# ¿PONER PUERTAS AL CAMPO? SOBRE LA POSIBILIDAD DE PROHIBIR PENALMENTE EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN[*]

David Felip i Saborit[**]

## Sumario



[*] Este trabajo se enmarca en el proyecto «Diez años del nuevo derecho penal de la criminalidad en la empresa: la intención del legislador y la actuación del sistema judicial», financiado por el Ministerio de Educación y Ciencia, Plan nacional de I+D+i (referencia SEJ 2005-03423/JURI).
[**] David Felip i Saborit, profesor titular de derecho penal del Departamento de Derecho de la Universidad Pompeu Fabra., c/ Ramon Trias Fargas, 25-27, 08005 Barcelona, david.felip@upf.edu.
Artículo recibido el 29.06.2007.

## I. Prefacio

El 8 de febrero del 2001, agentes del FBI se presentaron en casa de la familia de Brandon Lifshitz. Investigaban intercambios de pornografía infantil en los cuales estaba involucrado el ordenador de su madre. Lifshitz se mostró colaborador y admitió a los agentes que había descargado y difundido a través de Internet material de este tipo. La familia consintió la inspección de sus ordenadores, donde había almacenado numerosas fotografías. Lifshitz fue acusado de un delito federal por recepción e intercambio interestatal de pornografía infantil. Gracias a diversos informes sobre sus problemas psíquicos y a un acuerdo con el fiscal, finalmente fue condenado únicamente a tres años de *probation* (periodo de suspensión condicionada de la condena). Ahora bien, el juez le impuso, como condición de la *probation*, medidas de control de su ordenador. Concretamente se le exigía que aceptara la instalación de sistemas que permitieran a los funcionarios supervisores vigilar y filtrar el uso de cualquier equipamiento informático que poseyera o controlara el condenado. Adicionalmente, tenía que consentir el examen sin aviso previo de los equipamientos mencionados, incluyendo la copia de todo tipo de datos así como el decomiso de cualquier elemento de los equipos con el objetivo de examinarlo más a fondo.[1]

¿Es posible la imposición de medidas similares en nuestro país en la actualidad? ¿Si no es así, es previsible que, en el futuro, se adopten? Destinaré las próximas páginas a intentar dar respuesta a estas cuestiones.

## II. Introducción

1. La incidencia de las tecnologías de la información y la comunicación (TIC)[2] sobre el mundo de la criminalidad y del derecho penal crece por momentos. Su repentino desarrollo ha comportado, entre otros efectos, un incremento de la peligrosidad de las conductas delictivas convencionales (por ejemplo, las estafas o las defraudaciones de la propiedad intelectual). Por otra parte, ha implicado también una modificación profunda del *modus operandi* de otros delitos (por ejemplo, la difusión de contenidos ilícitos, con la pornografía infantil como caso paradigmático, o la pederastia). Finalmente, ha provocado la aparición de una nueva generación de delitos que tienen las TIC como objeto (por ejemplo, accesos ilícitos a sistemas y redes, diseminación de virus y provocación de otros daños informáticos, intercepción de comunicaciones, etc.).

[1] United States *vs.* Lifshitz, 369 F.3d 173 (2d Cir. 2004). Véase un resumen del caso en Curphey, Shauna, «*United States v. Lifshitz*: Warrantless Computer Monitoring and the Fourth Amendment», *Loyola of Los Angeles Law Review* 38, 2004-2005, p. 2251 y s., y en Harrold, Marc M., «Computers Searches of Probationers - Diminished Privacies, "Special Needs" & '*Whilst Quiet* Pedophiles" - Plugging the Fourth Amendment into the "Virtual Home Visit"», *Mississippi Law Journal* 75, 2005-2006, p. 324 y s. Después de recurrir la decisión, la defensa consiguió que las inspecciones sólo se pudieran llevar a cabo en caso de sospechas razonables de actuación incorrecta, y no en el caso de la vigilancia a distancia, que podía realizarse discrecionalmente.

[2] Conjunto de tecnologías utilizadas para procesar y transmitir información en formato digital.

Ante este fenómeno, la primera preocupación desde del derecho penal ha estado adecuar los tipos delictivos y los criterios de imputación de la responsabilidad a la nueva situación. Mientras tanto, desde del derecho procesal la prioridad ha sido hacer frente a los nuevos problemas técnicos de persecución y de prueba de unos hechos en los cuales, además, se ven implicadas normalmente las jurisdicciones de diversos países.[3]

2. En cambio, la revolución de las TIC no ha tenido todavía tanta incidencia sobre las penas y otras consecuencias jurídicas del delito, al menos en Europa. Sin embargo, a caballo entre estas tecnologías, se avista una serie de medidas penales "posmodernas" que implican cambios sugerentes, que quizás nos permitirán superar o limitar el recurso a la pena de prisión.[4] No obstante, existe el riesgo de que, tal vez, estas medidas se conviertan en el motor de una transformación, profunda y preocupante, del sistema penal, hacia situaciones de supervisión intensiva, en qué la custodia carcelaria sea sólo un episodio intermitente dentro de un cuadro más amplio de control permanente sobre capas enteras de la población.[5] La reciente y rápida expansión de la vigilancia electrónica puede ser la pionera en esta evolución paradójica.[6]

Si nos introducimos un poco más en la reflexión, aparece la cuestión de si las TIC, además de un instrumento por castigar, pueden ser también *el objeto* de penas y medidas penales, es decir, si, como consecuencia de la comisión de un delito, tiene sentido y es factible prohibir o restringir, por ejemplo, la posesión o el uso de ordenador o el acceso a Internet.[7] De entrada, la respuesta es que, si exceptuamos los efectos implícitos a la pena de prisión, medidas de este tipo ni parecen necesarias, ni son técnicamente factibles, y, consiguientemente, no están previstas en la mayoría de legislaciones, entre las cuales está la española. Sin embargo, una mirada más esmerada a nuestra legislación y, sobre todo, a las últimas experiencias en el mundo anglosajón que veremos más adelante, justifica un análisis más detallado de la cuestión.

---

[3] Una visión general de estos problemas, desde la perspectiva española, puede conseguirse, entre otros, con la obra colectiva de Romeo Casabona, Carlos María (coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, Comares, 2006. Hasta el momento, la culminación de estos esfuerzos se ha materializado en el Convenio sobre Cibercriminalidad de 23 de noviembre del 2001, impulsado por el Consejo de Europa (disponible en <http://conventions.coe.int>) y que ha sido ratificado también por países como los EE.UU. (y no España, a pesar de haber sido signataria).

[4] *Vid.* el informe de Crowe, ANN H. *et al*., *Offenders Supervision with Electronic Technology*, American Parole and Probation Association, Lexington, 2002, p. 57-69 (disponible en <http://www.ncjrs.gov/pdffiles1/nij/grants/197102.pdf>), que empieza a ser superado por los cambios tecnológicos: control de movimientos con GPS, identificaciones a distancia, análisis telemáticos, control instantáneo del consumo de alcohol y de otras drogas, etc.

[5] *Vid.* el inquietante escenario para el año 2016 descrito en Murakami Wood, David (ed.), *A Report the Surveillance Society*, Londres, 2006 (disponible en <http://www.privacyconference2006.co.uk/>).

[6] Las medidas de vigilancia electrónica, encarnada por las famosas "pulseras electrónicas", están plenamente implantadas en el mundo anglosajón y parece que se están consolidando como una alternativa a la prisión en toda la Europa continental, después de superar la de críticas que originaron inicialmente. Al menos, ésta es la conclusión a la cual, desde el Max Planck Institut, llega Hans-Joerg Albrecht en *Electronic Monitoring in Europe.* En *Summary and Assessment of Recent Developments in the Legal Framework and Implementation of Electronic Monitoring*, Freiburg i. B., 2005 (disponible en <http://www.mpicc.de/shared/data/pdf/albrecht.pdf>). Con respecto a su implantación en nuestro país, *vid*. Gudín Rodríguez-Magariños, Faustino, *Cárcel electrónica. Bases para la creación del sistema penitenciario del siglo XIX*, Valencia, Tirant lo Blanch, 2007.

[7] Cuestión que me fue planteada por mi colega de la Universidad Pompeu Fabra, el profesor Xavier Bernadí, y que ha provocado la elaboración de este trabajo.

3. De hecho, la irrupción y la amplia difusión de las TIC ha generado la *posibilidad* de crear nuevas penas. Hoy en día, limitar o prohibir el uso de las TIC a una persona es privarla de algo valioso y, por lo tanto, *podría ser una pena*. En efecto, es un daño desde un punto de vista estrictamente material: implica una restricción de derechos del individuo y se puede cuantificar económicamente (se limitan sus posibles actividades profesionales y de ocio, comporta pérdida de tiempo en la vida cotidiana, etc.). Asimismo, la privación de las TIC es también percibida psicológicamente por muchas personas como un daño y puede ocasionar un padecimiento nada negligible. Especialmente ahora que el acceso a estas tecnologías se ha generalizado, su posesión y su uso son cada vez más preciados, tanto para la autoestima personal como para la interrelación social. Por lo tanto, una restricción en el ámbito de las TIC puede servir como pena. Tiene un contenido aflictivo apreciable desde una perspectiva de retribución del hecho que se ha cometido y también desde una óptica de prevención general de delitos, es decir, es una medida que puede disuadir a los delincuentes potenciales y satisfacer al conjunto de la sociedad cuando espera una reacción ante ciertos delitos, sobre todo si no son hechos muy graves y siempre y cuando se garantice el  de la medida. En definitiva, las prohibiciones de uso de TIC son en teoría aptas para configurarse como una nueva pena privativa de derechos, junto con las que ya existen en la actualidad, como, por ejemplo, la privación del derecho a conducir vehículos o la inhabilitación para el ejercicio de una profesión.[8]

4. Por otra parte, la irrupción y el uso de las TIC en la actividad delictiva provoca la *necesidad* de modificar el contenido de las medidas penales actuales. Esta necesidad aparece, especialmente, cuando se trata de castigar nuevas manifestaciones delictivas, la denominada *cibercriminalidad*, entendida en sentido amplio: desde el pederasta que utiliza los *chats* para localizar víctimas hasta el *hacker*, pasando por el estafador informático. En efecto, de la misma manera que con otros delincuentes se intenta controlar el acceso a las drogas o a las armas de fuego, en este ámbito, la peligrosidad criminal de los infractores, es decir, el riesgo de que vuelvan a cometer hechos delictivos, está muy vinculada a las posibilidades de uso de las TIC.[9] Por lo tanto, cuando una persona responsable de hechos de este tipo está sometida a medidas penales que no implican privación efectiva de libertad, se presenta el problema de si es legítimo y factible controlar su peligrosidad criminal prohibiendo o limitando, por ejemplo, la utilización del ordenador o del teléfono móvil, el acceso a redes de comunicaciones, etc. En definitiva, aparte de un castigo, estas medidas se pueden concebir también como un instrumento para asegurar el riesgo que comporta el infractor y para contribuir a su rehabilitación.[10] Desde esta

[8] Cfr. el catálogo de penas privativas de derechos en los artículos 39 y s. del Código Penal (CP).

[9] Una muestra de las nuevas necesidades de control que generan las TIC son ciertas formas de delincuencia sexual, singularmente la pederastia: *vid.* Durkin, Keith F, «Misuse of the Internet by Pedophiles: Implications for Law Enforcement and Probation Practice », *Federal Probation* 61-3, 1997, p. 14-18 Y McKay, BRIAN W., «Guardrails  the Information Superhighway: Supervising Computer Use of the Adjudicated Sex Offender», *West Virginia Law Review* 106, 2003-2004, p. 205-212, con referencias abundantes. El uso de estas tecnologías se ha convertido en un elemento esencial en la dinámica de comisión de este tipo de hechos, especialmente por el *grooming* (proceso de manipulación de las víctimas para reducir la resistencia a los abusos) y porque facilita la formación de comunidades que mitigan el aislamiento social y dan apoyo y legitiman estos comportamientos.

[10] En efecto, saber que está bajo control puede ser un elemento que ayude al infractor a superar la tentación de reiterar las conductas delictivas y, por lo tanto, ser un elemento de apoyo de las eventuales terapias; tanto para un pederasta

perspectiva, la prohibición o restricción de acceso a las TIC puede dar contenido a medidas cautelares, de seguridad o a medidas alternativas a la prisión de naturaleza preventiva especial.

5. Finalmente, las TIC plantean *nuevos retos* a la pena criminal por excelencia, es decir, la prisión, tanto con respecto al contenido como a la ejecución.

En primer lugar, porque la prisión parece que implica una severa restricción del acceso a las TIC, si bien las razones pueden no ser del todo claras. Así, se podría pensar que la limitación es inherente al mismo "sentido de la pena" (art. 25.2 CE), en tanto que ésta supone un cierto apartamento de la sociedad y que, por lo tanto, la Administración penitenciaria puede modular libremente el eventual acceso a las TIC de acuerdo con las necesidades de tratamiento, tal como se hace con otros aspectos de la privación de libertad.[11] O, por el contrario, se puede entender que la prisión no implica, en tanto que pena, la privación del acceso a las TIC y que, por lo tanto, la justificación de las restricciones en este ámbito tiene que ser puramente instrumental, es decir, aceptable sólo por motivos regimentales o de seguridad.[12] Si fuera así, habrá que valorar muy esmeradamente la proporcionalidad de cualquier restricción que se aplique en este campo, especialmente si entra en colisión con determinados derechos fundamentales.[13]

> La STC 140/2002, de 3 de junio, parece orientarse de acuerdo con esta segunda perspectiva. El TC no otorgó el amparo a un preso a quien había sido denegada la disposición, por razones de estudios, de un ordenador en su celda y sólo se le permitía que lo utilizara en una sala destinada a tal efecto. El Tribunal entendió que se trataba de una modulación aceptable del derecho a la educación (art. 27.1 CE) por razones de seguridad y de organización del régimen del centro.

Sin embargo, la concreción del contenido y el alcance de estas restricciones se convierte en problemática, dado que buena parte de la normativa penitenciaria fue elaborada cuando las TIC no existían o se encontraban en un estado incipiente[14] y no ha sido todavía objeto de tratamiento doctrinal.

---

que sabe que su ordenador está intervenido, como para un drogodependiente que sabe que al día siguiente tiene que pasar un análisis de control periódico.

[11] Tal como sucede con las salidas al exterior (cfr. STC 204/1999, de 8 de noviembre) o la práctica de relaciones sexuales (cfr. STC 89/1987, de 3 de junio).

[12] O, aunque parezca paradójico, por necesidades del tratamiento. En efecto, desde esta perspectiva, si bien por regla general se tiene que potenciar el uso de las TIC por parte de la mayoría de internos, también se tiene que privar a aquellos internos que manifiesten, en determinadas fases del tratamiento penitenciario, una especial peligrosidad en relación con las TIC. Piénsese, por ejemplo, en el pederasta que las utiliza para continuar en contacto con su comunidad o el maltratador que las utiliza para continuar amenazando a su pareja.

[13] Sirva de ejemplo de este planteamiento la STC 89/2006, de 27 de marzo, en que se declara que las condiciones en las cuales se lleva a cabo un registro en una celda (sin informar de manera coetánea o posterior al interno afectado) constituyen una vulneración del derecho fundamental a la intimidad innecesaria. Supera, en cambio, el test constitucional de proporcionalidad y se entiende que no se vulnera el derecho a recibir información (art. 20.1.*d* CE) la retención de unas revistas destinadas a un penado con un historial terrorista importante (STC 11/2006, de 16 de enero).

[14] La única mención la encontramos en el artículo 129 del Reglamento penitenciario, que prevé la posibilidad de autorizar la disposición de un ordenador personal por razones de carácter educativo o cultural y que, en todo caso, prohíbe la conexión a redes de comunicación. Así, en Cataluña la cuestión ha sido desarrollada por la Instrucción 1/2006, que regula la disposición de ordenadores personales, y la Instrucción 7/2006, con respecto a la telefonía

En segundo lugar, estas tecnologías implican un reto porque se convierten en un instrumento del régimen y del tratamiento penitenciario de especial importancia, ya que permiten superar muchas de las barreras inherentes a la prisión y desarrollar las diferentes actividades en condiciones similares a las existentes en libertad, desde la asistencia médica o las visitas de los abogados hasta los estudios no presenciales o la capacitación profesional.[15] Obviamente, se producirán tensiones entre esta corriente favorable a la introducción de las TIC en la prisión y la tendencia restrictiva indicada anteriormente.[16]

Y, en tercer lugar, porque al permitir nuevas formas de control y vigilancia sobre las personas se amplían las posibilidades de ejecutar las penas y medidas privativas de libertad en régimen abierto: así, por ejemplo, el control telemático puede comportar un incremento de las salidas programadas, la concesión del régimen abierto a los internos en tercer grado, más limitaciones en la adopción de la prisión provisional, etc. La posibilidad de controlar el acceso y el uso de las TIC podría ser también un factor adicional de control y disminución del riesgo que permita una aplicación más amplia de las medidas mencionadas.

6. En definitiva, por su naturaleza, las prohibiciones y el control del uso de las TIC podrían ser una nueva pena si así lo decidiera el legislador pero, además, es una posibilidad que se tiene que considerar en la aplicación actual de medidas penales no privativas de libertad a ciberdelincuentes y, de hecho, es ya un problema real en la ejecución penitenciaria ordinaria. cuestiones de extensión, en este trabajo analizaré más a fondo los dos primeros aspectos mencionados.

## III. El modelo norteamericano

1. Si buscamos en derecho comparado penas o medidas penales en materia de TIC, podemos observar con una cierta sorpresa que desde mediados de los años noventa se está experimentando intensamente en los países anglosajones con estas sanciones, singularmente en

móvil de internos en régimen abierto cuando se encuentren en los centros penitenciarios. (disponibles en <http://www.gencat.net/justicia/temes/reinsercio_i_serveis _penitenciaris/centres/instruccions/index.html>).

[15] A modo de ejemplo, el Departamento de Justicia de la Generalitat de Catalunya ha puesto en marcha una serie de actuaciones para el fomento del uso de las TIC en los centros penitenciarios. Entre éstas, destaca la creación de *Punts Òmnia*, una iniciativa para facilitar el acceso a las TIC a la población en general (*vid*. <Http://xarxa-omnia.org/>) y que, a partir del año 2001, se han ido instalando en la mayoría de centros. La iniciativa no se limita a facilitar unos determinados equipamientos y el acceso —controlado— a Internet sino que se desarrollan diferentes actividades para conseguir "la alfabetización digital de los internos" (*vid*., por ejemplo, algunos blogs elaborados por los internos en <http://www.bloggersdesdeprision.blogspot.com>, fruto de la *experiencia Òmnia Blocger*). Por otra parte, algunos módulos penitenciarios disponen también de aulas de informática, pero el equipamiento es muy precario y no tienen acceso a Internet (información facilitada amablemente por la Dirección General de Recursos y Régimen Penitenciario).

[16] En efecto, la principal preocupación, por el momento, es controlar el acceso a redes exteriores. Así, con respecto a los equipamientos personales, en ningún caso se permite la posesión de ordenadores portátiles ni el acceso a redes de comunicación (*vid.* Instrucción 1/2006, nota 14), mientras que el control en los *Punts Òmnia* se ejerce a través de un cortafuegos elaborado *ad hoc* que impide enviar información al exterior.

los EE.UU.[17] Para los norteamericanos no son excepcionales las prohibiciones de usar ordenadores, telefonía móvil y otros equipamientos informáticos, de acceder a Internet, de utilizar el correo electrónico o de participar en chats. Se trata de medidas que se aplican básicamente a personas convictas por ciberdelitos, muy especialmente por delitos sexuales relacionados con menores y por intrusismo y sabotaje informático. El caso Lifshitz, reseñado en el prefacio de este trabajo, puede ser el arquetipo. Ocasionalmente estas medidas se aplican también a los autores de delitos convencionales en los cuales las TIC han sido el instrumento del delito.[18] En cambio, en Europa parece que estas medidas son desconocidas, si bien últimamente se detectan movimientos significativos en el Reino Unido.[19] Por lo tanto, en este ámbito podemos hablar del "modelo norteamericano".[20]

2. Estas restricciones han aparecido en el campo de la supervisión comunitaria (la intervención penal que opera fuera de las prisiones) en forma de condiciones para acceder a la *probation*, la *parole* o la *supervised release*. Se trata de situaciones de libertad vigilada que se imponen como consecuencia de la comisión de delitos.[21] La *probation* presenta muchas similitudes con la suspensión de la pena del CP español; se aplica a personas declaradas culpables de delitos no muy graves y consiste a dejar en el pronunciamiento de la condena durante un periodo de prueba. La *parole* se parece a nuestra libertad condicional; se otorga a presos que son puestos en libertad antes de haber cumplido enteramente su pena. Finalmente, la *supervised release* o liberación bajo vigilancia es una figura por el momento sin equivalente en España.[22] Está prevista para ser aplicada una vez el penado ha cumplido toda la pena de prisión y es liberado y,

[17] Cfr. el estudio empírico llevado a cabo por el criminólogo australiano Smith, Russel G., «Criminal Forfeiture and Restriction-of-Use Orders in Sentencing High Tech Offenders», *Trends & Issues in Crime and Criminal* Justice 286, Australian Institute of Criminology, 2004, p. 1-6 (disponible en <http://www.aic.gov.au/publications/tandi2/tandi286.html>). En efecto, dejando de lado algunos casos aislados detectados en Australia y Canadá, la inmensa mayoría de casos proceden de los EE.UU.

[18] Así, un joven australiano de 17 años estuvo acusado de tentativa de asesinato de un hombre que conoció en un chat y le fue impuesta, como medida cautelar, la prohibición de uso de Internet excepto para finalidades educativas y un "toque de queda" informático a partir de las 9 de la noche (Smith, *supra* nota 17, p. 1).

[19] En efecto, últimamente desde diversas instancias se ha señalado la posibilidad de introducir prohibiciones y vigilancia del uso de las TIC por parte de delincuentes sexuales al amparo de la *Sexual Offences Act*, aprobada en el 2003, especialmente a través de la *Sexual Offence Prevention Order*, que permite imponer diversas medidas a los acusados y convictos por este tipo de delitos: *vid.* las directrices establecidas en *el Sex Offender Strategy for the National Probation Service*, septiembre de 2004, p. 16 (disponible en <http://www.probation.homeoffice.gov.uk/output/page32.asp>). Recientemente, en el informe, encargado por la *Risk Manegement Authority* de Escocia, de la criminóloga Davidson, Julia, *Current Practice and Research into Internet Sex Offendig*, enero de 2007, p. 51 y s. y 69 (disponible en <http://www.rmascotland.gov.uk/rmapublications.aspx>), se recoge la demanda generalizada en este sentido por parte de los responsables policiales y de ejecución penal del Reino Unido.

[20] Con todas las cautelas y en un intento de simplificación máxima, vistas las notables diferencias, legales y prácticas, que existen entre los diferentes estados.

[21] Una referencia sucinta del sistema federal en McKay, *supra* nota 9, p. 219-220 y Wiest, Christopher, «The Netsurfing Split: Restrictions Imposed Internet and Computer Usage by Those Convicted of a Crime Involving a Computer», *University of Cincinnati Law Review* (72), 2003-2004, p. 848-850. Para poder entender las dimensiones del fenómeno, con 5 millones de personas bajo vigilancia, *vid.*, sencillamente el boletín del *Bureau of Justice Statistics*, «Probation and Parole in the United States», 2005 (disponible en <http://www.ojp.usdoj.gov/bjs/pub/pdf/ppus05.pdf>).

[22] En el proyecto de reforma en el CP, actualmente en curso pero que parece paralizado, se prevé una nueva pena, la "libertad vigilada", que en ocasiones puede ser aplicada como pena adicional a la pena de prisión en caso de reincidencia (cfr. los nuevos artículos 48.4, 88 y 94 CP según el Proyecto de ley 121/000119, *Boletín Oficial de las Cortes Generales, Congreso de Diputados*, Serie A, Proyectos de Ley, 15 de enero de 2007, nº. 119-1).

de hecho, está gestionada como una modalidad de *parole* y puede llegar a ser impuesta a perpetuidad. Pues bien, cuando un juez o un *parole board* acuerda alguna medida de este tipo, impone, discrecionalmente o por ministerio de la ley, la observancia de determinadas condiciones al sujeto. Estas condiciones están destinadas a hacer disminuir durante el periodo de control la capacidad y la oportunidad de cometer nuevos delitos, así como a facilitar la rehabilitación del delincuente. Su naturaleza es diversa: abstenerse de determinadas actividades (no delinquir, no consumir alcohol o drogas, evitar ciertos lugares y establecimientos, etc.), cumplir ciertas obligaciones (seguir un tratamiento, vivir en un determinado lugar, conservar un trabajo, etc.) y facilitar el control y la vigilancia (entrevistarse periódicamente con los supervisores, aceptar registros, someterse a análisis, etc.). Durante el tiempo de duración de la medida, se controla con una cierta intensidad la evolución del sujeto y el de las condiciones. Su vulneración (las denominadas *infracciones técnicas*) implica un endurecimiento de las condiciones o bien la revocación de la situación de libertad del sujeto y el ingreso en prisión. Esta decisión normalmente la adopta el juez pero con requisitos, sobre todo de prueba, menos estrictos que si se tratara de la comisión de un delito.

3. Por consiguiente, este tipo de medidas ha sido el medio idóneo para la aparición de las medidas penales restrictivas de las TIC. En efecto, si bien las legislaciones y las guías penológicas[23] detallan muchas de las condiciones que se pueden imponer, también permiten que los jueces establezcan las suyas propias, siempre que estén relacionadas con el delito concreto, y que sean necesarias para proteger a la sociedad y rehabilitar al infractor y no supongan una restricción de la libertad razonablemente innecesaria.[24] esta vía, los tribunales y las agencias de supervisión se han adaptado a los cambios tecnológicos y han introducido medidas "creativas" como, por ejemplo, la utilización del polígrafo o de los tests de drogas con el fin de detectar infracciones técnicas[25] o, por lo que aquí nos interesa, las restricciones en el uso de ordenadores y en el acceso a las redes de información.

Así, a partir de mediados de los años noventa aparecieron medidas de este tipo que se aplicaban especialmente a los poseedores y traficantes de pornografía infantil y a los delincuentes sexuales que habían utilizado las TIC para establecer contacto con menores y, posteriormente, estas medidas se extendieron a otros ciberdelitos. Las medidas restrictivas en el uso de nuevas tecnologías son, por lo tanto, fruto de la práctica diseminada de jueces y funcionarios de *probation* y *parole*, inicialmente sin directivas legislativas claras ni una jurisprudencia consolidada. Sin embargo, esta retahíla de decisiones han acabado generando una jurisprudencia

[23] Las *sentencing guidelines* son reglas de determinación de las penas con el fin de asegurar unas condenas más determinadas y uniformes. Las fijan las comisiones penológicas (*Sentencing Commissions*), órganos independientes del poder legislativo, y son vinculantes para los jueces en sus tomas de decisiones. Es ilustrativa una visita a la comisión inglesa (<http://www.sentencing-guidelines.gov.uk/>), la federal norteamericana (<http://www.ussc.gov/>) o la de Minnesota, pionera en su momento y aún referente actual (<http://www.msgc.state.mn.us/index.htm>).

[24] Pueden servir como muestra las guías penológicas genéricas para la *probation* establecidas en el § 3553 del título 18 del *United States Code* (dónde se recogen los delitos federales) y la lista de condiciones específicas fijadas en el § 3563 (localizable en <http://www2.law.cornell.edu/uscode/>); *vid.* también la descripción de Hyne, Doug, «Examining the Legal Challenges to the Restriction of Computer Access as a Term of Probation or Supervised Release», *New England Journal on Criminal and Civil Confinement* 28, 2004, p. 236 y s.

[25] *Vid.* McKay, *supra* nota 9, p. 220, n. 142.

de los tribunales superiores[26] y, finalmente, las legislaciones y guías penológicas estatales y federales han empezado a prever expresamente estos supuestos.[27]

4. Al amparo de todo lo que se acaba de describir, han ido surgiendo diversos tipos de medidas.[28] Si dejamos de lado la confiscación de los equipamientos utilizados como instrumento de delito, en un principio la medida más habitual ha consistido en la *prohibición genérica* de poseer o usar las TIC. La casuística es muy diversa y va desde las interdicciones más radicales, como la de prohibir poseer o utilizar todo tipo de equipamiento fotográfico o de vídeo o cualquier otro dispositivo con capacidad de producir imágenes incluyendo ordenadores, escáneres e impresoras,[29] hasta prohibiciones más concretas, como la de tener un ordenador conectado a la red o, sencillamente, la de acceder a Internet.[30]

> Un ejemplo extremo es el de Kevin Mitnick,[31] un famoso *hacker*, que fue condenado a una pena de prisión no inferior a los cinco años. Una vez cumplida esta pena, tuvo que pasar un periodo de tres años de *parole* bajo condiciones estrictas: prohibición absoluta de poseer o usar cualquier tipo de ordenador o de otros equipamientos informáticos, teléfonos móviles o cualquier otro tipo de aparatos que permitieran la conexión a ordenadores, a sistemas informáticos o a redes de comunicaciones. Asimismo, tenía prohibida cualquier actividad profesional o privada relacionada con los ordenadores o mantener contactos con personas o grupos relacionados con estas actividades.

Sin embargo, muchos jueces han ido aceptando que las prohibiciones globales podían ser excesivas y, incluso, contraproducentes. Poco a poco algunas restricciones se han ido modalizando para evitar la práctica "muerte informática" que comportan medidas (a veces perpetuas) de alcance tan amplio y diverso que implican la imposibilidad de realizar actividades como usar el correo electrónico, efectuar una transferencia bancaria o trabajar de chofer en vehículos equipados con GPS. En consecuencia, se observa una tendencia a *permitir un acceso bajo control*, en el sentido de consentir usos determinados —laborales, educativos, etc.— o bien de prohibir sólo usos o actividades muy concretas (visitar sitios web pornográficos o de apuestas, "descargar" material de esta naturaleza, participar en chats, entrar en comunicación en línea con menores de cierta edad, etc.). Este enfoque presenta la ventaja de permitir un uso

[26] *Vid.* un ilustrativo recorrido por las decisiones de los circuitos federales en Wiest, *supra* nota 22, p. 850-861. También es de utilidad McKay, *supra* nota 9, p. 221-234 y Harrold, *supra* nota 1 p. 345-355.

[27] Puede consultarse una recopilación legislativa de diferentes estados norteamericanos en Harrold, *supra* nota 1, p. 359 y s.

[28] *Vid.* modelos en Bowker, Arthur / Michael Gray, «An Introduction tono the Supervision of the Cybersex Offender», *Federal Probation* 68-3, 2004, pp. 5-7; también es de utilidad Painter, Christopher M. E., «Supervised Release and Probation Restrictions in Hacker Cases», *USA Bulletin*, March 2001 (disponible en <http://www.usdoj.gov/criminal/cybercrime/usamarch2001_7.htm>).

[29] *Vid. United States v. Fields*, 324 F.3d 1025 (8th Cir. 2003), reseñado en Wiest, *supra* nota 21, p. 859 y s., y United *States v. Paul*, 274 F.3d 155 (5th Cir. 2001), reseñado en Harrold, *supra* nota 1, p. 352; un resumen de las medidas impuestas en otros casos en Harrold, p. 346, n. 253.

[30] *United States vs. Peterson 248 F.3d 79* (2nd Cir. 2001): al convicto por un delito de estafa se le había prohibido la posesión de ordenadores con acceso a Internet, pero se le autorizó la utilización del ordenador de su negocio equipado exclusivamente con el software útil para el ejercicio de su actividad profesional.

[31] Mitnick ha sido considerado por el Departamento de Justicia de los EE.UU. como el criminal informático más buscado de la historia.; *vid.* la descripción del caso en Hyne, *supra* nota 24, pp. 243-245 y Smith, *supra* nota 17, p. 4.

selectivo de las TIC, de manera que no se afecte la posible resocialización del sujeto, y ha sido impulsado por algunos tribunales federales.[32]

En cualquier caso, se presenta también el problema de las *medidas para controlar* el de las restricciones. En efecto, como condición para la concesión de la *probation* o la *parole* a ciberdelincuentes, los jueces y las agencias de supervisión norteamericanas exigen, por ejemplo, que el sujeto acepte de antemano visitas y registros sin previo aviso, la copia de toda la información, la retirada de dispositivos informáticos para una inspección más a fondo o la instalación de programas —a costa de la persona controlada (!)— que permitan la del ordenador o limitar y filtrar las actividades que se pueden realizar. Además, para asegurar la efectividad de estos sistemas de control, se imponen condiciones adicionales para hacer disminuir el riesgo de maniobras evasivas: obligación de utilizar sólo un ordenador determinado o un proveedor de servicios de Internet, prohibición u obligación de utilizar ciertos programas o sistemas operativos, proscripción de la entrada en cibercafés, locutorios o bibliotecas, etc.

6. ¿Ahora bien, por más que se acuerden estas medidas, es realmente factible su puesta en práctica y la de los controles correspondientes? ¿Y, si se puede hacer, es efectiva? De entrada podríamos contemplarlo con un cierto escepticismo, pero hay que tener presente que las agencias de supervisión en estos países, muy particularmente en los EE.UU., están mucho más desarrolladas que las nuestras y disponen de una colaboración muy estrecha por parte de otras instancias, especialmente de la policía. Por lo tanto, pueden recurrir, para detectar eventuales vulneraciones de las prohibiciones y la limitación en el uso de las TIC, a los métodos que ya utilizan habitualmente con otros delitos: las entrevistas a terceros, las inspecciones no anunciadas, la ocupación de dispositivos para ser examinados más a fondo, el control de los movimientos bancarios, el uso del polígrafo, etc.[33]

No obstante, cada vez tienen un papel más importante los programas informáticos de control del uso del ordenador, un software que fue creado inicialmente para la investigación de delitos informáticos o para la vigilancia del uso de los ordenadores en el ámbito laboral o familiar pero que ha encontrado aquí un nuevo campo de aplicación.[34] Se comercializan con nombres tan sugerentes (o inquietantes) como *Cyber Cop*, *Cyber Sentinel* o *Spector Pro* y, a estas alturas, ya son un próspero sector de negocios.[35] Básicamente estas aplicaciones son de tres tipos: *programas forenses*, que crean copias (totales o selectivas) de los archivos almacenados en los equipamientos informáticos del sujeto controlado y examinan sistemáticamente su contenido; *programas de* , que permiten registrar rutinariamente la actividad del ordenador (programas

[32] Vid., por ejemplo, *United States vs. Sofsky*, 287 F.3d 122 (2nd Cir. 2002); múltiples referencias a los trabajos indicados *supra* nota 26.

[33] *Vid.* Kelly, Brian, «Supervising the Cyber Criminal», *Federal Probation* (65-2), 2001, p. 8-10 y Bowker / Gray, *supra* nota 28, p. 4 y s.

[34] Curphey, *supra* nota 1, p. 2263 y s. y Harrold, *supra* nota 1, p. 340 y s., con referencias abundantes. Hay que tener presente que el estándar de prueba de una infracción técnica es menos estricto que el exigido para probar un delito, de manera que los requerimientos técnicos y procedimentales son también menores.

[35] El National Law Enforcement and Corrections Technology Center, dependiente del Departamento de Justicia, ofrece gratuitamente el *Field Search*, un programa para no expertos idóneo para inspeccionar los ordenadores de los infractores (disponible en <http://www.justnet.org/fieldsearch/>).

utilizados, teclas pulsadas, movimientos de correo electrónico, navegación por Internet, etc.) y, incluso, hacer un seguimiento en línea del uso del ordenador; y *programas de filtraje* o *de bloqueo*, que impiden el acceso a  o servicios no autorizados. Las posibilidades de control remoto del uso de las TIC mediante estos programas evolucionan constantemente, aunque exigen un seguimiento muy estricto y cada vez más preparación del personal y auxilio de expertos externos.

> Últimamente se están desarrollando otros sistemas de control que no están ubicados en los equipamientos del infractor. Así, se está trabajando en tecnologías que permitan la detección y el bloqueo del acceso a determinados  y redes a los convictos mediante la conexión de las bases de datos de los usuarios de estas redes con los registros de delincuentes sexuales.[36]

Obviamente, la puesta en práctica de todas estas medidas de vigilancia implica numerosas dificultades técnicas y organizativas, especialmente si tenemos en cuenta la habilidad de muchas de las personas sometidas a supervisión, a menudo superior a la de sus controladores. Pero, sobre todo, obliga a someter al sujeto a un grado de vigilancia sin par,[37] que, además, puede afectar a otras personas que convivan con el infractor o que utilicen los equipamientos sometidos a supervisión. De hecho, las restricciones en el acceso a las TIC pueden tener un contenido aflictivo más intenso que las condiciones tradicionales.

Con respecto a la efectividad del sistema, no tengo conocimiento de la existencia de estudios empíricos que traten este tema.[38] Parecen, sin embargo, medidas más adecuadas a un mundo de PC de sobremesa y un acceso a las redes a través de líneas telefónicas fijas que empieza a estar superado. La facilidad creciente de acceder por múltiples vías a las redes de información y para almacenar externamente información plantea, por lo tanto, serios interrogantes a la viabilidad de estas medidas.[39] En cualquier caso, si el objetivo no es asegurar una vigilancia constante sino un

---

[36] Redes como *My Space*¸ de gran popularidad entre los adolescentes (*vid. infra* nota 38) lo están desarrollando: cfr., sobre este tema, el comentario de Hines, Nichol, «Blocking Former Sex Offenders from Online Social Networks: Is this a Violation of Free Speech?» (<disponible en http://www2.law.duke.edu/journals/dltr/iblawg/>).

[37] De hecho, el grado de injerencia en la vida de las personas sometidas a control penal fuera de la prisión está llegando al mundo anglosajón a extremos inimaginables en otras latitudes. Se ha llegado al punto de condicionar la concesión de la *probation* o la *parole* a no tener hijos durante el periodo de control y, incluso, para garantizar el  de esta condición, se ha impuesto la obligación de tomar anticonceptivos (las famosas *Norplant probation conditions*¸ en referencia a la marca de los implantes que se suelen utilizar); véanse numerosas referencias sobre estas medidas, aplicadas sobre todo a mujeres drogodependientes y maltratadoras en Harrold, *supra* nota 1, p. 289, n. 34.

[38] No obstante, se observan indicios de que, como mínimo, se descubren algunas infracciones con los registros: *vid*, por ejemplo, *Addleman vs. King County*, 2007 U.S. Dist. LEXIS 35117 (W.D. Wash. May 14, 2007). Recientemente, los administradores de la red social *My Space* han enviado a las autoridades de diversos estados los nombres, direcciones y perfiles de sus usuarios, y centenares de personas sometidas a *probation* y *parole* con la prohibición de acceder a Internet o de entrar en contacto con menores han sido descubiertos en los EE.UU. (*vid.* «Parolees on MySpace may land in jail», *Usa Today*, 5 de junio de 2007, disponible en <http://www.usatoday.com/tech/news/2007-06-05-myspace-parolees_N.htm>).

[39] Así, entre las recomendaciones en el ámbito de la supervisión comunitaria efectuadas por el Grupo de Trabajo sobre Tecnologías presentado en el encuentro del *National Law Enforcement and Corrections Technology Center* de 2006 destaca la necesidad de crear nuevas herramientas para controlar el uso y el contenido de teléfonos móviles, PDA y otros medios (presentación disponible en <http://www.nlectc.org/nlectcrm/rac_jul2006.html>).

control esporádico que permita la revocación de la *probation* o la *parole*, el sistema parece que es practicable.[40]

El modelo de infracción controlable sería el siguiente: un individuo que cambia de acera cuando ve a un policía, es desempleado y se lo identifica. Al contrastarse su identidad en el coche patrulla aparece que está sometido a *probation* y las condiciones que le han sido impuestas. Se efectúa un registro corporal y del vehículo y se descubre un teléfono móvil y un lápiz de memoria.[41]

7. La otra cuestión primordial que se plantea es la de la *legitimidad*. En efecto, pese a su progresiva implantación, desde un principio ha existido en los EE.UU. una fuerte controversia jurisprudencial sobre la admisibilidad de estas medidas. Sin sentencias del Tribunal Supremo sobre la cuestión y con discrepancias notables entre los diversos circuitos federales, sin embargo se puede identificar una cierta tendencia a considerar que las prohibiciones absolutas de uso y acceso a las TIC comportan a menudo una limitación de la libertad desproporcionada y con efectos contraproducentes para la rehabilitación, especialmente si, además, existe la posibilidad de adoptar medidas menos radicales pero igualmente efectivas para proteger a la colectividad.

Así, algunos tribunales han rechazado condiciones consistentes en la prohibición genérica de uso de las TIC.[42] Entienden que no son admisibles porque sus efectos son análogos a los que hubieran tenido, hace unos años, las prohibiciones de hacer uso del teléfono, del correo o de la televisión y que pueden comportar, por ejemplo, la práctica imposibilidad de encontrar un trabajo, acceder a la educación no presencial, ejercer electrónicamente el derecho de voto, consultar un diario o, sencillamente, comprar un libro en *Amazon*. Por lo tanto, provocan una limitación muy drástica de la libertad de los sujetos implicados que les impide llevar una vida cotidiana con normalidad y se convierten en un obstáculo para su rehabilitación. Contrariamente, algún tribunal tampoco ha considerado suficiente compensar las prohibiciones genéricas con la habilitación de los supervisores para autorizar algunos usos concretos: «el oficial de *probation* se convierte en un censor que determina que [el condenado] pueda leer el *New York Times* en línea y no, en cambio, la versión de *Ulysses* en bibliomania.com».[43]

[40] *Vid.* infra V.1.

[41] Ejemplo inspirado en la importante sentencia *Samson vs.* California. 547 U.S. ___ (2006), disponible en <http://www.oyez.org/cases/2000-2009/2005/2005_04_9728/>, un caso de registro corporal sin motivo específico en que se descubre una posesión de drogas. El Tribunal Supremo, por mayoría, ha considerado que quién accede anticipadamente a la libertad, continúa bajo custodia legal de la Administración de justicia penal y, por lo tanto, tiene severamente limitado su derecho a la privacidad.

[42] *Vid. supra* nota 32. Recientemente *United States vs.* Voelker, No. 05-2858 (3d Cir. June 5, 2007), disponible en <http://circuit3.blogspot.com/2007/06/in-united-states-v.html>: «Prohibir de por vida el acceso a cualquier equipamiento informático y a Internet es funcionalmente equivalente a prohibirle a un convicto poseer revistas de pornografía infantil, la posesión de libros y revistas de cualquier tipo el resto de su vida». Sin embargo, una parte de los circuitos federales continúan defendiendo posiciones más restrictivas (*vid.* referencias a Wiest, *supra* nota 21, p. 860 y s.

[43] United States *vs.* Scott, 316 F.3d 733 (7th Cir. 2003), referencia a Wiest, *supra* nota 21, p. 856-558.

En cualquier caso, a pesar de la eventual adopción de restricciones más limitadas, se siguen presentando problemas en relación con las medidas de vigilancia y control que las acompañan, especialmente con respecto a la obligación de aceptar registros domiciliarios, sin necesidad de indicios de actuación indebida, o el monitoreo intensivo del ordenador y otros equipamientos, que provoca una limitación extrema de la privacidad del sujeto controlado y de los terceros que conviven o trabajan con el infractor. Con todo, incluso las líneas jurisprudenciales más liberales no han rechazado completamente estas condiciones. Los tribunales se limitan a exigir que los jueces determinen muy claramente las restricciones y las medidas de control y que, como "un a medida" (*narrowly tailored sanction*), se adapten a la gravedad de los hechos cometidos y a las peculiaridades del sujeto controlado.[44]

En definitiva, se consideran legítimas las medidas restrictivas y las correspondientes formas de control y vigilancia, si bien hace falta que se adopten las menos intrusivas según la tecnología disponible en cada momento. De esta manera se pretende que las finalidades aseguративas e incapacitadoras de las medidas sean compatibles con el desarrollo de una vida en libertad mínimamente normal y el mantenimiento de una cierta expectativa de privacidad.[45] Sin embargo, aunque la doctrina de las restricciones "hechas a medida" ha sido un avance, hay que saber que continúan teniendo efectos muy severos sobre la vida del infractor.

## IV. La prohibición de uso de las TIC en el sistema penal español

### 1. ¿Existe una pena de prohibición o restricción de uso de las TIC?

1. Hoy por hoy, el impacto de las TIC no ha comportado ninguna modificación en el sistema de penas español y no han aparecido sanciones que priven del disfrute de estos nuevos derechos como pena.[46]

Ciertamente, en el catálogo de penas previstas en la legislación penal española, no existe ninguna sanción similar. La única —y remota— posibilidad la encontraríamos en el catálogo de penas privativas de derechos del CP, en que se hace referencia en el artículo 39.*b* a «la inhabilitación especial para [...] profesión, oficio, industria o comercio u otras actividades determinadas en este Código [...] o de *cualquier otro derecho*». Esta pena de inhabilitación tiene como efecto la privación de la facultad de ejercer la actividad o el derecho que se vean afectados durante el tiempo de la condena. Aparentemente, dentro de esta previsión se podría incluir la prohibición de realizar actividades profesionales y laborales vinculadas con las TIC así como, de manera más genérica, la limitación del derecho a utilizarlas. No obstante, estas

[44] *Vid*., para todos, United States *vs.* Lifshitz, *supra* nota 1, y United States *vs.* Voelker, *supra* nota 42.
[45] Curphey, *supra* nota 1, p. 2272.
[46] Señala precisamente la necesidad de incorporar inhabilitaciones, suspensiones o limitaciones del acceso a sistemas informáticos y, sobre todo, a redes de comunicación, Anarte Borrallo, Enrique, «Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información», *Derecho y conocimiento*,vol. 1, 2001, p. 248 (disponible en <http://www.uhu.es/derechoyconocimiento/contenido.htm>).

posibles inhabilitaciones se tendrían que especificar en las penalidades establecidas en los preceptos de la Parte Especial del CP, pero en ninguna se establece específicamente una pena principal relacionada con las TIC. De hecho, si prestamos atención a las figuras delictivas más próximas a la cibercriminalidad, observamos que las penas previstas son las tradicionales penas de prisión y multa.[47]

2. Sin embargo podemos encontrar una fisura cuando estas inhabilitaciones actúan en calidad de *penas accesorias*, es decir, aquéllas que el Código permite imponer, a pesar de no estar previstas expresamente en la penalidad de un delito concreto, como un añadido a la pena principal, normalmente con la misma duración. En efecto, el artículo 56.1.3 CP establece que la inhabilitación especial para profesión, oficio, industria o comercio o cualquier otro derecho que se ha mencionado anteriormente puede ser una pena accesoria a las penas de prisión de menos de diez años, siempre que el ejercicio de la actividad o el derecho objeto de la inhabilitación haya tenido relación directa con el delito cometido y así lo establezca el juez en la sentencia. De esta manera la previsión de una pena de prisión habilita al juez para acordar una inhabilitación ajustada a las peculiaridades del caso.

Así, en un caso reciente de descubrimiento y revelación de secretos por intrusismo informático, un *hacker* ha sido condenado a un año de prisión (al apreciarse como atenuante su adicción a los videojuegos) y, como pena accesoria, a la *inhabilitación para el ejercicio de la profesión de administrador de sistemas y programador informático* durante el tiempo de la condena.[48] Por lo tanto, si se acuerda la suspensión de la pena de prisión o bien si el condenado tiene la oportunidad de trabajar durante la ejecución de la pena (como trabajo penitenciario o por estar en régimen abierto o en libertad condicional), el sujeto no se puede dedicar a las ocupaciones referidas.

Más compleja es la aplicación, como accesoria, de la inhabilitación especial «para cualquier otro derecho», que, para aquello que a nosotros nos interesa, podría abrir la puerta a restricciones de diverso tipo, la del derecho a utilizar ordenadores o teléfonos móviles, a navegar por Internet o a utilizar el correo electrónico. El motivo es que la falta de determinación de esta cláusula genera fricciones con las garantías constitucionales a la legalidad y la proporcionalidad, lo cual ha provocado que mayoritariamente sea interpretado de manera restrictiva.

Según eso, sólo sería admisible imponer, como pena accesoria a una pena de prisión, una privación de derechos que ya esté expresamente descrita como principal en algún otro delito: así es admisible como accesoria la inhabilitación del derecho a cazar o pescar o la pérdida de la posibilidad de obtener subvenciones o ayudas públicas, por estar previstas como principales en

[47] Cfr., simplemente, los casos de la pornografía con menores (art. 189 CP), la estafa informática (art. 248.2 CP) o los daños informáticos (art. 264.2 CP).

[48] Sentencia del Juzgado de lo Penal nº. 2 de Badajoz, de 21 de febrero de 2006 (*Diario La Ley*, nº. 6445, 21 de marzo de 2006, p. 1 y s.).

los artículos 302 y 334 CP, mientras que no es posible privar del derecho a utilizar tarjetas de crédito o de participar en chats, por no ser "penas legales".[49]

A pesar de todo, puede entenderse que la mención a «cualquier otro derecho» del artículo 56 CP abre la puerta a una serie de inhabilitaciones accesorias bastante amplia y, por consiguiente, sería posible introducir por esta vía restricciones en el uso de las TIC siempre que guarden alguna relación con el sistema de penas genérico.[50]

3. En cualquier caso, en la práctica, los tribunales raramente hacen uso de la facultad de inhabilitar para actividades profesionales vinculadas a las nuevas tecnologías, aunque no existan impedimentos legales. Y, con respecto a la más polémica «inhabilitación de otros derechos», no he detectado ningún caso en que se haya aplicado en este ámbito.

En efecto, aparte de alguna excepción encomiable como la del programador informático mencionado anteriormente, llama la atención que la accesoria que sistemáticamente se impone a los ciberdelincuentes sea la inhabilitación especial para el derecho de sufragio pasivo.[51]

Por otra parte, carentes como estamos de una ley de ejecución penal que regule adecuadamente la implantación práctica de las penas privativas de derechos, la ejecución de estas inhabilitaciones se limita a un requerimiento al condenado a fin de que se abstenga de ejercer la actividad o el derecho, sin ningún tipo de control o seguimiento. Su efectividad es, por lo tanto, casi nula. Más allá del voluntario, el único efecto que podrían tener las inhabilitaciones profesionales en el campo de las TIC sería que, con ocasión de la comisión de un nuevo delito, se detectara que se estaba realizando una actividad sobre la cual pesaba una inhabilitación y que, por lo tanto, se castigara por el correspondiente delito de de condena.

4. Finalmente, existen otras penas o consecuencias penales que pueden incidir en el uso de las TIC, pero de manera tangencial. Éste es el caso de:

- La prohibición de entrar en comunicación por cualquier medio con la víctima, sus familiares u otras personas, pena utilizada principalmente en los delitos de violencia de género, doméstica o familiar y que incluye cualquier medio informático o telemático (art. 48.2 CP).[52]

[49] *Vid.* el resumen de la problemática, crítico con la postura restrictiva, de Boldova Pasamar en Gracia Martín, Luis (coord.), *Tratado de las Consecuencias Jurídicas del Delito*, Valencia, Tirant lo Blanch, 2006, p. 137-140, con muchas referencias.

[50] Relación que existe, por ejemplo, con las prohibiciones de comunicación o con las inhabilitaciones para actividades para las cuales no hace falta licencia previa establecida expresamente en el CP.

[51] Para comprobarlo, es suficiente con consultar en las recopilaciones jurisprudenciales las esporádicas condenas por estafas o daños informáticos (art. 248.3 y 264.2 CP) o por descubrimiento y revelación de datos de carácter personal (art. 197.2 CP). Es probable, sin embargo, que sea responsable en buena parte una cierta dejadez de las acusaciones.

[52] Nada inusual en caso de violencia de género, doméstica o familiar: *vid*., por ejemplo, SABE Cantabria (Sec. 3ª) de 22 de diciembre de 2006, donde expresamente se condena un estudiante, que había enviado frases amenazadoras a su chica a través del *Messenger*, a «una prohibición de comunicarse con ella por cualquier medio —incluyendo Internet—» durante seis meses (*Diario La Ley*, nº. 6674, 19 de marzo de 2007, p. 1 y s.).

- El decomiso, que permite la confiscación de ordenadores y todo tipo de equipamientos que se hayan utilizado como medio o instrumento para la comisión de un delito (art. 127 CP).
- La prohibición a una persona jurídica de realizar actividades en el ejercicio de las cuales se haya cometido, favorecido o encubierto un delito (art. 129.1.*c* CP).[53]

5. En definitiva, las prohibiciones de uso de las TIC como pena se mueven en un marco legal discutible y tienen una aplicación práctica insignificante.

## 2. ¿Se puede restringir el uso de las TIC con motivo de la aplicación de medidas penales alternativas?

1. Tal como hemos visto en el apartado III de este trabajo, la prohibición o las restricciones en el uso de las TIC y su vigilancia puede encontrar un espacio de aplicación en el marco de la suspensión de la ejecución de la pena de prisión y en la libertad condicional, que, a grandes rasgos, se puede equiparar respectivamente a la *probation* y la *parole* del mundo anglosajón.

2. En términos generales, cuando una persona ha sido condenada a una pena privativa de libertad inferior a dos años y no tiene antecedentes penales,[54] la ejecución de la pena puede ser suspendida durante un periodo nunca superior a los cinco años, transcurrido el cual queda extinguida la responsabilidad penal. Esta suspensión está condicionada, en todo caso, por el hecho de que el reo no vuelva a delinquir durante el periodo de suspensión y por el de una serie de obligaciones y deberes que el juez sentenciador puede imponer si lo considera necesario. El catálogo de obligaciones, denominadas también *reglas de conducta*, se concreta en el artículo 83 CP, donde se prevén medidas de naturaleza tanto asegurativa (por ejemplo, prohibición de acercarse a la víctima) como rehabilitadora (por ejemplo, participación en programas formativos, laborales, culturales, de educación vial, sexual y otros similares). Si no se cumplen estas reglas, el juez las puede modificar, prorrogar el periodo de suspensión o, incluso, revocar la suspensión y proceder a la ejecución de la pena de prisión. En la práctica, los jueces suelen conceder casi siempre la suspensión a quien reúne los requisitos para acceder.[55]

[53] Como sería, por ejemplo, el caso de un delito publicitario a través de Internet o de una estafa telefónica mediante una línea 900, de manera que se restringiera el uso de estos medios por parte de la empresa. Hay que reconocer, sin embargo, que la puesta en práctica de las consecuencias accesorias aplicables a las personas jurídicas del artículo 129 CP ha sido muy escasa.

[54] En el caso de los drogodependientes, las penas pueden llegar hasta cinco años y es posible aplicarlo a personas con antecedentes.

[55] Cfr. Cid Moliné, José / Elena Larrauri Pijoan (coords.), *Jueces penales y penas en España. (Aplicación de las penas alternativas en la privación de libertad en los juzgados de lo penal)*, Valencia, Tirant lo Blanch, 2002, p. 104-106, con algunas matizaciones con respecto a personas sin antecedentes penales vigentes pero con un cierto historial delictivo. Confirman esta conclusión los datos de Cid Moliné, José, «La suspensión de la pena en España: descarcelación y reincidencia», *Revista de Derecho Penal y Criminología,* nº. 15, 2005, p. 230. Actualmente en Cataluña hay 3.326 personas sometidas a medidas penales alternativas (concepto que engloba otras medidas aparte de las "reglas de conducta") según el *Boletín de datos semanales de la Secretaría de Servicios Penitenciarios, Rehabilitación y Justicia Juvenil*, 30 de mayo 2007 [no publicado]. No se dispone, sin embargo, de datos sobre el

Por otra parte, una vez cumplidas las tres cuartas partes de la pena de prisión, los penados que reúnen una serie de requisitos —el más importante de todos, estar en el tercer grado de tratamiento penitenciario— pueden ser liberados bajo condiciones, de manera que cumplirán el último tramo de la pena en régimen de libertad. La condición necesaria para alcanzar finalmente la extinción de la pena es no volver a delinquir durante este periodo. Sin embargo, además, el juez de vigilancia penitenciaria puede imponer adicionalmente alguna de las reglas de conducta de la suspensión de la pena previstas en el artículo 83 CP. La falta de respeto a estas reglas comporta la revocación de la libertad provisional y el reingreso en la prisión. En Cataluña, un 24% de los penados consiguen extinguir la pena en libertad condicional.[56]

3. Así pues, la posible restricción del uso de las TIC que pueda hacer una persona en libertad condicional o con una pena suspendida se tendría que plasmar a través de la imposición de alguna obligación basada en el artículo 83 CP. De entrada, ninguna de éstas expresamente parece aplicable a las TIC.[57] Ahora bien, lo que aquí interesa, hay que destacar que el catálogo finaliza con una cláusula abierta (art. 83.1.6è): aquellos deberes que el juez convenientes para la rehabilitación social del penado, con la conformidad previa de éste, siempre que no atenten contra su dignidad como persona. Queda claro que no se trata de medidas exclusivamente asegurativas, pero las necesidades de los programas formativos de rehabilitación que también se prevén como una posible condición de la suspensión o de la libertad condicionales pueden requerir el acompañamiento de medidas para controlar al sujeto mientras no se adquieren los hábitos o las capacidades que se persiguen:

Así, por ejemplo, en la STS 913/2006, de 20 de septiembre (ponente Martín Pallín), se impone una pena de un año y seis meses de prisión por un delito de posesión de pornografía infantil (art. 189.2 CP), que ha sido obtenida en "comunidades de Microsoft" y en *chats*, y se condiciona la suspensión al seguimiento de programas formativos de educación sexual (art. 83.1.5). Éste es un caso en que el juez podría haber acordado la imposición de medidas de limitación del uso de las TIC basadas en el art. 83.1.6).

Un primer problema sería si esta previsión genérica puede dar cobertura, sin vulneración del principio de legalidad, a medidas restrictivas de uso de las TIC y, sobre todo, a las medidas de vigilancia que las acompañan. En cualquier caso, tendrían que quedar claramente fijadas en la

número de suspensiones revocadas, elemento que permitiría evaluar el grado de control real, si bien, según las decisiones judiciales disponibles, parece que la revocación no es nada usual.

[56] En el año 2004, según los datos de Tébar VILCHES, Beatriz, «La aplicación de la libertad condicional en España», *Revista de Derecho Penal y Criminología*, nº. 18, 2006, p. 288. Actualmente hay 9.334 reclusos y 749 liberados condicionales *(Boletín de datos semanales, supra* nota 55). No se dispone de datos sobre el número de revocaciones, pero la impresión, a la vista de la jurisprudencia disponible, es que no son tan excepcionales como la suspensión de la pena.

[57] De manera indirecta, la prohibición de acudir a determinados lugares (art. 83.1.1 CP) también podría tener alguna virtualidad: por ejemplo, la prohibición de entrada en cibercafés, en locutorios o en otros locales donde se facilite el acceso a redes de información.

decisión judicial y no sería admisible que se determinaran en sede administrativa.[58] Sin embargo, el principal obstáculo no está en la regulación legal, sino que en la práctica parece que se imponen pocas veces condiciones del artículo 83, al menos en su modalidad 6ª. Y, además, no existen bastantes recursos institucionales, materiales y humanos para dar un auténtico contenido a estas medidas.[59] Ciertamente, en los últimos tiempos se observa una mejora en este ámbito, especialmente a la Administración catalana, pero los esfuerzos en las medidas penales alternativas están centrados en sectores muy determinados, concretamente la deshabituación de drogodependientes y las medidas que, imperativamente, se tienen que aplicar a los autores de violencia de género, domésticas y familiares.

## V. Balance

1. Para entender bien la naturaleza y el auténtico objetivo de las medidas de prohibición y restricción de uso de las TIC en los EE.UU., hay que situarla en el contexto de la práctica penal dominante hoy día. En su origen, *probation* y *parole* se idearon como alternativas a la prisión de inspiración rehabilitadora, pero, a partir de los años ochenta, la situación cambió radicalmente.[60] Actualmente son más bien concebidas como sanciones complementarias a la prisión[61] y se orientan de manera prioritaria hacia la protección de la comunidad y la incapacitación del infractor. Así, se ha pasado a un modelo de gestión de riesgos (el riesgo de que el condenado vuelva a delinquir), en que prima la vigilancia y la inocuidad.[62]

Las agencias que operan en este campo se han visto desbordadas por las demandas sociales de seguridad y han abandonado el modelo resocializador, aparentemente caro, lento y de resultados inciertos. Optan por "manejar el riesgo" a través de la detección, mediante formas baratas de vigilancia, de nuevos delitos o, sobre todo, de simples infracciones técnicas, de manera que la tarea esencial de los funcionarios es la de retornar a la prisión los sometidos a *parole* y

[58] Es decir que, al amparo de una mención genérica en la sentencia, se dejara para los programas y planes de intervención, control o seguimiento elaborados por los servicios sociales penitenciarios la concreción de las reglas de conducta y las condiciones de control más severas de la suspensión o la libertad condicional (cfr, respectivamente, art. 17 en 20 RD 515/2005, de 6 de mayo, y art. 195 y s., Reglamento penitenciario). De hecho, en el caso de la libertad condicional, se ha llegado a cuestionar que estos servicios puedan realizar tareas de investigación y control (*vid*. Vega Alocén, Manuel, *La libertad condicional en el Derecho español*, Madrid, Civitas, 2001, p. 321 y s.).

[59] Cfr. el diagnóstico de Díez Ripollés, José Luis, «La evolución del sistema de penas en España: 1975-2003», *Revista Electrónica de Ciencia Penal y Criminología*, nº. 8, 2006, p. 22 y s. (disponible en <http://criminet.ugr.es/recpc/08/recpc08-07.pdf>). En efecto, existe un cierto acuerdo en que la falta de organización y de medios sólo permite un "control pasivo, administrativo y burocrático" (Vega Alocén, *supra* nota 58, p. 359 y s.; *vid*., también, Tébar Vilches, Beatriz, *El modelo de libertad condicional*, Cizur Menor, Thomson Aranzadi, 2006, p. 245).

[60] La más impresionante descripción y el análisis más lúcido de estos cambios es la obra de Garland, David, *La cultura del control. Crimen y orden social en la sociedad contemporánea* (trad. de Máximo Sozzo), Barcelona, Gedisa, 2005, *passim*.

[61] En el sentido de que cada vez más las legislaciones presentan las formas de libertad vigilada como una sanción adicional a la pena de prisión y no como una alternativa o un sustitutivo de ésta.

[62] Silva Sánchez, Jesús María, *La expansión del Derecho Penal. Aspectos de política criminal en las sociedades postindustriales*, 2ª ed., Madrid, Civitas, 2001, p. 141 y s., con múltiples referencias, entiende que este hecho es una manifestación de la "administrativización" del derecho penal dentro del fenómeno más global de su expansión.

*probation*.[63] En efecto, al someter a vigilancia intensiva a personas que están en situación de riesgo de volver a delinquir, se acaban detectando infracciones, a menudo inevitables pero que, mal gestionadas, implican la interrupción del proceso rehabilitador y el reingreso en la prisión. La conclusión es clara: instituciones que, en teoría, son alternativas a la prisión, con el objetivo de disminuir la reincidencia se convierten en generadoras de más reincidencia.[64]

Esta tendencia ha alcanzado cotas orwellianas en la guerra total iniciada contra la delincuencia sexual (en sentido muy amplio), catalizado por la especial problemática de los "depredadores sexuales" (agresores sexuales muy violentos y tal vez incorregibles).[65] No olvidemos que las restricciones en las TIC se han aplicado básicamente a delincuentes sexuales.

Visto todo lo anterior, queda claro que el objetivo de la imposición de prohibiciones de uso de las TIC en los EE.UU. no es apoyar la rehabilitación, ni tan solo incapacitar completamente y constantemente al sujeto, sino limitar simplemente las oportunidades delictivas y, sobre todo, introducir una infracción técnica susceptible de ser detectada a medio plazo y que justifique la revocación de la medida y el retorno a la prisión.

2. Por lo contrario, la situación en nuestro país es la opuesta. Como se ha visto, nuestro marco legal continúa orientado hacia un modelo rehabilitador, en el cual las medidas de control cumplen sobre todo una función auxiliar del tratamiento y casi no están reguladas, de manera que sería muy cuestionable un sistema de control del de las condiciones tan agresivo como el norteamericano. Por otra parte, a pesar de algunas mejoras en los últimos años, en la práctica nuestro aparato de ejecución penal en el entorno comunitario es muy débil, a duras penas puede hacer frente a las necesidades más urgentes y no está en condiciones de llevar a cabo un control intensivo del .[66] En definitiva, no sé si queremos pero está claro que no podemos llevar a la práctica las prohibiciones de acceso a las TIC con el alcance, la intensidad y el control del "modelo norteamericano".

---

[63] Jacobson, Michael, *Downsizing Prisons. How to Reduce Crime and End Mass Incarceration*, New York-London, New York University Press, 2005, p. 172.

[64] Jacobson, *supra* nota 63, p. 221. Los datos son significativos: según las estadísticas oficiales (*supra* nota 21), sólo el 59% de los sometidos a *probation* la finalizan con éxito mientras que, en el caso de la *parole*, sólo lo hace el 45%. La mitad de los reingresos en la prisión son por infracciones puramente técnicas; el paroxismo se alcanza en California, donde las tres cuartas partes de las personas en régimen de *parole* vuelven a la prisión por este motivo (Jakobson, p. 39-40 y 144 y s.).

[65] *Doe vs.* City of Lafayette, 377 F.3d 757 (7th Cir. 2004) es ilustrativo de a que extremo se ha llegado: un pederasta sometido a *probation* reconoce, en una sesión de su terapia de grupo, haberse detenido en un parque y haber estado fantaseando mientras miraba a los niños que jugaban. Objeto de una denuncia anónima, las autoridades locales le prohíben el acceso, entre otros lugares, a los parques públicos del municipio y los tribunales confirman que es legítimo sancionar el hecho de fantasear si se involucraban niños reales. Un resumen de este caso y del conjunto de medidas "creativas" (como la rebaja de los estándares de la prueba, la castración química y los registros públicos de delincuentes sexuales) puede verse en el inquietante trabajo de. Siverts, Jennifer B.,«Punishing Thoughts too Close to Reality: en New Solution to Protect Children from Pedophiles», *Thomas Jefferson Law Review* 27, 2004-2005, p. 393-419.

[66] Las revocaciones de las suspensiones de la pena o de la libertad condicional son esporádicas y siempre vinculadas a la comisión de nuevos delitos.

Haciendo de la necesidad virtud, podríamos decir que, dado que el modelo de control penal anglosajón parece rechazable, la imposibilidad de implantar medidas en el campo de las TIC no es un problema. Pero esta imposibilidad es también el síntoma de nuestras carencias reguladoras y organizativas globales para dar un enfoque rehabilitador al sistema penal. Me temo que, finalmente, no gestionamos ni el riesgo ni la rehabilitación.

3. Sin embargo, por poco que mejore la situación descrita, las restricciones de uso de las TIC pueden tener un —modesto— papel.

En tanto que pena, ya ha quedado clara la posibilidad de aplicar inhabilitaciones profesionales accesorias en el campo de las TIC, la cual se podría aprovechar más, especialmente en la cibercriminalidad patrimonial. De hecho, las dificultades de ejecución y control no serían muy diferentes de las que existen con las inhabilitaciones para profesiones y actividades no regladas.

Con respecto a la suspensión y la libertad condicional, creo que las restricciones (que no las prohibiciones absolutas) tienen razón de ser. En efecto, desde una perspectiva rehabilitadora, se tendrían que aprovechar los periodos de libertad supervisada para la adquisición de hábitos de uso responsable de las TIC.[67] Y se ha demostrado empíricamente que los tratamientos "no funcionan" si no van acompañados de un seguimiento y de una vigilancia apreciable.[68] La alternativa al modelo de gestiones de riesgos no es, pues, el de la rehabilitación sin control. Seguramente el problema no está en el grado de control sino en la finalidad de este control, así como en las consecuencias de los posibles incumplimientos. En un modelo rehabilitador, dichos incumplimientos se tienen que considerar en el seno de un proceso de tratamiento en que la recaída es previsible y el avance no es lineal, de manera que tiene sentido evitar sanciones automatizadas por infracciones técnicas. Partiendo de estas premisas, las medidas restrictivas y de vigilancia del uso de las TIC en el marco de las reglas de conducta de la suspensión y de la libertad condicional no sólo me parece que pueden tener cabida legal, sino que, en ciertos casos, pueden ser recomendables.[69]

Ciertamente, la severidad de las medidas y la necesidad de vigilancia son de tal magnitud que sólo pueden justificarse en sujetos con un riesgo de reincidencia muy elevado en la comisión de delitos muy graves (básicamente, en ciertos delincuentes sexuales y algunos ciberdelincuentes peligrosos) y son desproporcionadas en perfiles delictivos más comunes. Asimismo, habría que dar mayor cobertura normativa a las eventuales medidas de control de las reglas de conducta. Por otra parte, desde una perspectiva práctica, las dificultades de ejecución son tales que no parece que tenga sentido preconizar su aplicación general y sólo vale la pena recurrir a estas

[67] En el mismo sentido, Wiest, *supra* nota 21, p. 847, n. 2.

[68] *Vid*., en el famoso informe encomendado por el Congreso de los EE.UU., *MacKenzie, Doris*, «Criminal Justice and *Crime Prevention*», *en* Sherman, Lawrence W. *y otros, Preventing Crime: What Works, What Doesn't, What Promising*, National Institute of Justice, 1998, p. 9-26 y s., 9-56 y 9-61 (disponible en <http://www.ncjrs.gov/works/>). De la misma autora, actualizando el planteamiento, *What works in corrections: reducing the criminal activities of offenders and delinquents*, New York, Cambridge University Press, 2006.

[69] Cuestión diferente es si no sería recomendable separar, hasta donde sea posible, las tareas de tratamiento y rehabilitación y las de vigilancia y control.

medidas cuando la utilización de las TIC constituya la vía principal para manifestar su peligrosidad criminal.

En cualquier caso, el futuro de estas posibles penas y medidas está condicionado por el hecho de que el legislador y el sistema de justicia criminal desarrollen, legalmente e institucionalmente, de forma plena un sistema de ejecución penal que no esté basado esencialmente en la prisión.