Internet: la paz del camino

Mercedes Fuertes
Catedrática de Derecho Administrativo
Universidad de León

I

Internet nos ha cautivado. Nadie podía imaginar en su inicial presentación que las relaciones sociales cambiarían (y cambiarán) tanto. Que morder ese fruto abriría de tal manera los ojos y la curiosidad hacia un nuevo mundo. Que, aunque sigamos con ciertas pautas de comportamiento tradicionales -porque desgraciadamente, las personas persistimos en los mismos errores-, sin embargo, tratamos de estar "conectados". La mayor parte de nuestro tiempo nos desenvolvemos en medio de una maraña de redes, a través de Internet buscamos información porque pensamos que todo es "accesible"... Muchos aparatos ya disponen de un código de identificación (el denominado coloquialmente "Internet de los objetos") para facilitar datos específicos y tratar de mejorar su funcionamiento o la gestión de servicios. Las principales infraestructuras dependen de la administración que se realiza de modo telemático y, por ello, son objeto de una especial atención. Se las califica como "críticas" o "estratégicas" con el fin de evitar que una incidencia o su paralización genere, de manera automática, sucesivos problemas de abastecimiento, de interrupción de servicios esenciales y básicos, de prestaciones indispensables para la vida de los ciudadanos, de graves riesgos a la seguridad pública. Con muchas empresas la relación se entabla únicamente a través de Internet: sólo disponemos de facturas electrónicas; y muchos utensilios y cachivaches sólo funcionan si los hemos dado de alta en la correspondiente página web de la empresa. Sin acceso a Internet se empiezan a perder oportunidades... Incluso, hay quien cree que todo lo que es, lo es a través de Internet, y lo que no, simplemente no existe, materializando el Aleph de Jorge Luis Borges. Mucho como digo nos ha cambiado Internet, quizás llegue a impulsar transformaciones en los paradigmas sociales y hay quien se atreve a anunciar "ciberutopías"[1].

[1] Sin embargo, las actuales tendencias están poniendo en duda algunas ilusiones como han explicado Jonathan Zittrain, *The future of the Internet*, http://futureoftheinternet.org/; o Evgeny Morozov, "*El desengaño de Internet. Los mitos de la libertad en la red*", Ed. Destino, Barcelona, 2012

Es cierto que otros grandes descubrimientos condujeron a fabulosas reformas sociales, porque la historia de la humanidad se puede contar a través de las consecuencias que han ido aportando los nuevos inventos y hallazgos... Pero han sido cambios localizados en un ámbito, por muy amplio que sea, como es el caso del desarrollo económico con la electricidad o el régimen de los salarios a raíz del diferente modo de concebir el trabajo. Podría seguir con otros ejemplos y tendrá muchos más en la cabeza el lector. Si destaco la diferencia que supone Internet frente a otros inventos es porque está originando una transformación social en todos los ámbitos de la vida. En las redes hay ideas, la comunicación y la información se multiplica, acelerado todo en trepidante taquicardia. Es una nueva sociedad la que está inmersa en Internet. En otras palabras, más que destacar la trascendencia del propio hallazgo, Internet tiene relevancia como la inmensa palanca de cambio que es, porque nuevos descubrimientos se verán impulsados como nadie pudo imaginar precisamente a través de las redes.

Si la caída del Imperio Romano o el descubrimiento de América, según la más común historiografía, abrieron sendas puertas para bautizar nuevos periodos históricos de la humanidad, en mi modesto entender, la generalización de Internet nos ha hecho entrar en otra nueva era. Exigirá repensar las relaciones sociales y las instituciones jurídicas, desde los palotes elementales del sistema político hasta las construcciones legales más afinadas. No es que crea que, gracias a Internet, se alcanzará una utopía en la organización social. En absoluto. Pero sí considero que, con la generalización de Internet, no se desenvolverá de igual manera el sistema democrático, por la sencilla razón de que choca con la inmediatez de las comunicaciones las convocatorias electorales basadas en llenar unos pabellones deportivos, así como que los representantes elegidos se reúnan en asambleas legislativas sin mayor relación con sus votantes. Ni tampoco podrán tramitarse con los mismos pausados tiempos muchos procedimientos administrativos, con plazos que se cuentan por meses cuando la comunicación telemática permite una mayor agilidad. Y qué decir de los procesos judiciales cuyos tiempos ya se expresan en años. Del mismo modo que, sólo gracias a la información que las editoriales jurídicas facilitan a través de Internet, podemos estar actualizados ante la vorágine normativa y la multitud de instancias procesales que existen. Tampoco será igual la participación ciudadana en los planes o proyectos de obras, en la gestión municipal, en la prestación de los servicios públicos, en la petición de responsabilidades ante la trasparencia que debe promover la actuación pública; ni serán iguales los detallados pliegos de cláusulas administrativas, ni la selección de los contratistas, ni las obligaciones de los concesionarios públicos que podrán estar sujetos a mayor supervisión a través de las redes...

Mucho habrá que estudiar para repensar los instrumentos de una nueva era que abre en canal sus incógnitas ante nuestros ojos anhelantes. Se puede

saber mucho y, a la vez, es difícil conseguir que algo se olvide porque, cuando un dato accede a Internet, resulta compleja su desaparición.

Piénsese que estamos ante una red donde se prefieren los derechos de uso frente a la titularidad dominical que fue, no lo olvidemos, el motor de grandes cambios en otras épocas[2].

En fin, variados son los nuevos interrogantes y desde hace años los juristas estamos tratando de aprestar nuestros conocimientos[3]. Sin embargo, en este momento, quisiera llamar la atención sobre una preocupación general que se está extendiendo como una densa sombra entre los ciudadanos fascinados por la comunicación, por descubrir algunas de las inmensas posibilidades que genera Internet, pero que no están (estamos) especialmente iniciados en las cuestiones tecnológicas. A saber, la desprotección e inseguridad de la comunidad y de las relaciones en Internet.

No es necesario presenciar la tragedia de una guerra o vivir sometido a una dictadura para sentir que, desde Internet, proceden en la actualidad dolorosos zarpazos a la limitación de los derechos y libertades públicas. También en las sociedades democráticas y civilizadas, Internet ofrece una faz oscura al ser una potente herramienta para consumar muchos delitos. La lesión a los intereses personales y patrimoniales se multiplica por su rápida difusión.

En Internet hay censuras procedentes de algunos Gobiernos pero también actuaciones de nuevos "partisanos" o de grupos de justicieros anónimos; hay violaciones a la intimidad de nuestras conversaciones y mensajes; hay programas espías que persiguen cualquier comunicación; hay conscientes alteraciones de la comunicación originando lentitud y conexiones fallidas; hay

---

[2] No es este el momento para seguir el hilo de esos interesantes asuntos por los interrogantes jurídicos que suscitan, pero hay que advertir la trascendencia del problema sobre el "derecho al olvido" con varios cientos de recursos en la Audiencia Nacional, alguno de los cuales ha generado la presentación de cuestiones prejudiciales ante el Tribunal de Justicia de la Unión Europea; o la negativa de muchas empresas y servidores de Internet a reconocer que los bienes que adquieren los internautas son en concepto de propiedad, admitiendo sólo un derecho de uso que no se puede transmitir.

[3] Entre la ingente bibliografía que se publica es de justicia citar la temprana sistematización que ofreció Santiago Muñoz Machado con el libro *La regulación de la red. Poder y Derecho en Internet*, Ed. Taurus, Madrid, 2000, completada luego por otros muchos artículos como "La libertad y el poder en la gran telaraña mundial", en la obra dirigida por E. Gómez Reino *Telecomunicaciones, infraestructuras y libre competencia*, Ed. Tirant lo Blanch, 2004, págs. 55 y ss., o "La república del ciberespacio" en El Cronista, núm. 10, 2010, págs. 78 y ss. Decenas de trabajos se han publicado sobre aspectos jurídico públicos de Internet. Sirva la referencia al artículo de J.C. Laguna de Paz, "Internet: aspecto de su régimen jurídico-público", *REDA* núm. 113, págs. 5 y ss., así como a los que recoge ya una revista específica "Revista de Internet, Derecho y Política". Desde la perspectiva de las relaciones privadas, es también muy recomendable un ambicioso trabajo de más de mil páginas de Pedro Alberto de Miguel Asensio, *Derecho privado de Internet*, Ed. Civitas, Madrid, 4ª ed. 2011; en fin, es también aleccionadora la obra de Pablo García Mexía, *Derecho europeo de Internet*, Ed. Netbiblo, La Coruña, 2009.

virus informáticos más letales que las grandes pestes que en la Historia se han sucedido; hay “gusanos” y “troyanos” que se introducen en los ordenadores personales para pudrir o dañar mucha documentación; hay “registradores de teclas” que permiten conocer las contraseñas que utilizamos; hay ataques que convierten a los ordenadores en una especie de “zombis” y quedan bajo el control de otro para multiplicar las campañas de acoso; hay actuaciones sobre la información que instituciones, empresarios o personas publican a través de sus páginas web, los denominados “ataques de denegación de servicio”, que consiguen la parálisis e, incluso, cambian el contenido, o desvían la atención hacia otros lugares bien distintos; hay suplantaciones de la personalidad; hay campañas de desprestigio cuya rapidez se extiende pugnando con la velocidad de la luz; hay “ciberacosos” que terminan en desgraciadas tragedias; hay robo de datos personales y económicos, hay un mercado internacional de datos robados[4]...

Y el daño se multiplica porque el escenario es el inmenso universo de Internet y porque cada vez, como he adelantado, nuestras relaciones se desarrollan más a través de la red. Los servicios públicos y las infraestructuras dependen mucho más de Internet.

Pero si estos riesgos son preocupantes, la alternativa de que las “huellas” en Internet permitan la posibilidad de un gran conocedor y supervisor de las comunicaciones también aterra, porque reproduciría el “panopticón” de Jeremy Bentham o la novela “*1984*" de Georg Orwell. ¿Puede garantizarse el libre desarrollo de la personalidad en una sociedad permanentemente vigilada?

Es más, junto a los riesgos derivados de los comportamientos dentro de las redes, también existen riesgos sobre la propia estructura de Internet, ya que hay quien ataca a las redes, quiebra el sistema, su integridad y la seguridad general.

---

[4] Las historias que se trenzan en las novelas, como la participación de Lisbeth Salander en una agrupación de “hackers” que robaban y negociaban con tarjetas de crédito no están sólo en la mente creativa de los escritores. Muchas obras de documentación recogen ya los casos concretos, como la de Misha Glenny, “*El lado oscuro de la red. La nueva mafia del ciberespacio*”, Ediciones Destino, Barcelona, 2012; o el Informe de la empresa seguridad Trend Micro sobre el comercio clandestino del cibercrimen. Es más, en los últimos meses hemos presenciado una preocupante escalada de “ataques” como los padecidos por los grandes medios de comunicación americanos, según se afirma en el Informe Mandiant, a raíz de los reportajes sobre las ganancias multimillonarias de los parientes del primer ministro chino; ataques a determinadas infraestructurastras energéticas, aeronáuticas y tecnológicas norteamericanas singularizadas en su XII Plan Quinquenal; la sustracción de datos en Global Payment que afectó a varias entidades financieras y a las tarjetas de crédito vinculadas; también se ha considerado una agresión cibernética las grandes pérdidas de la bolsa de Nueva York a mediados de abril originadas a través de la difusión de manera consciente de una falsa noticia; del mismo modo Twitter reconoció que había sufrido un “sofisticado ataque” en más de 250.000 cuentas... lo que ha dado lugar a un impulso de la controvertida legislación sobre protección y compartición en ciberinteligencia, la Cyber Intelligence Sharing and Protection Act, que pretende que las empresas privadas compartan sus datos con el Gobierno para evitar “ciberataques”. Y es que incidiría en las reglas de privacidad entre las empresas y sus clientes.

Se me dirá que todas estas actuaciones son sólo fruto de nuestra naturaleza humana. De las debilidades y maldades que durante siglos van integrando nuestra representación en el gran teatro del mundo. Se me dirá que muchos de estos ataques han de ser reconducidos a las clásicas instituciones de protección jurídica. Y no niego que algunas de las técnicas que durante décadas han puesto en pie los juristas para proteger los derechos y libertades públicas, para exigir las responsabilidades civiles, administrativas o penales oportunas, puedan ayudar a contrarrestarlos.

Es cierto que se están haciendo grandes esfuerzos desde la doctrina para responder a los nuevos problemas que la tecnología introduce en las relaciones jurídicas. Se tipifican delitos ante los atentados a la integridad de los sistemas informáticos, se añaden otros de hurto de soportes digitales, de utilización fraudulenta de equipos, de falsificación informática, de intrusismo informático, etc...[5]. Sin embargo, estos instrumentos me parecen todavía insuficientes.

El Derecho está acostumbrado a sopesar los tiempos. Y es lógico. Cualquier análisis o decisión lleva su estudio. Las actuaciones procedimentales requieren también su tiempo, que normalmente se cuentan por días o por meses. Cuesta por ello reaccionar ante conductas que se propagan y multiplican en segundos. Y con una circunstancia agravante: aparentemente, no hay fronteras. El poder coercitivo de los Estados se detiene en el límite de su territorio y ha de conseguir la colaboración de otros Estados para perseguir los saltos tecnológicos entre servidores alojados en distintos países o, en la metáfora que se ha generalizado, de esa nebulosa o "nube" inaccesible para muchos y que tanta información acoge.

Tampoco la tradicional respuesta jurídica frente a los graves ilícitos penales, esto es, la pena de privación de libertad que puede conllevar la prohibición de acceso a Internet, parece la más adecuada para corregir el comportamiento de personas, quienes, en bastantes ocasiones, son agudos matemáticos e informáticos que no han perseguido el lucro personal sino el capricho de superar barreras o muros de seguridad informática[6].

---

[5] Son importantes los estudios criminológicos que se están difundiendo y relevante la obra que está surgiendo desde la doctrina penal para atender a los delitos informáticos. Entre la mucha bibliografía sobre estas cuestiones sirva la remisión a una de las obras más reciente que he consultado, el libro colectivo dirigido por José Luis de la Cuesta Arzamendi "*Derecho penal informático*", Civitas, Madrid, 2012.

[6] Cuando escribo este texto, la Comisión del Mercado de Telecomunicaciones ha publicado en su página web la noticia que le requería un juzgado de Huelva. Y es que se había impuesto como regla de comportamiento al condenado, con apoyo en el artículo 83 del Código Penal "*la cancelación de la contratación de cualquier contrato de acceso a internet, bien asociado a números de telefonía fija o móvil, durante el plazo de condena, incluidos los actualmente mantenidos por él hasta el momento*", de tal modo que era necesario dar a conocer a todas las empresas operadoras dicha prohibición.

Por ello, ante las ineficiencias que resultan de utilizar las técnicas tradicionales habría que reiniciar con más convicción el camino para conseguir una protección. Pero antes de señalar el horizonte futuro, quiero recordar las soluciones que nuestros antepasados consiguieron y es que bien anunció el rey Salomón: *nihil novum sub sole*. Un recuerdo que se remonta a más de mil años.

II

Mitos y leyendas se engastan con frecuencia para adornar el avance en la Historia de la humanidad. De manera especial, ante fechas singulares. Y así ocurre con el paso hacia el primer milenio. Mucho se ha fabulado sobre la época oscura, de temor y represión religiosa que le precedió, de amenaza de fin del mundo. Trazos que han permitido construir relatos y novelas, aunque los historiadores han rechazado esos cuentos explicando las fuentes de esos errores[7].

No obstante, tampoco extraña pensar en una sociedad con miedos y temores, pues éstos siempre han acompañado los cambios. Si hoy es el miedo al cambio climático o a un riesgo nuclear, en el pasado fue el miedo a un cometa[8]. De ahí que poco sorprenda imaginar a unas poblaciones inseguras, a quienes volvían de las Cruzadas, a quienes no vieron cómo el cielo se rompía, a ladrones en los caminos... Estudios minuciosos ofrecen datos ilustrativos, sin esas ensoñaciones míticas, sobre la inseguridad y la consiguiente revolución feudal.

Porque el desmoronamiento del Imperio Carolingio fue aprovechado en muchas zonas de las marcas por señores que discutían y rompían la fidelidad

---

[7] Sirva entre la mucha bibliografía existente el recuerdo de los trabajos de José Angel García de Cortázar y Ruiz de Aguirre, "El milenarismo del año mil: ¿mito o realidad escondida?" en la obra coordinada por Luis Antonio Ribot García, Ramón Villares Paz y Julio Valdeón Baruque, *Año mil, año dos mil : dos milenios en la Historia de España* Ed. SEENM, Madrid, Vol. 1, 2001, págs. 49 y ss.; y de Alicia Yllera Fernández, "Los supuestos "terrores" del año 1000 (Una visión tergiversada del mundo medieval)" en la obra coordinada por Doina Popa-Liseanu y María Rosario Ozaeta Gálvez *Palabras y recuerdos : homenaje a Rosa María Calvet Lora* Ed. APFF, Madrid, 2004, págs. 227 y ss.; así como los libros de Robert Lacey y Danny Danzinger, "*El año 1000: formas de vida y temores ante el cambio de milenio*", Ed. Ediciones B, Barcelona, 1999; o, en fin, el libro de Edmond Pognon, "*La vida cotidiana en el año 1000*", Ed. Temas de hoy, Madrid, 1994.

[8] Sobre los paralelismos en los cambios de milenio, George Duby, "*El año mil*" Gedisa, Barcelona, 1988.

al rey y que querían consolidar su señorío[9]. En la práctica esas manifestaciones de poder generaban también la ocupación de fincas de los agricultores, la recolección de sus frutos, la reclamación de derechos sobre sus cosechas y, cómo no, constantes luchas entre los señores feudales por tratar de imponerse. Época de gran violencia y de venganza, de muchas zozobras ante los abusos de poder en esas zonas fronterizas que se extendían entre el Imperio carolingio y el espacio musulmán.

En medio de ese violento ambiente, la paz de un monasterio acoge en el año 1027 el Sínodo de Toulouges. Allí, se atribuye al renombrado abad benedictino Oliba, que iba de peregrinación, la proclamación de la primera "tregua de Dios", esto es, la obligación de que durante unos días, primero de sábado a lunes y, luego, desde el miércoles al lunes, no hubiera agresiones, ni se practicara la violencia, ni ataque bélico alguno contra personas ni bienes. Declaración de "paz y tregua" que también proclama ese mismo abad ya siendo obispo de Vich en esa diócesis en 1033 y que se reitera de manera sucesiva en los territorios colindantes extendiéndose por muchas zonas de la Marca[10]. "Paz y tregua" que se imponía para proteger a los clérigos y monjes. Declaraciones de paz "especial" que rápidamente se propagaron enarbolando a quienes la transgredieran la pena de excomunión.

La paz se respetaba, en principio, ante los temores de quedar apartado, repudiado. Pero, es más, se imprime un mayor carácter, una mayor fuerza y eficacia a esas declaraciones porque en las asambleas que se celebran se presentan los señores feudales. La asistencia de estos señores, que permite trenzar relaciones entre la Iglesia y el poder civil, constituyó una de las principales causas del fortalecimiento de régimen feudal.

Paz para los monasterios, paz para las iglesias y su entorno, los *sacraria*, paz para quienes se acerquen a lugares de culto, paz para los peregrinos y, también, paz para las ferias y mercados...Y para conseguir llegar en paz, que se desenvolviera el comercio y que se nutrieran las arcas feudales, surge la paz del camino[11]. Porque es en el camino donde se necesita más sosiego, seguridad y paz.

Con razón ha resaltado la doctrina que esta paz del camino supuso una importante novedad. Hasta entonces las declaraciones se dirigían, como he

---

[9] Sobre la consolidación del régimen feudal catalán son bien clarificadoras las explicaciones de Luis García de Valdeavellano, "*Curso de historia de las instituciones españolas. De los orígenes al final de la Edad media*", Alianza Editorial, Madrid, 1982, en especial, págs. 394 y ss.

[10] Por todos, Guilllem María de Brocà, "*Historia del Derecho de Cataluña*", Barcelona, reedición 1985.

[11] Rafael Gibert y Sánchez de la Vega, "La paz del camino en el derecho medieval español", en *Anuario de historia del Derecho español*, núms. 27-28, 1957-1958, págs. 831 y ss.

recordado, a proteger a determinadas personas, normalmente a los clérigos, o a los lugares donde se encontraban (monasterios o mercados). De manera similar, los "conductus" se entregaban a quienes se dirigían a la Corte, a los peregrinos, a los extranjeros, a los mercaderes... Frente a esas declaraciones personales, la paz del camino suponía una protección objetiva. Se atendía a los propios senderos, a las veredas y vías de comunicación, a esos serpenteantes y largos trayectos. Es el suelo que espera los pasos el objeto específico de consideración. Un singular avance en el pensamiento jurídico medieval aunque, como todo, también tenga sus antecedentes en el derecho anterior[12].

Son los *Usatges*, esas usanzas y costumbres que van asentando el terreno del Derecho, los que acogen las primeras previsiones. De textos del siglo XI recuerdan los historiadores la siguiente cita:

> "Los caminos y vías, por tierra y por mar, son de la potestad y para su defensa deben estar en paz y tregua todos los días y todas las noches, de modo que todos los hombres, tanto caballeros como peones, tanto mercaderes como negociantes, por ellos, yendo y viniendo, vayan y vuelvan seguros y tranquilos, sin ningún miedo, con todas sus cosas y si alguno les atacara, matara, hiriera o deshonrara en algo o les quitare algo de sus cosas, el mal o deshonor que les hizo en su cuerpo se lo enmende en el doble, según su valor, y lo que les quitares se lo restituya multiplicado por once..."

A partir de ahí se reiteran y extienden estas previsiones en muchos fueros medievales[13]. Por ejemplo, en las Constituciones de Aragón de 1188, donde perdía "el amor del rey" quien robara en camino público; o en el Fuero de Huesca, donde se insiste en la obligación de todos los súbditos a la hora de ayudar al monarca a guardar los caminos. Muchos son los fueros que reiteran la protección y las penas. En el Fuero Real se afirma que los romeros,

> "cualesquiera que sean y de donde quiera que vengan, y especialmente los que vinieran a Santiago, tengan por todo el Reino el privilegio de que ellos y los que les acompañan, juntamente con todas las cosas de

---

[12] Sin detenernos en las explicaciones que ofrecen los historiadores, siempre tan atractivas, sí hay que recordar que esa paz del camino encuentra sus antecedentes en el Derecho romano, donde también se obligaba a mantener la seguridad de los caminos. Desde la tradición de atribuir a Rómulo el trazado con el arado de los terrenos sagrados, el Derecho romano insiste en que hay bienes inviolables, como las murallas, así como bienes públicos como las vías romanas. Vías cuya trascendencia se incrementa porque garantizan el poder y la seguridad del Imperio, de ahí que estuvieran protegidas por el ejército a través de sucesivos puestos de vigilancia. Estas y otras interesantes precisiones relata César Rascón en su *Manual de Derecho Romano*, Tecnos, Madrid, 2000. Obligada es también la cita por el análisis de los textos de la obra de Gonzálo Menéndez Pidal, "*Los caminos en la historia de España*", Madrid, 1951.

[13] Por todos el citado trabajo de Rafael Gibert. También resulta muy aleccionador el artículo de Agustín Sánchez Rey "Los caminos en las leyes y en los fueros medievales españoles", *Revista de obras públicas*, núm. 3777, 2007, págs. 51 y ss.

> su propiedad, vayan, vengan y estén en seguridad en los caminos, sean albergados sin obstáculo, etc".

En fin, en estos textos se recogen las penas, las caloñas, que se impondrán a quienes quebranten la paz, a los salteadores y ladrones; así como la muerte para aquellos que también mataren[14]. Similares previsiones se adoptaron y se fueron extendiendo en otros reinos europeos como ha estudiado la doctrina[15].

Y es que el tránsito exige seguridad. Puede decirse que alrededor de esa paz del camino creció la comunicación y, con ello, el Derecho: porque había que mantener y cuidar los caminos, porque surgieron privilegios de portazgo, porque había que dar sentido a las cosas pérdidas en el camino; porque los caminos permitían alcanzar los pueblos y ciudades que crecieron, multiplicaron las relaciones y los negocios y con ello el pensamiento que se extendió, abatió prejuicios y limpió miradas...

Tal es la importancia de la paz del camino y esa paz es la que ahora, mil años después, ha de reconquistarse para los caminos virtuales, para las redes, para las comunicaciones y servicios de Internet.

III

Hoy día no contamos todavía con un abad Oliba que formule una tregua y mucho menos cabe pensar en que fuera respetada en todo el mundo porque han desaparecido los temores a las penas de excomunión. Es cierto que científicos, como los grandes impulsores de Internet y de la web, y otros muchos, siguen trabajando para conseguir unas comunicaciones seguras manteniendo su esencia, porque la web nació libre y abierta y así debe mantenerse [16]. De ahí la complejidad para que la técnica y los instrumentos jurídicos conocidos garanticen la seguridad de la red y de sus comunicaciones.

---

[14] Para los curiosos ofrece Rafael Gibert algunos ejemplos: los sesenta sueldos del Fuero de Salamanca, los mil del Derecho navarro o los seiscientos mrs. del Ordenamiento de Alcalá, págs 847 y ss.

[15] Me remito a las lecciones sobre el feudalismo alemán ofrecidas por Uwe Wechsel, *Geschichte des Rechts in Europa*, C.H. Beck, München, 2010, en especial, págs. 146 y ss.; o las de Ulrich Eisenhardt, *Deutsche Rechtsgeschichte* , C.H. Beck, München, 3ª ed., 1999, págs. 37 y ss.

[16] La explicación de esta filosofía sobre la estructura de la web la formula Tim Berners-Lee en su libro *Weaving the Web*, Ed. HarperBusiness, 2000. Son varios los proyectos que dirige Tim Berners-Lee para fomentar la seguridad de Internet, como la denominada "web platorm documents" que, siguiendo con el recordatorio del ambiente medieval, recuerda a un antiguo monasterio, centro de la cultura y documentación, porque esta web pretender reunir toda la documentación existente sobre los estándares para que los profesionales cuenten con una fuente fiable y abierta. Otro investigador, Alexis Ohanian, promueve "Internet defense league" para garantizar la libertad de Internet; y así se podría seguir con la referencia a otros interesantes proyectos de investigación.

Carecemos igualmente de una Declaración general sobre el régimen de Internet, sus derechos y obligaciones. Y no ha sido por falta de intentos. Dejando a un lado las iniciativas individuales que han pretendido declarar la independencia de Internet[17], algunas instituciones políticas han impulsado la aprobación de Declaraciones de derechos. Así, una Comisión del Senado español aprobó una moción para formular una Declaración de derechos de Internet en diciembre de 1999. Junto a los derechos básicos, se insistía también en la necesidad de garantizar la seguridad de las infraestructuras y la seguridad de las comunicaciones, protegiendo la intimidad, la reputación, a los menores... Con posterioridad, durante la Presidencia española de la Unión europea en el primer semestre de 2010, se promovió la elaboración de una Carta de Derechos de Internet para declarar el derecho de acceso a la red, la libertad de expresión, la protección a la intimidad y a la reputación, la protección de los derechos de autor, las garantías judiciales ante las técnicas de control, etc. Finalmente no se aprobó, quizá quedó enredada en algún trámite dentro de las reuniones y comisiones de las instituciones europeas. No obstante, el Parlamento europeo sí aprobó un Informe en junio de 2010 sobre la "gobernanza de Internet" en el que resalta la necesaria protección de los derechos fundamentales y de las libertades públicas en este ámbito.

Estamos faltos, por tanto, de ese primer marco específico, ese primer paso que ya después de tantos siglos los juristas utilizamos para iniciar la sistematización de una regulación general.

Sí se está avanzando, por el contrario, en protecciones específicas del mismo modo que, en los inicios del milenio, se posaba la mirada sobre los monjes o algunos lugares. Caso paradigmático es la protección a las infraestructuras "críticas", lugares que podrían considerarse como los *sacraria* medievales[18]; así como la posibilidad de que algunas comunicaciones se desenvuelvan totalmente encriptadas (como si contaran con un salvoconducto especial, volviendo a la analogía con la época medieval) o se mantengan en redes internas o reservadas. Algunos especialistas aseguran que estas opciones no se pueden generalizar a toda la comunicación a través de Internet porque, para mantener una eficaz gestión de las redes, parece necesario que algunas de las capas en las que se estructuran las comunicaciones no estén encriptadas. Las

---

[17] Recogen Tim Wu y Jack Goldsmith en su libro *Who controls the Internet?*, Oxford University Press, 2006, las iniciativas de algunos activistas digitales que han promovido esas declaraciones de independencia y declaraciones de derechos, págs. 20 y ss.

[18] En concreto, la Directiva 2008/114, de 8 de diciembre, regula la identificación y designación de las infraestructuras críticas europeas, así como la evaluación dirigida a mejorar su protección. En España se incorporaron esas previsiones a través de la Ley 8/2011, de 28 de abril, de medidas para la protección de infraestructuras críticas que, esencialmente, organizada el Centro nacional de protección y establece las líneas básicas de los planes estratégicos, de seguridad, de protección y de apoyo. Desarrolla esta ley el Real Decreto de 20 de mayo de 2011, así como varios planes de seguridad que se han aprobado.

empresas de telecomunicaciones que facilitan el servicio de acceso a Internet insisten en esta idea para favorecer un mejor control de los virus, desechar los mensajes basura y proteger una comunicación eficaz[19].

Además, se han dado más pasos en la precisión de los delitos informáticos. Un relevante avance se consiguió a partir del Convenio del Consejo de Europa sobre cibercriminalidad que se suscribió en Budapest el 23 de noviembre de 2001. Ratificado e incorporado a la legislación de la mayoría de los países europeos ha servido, además, de modelo a otros muchos Estados en Hispanoamérica y en otras latitudes. Se trata de un texto que trata de armonizar la tipificación de algunos delitos informáticos, como los relativos a la confidencialidad, la protección de datos, la lucha contra la pornografía infantil, la persecución de las falsificaciones y estafas. Con posterioridad se incluyó la incriminación de actos de naturaleza racista y xenófoba. Desde un punto de vista procesal, el Convenio fomenta la ayuda y la cooperación internacional, ya que resulta indispensable superar la situación paradójica de contar con un Ordenamiento y unas policías fragmentadas por las fronteras y los efectos mundiales del acceso y comunicación de Internet. No obstante, los especialistas insisten en que resulta algo escaso este texto ante la convulsa evolución de muchas prácticas nocivas[20]. De ahí que se promuevan foros para analizar el avance de los riesgos a través de Internet[21].

Todos estos problemas tienen ciertamente un alcance mundial, de ahí la importancia de informes como el publicado en febrero de 2013 por las Naciones Unidas *Comprenhensive study on cybercrime* o el denominado *Manual de Tallín*[22]. Sin embargo, por el momento, los instrumentos jurídicos

---

[19] Sin embargo, últimas noticias dan cuenta de nuevos sistemas que permite encriptar todas las comunicaciones, que no deja huella y que borra las claves. Así, por ejemplo, el sistema "Silent Circle", última creación de Phil Zimmermann, uno de los mayores especialistas mundiales en computación y cifrado. Es esta una cuestión compleja, objeto de otra investigación, y que deben partir de las pautas señaladas por la Comisión federal de telecomunicaciones de los Estados Unidos ("*Preserving the open Internet. Broadband industry practices*"), así como de las ideas recogidas por la Comisión europea tras la consulta pública titulada "*Internet abierta y neutralidad de la red*".

[20] Para más conocimiento del contenido y efectos del Convenio puede leerse el trabajo de Norberto J. de la Mata y Ana I. Pérez Machío, "La normativa internacional para la lucha contra la cibercriminalidad como referente a la regulación penal española" en *Derecho penal informático*, cit, págs. 123 y ss, así como a la bibliografía más específica que estos autores citan.

[21] Un ejemplo, en Gran Bretaña el Britain's Crown Prosecution Service (CPS) -departamento responsable de la acción pública de personas acusadas de delitos penales en Inglaterra y Gales - ha invitado a académicos, abogados, blogueros y a la policía a participar en una discusión de un mes de duración. Este servicio está manteniendo conversaciones sobre las leyes que afectan a los medios sociales con el objetivo de publicar unas normas, después de varios casos sobre comentarios escandalosos y subversivos en Twitter y Facebook.

[22] En concreto, a propuesta de la OTAN técnicos expertos han redactado este Manual *(Tallinn Manual on the International Law Applicable to Cyber Warfare*) en el que se ofrecen directrices de

derivan de la concreta actuación de los Estados y los avances se están advirtiendo en la normativa interna[23].

En nuestro ámbito, hay que saber que las instituciones de la Unión europea se han ocupado de varios problemas específicos que suscita la seguridad de Internet. Primero en la normativa sobre comercio electrónico. Una vez más, se presenta el "mercado" como el impulsor de la armonización europea; después, ya se han empezado a atender aspectos más específicos como son la protección de datos o la pornografía infantil[24]. Y, finalmente, se ha adoptado una Decisión con el objetivo de promover la colaboración entre los Estados para perseguir los accesos e intromisiones ilegales en los sistemas informáticos. Se trata de la Decisión 2005/222, de 24 de febrero. Sin embargo, sus previsiones son realmente escuetas y limitadas. Y es que propone que la legislación de los Estados persigan las intromisiones ilegales en los sistemas de información o en los datos, así como el acceso ilegal a los sistemas; que haya sanciones; que se consideren las circunstancias atenuantes y agravantes; y que se colabore entre los Estados facilitando información. No incorpora, por tanto, mecanismos efectivos para la persecución de los delitos informáticos y, es más, no alude a otras peligrosas situaciones que habían sido ya destacadas por el Consejo de Europa hace años.

También en las directrices de telecomunicaciones, en concreto la Directiva que establece el marco regulador común, se ha insistido en la necesaria cooperación de las autoridades nacionales para garantizar la integridad y la seguridad de las redes[25]. Se ha creado un centro de conocimiento

---

actuación amparadas en normas de Derecho internacional, como la Declaración de San Petersburgo de 1868 o la Convención de Ginebra de 1949, para hacer frente a las amenazas y ataques sobre Internet. Sobre el mismo puede verse M.N. Schmitt, en "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", 54 Harvard International Law Journal Online 13 (2012), http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/.

[23] Resulta muy recomendable la lectura de las explicaciones de Tim Wu y Jack Goldsmith en el libro ya citado *Who controls the Internet?*, para advertir cómo deben volverse la mirada a los poderes de los Estados para mantener la seguridad en Internet.

[24] En concreto en la Directiva 2000/31, de 8 de junio sobre determinados servicios de la sociedad de la información y el comercio electrónico; la Directiva 2002/58, de 12 de julio, relativa al tratamiento de datos y a la protección de la intimidad en el ámbito de las comunicaciones electrónicas; la Directiva 2006/24, de 15 de marzo, sobre conservación de datos generados o tratados en la prestación de servicios de comunicaciones electrónicas; la Decisión 2000/375, de 29 de mayo, de lucha contra la pornografía infantil en Internet.

[25] Me refiero a la Directiva 2002/21/CE, marco regulador común de las redes y servicios de comunicación electrónica («Directiva marco»), que es completada por la Directiva 2002/19, de acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión; por la Directiva 2002/20, de autorización de redes y servicios de comunicaciones electrónicas; por la Directiva 2002/22, de servicio universal y derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (estas cuatro tienen fecha 7 de marzo); y por la Directiva 2002/58, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las

especializado, una nueva "agencia europea", con el fin de que asista a las instituciones comunitarias en garantizar la seguridad de la red a partir de recabar datos, información y analizarla[26]. Un nuevo organismo, de carácter asistencial, y que trata de encontrar su sitio en un tejido ya suficientemente poblado de autoridades, reguladores y otros entes. No olvidemos que también en la malla que va conformando el complejo Derecho comunitario europeo está ya trenzado otro bien relevante, el denominado Organismo de los reguladores europeos de las comunicaciones electrónicas que acoge a las autoridades nacionales competentes en materia de telecomunicaciones y cuyas funciones se dirigen de manera preferente a analizar los mercados, promover la armonización legislativa de este sector y resolver conflictos transfronterizos[27].

En estos momentos se está discutiendo la posible ampliación de las funciones de esta Agencia europea de seguridad. Tras varias consultas, conferencias y debates, se ha presentado una propuesta de reforma de su regulación para incorporar la protección de la intimidad y a las autoridades encargadas de aplicar la ley. Sin embargo, todavía quedan fuera otros importantes aspectos como la respuesta a los incidentes, la lucha contra los ataques en Internet o el apoyo a las autoridades policiales y judiciales. Quizás se progrese en estos aspectos con el nuevo Centro europeo de delincuencia informática que se acaba de crear en abril de 2013 en la Oficina Europea de Policía (Europol). En todo caso, falta mucho por avanzar, a mi juicio, si realmente desde las

---

comunicaciones electrónicas. Sobre las mismas puede verse la obra colectiva *La nueva regulación de las telecomunicaciones, la televisión e Internet*, dir. José Manuel Villar Uríbarri, Ed. Aranzadi, Pamplona, 2003. Con posterioridad se han introducido importantes modificaciones en estos textos a raíz del denominado "paquete Telecom", esto es, las Directivas núms. 136 y 140, de 25 de noviembre, que han incorporado modificaciones en todas las del año 2002. Resulta interesante el análisis que realiza P.M. Arenas Naos, en "La reforma del marco europeo de las comunicaciones electrónicas", Noticias de la Unión Europea, núm. 313, febrero 2011, págs. 97 y ss.; así como el libro de Luis González de la Garza *El nuevo marco jurídico de las telecomunicaciones en Europa*, Ed. La Ley, Madrid, 2011.

[26] Esta nueva agencia se creó mediante el Reglamento 460/2004, de 10 de marzo, inicialmente por cinco años (redacción originaria del artículo 27). Sucesivas modificaciones de este texto han prorrogado su vida, primero ocho años (Reglamento 1007/2008), luego nueve años y seis meses (Reglamento 580/2011, de 8 de junio) y ahora hay sobre la mesa de las instituciones europeas muy avanzada otra reforma para ampliar de nuevo el plazo. Por el momento está alojada en la mítica Creta, el "primer eslabón de Europa" como repetía el arqueólogo Evans. Sin embargo, hay fuertes tensiones para que se traslade al Bruselas. Un imán centralista que entiendo poco y mucho menos en el ámbito de las redes de telecomunicaciones porque, por su propia configuración se estructuran sin un polo central y porque las telecomunicaciones no exigen la presencia física.

[27] Reglamento 1211/2009, de 25 de noviembre de 2009, por el que se establece el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas y la Oficina (sic), que también es otro organismo comunitario, con personalidad jurídica propia y cuya función es asistir al anterior. Este Organismo sustituyó a su precedente el "Grupo de entidades reguladoras europeas de las redes y los servicios de comunicaciones electrónicas" que se había creado mediante la Decisión 2002/627, de 29 de julio.

instituciones comunitarias se quieren proteger las redes y las comunicaciones[28].

Los pasos son más visibles en los países miembros donde existen otros muchos organismos cuyas competencias inciden en la seguridad de Internet, como ocurre con las agencias que velan por la protección de datos. Pero, sobre todo, proliferan otros para atender de manera ya general a los problemas de la seguridad en las redes. Tal es el caso en España del Instituto nacional de tecnologías de la comunicación (Inteco). Con forma de sociedad unipersonal se creó por la entidad pública empresarial Red.es, como consecuencia de la encomienda de gestión que le atribuyó la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información (Convenio de colaboración suscrito el día 20 de mayo de 2005). Entre las actuaciones propias de esta nueva entidad se destaca el impulso de proyectos para mejorar la calidad democrática, la participación ciudadana y, con relación a lo que ahora más me interesa, establecer los criterios básicos para coordinar las iniciativas públicas sobre seguridad informática[29].
Junto a este relevante organismo público, ha sido la aprobación de la Ley de acceso electrónico de los ciudadanos a los servicios públicos la disposición que ha puesto en marcha el mecanismo para establecer un sistema de seguridad, al menos en las comunicaciones de las Administraciones públicas. Pues esta Ley anunció la elaboración y aprobación de un "esquema nacional de seguridad" en el que deben establecerse unos principios y requisitos mínimos de seguridad para que la protección de la comunicación telemática sea adecuada (art. 42.2)[30]. Siguiendo con el símil medieval, podemos contar ya con unas "reglas monásticas", para las Administraciones públicas, para sus funcionarios, que fijan las normas mínimas de comportamiento y un voto similar al silencio, como es el de la información reservada o confidencial que estas

[28] Desde su creación, la Comisión europea ha promovido varios debates sobre la seguridad en Internet. Una consulta pública sobre los objetivos de seguridad, en noviembre de 2008, que concluyó con un informe "Towards a strengthened network and information security policy in Europe". Con posterioridad se han publicado una Comunicación sobre protección de infraestructuras críticas de información (COM 2009, núm. 149, de 30 de marzo); y también se menciona la trascendencia de la seguridad en la Agenda digital europea (COM 2010, núm. 245, de 19 de mayo).

[29] Otros convenios han ampliado sus funciones, como el que se suscribió el 27 de diciembre de 2005 para realizar determinadas actividades de fomento de la sociedad de la información; o el suscrito con el Ministerio de Interior para desarrollar instrumentos y colaborar con las Fuerzas y Cuerpos de Seguridad del Estado en la prevención, investigación y persecución de los ciberdelitos (octubre de 2012).

[30] Se ofrecen un completo análisis sistemático de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en la obra colectiva bajo la dirección de Eduardo Gamero y Julián Valero *La Ley de Administración electrónica*, Aranzadi, Pamplona, 2009, 2ª ed.

normas también preservan. Reglas que se inspiran en las tradicionales previsiones de seguridad[31].

El esquema nacional de seguridad se ha aprobado mediante el Real Decreto 3/2010, de 8 de enero, con el fin de establecer los instrumentos adecuados para que las redes y los sistemas de información que utilizan las Administraciones públicas relativos al ejercicio de derechos por los ciudadanos, el cumplimiento de sus deberes por medios electrónicos, así como el acceso a la información y procedimiento administrativo electrónico. En estos casos, el sistema debe ofrecer la suficiente confianza a los ciudadanos, resistir acciones ilícitas y garantizar la confidencialidad y la autenticidad de las comunicaciones. Unos loables objetivos que vuelven a traernos los ecos medievales de la tregua de dios porque se pretende que las redes de las Administraciones y las comunicaciones que realicen sean seguras. Se quiere la tregua en las relaciones con el poder público. Y es posible que en estas comunicaciones la paz se consiga porque se busca prevenir los ataques (art. 7), se establecen líneas de defensa (art. 8), se precisan los instrumentos de seguridad (arts. 11 y ss.), se fijan controles de acceso (art. 16) y mecanismos para proteger las instalaciones (art. 17). Además, el Centro criptológico nacional difundirá guías (art. 29), se auditarán los sistemas de seguridad (art. 35), y habrá respuestas ante los incidentes y problemas (arts. 36 y ss.). En fin, se formará a los funcionarios y personal que trabaja para las Administraciones públicas para que "*ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad*" (art. 5 y disposición adicional primera).

Es cierto que el plazo establecido para conseguir la adecuación de los sistemas de seguridad se fijó en doce meses desde la entrada en vigor del reglamento -como es práctica viciosa, el día siguiente de su publicación en el Boletín oficial del Estado-, pero, al mismo tiempo, se reconocía que la existencia de circunstancias que impidieran su aplicación, sin mayores precisiones, permitía extender el periodo de adaptación hasta los cuarenta y ocho meses desde la entrada en vigor. ¡Dilatado plazo que nos lleva a esperar hasta enero de 2014!

Podríamos decir que, del mismo modo que el Sínodo de Toulouges sirvió para instaurar la tregua de dios, este esquema nacional de seguridad permitirá con sus reglas garantizar la protección y la confianza de muchas relaciones entre los ciudadanos y las Administraciones públicas.

Pero no es suficiente ese instrumento, como no fue suficiente la tregua de dios; ni tampoco es deseable trasladar el esquema que se establece para garantizar

---

[31] Se recuerdan de manera explícita las Decisiones de las instituciones europeas sobre sus procedimientos internos para garantizar la seguridad y confidencialidad de las comunicaciones; así como la protección de la documentación. En concreto, la Decisión de la Comisión 2001/844, de 29 de noviembre; y la Decisión del Consejo 2001/264, de 19 de marzo.

la seguridad de las comunicaciones con las Administraciones a las relaciones privadas. Porque hay que saber que ese reglamento impone un registro de actividad de tal modo que se retendrán las informaciones para su análisis e investigación o, como se reitera ahora con un horrible palabro, se "monitorizarán" (art. 23). Esto, que puede admitirse en las comunicaciones oficiales porque tanto la seguridad de lo público como el principio de transparencia así lo demandan, debe rechazarse en el desenvolvimiento cotidiano de los ciudadanos al comunicarse o informarse entre ellos pues afectaría a la esencia de varios derechos fundamentales como la intimidad, la libertad de expresión, la comunicación o la información[32].

Se requiere la paz de todos los caminos, la seguridad en las relaciones privadas, pero sin que haya ningún permanente vigía o carcelero que pueda fabricar nuevos e inesperados grilletes.

Por el momento, la regulación está trasladando a las empresas de telecomunicaciones la carga de proteger la integridad de las redes. Así, en la reforma que se realizó de la Directiva "marco" de telecomunicaciones en el año 2009, se incorporaron dos nuevos preceptos con obligaciones concretas a las empresas que suministran las redes públicas de comunicaciones para que mantengan medidas técnicas y organizativas que garanticen su seguridad y la continuidad de la prestación, que reduzcan al mínimo posible los incidentes que puedan producirse, que faciliten información sobre los problemas que hayan existido y que se realicen auditorías de seguridad. Las autoridades nacionales pueden requerir la información que estimen adecuada, así como realizar las investigaciones oportunas para garantizar la aplicación de la normativa y la integridad de las redes de comunicaciones[33]. Y es que en los contratos que suscribimos los ciudadanos y empresas con las compañías de telecomunicaciones que prestan el servicio de acceso a Internet existen

---

[32] Esta es una de las cuestiones centrales del estudio jurídico de los problemas que genera el entorno de Internet, la protección de los derechos fundamentales. Entre los estudios que analizan con rigor el sistema de protección de los derechos fundamentales ante otros avances científicos, debe destacarse el libro de Gabriel Doménech Pascual, *Derechos fundamentales y riesgos tecnológicos*, Ed. CEC, Madrid, 2006; expone también algunas propuestas de protección M.L. Fernández Esteban, *Nuevas tecnologías, Internet y derechos fundamentales*, McGraw Hill, Madrid, 1998; en fin, no debe desconocerse la trascendencia del principio de proporcionalidad en todo lo que afecta a este ámbito como estudia Carlos Bernal Pulido, *El principio de proporcionalidad y los derechos fundamentales*, Ed. CEC, Madrid, 2005.

[33] En concreto son las nuevas redacciones de los arts. 13 bis y ter de la Directiva 2002/21, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas tras la reforma mediante la Directiva 140/2009, de 25 de noviembre. En la Ley general de telecomunicaciones estas previsiones se contienen en el nuevo artículo 36 bis, introducido mediante el Real Decreto Ley 13/2012, de 30 de marzo, que establece las competencias del Ministerio para requerir la información necesaria de las empresas, dictar las instrucciones necesarias y supervisar la integridad y seguridad de las redes

cláusulas de compromiso para respetar la integridad de la red, así como otras relativas a la legalidad de los comportamientos[34].

Sin embargo, ese traslado de cierta responsabilidad a las empresas debe mantenerse en unos justos términos, en lo que afecta a la seguridad de los servicios que prestan y nunca a garantizar una protección de todas las comunicaciones, impidiendo cualquier ataque. La red es un instrumento y, como tantos otros instrumentos, es quien lo utiliza quien le otorga un efecto beneficioso y nocivo. El armero no puede responder de todo lo que hace el cazador que compra la escopeta.

La responsabilidad debe seguir siendo personal. De ahí que, para garantizar la paz de los caminos de Internet, debamos insistir en la educación y en la formación de los usuarios. Del mismo modo que se enseñan las normas de circulación vial, debería promoverse una buena educación personal para el adecuado comportamiento de los ciudadanos responsables en Internet.

Carecemos en nuestra sociedad ya de temores similares a los que causaba la pena religiosa de la excomunión, que contribuyó en mucho a mantener la paz de los caminos medievales. Sin embargo, la técnica sí podría impedir a los responsables de ataques su acceso a Internet. Ya hemos visto como un juez penal ha incluido esa medida en una sentencia condenatoria. Pero, si en el futuro prosperara la identificación personal, además del IP de la conexión, sería posible “excomulgar” a los infractores.

En el pasado los cambios de era histórica abrieron las puertas a nuevas ideas, a instrumentos y figuras jurídicas que fortalecieran las instituciones, de la alta edad media al régimen feudal, y después a la llegada del Estado moderno y, así, sucesivamente, ésta es también la hora de dar vigor y robustecer las reglas que sirvan de otero para dar tranquilidad a quienes transitan por los caminos de Internet. Hemos de dar muestra de que hemos aprendido algo al recorrer la historia del Derecho y que portamos en nuestra mochila conocimientos e instrumentos jurídicos adecuados. Provienen del Derecho internacional, del Derecho penal, pero sobre todo del Derecho público, y justifican una mínima intervención del poder para garantizar también con Internet el libre desenvolvimiento de la personalidad. Un mandato constitucional, no lo olvidemos. Hay que aprestar esas técnicas, ante tanta vorágine tecnológica, ante las guerrillas y conflictos, para mantener la paz de los caminos de Internet. Esta es la relevante misión que tenemos ahora entre manos los juristas.

---

[34] Resulta imprescindible insistir en el conocimiento de las cláusulas que acogen los contratos para formar en la conciencia y trascendencia de lo que suponen las comunicaciones telemáticas. Sólo así se podrán exigir las adecuadas responsabilidades, como demanda Rebecca MacKinnon, en su libro “*No sin nuestro consentimiento. Qué ocurre cuando los gobiernos se apropian de la red. La lucha por la libertad en Internet*”, Ed. Deusto, Barcelona, 2012.