



ARTÍCULO ESPECIAL

Las responsabilidades derivadas del uso de las tecnologías de la información y comunicación en el ejercicio de las profesiones sanitarias



Laura Muñoz Fernández^a, Elena Díaz García^b y Sergio Gallego Riestra^{a,*}

^a *Consejería de Salud del Principado de Asturias, Oviedo, España*

^b *Servicio de Salud del Principado de Asturias, Oviedo, España*

Recibido el 3 de marzo de 2020; aceptado el 5 de marzo de 2020

Disponibile en Internet el 9 de abril de 2020

PALABRAS CLAVE

TIC;
Tecnologías de la Información y Comunicación;
eSalud;
Responsabilidad profesional;
Telemedicina;
Interconsultas digitales;
Salud 2.0;
Protección de datos

Resumen La evolución de las tecnologías de la información y comunicación (en adelante TIC) en el ámbito sanitario ha dado lugar al fenómeno actual de la eHealth o eSalud, términos equivalentes al concepto de ciberespacio, pero referido exclusivamente a la salud. Fruto de la aparición de la web 2.0 se puede afirmar que nos encontramos ante un fenómeno mucho mayor que lo que sería el mero uso de tecnologías: estamos ante un verdadero cambio social dando lugar a la denominada Salud 2.0.

La regulación jurídica de este ciberespacio exige 2 tipos distintos de normas. Unas que regulen el ciberespacio en sí mismo y otras los hechos que se realizan con el uso del mismo y a las que parece aplicable el derecho convencional. En este último caso nos estamos refiriendo a la aplicación del derecho ya existente a los actos realizados a través de las TIC, como es el caso de los actos médicos.

Dentro de estos últimos también hay que distinguir 2 situaciones claramente diferentes: las responsabilidades profesionales derivadas de actos médicos ejecutados dentro del ejercicio profesional, llevado a cabo en el seno de las organizaciones sanitarias cuando se implanta el uso de las TIC y aquellos otros actos ejecutados de manera voluntaria y a título individual y privado, utilizando medios y dispositivos propios. Es en este tipo de actos donde la legalidad se ve generalmente conculcada respecto a la protección de datos y la intimidad de los pacientes, y a la vez los profesionales pueden incurrir en responsabilidades.

© 2020 Publicado por Elsevier España, S.L.U. en nombre de Asociación Española de Pediatría. Este es un artículo Open Access bajo la licencia CC BY-NC-ND (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

* Autor para correspondencia.

Correo electrónico: sergiomael.gallegoriestra@asturias.org (S. Gallego Riestra).

KEYWORDS

ICT;
Information and communication technologies;
eHealth;
Professional responsibility;
Telemedicine;
Digital consultations;
Health 2.0;
Data protection

The responsibilities arising from the use of information and communication technologies in health professional practice

Abstract The increasing use of Information and Communication Technologies (ICT) in the health setting has given rise to the current phenomenon of eHealth or eMedicine, terms equivalent to the cyberspace concept, but refer exclusively to health. Due to the appearance of Web 2.0 it can be stated that we are dealing with a phenomenon much greater than just using the technologies: we are facing a real social change, giving rise to that called Health 2.0.

The legal regulation of this cyberspace requires two different types of rules. Some that regulate cyberspace itself, and others, the actions performed with its use and to those that appear applicable to conventional law. In this latter case, we are referring to the applying of already existing laws to actions performed using ICT, as is the case of medical actions.

Within these latter situations, two clearly different ones have to be distinguished: the professional responsibilities arising from medical actions carried out within health organisation settings when the use of ICT is introduced, and those other actions carried out voluntarily, individually and privately, using personal media and devices. It is in these types of actions where the legality, as regards data protection and privacy of the patient, appears to be violated, and at the same time the professional may be held responsible.

© 2020 Published by Elsevier España, S.L.U. on behalf of Asociación Española de Pediatría. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Delimitación del marco en el que nos encontramos

La sociedad actual está viviendo un gran cambio ligado a las tecnologías de la información y las comunicaciones (TIC) propiciado por el aumento sostenido en las capacidades de computación, de almacenamiento general, de generación de contenidos y de velocidad en el intercambio de los mismos. El resultado es una auténtica transformación social: las TIC están cambiando la forma en que nos relacionamos, trabajamos o llenamos el espacio de ocio. Quizá el motor de cambio más potente ha sido la web 2.0 o web social, definida por Tim O'Reilly en 2005 como una plataforma extendida a todos los dispositivos conectados que actúa creando efectos de red a través de una arquitectura de participación. En contraposición a lo que entonces pasó a denominarse web 1.0, que estaba diseñada como un contenedor de información, la web 2.0 permite a los usuarios interactuar y colaborar entre sí, pasando de usuarios pasivos a usuarios activos con capacidad para participar, crear contenidos y dar soporte y formar parte de sociedades y/o comunidades a distintos niveles¹. Más que un cambio tecnológico supone un cambio en el enfoque de las aplicaciones tecnológicas tradicionales, que pasan a centrarse en el usuario. Esto es la conocida transformación digital, que implica la participación activa y voluntaria de sujetos, pero que a la vez conlleva la implicación pasiva, es decir, inducida, arrastrada, de otros sujetos que van desde personas físicas hasta organizaciones, asociaciones y estados².

En el ámbito sanitario, tras los inicios de la informatización en los años 70, hemos pasado de la informática médica a la eHealth o eSalud. La informática médica se limita a combinar la ciencia médica con varias disciplinas de las ciencias de la información y la computación, proporcionando metodologías por las que intenta contribuir a una mejor atención

al paciente. Sin embargo, la eHealth o eSalud va más allá, ya que supone el uso de las TIC para la salud en un sentido amplio, incluyendo entre sus dominios de aplicación los sistemas y herramientas para tratar a los pacientes, la investigación, la formación de los profesionales sanitarios, el seguimiento de enfermedades y la monitorización de la salud pública³, hasta llegar a lo que por similitud se ha venido a denominar salud 2.0, entendida como un nuevo enfoque de la sanidad aprovechando las oportunidades que ofrece la web 2.0.

En este nuevo paradigma los pacientes evolucionan hacia «tecnopacientes», «pacientes digitales», «pacientes empoderados» o incluso pacientes «impacientes»: se trata de pacientes con una actitud proactiva hacia su estado de salud y/o enfermedad, que buscan información a través de Internet y haciendo uso de las redes sociales, que demandan más información a los profesionales y que participan en la toma de decisiones que afectan a su estado de salud⁴.

Es indudable, por tanto, que la aparición de la web 2.0 ha supuesto un paso de gigante en cuanto al acceso a la información y libertad de expresión y la facilidad y fluidez de las comunicaciones interpersonales, pero también está fuera de toda duda que conlleva la aparición de unos importantísimos riesgos para los derechos relativos al honor, la intimidad personal y familiar, la propia imagen y la protección de datos, pero junto a ellos también aparecen riesgos más específicos derivados de la actividad concreta que se lleva a cabo, especialmente cuando es una actividad profesional como es el caso del ejercicio de la medicina. Ciertamente nos encontramos ante un fenómeno mucho mayor que lo que sería el mero uso de tecnologías: estamos ante un verdadero cambio social que incluye modelos de comportamiento que nos permiten dudar sobre la validez de los ordenamientos jurídicos actuales para solventar las nuevas situaciones que se producen, y nos llevan a tener que preguntarnos hasta qué punto

el derecho actual es directamente aplicable a las nuevas situaciones creadas.

El desarrollo de las TIC, conectando a las personas entre sí, ha dado lugar a lo que se conoce como ciberespacio. Es definido por Barrio Andrés como «el espacio global en el entorno de la sociedad de la información que consiste en el conjunto interdependiente de infraestructuras de TIC, y que incluye Internet, las redes de telecomunicaciones, los sistemas informáticos y los procesadores y controladores integrados propios del Internet de la cosas»⁵. La regulación jurídica de este ciberespacio supone un gran desafío para el derecho, y exigiría 2 tipos distintos de estructuras normativas. Por un lado es necesario regular el propio ciberespacio en sí mismo, como una realidad nueva que hasta ahora no ha sido objeto de normativización y una regulación de los hechos que se realizan con el uso del mismo, y a las que es aplicable el derecho convencional. En este último caso nos estamos refiriendo a la aplicación del derecho ya existente a los actos realizados a través de las TIC, pero que pueden tener consecuencias jurídicas al tratarse de actos delimitados espacial y temporalmente, como es el caso de los actos médicos efectuados, dentro del ciberespacio, pero en un territorio concreto y claramente definido y con sujetos perfectamente identificados.

La necesidad de dar seguridad jurídica al ciberespacio es puesta de manifiesto por la nueva normativa europea en materia de protección de datos⁶, cuando señala que su razón de ser es dar cobertura a una imprescindible libre circulación de los mismos. Pone de manifiesto que la evolución tecnológica y la globalización plantean nuevos retos para la protección de los datos personales al aumentar de forma significativa su recogida y su intercambio, y resalta que deben utilizarse formatos interoperables que permitan la portabilidad de los datos. Destaca que la tecnología permite que empresas y autoridades públicas utilicen datos personales en una escala sin precedentes, a la vez que las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial, siendo por ello necesario reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

Centrada la cuestión en estos términos, damos por sentado que la regulación del ciberespacio se irá produciendo paulatinamente y con una normativa nueva y especial. Respecto a la aplicación del derecho ya existente a los actos concretos y bien delimitados que se realizan en el ciberespacio, nos invita a distinguir 2 situaciones claramente diferentes en relación con el uso de las TIC: las responsabilidades profesionales derivadas de actos médicos ejecutados dentro del ejercicio profesional, llevado a cabo en el seno de las organizaciones, y aquellos otros actos ejecutados de manera voluntaria y a título individual y privado.

Las posibles responsabilidades derivadas de la implantación de las tecnologías de la información y la comunicación en el sistema sanitario

Ya hace muchos años que en el sistema público sanitario se han empezado a implementar formas de asistencia utilizando las TIC, dando lugar a distintas modalidades, entre las que merece citar la teleinterconsulta y el

telediagnóstico, cuya finalidad es la valoración de una enfermedad o el diagnóstico, previo intercambio de información entre profesionales incluyendo el uso de imágenes. En su seno se enmarcan la teledermatología, la telerradiología, la telecardiología o la teleoftalmología como procedimientos ya implantados en el sistema público sanitario bajo el auspicio y promoción del mismo. Tiene además la peculiaridad de que se llevan a cabo con medios proporcionados por la propia administración sanitaria, y tiene normas de funcionamiento instauradas.

Este conjunto de técnicas es habitualmente conocido ahora como telemedicina. La OMS la definió hace 20 años como «el suministro de servicios de atención sanitaria, en los que la distancia constituye un factor crítico, por profesionales que apelan a las tecnologías de la información y de la comunicación con objeto de intercambiar datos para hacer diagnósticos, preconizar tratamientos y prevenir enfermedades y heridas, así como para la formación permanente de los profesionales de atención a la salud y en actividades de investigación y evaluación, con el fin de mejorar la salud de las personas y de las comunidades en las que viven»⁷. Por su parte, la Asociación Médica Mundial, hace también 20 años, consideraba que la «telemedicina es la práctica de la medicina a distancia gracias a la cual las intervenciones, el diagnóstico, las recomendaciones y las decisiones terapéuticas se fundamentan en los datos clínicos, documentos y otras informaciones transmitidas por los sistemas de comunicación»⁸. La Asociación señalaba que la utilización de la telemedicina debe ser excepcional y circunscribirse nada más que a los casos en los que el médico no pueda, dentro de un retraso aceptable y en las condiciones de seguridad requeridas, estar presente físicamente, es decir, que no debe prescindirse, si es posible, de la relación de contacto físico y personal entre el médico y el paciente.

Vemos cómo la telemedicina es vista en sus comienzos exclusivamente ligada al hecho de permitir prestar asistencia salvando las distancias. Sin embargo, se ha ido ampliando su concepto aproximándose a la idea actual de globalización e interoperabilidad a la que antes hemos hecho referencia de la mano de la nueva normativa europea. El debate ético que suscitó la práctica de la telemedicina desde un principio fue analizar si solo tiene cabida cuando existe una situación de urgencia o distancia que imposibilita la asistencia directa, o si puede admitirse su ejercicio como una alternativa a la medicina convencional, y es evidente que esta es la línea por la que definitivamente se ha decantado, al permitir un mejor uso de recursos, claras ventajas en la gestión y una gran fiabilidad diagnóstica en determinados usos asistidos por inteligencia artificial.

El uso de la telemedicina, cualquiera que sea el ámbito en el que se desarrolle, tiene que estar sujeto a unas normas de mínimos. Sánchez Caro y Abellán⁹ enunciaron ya en 2002 cuáles eran los requisitos que deben darse para practicar la telemedicina evitando incurrir en responsabilidades (tabla 1). Resumidamente podemos concretarlos de la siguiente manera:

- 1) El uso de la telemedicina se legitima por el beneficio al paciente, pero nunca por la mayor comodidad exclusiva del médico.

Tabla 1 Requisitos para practicar telemedicina sin incurrir en responsabilidades

El uso de la telemedicina se legitima por el beneficio al paciente, pero nunca por la mayor comodidad exclusiva del médico. Se debe obtener el consentimiento del paciente y asegurar las normas de seguridad que garanticen su confidencialidad. Se deben conservar en la historia clínica todos los datos concernientes a cada caso garantizando la perennidad, seguridad y recuperación de la información. Los profesionales intervinientes deben estar autorizados para ejercer en el país en que estén establecidos y ser competentes en su especialidad médica.

- 2) Es preciso obtener el consentimiento del paciente, y con el fin de evitar los riesgos de fuga de información inherentes a las comunicaciones electrónicas deberá asegurarse la adopción de las normas de seguridad que garanticen la confidencialidad del paciente, en un doble sentido:
 - Los datos relativos al paciente y otras informaciones que le conciernen no pueden ser transmitidos a un médico o a otro profesional de la salud más que a petición del paciente, o con su consentimiento, y en la medida en que él determine.
 - Las informaciones que se transmitan deben referirse al problema médico concreto de que se trate.
- 3) Es relevante la conservación en la historia clínica de todos los aspectos concernientes a cada caso quedando debidamente documentados, tratando de garantizar la perennidad, así como su seguridad y la recuperación de la información.
- 4) Los profesionales intervinientes deben encontrarse autorizados para ejercer en el país en que se halle establecido y sea competente en su especialidad médica. Resulta curiosa esta previsión realizada hace casi 20 años por estos autores, cuando hoy día insistimos en la aplicación de un derecho territorial a los actos efectuados en el ciberespacio.

El Código de Deontología Médica de 2011 ha abordado la cuestión de la telemedicina amparando su uso y estableciendo unas consideraciones que podemos sistematizar en las siguientes reglas (artículo 26):

- El ejercicio clínico de la medicina mediante consultas exclusivamente por carta, teléfono, radio, prensa o Internet es contrario a las normas deontológicas. La actuación correcta implica ineludiblemente el contacto personal y directo entre el médico y el paciente.
- Es éticamente aceptable, en caso de una segunda opinión y de revisiones médicas, el uso del correo electrónico u otros medios de comunicación no presencial y de la telemedicina, siempre que sea clara la identificación mutua y se asegure la intimidad. Los sistemas de orientación de pacientes, mediante consulta telefónica o telemedicina, son acordes a la deontología médica cuando se usan exclusivamente como una ayuda en la toma de decisiones.
- Las reglas de confidencialidad, seguridad y secreto se aplicarán a la telemedicina en los mismos términos establecidos en el Código de Deontología para el ejercicio de la medicina convencional.

El ejercicio clínico de la medicina mediante consultas por medios virtuales exclusivamente es contrario a la deontología médica, pero estos medios sí pueden utilizarse como orientación o ayuda en la toma de decisiones.

Fruto de la progresiva implantación del uso de las redes sociales, la Organización Médica Colegial, en 2014, publicó un *Manual de estilo* dirigido a los profesionales sobre el uso de las redes sociales¹⁰. Basándose en el contenido del citado artículo 26 del Código de Deontología Médica elabora un capítulo II titulado *Consejo médico a pacientes virtuales* cuya lectura es francamente recomendable.

Todos los requisitos señalados constituyen normas de obligado cumplimiento que las organizaciones tendrán que garantizar para la implantación de programas de telemedicina, quedando la responsabilidad de los profesionales limitada al mero ejercicio profesional. Es evidente que ninguna responsabilidad podrá exigirse al médico por las violaciones de seguridad que pudieran producirse en materia de protección de datos, por la pérdida de información relevante o por errores en el proceso asistencial derivados directamente de las tecnologías utilizadas. Su responsabilidad quedaría reducida al estricto acto médico que lleve a cabo, sin diferenciación alguna de la derivada del ejercicio de la medicina convencional.

Las posibles responsabilidades derivadas del uso de las tecnologías de la información y la comunicación de manera voluntaria y a título individual y privado con medios ajenos al sistema sanitario

Paralelamente a la telemedicina implantada institucionalmente están apareciendo la teleasistencia y las consultas virtuales en las que la relación no es entre profesionales dentro de un sistema sanitario organizado y responsable de los dispositivos, sino entre paciente y profesional directamente, y se realiza generalmente con medios ajenos a los proporcionados por la empresa. Junto con ellos también coexisten actos de teleconsulta y telediagnóstico entre profesionales realizados por medios propios y fuera de los canales y medios establecidos por la organización sanitaria. Debe descartarse el uso de las redes sociales en abierto, pues no constituyen un medio adecuado para mantener una relación profesional, ya que no permiten una identificación correcta ni son entornos de confianza¹¹.

En primer lugar, ha de señalarse que el uso de dispositivos privados en los que se almacenan y transmiten datos de salud plantea serios problemas de legalidad, pero tan importante como lo anterior es dilucidar el alcance de este tipo

de actuaciones y las responsabilidades que podrían derivarse de ellas. La utilización de correos y sistemas tipo WhatsApp para intercambiar información relativa a pacientes, en la que hay datos de salud de personas identificadas o identificables, es una práctica ilegal que contraviene frontalmente lo establecido en la normativa de aplicación. Así, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal¹² (norma que continúa vigente), establece las medidas de seguridad que debe reunir este tipo de tratamientos, y en concreto determina que el almacenamiento de datos de salud en equipos informáticos exige unas medidas de nivel alto de seguridad. Entre ellas, se encuentra la obligación de realizar copias de respaldo, identificar cada acceso y mantener durante 2 años un registro de estos. Igualmente declara que deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado, y que la transmisión de datos de carácter personal de salud a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará necesariamente cifrando dichos datos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros, cosa que evidentemente no se realiza en los correos y whatsApps enviados en los supuestos a los que hacemos referencia.

Redes públicas son todas aquellas en las que un particular puede obtener sus servicios. Por el contrario son privadas las redes corporativas como la intranet del Ministerio de Sanidad y de los Servicios de Salud del SNS o la red corporativa de la Administración Pública española. Precisamente por eso los servicios de salud utilizan esas intranets privadas para el desarrollo de sus programas de telemedicina y las actividades que conllevan interoperabilidades, como es el caso de los proyectos a nivel nacional de receta electrónica y de historia clínica digital del Sistema Nacional de Salud. En resumen, el almacenamiento y la transmisión de datos de salud entre profesionales, fuera de estos sistemas, es decir, con teléfonos móviles, ordenadores privados, tabletas, etc., y a través de redes inalámbricas y públicas exige el uso de programas de encriptamiento y medidas de seguridad incumplibles en estos dispositivos.

Cuando el intercambio de datos personales de salud se lleva a cabo entre el propio paciente o sus representantes legales podría entenderse que hay un consentimiento del interesado. No estamos recurriendo a la figura del consentimiento tácito, sino manifiestamente expreso cuando es el paciente el que envía sus propios datos para obtener una orientación del profesional sobre sus problemas de salud. Queda desechada la posibilidad de que sea el profesional el que inicie este tipo de relación digital con el paciente y le envíe resultados de estudios o recomendaciones sobre su proceso patológico, lo que sería totalmente ilegal salvo que contase con un consentimiento expreso y así pudiera acreditarlo. Nos estamos refiriendo a la cada vez más extendida costumbre de mantener un contacto digital con pacientes crónicos para darles orientaciones a demanda sobre lo que deben hacer. En estos casos pudiera admitirse que no hay una infracción en materia de protección de datos, pero sin

embargo sí que se plantean serias dudas sobre la conveniencia de estas prácticas. Si a ellas aplicamos el derecho positivo vigente deberíamos empezar por cuestionarnos si este tipo de conductas están amparadas por la relación del profesional con su empleador, en este caso la Administración Sanitaria, cuando ni son conocidas ni autorizadas por él y se realizan en dispositivos privados y al margen de toda regulación. En otras palabras ¿estamos ante actos médicos?, ¿el seguro de responsabilidad civil de la Administración se haría cargo de la cobertura de un siniestro derivado de este tipo de relaciones digitales?, ¿debería abonarse con dinero público una indemnización de esta índole?, condenada la Administración como empleadora del profesional ¿debería esta llevar a cabo una acción de regreso o repetición contra el profesional? No parece que haya muchas respuestas alentadoras para los profesionales en este tipo de supuestos que se contestan por sí solos.

Conflicto de intereses

Los autores declaran no tener ningún conflicto de intereses.

Bibliografía

1. Web 2.0. Wikipedia [consultado Dic 2019]. Disponible en: https://es.wikipedia.org/wiki/Web_2.0.
2. Hoffman-Riem W. Big Data. Desafíos también para el derecho. Cuadernos Cívitas. 2018.
3. Monteagudo Peña JL. El marco del desarrollo de la e-salud en España. Área de investigación en telemedicina y sociedad de la información. Madrid: Instituto de Salud Carlos III; 2001.
4. Sánchez-Caro J, Abellán-García Sánchez F. El paciente (impaciente) del siglo XXI. En: Sánchez-Caro J, Abellán-García Sánchez F (Coords), editores. Avances en salud: aspectos científicos, clínicos, bioéticos y legales. Fundación Merck Salud; 2018. p. 219-34.
5. Barrio Andrés M. Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza en Internet. Valencia: Tiran lo Blanch; 2018.
6. Unión Europea. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Unión Europea L 119, 4 de mayo de 2016, pp. 1-88.
7. Plan de telemedicina del INSALUD. Área de estudios, documentación y coordinación normativa. Madrid; 2000.
8. Toma de posición de la Asociación Médica Mundial sobre las responsabilidades y las directrices éticas ligadas a la práctica de la telemedicina, adoptada por la 51 Asamblea, celebrada en Tel Aviv (Israel), en octubre de 1999. Actualidad del Derecho Sanitario. 2000;62:481-4.
9. Sánchez Caro J, Abellán F. Telemedicina y protección de datos sanitarios. Granada: Fundación Salud; 2000. p. 2002.
10. Organización Médica Colegial. Ética y Redes Sociales. Manual de estilo para médicos y estudiantes de medicina. Sobre el buen uso de las redes sociales. OMC. Consejo General de Colegios de Médicos de España [Consultado Ene 2020]. Disponible en: <https://www.cgcom.es/sites/default/files/u183/Manual%20Redes%20Sociales%20OMC.pdf>.

11. Bataller A, Cassasa A, de Carreras LL, Martínez M, Moro M, Pidevall I, et al. Recomendaciones sobre el uso de información médica y el ejercicio de la libertad de expresión en las redes sociales. Consejo de Colegios de Médicos de Cataluña [consultado Ene 2020]. Disponible en: <https://www.comb.cat/Upload/Documents/7778.PDF>.
12. España. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Boletín Oficial del Estado, 19 de enero de 2008, núm. 17. pp. 4103 a 4136 [consultado Ene 2020]. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2008-979&p=20120308&tn=1>.