Poder en Internet en la Sociedad del riesgo y la Información

Christian Scheechler Corona[1]

Resumen

Innegable a esta altura es el impacto que las tecnologías de la información y las comunicaciones TIC, y especialmente Internet, han tenido en la configuración social. El Derecho no ha estado ajeno a tal realidad y muchas de sus áreas han visto modificadas tradicionales categorías. Las características de la Red propician, junto con esta mutación, una redistribución de las relaciones jurídicas y sociales en el ciberespacio. El ejercicio del poder estatal comienza a disminuir su monopolio debido a que tajadas importantes de su control han sido compartidas con otros Estados, con la empresa privada y los particulares, a objeto de lograr una efectiva regulación y ejercicio del poder en el ciberespacio.

[1] Abogado. Licenciado en Ciencias Jurídicas y Sociales, Universidad Católica de Temuco. Profesor de Derecho Penal e Introducción al Derecho, Escuela de Derecho, Universidad Católica del Norte. Postgrado en Propiedad Intelectual, Universidad Castilla La Mancha, España. Diploma de Estudios Avanzados del Doctorado en Derecho y Justicia de la Universidad de Deusto, Bilbao. Actualmente en desarrollo de Tesis doctoral sobre los Problemas de la parte general del derecho penal en el cibercrimen, bajo la dirección del Prof. Dr. iur. Dr. med. Dr. h. c. mult. D. Carlos María Romeo Casabona, Catedrático de Derecho Penal, Director Cátedra Interuniversitaria Fundación BBVA - Diputación Foral de Bizkaia de Derecho y Genoma Humano, Universidad de Deusto y Universidad del País Vasco.

En el presente trabajo se revisará brevemente la configuración de la sociedad postindustrial, la importancia que Internet y las TIC tienen en ella, como estas han modificado las relaciones de poder en la Red, merced de una redistribución entre actores distintos del Estado, y el papel que nuevas realidades tecnosociales como el tráfico de datos personales o los contenidos nocivos han jugado en este fenómeno.

Palabras Clave

Internet – Poder- Derecho- Sociedad del riesgo – Ciberespacio.

SUMARIO: I. LA SOCIEDAD DEL RIESGO Y LA INFORMACIÓN. 1. Las primeras aproximaciones. 2. La sociedad de la información. 3. La sociedad del riesgo. 3.1. Las tecnologías y el riesgo. 3.2. Características de la sociedad del riesgo. II. INTERNET Y LAS TIC EN LA SOCIEDAD DE LA INFORMACIÓN Y EL RIESGO. 1. La tecnología y las redes. 2. Desde los ordenadores con camuflaje. 3. Internet aparece en escena. 4. La libertad en Internet. 5. Poder y control en la Red. 6. El tráfico de datos y contenidos como eje de las relaciones de poder en la Red. III. EL ESCENARIO DE LAS RELACIONES DE PODER EN INTERNET. 1. El nuevo rol del estado. 2. La acción internacional conjunta. 3. El poder en manos de los usuarios. IV. IDEAS FINALES.

I. LA SOCIEDAD DEL RIESGO Y LA INFORMACIÓN.

1. Las primeras aproximaciones.

Cualquier trabajo o investigación que quiera tocar algún aspecto determinado del Derecho en la actual sociedad se tropezará con *clichés* tan repetitivos como ineludibles. Que estamos en una sociedad cambiante, que Internet y las nuevas expresiones tecnológicas han transformado todo, que ahora todo es globalizado, etc. En mayor o menor medida, existe un importante cúmulo de hechos que respaldan tales afirmaciones. Estamos ante una sociedad distinta en muchos aspectos a la sociedad industrial,

aquella caracterizada por la producción en masa, las grandes industrias jerárquicamente organizadas y el trabajador sustituible[2].

Desde las primeras aproximaciones conceptuales a la sociedad actual, aquellas de Toffler y su "sociedad de tercera ola", o de McLuhan y la archiconocida "aldea global"[3], gobiernos y autores han intentado esbozar conceptos que describan de forma acertada la fenomenología social contemporánea[4]. Uno de los más conocidos es el de "sociedad de la información", pero que no deja de tener detractores, que postulan otras opciones como la "sociedad red", la "sociedad digital" o la "sociedad del riesgo".

De todas formas los autores mencionados tienen prismas distintos en su análisis. Si para Toffler los medios de producción eran el punto a considerar, McLuhan ponía el acento en los *mass media*. En ambas visiones las anotaciones jurídicas son más bien escasas. Sin embargo, no debe desconocérseles el que ambos apuntaron a la ingente importancia de la información como factor económico y elemento de poder en la sociedad postindustrial.

2. La sociedad de la información.

En 1969, el Ministerio de Industria y Comercio japonés publica un informe denominado *Towards The Information Society*, y que dio lugar mas tarde, en 1972, a la propuesta nipona de plan para encarar el año 2000 (Propuesta de Plan para la Sociedad de la Información). Era la visión de

---

[2] TOFFLER, Alvin. *La tercera ola*. 2ª. Edición. Barcelona: Ed. Plaza & Janes, 1980, p. 59-72.

[3] Visión que, sobre todo, se refería a la creciente influencia de los *mass media* en la sociedad contemporánea, marcada por una globalidad que, él adelantaba, era producto de la aceleración de la tecnología y tenía al satélite como eje central. MCLUHAN, Marshal; POWERS, B. R. *La aldea global*. 3ª. Edición. Barcelona: Gedisa Editorial, 1995, p. 122-123.

[4] Un estudio de Beninger recopila, entre 1950 y 1984, hasta 75 denominaciones diferentes, de las que pueden nombrarse: sociedad postindustrial, tecnópolis, sociedad multimedia, mundo digital, era digital, infolítico, sociedad digital, mundo virtual, mundos artificiales y sociedad teledirigida, entre otros. Todos ellos tienen como denominador común a la información, o a la técnica de su tratamiento automatizado, la informática. En general, aluden a la tecnología como elemento diferenciador. No cabe duda también que existe una especie de carrera cultural entre los países e investigadores por constituirse en los padres del concepto que identifique el nuevo entorno. BENINGER, J., citado en GARCIA ARETIO, Lorenzo; et al (Coords.). *De la educación a distancia a la educación virtual*. Barcelona: Ed. Ariel, 2006, p. 27.

futuro que tenía Japón en esa época, y al mismo tiempo los primeros rayos de sol para el concepto en comento. En 1993 surge en Estados Unidos el "Plan Gore", *Technology for American´s Economic Growth. A New Direction to Build Economic Strength*, con el claro objetivo se seguir liderando la economía mundial en la naciente sociedad de la información. Para ello se establecían objetivos tales como el mejoramiento de la tecnología en la educación y en la información, y generar una política de comunicaciones a nivel nacional que facilite la rápida implantación de las nuevas tecnologías[5].

Europa no se quedó atrás y el Consejo de Ministros de la Unión Europea redactó, en 1994, el denominado Plan Delors, documento cuyo objetivo primordial era "contar con el potencial de mejorar la calidad de vida de los ciudadanos europeos, aumentar la eficacia de la organización social y económica y reforzar la cohesión"[6]. El Plan Delors fue el antecedente para la redacción de un nuevo informe, coordinado por Martín Bangemman, titulado "Europa y la sociedad global de la información. Recomendaciones del Consejo de Europa"[7].

Junto a estos puntos casi icónicos, una serie de países e instituciones a nivel mundial han intentado dar con la definición exacta de sociedad de la información, manteniendo este concepto de forma mayoritaria por sobre otros vistos o por ver[8].

---

[5] CELA, Julia R. "Sociedad del conocimiento y sociedad global de la información: implantación y desarrollo en España". Universidad de La Rioja, DIALNET. http://www.ucm.es/BUCM/revistas/inf/02104210/articulos/DCIN0505110147A.PDF (última visita 13 de Septiembre de 2008).

[6] *Ibíd.*

[7] AGUADERO, Francisco. *La sociedad de la información*. Madrid: Ed. Acento, 2002, p. 20.

[8] En el Reino Unido, en el documento denominado Iniciativa para la Sociedad de la Información (1998), define a esta como "El entorno en el que la información es un factor clave del éxito económico, y en el que se hace uso intenso y extenso de las tecnologías de la información y las comunicaciones" TELEFÓNICA. "Concepto de Sociedad de la Información". Telefónica España. http://www.telefonica.es/sociedaddelainformacion/pdf/informes/espana_2000/parte1_1.pdf (última visita 13 de Abril de 2008). En Chile, el Informe de la Comisión de Nuevas Tecnologías de Información y Comunicación (1999), concibe a la Sociedad de la Información como "Sistema económico y social donde la generación, procesamiento y distribución del conocimiento e información constituye la fuente fundamental de productividad, bienestar y poder". GOBIERNO DE CHILE "Informe Comisión Presidencial Nuevas Tecnologías de la Información y las Comunicaciones 1999". Red Universitaria Nacional. http://www.reuna.cl/documentos/DOC2006/historico/chile_hacia_soinfo_1999.pdf (última

Se critica que su enfoque es eminentemente economista, y se centra en el valor dado a la información como materia prima de la producción, visión que es enteramente concordante con el hecho de que la información en si se transforme en un bien jurídico protegido[9]. Campoli aclara que la información por si misma, y su acumulación, no constituye el bien más

consulta 11 de Abril de 2008). El Libro Verde sobre la Sociedad de la Información en Portugal, que data de 1997, la define como "una forma de desarrollo económico y social en el que la adquisición, almacenamiento, procesamiento, evaluación, transmisión, distribución y diseminación de la información con vistas a la creación de conocimiento y a la satisfacción de las necesidades de las personas (y) de las organizaciones, juega un papel central en la actividad económica, en la creación de riqueza y en la definición de la calidad de vida y de las prácticas culturales de los ciudadanos". VALENTI, Pablo. "La sociedad de la información en América Latina y el Caribe: TIC´s y un nuevo Marco Institucional". Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Salud. Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación, Nº 2, 2002. http://www.oei.es/revistactsi/numero2/valenti.htm (última consulta 11 de Abril de 2008). Ante esta multiplicidad de definiciones, Reusser señala que esto no es sino otro escenario de la guerra de influencias entre estados Unidos y Europa por imponer sus conceptos, criterios y parámetros en los países menos desarrollados (principalmente de Asia y Latinoamérica), tal como sucede con otros términos como teletrabajo o *telecommuniting*, o los estándares de televisión de Estados Unidos o la Unión Europea. REUSSER MONSÁLVEZ, Carlos. "¿Qué es la sociedad de la información?". Centro de Estudios de Derecho Informático U. de Chile. Revista Chilena de Derecho Informático, Nº 2, año 2003. http://www.derechoinformatico.uchile.cl/CDA/der_informatico_complex/0,1491,SCID%253D14670%2526ISID%253D292,00.html (última consulta 10 de Abril de 2008).

[9] En este sentido, y penalmente hablando, la información en la actualidad tiene un preciado valor en varios ámbitos, como en la intimidad y la libertad de expresión o de prensa, pero sin duda cobra una especial relevancia en el tráfico económico e industrial, dada la sistematización informática que sufre en esos sectores. Muñoz Lerma afirma que la información, y su dominio, se convierte en el centro de gravedad en la lucha por el poder político y económico, constituyéndose en "un bien de incuestionable valor, cuyo tratamiento automatizado tiene repercusión en múltiples ámbitos…y cuya salvaguardia ha merecido tutela jurídica, incluso protección jurídico penal", en MORÓN LERMA, Esther. *Internet y derecho penal: hacking y otras conductas ilícitas en la red*. Pamplona: Ed. Aranzadi, 1999, p. 23-24. Romeo Casabona ahonda en esta idea, a propósito del espionaje informático, señalando que la información que interesa a efectos de la tutela jurídico penal es aquella recogida en bases de datos en el ámbito económico empresarial, como las carteras de clientes, acreedores y deudores, situación financiera de la empresa, estado del mercado en el que opera, entre otros. Datos que en su conjunto importan una realidad y un valor claramente diferenciado de cada uno de ellos considerados individualmente. Pero para efectos de la tutela ya referida, esta información además debe cumplir con los requisitos de precisión, esto es, que pueda ser delimitada en sus contornos, y de originalidad, "entendida no como pura creación, sino no común ni accesible a los demás", pudiéndose vincular a una persona o categoría de personas, vinculación que se puede presentar bajo las formas de confidencialidad o exclusividad. Ambas ideas confluyen a la existencia de restricciones en la circulación de la información, es decir, que no sea susceptible a terceros, y en la obligación del titular de la información de adoptar las medidas de seguridad para la salvaguardia de

importante de la sociedad actual, mostrándose crítico del concepto. El mismo autor afirma que no todos los cambios sociales, por grandes que sean, implican un cambio de sociedad, pues para considerarlo así hay que atender a su magnitud y si este logra remover los cimientos de una sociedad anterior[10].

Otros autores, si bien reconocen que estamos en una etapa social distinta a la época postindustrial, prefieren poner el énfasis en otros elementos, pero sin descartar el valor esencial de la información. Castells amplía su visión, poniendo el eje en otro punto: la construcción de redes[11]. Las características de la que él llama "sociedad red" son: su fundamento es la generación del conocimiento y procesamiento de la información con

aquellos datos. Agrega el autor que dado su "potencial trascendencia económica en el tráfico mercantil e industrial, no parece excesiva la llamada a la intervención del Derecho penal, como instrumento protector más eficaz". En ROMEO CASABONA, Carlos. *Poder informático y seguridad jurídica*. Madrid: Ed. Fundesco, 1997, p. 168-170. Morales Prats y la citada Morón Lerma, en la misma línea de Romeo Casabona, señalan que cuando el titular de la información susceptible de ser vinculada a un sujeto la desprotege, quedando al alcance de terceros no autorizados, se produce un comportamiento significativo para el Derecho penal. Morales Prats y Morón Lerma en MORALES PRATS, Fermín (Coord.); QUINTERO OLIVARES, Gonzalo (Dir.) et al. *Comentarios al nuevo Código Penal*. 2ª. Edición. Pamplona: Aranzadi, 1996, p. 1276-1281. Finalmente, Morón Lerma caracteriza a la información como bien económico, afirmando que "se trata de un bien que no se agota con su consumo, lo que permite que su expansión se haya producido no sólo a través de nuevas y mayores creaciones de información, sino que, en gran medida, haya sido provocada por el desarrollo de los sistemas de telecomunicación, que facilitan el acceso de la misma información a un número plural de usuarios", MORÓN LERMA, Esther. *Internet y…op. cit*., p. 87.

[10] CAMPOLI, Gabriel Andrés. "Nuevas tendencias criminológicas y victimológicas en la sociedad de la información". Alfa Redi. AR Revista de Derecho Informático, Nº 65- Diciembre 2003. http://www.alfa-redi.org/rdi-articulo.shtml?x=1248 p.3. (última consulta 01 de Septiembre 2008). Respecto a la extensión del cambio social atribuido como elemento básico de la sociedad de la información, también se muestra crítico Herrera, para quien la sociedad actual está llena de comunidades de tercera ola, al estilo McLuhan, dependientes de la tecnología y altamente comunicadas entre si. Sin embargo, esto no permite hablar de una sociedad de la información, pues este concepto es poco exacto y eminentemente económico. HERRERA, Rodolfo. "Ciberespacio, sociedad y derecho". Alfa Redi. AR Revista de Derecho Informático, Nº 63- Octubre 2003. http://www.alfa-redi.org/rdi-articulo.shtml?x=1276 (última consulta 30 de Marzo 2008). En similar sentido, Reusser, afirmando que la "sociedad de la información está muy lejos de ser alcanzada o que sólo es aplicable a los países desarrollados del mundo occidental", REUSSER MONSÁLVEZ, Carlos. *¿Qué es la sociedad…op.cit.*

[11] Para el autor, las nuevas tecnologías permiten que la "generación, el procesamiento y la transmisión de la información se convierten en las fuentes fundamentales de productividad y poder". CASTELLS, Manuel. *La sociedad red*. 2ª. Edición. Madrid: Alianza Editorial, 2001, p.51.

ayuda de tecnologías informacionales basadas en la microelectrónica; está organizada en redes; y sus actividades están fundamentalmente interconectadas en red en una escala global, actuando como una unidad en tiempo real gracias a las telecomunicaciones[12].

Para Terceiro, la clave está en los ordenadores y las redes que los interconectan, poniéndose en la misma línea que Castells, aminorando el rol de la información como elemento clave de la sociedad actual, trasladándolo a las redes informáticas, telemáticas, económicas y sociales.

En especial, pone el énfasis en la forma que adquiere la información en las redes, es decir, en la digitalización de esta[13].

Como se ve, los elementos son más menos comunes, aun cuando se acentúen unas u otras características para resaltarlas en una u otra construcción teórica. Donde si existe un nuevo elemento, y con un importante matiz jurídico, es en la teoría de Beck.

3. La sociedad del riesgo.

3.1. Las tecnologías y el riesgo. La idea central de la teoría de la sociedad del riesgo, perteneciente a Ulrich Beck, apunta a que en la época actual, aun en desarrollo y que se constituye como la continuación de la sociedad industrial, los riesgos producidos por las implicancias negativas del desarrollo tecnológico (así como por el modelo de producción y consumo moderno) adquieren una característica de globalidad y lesividad no conocidas hasta el momento. Llevados al extremo, estas fuentes de peligro han derivado en la creación de nuevos riesgos inexistentes previamente[14].

Así como en el concepto de sociedad digital el rol de las TIC es considerado como transversal y moldeador de la realidad actual,

---

[12] CASTELLS, Manuel; HIMANEN, Pekka. *La sociedad de la información y el estado de bienestar. El modelo finlandés*. Madrid: Alianza Editorial, 2002, p18.

[13] TERCEIRO, José B. *La sociedad digital*. Madrid: Alianza Editorial, 1996, p. 215.

[14] "…este concepto (sociedad del riesgo) describe una fase del desarrollo de la sociedad moderna en la que los riesgos sociales, políticos, ecológicos e individuales creados por el impulso de la innovación eluden cada vez más el control y las instituciones protectoras de la sociedad industrial". BECK, Ulrich. *La sociedad del riesgo global*. Madrid: Siglo Veintiuno de España Editores, 2002, p. 113.

específicamente a través de la digitalización de los contenidos y las redes que conlleva a la convergencia tecnológica, en la sociedad del riesgo dicha tecnología es considerada como un factor creador de riesgos, pero uno más de esos factores, y no el que determina en su totalidad el estadio estudiado (comparte ese papel con la energía nuclear, la química o la biotecnología).

Beck en su teoría sociológica aproxima las primeras características sobre el riesgo, señalando que "…es el enfoque moderno de la previsión y control de las consecuencias futuras de la acción humana, las diversas consecuencias no deseadas de la modernización radicalizada... el régimen de riesgo es una función de un orden nuevo: no es nacional, sino global.

Está íntimamente relacionado con el proceso administrativo y técnico de decisión. Anteriormente, esas decisiones se tomaban con normas fijas de cálculo de probabilidades, ligando medios y fines o causas y efectos. La sociedad del riesgo global ha invalidado precisamente esas normas"[15].

Rovira del Canto, siguiendo al mismo Beck, diferencia tres categorías de riesgos: los tradicionales, los propios del Estado industrial del bienestar y los nuevos. Los primeros, los riesgos tradicionales, son aquellos de carácter personal, individualmente imputables y limitados en el tiempo. Aquí nos encontramos con cuestiones habituales y casi cotidianas como los deportes extremos o la adicción a la nicotina. Los propios del Estado industrial de bienestar, en tanto, son soportados de forma socializada en sus costes, a pesar de ser perfectamente identificables sus autores individuales. Podemos encontrar aquí, según indica el propio Rovira, el caso de los contratos de seguros, donde es el conjunto de asegurados quienes asumen la eventualidad de ocurrencia del hecho peligroso asegurado. Finalmente están los nuevos riesgos, que participan de las características de las dos categorías antes mencionadas. No son aceptados voluntariamente pero producen efectos colectivos que no han sido perseguidos por quien creó el riesgo[16].

---

[15] *Ibíd.,* P. 8.

[16] En esta última categoría encontraremos los riesgos relacionados con las nuevas tecnologías como la informática o la telemática, así como los generados por la biotecnología, la energía nuclear o la química, y que, particularmente estos últimos, producen eventualmente fuertes daños medioambientales. ROVIRA DEL CANTO, Enrique. *Delincuencia informática y fraudes informáticos*. Granada: Ed. Comares, 2002, p. 19. Beck minimiza la incidencia de la informática y las técnicas de telecomunicaciones como fuente

Si bien es perfectamente posible concederle a Beck la idea (también frecuente en su obra) de que los nuevos riesgos, a diferencia de los antiguos, importan la posibilidad de autodestrucción de la especie humana[17], y que la informática y la telemática por si solas no importan este riesgo, no puede desconocerse el hecho de que ambas tecnologías están completa y transversalmente inmersas en el mundo global actual, atravesando funcionalmente las áreas consideradas "sensibles" por Beck, como la energía nuclear o la bioquímica. Sin ir más lejos, un fallo en los sistemas informáticos de las plantas nucleares puede generar una catástrofe de incalculable nivel temporal y espacial.

Es necesario entender que la masificación de la informática hace que los riesgos que las nuevas tecnologías traen consigo amenacen a cualquier persona sobre la faz de la tierra, directa o indirectamente, tanto como otros peligros de los considerados en la sociedad del riesgo. Siguiendo al mismo Rovira, que intenta reafirmar el rol de la informática y la telemática como fuentes generadoras de riesgos de la misma magnitud de otros recién vistos, "los límites del riesgo permitido han cambiado y siguen cambiando,

---

de riesgos. A pesar de que no lo hace de forma expresa, sus obras centran el análisis en la generación de riesgos principalmente de otras fuentes, como la energía nuclear o la bioquímica, que tienen impactos fuertes en el medio ambiente, más que en la informática o la telemática, estas últimas con mayores impactos en el patrimonio, la seguridad personal o la honra de las personas. BECK, Ulrich. *La sociedad… op. cit.,* p. 8. Carlos Pérez Del Valle en tanto considera a las tecnologías como la informática y la telemática como un mero fenómeno asociado en el tiempo al nacimiento de los nuevos riesgos, acorde con esta idea minimizadora de su importancia como generadoras de nuevos riesgos. PÉREZ DEL VALLE, Carlos. "Sociedad de riesgos y reforma penal", en *Poder Judicial. Vol. II*, 1996. Madrid: Ed. Consejo General del Poder Judicial, p. 43-44. Cfr., con Rovira, quien sostiene que ésta tiene la "categoría suficiente para ser considerada como una parte de la propia sociedad de riesgos, como un nuevo riesgo en si mismo", ROVIRA DEL CANTO, Enrique. *Delincuencia informática… op. cit.,* p. 21-22. En la misma línea está Silva Sánchez, para quien la informática y las comunicaciones generan nuevos riesgos que contribuyen al fenómeno expansivo del Derecho penal. SILVA SÁNCHEZ, Jesús-María. *La expansión del derecho penal. Aspectos de la política criminal en las sociedades postindustriales*. 2ª. Edición. Montevideo: Ed. B de F, 2006, p. 14; y GALÁN MUÑOZ, Alfonso. "Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática". *Revista de derecho y proceso penal*, Nº 15. Navarra: Ed. Aranzadi, 2006, p. 17-22.

[17] Sobre esta característica de cortes apocalípticos, véase también JESCHEK, Han H. "Franco Bricola e la sua opera vista dalla Germania", en CANESTRARI, Stefano (Dir.). *Il diritto penale alla svolta di fine millennio*. Torino: Ed. Giappichelli, 1998, p. 16.

lo que hace imposible una determinación de forma exacta, *a priori*, de dicha sociedad que se encuentra permanentemente en el riesgo"[18].

3.2. Características de la sociedad del riesgo. Siguiendo a Mendoza Buergo[19], las características definitorias de esta son:

a) Cambio en el potencial de los peligros actuales[20]. Los actuales riesgos son artificiales, en el sentido de que nacen del actuar particular o colectivo del ser humano, y no de la naturaleza (al menos no de esta sola como huracanes o terremotos, sino que en el actuar conjunto con el ser humano). A su vez son tremendamente masivos e importan, quizás por primera vez en la historia de la humanidad, la posibilidad real y concreta de llevar a la autodestrucción de la especie. Son, como dice la autora, "consecuencias secundarias del progreso tecnológico"[21].

b) La complejidad organizativa de las relaciones de responsabilidad. La organización social aumenta en complejidad, ya que, entre otras cosas, el individuo que forma parte de ella resulta cada vez más intercambiable, lo

---

[18] ROVIRA DEL CANTO, Enrique. *Delincuencia informática… op. cit.,* p. 25. Sobre este cambio en los límites, Silva Sánchez afirma que en el modelo de sociedad del riesgo se parte de la idea que un porcentaje de accidentes graves producto de fallos técnicos es inevitable. SILVA SÁNCHEZ, Jesús-María. *La expansión…op. cit.*, p. 15. El mismo agrega que "la disminución de los niveles de riesgo permitido es producto directo de la sobrevaloración esencial de la seguridad…frente a la libertad". *Ibíd.,* p. 37. Herzog marca la misma línea, al afirmar que el riesgo en esta sociedad proviene del desarrollo de la tecnología y de la economía, que produce la desestructuración y la reestructuración local, nacional e internacional, acompañada de una desorientación normativa. HERZOG, Félix. "Società del rischio, Diritto penale del rischio, regolazione del rischio. Prospettive al di la del Diritto penale", en FOFFANI, Luigi; y STORTONI, Luigi (editores). *Critica e giustificazione del diritto penale nel cambio si secolo*. Milano: Giuffrè Editore, 2004.

[19] MENDOZA BUERGO, BLANCA. *El derecho penal en la sociedad del riesgo*. Madrid: Ed. Civitas, 2001, p. 25.

[20] Sobre este punto en particular y en referencia a las figuras de delitos cometidos en la Red, Romeo Casabona afirma que esto es particularmente importante respecto a los ilícitos cuyo injusto se fundamenta en los contenidos de la información, como la pornografía infantil, la xenofobia, las acciones atentatorias contra la propiedad intelectual y la apología al terrorismo. La Red, señala el autor, no sólo facilita su difusión, sino también abarata los costes y favorece la comunicación entre personas afines (que siguiendo la idea de Castells, se agrupan socialmente en redes de contenido o accionar ilícito). ROMEO CASABONA, Carlos. "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político criminal", en ROMEO CASABONA, Carlos (Coord.). *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Granada: Ed. Comares, 2006, p. 4.

[21] MENDOZA BUERGO, BLANCA. *El derecho penal… op. cit.,* p. 27.

que produce una asignación difusa de responsabilidades (jurídicas y no jurídicas)[22]. Ciertamente disminuye su sensación de responsabilidad, lo que se genera tanto por la suma de una multiplicidad de acciones individuales como por la sistemática divergencia entre producción de riesgos y afectación por el mismo en sociedades funcionalmente diferenciadas[23].

c) Sensación de inseguridad subjetiva. El aumento de esta hace que se exija al sistema jurídico, principal aunque no excluyentemente al Derecho penal, tanto el aumento de la protección objetiva de la seguridad como de que esta misma se traduzca en un aumento de la sensación de seguridad subjetiva[24].

La red Internet participa de las características generales de la sociedad del riesgo y es, como se veía *supra*, uno de los nuevos riesgos de la era postindustrial. Su irrupción ha impactado drásticamente distintas áreas del quehacer social, provocando una revisión masiva de los distintos sectores del Derecho y una modificación progresiva de las relaciones de poder en la Red. Algunas de estas ideas se esbozarán a continuación.

II. INTERNET Y LAS TIC EN LA SOCIEDAD DE LA INFORMACIÓN Y EL RIESGO.

1. La tecnología y las redes.

Internet es el sistema nervioso de nuestra sociedad, y constituye la base tecnológica del modelo organizativo de la era de la información: la red[25]. De todas formas no debe pensarse que las redes son una propiedad

[22] Silva Sánchez recuerda que la construcción teórica de Beck descansa sobre la idea de que el trasfondo de todos los nuevos riesgos está en las decisiones humanas. A esto el español aporta que no solamente importa al Derecho y a la vida social en general las decisiones humanas que generan riesgos, sino también, y en igual medida aquellas que distribuyen estos riesgos. SILVA SÁNCHEZ, Jesús-María. *La expansión…op. cit.*, p. 16.

[23] MENDOZA BUERGO, Blanca. *El derecho penal… op. cit.*, p. 29.

[24] El hecho de que algunas de las fuentes generadoras de riesgos provoquen los efectos dañinos muchos años después de la ocurrencia del hecho riesgoso aumenta la sensación de inseguridad, pues el ciudadano intuye que se le causa un perjuicio, pero desconoce como y cuando se visualizará éste. Claro ejemplo es el de derrame de sustancias tóxicas en caudales de agua. Esto mismo produce además una elevadísima sensibilidad al riesgo, que lleva a que la apreciación subjetiva del mismo sea muchas veces mayor a la entidad dañina del factor de riesgo en si. SILVA SÁNCHEZ, Jesús-María. *La expansión…op. cit.*, p. 16.

[25] CASTELLS, Manuel. *La galaxia Internet*. Barcelona: Ed. Plaza y Janés, p. 15

exclusiva de la actual sociedad. Afirmar eso sería un craso error. Las redes en la morfología social humana existen desde antiguo. Principalmente se organizaban así con objetivos comerciales, así como también en el arte o en la política. Las alianzas bélicas no son sino redes con un objetivo político-militar específico. Todas ellas se enfrentaban con grandes escollos para coordinar sus movimientos, para concentrar recursos técnicos, humanos o económicos, y, finalmente, para la gobernación de la misma red[26].

Este es el modelo que ha comenzado a superarse, o mejor dicho, a transformarse, con la inclusión de las redes informáticas y telemáticas en la realidad social, principalmente desde la masificación de Internet. Esto ha permitido, por ejemplo, una gran capacidad de comunicación *on line* para la coordinación de los nodos integrantes de la red, lo que a su vez deriva en la flexibilización necesaria para la toma de decisiones y la desconcentración de recursos de todo tipo. Surge, en voz de Castells, "el desarrollo de una forma organizativa superior de la actividad humana"[27].

Las redes informáticas trasladan información. Esta es su materia prima, y como señala Sieber, además de ser un valor es un factor de poder y un peligro potencial[28]. Aprovechando los avances en la ciencia y la tecnología, la transmisión de la información a través de redes se hace a velocidades difícilmente comprensibles. Esto, junto a su flexibilidad y adaptabilidad, la transforman en una herramienta clave de la organización social actual y del ejercicio del poder.

Definir Internet puede ser una tarea tan titánica como infructuosa, pues a pesar de ser una red informática, es también una red que aglutina otras, y que en el proceso convergente de su evolución se ha transformado en "un poco de mucho y mucho de todo". Entender que es puede ser un ejercicio inabarcable para un artículo de unas pocas hojas como este, por lo

---

[26] "…las redes se vieron superadas como sistemas instrumentales por organizaciones capaces de concentrar sus recursos en torno a proyectos definidos de manera centralizada, y llevados a cabo mediante la ejecución de tareas en cadenas verticales y de mando. Las redes estaban circunscritas al entorno de la vida privada, mientras que las jerarquías centralizadas eran el feudo del poder y la producción". CASTELLS, Manuel. *La galaxia…op. cit.*, p. 16.

[27] Castells define Red como "un conjunto de nodos interconectados". A su vez, Nodo es "el punto en que una curva se intersecta a si misma. Lo que un nodo es concretamente depende del tipo de redes a que nos refiramos. *Ibíd.,* p. 16; *La sociedad red…op. cit.,* p.550.

[28] SIEBER, Ulrich. *The international handbook on computer crime: computer-related economic crime and the infringements of privacy*. Chichester: Ed. John Wiley & Sons, 1986.

que se saltará cualquier intento por hacerlo y se seguirá entendiendo, salvo que se diga lo contrario, como una gran red informática[29].

Una breve revisión de la historia y evolución de Internet también puede ayudar a generar luces sobre su naturaleza, características y desarrollo que serán útiles para entender las relaciones de poder que se dan en el ciberespacio.

2. Desde los ordenadores con camuflaje.

El 01 de Septiembre de 1969 podría señalarse como la fecha natal de Internet. La ARPA (*Advanced Research Projects Agency*) del Departamento de Defensa de EEUU emprendió una serie de medidas que buscaban situar a ese país a la saga de la tecnología militar mundial. Entre estas se encontraba una que buscaba crear una red de comunicaciones que no dependiera de un único mando central, sino que permitiera la comunicación directa e independiente entre sus nodos[30].

Los primeros nodos de esta red de ordenadores fueron universidades o centros de investigación universitaria que colaboran estrechamente con el Ministerio de Defensa. La red fue bautizada como ARPANET, y sus tres primeras líneas de acción fueron la comunicación militar, la defensa y la investigación científica. La característica estructural

[29] Valga para estos efectos la efectiva descripción que hace Graham de la Red, "para hacernos una idea de lo que es Internet, necesitamos imaginar una combinación de biblioteca, galería, estudio de grabación, cine, cartelera, sistema de correo, galería de compras, tabla horaria, banco, aula, boletín de club y periódico. Luego, deberíamos multiplicar esto por un número infinitamente grande y darle una diseminación geográfica ilimitada". GRAHAM, Gordon. *Internet. Una indagación filosófica*. Madrid: Ed. Cátedra, 2001, p. 33-34.

[30] Este objetivo se lograba conectando en red los ordenadores del sistema de defensa de ese país, utilizando una aplicación de conmutación de paquetes que permitía al mensaje enviado desde un punto/nodo de la red encontrar su propia ruta dentro de esta, para llegar a su destino, incluso segmentándose en el camino y rearmándose en algún punto del trayecto anterior a la salida. Desde la perspectiva militar, el objetivo era permitir que, ante un ataque enemigo, las unidades militares pudieran coordinar acciones defensivas aun a falta de un mando central que comunicara órdenes. Esta red se obtuvo del trabajo de una unidad del ARPA llamada IPTO (*Information Processing Techniques Office*), cuyo producto era un medio que buscaba compartir el recurso "tiempo *online*" entre ordenadores del centro. En el diseño de esta participó también la empresa privada, a través de la BNN, una corporación de informática aplicada.

de esta red es que se centraba en un punto de control ARPA y nodos conectados a este punto, pero conectados también entre si.

Hacia 1973 ya había 15 nodos acoplados, la mayoría de ellos universidades y centros de investigación. La idea siguiente era conectar ARPANET a otras redes de ordenadores, para dar sentido a lo que se entiende por "red de redes". Sin embargo, para que esto fuera posible técnicamente hablando, dichos ordenadores debían hablar un "lenguaje común", una especie de lengua franca que facilitara la comunicación entre máquinas y la emisión, recepción y ejecución de las instrucciones o mensajes puestos en circulación. Gracias a la colaboración de investigadores franceses y, nuevamente, de la empresa privada, este lenguaje común vio cuerpo en los TCP (*Transmisión Control Protocol*) y el IP *(Internets Protocol)* que pasaron a constituir el protocolo que aun se usa en Internet, el TCP/IP

3. Internet aparece en escena.

Por motivos de defensa en las comunicaciones militares, ARPANET fue dividida en dos redes: MILNET, que se mantuvo con usos estrictamente militares, y ARPANET-INTERNET[31], destinada principalmente a la investigación[32]. En Febrero de 1990, ARPANET fue clausurada y el centro de gravedad pasó a ser la NSFNET.

Durante la primera mitad de los noventa, los particulares (principalmente aquellos *hackers* que habían creado distintas aplicaciones para la nueva red), las universidades, los centros de investigaciones y las empresas comenzaron a implementar las condiciones necesarias para el tramo final del control por una sola entidad. Se abrían las puertas de la privatización y la masificación de Internet, merced de los avances tecnológicos que estaban implementándose[33]. La creación de la *World Wide*

[31] Esta nueva red se convirtió en el eje de otras redes, como CSNET o BISNET, y comenzó a ser gestionada por la NSF *(Nacional Science Foundation)* norteamericana, lo que significó prácticamente el alejamiento total de las entidades militares de Internet.

[32] Aunque parezca difícil de creer, también fue destinada desde sus inicios al ocio, pues los mismos investigadores usaban la red tanto para fines científicos como para compartir comunicaciones temáticas –se formaron grupos de seguidores de la ciencia ficción- y personales.

[33] Los computadores comenzaron a venderse con los hardwares y softwares necesarios para trabajar en red y el hipertexto permitió el intercambio de datos entre los ordenadores

Web,[34] junto al aumento en la venta de computadores debido principalmente a la baja en el precio de adquisición, la aparición de los navegadores que permitían a los usuarios moverse dentro de este nuevo espacio, mas unas décadas de experticia, mucha experimentación y las constantes mejoras en equipos y aplicaciones,

entregaban la moderna Internet lista para ser accedida por millones de usuarios a nivel mundial. La Red había llegado a la mayoría de edad[35].

4. La libertad en Internet.

La idea de que la Red es un espacio pleno de libertad cercano casi a la anarquía, tiene su origen en lo que Castells llama "ética *hacker"*[36], y que constituyó una parte importante de la motivación de quienes cimentaron, durante las décadas de los setenta y los ochenta principalmente, lo que es Internet hoy en día.

"La cultura de los productores de Internet dio forma a este medio", es la afirmación del autor al respecto[37], y esto se tradujo en que sus

---

conectados, gracias a la creación en el *Centre Européen pour Recherche Nucleaire* CERN suizo, de un nuevo formato para los documentos que se intercambiarían, el HTML (*Hypertext Markup Language*). Un nuevo protocolo de transferencia de hipertexto, el HTTP (*Hypertext Transfer Protocol*) y un sistema de direcciones para los recursos existentes en la red, el URL (*Uniform Resource Locutor*) fueron las bases del moderno Internet.

[34] Aclara Graham en todo caso que Internet y *World Wide Web*, aunque parezcan asimilarse, no son lo mismo. "El primero es un sistema electrónico de intercomunicación; la segunda es una forma de procesar y presentar información digital. Pero la distinción tiene cada vez menos interés, porque la web ha terminado por dominar Internet". GRAHAM, Gordon. *Internet. Una indagación… op. cit.*, p. 32.

[35] Historia y evolución de Internet en: CASTELLS, Manuel. *La galaxia… op. cit.*, p. 23-40; CASTELLS, Manuel. *La sociedad red…op. cit.*, p. 70-102; CEBRIÁN, Juan Luís. *La red*. 2ª Edición. Madrid: Ed. Taurus, 1998, p. 40-50.

[36] Cabe hacer presente desde ya que al utilizar el concepto "*hacker*", Castells hace alusión a un colectivo de personas que no es asimilable a la restringida visión de "delincuente informático", "pirata informático" o "experto en computadoras" que se transmite a través de los medios de comunicación masivos. La ética *hacker* se traduce en la realización de la pasión creativa y es la ideología central de la economía informacional, contraponiéndose a la "ética del trabajo", propia de la sociedad industrial, y que representa el trabajo como un deber que llevado a sus extremos otorga un carácter ennoblecedor a quien lo realiza (algo así como "hay que sufrir en el trabajo para ser digno"), CASTELLS, Manuel; HIMANEN, Pekka. *La sociedad…op.cit*. p. 59-60. Para más sobre ética *hacker*, véase CASTELLS, Manuel; HIMANEN, Pekka; y TORVALDS, Linus. *"La ética del hacker y el espíritu de la era de la información"*. Barcelona: Ed. Destino, 2002.

[37] CASTELLS, Manuel. *La galaxia… op. cit.*, p.51.

componentes de cooperatividad y libre comunicación han dado lugar a importantes innovaciones tecnológicas, así como también sirvió y sigue sirviendo de puente entre la tecnomeritocracia y los proyectos que surgen en el ciberespacio[38]. La creación de Linux es uno de los más claros ejemplos de la ética *hacker*. Un sistema operativo ideado por Linus Torvalds, bajo código abierto, y mejorado a través de los aportes de miles de internautas que lo descargaron, ocuparon y aportaron sus mejoras para compartirlas con los otros internautas y el creador original, y que al 2001 tenía ya unos 30 millones de usuarios a nivel mundial.

Sin duda un valor fundamental que se grafica aquí es la libertad, inherente a la cultura *hacker* y expresable en ejemplos como el anterior. Castells la asume como libertad para crear, para absorber los conocimientos disponibles y para redistribuirlos en la forma y en el canal elegido por el *hacker*. La libertad es un componente central de la filosofía y la visión del mundo –de Internet- y de su actividad como tal[39].

Sin embargo, dicha libertad como concepción tecnofilosófica no puede extenderse mucho más allá de la cultura *hacker* o de la tecnomeritocracia, y tampoco implica la falta o insuficiencia de regulación en la Red, o en las actividades que en ella se realizan. Es más, los principios de la ética *hacker* no rechazan el control en si, moviéndose ellos mismos por férreos principios provenientes de su ética. Esto no es otra cosa que el autocontrol, o mejor dicho, la autorregulación en su accionar en la Red.

La idea de una completa libertad en Internet no pasa de ser hoy en día, e insisto en ello, una mera declaración de buenas intenciones. Pensar y concebir el ciberespacio como una "tierra de nadie", un lugar sin control donde las ideas reguladoras y totalitarias del Estado no tienen cabida y donde los usuarios- internautas pueden ser lo que quieren, cuando quieren, y haciendo lo que se les antoje sin limitación alguna tienen más de idealismo romántico que de realidad concreta[40].

---

[38] *Ibíd.*, p. 56.

[39] CASTELLS, Manuel; HIMANEN, Pekka. *La sociedad…op. cit*., p. 88-89

[40] Quizás la máxima expresión de este romanticismo es la Declaración de independencia del ciberespacio, del ensayista norteamericano Jhon Perry Barlow, quien en su texto declama contra cualquier intervención estatal en la Red y la completa libertad de los ciudadanos en el ciberespacio, "el nuevo hogar de la mente". Véase http://es.wikisource.org/wiki/Declaraci%C3%B3n_de_independencia_del_ciberespacio, texto

5. Poder y control en la Red.

La realidad política, económica, jurídica, tecnológica y social actual muestra una situación que parece innegable: Internet es un espacio sujeto a las mismas regulaciones y expresiones de poder del espacio físico[41]. Lo que es lícito en el mundo real lo es también en el ciberespacio (o debería serlo al menos) y viceversa.

El ejercicio del poder en el espacio virtual ya no sorprende y las herramientas jurídicas abarcan buena parte de Internet como red informática y telemática, así como las conductas que allí ocurren. Un ejemplo (en negativo, axiológicamente hablando) lo representa China, donde Internet está configurada (manipulada se podría decir) para el control por parte del gobierno, que la utiliza a su favor imponiendo serias limitaciones a los usuarios de ese país. Como diría Lessig, allí se controla la arquitectura de la Red[42]. El mismo país, junto a otros como Egipto, Birmania, Pakistán o Irán tienen como punto en común el que, según observa la prensa internacional periódicamente, *bloggers* de todas partes del mundo y principalmente de esos países son investigados, acusados, detenidos o sentenciados por el material publicado en sus propias bitácoras *online*[43].

En Internet, como muestra el ejemplo recién citado, se producen constantes y progresivos conflictos de intereses que invitan a una mayor regulación, a un mayor ejercicio del poder. Esto se da así tanto por las características técnicas de la Red como por los sujetos que actúan allí.

Respecto a lo primero, puede considerarse su ingente cantidad de contenidos, entre los que se encuentran los considerados ilícitos y nocivos.

---

traducido al castellano. En profundidad sobre el documento, PÉREZ LUÑO, Antonio E. *La tercera generación de Derechos Humanos*. Cizur Menor: Ed. Aranzadi, 2006, p. 115-117.

[41] Cuestión distinta es el juicio valórico que se tenga sobre este hecho, es decir, que tan conveniente pueda considerarse que las esferas de poder y control aterricen en el espacio virtual, y que tan razonable sea que esto se haga a través de las normas jurídicas.

[42] LESSIG, Lawrence. *El código y otras leyes del ciberespacio*. Madrid: Ed. Taurus, 2001.

[43] La edición 2008 de los Juegos Olímpicos en Beijing, China, ha sido la comprobación a nivel mundial de las serias restricciones a la prensa en ese país, y a la prensa internacional, y las que los *bloggers* de ese país no escapan. Al respecto véase http://news.bbc.co.uk/2/hi/uk_news/wales/north_east/7373639.stm o http://es.noticias.yahoo.com/rtrs/20080709/tbs-Internet-myanmar-bloguero-a0280fe.html, entre otras.

Además esa misma masa puede ser comunicada a una gran velocidad y a una multiplicidad de personas en una ínfima cantidad de tiempo[44]. Esto es más peligroso aún considerando la altísima dependencia de la sociedad actual de la técnica y la automatización, y del tráfico de información y datos, lo que se hace predominantemente en Internet[45]. Y por si fuera poco, como señala Hassemer, la gente no nota la amenaza de las nuevas tecnologías, siendo esta invisible frente a la promesa de múltiples ventajas[46].

En relación al segundo de los puntos en comento, aparte de los usuarios, los privados y el Estado tienen un rol sumamente activo en el ciberespacio. En este último caso hablamos de una dualidad de roles pues, por una parte, es el Estado por antonomasia la entidad encargada de la protección de los derechos de las personas, pero al mismo tiempo tiene la capacidad de vulnerar dichos derechos. Silva Sánchez explica, a propósito del fenómeno expansivo del Derecho penal, que la intervención creciente en la esfera más íntima de los ciudadanos se explica, entre otros factores, por la continua disminución del rol del Estado como prestador de servicios

---

[44] El riesgo multiplicador contra bienes, derechos e intereses jurídicos, del que habla Pérez Luño, PÉREZ LUÑO, Antonio E. *La tercera...op. cit.*, p. 93, o la extraordinaria capacidad multiplicadora de acciones ilícitas, en términos de Romeo Casabona, ROMEO CASABONA, Carlos. *De los delitos…op. cit.*, p. 4. Gonzáles Rus en tanto habla de la superior dimensión lesiva de Internet en el marco de los delitos informáticos, al importar una lesión más extensa y/o intensa de los bienes jurídicos protegidos. No obstante no se trate esto, para el autor, de una característica exclusiva ni novedosa de Internet. GONZÁLEZ RUS, Juan José. "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", en GONZÁLEZ RUS, Juan José (Coord.). *Delito e informática: algunos aspectos*. Bilbao: Ed. Universidad de Deusto, 2006, p. 32-33.

[45] Mata atribuye justamente a esta característica la vulnerabilidad de los Derechos Fundamentales en el ámbito de Internet. MATA, Ricardo. "La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías". *Revista penal*. Nº 18, 2006. Barcelona: Ed. Praxis, p. 218. Estos nuevos usos de las tecnologías provocan lo que Pérez Luño ha denominado "contaminación de libertades", y que han generado el nacimiento de los Derechos Humanos de tercera generación, como la libertad informática. Sostiene él mismo que "la revolución tecnológica ha redimensionado las relaciones del hombre con los demás hombres, las relaciones entre el hombre y la naturaleza, así como las relaciones entre el ser humano con su contexto o marco cultural de convivencia. Estas mutaciones no han dejado de incidir en la esfera de los Derechos Humanos". PÉREZ LUÑO, Antonio E. *La tercera...op. cit.*, p. 28-29.

[46] Agrega el autor alemán que la decisión de una persona de automarginarse de la avalancha tecnológica lo dejaría al margen de la modernización, siendo las nuevas tecnologías una corriente contra la cuál apenas puede oponerse resistencia. HASSEMER, Winfried. "Sobre el previsible futuro de la protección de datos". *Revista de ciencias penales*. Vol. 2, Nº 1, 1999. Vigo: Ed. Asociación Española de Ciencias Penales, p. 257.

y factor activo de la economía, lo que da paso a un Estado policial[47]. Los privados, específicamente las empresas y corporaciones que tienen un activo rol en la Red a través de la captación, uso y comunicación de información y datos personales, también se han transformado en un agente amenazante a las garantías y derechos, toda vez que en muchos casos hay una preeminencia de sus intereses comerciales por sobre los de los ciudadanos[48]. Ni hablar cuando existe una asociación entre el Estado y las empresas en este ámbito, pues tiembla la seguridad de los ciudadanos respecto a sus datos personales[49].

Se produce así un conflicto multipartito de derechos e intereses entre las personas, el Estado y las empresas, donde las primeras buscan resguardar sus derechos y libertades fundamentales frente al accionar de privados y gobiernos, mientras estos últimos buscan el incremento patrimonial y el incremento en la seguridad, respectivamente. Todo en un marco jurídico que vive un proceso de adaptación a la realidad digital, que

[47] SILVA SÁNCHEZ, Jesús-María. *La expansión…op. cit.*, p. 150.

[48] Para Morón Lerma, el hecho que Internet esté dominada por los privados hace aún más necesaria la protección de los derechos de los usuarios, MORÓN LERMA, Esther. *Internet y…op. cit*., p. 105. Cfr., con Hassemer, para quien "la elaboración de datos en manos privadas no es menos peligrosa para la privacidad del ciudadano que la que está en manos públicas", lo que exige a su vez nuevas orientaciones en la protección de los datos de carácter personal. Para el alemán además el estándar de protección de los datos personales debería unificarse, evitando considerar la utilización de estos datos por los privados como una especie de mal menor. HASSEMER, Winfried. *Sobre el previsible…op. cit*., p. 255, 257.

[49] Como ilustración es posible citar el acuerdo al que llegaron el Gobierno de Chile y Microsoft Inc., en Julio del 2007, en el que la empresa norteamericana se comprometía a prestar apoyo a planes de digitalización del sector público chileno, a cooperar a través de becas y otros planes en la alfabetización digital, así como desarrollar proyectos de gestión en distintos frentes sociales y económicos, entre otros puntos. El Gobierno chileno en tanto asumía el compromiso de poner a disposición de Microsoft el apoyo de todo el aparato estatal, incluyendo entidades tan importantes, y críticas, como el Servicio de Registro Civil e Identificación, que tiene entre sus haberes los datos personales de los más de 15 millones de chilenos. Esto, y sin necesidad de ver bajo el agua, enciende las alarmas sobre la proximidad que la empresa de *softwares* tendrá con información personal de los chilenos, como el estado civil, antecedentes penales o bienes inscritos, entre otros. Para ver más detalles sobre las principales características y riesgos del acuerdo http://lamatriz.wordpress.com/2007/07/27/el-errorneo-acuerdo-del-gobierno-chileno-con-microsoft/ (última consulta 20 de agosto de 2008), o http://www.fayerwayer.com/2007/07/ciudadanos-chilenos-ahora-son-propiedad-de-microsoft-corporation/ (última consulta 20 de Agosto de 2008).

lleva a la construcción incluso de nuevos derechos y libertades[50], y la consecuente aparición de nuevos bienes jurídicos, muchos de ellos que reciben protección jurídico penal[51].

6. El tráfico de datos y contenidos como eje de las relaciones de poder en la Red.

Se hablaba *supra* de la dependencia que el mercado actual tiene de las tecnologías informáticas y del tráfico de información, contenidos y datos personales, cuestión evidente en Internet. La acumulación y el tratamiento de datos de carácter personal generan un creciente peligro para los derechos y libertades de los ciudadanos frente al Estado, las empresas y los mismos particulares[52]. Colisionan los intereses de protección de la ciudadanía y la seguridad de la nación a cargo del Estado, en su doble rol de protector y potencial vulnerador de la intimidad de los ciudadanos, con los intereses comerciales de aprovechamiento de los datos personales para el lucro por parte de las corporaciones, los intereses delictuales que con el mismo objetivo actúan al margen de la ley, y aquellos de los ciudadanos, que ven escapar tajadas de intimidad cada vez mayores merced de Internet y las TIC.

El juego de intereses que así se ha generado produjo una desestabilización en el centro tradicional del poder, y del poder jurídico específicamente, como es el Estado. La importancia de los datos de carácter personal y la amenaza de cierto tipo de información que circula por la Red, los denominados contenidos nocivos[53], en relación con la escasa efectividad

---

[50] Cfr., con la visión minimizadora de González Rus, quien reduce a un mínimo la injerencia de Internet en este sentido. GONZÁLEZ RUS, Juan José. *Precisiones conceptuales…op. cit.*, p. 30.

[51] En este sentido, la tensión está entre la regulación estatal y la libertad de expresión, información y el mercado. MORÓN LERMA, Esther. *Internet y…op. cit*., p. 30, 132-133.

[52] En este sentido, FERNÁNDEZ ESTEBAN. María Luisa. *Nuevas tecnologías, Internet y Derechos Fundamentales*. Aravaca, Madrid: Ed. McGraw-Hill/ Interamericana de España, 1998, p. 128; MORALES PRATS, Fermín. "Internet: riesgos para la intimidad", en AAVV. *Internet y derecho penal*. Madrid: Ed. Consejo General del Poder Judicial, Centro de Documentación Oficial, 2001, p. 70; MORÓN LERMA, Esther. "Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos", en GONZÁLEZ RUS, Juan José (Coord.). *Delito e informática: algunos aspectos*. Bilbao: Ed. Universidad de Deusto, 2006, p. 85.

[53] El origen del término contenidos nocivos y su distinción de los contenidos ilícitos proviene del Libro Verde sobre la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información, COM/96/0483 FINAL, sin publicar en el Diario Oficial. El contenido ilícito no presenta mayores problemas, pues lo ilícito o antijurídico es

que la regulación jurídica interna de cada Estado ha mostrado en el ciberespacio, han propiciado que el poder de controlar lo que ocurre en Internet abandone en parte al Estado para redistribuirse en otras instancias.

Cuáles son estas instancias y como se redistribuyen las cuotas de poder y control se verá en el siguiente capítulo.

III. EL ESCENARIO DE LAS RELACIONES DE PODER EN INTERNET.

1. El nuevo rol del Estado.

Para Castells, quien no es precisamente optimista respecto al papel que el Estado asume como entidad reguladora en la Red, existe una fuerte contradicción en las relaciones de poder existentes en Internet en el ámbito de su regulación, siendo el reto fundamental en la sociedad actual superar la "ausencia de actores e instituciones con capacidad y voluntad suficientes para asumir dichos retos"[54]

De las instituciones llamadas a "gobernar" en el ciberespacio, el Estado tiene un papel protagónico. Sin embargo, ese rol se mantiene aun algo difuso. Como indica Muñoz Machado, no es por que en el proceso de globalización el Estado haya perdido importancia o capacidad de gobernar, sus facultades se mantienen intactas. El asunto para el autor es que la globalización, y no se debe olvidar que Internet es el símbolo de aquel fenómeno y su instrumento mas eficiente, obliga al Estado a desarrollar nuevas estrategias y capacidades para no perder poder, y esa obligación aun no es del todo resuelta en el caso de la red más importante de todas[55].

---

un juicio de contraposición que dependerá del ordenamiento jurídico respectivo donde quiera averiguarse si un contenido es ilícito o no, sin obviar de todos modos los inconvenientes existentes en la aplicación de la ley penal. El problema lo da la definición de nocividad. En la doctrina, Santaella García-Royo entiende por contenido nocivo aquella "información presente en Internet que, amparada por la libertad de expresión es legal, aunque sea perjudicial para un determinado tipo de personas. Tal es el caso de la pornografía, que, aun siendo un tipo de información legal, es dañina para los menores. SANTAELLA GARCÍA-ROYO, Isabel. "Restricciones a la prestación de servicios", en CREMADES, Javier; GONZÁLEZ MONTES, José Luis (Coords.). *La nueva ley de Internet*. Madrid: Ed. La Ley, 2003, p. 185.

[54] CASTELLS, Manuel. *La galaxia… op. cit.*, p. 310.

[55] Claro que la respuesta a esta crítica es que el Estado no necesita desarrollar estas nuevas estrategias por que lo existente (normas, principios o instituciones) permite resolver el

El Estado moderno ha visto disminuido su poder, principalmente a partir del periodo posterior a la Segunda Guerra Mundial. A finales del siglo pasado este poder, sobre todo en cuanto a su facultad coactiva sobre determinadas conductas castigadas penalmente, ha aminorado también merced de los problemas que la informática, la telemática y la irrupción masiva de Internet le han presentado[56].

El problema no es que el Estado, y el Derecho, no puedan regular, sino que esta regulación está siendo poco efectiva, y aunque esto parezca de perogrullo mencionar, el valor de evidenciarlo es que el énfasis del estudio y las soluciones deben estar puestos no sólo en el Derecho sustantivo, sino en cuestiones más cercanas al Derecho procesal, asuntos de policía, de competencias de los Tribunales de Justicia y del cumplimiento de resoluciones judiciales, entre otras cosas.

En el ámbito de Internet, y del gigantesco mercado que esta ha abierto,[57] el Estado está compartiendo parte de su poder regulador con las grandes empresas que dominan las telecomunicaciones, tanto por capacidad técnica y económica como por el hecho de que el desarrollo de Internet está, a esta altura, de la mano de los privados más que del sector público. Sin embargo el Estado debe encontrar formas de regulación acordes a la nueva realidad tecnosocial, lo que implica que el Derecho debe acomodarse a esta realidad, como única forma de que los gobiernos no pierdan poder por no ser capaces de entrar al escenario de la globalización[58].

El Libro Verde sobre la Convergencia,[59] aunque implícitamente, mantiene la idea de la capacidad reguladora del Estado sobre la

problema sin inconvenientes. MUÑOZ MACHADO, Santiago. *La regulación de la red. Poder y derecho en Internet*. Madrid: Ed. Taurus, 2000, p. 96, 104.

[56] Ciertamente no son los únicos factores. Véase *supra* la sociedad del riesgo.

[57] Terceiro afirma esta visión al señalar que el Estado "con su asentamiento físico y espacial, reacciona con una gran lentitud ante la rápida evolución de las empresas multinacionales que, por su naturaleza, son más temporales que espaciales". TERCEIRO, José B. *La sociedad…op.cit.*, p. 225.

[58] MUÑOZ MACHADO, Santiago. *La regulación…op. cit.,* p. 96.

[59] COM/97/0623 final, no publicado en el Diario Oficial. Cabe mencionar que los principios sólo están orientados a la regulación del fenómeno convergente, esto es, las infraestructuras que contribuyen a crear los servicios de la sociedad de la información, y no los servicios en si, lo que podemos interpretar como principios válidos para la regulación de la arquitectura de la Red, (o de cómo se estructura en la UE).

infraestructura de redes. Sin embargo, al mismo tiempo entrega pistas suficientes para que el Derecho vaya adquiriendo un carácter mínimo, dando un paso hacia la flexibilización y la autorregulación principalmente[60].

Esto implica no otra cosa sino que el Estado ve actualmente como su aparato de poder se adapta a la nueva realidad tecnosocial y comparte el rol de control con otras instancias. Por una parte, se entrega una cuota importante de responsabilidad a los mismos usuarios de la Red, a través de la autorregulación. Por otra, y quizás aquí va lo más trascendente, comienza a ceder parte de su soberanía, compartiéndola con otros Estados. La causa de esto se encuentra en los problemas de investigación, juzgamiento y penalización que las TIC e Internet le espetan al Derecho interno.

El Derecho clásico del Estado posee las estructuras e instituciones suficientes para regular algunas de las cuestiones surgidas en el seno de la Red, pero es pobre, en mayor o menor medida, para regular otras que suponen transformaciones importantes a situaciones preexistentes a Internet, cuantitativa o cualitativamente. En muchos de los casos, sobre todo en lo relativo a ciberdelitos, datos personales, propiedad intelectual y pornografía infantil, el problema es en gran parte de eficacia de lo legislado, de la investigación policial y de lo resuelto por los Tribunales. Esto pues dichos fenómenos tienen componentes locales e internacionales al mismo tiempo[61].

El caso de los cibercrímenes es quizás el más emblemático al respecto, gracias a su impacto en los principios de jurisdicción y

[60] Para Graham, y en concordancia con los autores citados, la Internet agrega novedades al ámbito del Derecho, pero no necesariamente esto se traducirá en elementos normativos nuevos, "sólo aumenta la calidad, y quizás la cantidad de estos… por lo que es cuestionable que se regule más de lo que ya es como cualquier otro medio de comunicación". Aunque la intención de sus palabras pareciera menos drástica de lo que sugieren, el autor afirma que "la ley no tiene función alguna en Internet, aparte de la que tiene y ha tenido siempre en otros medios, respecto a los derechos de autor, el fraude, el libelo, el robo de la propiedad intelectual, etc.". GRAHAM, Gordon. *Internet. Una indagación… op. cit.*, p. 120, 128-129.

[61] La doble faz, en el caso de los ciberdelitos, se expresa en la persecución policial que perfectamente puede extenderse a través de varios países, tantos como involucrados puedan existir, sobre todo en redes delictuales. Esta sería la faz internacional, complementada con la faz local, que se refleja en cuestiones como el cumplimiento de la pena o medida de seguridad.

competencia del Derecho penal, como deja en evidencia Marchena, al señalar que "el delito en la Red y la sagacidad del delincuente cibernético ponen en cuestión la fragilidad de los sistemas penales tradicionales. Especialmente en cuanto a la determinación del *forum delicti comisi* ya que como se sabe la apreciación del lugar en que se ha producido el delito determina la jurisdicción competente"[62].

De ahí que, a continuación del supuesto que el Estado moderno no es suficiente, por si sólo, para regular o ejecutar lo regulado en cuestiones relativas a la Red, viene el supuesto de la interacción de los Estados como otro supuesto de heterorregulación[63].

2. La acción internacional conjunta.

Romeo Casabona afirma que "las nuevas manifestaciones de criminalidad en el ciberespacio exige su tratamiento jurídico penal desde una perspectiva internacional, pues la sola acción de los Estados, la aplicación de las leyes penales nacionales, se agota en su propio estado territorial, mientras que la Red es global y transnacional"[64].

Esta perspectiva internacional de la que habla Romeo Casabona tiene, eso sí, más de una salida, ya que en la idea cabe desde un Derecho Internacional para Internet hasta los acuerdos de tipo multilateral entre los Estados, pasando por la opción de Tribunales Internacionales especializados para la materia.

---

[62] MARCHENA GÓMEZ, Manuel. "Algunos aspectos procesales en Internet", en MARTÍN CASALLO-LÓPEZ, J. J. (Dir.). *Problemática en torno al fenómeno de Internet*. Madrid: Ed. Consejo General del Poder Judicial, 2000, p. 72-73.

[63] Lo defiende así Muñoz Machado, al señalar que "la disyuntiva sobre la regulación global intensiva o su olímpica ausencia debe resolverse a favor de complementar las desfallecientes posibilidades de los Estados, mediante fórmulas que… tendrán que ser necesariamente plurales". Plurales en el sentido de que los mecanismos utilizados para este fin, si bien desbordan al Estado como ente regulador, no lo suprimen. Es decir, sea a través de instituciones supranacionales o tratados internacionales, el Estado sigue siendo un eje importante en la regulación. El mismo autor afirma que "…el Estado sigue siendo una estructura de poder territorial insustituible para contribuir a una ordenación razonable de estos nuevos fenómenos económicos. Su acción debe ser complementada…pero no plenamente sustituida", MUÑOZ MACHADO, Santiago. *La regulación…op. cit.,* p. 108.

[64] ROMEO CASABONA, Carlos. *De los delitos…op. cit.,* p. 39.

La doctrina ha descartado la opción de un único Derecho internacional para regular la Red, una *lex mundialis*, ya que plantea varios problemas. Existe un gran inconveniente en cuanto a la imposibilidad empírica de aunar criterios en torno a lo ilícito y lo nocivo en Internet para todas las legislaciones. Esto produciría un Derecho sin las características necesarias que lo justifiquen: la uniformidad y la generalización[65].

Además con lo que cuesta promulgar una ley a nivel nacional, no es difícil pensar lo que costaría eso a nivel internacional, contrastado con lo fácil que mutan los problemas y las actividades en la Red. No sería extraño entonces imaginar que un problema tecnológico determinado, cuando logre encontrar una solución normativa internacional, ya haya dejado de ser problema, sea por haberse solucionado técnicamente, o por haber sido superado por un mecanismo superior[66].

El problema que en este sentido plantea Internet es un problema propio de la globalización. El fenómeno es a escala mundial, y las soluciones normativas han sido, en general, soluciones locales ancladas en lo territorial, y si la solución de una única normatividad global o un súper organismo internacional que regente Internet parece inviable, el acercamiento y la cooperación entre los Estados se vislumbra, a la luz de la práctica, como la alternativa más viable a la mera regulación jurídica estatal. Ahora, esto no significa prescindir completamente del Derecho internacional, sino contar con una capa levísima de este, con un Derecho internacional mínimo[67].

---

[65] Cfr. Hassemer, para quien es necesario el desarrollo de un Derecho penal internacional al menos en una parte, que traslade las agresiones a los Derechos Humanos al Derecho penal vigente y que implante las condiciones procesales necesarias para la persecución de tales agresiones, HASSEMER, Winfried. "Perspectivas del Derecho penal futuro". *Revista penal*. Nº 1, 1998. Barcelona: Ed. Praxis, p. 41. En similar sentido, y calificándolo como exigencia propia del Derecho penal del riesgo, en especial por los problemas generados vía TIC, como los "paraísos informáticos" (Jurisdicciones con bajo nivel de protección penal contra actividades delictuales en la Red y que son escogidos por los ciberdelincuentes como centro de operaciones). DE LA CUESTA AGUADO, Paz. "Sociedad tecnológica y derecho penal del riesgo". *Revista de derecho y proceso penal*, Nº 4, 2000. Navarra: Ed. Aranzadi, p. 142.

[66] "más que acreditar la idea de una *lex mundialis…* de lo que se trata es de discernir según áreas de problemas…y establecer un cuadro institucional y cooperativo complejo que pueda ofrecer respuestas adecuadas a las particularidades de cada uno de estos problemas". MUÑOZ MACHADO, Santiago. *La regulación…op. cit.,* p. 102.

[67] "…de momento…la forma más efectiva de regular la Red implica el ejercicio de la soberanía compartida por parte de los Estados nacionales, mediante la elaboración de Tratados Internacionales que incidan sobre la ordenación parcial del ciberespacio". LÓPEZ

La vía de los acuerdos entre Estados debe abarcar el núcleo de los comportamientos nocivos e ilícitos que se dan en la Red (datos, cibercrimen, pornografía o *spam*, principalmente), que sería el aspecto sustancial de los mismos, junto con las cuestiones procesales y policiales, sin los cuales lo sustancial no sería mas que una declaración jurídica de buenas intenciones[68].

Los ejemplos normativos europeos demuestran la efectividad en un ámbito supranacional de los esfuerzos legislativos comunes. El Convenio de cibercriminalidad (Cciber)[69] y la Decisión Marco 190/1 del 17 de Julio de 2002, Relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros,[70] conocida como la DM del euroarresto[71], son casos concretos de ello, al aunar los esfuerzos de los gobiernos europeos en el combate y la penalización contra el cibercrimen y otros delitos cometidos a través de las redes telemáticas.

Este CCiber se dicta en concordancia con la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 08 de Junio del 2000, relativa a determinados aspectos de los servicios de la sociedad de la información y el comercio electrónico en el mercado interior,[72] toda vez que el desarrollo del comercio electrónico en la UE va de la mano con el grado de confiabilidad que se logre entre sus agentes y usuarios, y esto va encadenado al control de los ciberdelitos. Su preámbulo reconoce expresamente la necesidad de cooperación rápida, acrecentada y eficaz entre los Estados firmantes, y entre estos y la empresa privada, con el objeto de llevar a cabo una política

---

ZAMORA, Paula. *El ciberespacio y su ordenación*. Madrid: Ed. Grupo Difusión, 2006, p. 148. Coincide Muñoz Machado, "…se contemplan como soluciones idóneas los acuerdos internacionales o supraestatales…capaces de proponer un derecho común". MUÑOZ MACHADO, Santiago. *La regulación…op. cit.*, p. 102, 108.

[68] La perspectiva entonces es mas menos clara, dicha en palabras de Muñoz Machado: "(El proceso de globalización) multiplicado gracias a la ayuda de las tecnologías de la comunicación, necesita ahora una regulación que se enfrenta a los mismo problemas que la ordenación mundial del tráfico en la gran red, a efectos de la protección de valores e intereses que los Estados habían consolidado y que deben seguir prevaleciendo". *Ibíd.*, p. 49.

[69] Convenio Nº 185 del Consejo de Europa adoptado por el Consejo de Ministros el 08.11.2001.

[70] DOCE L 190, de 17.7.2002, p. 1-18.

[71] Por ejemplo en QUINTERO OLIVARES, Gonzalo. "El euroarresto en la perspectiva europeísta de unificación de la justicia penal", en AAVV. *El derecho penal frente a la inseguridad global*. Albacete: Ed. Bomarzo, 2007.

[72] DOCE L 178 de 17.7.2000, p. 1-16.

común frente a la cibercriminalidad y proteger los legítimos intereses amenazados por el mal uso de las nuevas tecnologías.

Los objetivos principales del Cciber son: armonizar el Derecho penal material; establecer medidas procesales o cautelares adaptadas al medio digital; y poner en funcionamiento un régimen rápido y eficaz de cooperación internacional[73].

Cabe señalar que la armonización sustancial y procesal en la normativa contra la ciberdelincuencia era un objetivo perseguido por la UE ya desde el año 1989, con la Recomendación R (1989) 9,[74] y que se plasma en el Cciber como un esfuerzo para que las autoridades estatales encaren la volátil particularidad de la investigación de la ciberdelincuencia con un marco de reglas comunes que permitan su persecución eficaz[75]. Para Morón y Rodríguez este instrumento comunitario debe destacarse por su carácter pionero, atingente al fenómeno de la globalidad y flexible en dos sentidos, al respetar la tradición jurídica de los Estados miembros pero aun así ser idóneo para aprehender y responder al voluble fenómeno de la ciberdelincuencia[76]. Algunas de sus falencias en tanto han sido bien suplidas por otro instrumento importante en la iniciativa europea contra la delincuencia informática, la DM del euroarresto.

---

[73] El acuerdo supranacional busca unificar las legislaciones internas, específicamente en el ámbito de la sanción a conductas contra la confidencialidad, integridad y disponibilidad de los datos informáticos (artículos 2 al 6); las infracciones informáticas (artículos 7 y 8); las infracciones relativas al contenido, como aquellas vinculadas a la pornografía infantil y la propiedad intelectual (artículos 9 y 10), entre otras. Sobre los grupos de infracciones, véase MATA, Ricardo. *La protección penal…op. cit.,* p. 234-235; Otros aspectos del Convenio en MORÓN LERMA, Esther; RODRÍGUEZ PUERTA, María José. "Traducción y breve comentario del Convenio sobre cibercriminalidad", en *Revista de derecho y proceso penal*, Nº 7, 2002. Navarra: Ed. Aranzadi, p. 169.

[74] COUNCIL OF EUROPE. COMMITTEE OF MINISTERS; COUNCIL OF EUROPE. EUROPEAN COMMITTEE ON CRIME PROBLEMS. *Computer related crime: Recommendation N° R (89) 9 on computer related crime and final report of the European Committee on Crime Problems*. Strasbourg: Ed. Council of Europe, 1990.

[75] Lezertúa manifiesta sus dudas sobre ciertas medidas particularmente invasivas consideradas en el Convenio para la investigación de la ciberdelincuencia, especialmente las de los artículos 20 y 21 de dicha norma, que pone en entredicho el equilibrio entre los poderes de investigación y el respeto a las garantías fundamentales. LEZERTÚA, Manuel. "El proyecto de Convenio sobre el cibercrimen del Consejo de Europa- proteger el ejercicio de los derechos fundamentales en redes informáticas", en AAVV. *Cuadernos europeos de Deusto, Nº 25/2001.* Bilbao: Ed. Instituto de Estudios Europeos de la U. de Deusto, 2001, p. 109 y ss.

[76] MORÓN LERMA, Esther; RODRÍGUEZ PUERTA, María José. *Traducción…op. cit.,* p, 174.

Esta DM sustituye las relaciones clásicas de cooperación que prevalecían entre Estados miembros por un sistema de libre circulación de decisiones judiciales en materia penal. La orden de detención europea debe valorarse como la primera concreción, en el ámbito del Derecho penal, del principio del reconocimiento mutuo, que el Consejo Europeo ha calificado como piedra angular de la cooperación judicial. Quintero Olivares reputa la superación de la doble incriminación y la extradición existente en la UE como un paso imprescindible para alcanzar soluciones efectivas en el espacio judicial europeo[77]. Dicho paso se entiende como lógico en el marco de la unidad europea y de la colaboración entre los Estados miembros en la lucha de aquellos delitos de mayor peligrosidad.

El artículo 2.2 de la DM es el encargado de señalar los delitos que podrán ser objetos de una orden de euroarresto, siempre y cuando traigan adjunta una pena o medida de seguridad privativa de libertad igual o superior a 3 años. Los delitos de alta tecnología se encuentran en el listado del citado artículo, con lo que el aparato judicial de cada Estado de la UE cuenta con una herramienta de efectividad en la investigación y captura de los ciberdelincuentes, que muchas veces actúan al amparo de los paraísos informáticos o de legislaciones más benignas en la materia.

Siendo un avance respecto a la reglamentación por el Derecho interno individualmente considerado, la heterorregulación supranacional también adolece de defectos que no permiten dejar a su sola presencia la regulación total de la Red y las conductas que en ella se suscitan.

A modo de resumen, se puede mencionar en primer lugar el que una máquina normativa constituida a partir de la cooperación supranacional no sea capaz de responder con la suficiente rapidez frente a los embates tornadizos y acelerados que generan las tecnologías informáticas. Por otra parte, una excesiva producción de normas jurídicas, tal como sucede en el Derecho interno, genera un fenómeno del que se conoce perfectamente en la actualidad, la inflación normativa, que unida a deficiencias en la técnica legislativa, puede redundar en mayores problemas que soluciones a los problemas que la originan. En tercer lugar, la falta de órganos ejecutores también es un problema, que deviene en la necesidad de ocupar los Tribunales nacionales para hacer cumplir lo normado. Finalmente, y sin ánimo de ser taxativo, es posible mencionar la

[77] QUINTERO OLIVARES, Gonzalo. *El euroarresto…op. cit.*, p. 359.

necesidad de que exista una regulación "minorista", es decir, que se adapte a situaciones particulares, menores, altamente cambiantes y donde es necesaria la aceptación voluntaria de los normados más que la imposición de las reglas[78].

En este último punto, sobre todo, es donde aparece otro ejercicio de poder y control en Internet, la autorregulación.

3. El poder en manos de los usuarios.

Dos claves para entender la importancia y ventajas de la autorregulación son la flexibilidad y la adaptabilidad. Los mecanismos de este tipo presentan una serie de ventajas en relación con la regulación jurídica tradicional, como la rapidez de actuación y la elasticidad, así como la capacidad de integración y coordinación en el ámbito transnacional o supranacional. Esto constituye una vía de superación de los problemas que la globalidad y la falta de territorialidad de Internet plantean para el Estado moderno en el ejercicio de su poder y para la judicatura en la aplicación de la ley[79]. La autorregulación como medio de control en la Red deja en evidencia que sus principales características, como las ya citadas, son elementos propios de Internet, y que justamente el Derecho interno no posee o lo hace en mínimos grados.

Litan y Niskanen[80] entregan un listado de asuntos en Internet que podrían ser reguladas únicamente a través de privados. Entre estos cuentan la asignación de nombres de dominio, las funciones sobre firma digital, entidades de certificación, el control de algunos contenidos y el respeto a los derechos de la propiedad intelectual, entre otros. Para la regulación estatal se imputan funciones como vigilar la libre competencia, la regulación general de los contenidos de las telecomunicaciones, la contratación pública, la regulación de los impuestos, etc.[81]

---

[78] Muñoz Machado expone el acuerdo de Puerto Seguro entre Estados Unidos y la Unión Europea, MUÑOZ MACHADO, Santiago. *La regulación…op. cit.,* p. 182.
[79] LÓPEZ ZAMORA, Paula. *El ciberespacio…op. cit.,* p. 250.
[80] LITAN, Robert E.; NISKANEN, William A. "El horizonte digital: manual de directrices para la era digital". Cato Institute. http://www.elcato.org/publicaciones/libros/lib-2001-01-25.pdf, p. 14 y ss. (última consulta, 29 de Agosto de 2008).".
[81] MUÑOZ MACHADO, Santiago. *La regulación…op. cit.,* p. 60.

Una buena parte de este listado efectivamente se realiza por instituciones privadas de corte técnico, como la ICANN (*Internet Corporation for Assigned Names and Numbers*), a cargo de la asignación de nombres de dominio, o asociaciones de profesionales como la Asociación Española de Comercio Electrónico, cuyo Código Ético de Protección de Datos Personales en Internet busca sobremanera la protección de la información personal en las transacciones realizadas *online* y consideradas necesarias para el tráfico en el ciberespacio.[82] También los hay de carácter mixto, como la certificación, realizada tanto por organismos públicos como entidades particulares. Otras, por razones lógicas como su potencialidad de riesgo, han sido asumidas por la administración pública, tipificando figuras delictivas para la protección de los datos personales o del grupo infanto-adolescente, por ejemplo.

Pareciera que la autorregulación es casi de forma innata la modalidad de control más acorde a la realidad de Internet[83]. Esa necesidad del autogobierno y la autorregulación viene dada además por ese mismo carácter descentralizado ya visto, y por la desvinculación del concepto jurídico-material de fronteras. Es esta configuración la que invita a una regulación jurídica que se adapte a dichas cualidades, apareciendo en este plano la opción de la autorregulación, moldeable por esencia, como complemente perfecto de la regulación estatal, rígida y estacionaría.

---

[82] Gómez Castallo realiza una importante reseña a algunas de las iniciativas más destacadas de códigos de conducta en Europa y en EEUU. Se destacan, entre otras, el sistema TRUSTe, uno de los primeros sistemas de autorregulación norteamericanos que fijó reglas de conducta, sistemas de resolución de conflictos extrajudiciales y un sello de calidad para identificar sitios *webs* comprometidos con las políticas de protección de datos personales. Véase www.truste.org. En el Reino Unido, el *Better Business Bureau* lanzó el Código sobre prácticas comerciales en línea, que establece una guía de conductas éticas para las relaciones empresas-consumidores, a nivel nacional y transnacional, instituyendo cinco principios básicos para lograr el objetivo, entre los que se cuentan transparencia e identificación suficiente de las empresas y sus ofertas comerciales, y la protección de la infancia, entre otros (véase www.bbbonline.org). GÓMEZ CASTALLO, José D. "La autorregulación en Internet", en GÓMEZ SEGADE. José A (Coord.). *Comercio electrónico en Internet.* Madrid: Ed. Marcial Pons, 2001, p. 465-473. En detalle, véase RUIZ NUÑEZ, Mariola. "Códigos de conducta", en CREMADES, Javier; GONZÁLEZ M. José L. (Coords.). *La nueva ley de internet*. Las Rozas, Madrid: Ed. La Ley, 2003, p. 295- 308.

[83] Sobre este punto, Negroponte afirma con claridad que "una estructura descentralizada y altamente intercomunicada sería mucho más resistente y tendría mayores posibilidades de sobrevivir. Es mucho más duradera y tiene muchas más probabilidades de evolucionar en el tiempo". NEGROPONTE, Nicholas. *El mundo digital*. Barcelona: Ediciones B, 1996, p. 190.

Además de su flexibilidad, otra característica que condiciona la conveniencia de la autorregulación es la existencia de un mercado en la Red, cuyos elementos esenciales son los mismos del mercado "real", bajo las normas de libre competencia y el rol subsidiario del Estado. En Internet, el desarrollo del mercado y el de las tecnologías que en ella convergen está entregado en su inmensa mayoría a los privados[84].

La UE ha seguido ese camino, el de la regulación mínima y subsidiaria, principalmente por cuatro motivos. En primer lugar, el problema es territorialmente más basto que la sola UE. Luego, el mercado de Internet es altamente competitivo, por lo que una regulación mínima permite que se logren equilibrios por la acción de las mismas fuerzas que participan del mercado. En tercer lugar, por que la regulación centralizada no es la única vía para lograr uniformidad en un sistema normativo aplicable a un territorio determinado. Finalmente, por que las diversas formas de autorregulación de los sujetos actuantes en los mercados, y las normas privadas, cubran las necesidades de regulación en el ciberespacio[85]. El organismo europeo lo propuso como línea de acción prioritario en la Resolución de 24 de abril de 1997 sobre la Comunicación de la Comisión relativa a los contenidos ilícitos y nocivos en Internet[86], donde se instó a la Comisión a proponer, previa consulta al Parlamento, un marco común de autorregulación en el ámbito de la organización, y lo confirmó y profundizó en la Decisión Nº 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999, por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales[87]. En esta Decisión se considera que el fomento de la

---

[84] Aporta Muñoz Machado al respecto que "El Derecho de la Red tiene también que estar organizado en Red. Con múltiples puntos de apoyo y decisión, pluralmente, dando lugar a la participación de todas las comunidades de destino, con base territorial o sin ella, que utilizan la Red como instrumento de comunicación o para prestar o recibir servicios", agregando que "…esto rompe con la característica mas notable del Derecho público continental europeo desde el inicio del constitucionalismo: su carácter jerarquizado, vertical, ordenado a partir de la ley". MUÑOZ MACHADO, Santiago. *La regulación…op. cit.*, p. 59, 105.

[85] *Ibíd.*, p. 57-58.

[86] DOCE C Nº 150 de 19.5.1997, p. 38.

[87] DOCE L 33, del 6.2.99, p. 1-11, con sus respectivas modificaciones, además de la Decisión Nº 854/2005/CE del Parlamento Europeo y del Consejo de 11 de Mayo de 2005, por la que se crea un programa comunitario plurianual para el fomento de un uso más seguro de Internet y las nuevas tecnologías en línea, conocido como "Una Internet más segura plus" o "*Safer Internet plus*". Estas iniciativas promueven un uso más seguro de la Red, concientes de la

autorregulación y el desarrollo de medios técnicos como filtros o sistemas de clasificación proporcionados por la industria, entre otras medidas correctamente respaldadas por el ordenamiento jurídico, puede prevenir eficazmente a limitar el flujo de contenidos ilícitos en Internet[88].

La autorregulación implica que el Estado trasvasija a los usuarios, es decir, a los mismos sujetos que navegan, compran bienes, adquieren servicios, se comunican o simplemente curiosean en Internet, una cuota de poder y autonomía para ser sus propios "guardianes del templo", parafraseando a McLuhan. Estos tienen la posibilidad técnica y jurídica de hacerse con el control de situaciones en las que el Estado se ha dejado como *ultima ratio*. Más específicamente, el control entregado a los ciudadanos para el manejo de sus datos personales, por ejemplo, o de los contenidos nocivos que circulan por la Red, son una muestra palpable de cómo se transfieren responsabilidades a los particulares en consideración a que estos cuentan con factores técnicos para cumplirlas.

No puede obviarse por supuesto que los sistemas de autorregulación poseen una serie de desventajas que impide que sean considerados como la única forma de ejercer control en la Red. Estas desventajas, que pueden considerarse relativamente comunes tanto a la regulación de los mismos usuarios, sea por si mismos, a través de organizaciones vía Códigos de conducta o bien la hecha por las Organizaciones técnicas de la Red, como la Internet Society, son en gran

---

facilidad con que niños y adolescentes llegan a ella, y del importante rol social que juega. Por lo mismo se insiste en los controles técnicos y la autorregulación como medidas idóneas para lograr los objetivos propuestos. Llaneza González señala que con estas medidas "se pretende, únicamente, determinar la existencia de contenidos ilícitos y nocivos con el fin de restringir, en lo posible, su circulación, respetando la competencia de perseguir y castigar a los responsables de los contenidos ilícitos, que corresponde a las autoridades nacionales, policiales y judiciales, así como las diferencias existentes entre los diversos ordenamientos jurídico y culturales nacionales". LLANEZA GONZÁLEZ, Paloma. *Internet y comunicaciones digitales.* Barcelona: Bosch, 2000, p. 209.

[88] Considerandos número 5, 9, 10, 12 y 13 de la Decisión. El propio Consejo de la UE insta a los Estados miembros a fomentar sistemas de autorregulación como los filtros, creando sistemas de evaluación, como la norma PICS (*Platform for Internet Content Selection*. Las PICS funciona insertando etiquetas electrónicas en los documentos web, sean de texto o icónicos, y que señalan el contenido del documento. Dichas etiquetas son invisibles para el lector), establecida por el Consorcio 3W y la propia entidad supranacional, mediante las Conclusiones del Consejo de 17 de Febrero de 1997 relativas al Libro Verde sobre la Protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información, publicada en el DOCE C 70, del 6.3.1997, p. 4.

medida las mismas que los usos sociales y costumbres tienen en el "mundo real". Le falta de coactividad para hacer cumplir las normas es la principal, cuestión que se intenta minimizar con la autoaceptación de estas y las resoluciones que dicten organismos en el marco de los mencionados códigos, en base a la confianza en el sistema. También, en el caso de las normas que provienen de instituciones, se critica la falta de mecanismos, e incluso de intención, de hacer cumplir la normativa, aplicar sanciones o investigar la ocurrencia de hechos contrarios a los códigos[89]. Debe agregarse la falta de conocimiento de las normas por parte de los usuarios, o incluso de los miembros de asociaciones de profesionales, así como la falta de medidas disciplinarias[90]. Esa falta de conocimiento es un hecho verdaderamente imperdonable en Internet, donde la difusión es a costos ínfimos y la masificación enorme. Finalmente, organismos como la ICANN tampoco está exenta de críticas, y estas apuntan principalmente al nexo con el gobierno norteamericano, lo que implica un control soterrado de un solo país, al estar sometida a su Derecho (al Derecho del Estado de California y al Derecho nacional norteamericano)[91]. Junto con esto, falta aún una mayor representatividad y poder a los miembros de la GAC (*Gobernmental Advisory Comiteé)*, que son quienes representan a los distintos Estados en una red que es, como se sabe, transnacional[92].

---

[89] Marchena Gómez realiza una crítica indirecta a estas normas, al reprochar la falta de estudios de ciertos aspectos de la Red, señalando que "la tendencia –cada vez más extendida- a proclamar soluciones metajurídicas basadas en la firma de voluntaristas códigos de conducta, tampoco puede hacer entendible el llamativo silencio de los tratadistas". MARCHENA GÓMEZ, Manuel. *Algunos…op. cit.,* p. 52.

[90] "Sobre todo necesarias cuando las actividades de un miembro están en conflicto con la letra o el espíritu del código". LÓPEZ ZAMORA, Paula. *El ciberespacio…op. cit.,* p. 255.

[91] El mismo Muñoz Machado especifica que la ICANN está sometida a la supervisión del Departamento de Comercio norteamericano, lo que en última instancia, debido al acuerdo entre ambas entidades, obliga a la ICANN a ceder al mencionado Departamento todos sus derechos en relación con los registros y nombres registrados. MUÑOZ MACHADO, Santiago. *La regulación…op. cit.,* p. 113. En el mismo sentido, López Zamora agrega que cada año el Departamento ha realizado enmiendas al Memorando de Entendimiento firmado entre ambas entidades, exigiéndosele además a la ICANN que rinda cuentas al gobierno de EE.UU. sobre su gestión. LÓPEZ ZAMORA, Paula. *El ciberespacio…op. cit.,* p. 259.

[92] Respecto a su carácter democrático, Castells señala críticamente que "la visión romántica de una comunidad global de Internet representada por miembros de la misma mediante elecciones electrónicas debe atemperarse con la realidad de los *lobbies*, de poderosas redes de influencia y de la preponderancia de ciertos candidatos…en efecto, en la votación del 2000, tan sólo 35.000 de los 158.000 miembros participaron en la votación". CASTELLS, Manuel. *La galaxia… op. cit.,* p. 47. Aunque la ICANN, tal como la IANA (*Internet Assigned Numbers Authority*), sigue ligada al gobierno norteamericano, supera en representatividad a esta última gracias a algunos de sus organismos internos, como el Consejo de Directores, que es el principal órgano de administración de la entidad, compuesto por 21 miembros

IV. IDEAS FINALES.

El Estado se ha mostrado insuficiente para abarcar toda la gama de conductas y fenómenos ocurridos en Internet, pero sobre todo ha evidenciado debilidades en el cumplimiento y aplicación de sus normas, debido en gran parte a que el ciberespacio no conoce de fronteras territoriales. Surge entonces la alternativa complementaria de la regulación supra e internacional, concretada sobre todo en acuerdos multilaterales de cooperación que armonicen las legislaciones internas de cada Estado y establezcan mecanismos de cooperación que disminuyan las falencias del Derecho interno en ese punto. Dos buenos ejemplos de aquello en el ámbito penal son el Cciber y la DM sobre el euroarresto. La autorregulación funciona como un verdadero control social en la Red, con las ventajas y desventajas propias que se dan en el mundo físico. Si bien es rápida en su germinación, no posee la fuerza coactiva de las normas jurídicas. No obstante ello, se ha transformado en una instancia receptora de cuotas de poder que el Estado ha traspasado para poder afrontar técnicamente de mejor manera el aspecto delictivo y nocivo de la Internet. Finalmente, cabe destacar la importancia que las instituciones privadas de corte técnico adquieren en la regulación de Internet. Sus normas permiten la estandarización en los aspectos esenciales para la configuración, el funcionamiento y la evolución del ciberespacio. El papel de la ICANN en la gestión de los nombres de dominio es una muestra de un ámbito entregado de forma casi íntegra a los privados y que funciona eficientemente. Es necesario en último término una mayor coordinación de estas instancias institucionales con los gobiernos y organismos supranacionales, a fin de un actuar como frente común y una armonización de las legislaciones con respecto a las situaciones técnicas más complejas de la Red.

En suma, Internet y su alocado ritmo evolutivo han comenzado a cimentar nuevas relaciones de poder y control, fomentado en buena parte por la ingente cantidad de contenidos nocivos que circulan en la Red, y por el incesante tráfico de datos personales que circulan entre particulares, empresas y gobiernos. El Estado como máxima y monopólica expresión de

representativos (no igualitariamente) de todos los continentes. Además está el GAC, que está compuesto por miembros representativos de 101 países de los cinco continentes, además de nueve observadores, aunque a pesar de esto su carácter es más consultivo que decisorio. Véase organización y miembros en http://www.icann.org/general/board.html y http://gac.icann.org.

poder deja inexorablemente su pedestal solitario para compartirlo con los privados, los particulares, las entidades técnicas y los otros Estados, en lo

que es casi una metáfora cibernética de aquel viejo refrán que dice que "la unión (en la Red) hace la fuerza".