Delincuencia informática y control social: ¿excusa y consecuencia?[1]

Marcelo A. Riquert[2]

Sumario: I. Recordando anteriores Encuentros de la AAPDP. II. ¿Delitos informáticos o delincuencia informática? III. Las "oleadas" de reforma legal. IV. Normativa argentina y "Budapest": concordancias y carencias. V. Breve recordatorio de la evolución de la legislación nacional. VI. Reformando las primeras reformas. VII. ¿Hacia el "Estado Panóptico"? VIII. La inseguridad y las cámaras de vigilancia en espacios públicos. IX. Autoría y responsabilidad del proveedor de servicio. X. Cuestiones pendientes.

I. Recordando anteriores Encuentros de la AAPDP

Este trabajo retoma y amplía la tercera ocasión que tuve de referirme a esta problemática en el marco de los anuales encuentros de la Asociación Argentina de Profesores de Derecho Penal. La intención, sencillamente, es aclarar algunos puntos que pudieran haber quedado insuficientemente expuestos constreñido por el breve espacio temporal que brinda la participación en un panel, así como incorporar algunas novedades que habían "quedado en el tintero".

En cuanto a las anteriores ocasiones aludidas, la primera fue justamente en el encuentro fundacional, en el año 2001, en la Universidad Nacional del Litoral. En síntesis, había concluido en ese momento que era necesario actualizar nuestra legislación penal ante las novedosas formas de afectación de bienes jurídicos tradicionalmente protegidos por la rama punitiva del derecho. Esto se imponía tanto por la necesidad de respetar las demandas del principio constitucional de legalidad, como para evitar las ya por entonces numerosas divergencias interpretativas sobre el alcance de la redacción histórica de los tipos penales para aprehender las nuevas modalidades de ataque mencionadas, lo que traducía en una clara situación de inseguridad jurídica.

Además, señalé que, a la vez de actualizar, debía hacerse teniendo en cuenta la necesidad de armonizar nuestra legislación con la internacional para evitar "paraísos delictivos" o "santuarios de impunidad", teniendo en cuenta que se trata de conductas

---

[1] El texto retoma la conferencia *"Informática y derecho penal: ¿entre el control social y el delito?"*, interviniendo en el panel sobre *"Delitos Informáticos"*, junto a los profs. Nora Cherñavsky y Marco A. Terragni, en el XI Encuentro de la AAPDP, celebrado en sede de la Facultad de Derecho de la Universidad Nacional de Rosario, 2 de junio de 2011. En consecuencia, se ha prescindido de la individualización particularizada del aparato dogmático y fuentes que se citan, cuyo detalle mayormente puede encontrarse en la bibliografía de la monografía *"Delincuencia Informática en Argentina y el MERCOSUR"*, Ediar, Bs.As., 2009. Sí se han precisado citas posteriores y las correspondientes a las ampliaciones que se efectúan en este trabajo.

[2] Profesor Titular Regular a cargo de la Cátedra 01 de "Derecho Penal 1, Parte General", Facultad de Derecho de la Universidad Nacional de Mar del Plata.

que se desarrollan al amparo de un medio globalizado, siendo el primer paso natural en este camino el de hacerlo en el ámbito regional, más concreto, en el MERCOSUR. Precisamente, a relevar el estado de situación legislativa en sus miembros plenos y adherentes, dediqué la segunda ocasión, en el VI Encuentro, en 2006, en la Universidad Nacional de Mar del Plata.

En definitiva, nada demasiado novedoso habría en esta preocupación por la armonización ya que, como refiere Gonzalo Quintero Olivares, no es la primera vez que se enfrenta problemas que trasbordan fronteras[3]. Antes, por ejemplo, lo hicieron la navegación aérea y marítima, la telefonía y la telegrafía. Esto no debe hacer perder de vista que, comparativamente, el ciberespacio es cualitativa y cuantitativamente una realidad muy superior.

II. ¿Delitos informáticos o delincuencia informática?

No obstante la habitualidad con que se mencionan los "delitos informáticos" (de hecho, es el título que presidió el panel aludido), la existencia misma de la categoría es muy discutida. Sin temor a equivocación, sólo podría decirse que hay consenso en orden a reconocer que la informática se ha constituido como un factor criminógeno y que, naturalmente, en la medida en que se expande la "ciberpoblación", también lo hace su incidencia para que surjan nuevos autores, víctimas y objetivos.

Luego, ante la pregunta concreta *¿existen los delitos informáticos?*, básicamente hay dos respuestas:

a) Negativa: no hay ninguna noción que genere consenso y, por eso, se opta por hablar de "delincuencia o criminalidad informática", como suerte de categoría criminológica. Esta es la que vislumbro como tesis mayoritaria y con la que coincido. Como dice Quintero Olivares, de lo que se trata es de la aparición de nuevos modos de agresión, pero no de nuevos delitos, sin que esto implique negar la posibilidad de potenciar algunas conductas como el acoso (ciberbullying) o la discriminación (ciberhate u "odio cibernético")[4]. Así, recuerda Gil Belloni, la preocupación sobre estos aspectos corporiza en instituciones como la Anti Defamation League (ADL) o la internacional Network Against Cyber Hate (INACH), del año 2002[5], o en lo normativo en nuestro país, en la Ley 23592. En suma, siempre existió la actividad de acoso u abuso en el ámbito escolar entre adolescentes, sólo que antes estaba limitada por una cierta necesidad de presencia física, había que estar en el colegio para "sufrir" las cargadas, las bromas pesadas sobre algún "defecto" personal, pero vuelto al hogar o simplemente fuera del aula, era posible una suerte de "descanso". Hoy día, se vivencia una inédita posibilidad de intensificación de estas conductas disvaliosas en la medida que adolescentes y adultos jóvenes a través de las llamadas "redes sociales" han trasladado una significativa porción de su vida, de su sociabilidad, al ciberespacio, que se constituye entonces en una suerte de prolongación de la vida privada (al punto de hablarse de la era de la "extimidad"), derivando en la real imposibilidad de "retiro", en la inexistencia de un lugar donde refugiarse de la agresión, que se multiplica en el medio virtual.

---

[3] Quintero Olivares, "Internet y Derecho Penal. Imputación de los delitos y determinación de la competencia", pub. en "Estudios monográficos", N° 37, Año IV, abril de 2007, punto II.

[4] Ya citado, punto I.

[5] Ponencia de Agustina Gil Belloni en el mencionado XI Encuentro de la AAPDP (2011), titulada *"Auspicios y concreciones de la internet. Algunas reflexiones en torno a los delitos informáticos, con especial referencia al odio cibernético"*.

b) Positiva: habitualmente relacionada con un nivel de discusión previo, cual es el vinculado al reconocimiento de un "derecho informático" como rama autónoma del derecho. En estos casos, su admisión traduce lógicamente en el sostenimiento de un "derecho penal informático", que se ocupa de los "ciberdelitos" que, a su vez, tienen un bien jurídico protegido que le es propio, siendo para algunos la "información" en términos macrosociales y, para otros, la "pureza" de la técnica informática o la "seguridad informática"[6]. Finalmente, hay quienes postulan la protección de un "orden público tecnológico". Horacio Granero lo define como *"el conjunto de medidas tomadas por los poderes públicos, tendientes a organizar las relaciones de los usuarios de bienes o servicios tecnológicos con los responsables de su desarrollo o producción"* y Romo Santana afirma la necesidad y urgencia de aplicarlo como una política de estado[7].

Cierro este punto recordando que por la primera respuesta se ha inclinado el *"Convenio sobre Cibercriminalidad de Budapest"*[8] (2001), que no define "cibercrimen", sino que enumera nueve tipos de ofensas y exhorta a los Estados a contemplarlas como infracciones penales, las que sistematiza en cuatro grupos: infracciones contra la confidencialidad y disponibilidad de datos y sistemas, infracciones relativas al contenido, infracciones contra la propiedad intelectual y derechos afines e infracciones informáticas.

III. Las "oleadas" de reforma legal

Así como cuando se consulta acerca del desarrollo informático, en cuanto a lo tecnológico, se verifica usual su división en "generaciones"[9] que se corresponden con

---

[6] Esta se trataría, según destaca Luz María Puente Aba, de un concepto abstracto que se pretende tutelar para evitar que se lleguen a ejecutar múltiples comportamientos delictivos, ya sea que afecten la intimidad, el patrimonio, la integridad sexual, etc. Se configuraría un nuevo bien jurídico supraindividual espiritualizado que conglobaría los demás mencionados, *"de modo que se castigaría ya la lesión del bien supraindividual para conjurar el peligro creado para los demás bienes jurídicos"* (ej.: la tipificación del intrusismo como "norma obstáculo").} Alerta que se trata de una construcción ya empleada al tipificar los delitos contra los consumidores, contra los derechos de los trabajadores o contra la salud pública y se comparte su advertencia y propuesta en cuanto a ser reacios a este orden de propuestas (en su trabajo *"Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿debe protegerse de forma autónoma la seguridad informática?"*, pub. en AAVV "Nuevos retos del Derecho Penal en la era de la globalización", Patricia Faraldo Cabana directora, Tirant lo blanch, serie Alternativa, Valencia, 2004, págs. 399/400 y 409).

[7] Cf. cita José Luis Romo Santana, en su trabajo "Ciberterrorismo. Terrorismo a la luz de las nuevas tecnologías", pub. en la biblioteca jurídica virtual "elDial.com", Suplemento de Derecho de la Alta Tecnología, edición del 9 de marzo de 2011, ref.: DC153A.

[8] En vigor desde el 1/7/04, tiene un protocolo adicional del 28/1/03 sobre lucha contra el racismo y la xenofobia por Internet. Si bien el Convenio es una iniciativa de la Unión Europea, ha sido firmado por numerosos países extracomunitarios, como Estados Unidos o Japón. Argentina adhirió en 2010, pudiéndose mencionar del margen latinoamericano también a Costa Rica, República Dominicana, México y Chile.

[9] La primera corresponde con la válvula (década del '40), la segunda con los transistores (1959), la tercera con el circuito integrado (1964), la cuarta con el microprocesador (1974), la quinta con la interconectividad o intercomunicabilidad (década del '80). Hay quienes marcan el cambio de milenio como punto de inflexión para una sexta generación, la de la inteligencia artificial.

También es habitual el recurso de diferenciar "generaciones" para marcar diferencias entre los llamados "nativos digitales" y los "inmigrantes digitales". En su ponencia en el XI Encuentro de la

algún descubrimiento de significación para constituirse en suerte de hito o mojón que marca un salto cualitativo, si desviamos la mirada hacia su consideración jurídica, desde la sistematización que formuló Sieber suele distinguirse "oleadas" de reforma legal.

El profesor alemán individualiza cuatro: la primera, a comienzos de la década del '70, correspondió a la protección de la privacidad; la segunda, a comienzos de la década del '80, se vinculó a la represión de delitos económicos cometidos mediante ordenadores; la tercera, en el segundo segmento de la misma década, se ocupó de la protección de la propiedad intelectual en el campo de la informática; finalmente, la cuarta, ya en la década del '90, abarcó las reformas procesales atinentes a todo lo relativo con la adquisición, preservación y validación en juicio de la prueba en entorno digital.

En lo personal, coetáneo con el fenómeno de proliferación a escala global de legislación antiterrorista producto de los atentados en Nueva York y Washington del 2001 (comenzando con la llamada "Patriot Act"), he planteado la aparición de una quinta etapa que corresponde a la que se presenta como lucha contra el "enemigo" terrorista y la consolidación de un "panóptico tecnológico". Ha tornado usual encontrar trabajos referidos al "hacktivismo"[10] o al "ciberterrorismo"[11] –podría decirse que, muchas veces, carecen de rigor conceptual–, así como noticias sobre una "nueva guerra fría" o la "guerra de los códigos", por los ataques virtuales que recibieron agencias y organismos gubernamentales estadounidenses[12], siendo casos paradigmáticos el affaire "WikiLeaks"[13] y "Anonymous"[14].

AAPDP (titulada "*La eficiencia de la ley 26388 de reforma en materia de criminalidad informática al código penal de la nación*"), Carlos C. Sueyro nos recordó la identificación como "generación X" para los nativos entre 1970 y 1981, que vieron los primeros pasos del desarrollo digital; "generación Y", de 1982 a 1992, que crecieron con la popularización de las PC, los videojuegos o los celulares; "generación Z", de 1993 a 2004, que asumen como "natural" el mundo informatizado actual.

10 Sería, conforme Sebastián Masana, la convergencia del hacking con el activismo social o político, incluyendo la desobediencia civil electrónica, que se trataría del traslado al ciberespacio del concepto tradicional de desobediencia civil (cf. Romo Santana, ya citado, quien con idéntica fuente indica que el ciberterrorismo podría tener su origen en el hacktivismo cuando persigue fines políticos). Por su parte, Miguel Ángel Cano Paños, sostiene que el ciberespacio se ha convertido en muchos sentidos en un nuevo escenario de conflicto cuando se asocia a la amenaza que viene constituyendo el terrorismo islamista de base yihadista, señalando que internet ha pasado a ser un espacio ideal para las actividades de reclutamiento y radicalización, en particular, por su fácil acceso, poco o ningún control gubernamental, el anonimato en las comunicaciones, el rápido flujo de información, un público potencialmente enorme y una difusión a nivel planetario (en su trabajo "Internet y terrorismo islamita. Aspectos criminológicos y legales", pub. en "Eguzkilore", San Sebastián, N° 22, diciembre de 2008, pág. 88).

11 Ignacio José Subijana Zunzunegui, señala que para una mayor precisión conceptual, el cibeterrorismo puede ser analizado desde una perspectiva final o medial. La última, viene definida por el Consejo de Europa como la forma de terrorismo que utiliza las tecnologías de la información para intimidar, coaccionar o causar daños a grupos sociales con fines político-religiosos. En cuanto a la perspectiva final, define al ciberterrorismo como el ataque ilegal contra ordenadores, sus redes y la información contenida en ellas cuando se lleva a cabo con la finalidad de coaccionar a un gobierno o a su población para conseguir objetivos políticos o sociales. Integrando ambas, llega al siguiente concepto: ciberterrorismo es "cualquier acto realizado a través de tecnologías de la información que pueda lograr directa o indirectamente causar terror o generar daños significativos a un grupo social o político a través de la destrucción del soporte tecnológico de cualquiera de sus estructuras fundamentales" (en su trabajo "El ciberterrorismo: una perspectiva legal y judicial", pub. en "Eguzkilore", N° 22, San Sebastián, diciembre de 2008, págs. 172/173).

12 Así, la sección "Ciencia" del diario "Perfil", en su edición del 14/8/11 (pág. 40), encabeza "Nueva amenaza global" y titula "Argentina lanza un plan contra el cibercrimen", en una nota que resume con el copete "En medio del desconcierto que generan los ataques de grupos de hackers a distintos

Entre quienes formulan advertencias en este sentido puede contarse a Quintero Olivares, cuando enfatiza que la red brinda posibilidades inmensas a los hackers, pero aún más a los servicios de investigación de los Estados, recordando que en 2006 el Tribunal de Justicia de las Comunidades Europeas anuló una decisión del Consejo relativa a un acuerdo entre la Unión Europea y Estados Unidos para que este último tenga acceso electrónico a los datos contenidos en el sistema de reservas y control de salida de las aerolíneas comerciales, como medida preventiva contra el terrorismo y el crimen organizado. Justamente en este país, a través del "SWIFT" (Sociedad para la Telecomunicación Financiera Interbancaria Mundial), se espían aproximadamente once millones de transferencias bancarias diarias so pretexto de combate al terrorismo[15].

IV. Normativa argentina y "Budapest": concordancias y carencias

Siendo que el citado "Convenio sobre Cibercriminalidad de Budapest" se ha constituido en una referencia insoslayable en términos de armonización legislativa en la materia, sin perjuicio de volver luego con mayor detalle, puede anticiparse que nuestro país no tiene al presente mayor problema en lo referente al derecho penal sustantivo ya que, mediante la ley 26388 del año 2008, ha realizado una extensa reforma del Código Penal que, unida a otras que la precedieron, conforma un cuadro que abastece los requerimientos de aquel, sin que esto importe negar algunas pequeñas discrepancias.

En lo fondal, el convenio también incluye previsiones sobre la tentativa, la complicidad, la responsabilidad penal de las personas jurídicas y las penas, sugiriendo la adopción tanto de privativas de libertad como pecuniarias.

Es en lo adjetivo o formal donde puede advertirse un déficit significativo en la normativa nacional[16]. El convenio prevé reglas relativas al ámbito de aplicación (art. 14), condiciones y garantías (art. 15), competencia, conservación inmediata de datos, preservación de datos incluidos los de tráfico[17] (art. 16), registro y decomiso de datos informáticos almacenados (Título 4 de la Sección 2°), recogida en tiempo real de datos informáticos y datos de tráfico (art. 20), interceptación de datos relativos al contenido (art. 21), cooperación (cuyos principios generales enuncia el art. 23), colaboración y asistencia internacionales en investigación (art. 31) y medidas cautelares (art. 29; incluyendo en su art. 35 la llamada "Red 24x7", es decir, constituir un punto de

---

organismos oficiales del mundo, se acaba de crear el Programa Nacional de Ciberseguridad". Este programa para la seguridad digital (Programa Nacional de Infraetructuras Críticas de Información y Ciberseguridad), por decisión de la Jefatura de Gabinete del 2 de agosto depende de la Oficina Nacional de Tecnologías de Información (ONTI).

13 La versión local del fenómeno WikiLeaks ha sido el blog "Leakymails".

14 Se trata de un movimiento internacional, sin líderes, cuyo lema es *"El conocimiento es libre. Somos Anonymous. Somos Legión. No perdonamos. No olvidamos"*. Se declararon enemigos de los enemigos de WikiLeaks y, en apoyo a Julian Assange, atacaron los sitios web de Visa, Mastercard, Sony o Amazon, entre otros, saturándolos de peticiones hasta bloquear los servidores y lograr la suspensión del servicio. En España, manifestaron contra la ley Sinde, usando las caretas de Guy Fawkes, popularizadas en la película "V for Vendetta" (fuente: *"Anonymous, ¿quiénes son y cómo actúan?"*, disponible en http://www.rtve.es/noticias/20110610/anonymous-quienes-son-como-actuan-438765.html).

15 Antes citado, punto III.

16 Ccte.: Sueyro, ya citado, conclusión sobre "limitaciones" N° 3.

17 En Argentina se reguló por Ley 25873, con la excesiva previsión de guarda por el plazo de diez años, habiendo sido declarada inconstitucional por la CSJN en el caso "Halabi", sentencia del 24/2/09.

contacto las 24 horas del día, los 7 días de la semana) o a la extradición (art. 24). Al presente, nuestra regulación del derecho al secreto de las comunicaciones y su limitación, es *"insuficiente y asistemática"*, para hacer propia la descripción que formula Esther Morón Lerma respecto de la situación en el derecho español[18].

Aún inmersos en el país y en la región en un fenomenal proceso de reforma de la legislación procesal que incluye el masivo abandono de los códigos de cuño inquisitivo o mixto (inquisitivo mitigado) y la migración hacia sistemas acusatorios, estos nuevos códigos de última generación siguen ofreciendo en su diseño de los capítulos dedicados a los medios de prueba reglas anacrónicas, normas que reproducen el texto de las viejas que vienen a sustituir, omitiendo la mayoría toda referencia a la adquisición, preservación y validación en juicio de la evidencia digital. De tal suerte, lo relativo a las comunicaciones a través de Internet, cómo intervenirlas, por quién, con qué límites, etc., sigue librado a la "inspiración" del operador judicial de turno.

En una y otra jurisdicción se reproducen las discusiones acerca de la necesidad o no de contar con autorización judicial para el pedido de informe sobre datos de tráfico[19], la validación o no del registro de llamadas de un celular en un procedimiento o la consulta de su agenda de contactos por un Fiscal o la prevención policial. La toma de conocimiento del número IP (Internet Protocole) de una máquina que accede a la red permite luego solicitar la identificación personal al proveedor de servicio. A través de los números IMSI (Internacional Mobile Subscriber Identity) e IMEI (Internacional Mobile Equipment Identity), es posible obtener información de sumo interés acerca del usuario y ubicación del equipo en un determinado momento, que puede servir tanto para corroborar como descartar una coartada o versión durante el curso de la investigación de un hecho. Sin perjuicio de alguna regla genérica[20], en muchos casos, se sigue sin tener regulado el por quién, cuándo, con qué límites y cómo requerir este tipo de datos[21].

Sin perjuicio de que la definición clara sobre si el secreto de las comunicaciones comprende sólo el contenido o también incluye el proceso de comunicación (esta última

---

[18] En la primera conclusión de su trabajo titulado *"La restricción del derecho al secreto de las comunicaciones: algunos supuestos controvertidos"*, pub. en AAVV "Garantías penales en Argentina, España y sus sistemas de inserción regional", García Rivas-Riquert directores, Ediar, Bs.As., 2011, pág. 508.

[19] En fallo del 12/5/11, causa, "B.G. s/nulidad", la Sala VI de la CNCyCorreccional, declaró la nulidad del control de llamadas entrantes y salientes de un celular ordenado por un Agente Fiscal sin autorización judicial previa, invocando el art. 236 2° párr. del CPPN.

[20] Como podría ser el art. 229 del CPPBA, "Intervención de comunicaciones telefónicas", que dice: *"El Juez podrá ordenar a pedido del Agente Fiscal, y cuando existan motivos que lo justifiquen y mediante auto fundado, la intervención de comunicaciones telefónicas del imputado* ***y las que realizare por cualquier otro medio****, para impedirlas o conocerlas"* (el resaltado en negrita es personal). El art. 236 del CPPN, cuyo primer párrafo es similar (aunque sin necesidad de pedido fiscal ya que el Juez instruye), incorporó un 2° párrafo en 2003 por Ley 25760, que dice: *"Bajo las mismas condiciones, el Juez podrá ordenar también la obtención de los registros que hubiere de las comunicaciones del imputado o de quienes se comunicaran con él"*.

[21] Ilustra el estado de situación en España el trabajo de la profesora de Valencia, Paz Lloria García, *"El secreto de las comunicaciones: su interpretación en el ámbito de los delitos cometidos a través de Internet. Algunas consideraciones"*, pub. en AAVV "La protección jurídica de la intimidad", Javier Boix-Reig, director, y Ángeles Jareño Leal, coordinadora, Iustel, Madrid, 2010, pág. 170 y ss., cuya lectura se recomienda.

parece ser la tesis más razonable[22]), no es un problema exclusivo del derecho penal, no puede dejar de llamar la atención en la actualidad la existencia de una clara línea jurisprudencial contradictoria entre los fueros del trabajo y penal en materia de admisión y validación de actividades de control por el empleador del uso por el dependiente de los medios informáticos facilitados para el desempeño de la tarea laboral específica. No resulta inusual que se consideren despidos con justa causa casos en los que el empleador ha realizado un control particular del uso de herramientas como el correo electrónico por el empleado, ingerencias que trasladadas al fuero penal son consideradas nulas e, incluso, fuente de promoción de causas contra el que realizó la actividad intrusiva mencionada.

Corroborando similar percepción en derecho comparado, la citada Morón Lerma señala que la ausencia de reglas de juego claras sobre las intervenciones de las comunicaciones electrónicas contribuye a que se produzcan injerencias en el derecho al secreto de las comunicaciones especialmente controversiales, entre las que destaca justamente a las que se producen en ámbito laboral, donde el poder de fiscalización es interpretado por la jurisprudencia y los empresarios en sentido amplio y altamente permisivo en lo que a modalidades y alcance del control se refiere, en gran parte, debido a los déficits legales mencionados[23].

V. Breve recordatorio de la evolución de la legislación nacional

Retomo el estado de la legislación sustancial argentina. En ocasión del 1° Encuentro de la AAPDP, individualicé como normas que se habían referido especialmente a la incidencia del medio informático en diversas conductas delictivas a las siguientes: a) Ley 24766 (1997) de *"Confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos"*, que consagró una figura de violación de secreto de empresa; b) Ley 24769 (1997), que estableció el vigente régimen penal tributario y previsional, en el que incorporó como art. 12 la figura de alteración dolosa de registros fiscales incluyendo a los que estuvieren en soporte informático; c) Ley 25036 (1998), que modificó la vieja Ley de Propiedad Intelectual 11723, agregando como objeto de protección a los programas de computación; d) Ley 25286 (2000) de "Protección de Datos Personales", que modificó el Código Penal incorporándole los arts. 117bis y 157 bis; e) Ley 25506 (2001) de "Firma Digital", que modificó también el

---

[22] La citada Paz Lloria García recuerda que es doctrina constitucionalmente asentada en España que el derecho al secreto abarca tanto el contenido comunicado como al proceso de la comunicación (ob.cit., pág. 183; ccte.: Eliseu Frígols i Brines, en su trabajo *"La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto a la intimidad a la luz del uso de las nuevas tecnologías"*, pub. en AAVV "La protección jurídica de la intimidad", Javier Boix-Reig, director, y Ángeles Jareño Leal, coordinadora, Iustel, Madrid, 2010, págs. 47/48). Señala además la nombrada que se trata de una toma de posición que se compadece con la emitida por el TJCE, en sentencia de 29 de enero de 2008, caso "Promusicae", donde dijo que no existe obligación por parte de los proveedores de servicios, de proporcionar los datos de identificación que se corresponden con cada IP para proteger o averiguar los ilícitos civiles cometidos a través de intercambio de archivos P2P. Promusicae pretendía tal individualización de Telefónica para poder iniciar acciones civiles. Telefónica se negó a proporcionar los datos relativos a las direcciones IP, alegando que sólo estaba obligada a hacerlo en el marco de una investigación criminal o en un proceso para la salvaguarda de la seguridad pública y de la defensa nacional, pero nunca en el marco de un proceso civil (pág. 184).

[23] Trabajo citado, pág. 509.

C.P. incluyendo el art. 78bis por cuya vía se ingresó la consideración de la firma y el documento digitales.

En el lustro transcurrido hasta el VI Encuentro se agregaron: a) la incorporación al art. 173 del C.P. del inciso 15, por vía de la Ley 25930 (2004), referido a la defraudación mediante el uso de tarjeta de compra, débito o crédito; b) la regulación del servicio de comunicaciones móviles mediante Ley 25891 (2004), que incluyó figuras penales entre sus arts. 10 a 13 relacionadas con el ilegal uso de telefonía celular, módulos de identificación removible de usuario *"o la tecnología que en el futuro la reemplace"*.

Por último, al presente, podrían mencionarse, en modo indirecto, una cierta restricción a la penalización de afectaciones a la propiedad intelectual mediante la Ley 26285 (2007), que estableció la eximición de pago de derechos de autor en sistemas especiales para ciegos y personas con otras discapacidades perceptivas y, en forma directa y masiva, la reforma al C.P. por Ley 26388 (2008), que producto de la conjugación de 16 proyectos que estaban en estudio en el Congreso, concreta la derogación de dos artículos y la modificación, sustitución o incorporación de doce.

En el mínimo espacio de esta intervención sólo puedo destacar que, en lo central: a) se fijó un nuevo epígrafe al cap. III del Título V (Delitos contra la libertad): "Violación de secretos y de la privacidad", modificando el art. 157 (proporcionar o revelar información registrada secreta) y el art. 157 bis (acceso ilegítimo a banco de datos personales e inserción ilegítimas de datos personales), al que agregó parte del derogado tipo del 117bis; b) la derogación del art. 78 importó, con algunos retoques, el traslado de su texto como los nuevos tres párrafos finales del art. 77 (conceptos de documento, firma/suscripción, instrumento privado y certificado digitales); c) una nueva modalidad de defraudación informática se incorporó como inc. 16 al art. 173; d) se modificó el art. 128 para aprehender más allá de toda duda la ciberpornografía infantil; e) se adecuó la redacción del tipo de daño del art. 183 y se sustituyó el art. 184, incluyendo dentro de su objeto al producido en datos, documentos, programas o sistemas informáticos; f) en materia de comunicaciones electrónicas se modificaron los arts. 155 y 197; g) se incorporó la figura del intrusismo informático con el nuevo art. 153bis.

VI. Reformando las primeras reformas

No obstante haber anticipado que hoy día nuestro estado de situación en derecho fondal es más que aceptable y se ajusta en general a las recomendaciones del Convenio de Budapest, puede vislumbrarse una suerte de segunda oleada reformista que afectaría las primeras modificaciones sistematizadas en el punto anterior. Así, mientras las incorporadas por leyes 25286 y 25506 han sido derogadas, se propone otra reforma al régimen penal tributario incorporándole un nuevo tipo vinculado a la afectación de los controladores fiscales, que sería el art. 12 bis, que pareciera en principio innecesario si se atiende adecuadamente a la incidencia de la Ley 26388.

A su vez, no son pocos los que proponen la puesta en estudio de una posible modificación al régimen de la propiedad intelectual, en particular, para definir posición en torno al fenómeno del intercambio de archivos P2P que, superada ya la primera generación (la de "Napster", cuyas notas distintivas eran la centralización, el almacenaje de archivos, la intermediación, reproducción y comunicación pública), en la segunda, caracterizada por la descentralización técnica y económica que significa que la descarga e intercambio se haga en forma directa entre usuarios, ofrece como problema justamente la pretensión de punición de estos. Para brindar una mínimo noción de su extensión, la Unión Europea en 2008 estimó que, mientras se vendieron legalmente online dos

millones de canciones, fueron intercambiadas por afuera dos mil millones[24]. De tal suerte, es esta actividad de reproducción no autorizada la que preocupa a la industria con más gravedad, aún más que otra de mayor visibilidad como los CDs y DVDs "truchos" o pirateados que comercializan los "manteros" en la vía pública. Esta última modalidad de distribución y venta es un problema compartido con la falsificación de marcas y, como derivación, se viene observando una cierta tendencia a unificar la regulación de la propiedad intelectual y la propiedad industrial.

Se trata de una actividad que, en su último eslabón, tiene al llamado en España fenómeno del "top manta/top mochila". En la mayoría de los casos, inmigrantes ilegales que se dedican a este comercio menor e informal como único modo de subsistencia, de allí que -señala García Rivas- se verifique un movimiento jurisprudencial y social contra criminalizarlo, que significaría un evidente efecto "expulsión" de los implicados. Podría decirse que algo –aunque poco en definitiva- del exceso de la intervención punitiva en este campo, se ha mitigado por vía de la L.O. 5/2010, de 22 de junio, que modificó los arts. 270.1 y 623.5 del CPE, estableciendo que cuando el beneficio no exceda de la suma de cuatrocientos euros, el hecho será considerado falta.

En cuanto al tratamiento de los usuarios que intercambian archivos P2P, podría sintetizarse la situación diciendo que hay dos tendencias: a) como en España, considerar que no es delito, por tratarse de una actividad sin ánimo de lucro[25], que debiera considerarse similar a la copia de uso privado[26] y que es suficiente la contención que brindan los sistemas de prevención administrativo y civil; b) utilizar el derecho penal para perseguir esta conducta, como en Estados Unidos. Podría agregarse que es observable incluso una tendencia al uso de los reclamos civiles con una orientación propia de la teoría de la prevención general negativa de la pena, es decir, coaccionante, intimidatorio, al demandar por cifras absolutamente escandalosas y desproporcionadas a usuarios individuales, verdaderos chivos expiatorios, rodeando la acción con una gran difusión pública en procura de asustar o disuadir a otros.

Una aclaración pertinente con relación a la llamada copia de uso privado es que, a la luz de la Ley 11723, se trata de una reproducción no autorizada, ya que no incluye ninguna excepción en particular. Si bien la ley 25036, al incorporar como objeto de protección

---

[24] Cf. Nicolás García Rivas, en su conferencia "Protección penal de la propiedad intelectual", brindada en sede de la Facultad de Derecho de Valencia, el 13 de abril de 2011. En la ocasión, destacando la naturaleza económica del problema, puso de manifiesto que España es uno de los peores países de la Unión Europea en lo que se refiere a la piratería por Internet, ya que el 32 % de los usuarios utilizan P2P, mientras que la media europea es el 15 %.

[25] Esto, como señala García Rivas (ya citado), si lo equiparamos con "finalidad comercial" que, naturalmente, el usuario referido en el texto principal, no tiene. No obstante, Xavier Ribas, propone una sistematización de mayor amplitud para valorar la existencia de ánimo de lucro en los delitos contra la propiedad intelectual cometidos mediante plataformas P2P, distinguiendo: 1) lucro en metálico, 2) lucro mediante intercambio, 3) lucro para un tercero, 4) lucro mediante la obtención de puntos, 5) lucro como antítesis del perjuicio causado a titular de los derechos y, 6) lucro consistente en el ahorro del precio que debería haber pagado para aprovecharse del bien (en "Tipos de lucro", pub. en vlex, disponible en http://vlex.com/vid/185815).

[26] Aclara García Rivas que este aspecto ha cambiado a partir del art. 31.2 de la LPI reformado en 2006, ya que se pone como condición que se trate de una obra a la que se haya accedido legalmente y la copia obtenida no sea objeto de una utilización colectiva o lucrativa. Esta reforma es utilizada como uno de los fundamentos jurídicos de la Audiencia Provincial de Cantabria, Sección 1°, en decisorio del 18/2/08 en causa N° 40/2008, para declarar punible la conducta de ofrecer en general libre acceso o intercambio de obras sin autorización de sus titulares en redes P2P.

de la "Ley Noble" a los programas de computación, previó la llamada copia de salvaguardia del original (art. 9 in fine), habla de una sola reproducción y como respaldo, de lo que no puede derivarse el reconocimiento de un general derecho a una copia de uso privado, al menos en forma directa.

VII. ¿Hacia el "Estado Panóptico"?

Hace poco más de una década, en el I° Encuentro de la AAPDP, postulé la necesidad de legislar en materia de delincuencia informática. También que esto aparejaba un interrogante fundamental: ¿cómo hacerlo?. Aún cuando fue en forma anárquica, espaciada y difusa, según se expuso, se ha avanzado. Sin perjuicio de eso, la pregunta se mantiene vigente porque hay campos en que el déficit sigue siendo manifiesto, ya se ha puesto esto en claro en lo referente a lo procesal, pero también porque se advierte un serio avance en términos de legalización de acciones estatales que importan una intensificación significativa de la posibilidades de intrusión en la esfera de intimidad, en la privacidad y en la autodeterminación informativa del ciudadano.

Se trata de otro posible nivel de incidencia de las nuevas tecnologías de la comunicación en relación con el poder punitivo. Un nivel respecto del que media una cierta despreocupación, ya que la atención de la academia se ha concentrado en general en el problema de la delincuencia informática, en la posibilidad de desplegar conductas ilícitas mediante la herramienta computacional. En cambio, las posibilidades que se ofrecen en términos de incremento del control social, sólo aparecen en escena en sentido crítico en forma esporádica.

Coincide en esta perspectiva Mariluz Gutiérrez Francés cuando señala que la revolución tecnológica ha potenciado la delincuencia transnacional, globalizada y sin fronteras, lo que urge una respuesta que no puede ser unilateral e individualizada, aclarando que *"no puede ser una respuesta a cualquier precio. El otro gran riesgo de la sociedad cibernética concierne más directamente al hombre en sus más íntimos y personalísimos bienes: el ciudadano transparente controlado en todas sus dimensiones y actividades por el ojo, siempre atento e implacable, del estado"*[27]. A su vez, Puente Aba llama la atención sobre la *"falta de sintonía"* observable entre la preocupación de los Estados de tipificar las interferencias a sistemas informáticas aún de menor levedad (simple intrusismo), para impedir la vulneración de la intimidad o la producción de diversos daños y, por otro lado, la iniciativa de los propios Estados realizando actividades que suponen precisamente el acceso o interferencia ilegal en sistemas informáticos, como el caso del sistema de vigilancia de las comunicaciones en Internet denominado "Echelon", cuyo funcionamiento implica *"un serio menoscabo del derecho de los ciudadanos a la salvaguarda de su intimidad"*[28].

Stéfano Rodotá cuenta entre los pensadores que han puesto sobre la mesa que la era digital obliga a repensar todo: la organización social, la democracia, la tecnología, la privacidad, la libertad. Enfatiza que, cuando se reflexiona sobre esto, muchas veces se lo hace en forma acrítica. Con clara reminiscencia a la obra de Aldous Huxley, *"Un mundo feliz"* (en realidad, "Brave New World"), dice que media una visión *"ingenuamente feliz"* de lo informático.

---

[27] En su trabajo *"La ciberdelincuencia en Europa hoy"*, pub. en AAVV "Delincuencia económica y corrupción", Baigún-García Rivas directores, EDIAR, Bs.As., 2006, pág. 353.

[28] Trabajo citado, pág. 407.

Creo que algo de esto puede observarse en torno a las visiones que ofrece el problema de la "brecha digital". De momento, la dominante es que para superarlo, se trata de generar conectividad y confiar en el efecto "derrame". Aún sin descartar su buena intención, enrolaría aquí la iniciativa *"one laptop for child"* del gurú informático del MIT, Nicholas Negroponte. Desde esta perspectiva, se trataría de facilitar el acceso al medio informático a todos, la conexión permitiría, a la larga, superar las diferencias que generaron la brecha. La visión alternativa, subraya que esta es el fruto de la desigualdad económica y social y que es sobre estos aspectos que debe operarse. No es la conectividad la que permitirá superar estos déficits, sino que medidas directas que mejoren la situación económica, que eleven el nivel o calidad de vida, provocarán más accesibilidad tecnológica. En cualquier caso, la perspectiva desde la "periferia" pone el acento en que aún cuando hubiere conectividad, el problema central es el de los contenidos. En otras palabras, a qué me conecto. Sin previsión sobre la producción de contenidos, la conexión sólo terminaría siendo otra manifestación o campo donde profundizar la dominación cultural. Esto es ciertamente un tema de rigurosa actualidad porque en muchos países, incluido el nuestro, se viene dando impulso a programas derivados de la propuesta de Negroponte.

Retomo a Rodotá para recordar que, en su análisis sobre la relación entre tecnologías y democracia, señala que aparecen claramente dos utopías, una positiva y otra negativa. La positiva nos habla de la posibilidad del retorno de la democracia asamblearia ateniense, nueva ágora, la plaza electrónica, el gobernante que puede consultarnos con facilidad, rapidez y frecuencia acerca de nuestro parecer sobre la cosa pública. La negativa traduce en la imagen orwelliana del "Gran Hermano"[29], la posibilidad ahora tecnológicamente accesible de consagrar un verdadero "Estado Panóptico". Sintetiza el problema de las relaciones entre las nuevas tecnologías y la democracia, diciendo que emerge la visión de una tecnología bifronte, como el dios Jano, que provoca la pregunta de si lo que tenemos son tecnologías de libertad o tecnologías de control. Más inquietante, interpela si en realidad no estaremos frente a una nueva imagen, la de la instalación de Orwell en Atenas.

El profesor canadiense Reg Whitaker, a fines de los '90, sostenía que se avanza hacia un nuevo modelo de panóptico, justamente el "Estado Panóptico". Nuevo, porque algunas de las notas básicas que informaban al pensado por Bentham para el medio carcelario y llevado luego por Taylor y Ford a las fábricas, se ven profundamente cambiadas, al punto que en el panóptico estatal lo característico es la descentralización (ya no hay puesto central del control, sino que se ejerce en forma multisectorial, desde todos lados por diversas personas y a la vez) y la consensualidad, entendiendo por tal la activa participación pacífica del controlado que favorece/reclama el control que sobre él se ejerce. Hoy se advierte un manejo y facilitación absolutamente irresponsable de datos sensibles que potencia la clásica ecuación de Crozier: la técnica de control descansa sobre la opacidad del controlador y la transparencia del controlado.

Se entrega información sensible, personal, ingenuamente, sin medir consecuencias y so pretexto de cualquier cosa. Tanto da el sorteo de una plancha como la inscripción a un Congreso. Se lleva la vida privada a las redes sociales, depositando una infundada confianza en que se actuará en círculos cerrados e ignorando que la real baja del servicio es imposible: en el ciberespacio permanecerá conservada nuestra "identidad

---

[29] Que vale la pena aclarar que en la famosa novela "1984" es algo bastante alejado de los reality-shows que con este nombre pueden mencionarse como ejemplo patente de técnica sinóptica hoy día.

digital" y siempre será posible que resurjan aquellas imágenes, datos y perfiles personales que se creyó haber cerrado. En la actualidad, los prestadores de servicio nos ofrecen insistentemente que nos pleguemos al sistema de *"cloud computing"*, es decir, que migremos o externalicemos el contenido de nuestros discos rígidos a la "nube" para tener más seguridad y ahorrar en dispositivos físicos de almacenamiento, que pasará a hacerse en la "nube" a cambio de un precio determinado o determinable, que no es más que un grupo de potentísimos servidores diseminados sin identificación necesaria de su ubicación. Por ejemplo, una empresa contrata el servicio con un servidor que es un tercero ajeno a su organización y se provee por medio de internet, recurriendo a los sistemas de software ubicados en computadoras ajenas, incluyendo aplicaciones como el correo electrónico o los procesadores de texto, de tal suerte que toda la información queda almacenada en la red del servidor del tercero y no en las de la firma que contrata el servicio.

Muchos en la industria sostienen que esta es una tendencia irreversible[30] y que se avanza hacia la imposición en el mercado de dispositivos más pequeños, livianos, portátiles y ágiles porque prescindirán de las unidades de almacenamiento interno, desplazadas por la "virtual". Será interesante ver la incidencia de esto en términos de adquisición de prueba en entorno digital ya que, como enfatiza Elizalde, la mayor parte de las instalaciones virtuales donde se almacena la información son compartidas, por lo que varios usuarios (como la empresa del ejemplo) pueden usar el mismo hardware y aplicaciones, pero el acceso es independiente. El "e-discovery" anglosajón o actividad de prueba digital, antes se practicaba sobre una PC o sobre la red de una empresa, ahora la "materia prima" está afuera. Pareciera que si se ciñe el tema a la "private cloud", en que hardware, software y aplicaciones están sólo al alcance del suscriptor, el control y adquisición pueden inspirarse en forma más directa en las tradicionales reglas del "e-discovery", pero cuando se trata de "public cloud", es decir, media posibilidad de acceso al público en general, la aplicación de un modelo convencional tropieza con ese espacio de zonas y cuestiones no claramente delimitadas[31]. No parece preciso recordar que nada sobre el particular tenemos regulado en nuestro país.

Del otro lado, las iniciativas como la de la Electronic Frontier Foundation (EFF), promoviendo el uso de TOR (software que enmascara las IP) para proteger la intimidad y libre expresión, facilitando el anonimato online, aparecen aisladas y no carentes de contraindicaciones (en nueva perspectiva bifronte, también facilitaría el despliegue de conductas de tinte delictuoso dificultando la determinación de autoría).

VIII. La inseguridad y las cámaras de vigilancia en espacios públicos

Si hablamos de posibilidades de control social, tal vez hoy día uno de los ejemplos en los que es posible observar con mayor claridad la nota de consensualidad aludida en el punto anterior es el del avance de las cámaras, verdaderos "ojos electrónicos", sobre los espacios públicos. Bajo la impronta que Hassemer resumió como el "cambio libertad por seguridad", el manejo mediático de delitos comunes graves provoca una situación social de reclamo de seguridad y prácticamente no hay partido político que no incluya

---

30 Lo afirma Martín Francisco Elizalde, en su trabajo "Prueba en la Cloud Computing: Cloud Computing & Service Level Agreements. El modelo en los Estados Unidos de América y su proyección al ámbito legal argentino", pub. en la biblioteca jurídica online "elDial.com", edición del 08/06/11, ref.: DC15EE.

31 Cf. Elizalde, antes citado.

en su receta para el logro anhelado un programa de instalación de cámaras. En todo caso, si ya las hay, se promete que se agregarán en corto plazo muchas más.

Indudable que las cámaras importan la existencia de un ojo electrónico más penetrante, dominante y ubicuo que el humano. Comenzaron en medios cerrados como la cárcel, los bancos, oficinas, grandes comercios y, luego, llegaron al espacio público. El factor disuasivo o preventivo es invocado usualmente como fundamentador o legitimante. Antes del atentado del "7-J" en Londres, ya era la ciudad más vigilada del mundo, al punto de que contaba con más de 50.000 cámaras instaladas, una cada catorce personas, calculándose que alguien que circulaba por el microcentro podía su imagen ser tomada más de trescientas veces en un solo día. Aquél igual se produjo e incluso tampoco se impidió que llevaran a cabo la equivocada represión del ciudadano brasileño Menezes, a quien tomaron por terrorista árabe.

A esta altura, una aclaración importante: no estoy en contra del uso de cámaras, sólo planteo que no pueden usarse indiscriminadamente y que están muy lejos de ser la herramienta que solucione el problema de la inseguridad, cualquiera que fuese su real extensión. En una de sus obras más recientes, Zaffaroni señala que el *"síndrome de Disneylandia"* es hoy una realidad y casi no hay momento en que una cámara no nos esté registrando apenas salimos de nuestras casas, que convivimos rodeados de controles electrónicos que no sólo no alarman a la "criminología mediática", sino que los muestra como proveedores de seguridad. De tal suerte *"nos convierte a todos en consumidores de la industria de la seguridad y en pacíficas ovejas que no sólo nos sometemos a las vejaciones del control sino que incluso las reclamamos y nos llenamos de aparatos controladores"*[32].

Estos modernos artilugios intrusivos permiten obtener imágenes a una distancia de hasta 300 metros, 360° en sentido horizontal y 180° vertical. En la Ciudad Autónoma de Buenos Aires, durante 2011, se instalaron 750 cámaras fijas y 200 móviles sobre 50 patrulleros de la Policía Metropolitana, a las que se agregan otras 120 de control de tránsito[33]. Se anuncia que para fin de año habrá 2000 y otras 1000 más se agregarán durante 2012. El Centro de Monitoreo se coordinará con el Centro Único de Coordinación de Emergencias, para facilitar actuaciones ante siniestros. Las grabaciones se guardan durante 60 días y se noticia que se contestan un promedio de cinco oficios judiciales por día aportando imágenes que pueden servir como prueba en más de dos mil casos desde la puesta en marcha. Es decir, el sistema ya está operativo y, para estarlo, evidentemente se han tomado decisiones estratégicas acerca de los lugares donde se instalaron las cámaras fijas, por dónde circularán las móviles, se "seleccionó" el personal a cargo de la delicada tarea, entre otras tantas cosas. No digo que esto se hiciera en forma absolutamente inconsulta pero, creo haber establecido con claridad que no sólo el factor "seguridad" es lo que está en juego, sino que por "luchar" contra la inseguridad se adoptan medidas que afectan otros, como la intimidad, privacidad y autodeterminación informativa de todos aquellos cuyos movimientos diarios son observados. Si se atiende a esto, observo que, en general, en la mayoría de los casos, la adopción de reglas acerca de estos aspectos y otros como el funcionamiento del

---

[32] Zaffaroni, *"La palabra de los muertos. Conferencias de criminología cautelar"*, EDIAR, Bs.As., 2011, pág. 378.

[33] Nada distinto sucede en la provincia de Buenos Aires. En el Gran Buenos Aires, al mismo momento ya había instaladas 2784 cámaras, siendo los lugares de mayor concentración Tigre (550), San Isidro (450) y La Matanza (250).

software de alerta automática[34] o del software de privacidad[35], no han sido precedidas de una discusión pública y abierta suficiente.

La provincia de Buenos Aires modificó a fines de 2010 su código adjetivo, incorporando en el Título VIII del Libro I (*"Medios de prueba"*), el capítulo X *"Filmaciones y grabaciones"*, con un único artículo, el 265bis[36], referido tanto a las grabaciones de llamadas a los teléfonos del sistema de emergencias (el "911"), como a las filmaciones obtenidas mediante sistema de monitoreo, tanto fueren de organismos públicos como privados e incluyendo las de particulares en lugares públicos o de acceso público, estableciendo la obligación de su requerimiento al Agente Fiscal y fijándole pautas vinculadas a su resguardo y copia. Se trata, sin dudas, de un positivo avance en dirección a superar el denunciado déficit de la ley procesal en nuestro país aunque, naturalmente, acotado al territorio bonaerense. De todos modos, las "lagunas" permanecen en muchos ámbitos problemáticos que antes se mencionaran.

Si hace dos décadas Hassemer se hacía la ahora desactualizada pregunta acerca de la criptocontroversia[37] *(¿El Estado tiene el derecho de realizar sus pretensiones de intervención y ataque, que le han sido concedidas legalmente, de tal manera que pueda prohibir el proceso criptográfico en todo caso que estas sean afectadas por este procedimiento?*), al presente bien destacan Gilbert y Kerr que los prestadores de servicios de telecomunicación (PST) pasaron de *"centinelas de la vida privada"* a ser *"agentes estatales en la lucha contra la cibercriminalidad"*, lo que se ha evidenciado en el Convenio de Budapest cuando habla de la *"cooperación entre los Estados y la industria privada en la lucha contra el cibercrimen"*. En mayo de este año, durante la Cumbre del G-8 en París, se produjo un debate sobre la regulación y control de Internet entre los gobiernos y empresas, entre las que contaron verdaderos gigantes como Google, Amazon y Facebook.

IX Autoría y responsabilidad del proveedor de servicio

Estrechamente vinculado con lo anterior está la problemática de determinación de autoría por los hechos en el espacio virtual. Las dificultades de individualización del responsable personal, sea por limitaciones técnicas o por trabas derivadas del sistema legal, han generado la pretensión de una mayor "colaboración" de los proveedores de

---

[34] Es el que fija parámetros de atención automatizada para focalizar la cámara ante determinadas situaciones como, por ejemplo, una reunión masiva de personas.

[35] Es el que en forma predeterminada censura o impide determinadas tomas o acercamientos como, por ejemplo, las aberturas de espacios privados.

[36] Por Ley 14172, pub. en el BO del 8/11/10. El art. 265bis dice: *"El Fiscal deberá requerir a organismos públicos y/o privados las filmaciones obtenidas mediante sistema de monitoreo, y las grabaciones de llamadas a los teléfonos del sistema de emergencias.*

La totalidad del material obtenido será entregado al Fiscal en su soporte original sin editar, o de no ser posible, en copia equivalente certificada en soporte magnético y/o digital. El Fiscal conservará el material asegurando su inalterabilidad, pondrá a disposición de las partes copia certificada, debiendo facilitar las copias que le solicitaren.

Las reglas precedentes serán aplicables a las filmaciones obtenidas por particulares mediante sistema de monitoreo en lugares públicos o de acceso público".

[37] Valga el recuerdo del caso federal iniciado en Estados Unidos en 1996 a Philip Zimmermann, creador de programa de encriptación "Pretty Good Privacy", por supuesta exportación de tecnología bélica sin licencia.

servicio en términos de brindar acceso a datos amparados bajo el secreto de las comunicaciones o también en poner a su cargo tareas de control del contenido intercambiado por los usuarios.

En la reunión antes mencionada, como consecuencia de una jurisprudencia que en casos como los de sistemas P2P tiende a no responsabilizar penalmente a los usuarios (con variada argumentación que antes se explicó), la iniciativa europea (a requerimiento o por influencia del lobby empresario vinculado a la industria derivada del derecho autoral) es que los ISP revelen los usuarios que bajen contenidos ilegales para poder accionarlos civil o comercialmente, lo que es resistido por aquellos, aunque no se puede aventurar por cuánto tiempo seguirán así.

Mientras tanto, en paralelo, para superar las dificultades en la identificación de autores se intenta responsabilizar a los proveedores de servicio por vía de entender que su actividad facilita el ilícito o por vía de atribuirles omisión de control sobre el uso que se da a sus plataformas. Uno de los focos de atención actual es, sin dudas, el relacionado con la eventual responsabilidad de los facilitadores de enlaces. Esta suerte de "bibliotecas de links" viene provocando encontrados criterios jurisprudenciales. En Estados Unidos, la opción por responsabilizar penalmente se ha expuesto en una serie de casos (A&M vs. Napster, de 2001; Aimster, de 2003[38]; MGM vs. Grokster, de 2005 –en el que la CSJ propició un estudio de campo que reveló que el 90 % del material estaba sujeto a copyright). La línea europea, informa García Rivas, caminaría en sentido contrario (porque hay algunos precedentes que responderían a la anterior), habiéndose consagrado por la Corte de Casación italiana la impunidad del usuario en 2007, o fijado por la Audiencia Provincial de Valencia que el simple enlace no es delito porque se limita a informar, aunque reproducir en la propia web películas sí lo sería, porque constituiría un acto de comunicación pública (causa Divixonline, del 26/10/10; cctes.: Audiencia Provincial de Murcia, Sección 2°, causa N° 582/2008, 11/09/08 –diciendo que *"el link de superficie, en la medida que simplemente dirige al usuario a teclear más fácilmente el nombre de una página web, no está infringiendo la propiedad intelectual*

---

[38] Carla P. Delle Donne y Pablo A. Palazzi, destacan este caso como uno de aquellos en que la atribución de responsabilidad se hizo bajo la aplicación de la doctrina del "willful blindness" o ignorancia deliberada. Aimster es un servicio de acceso a música similar a Napster, pero cuyas comunicaciones estaban encriptadas entre los usuarios, por lo que los demandados (el dueño del sitio era el actor Johny Depp) alegaban que no podían monitorear los contenidos y desconocían qué intercambiaban los usuarios pues los mensajes estaban cifrados. El tribunal sostuvo que la encriptación había sido hecha específicamente para evitar conocer lo que seguramente los dueños del sitio sospechaban: que los usuarios eran infractores del derecho de autor (en su trabajo *"El caso Taringa!:la responsabilidad penal de los intermediarios de Internet por infracción a los derechos de propiedad intelectual"*, pub. en "Revista de Derecho Penal y Procesal Penal", dirigida por Bertolino y Ziffer, Abeledo Perrot, N° 9, Setiembre 2011, pág. 1548).

Como bien señala María Victoria Huergo, la doctrina del willful blindness –que básicamente sostiene un tratamiento equivalente entre el dolo y el desconocimiento voluntario–, aunque no en forma expresa, sino implícita, aislada y esporádica, ya encuentra algún grado de reconocimiento en la jurisprudencia argentina en casos en los que se condena a título de dolo prescindiendo de la prueba del conocimiento de un elemento del tipo. Concretamente individualiza la nombrada un caso paradigmático en el plenario "Iriart" de la C.N.Cas.P., del 30/9/03, cuando se discutió con relación al delito del art. 302 inc. 1° del CP si basta que la interpelación cursada por el tenedor del cheque sea al domicilio constituido por el librador en el banco (doctrina fijada por la mayoría) o resulta imprescindible acreditar que tuvo efectivo conocimiento de la intimación (en su trabajo *"Reflexiones en torno de la doctrina de la* willful blindness *y su posible recepción en Argentina"*, pub. en la revista "El Derecho Penal", Carlos A. Mahiques director, Ed. El Derecho, N° 5, mayo de 2010, pág. 15).

de ésta"-; Juzgado de Instrucción 4 de Cartagena a cargo del Magistrado Francisco Javier de la Torre Guzmán, causa "Elitedivix", fallo del 4/6/08[39], que fuera luego revocada por la misma Audiencia Provincial de Murcia, pero su Sección 5°, por auto de 16 de setiembre de 2009[40]).

En nuestro medio, el caso más reciente es "Taringa!", con un publicitado auto de procesamiento por infracción al art. 72 inc. a) de la Ley 11723 (edición, venta o reproducción por cualquier medio o instrumento de una obra inédita o publicada sin autorización de su autor o derechohabiente), resuelto el 29 de abril por la Sala VI de la CNCyCorreccional[41]. El 7 de octubre, por la misma Sala se confirmó la ampliación de procesamiento respecto de otro imputado[42].

En síntesis, entendió que autores son los anónimos usuarios que suben y bajan la obra, pero los administradores del website –que obtienen un rédito económico por la publicidad en el portal– son, al menos, partícipes necesarios de la maniobra y claros conocedores de su ilicitud, por lo que el convenio que exhiben para pretender exonerarse de responsabilidad no puede ser tenido en cuenta. Se refieren a la pestaña de denuncias con que cuenta el sitio, donde se inserta una advertencia que dice: *"Los usuarios sólo podrán asociar a sus posts, links que refieran a obras que hubiesen sido lícitamente publicadas en Internet por su titular"*. La defensa destacó que se cargan diariamente unos veinte mil (20.000) posts, lo que imposibilita su control, a lo que se agrega la falta de acceso al Registro de la Propiedad Intelectual para cotejarlos.

Perseguir al partícipe prescindiendo de individualizar al autor es ciertamente problemático a la luz del principio de accesoriedad limitada de la participación[43]. Esta

---

39 En sus fundamentos jurídicos, lucen centrales las referencias al principio de mínima intervención y al de proporcionalidad, destacando que *"Cuando el hecho en cuestión puede ser sancionado a través de la legislación civil o de la administrativa y cuando a través de éstas se pueden conseguir los mismos fines, a efectos sancionadores, resarcitorios o de finalización de la actividad ilícita, que se pueden obtener mediante la Ley Penal, se hace necesario que exista algún elemento más añadido que lleve a aplicar ésta"*, por lo que luego de aclarar que el sitio daba acceso a programas P2P como "emule" y "eDonkey", concluye que la labor de mera intermediación no tiene trascendencia penal y que tampoco puede considerarse la conducta como una comunicación pública a los efectos del art. 270 del CPE. Tras recordar que por ánimo de lucro ha de entenderse -conforme la Circular 1/2006 de la Fiscalía General de Estado- uno de tipo comercial, que no se da en el caso, ni tampoco un perjuicio real y directo a tercero, termina sobreseyendo libremente a los imputados.

40 En sus "razonamientos jurídicos" cobra valor decisivo la reforma del art. 32.1 de la LPI, que ya ha sido destacada referido en una nota al pié anterior. El ponente fue el Magistrado José Manuel Nicolás Manzanares, pub. en La Ley 175980/2009.

41 Integrada por los jueces Mario Filosof y Julio M. Lucini. La causa es la N° 41181, originaria del Juzgado de Instrucción N° 44, caratulada *"www…..net y otros s/procesamiento"*. Entre otras publicaciones en papel, en "Revista de Derecho Penal y Procesal Penal", dirigida por Bertolino y Ziffer, Abeledo Perrot, N° 9, Setiembre 2011, págs. 1542/1543.

42 Causa N° 42318 "N., A. s/procesamiento", vinculada porque A.N., propietario de "W… S.R.L.", contrató el servicio de hosting del portal web "Taringa", ofreciendo a usuarios anónimos la posibilidad de compartir y descargar gratuitamente archivos cuyo contenido no está autorizado para publicar por el autor, facilitando con ello la reproducción ilícita del material que se publica (en concreto, libros). La resolución fue publicada por el medio virtual "Diario Judicial", acompañando la nota titulada "Taringa sigue cosechando procesamientos", edición del día 29/11/11, disponible en http://www.diariojudicial.com/contenidos/2011/10/25/noticia_0005.html

43 Como recuerda Maximiliano Rusconi, la exigencia conceptual de una participación "accesoria" surge de entender que el rol de los partícipes como colaboradores en un hecho ajeno (en su aporte "Arts. 45/49" en AAVV "Código Penal y normas complementarias. Análisis doctrinario y jurisprudencial",

idea es enfatizada por Cordoy Bidasolo, quien señala que es por eso que en derecho comparado se advierten redacciones tendientes a equiparar las conductas de facilitamiento a las de ejecución directa en delitos relacionados con las nuevas tecnologías lo que, en su opinión, sería una metodología por la que desde la parte especial se pretendería derogar principio de la parte general en relación a la autoría, por lo que concluye que *"en el proceso se deberá probar que ese autor desconocido ha realizado un hecho antijurídico"*[44].

El breve considerando dedicado por la Cámara al procesamiento de los hermanos M. y H.B., destaca que los imputados a través de su sitio permiten que se publiciten obras que finalmente son reproducidas sin consentimiento de sus titulares, lo que si bien ocurre a través de la remisión a otro espacio de Internet, es justamente su servicio el que brinda tal posibilidad. Otros agravios de la defensa se afirma serán disipados en una eventual etapa de debate, con oralidad e inmediación, por lo que "*se impone homologar"* el procesamiento de los cotitulares del sitio web. Esta derivación a lo que resulte del juicio propiamente dicho y la falta de conocimiento directo del legajo, recorta sensiblemente la posibilidad de expedirse sobre el acierto de una decisión de carácter provisorio. Sin embargo, el mínimo material disponible ha ofrecido lugar a la discusión.

Comentando favorablemente el auto de procesamiento inicial, Delle Donne y Palazzi son de la opinión que los titulares del sitio actúan no con dolo directo, sino con dolo eventual: *"existen sobrados indicios que nos permiten afirmar que los imputados se representaron la posibilidad de la comisión del ilícito y que, teniendo conocimiento acerca de la ilicitud de las cargas y descargas, optaron por ignorar ese conocimiento. Los imputados obraron en contra del bien jurídico protegido al poner a disposición de los usuarios una plataforma destinada, en esencia, a facilitar la descarga ilegal de archivos"*[45]. A la vez, enfatizan que no se trata de una responsabilidad por omisión, es decir, por falta o inexistencia de control estricto sobre el contenido e hipervínculos de quienes postean, sino por la activa conducta de crear y poner a disposición un sitio que tiene como fin último la reproducción ilícita de obras protegidas[46].

Contrario a este orden de afirmaciones, Eduardo Bertoni enfatiza que la misma tecnología facilita tareas que no son ilegales y que pareciera volverse sobre una vieja discusión que se dio cuando se popularizaron las videograbadoras porque, justamente,

---

Baigún-Zaffaroni directores, Hammurabi, Bs.As., 2002, pág. 165). Se trata de un concepto referenciado: participar siempre indica una relación, porque siempre se participa en algo (cf. Chiara Díaz, Grisetti y Obligado, *"Derecho Penal. Parte General"*, La Ley, Bs.As., 2011, págs. 561 y 566). Esto, en la fórmula de mayor consenso, desde el plano "externo" reclama que el autor haya comenzado la ejecución (si no hay tentativa, no hay forma de penar, conf. art. 47 CP), mientras que en el "interno" –que vincula las características dogmáticas del hecho principal en el hecho del partícipe–, la llamada teoría de la accesoriedad limitada importa que lo es respecto de una conducta típica y antijurídica (injusto).

[44] Cf. Mirentxu Corcoy Bidasolo, *"Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos"*, pub. en "Eguzkilore", N° 21, San Sebastián, diciembre de 2007, pág. 25.

[45] Trabajo citado, pág. 1548. El giro usado por los comentaristas (*"optaron por ignorar ese conocimiento"*) tiene una evidente reminiscencia a la ya mencionada teoría norteamericana de la ignorancia deliberada.

[46] Trabajo citado, pág. 1550.

podían facilitar una reproducción ilegal[47]. No está demás recordar que hace unos años se conocieron variadas iniciativas tendientes a establecer un adicional impositivo a la comercialización de tales productos, así como CDs y DVDs vírgenes o cualquier tipo de soporte físico que facilite el copiado, con destino de "compensación" por el eventual uso en afectación de contenidos amparados. Tampoco lo está que, en ocasiones, la misma empresa que edita, produce y comercializa las obras bajo amparo de propiedad intelectual es la que, por otra de sus divisiones, vende el hardware capaz de hacer las copias cuya realización luego busca perseguir penalmente. Parece difícil sustraerse a la realización de este paralelo sobre el conocimiento de posibilidad que no podría ignorar.

En el procesamiento de A.N., se incluye alguna consideración de interés en términos de ámbito espacial de aplicación de la ley penal, ya que se argumentó que los links desde los que se habrían descargado las obras reproducidas ilegalmente están ubicados fuera de nuestro país. La Cámara rechazó la pretensión de incompetencia argumentando que los servidores del dominio "Taringa!", que es desde donde se ofrecía la descarga, del que serían titulares los imputados, registran domicilio en Argentina. Además, que "*los efectos del delito se habrían producido en el territorio nacional, por lo que en virtud del principio de ubicuidad previsto en el art. 1° del Código Penal es procedente la aplicación de la ley penal argentina*".

De tal suerte, se advierte que la cuestión ha sido resuelta siguiendo reglas tradicionales, como los principios consagrados en el artículo inicial del código sustantivo, lo que luce correcto si se defiende, como dice Gutiérrez Francés, la tesis de que "*la utilización pervertida y abusiva de las altas tecnologías en la dinámica comisiva de un hecho ilícito no cambia ni la naturaleza de éste (el delito seguirá siendo, por ejemplo, una estafa, o un delito de falsedad documental, o de blanqueo de capitales o fraude fiscal…) ni las reglas tradicionales de vigencia de la ley penal*", ello sin perjuicio de que *"Evidentemente, pueden plantearse problemas adicionales de detección, prueba y persecución, pero no se modifican con carácter general los criterios clásicos"*[48] y teniendo presente las modificaciones que pudieran resultar en el futuro de la adopción de reglas de cooperación y auxilio convencionales de orden supranacional.

Con relación a esto último, Cordoy Bidasolo apunta que soluciones que podrían ser incluso concurrentes resultan ser tanto la armonización de las legislaciones y el facilitamiento de mecanismos de cooperación internacional, como la introducción o establecimiento de cláusulas de extraterritorialidad similares a las existentes, por ejemplo, en materia de terrorismo, genocidio o trata de personas. Así lo ha concretado el CPE en su art. 189.1.b), fijando la extraterritorialidad en la corrupción de menores, para la que no interesa si el material pornográfico tuvo su origen en el extranjero o es directamente desconocido. No obstante, en línea con el criterio antes explicitado, coincide en que la solución puede buscarse a través de determinar el lugar de comisión del delito, haciendo jugar tres construcciones jurídicas conocidas como son las teorías de la acción, del resultado y de la ubicuidad[49] (que, vale aclarar, es la tradicionalmente reconocida como vigente en el derecho argentino). Esto no significa que se avente todos los problemas porque, bien resalta la autora citada, subsisten cuestiones espinosas como la competencia jurisdiccional cuando conductas que serían de "cooperación" se

---

47 En su nota en la sección "Opinión" del diario "La Nación", titulada "La libertad de expresión en internet", ejemplar del 9/12/11, pág. 23

48 Trabajo citado, pág. 379.

49 Ob.cit., pág. 31.

concretan en distintos Estados, por ejemplo, que los prestadores de servicios estén en un país diferente de aquel donde se produjeron y desde donde se subieron a la red los contenidos ilícitos. En ese contexto, la confluencia de reclamos de intervención en el caso puede multiplicarse basándose en reglas de territorialidad, del principio de defensa, del de universalidad o de personalidad, por lo que se comparte su conclusión en orden a la necesariedad de tratados de cooperación específicos a nivel mundial[50].

Por estos días, se publicita el inicio de una investigación similar respecto del sitio "Cuevana"[51], a la vez que se ha dado a conocer una iniciativa del legislador de la C.A.B.A. Julio Raffo (Proyecto Sur), quien ha elaborado un proyecto de ley para que sea presentado por el bloque de su partido en el Congreso nacional, tendiente a permitir que las obras culturales puedan ser divulgadas por Internet en sitios sin fines de lucro[52]. Se trataría de una modificación a la L.P.I. para que se reconozca el derecho de libre acceso a las obras culturales a través de la red cuando no mediaren fines lucrativos. El antes citado Bertoni, por su parte, señala que las acciones contra "Cuevana" y decisiones judiciales desacertadas como la del caso "Taringa!", pueden proyectar como consecuencia una afectación a la libertad de expresión en internet. Enfatiza que se ha dejado de lado un estándar internacional –la declaración firmada el 1º de junio por las relatorías especiales de libertad de expresión de África, las Américas, Europa y la ONU-, so pretexto de no haber sido suscripto por nuestro país, siendo que se trata de una interpretación autorizada de tal derecho que no requiere que ningún Estado la suscriba. Por ella, se sostiene que no debe responsabilizarse a los intermediarios por los contenidos que circulan en la red, ni debiera imponérseles a aquellos el control de contenidos de los usuarios. No puede soslayarse que, en este último caso, estaría dejándose en manos de particulares el ejercicio de un poder de censura que podría llegar a comprender contenidos que debieran tener estado público en la red[53].

Volviendo con Cordoy Bidasolo, en la misma dirección enfatiza que debiéramos partir de la inexistencia de una obligación general de control por parte del proveedor en relación con los contenidos y actividades ajenas, al menos desde una perspectiva penal. Sin perjuicio de no mediar imposibilidad de establecerla, lo cierto es que la hay en el plano civil y administrativo a través de variada normativa, de lo que deriva que en caso de incumplimiento de la labor de vigilancia, en todo caso, "*la intervención penal debería reservarse para conductas dolosas de los prestadores de servicios*"[54].

Cerrando este punto, recuerdo que los citados Delle Donne y Palazzi señalan la existencia en la actualidad de "*cierta permisividad social (y hasta legal)*" para la reproducción de obras intelectuales en internet "*erosionando el derecho de los autores*"[55]. Es probable que lo más erosionado no sea el derecho de los autores sino la

---

[50] Ob.cit., pág. 32.

[51] La denuncia fue presentada por HBO y el expediente tramita ante el Juzgado de Instrucción N° 36, con intervención de la Fiscalía de Instrucción N° 4, causa "E.,T. y Cuevana.com s/infracción a la ley 11723".

[52] La noticia ha sido publicada por el medio virtual "Diario Judicial", nota titulada "Derechos de autor en la web: ¿tolerancia o persecución?", edición del día 29/11/11, en la que se aclara que Raffo es autor del libro "Derecho autoral: hacia un nuevo paradigma". Texto disponible en http://www.diariojudicial.com/contenidos/2011/10/25/noticia_0009.html

[53] En la nota antes citada.

[54] Ya citada, págs. 24/25. La cita textual es del punto 3.5.

[55] Ob.cit., pág. 1545.

pérdida de ganancias de quienes ostentan el monopolio de edición, distribución y comercialización de las obras que crearon los autores. En todo caso, la razonabilidad del sostenimiento del paradigma del copyright utilizando el derecho penal se trata de un tema que excede los límites de esta presentación[56]. En cuanto a la absoluta corrección de lo afirmado sobre la permisividad social, clara muestra ofrece una encuesta realizada por el sitio especializado en noticias judiciales "Diario Judicial" preguntando a sus lectores si estaban de acuerdo con el procesamiento de los titulares de "Taringa!" por considerarlos partícipes necesarios de infringir la Ley 11723, ofreció como resultado que sólo el 13,4 % entendió que *"la justicia hizo lo que tenía que hacer para proteger derechos registrados"*, mientras que el 86,6 % opinó que "*al publicar un link no hay responsabilidad por lo que haga el sitio (es como publicar un aviso clasificado sin que el diario tenga responsabilidad por lo que se vende)"*[57].

X. Cuestiones pendientes

Junto al de la responsabilidad de los proveedores (ya sean Network Providers, Information Content Providers, Internet Acces Providers o Hosting Service Providers), hay otros núcleos problemáticos pendientes, como la responsabilidad penal de las personas jurídicas o, en términos procesales, las reglas para esclarecer la cuestión del ámbito de aplicación espacial de la ley penal, las de cooperación internacional o las concernientes a la prueba en entorno digital.

En muchas ocasiones se denuncia que la responsabilidad de los proveedores se busca, en realidad, como una salida fácil ante las dificultades de identificar a los verdaderos autores de afectaciones, sobre todo, a la propiedad intelectual. Diferenciar entre los distintos tipos de proveedores es un primer paso de racionalidad. No es lo mismo quien sólo brinda la estructura a la red (cableado, por ejemplo), para quien no puede haber atribución de responsabilidad alguna en esta materia, que el provee contenidos, para quien es obvio que sí puede haberla. En cuanto a los que dan acceso o alojamiento, la clave pasa por el conocimiento, que encuentra un natural indicio de su existencia cuando median tareas de edición o publicación. Si hay conocimiento es posible responsabilizar, si no lo hay, parece irrazonable. Un segundo paso hacia la racionalidad es distinguir la responsabilidad civil de la penal. La última, de aceptarse, sólo debiera reservarse para casos extremos, coherente con la idea de "ultima ratio" que debe presidir toda habilitación de ejercicio de poder punitivo.

El problema de la competencia para investigar, perseguir y punir conductas disvaliosas en el ciberespacio, viene encontrando diversas propuestas de solución que van desde una suerte de foro universal, hasta dar preeminencia al estado que previno o, directamente, al estado que esté en condiciones técnicas de llevar adelante la investigación, que cuente con los medios para ello. En lo personal, creo que los principios tradicionales consagrados en nuestra normativa, básicamente los de territorialidad y real o de defensa, enmarcados por adecuados convenios de asistencia y cooperación penal (cuyas líneas básicas fija la Ley 24767), son herramientas suficientes,

---

[56] Me remito sobre el particular a lo expuesto en la monografía "Delincuencia informática", Ediar, Bs.As., 2009.

[57] El resultado ha sido destacado por el propio "Diario Judicial", en nota titulada "Copyright vs. Copyleft", en la edición N° 3040 del mismo día antes citado. Disponible en http://www.diariojudicial.com/contenidos/2011/05/27/noticia_0009.html

sin perjuicio de posibles superposiciones en la persecución de algún hecho en particular que, por otra parte, no son patrimonio exclusivo de esta modalidad delincuencial.

También median algunas discusiones sobre supuestos déficits en materia de tipicidad, ya que no faltan quienes denuncian le necesidad de:

a) establecer el delito de ciberocupación o registro impropio de nombres de dominio que, destaca Farah, es un acto que pudiera ser la antesala de una defraudación básica del art. 172 del CP, o bien de un fraude a la propiedad intelectual (art. 72bis Ley 11723) o de la competencia desleal prevista por el art. 159 del código citado. También podría preceder engaños para "phishing", sobre todo cuando se involucran caracteres orientales para occidentales (o viceversa).

b) penalizar la conducta de "spamming" (correo basura o publicidad no solicitada[58]), cuya ilegalidad ya ha sido reconocida en sede civil y que, a la luz de Ley 25326, tiene previstas consecuencias como la cancelación en base de datos y sanciones económicas, lo que en mi opinión evidenciaría que la intervención penal es innecesaria.

c) tipificar la posesión o tenencia simple de material pornográfico infantil, además de la ya prevista cuando tiene finalidad de distribución o comercialización, lo que es propiciado por el Convenio de Budapest.

Si agregamos los que se fueran mencionando antes, como el delito de modificación o adulteración de sistemas informáticos o equipos electrónicos fiscales, o la definición acerca de recurrir al derecho penal respecto de los usuarios de intercambios de archivos P2P o para los "manteros", puede advertirse que son muchas aún las cuestiones que en el futuro próximo deben analizarse.

Finalmente, sin desmerecer el conjunto de problemas que acabo de individualizar, permanece como un objeto central de reflexión en cada paso que se da tendiente a dar un adecuada tratamiento normativo a los problemas que ofrecen las nuevas tecnologías en términos delincuenciales, la incidencia que pudieran tener como herramienta potenciadota del control social, de tal suerte que aquellos no operen como mera "excusa" para fomentar un incremento irrazonable de este que, si se presenta como inevitable "consecuencia", debe procurarse su limitación lo máximo posible.

---

[58] Los mayores emisores de correo basura están concentrados en Estados Unidos (15,4 %) y Rusia (7,4 %).