Derecho y Ciberespacio

Un primer enfoque

Hernando Gutiérrez Prieto
Director del Departamento de Sociología y Política Jurídica.
Pontificia Universidad Javeriana.

Las relaciones entre Derecho y Ciberespacio no parecen ser especialmente difíciles de entender si se mira al derecho desde una perspectiva regulatoria. La idea es identificar aquellos aspectos de internet (en su estructura, uso, o aplicación) para convertir a la Red en un objeto de regulación jurídica.

Las dimensiones del ciberespacio: de arpanet a la www.

En octubre de este año se celebrará el trigésimo aniversario de la primera demostración pública de lo que quizás es hoy uno de los procesos más impresionantes del desarrollo contemporáneo en telecomunicaciones: la Red Mundial de comunicaciones por computador o "World Wide Web" (WWW).

Durante la "Primera Conferencia Internacional sobre Computadores y Comunicaciones", celebrada en octubre de 1972 en la ciudad de Washington, los científicos de ARPA[1] mostraron el enlace entre 40 computadores localizados en diferentes lugares de los Estados Unidos. Tres años antes, se había realizado

[1] Sigla de la *Advanced Research Projects Agency*: Agencia para Proyectos de Investigación Avanzados, que había sido creada en 1958 como un organismo al interior del Ministerio de Defensa de Estados Unidos.

exitosamente la prueba de comunicaciones entre computadores de las universidades de UCLA y Stanford; fue el origen de lo que se denominó ARPANET.

En 1974, los científicos de ARPA, en estrecho trabajo conjunto con científicos de la Universidad de Stanford, generaron el protocolo TCP/IP[2] que no sería acogido internacionalmente hasta 1982, dando lugar al nacimiento de internet.[3]

1984 y 1985 fueron años clave en el desarrollo de internet por varias razones: en 1984 se establecieron nombres de dominio[4] de los un poco más de 1000 servidores conectados a la red y el gobierno británico anunció la creación de JANET (Joint Academic Network); una red conjunta para fines académicos. Al año siguiente, Estados Unidos creó la NSFNet[5] para los mismos propósitos académicos con financiación del gobierno federal y con la condición de que el acceso a la red así creada fuera para "usuarios calificados" en las instalaciones universitarias. De esta manera, quedaban excluidas instituciones privadas no universitarias lo que no impidió que se iniciaran conversaciones para permitirles el acceso a una red que en 1985 ya tenía 5.000 servidores y que en 1986 sobrepasaba los 28.000.

Este hecho explica que la mayor parte de la información disponible en la red fuera útil para las actividades científicas y académicas: consultas de bases de

[2] Transmission Control Protocol/Internet Protocol: protocolo de control de transmisión.

[3] Entre 1974 y 1982 se utilizaron varios protocolos de comunicación entre redes de computadores que se crearon en Estados Unidos y en Europa. Vale la pena destacar en Estados Unidos a Usenet, Bitnet y Csnet y en Europa a Eunet y EARN.

[4] DNS (*Domain Name Servers*).

[5] National Science Fundation Net.

datos bibliográficos, correo electrónico y grupos de discusión. En 1987 fue fundada la primera compañía que permitía acceso a internet mediante la suscripción de usuarios; tres años después la cifra de servidores ya había llegado a los 300.000.

Aquellos lectores que tuvieron la oportunidad de utilizar la red en estos últimos años de la década de los 80 recordarán cómo la información que era posible consultar en esta época eran textos (en pantallas con fondo en un color) y cómo era necesario utilizar comandos desde el teclado de los computadores para pasar a la página siguiente de un documento o para abrir un documento nuevo. La simplificación de este sistema, mediante la creación de "miradores" (*browsers*), un nuevo lenguaje para ocultar enlaces (*links*) en textos o imágenes[6] y el uso de un "ratón" (*mouse*) para activarlos, permitió en 1990 el surgimiento de la WWW.[7]

Para finales de 1992 el número de lugares de la WWW (*web-sites*) era de 50. En 1993 esta cifra apenas llegaba a 150 sitios en el mundo. El desarrollo de los programas "miradores" o *browsers* como Netscape o Internet Explorer, la facilidad de incorporar imágenes a los sitios, el desarrollo de nuevas plataformas en computadores que cada vez se fabricaban a precios más asequibles a individuos, son hechos que determinaron un creciente interés para el uso de la red con fines comerciales adicionalmente a los académicos que seguían siendo los principales. En 1994, el número de servidores era ya de 3.2 millones y el de sitios de la WWW se había elevado a 3.000. Doce meses después, los servidores

[6] HTML (Hypertext Makeup Language).

[7] El concepto y los desarrollos de los programas los debemos a Tim Berners-Lee y a los trabajos de los científicos del CERN (European Centre for High Energy Physiscs) con sede en Ginebra.

se duplicaban y los sitios llegaban a 25.000. A finales de 1996, los sitios de la WWW se habían multiplicado por diez, siendo más de 250.000, y los servidores conectados a la red habían superado la barrera de los 12 millones. Cinco años más tarde[8], enero de 2002, se calculan alrededor de:

- 150 millones de servidores en la red;
- 603 millones de computadores personales en el mundo;
- 500 millones de personas con acceso a la red, que dedican al mes un promedio 10 horas y cuarto a su consulta;
- Más de 2.000 millones de páginas en sitios de la WWW con un incremento de alrededor de 7 millones de páginas al día;
- Más de 150.000 millones de dólares por ingresos en transacciones de comercio electrónico (comparado a ingresos reportados de 58.000 millones de dólares en 1999)...

La creciente complejidad de esta Red Mundial de comunicaciones, en apenas diez años, se deriva no sólo del crecimiento exponencial que aún presenta en algunos de sus elementos, sino en la multiplicidad de impactos que está produciendo en las relaciones sociales, políticas, económicas y jurídicas, su valoración y su diferenciado desarrollo global. La percepción de las relaciones entre esta nueva forma de ciberespacio y el derecho está matizada por estas diferenciaciones, como se mostrará a continuación.

[8] Estas, y otras estadísticas utilizadas en este artículo, han sido tomadas de distintas fuentes disponibles en internet. Las principales son "cyberatlas" en http://www.cyberatlas.internet.com y Nielsen/Netraitings en http://www.nielsen-netraitings.com.

Las controversias actuales

Las relaciones entre Derecho y Ciberespacio no parecen ser especialmente difíciles de entender si se mira al derecho desde una perspectiva regulatoria. La idea es identificar aquellos aspectos de internet (en su estructura, uso, o aplicación) para convertir a la Red en un objeto de regulación jurídica. En esta perspectiva, la Red no es más que una herramienta de comunicación que no plantea especiales retos a la regulación jurídica; al fin y al cabo, se puede argumentar, se trata de nuevas conductas frente a las cuales la respuesta del derecho es la misma que ha tenido históricamente: sancionar aquellas que se consideran violatorias de derechos, modificar la normatividad para aceptar las nuevas formas de comunicación en el campo jurídico (darle valor como documento con valor legal a los mensajes electrónicos, por ejemplo) o regular las nuevas formas de contratos surgidas en la Red (como el contrato que provee el acceso a internet, o los de suscripción para la provisión de información especializada).

Las controversias actuales se han concentrado en los siguientes aspectos: la regulación del comercio electrónico (autenticidad de las transacciones y protección contra el fraude); la difusión de material pornográfico (especial problema de debate es la difusión de material pornográfico infantil); la difusión de material contentivo expresiones de odio, racismo o incitación a actos terroristas; las conductas relacionadas con generación y transmisión de virus, acceso y adulteración de la información de los servidores; la vulneración de la privacidad de los usuarios y su protección.

Si se tiene en cuenta que aún hoy más del ochenta por ciento (84.7%) de las páginas de la Red Mundial están localizadas en servidores de los Estados

Unidos[9], parece comprensible que sea la regulación de ese país la que se ha colocado en una posición de liderazgo internacional para generar nuevos sistemas normativos respecto de internet. En lo que se refiere, por ejemplo, a la difusión de material pornográfico en la Red, merece tenerse en cuenta la siguiente información de Estados Unidos:

- En 1998, sus usuarios de internet gastaron 970 millones de dólares en el pago de tarifas de acceso a sitios con material pornográfico;
- En el año 2000, se estimó que 21 millones de sus usuarios (casi uno de cada cuatro) ingresaron, al menos una vez al mes, a sitios que ofrecen esta clase de material;
- En 1999, la participación de ventas de material pornográfico significó el 9% del total de ventas de comercio electrónico.

Estas tendencias de uso han generado preocupación en la forma como se utiliza la Red por parte de usuarios menores de edad. En un estudio realizado en marzo de 2001 en Gran Bretaña, por ejemplo, se identificó que la mitad de sus usuarios menores de 17 años había visitado sitios con información sobre música o literatura en la Red; el cuarenta por ciento visitó sitios de juegos; una cuarta parte de estos usuarios ingresó a sitios de juegos de azar permaneciendo en ellos un promedio de 11.3 minutos y el veinte por ciento de estos usuarios (290.000) visitó sitios de pornografía permaneciendo en ellos un promedio de 28 minutos.

[9] A pesar de que la distribución geográfica de los servidores de la Red ya no presenta una concentración mayoritaria en ese país.

Dos reacciones principales desde el punto de vista jurídico se han presentado ante este fenómeno: por un lado, el ofrecimiento a través de la Red se este material se ha constituido en un delito. El FBI, por ejemplo, investigó en el año 2000 más de 1.600 casos de pornografía infantil, lo que significó un incremento de 13 veces las investigaciones que había realizado en 1996. Por otro lado, varios gobiernos han optado por establecer una forma de bloqueo a sitios de internet que contienen información no deseable para menores de edad o para usuarios en general. Desde julio del año pasado, por ejemplo, una Comisión especial designada para el efecto en Corea, determinó el bloqueo general de más de 120.000 sitios de la Red por considerar que contienen información sobre crímenes informáticos, ofrecen material obsceno o difamatorio, han realizado fraudes en la negociación electrónica, u ofrecen material induciendo al suicidio o a la construcción de bombas y artefactos explosivos.[10]

En lo que se refiere al comercio electrónico las regulaciones legales se han concentrado en los problemas de autenticidad de las transacciones y en otros aspectos que garanticen su seguridad. Se trata de una tendencia internacional que ya ha generado una primeras formas de legislación en diferentes países.[11]

El campo principal de las controversias está en la posibilidad de la aplicación internacional de estas legislaciones. Puesto que el esquema legislativo sigue funcionando desde una perspectiva nacional, la discusión es hasta qué punto estas regulaciones pueden aplicarse a extranjeros. Mientras no se cuente con

[10] Esta información apareció publicada en The Korea Herald, abril 11 de 2001.

[11] En el año 2000, ya se tenía legislación aprobada en Australia, Estados Unidos, Canadá, Irlanda, Reino Unido, Bermudas, Francia, Alemania, Italia, Dinamarca, España, Portugal, Colombia, Méjico, Singapur, Hong Kong, Corea, Malasia e India. Existían proyectos de ley, ya avanzados en su discusión, en Argentina, Chile, Brasil, Ecuador, Perú y Japón.

regulaciones aplicables internacionalmente[12], el esquema actual consistirá en la multiplicaciones de legislaciones nacionales, no siempre coherentes, y muy limitadas en su aplicación.

Los retos futuros (variando el enfoque: ciberespacio y derecho)

El giro en la relación de los términos ciberespacio y derecho otorga nuevas posibilidades de análisis. Las limitaciones del enfoque anterior, aún dominante, están determinadas no sólo por la limitación en la aplicación de la normatividad sino porque la atención deja de lado importantes relaciones que la Red está generando desde el punto de vista social.

Internet, por ejemplo, está significando un espacio de autorregulación no jurídica, que no podría desconocerse. Más allá del control legal estatal, internet está hoy regulada en aspectos importantísimos por la expedición de normas técnicas globalizadas, por procedimientos establecidos por parte de instituciones no gubernamentales y por el ofrecimiento de servicios privados para el control de producción y manejo de la información. Veamos sólo algunos de estos ejemplos.

La ICANN (The Internet Corporation for Assigned Names and Numbers: Corporación de Internet para la asignación de nombres y números) es una institución privada, sin ánimo de lucro, que tiene a su cargo la determinación de las políticas y determinación de reglas para la denominación y asignación de

[12] La creación de una Corte Internacional de Justicia puede ser un ejemplo de estas organizaciones internacionales.

nombres de dominio y de servidores de la Red (sin los cuales no es posible tener acceso a internet o un sitio dentro del ciberespacio). Fue creada en noviembre de 1998 y tiene cobertura global. Es la ICANN quien determina, por ejemplo, la posibilidad de que se creen nuevos nombres de dominio en la Red[13], autoriza a empresas privadas para la asignación de nombres de dominio y establece mecanismos internacionales para la solución de conflictos en estos campos. Su junta directiva está compuesta por 19 miembros: 9 de ellos son elegidos por las tres organizaciones[14] (también privadas) que soportan la institución en aspectos técnicos; otros 9 directores son elegidos en foros distintos (5 de los cuales son elegidos mediante voto de los usuarios de la Red en todo el mundo) y un presidente de la organización. Su sede se encuentra en California, pero realiza reuniones rotativas de discusión en diferentes países.[15]

Paralelamente a las reacciones legislativas producidas para controlar el acceso a los sitios de internet (especialmente por menores de edad), la producción o difusión de material considerado obsceno, fraudulento, peligroso o sencillamente inconveniente, o para la protección de la privacidad de los usuarios, es la Red la que ha generado nuevas estructuras de control bajo la forma de servicios públicamente disponibles o mediante el pago de una contraprestación. Basta, quizás, señalar algunos de ellos como los servicios relacionados con el filtro o bloqueo de páginas con contenido pornográfico o fraudulento, programas diseñados para limitar el tiempo de acceso a internet, buscadores y "browsers" especializados

[13] A los ya conocidos .com, .org, .mil, .gov .net y .edu se han incrementado varios otros en los últimos dos años, tales como .biz, .pro, .tv, .museum, .kids o .info.

[14] Domain Name Supporting Organization (DNSO), Address Supporting Organization (ASO), Protocol Supporting Organization (PSO).

[15] Para una información completa se recomienda consultar el sitio oficial de la ICANN en http://www.icann.org

en niños, servicios para realizar búsquedas anónimas, eliminar rastros de consulta, eliminar correos electrónicos de fuente no deseada, programas especializados en la encriptación de información, antivirus, etc.

La explicación de estos fenómenos no se encuentra sólo en la limitación de la perspectiva legal. Mirado el fenómeno en un nuevo contexto, lo que todo esto parece indicar es que nos encontramos ante la emergencia de un nuevo fenómeno que confronta varios de los principios en los que descansan los actuales sistemas legales. Un caso típico se encuentra en lo que se ha denominado "gobierno virtual" (*e-government*). No se trata sólo del otorgamiento de información por parte de las instituciones gubernamentales a los ciudadanos. Se trata de un nuevo estilo de relación que está exigiendo la revisión de los fundamentos que gobiernan temas tan importantes como la contratación con el Estado, la participación ciudadana, la posibilidad de control de la gestión gubernamental y del ejercicio de derechos políticos como el voto.

Simultáneamente, lo que queda planteado como reto al futuro, es el papel de los sistemas legales para incentivar y fortalecer los efectos positivos que la Red produce y orientar los cambios necesarios para reducir los negativos. Investigaciones jurídicas que sólo eran posibles hace poco a un gran costo hoy son factibles por la calidad de la información jurídica que se va incorporando a la Red[16]. Los desarrollos son diferenciados en los países, pero, por ejemplo, es posible encontrar los textos de casi todas las constituciones del planeta traducidos al inglés. Un país como Colombia ha producido desde 1992 más de 730 leyes y más de 20.000 de-

[16] Por ejemplo, en el campo de la legislación comparada.

cretos. Gran parte de esta información (la de carácter general) se encuentra hoy en la Red y puede tenerse acceso gratuito a ella,[17]lo cual no era posible hace apenas unos años. La Red implica también modificaciones importantes para el quehacer profesional de los abogados y de la academia jurídica internacional. Los costos involucrados en procesos de conformación de redes profesionales o académicas son, por la existencia de internet, notoriamente menores hoy que lo que eran hace cinco años. El trabajo jurídico no implica ya, de una manera necesaria, una localización profesional específica; de manera similar a como está sucediendo en otras profesiones, se ha comenzado a "des-localizar".

Pero el reto próximo implica abordar cuestiones trascendentales como la relativa a la falta de acceso a las herramientas de información y relación que entrega internet con un efecto indirecto de aumentar exclusiones sociales. Basta considerar que apenas nos aproximamos a un 10% de la población mundial con acceso a la Red[18] y que hacia el año 2015, en el escenario más positivo, se estima que alrededor de 1.000 millones de personas en el planeta subsistirán con ingresos inferiores a un dólar diario[19]. El crecimiento de usuarios comenzará a presentar límites derivados de los factores económicos de acceso; simultáneamente, aspectos culturales, como el idioma en que se encuentra la información[20], son también percibidos como determinantes de exclusión.

[17] El proyecto, al que se asignó el nombre de juriscol, es manejado por el Banco de la República y se consulta a través del sitio en la Red de esta institución: http://www.banrep.gov.co

[18] Los porcentajes de población con acceso a internet son, una vez más, diferenciados: países como Estados Unidos se acercan a la mitad de su población con acceso a la Red; en Colombia estaríamos llegando al 3% de la población.

[19] Los estimativos son del Banco Mundial. Puede consultarse en http://www.worldbank.org

[20] En una revisión realizada en el año 2000 se encuentra que los sitios europeos suelen presentar la información en tres idiomas (uno de ellos el inglés), los asiáticos suelen ser bilingües (lengua del país en que se origina e inglés), mientras que la tendencia general de las páginas originadas en Estados Unidos es la de presentar la información sólo en este idioma. Al respecto debe recordarse la gran concentración del origen de las páginas de la WWW: 84.7% en Estados Unidos.

Es en la valoración jurídica de dos aspectos centrales (auto-regulación y exclusión) donde radica la mayor fuente de indagación sobre las relaciones entre el Ciberespacio y el Derecho en los próximos años. Quizás valdría la pena evaluar más detenidamente lo que hemos venido considerando hasta ahora, abordando los retos desde su complejidad.

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la OCDE a PARIS en MAY83, el término ***delitos relacionados con las computadoras*** se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.

El autor mexicano **Julio TELLEZ VALDEZ** señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".

El tratadista penal italiano **Carlos SARZANA**, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".

Características de los delitos informáticos

a. Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

b. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
c. Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
d. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
e. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
f. Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
g. Son muy sofisticados y relativamente frecuentes en el ámbito militar.
h. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
i. En su mayoría son imprudenciales y no necesariamente se cometen con intención.
j. Ofrecen facilidades para su comisión a los menores de edad.
k. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
l. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Clasificación de los delitos

1. **Como instrumento o medio.**
   En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
b. Variación de los activos y pasivos en la situación contable de las empresas.
c. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
d. Lectura, sustracción o copiado de información confidencial.
e. Modificación de datos tanto en la entrada como en la salida.
f. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
g. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
h. Uso no autorizado de programas de computo.
i. Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
j. Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
k. Obtención de información residual impresa en papel luego de la ejecución de trabajos.
l. Acceso a áreas informatizadas en forma no autorizada.
m. Intervención en las líneas de comunicación de datos o teleproceso.

2. Como fin u objetivo.

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a. Programación de instrucciones que producen un bloqueo total al sistema.
b. Destrucción de programas por cualquier método.

c. Daño a la memoria.
d. Atentado físico contra la máquina o sus accesorios.
e. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
f. Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

Otros delitos

- **Acceso no autorizado:** Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
- **Destrucción de datos:** Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- **Infracción al copyright de bases de datos:** Uso no autorizado de información almacenada en una base de datos.
- **Interceptación de e-mail:** Lectura de un mensaje electrónico ajeno.
- **Estafas electrónicas:** A través de compras realizadas haciendo uso de la red.
- **Transferencias de fondos:** Engaños en la realización de este tipo de transacciones.
- **Espionaje:** Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- **Terrorismo:** Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- **Narcotráfico:** Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

Problemas para la legislación según la onu

a. Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
b. Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
c. Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
d. No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
e. Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
f. Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

PRIETO GUTIÉRREZ, Hernando. Derecho y ciberespacio "Un primer enfoque". En: Revista Javeriana No. 684, tomo 138. Bogotá, Pontificia Universidad Javeriana, Mayo de 2002.