega (dir.). *Perfiles del derecho constitucional a la vida privada y familiar* (pp. 49-98). Madrid: Consejo General del Poder Judicial.

López Guerra, L. (2018). El papel del juez en una sociedad democrática. *Revista de estudios jurídicos*, 18, 1-16. Disponible en: http://tinyurl.com/2sehzhpj.

López Ortega, J. J. (2017). La utilización de medios técnicos de observación y vigilancia en la LECrim (LO 13/15). En J. J. López Ortega, J. D. Salón Piedra y F. Valenzuela Ylizarbe (eds.). *El derecho a la intimidad: nuevos y viejos debates* (pp. 15-47). Madrid: Dykinson. Disponible en: http://tinyurl.com/bdh2pm2e.

López-Barajas Perea, I. (2016). Aplicación de las Tecnologías de la Información y de la Comunicación a la Investigación Criminal: la Reforma de la Ley de Enjuiciamiento Criminal Española de 2015. *Revista Iberoamericana de Sistemas, Cibernética e Informática*, 13 (2), 14-18. Disponible en: http://tinyurl.com/4fvx5ucz.

Lucas Murillo de la Cueva, P. (2008). El derecho a la autodeterminación informativa y la protección de datos personales. *Azpilcueta: cuadernos de derecho*, 20, 43-58.

Magro Servet, V. (2013). La medida de intervención telefónica en el nuevo Código Procesal Penal. Actuación del Juez de Garantías y de la Fiscalía. *Revista Derecho y Proceso Penal*, 31, 199-213.

Marchena Gómez, M. y González-Cuellar Serrano, N. (2015). La reforma de la Ley de Enjuiciamiento Criminal en 2015. Madrid: Ediciones Jurídicas Castillo de Luna.

McLuhan, M. y Powers, B. (1995). *La aldea global*. Barcelona: Gedisa.

Meyer, L. (2013). La sociedad de la distracción. *Ethic* [blog], 24-7-2023. Disponible en: http://tinyurl.com/2s4kb32y.

Moreno Catena, V. (2010). Garantía de los derechos fundamentales durante la investigación penal. En VV.AA. *Problemas actuales del proceso penal y derechos fundamentales* (pp. 13-54). Bilbao: Universidad de Deusto.

Nieva Fenoll, J. (2016). La recuperación de la privacidad de las comunicaciones. *Noticias jurídicas*, [blog] 25-5-2016. Disponible en: http://tinyurl.com/3j3uukhv.

Noya Ferreiro, L. (2018). *Derecho de defensa e intervención de las comunicaciones de los abogados*. Valencia: Tirant lo Blanch.

Ocón García, J. (2022). Constitución y secreto de las comunicaciones: desafíos tecnológicos para el derecho fundamental. Nuevos horizontes del Derecho Constitucional, 2, 86-104.

Ortiz Pradillo, J.C. (2013). *La investigación del delito en la era digital: los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*. Madrid: Fundación Alternativas, Estudios de progreso.

Ortiz Pradillo, J. C. (2020). Europa: auge y caída de las investigaciones penales basadas en la conservación de datos de comunicaciones electrónicas. *Revista General de Derecho Procesal*, 52, 1-28. Disponible en: http://tinyurl.com/mpv9v6ee.

Pérez de los Cobos Orihuel, F. (2018). *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho Comparado*. Estrasburgo: Parlamento Europeo.

Pérez Gil, J. (2018). Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución. En R. Brighi, M. Palmirani y M. E. Sánchez Jordán (eds.). *Informatica giuridica e informatica forense al servizio della società della*

conoscenzascritti in onore di Cesare Maioli (pp. 187-198). Roma: Aracne. Disponible en: http://tinyurl.com/5n7k6pzs.

Pérez Latre, F. J. (2015). La «tercera revolución digital»: Tecnologías con rostro humano y evaluación antropológica. *Revista de Comunicación*, 14, 100-113. Disponible en http://tinyurl.com/3wpvdet8.

Pesqueira Zamora, M. J. (2020). Diligencias de investigación, cesión de datos y principio de proporcionalidad. *InDret: Revista para el análisis del derecho*, 4, 419-445. Disponible en: http://tinyurl.com/2s49pf92.

Requejo Pagés, J. L. (2020). La protección de datos: en la encrucijada entre el Derecho de la Unión y la Constitución Española. En M. E. Casas Baamonde (coord.). *El derecho a la protección de datos de carácter personal en la sociedad digital* (pp. 21-38). Madrid: Fundación Ramón Areces.

Riesman, D., Glazer, N. y Denner R. (1989). *The Lonely Crowd: a study of the changing American character*. New York: The American Center Library.

Rodríguez-Yzquierdo Serrano, M. (2021). La extraterritorialidad en las comunicaciones digitales y las empresas tecnológicas ante el derecho a su secreto: reflexión en torno al caso Microsoft corp. vs. United States. *Asuntos Constitucionales*, 0, 131-139. Disponible en http://tinyurl.com/4cfdj34n.

Sanchís Crespo, C. (2017). Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas. La ley penal: revista de derecho penal, procesal y penitenciario, 125, 1-17. Disponible en http://tinyurl.com/4cfdj34ny.

Stuart., A., Bandara, A. y Levine, M. (2019). The Psychology of Privacy in the Digital Age. *Social and Personality Psychology Compass*, 13 (11), 1-14. Disponible en: http://tinyurl.com/mv867vza.

Suárez Robledano, J. M. (2011). Intervención de comunicaciones electrónicas. Foro: Revista de ciencias jurídicas y sociales, 14, 74-99. Disponible en: http://tinyurl.com/4st8pbsy.

Varona Jiménez, A. (2020). Aspectos relevantes de la interceptación de las comunicaciones telefónicas en el proceso penal español. *Ius Inkarri: Revista de la Facultad de Derecho y Ciencia Política*, 9, 159-172. Disponible en: http://tinyurl.com/mpc5k7tb.

Waltz, B. (2014). Privacy in the Digital Age, *Indiana Law Review*, 48 (205), 205-211. Disponible en http://tinyurl.com/3uzm6cb6.