

DEMANAR LA LLUNA EN UN COVE? SOBRE LA POSSIBILITAT DE PROHIBIR PENALMENT L'ÚS DE LES TECNOLOGIES DE LA INFORMACIÓ I LA COMUNICACIÓ*

David Felip i Saborit**

Sumari

- I. Prefaci
- II. Introducció
- III. El model nord-americà
- IV. La prohibició d'ús de les TIC al sistema penal espanyol
 1. Existeix una pena de prohibició o restricció d'ús de les TIC?
 2. Es pot restringir l'ús de les TIC amb motiu de l'aplicació de mesures penals alternatives?
- V. Balanç

* Aquest treball s'emmarca en el projecte «Diez años del nuevo derecho penal de la criminalidad en la empresa: la intención del legislador y la actuación del sistema judicial», finançat pel Ministeri d'Educació i Ciència, Pla nacional d'R+D+I (referència: SEJ2005-03425/JURI). Totes les pàgines web eren accessibles el 10 de juny del 2007.

** David Felip i Saborit, professor titular de dret penal del Departament de Dret de la Universitat Pompeu Fabra, c/ Ramon Trias Fargas, 25-27, 08005 Barcelona, david.felip@upf.edu.
Article rebut el 29.06.2007.

I. Prefaci

El 8 de febrer del 2001, agents de l'FBI es van presentar a casa de la família de Brandon Lifshitz. Investigaven intercanvis de pornografia infantil en els quals estava involucrat l'ordinador de la seva mare. Lifshitz es va mostrar col·laborador i va admetre als agents que havia descarregat i difós a través d'Internet material d'aquesta mena. La família va consentir l'escorcoll dels seus ordinadors, on hi havia emmagatzemades nombroses fotografies. Lifshitz fou acusat d'un delictes federal per recepció i intercanvi interestatal de pornografia infantil. Gràcies a diversos informes sobre els seus problemes psíquics i a un acord amb el fiscal, finalment fou condemnat únicament a tres anys de *probation* (període de suspensió condicionada de la condemna). Ara bé, el jutge li va imposar, com a condició de la *probation*, mesures de control del seu ordinador. Concretament se li exigia que acceptés la instal·lació de sistemes que permetessin als funcionaris supervisors vigilar i filtrar l'ús de qualsevol equipament informàtic que posseís o controlés el condemnat. Addicionalment, havia de consentir l'examen sense avís previ dels equipaments esmentats, incloent-hi la còpia de tota mena de dades així com el comís de qualsevol element dels equips amb l'objectiu d'examinar-lo més a fons.¹

És possible la imposició de mesures similars al nostre país en l'actualitat? Si no és així, és previsible que, en el futur, se n'adoptin? Destinaré les properes pàgines a intentar donar resposta a aquestes qüestions.

II. Introducció

1. La incidència de les tecnologies de la informació i la comunicació (TIC)² sobre el món de la criminalitat i del dret penal creix per moments. El seu sobtat

1. *United States vs. Lifshitz*, 369 F.3d 173 (2d Cir. 2004). Vegeu un resum del cas a Curphey, Shauna, «*United States v. Lifshitz: Warrantless Computer Monitoring and the Fourth Amendment*», *Loyola of Los Angeles Law Review* 38, 2004-2005, p. 2251 i s., i a 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 i s. Després de recórrer la decisió, la defensa va aconseguir que els escorcolls només es poguessin portar a terme en cas de sospites raonables d'actuació incorrecta, i no en el cas de la vigilància a distància, que podia realitzar-se discrecionalment.

2. Conjunt de tecnologies utilitzades per processar i transmetre informació en format digital.

desenvolupament ha comportat, entre altres efectes, un increment de la perillositat de les conductes delictives convencionals (per exemple, les estafes o les defraudacions de la propietat intel·lectual). D'altra banda, ha implicat també una modificació profunda del *modus operandi* d'altres delictes (per exemple, la difusió de continguts il·lícits, amb la pornografia infantil com a cas paradigmàtic, o la pederàstia). Finalment, ha provocat l'aparició d'una nova generació de delictes que tenen les TIC com a objecte (per exemple, accessos il·lícits a sistemes i xarxes, disseminació de virus i causació d'altres danys informàtics, intercepció de comunicacions, etc.).

Davant d'aquest fenomen, la primera preocupació des del dret penal ha estat adequar els tipus delictius i els criteris d'imputació de la responsabilitat a la nova situació. Mentrestant, des del dret processal la prioritat ha estat fer front als nous problemes tècnics de persecució i de prova d'uns fets en els quals, a més, es veuen implicades normalment les jurisdiccions de diversos països.³

2. En canvi, la revolució de les TIC no ha tingut encara tanta incidència sobre les penes i altres conseqüències jurídiques del delictes, almenys a Europa. Tanmateix, a cavall d'aquestes tecnologies, s'albira un seguit de mesures penals «postmodernes» que impliquen canvis suggeridors, que potser ens permetran superar o limitar el recurs a la pena de presó.⁴ No obstant això, existeix el risc que, tal vegada, aquestes mesures es converteixin en el motor d'una transformació, profunda i preocupant, del sistema penal, cap a situacions de supervisió intensiva, en què la custòdia carcerària sigui només un episodi intermitent dins d'un quadre més ampli de control permanent sobre capes senceres de la població.⁵

3. Una visió general d'aquests problemes, des de la perspectiva espanyola, pot aconseguir-se, entre d'altres, amb l'obra col·lectiva de Romeo Casabona, Carlos María (coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, Comares, 2006. Fins al moment, la culminació d'aquests esforços s'ha materialitzat en el Conveni sobre Cibercriminalitat de 23 de novembre del 2001, impulsat pel Consell d'Europa (disponible a <<http://conventions.coe.int>>) i que ha estat ratificat també per països com els EUA (i no per Espanya, malgrat haver-ne estat signatària).

4. *Vid.* l'informe de Crowe, Ann H. *et al.*, *Offenders Supervision with Electronic Technology*, American Parole and Probation Association, Lexington, 2002, p. 57-69 (disponible a <<http://www.ncjrs.gov/pdffiles1/nij/grants/197102.pdf>>), que comença a ser superat pels canvis tecnològics: control de moviments amb GPS, identificacions a distància, anàlisis telemàtiques, control instantani del consum d'alcohol i d'altres drogues, etc.

5. *Vid.* l'inquietant escenari per a l'any 2016 descrit a Murakami Wood, David (ed.), *A Report on the Surveillance Society*, Londres, 2006 (disponible a <<http://www.privacyconference2006.co.uk/>>).

La recent i ràpida expansió de la vigilància electrònica pot ser la pionera en aquesta evolució paradoxal.⁶

Si ens endinsem una mica més en la reflexió, apareix la qüestió de si les TIC, a més d'un instrument per punir, poden ser també *l'objecte* de penes i mesures penals, és a dir, si, com a conseqüència de la comissió d'un delictes, té sentit i és factible prohibir o restringir, per exemple, la possessió o l'ús d'ordinador o l'accés a Internet.⁷ D'entrada, la resposta és que, si exceptuem els efectes implícits a la pena de presó, mesures d'aquesta mena ni semblen necessàries, ni són tècnicament factibles, i, consegüentment, no estan previstes a la majoria de legislacions, entre les quals l'espanyola. Això no obstant, una mirada més acurada a la nostra legislació i, sobretot, a les darreres experiències al món anglosaxó que veurem més endavant, justifica una anàlisi més detallada de la qüestió.

3. De fet, la irrupció i l'àmplia difusió de les TIC ha generat la *possibilitat* de crear noves penes. Avui dia, limitar o prohibir l'ús de les TIC a una persona és privar-la de quelcom valuós i, per tant, *podria ser una pena*. En efecte, és un mal des d'un punt de vista estrictament material: implica una restricció de drets de l'individu i es pot quantificar econòmicament (es limiten les seves possibles activitats professionals i d'oci, comporta pèrdua de temps en la vida quotidiana, etc.). Així mateix, la privació de les TIC és també percebuda psicològicament per moltes persones com un mal i pot ocasionar un patiment gens negligible. Especialment ara que l'accés a aquests tecnologies s'ha generalitzat, la seva possessió i el seu ús són cada vegada més preuats, tant per a l'autoestima personal com per a la interrelació social. Per tant, una restricció en l'àmbit de les TIC pot servir com a pena. Té un contingut aflictiu apreciable des d'una perspectiva de retribució del fet que s'ha comès i també des d'una òpti-

6. Les mesures de vigilància electrònica, encarnada per les famoses «polses electròniques», estan plenament implantades en el món anglosaxó i sembla que s'estan consolidant com una alternativa a la presó a tota l'Europa continental, després de superar l'allau de crítiques que van originar inicialment. Almenys, aquesta és la conclusió a la qual, des del *Max Planck Institut*, arriba Hans-Joerg Albrecht a *Electronic Monitoring in Europe. A Summary and Assessment of Recent Developments in the Legal Framework and Implementation of Electronic Monitoring*, Freiburg i. B., 2005 (disponible a <<http://www.mpicc.de/shared/data/pdf/albrecht.pdf>>). Respecte a la seva implantació al nostre país, *vid.* Gudín Rodríguez-Magariños, Faustino, *Cárcel electrónica. Bases para la creación del sistema penitenciario del siglo XIX*, València, Tirant lo Blanch, 2007.

7. Qüestió que em fou plantejada pel meu col·lega de la Universitat Pompeu Fabra, el professor Xavier Bernadí, i que ha provocat l'elaboració d'aquest treball.

ca de prevenció general de delictes, és a dir, és una mesura que pot dissuadir els delinqüents potencials i satisfer el conjunt de la societat quan espera una reacció davant de certs delictes, sobretot si no són fets gaire greus i sempre que es garanteixi el compliment de la mesura. En definitiva, les prohibicions d'ús de TIC són en teoria aptes per configurar-se com una nova pena privativa de drets, juntament amb les que ja existeixen en l'actualitat, com, per exemple, la privació del dret a conduir vehicles o la inhabilitació per a l'exercici d'una professió.⁸

4. D'altra banda, la irrupció i l'ús de les TIC en l'activitat delictiva provoca la *necessitat* de modificar el contingut de les mesures penals actuals. Aquesta necessitat apareix, especialment, quan es tracta de castigar noves manifestacions delictives, la denominada *cibercriminalitat*, entesa en sentit ampli: des del pederasta que utilitza els *xats* per localitzar víctimes fins al *hacker*, passant per l'estafador informàtic. En efecte, de la mateixa manera que amb altres delinqüents s'intenta controlar l'accés a les drogues o a les armes de foc, en aquest àmbit, la perillositat criminal dels infractors, és a dir, el risc que tornin a cometre fets delictius, està molt vinculada a les possibilitats d'ús de les TIC.⁹ Per tant, quan una persona responsable de fets d'aquesta mena està sotmesa a mesures penals que no impliquen privació efectiva de llibertat, es presenta el problema de si és legítim i factible controlar la seva perillositat criminal prohibint o limitant, per exemple, la utilització de l'ordinador o del telèfon mòbil, l'accés a xarxes de comunicacions, etc. En definitiva, a banda d'un càstig, aquestes mesures es poden concebre també com un instrument per assegurar el risc que comporta l'infractor i per contribuir a la seva rehabilitació.¹⁰ Des d'aquesta perspec-

8. Cfr. el catàleg de penes privatives de drets als articles 39 i s. del Codi penal (CP).

9. Una mostra de les noves necessitats de control que generen les TIC són certes formes de delinqüència sexual, singularment la pederàstia: *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 i McKay, Brian W., «Guardrails on the Information Superhighway: Supervising Computer Use of the Adjudicated Sex Offender», *West Virginia Law Review* 106, 2003-2004, p. 205-212, amb referències abundoses. L'ús d'aquestes tecnologies s'ha convertit en un element essencial en la dinàmica de comissió d'aquesta mena de fets, especialment pel *grooming* (procés de manipulació de les víctimes per reduir la resistència als abusos) i perquè facilita la formació de comunitats que mitiguen l'aïllament social i donen suport i legitimen aquests comportaments.

10. En efecte, saber que s'està sota control pot ser un element que ajudi l'infractor a superar la temptació de reiterar les conductes delictives i, per tant, ser un element de suport de les eventuals teràpies; tant per a un pederasta que sap que el seu ordinador està intervingut, com per a un drogodependent que sap que l'endemà ha de passar una anàlisi de control periòdic.

tiva, la prohibició o restricció d'accés a les TIC pot donar contingut a mesures cautelars, de seguretat o a mesures alternatives a la presó de naturalesa preventiva especial.

5. Finalment, les TIC plantegen *nous reptes* a la pena criminal per excel·lència, és a dir, la presó, tant pel que fa al contingut com a l'execució.

En primer lloc, perquè la presó sembla que implica una severa restricció de l'accés a les TIC, si bé les raons poden no ser del tot clares. Així, es podria pensar que la limitació és inherent al mateix «sentit de la pena» (art. 25.2 CE), en tant que aquesta comporta un cert apartament de la societat i que, per tant, l'Administració penitenciària pot modular lliurement l'eventual accés a les TIC d'acord amb les necessitats de tractament, tal com es fa amb altres aspectes de la privació de llibertat.¹¹ O, per contra, es pot entendre que la presó no implica, en tant que pena, la privació de l'accés a les TIC i que, per tant, la justificació de les restriccions en aquest àmbit ha de ser purament instrumental, és a dir, acceptable només per motius regimentals o de seguretat.¹² Si fos així, caldrà valorar molt acuradament la proporcionalitat de qualsevol restricció que s'apliqui en aquest camp, especialment si entra en col·lisió amb determinats drets fonamentals.¹³

La STC 140/2002, de 3 de juny, sembla orientar-se d'acord amb aquesta segona perspectiva. El TC no va atorgar l'empara a un pres a qui havia estat denegada la disposició, per raons d'estudis, d'un ordinador a la seva cela i només se li permetia que l'emprés en una sala destinada a tal efecte. El Tribunal va entendre que

11. Tal com succeeix amb les sortides a l'exterior (cfr. STC 204/1999, de 8 de novembre) o la pràctica de relacions sexuals (cfr. STC 89/1987, de 3 de juny).

12. O, encara que sembli paradoxal, per necessitats del tractament. En efecte, des d'aquesta perspectiva, si bé per regla general s'ha de potenciar l'ús de les TIC per part de la majoria d'interns, també se n'ha de privar aquells interns que manifestin, en determinades fases del tractament penitenciari, una especial perillositat en relació amb les TIC. Pensi's, per exemple, en el pederasta que les utilitza per continuar en contacte amb la seva comunitat o el maltractador que les empra per continuar amenaçant la seva parella.

13. Serveixi d'exemple d'aquest plantejament la STC 89/2006, de 27 de març, en què es declara que les condicions en les quals es porta a terme un escorcoll en una cel·la (sense informar-ne de manera coetània o posterior l'intern afectat) constitueixen una vulneració del dret fonamental a la intimitat innecessària. Supera, en canvi, el test constitucional de proporcionalitat i s'entén que no es vulnera el dret a rebre informació (art. 20.1.d CE) la retenció d'unes revistes destinades a un penat amb un historial terrorista important (STC 11/2006, de 16 de gener).

es tractava d'una modulació acceptable del dret a l'educació (art. 27.1 CE) per raons de seguretat i d'organització del règim del centre.

Tanmateix, la concreció del contingut i l'abast d'aquestes restriccions esdevé problemàtica, atès que bona part de la normativa penitenciària fou elaborada quan les TIC no existien o es trobaven en un estat incipient¹⁴ i no ha estat encara objecte de tractament doctrinal.

En segon lloc, aquestes tecnologies impliquen un repte perquè esdevenen un instrument del règim i del tractament penitenciari d'especial importància, ja que permeten superar moltes de les barreres inherents a la presó i desenvolupar les diferents activitats en condicions similars a les existents en llibertat, des de l'assistència mèdica o les visites dels advocats fins als estudis no presencials o la capacitació professional.¹⁵ Òbviament, es produiran tensions entre aquest corrent favorable a la introducció de les TIC a la presó i la tendència restrictiva indicada anteriorment.¹⁶

I, en tercer lloc, perquè en permetre noves formes de control i vigilància sobre les persones s'amplien les possibilitats d'executar les penes i mesures privatives de llibertat en règim obert: així, per exemple, el control telemàtic pot com-

14. L'única menció la trobem a l'article 129 del Reglament penitenciari, que preveu la possibilitat d'autoritzar la disposició d'un ordinador personal per raons de caràcter educatiu o cultural i que, en tot cas, prohibeix la connexió a xarxes de comunicació. Així, a Catalunya la qüestió ha estat desplegada per la Instrucció 1/2006, que regula la disposició d'ordinadors personals, i la Instrucció 7/2006, pel que fa a la telefonia mòbil d'interns en règim obert quan es trobin als centres penitenciaris. (disponibles a <http://www.gencat.net/justicia/temes/reinsercio_i_serveis_penitenciaris/centres/instruccions/index.html>).

15. A tall d'exemple, el Departament de Justícia de la Generalitat de Catalunya ha engegat una sèrie d'actuacions per al foment de l'ús de les TIC als centres penitenciaris. Entre aquestes, destaca la creació de *Punts Òmnia*, una iniciativa per facilitar l'accés a les TIC a la població en general (vid. <<http://xarxa-omnia.org/>>) i que, a partir de l'any 2001, s'han anat instal·lant a la majoria de centres. La iniciativa no es limita a facilitar uns determinats equipaments i l'accés –controlat– a Internet sinó que s'hi desenvolupen diferents activitats per aconseguir «l'alfabetització digital dels interns» (vid., per exemple, alguns blocs elaborats pels interns a <<http://www.bloggersdes-deprison.blogspot.com>>, fruit de l'experiència *Òmnia Blogger*). D'altra banda, alguns mòduls penitenciaris disposen també d'aulas d'informàtica, però l'equipament és molt precari i no tenen accés a Internet (informació facilitada amablement per la Direcció General de Recursos i Règim Penitenciari).

16. En efecte, la principal preocupació, pel moment, és controlar l'accés a xarxes exteriors. Així, pel que fa als equipaments personals, en cap cas es permet la possessió d'ordinadors portàtils ni l'accés a xarxes de comunicació (vid. Instrucció 1/2006, nota 14), mentre que el control als *Punts Òmnia* s'exerceix a través d'un tallafocs elaborat *ad hoc* que impedeix enviar informació a l'exterior.

portar un increment de les sortides programades, la concessió del règim obert als interns en tercer grau, més limitacions en l'adopció del la presó provisional, etc. La possibilitat de controlar l'accés i l'ús de les TIC podria ser també un factor addicional de control i disminució del risc que permeti una aplicació més àmplia de les mesures esmentades.

6. En definitiva, per la seva naturalesa, les prohibicions i el control de l'ús de les TIC podrien ser una nova pena si així ho decidís el legislador però, a més, és una possibilitat que s'ha de considerar en l'aplicació actual de mesures penals no privatives de llibertat a ciberdelinqüents i, de fet, és ja un problema real en l'execució penitenciària ordinària. Per qüestions d'extensió, en aquest treball analitzaré més a fons el dos primers aspectes esmentats.

III. El model nord-americà

1. Si busquem en dret comparat penes o mesures penals en matèria de TIC, podem observar amb una certa sorpresa que des de mitjan anys noranta s'està experimentant intensament als països anglosaxons amb aquestes sancions, singularment als EUA.¹⁷ Per als nord-americans no són excepcionals les prohibicions d'usar ordinadors, telefonia mòbil i altres equipaments informàtics, d'accedir a Internet, d'utilitzar el correu electrònic o de participar en xats. Es tracta de mesures que s'apliquen bàsicament a persones convictes per ciberdelictes, molt especialment per delictes sexuals relacionats amb menors i per intrusisme i sabotatge informàtic. El cas Lifshitz, ressenyat al prefaci d'aquest treball, en pot ser l'arquetipus. Ocasionalment aquestes mesures s'apliquen també als autors de delictes convencionals en els quals les TIC han estat l'instrument del delicte.¹⁸ En canvi, a Europa sembla que aquestes mesures són desconegudes, si bé darrerament es detecten moviments significatius

17. Cfr. l'estudi empíric portat a terme pel criminòleg australià 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 a <<http://www.aic.gov.au/publications/tandi2/tandi286.html>>). En efecte, deixant de banda alguns casos aïllats detectats a Austràlia i Canadà, la immensa majoria de casos provenen dels EUA.

18. Així, un jove australià de 17 anys va estar acusat de temptativa d'assassinat d'un home que va conèixer en un xat i li fou imposada, com a mesura cautelar, la prohibició d'ús d'Internet excepte per a finalitats educatives i un «toc de queda» informàtic a partir de les 9 del vespre (Smith, *supra* nota 17, p. 1).

al Regne Unit.¹⁹ Per tant, en aquest àmbit podem parlar del «model nord-americà».²⁰

2. Aquestes restriccions han aparegut en el camp de la supervisió comunitària (la intervenció penal que opera fora de les presons) en forma de condicions per accedir a la *probation*, la *parole* o la *supervised release*. Es tracta de situacions de llibertat vigilada que s'imposen com a conseqüència de la comissió de delictes.²¹ La *probation* presenta moltes similituds amb la suspensió de la pena del CP espanyol; s'aplica a persones declarades culpables de delictes no gaire greus i consisteix a deixar en suspens el pronunciament de la condemna durant un període de prova. La *parole* s'assembla a la nostra llibertat condicional; s'atorga a presos que són posats en llibertat abans d'haver complert enterament la seva pena. Finalment, la *supervised release* o alliberament sota vigilància és una figura pel moment sense equivalent a Espanya.²² Està prevista per ser aplicada una vegada el penat ha complert tota la pena de presó i és alliberat i, de fet, és gestionada com una modalitat de *parole* i pot arribar a ser imposada a perpetuïtat. Doncs bé, quan un jutge o un *parole board* acorda

19. En efecte, darrerament des de diverses instàncies s'ha assenyalat la possibilitat d'introduir prohibicions i vigilància de l'ús de les TIC per part del delinqüents sexuals a l'empara de la *Sexual Offences Act*, aprovada el 2003, especialment a través de la *Sexual Offence Prevention Order*, que permet imposar diverses mesures als acusats i convictes per aquesta mena de delictes: *vid.* les directrius establertes al *Sex Offender Strategy for the National Probation Service*, setembre de 2004, p. 16 (disponible a <<http://www.probation.homeoffice.gov.uk/output/page32.asp>>). Recentment, a l'informe, encarregat per la *Risk Management Authority* d'Escòcia, de la criminòloga Davidson, Julia, *Current Practice and Research into Internet Sex Offending*, gener de 2007, p. 51 i s. i 69 (disponible a <<http://www.rmascotland.gov.uk/rmapublications.aspx>>), es recull la demanda generalitzada en aquest sentit per part dels responsables policials i d'execució penal del Regne Unit.

20. Amb totes les cauteles i en un intent de simplificació màxima, ateses les notables diferències, legals i pràctiques, que existeixen entre els diferents estats.

21. Una referència succinta del sistema federal a McKay, *supra* nota 9, p. 219-220 i Wiest, Christopher, «The Netsurfing Split: Restrictions Imposed on Internet and Computer Usage by Those Convicted of a Crime Involving a Computer», *University of Cincinnati Law Review* (72), 2003-2004, p. 848-850. Per fer-se el càrrec de les dimensions del fenomen, amb 5 milions de persones sota vigilància, *vid.*, senzillament, el butlletí del *Bureau of Justice Statistics*, «Probation and Parole in the United States», 2005 (disponible a <<http://www.ojp.usdoj.gov/bjs/pub/pdf/ppus05.pdf>>).

22. En el projecte de reforma al CP, actualment en curs però que sembla paralitzat, es preveu una nova pena, la «llibertat vigilada», que en ocasions pot ser aplicada com a pena addicional a la pena de presó en cas de reincidència (cfr. nous art. 48.4, 88 i 94 CP segons el Projecte de llei 121/000119, *Boletín Oficial de las Cortes Generales, Congreso de Diputados*, Sèrie A, Projectes de Llei, 15 de gener de 2007, núm. 119-1).

alguna mesura d'aquesta mena, imposa, discrecionalment o per ministeri de llei, l'observança de determinades condicions al subjecte. Aquestes condicions estan destinades a fer disminuir durant el període de control la capacitat i l'oportunitat de cometre nous delictes, així com a facilitar la rehabilitació del delinqüent. La seva naturalesa és diversa: abstenir-se de determinades activitats (no delinquir, no consumir alcohol o drogues, evitar certs llocs i establiments, etc.), complir certes obligacions (seguir un tractament, viure a un determinat lloc, conservar una feina, etc.) i facilitar el control i la vigilància (entrevistar-se periòdicament amb els supervisors, acceptar escorcolls, sotmetre's a anàlisis, etc.). Durant el temps de duració de la mesura, es controla amb una certa intensitat l'evolució del subjecte i el compliment de les condicions. La seva vulneració (les denominades *infraccions tècniques*) implica un enduriment de les condicions o bé la revocació de la situació de llibertat del subjecte i l'ingrés a la presó. Aquesta decisió normalment l'adopta el jutge però amb requisits, sobretot de prova, menys estrictes que si es tractés de la comissió d'un delicte.

3. Per consegüent, aquesta mena de mesures han estat el medi idoni per a l'aparició de les mesures penals restrictives de les TIC. En efecte, si bé les legislacions i les guies penològiques²³ detallen moltes de les condicions que es poden imposar, també permeten que els jutges n'estableixen de pròpies, sempre que estiguin relacionades amb el delicte concret, i que siguin necessàries per protegir la societat i rehabilitar l'infractor i no suposin una restricció de la llibertat raonablement innecessària.²⁴ Per aquesta via, els tribunals i les agències de supervisió s'han adaptat als canvis tecnològics i han introduït mesures «creatives» com, per exemple, la utilització del *polígraf* o dels test de drogues

23. Les *sentencing guidelines* són regles de determinació de les penes per tal d'assegurar unes condemnes més determinades i uniformitzades. Les fixen les comissions penològiques (*Sentencing Commissions*), òrgans independents del poder legislatiu, i són vinculants per als jutges en les seves preses de decisions. És il·lustrativa una visita a la comissió anglesa (<<http://www.sentencing-guidelines.gov.uk/>>), la federal nord-americana (<<http://www.ussc.gov/>>) o la de Minnesota, pionera en el seu moment i encara referent actual (<<http://www.msgc.state.mn.us/index.htm>>).

24. Poden servir de mostra les guies penològiques genèriques per a la *probation* establertes al § 3553 del títol 18 de l'*United States Code* (on es recullen els delictes federals) i la llista de condicions específiques fixades al § 3563 (localitzable a <<http://www2.law.cornell.edu/uscode/>>); *vid.* també la descripció 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 i s.

per tal de detectar infraccions tècniques²⁵ o, pel que aquí ens interessa, les restriccions en l'ús d'ordinadors i en l'accés a les xarxes d'informació.

Així, a partir de mitjan anys noranta van aparèixer mesures d'aquesta mena que s'aplicaven especialment als posseïdors i traficants de pornografia infantil i als delinqüents sexuals que havien utilitzat les TIC per establir contacte amb menors i, posteriorment, aquestes mesures van estendre's a altres ciberdelictes. Les mesures restrictives en l'ús de noves tecnologies són, per tant, fruit de la pràctica disseminada de jutges i funcionaris de *probation* i *parole*, inicialment sense directives legislatives clares ni una jurisprudència consolidada. Tanmateix, aquest reguitzell de decisions han acabat generant una jurisprudència dels tribunals superiors²⁶ i, finalment, les legislacions i guies penològiques estatals i federals han començat a preveure expressament aquests supòsits.²⁷

4. A l'aixopluc de tot el que s'acaba de descriure, han anat sorgint diverses menes de mesures.²⁸ Si deixem de banda la confiscació dels equipaments emprats com a instrument de delictes, en un principi la mesura més habitual ha consistit en la *prohibició genèrica* de posseir o usar les TIC. La casuística és molt diversa i va des de les interdiccions més radicals, com la de prohibir posseir o utilitzar tota mena d'equipament fotogràfic o de vídeo o qualsevol altre dispositiu amb capacitat de produir imatges incloent-hi ordinadors, escàners i impressores,²⁹ fins a prohibicions més concretes, com la de tenir un ordinador connectat a la xarxa o, senzillament, la d'accedir a Internet.³⁰

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

26. *Vid.* un il·lustratiu recorregut per les decisions dels circuits federals a Wiest, *supra* nota 22, p. 850-861. També és d'utilitat McKay, *supra* nota 9, p. 221-234 i Harrold, *supra* nota 1 p. 345-355.

27. Pot consultar-se un recull legislatiu de diferents estats nord-americans a Harrold, *supra* nota 1, p. 359 i s.

28. *Vid.* models a Bowker, Arthur / Michael Gray, «An Introduction to the Supervision of the Cybersex Offender», *Federal Probation* 68-3, 2004, p. 5-7; també és d'utilitat Painter, Christopher M. E., «Supervised Release and Probation Restrictions in Hacker Cases», *USA Bulletin*, March 2001 (disponible a <http://www.usdoj.gov/criminal/cybercrime/usamarch2001_7.htm>).

29. *Vid.* *United States v. Fields*, 324 F.3d 1025 (8th Cir. 2003), ressenyat a Wiest, *supra* nota 21, p. 859 i s., i *United States vs. Paul*, 274 F.3d 155 (5th Cir. 2001), ressenyat a Harrold, *supra* nota 1, p. 352; un resum de les mesures imposades en d'altres casos a Harrold, p. 346, n. 253.

30. *United States. vs. Peterson* 248 F.3d 79 (2nd Cir. 2001): al convicte per un delictes d'estafa se li havia prohibit la possessió d'ordinadors amb accés a Internet, però se li va autoritzar la utilització de l'ordinador del seu negoci equipat exclusivament amb el software útil per a l'exercici de la seva activitat professional.

Un exemple extrem és el de Kevin Mitnick,³¹ un famós *hacker*, que fou condemnat a una pena de presó no inferior als cinc anys. Una vegada complerta aquesta pena, va haver de passar un període de tres anys de *parole* sota condicions estrictes: prohibició absoluta de posseir o usar qualsevol mena d'ordinador o d'altres equipaments informàtics, telèfons mòbils o qualsevol altra mena d'aparells que permetessin la connexió a ordinadors, a sistemes informàtics o a xarxes de comunicacions. Així mateix, li fou prohibida qualsevol activitat professional o privada relacionada amb els ordinadors o mantenir contactes amb persones o grups relacionats amb aquestes activitats.

Tanmateix, molts jutges han anat acceptant que les prohibicions globals podien ser excessives i, fins i tot, contraproductes. A poc a poc algunes restriccions s'han anat modalitzant, per evitar la pràctica «mort informàtica» que comporten mesures (a vegades perpètuas) d'abast tan ampli i divers que impliquen la impossibilitat de realitzar activitats com ara usar el correu electrònic, efectuar una transferència bancària o treballar de xofer en vehicles equipats amb GPS. En conseqüència, s'observa una tendència a *permetre un accés sota control*, en el sentit de consentir usos determinats –laborals, educatius, etc.– o bé de prohibir només usos o activitats molt concretes (visitar llocs web pornogràfics o d'apostes, «baixar» material d'aquesta naturalesa, participar en xats, entrar en comunicació en línia amb menors de certa edat, etc.). Aquest enfocament presenta l'avantatge de permetre un ús selectiu de les TIC, de manera que no s'afecti la possible ressociabilització del subjecte, i ha estat impulsat per alguns tribunals federals.³²

En qualsevol cas, es presenta també el problema de les *mesures per controlar* el compliment de les restriccions. En efecte, com a condició per a la concessió de la *probation* o la *parole* a ciberdelinqüents, els jutges i les agències de supervisió nord-americanes exigeixen, per exemple, que el subjecte accepti per endavant visites i registres sense avís previ, la còpia de tota la informació, la retirada de dispositius informàtics per a una inspecció més a fons o la instal·lació de programes –a costa de la persona controlada (!)– que permetin el monitoratge de l'ordinador o limitar i filtrar les activitats que s'hi poden realitzar.

31. Mitnick ha estat considerat pel Departament de Justícia dels EUA com el criminal informàtic més buscat de la història.; *vid.* la descripció del cas a Hyne, *supra* nota 24, pp. 243-245 i Smith, *supra* nota 17, p. 4.

32. *Vid.*, per exemple, *United States vs. Sofsky*, 287 F.3d 122 (2nd Cir. 2002); múltiples referències als treballs indicats *supra* nota 26.

A més, per assegurar l'efectivitat d'aquests sistemes de control, s'imposen condicions addicionals per fer disminuir el risc de maniobres evasives: obligació d'utilitzar només un ordinador determinat o un proveïdor de serveis d'Internet, prohibició o obligació d'utilitzar certs programes o sistemes operatius, proscripció de l'entrada a cibercafès, locutoris o biblioteques, etc.

6. Ara bé, per més que s'acordin aquestes mesures, és realment factible la seva posada en pràctica i la dels controls corresponents? I, si es pot fer, és efectiva? D'entrada podríem contemplar-ho amb un cert escepticisme, però cal tenir present que les agències de supervisió en aquest països, molt particularment als EUA, estan molt més desenvolupades que les nostres i disposen de la col·laboració molt estreta d'altres instàncies, especialment de la policia. Per tant, poden recórrer, per detectar eventuais vulneracions de les prohibicions i la limitació en l'ús de les TIC, als mètodes que ja utilitzen habitualment amb altres delictes: les entrevistes a tercers, les inspeccions no anunciades, l'ocupació de dispositius per ser examinats més a fons, el control dels moviments bancaris, l'ús del polígraf, etc.³³

No obstant això, cada vegada tenen un paper més important els programes informàtics de control de l'ús de l'ordinador, un programari que fou creat inicialment per a la investigació de delictes informàtics o per a la vigilància de l'ús dels ordinadors en l'àmbit laboral o familiar però que ha trobat aquí un nou camp d'aplicació.³⁴ Es comercialitzen amb noms tant suggeridors (o inquietants) com *Cyber Cop*, *Cyber Sentinel* o *Spector Pro* i, a hores d'ara, ja són un pròsper sector de negocis.³⁵ Bàsicament aquestes aplicacions són de tres menes. *Programes forenses*, que creen còpies (totals o selectives) dels arxius emmagatzemats als equipaments informàtics del subjecte controlat i examinen sistemàticament el seu contingut; *programes de monitoratge*, que permeten enregistrar ru-

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

34. Curphey, *supra* nota 1, p. 2263 i s. i Harrold, *supra* nota 1, p. 340 i s., amb referències abundoses. Cal tenir present que l'estàndard de prova d'una infracció tècnica és menys estricte que l'exigit per provar un delicte, de manera que els requeriments tècnics i procedimentals són també menors.

35. El National Law Enforcement and Corrections Technology Center, dependent del Departament de Justícia, ofereix gratuïtament el *Field Search*, un programa per a no experts idoni per inspeccionar els ordinadors dels infractors (disponible a <<http://www.justnet.org/fieldsearch/>>).

tinàriament l'activitat de l'ordinador (programes utilitzats, tecles premudes, moviments de correu electrònic, navegació per Internet, etc.) i, fins i tot, fer un seguiment en línia de l'ús de l'ordinador; i *programes de filtratge o de bloqueig*, que impedeixen l'accés a llocs o serveis no autoritzats. Les possibilitats de control remot de l'ús de les TIC mitjançant aquests programes evolucionen constantment, tot i que exigeixen un seguiment molt estricte i cada vegada més preparació del personal i auxili d'experts externs.

Darrerament s'estan desenvolupant altres sistemes de control que no estan ubicats als equipaments de l'infractor. Així, s'està treballant en tecnologies que permetin la detecció i el bloqueig de l'accés a determinats llocs i xarxes als convicts mitjançant la connexió de les bases de dades dels usuaris d'aquestes xarxes amb els registres de delinqüents sexuals.³⁶

Òbviament, la posada en pràctica de totes aquestes mesures de vigilància implica nombroses dificultats tècniques i organitzatives, especialment si tenim en compte la traça de moltes de les persones sotmeses a supervisió, sovint superior a la dels seus controladors. Però, sobretot, obliga a sotmetre el subjecte a un grau de vigilància sense parió,³⁷ que, a més, pot afectar altres persones que conviuen amb l'infractor o que utilitzin els equipaments sotmesos a supervisió. De fet, les restriccions en l'accés a les TIC poden tenir un contingut aflictiu més intens que les condicions tradicionals.

Pel que fa a l'efectivitat del sistema, no tinc coneixement de l'existència d'estudis empírics que tractin aquest tema.³⁸ Semblen, però, mesures més adequades a un món de PC de sobretaula i un accés a les xarxes a través de línies te-

36. Xarxes com *My Space*, de gran popularitat entre els adolescents (*vid. infra* nota 38) ho estan desenvolupant: cfr., sobre aquest tema, el comentari de Hines, Nichol, «Blocking Former Sex Offenders from Online Social Networks: Is this a Violation of Free Speech?» (disponible a <<http://www2.law.duke.edu/journals/dltr/iblawg/>>).

37. De fet, el grau d'ingerència en la vida de les persones sotmeses a control penal fora de la presó està arribant en el món anglosaxó a extrems inimaginables en altres latituds. S'ha arribat al punt de condicionar la concessió de la *probation* o la *parole* a no tenir fills durant el període de control i, fins i tot, per garantir el compliment d'aquesta condició, s'ha imposat l'obligació de prendre anticonceptius (les famoses *Norplant probation conditions*, en referència a la marca dels implants que se solen utilitzar); vegeu nombroses referències sobre aquestes mesures, aplicades sobretot a dones drogodependents i maltractadores a Harrold, *supra* nota 1, p. 289, n. 34.

38. No obstant això, s'observen indicis que, com a mínim, es descobreixen algunes infraccions amb els escorcolls: *vid.*, per exemple, *Addleman vs. King County*, 2007 U.S. Dist. LEXIS 35117 (W.D. Wash. May 14, 2007). Recentment, els administradors de la xarxa social *My Space* han

lefòniques fixes que comença a estar superat. La facilitat creixent d'accedir per múltiples vies a les xarxes d'informació i per emmagatzemar externament informació planteja, per tant, seriosos interrogants a la viabilitat d'aquestes mesures.³⁹ En qualsevol cas, si l'objectiu no és assegurar una vigilància constant sinó un control esporàdic que permeti la revocació de la *probation* o la *parole*, el sistema sembla que és practicable.⁴⁰

El model d'infracció controlable seria el següent: un individu que canvia de vorera quan veu un policia, és aturat i se l'identifica. En contrastar-se la seva identitat al cotxe patrulla apareix que està sotmès a *probation* i les condicions que li han estat imposades. S'efectua un escorcoll corporal i del vehicle i es desobreix un telèfon mòbil i un lllapis de memòria.⁴¹

7. L'altra qüestió cabdal que es planteja és la de la *legitimitat*. En efecte, a desgrat de la seva progressiva implantació, des d'un principi ha existit als EUA una forta controvèrsia jurisprudencial sobre l'admissibilitat d'aquestes mesures. Sense sentències del Tribunal Suprem sobre la qüestió i amb discrepàncies notables entre els diversos circuits federals, tanmateix es pot identificar una certa tendència a considerar que les prohibicions absolutes d'ús i accés a les TIC comporten sovint una limitació de la llibertat desproporcionada i amb efectes contraproduents per a la rehabilitació, especialment si, a més, existeix la possibilitat d'adoptar mesures menys radicals però igualment efectives per protegir la col·lectivitat.

tramès a les autoritats de diversos estats els noms, adreces i perfils dels seus usuaris, i centenars de persones sotmeses a *probation* i *parole* amb la prohibició d'accedir a Internet o d'entrar en contacte amb menors han estat descoberts a tots els EUA (vid. «Parolees on MySpace may land in jail», *USA Today*, 5 de juny de 2007, disponible a <http://www.usatoday.com/tech/news/2007-06-05-myspace-parolees_N.htm>).

39. Així, entre les recomanacions en l'àmbit de la supervisió comunitària efectuades pel Grup de Treball sobre Tecnologies presentat a la trobada del *National Law Enforcement and Corrections Technology Center* de 2006 destaca la necessitat de crear noves eines per controlar l'ús i el contingut de telèfons mòbils, PDA i altres mitjans (presentació disponible a <http://www.nlectc.org/nlectcrm/rac_jul2006.html>).

40. Vid. *infra* V.1.

41. Exemple inspirat en la important sentència *Samson vs. California*, 547 U.S. ____ (2006), disponible a <http://www.oyez.org/cases/2000-2009/2005/2005_04_9728/>, un cas d'escorcoll corporal sense cap motiu específic i en què es descobreix una possessió de drogues. El Tribunal Suprem, per majoria, ha considerat que qui accedeix anticipadament a la llibertat, continua sota custòdia legal de l'Administració de justícia penal i, per tant, té severament limitat el seu dret a la privadesa.

Així, alguns tribunals han rebutjat condicions consistents en la prohibició genèrica d'ús de les TIC.⁴² Entenen que no són admissibles perquè els seus efectes són anàlegs als que haguessin tingut, fa uns anys, les prohibicions de fer ús del telèfon, del correu o de la televisió i que poden comportar, per exemple, la pràctica impossibilitat de trobar una feina, d'accedir a l'educació no presencial, d'exercir electrònicament el dret de vot, de consultar un diari o, senzillament, de comprar un llibre a *Amazon*. Per tant, provoquen una limitació molt dràstica de la llibertat dels subjectes implicats que els impedeix menar una vida quotidiana amb normalitat i es converteixen en un obstacle per a la seva rehabilitació. Altrament, algun tribunal tampoc ha considerat suficient compensar les prohibicions genèriques amb l'habilitació dels supervisors per autoritzar alguns usos concrets: «l'oficial de *probation* esdevé un censor que determina que [el condemnat] pugui llegir el *New York Times* en línia i no, en canvi, la versió d'*Ulysses* a *bibliomania.com*».⁴³

En qualsevol cas, malgrat l'eventual adopció de restriccions més limitades, se segueixen presentant problemes en relació amb les mesures de vigilància i control que les acompanyen, especialment pel que fa a l'obligació d'acceptar escorcolls domiciliaris, sense necessitat d'indicis d'actuació indeguda, o el monitoratge intensiu de l'ordinador i altres equipaments, que provoca una limitació extrema de la privadesa del subjecte controlat i dels tercers que conviuen o treballen amb l'infractor. Amb tot, fins i tot les línies jurisprudencials més liberals no han rebutjat completament aquestes condicions. Els tribunals es limiten a exigir que els jutges determinin molt clarament les restriccions i les mesures de control i que, com «un vestit a mida» (*narrowly tailored sanction*), s'adaptin a la gravetat dels fets comesos i a les peculiaritats del subjecte controlat.⁴⁴

En definitiva, es consideren legítimes les mesures restrictives i les corresponents formes de control i vigilància, si bé cal que s'adoptin les menys intrusives segons la tecnologia disponible en cada moment. D'aquesta manera es pretén

42. *Vid. supra* nota 32. Recentment *United States vs. Voelker*, No. 05-2858 (3d Cir. June 5, 2007), disponible a <<http://circuit3.blogspot.com/2007/06/in-united-states-v.html>>: «Prohibir de per vida l'accés a qualsevol equipament informàtic i a Internet és funcionalment equivalent a prohibir a un convicte de posseir revistes de pornografia infantil la possessió de llibres i revistes de qualsevol mena la resta de la seva vida». Tanmateix, una part dels circuits federals continuen defensant posicions més restrictives (*vid. referències a Wiest, supra* nota 21, p. 860 i s.).

43. *United States vs. Scott*, 316 F.3d 733 (7th Cir. 2003), referència a Wiest, *supra* nota 21, p. 856-58.

44. *Vid.*, per a tots, *United States vs. Lifshitz*, *supra* nota 1, i *United States vs. Voelker*, *supra* nota 42.

que les finalitats asseguratives i incapacitadores de les mesures siguin compatibles amb el desenvolupament d'una vida en llibertat mínimament normal i el manteniment d'una certa expectativa de privadesa.⁴⁵ Tanmateix, malgrat que la doctrina de les restriccions «fetes a mida» ha estat un avanç, cal no desconeixer que continuen tenint efectes molt severos sobre la vida de l'infractor.

IV. La prohibició d'ús de les TIC al sistema penal espanyol

1. Existeix una pena de prohibició o restricció d'ús de les TIC?

1. Ara com ara, l'impacte de les TIC no ha comportat cap modificació en el sistema de penes espanyol i no han aparegut sancions que privin del gaudi d'aquests nous drets.⁴⁶

Certament, en el catàleg de penes previstes a la legislació penal espanyola, no existeix cap sanció similar. L'única –i remota– possibilitat la trobaríem en el catàleg de penes privatives de drets del CP, en què es fa esment a l'article 39.b a «la inhabilitació especial per a [...] professió, ofici, indústria o comerç o altres activitats determinades en aquest Codi [...] o de *qualsevol altre dret*». Aquesta pena d'inhabilitació té com a efecte la privació de la facultat d'exercir l'activitat o el dret que es vegin afectats durant el temps de la condemna. Aparentment, dins d'aquesta previsió s'hi podria incloure la prohibició de realitzar activitats professionals i laborals vinculades amb les TIC així com, de manera més genèrica, la limitació del dret a emprar-les. Nogensmenys, aquestes possibles inhabilitacions s'haurien d'especificar en les penalitats establertes als preceptes de la Part Especial del CP, però en cap s'estableix específicament una pena principal relacionada amb les TIC. De fet, si pensem atenció a les figures delictives més properes a la cibercriminalitat, observem que les penes previstes són les tradicionals penes de presó i multa.⁴⁷

45. Curphey, *supra* nota 1, p. 2272.

46. Assenyala precisament la necessitat d'incorporar inhabilitacions, suspensions o limitacions de l'accés a sistemes informàtics i, sobretot, a xarxes de comunicació, 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 a <<http://www.uhu.es/derechoyconocimiento/contenido.htm>>).

47. Cfr., simplement, els casos de la pornografia amb menors (art. 189 CP), l'estafa informàtica (art. 248.2 CP) o els danys informàtics (art. 264.2 CP).

2. Tanmateix podem trobar una escletxa quan aquestes inhabilitacions actuen en qualitat de *penes accessòries*, això és, aquelles que el Codi permet imposar, malgrat no estar previstes expressament en la penalitat d'un delictes concret, com un afegit a la pena principal, normalment amb la mateixa durada. En efecte, l'article 56.1.3r CP estableix que la inhabilitació especial per a professió, ofici, indústria o comerç o qualsevol altre dret que s'ha esmentat anteriorment pot ser una pena accessòria a les penes de presó de menys de deu anys, sempre que l'exercici de l'activitat o el dret objecte de la inhabilitació hagi tingut relació directa amb el delictes comès i així ho estableixi el jutge a la sentència. D'aquesta manera la previsió d'una pena de presó habilita al jutge per acordar una inhabilitació ajustada a les peculiaritats del cas.

Així, en un cas recent de descobriment i revelació de secrets per intrusisme informàtic, un *hacker* ha estat condemnat a un any de presó (en apreciar-se com a atenuant la seva addicció als videojocs) i, com a pena accessòria, a la *inhabilitació per a l'exercici de la professió d'administrador de sistemes i programador informàtic* durant el temps de la condemna.⁴⁸ Per tant, si s'acorda la suspensió de la pena de presó o bé si el condemnat té l'oportunitat de treballar durant l'execució de la pena (com a treball penitenciari o per estar en règim obert o en llibertat condicional), el subjecte no pot dedicar-se a les ocupacions referides.

Més complexa és l'aplicació, com a accessòria, de la inhabilitació especial «per a qualsevol altre dret», que, per a allò que a nosaltres ens interessa, podria obrir la porta a restriccions de diversa mena, com la del dret d'utilitzar ordinadors o telèfons mòbils, a navegar per Internet o a emprar el correu electrònic. El motiu és que la manca de determinació d'aquesta clàusula genera friccions amb les garanties constitucionals a la legalitat i la proporcionalitat, la qual cosa ha provocat que majoritàriament sigui interpretada de manera restrictiva.

Segons això, només seria admissible imposar, com a pena accessòria a una pena de presó, una privació de drets que ja estigui expressament descrita com a principal en algun altre delictes: així és admissible com a accessòria la inhabilitació del dret a caçar o pescar o la pèrdua de la possibilitat d'obtenir subvencions o ajuts públics, per estar previstes com a principals en els articles 302 i 334 CP, mentre que

48. Sentència del Jutjat Penal núm. 2 de Badajoz, de 21 de febrer de 2006 (*Diario La Ley*, núm. 6445, 21 de març de 2006, p. 1 i s.).

no seria possible privar del dret a utilitzar targetes de crèdit o de participar en xats, per no ser «penes legals».⁴⁹

Malgrat tot, pot entendre's que la menció a «qualsevol altre dret» de l'article 56 CP obre la porta a una sèrie d'inhabilitacions accessòries força àmplia i, per consegüent, seria possible introduir per aquesta via restriccions en l'ús de les TIC sempre que guardin alguna relació amb el sistema de penes genèric.⁵⁰

3. En qualsevol cas, en la pràctica, els tribunals rarament fan ús de la facultat d'inhabilitar per a activitats professionals vinculades a les noves tecnologies, malgrat que no existeixin impediments legals. I, pel que fa a la més polèmica «inhabilitació d'altres drets», no he detectat cap cas en què s'hagi aplicat en aquest àmbit.

En efecte, a banda d'alguna excepció encomiable com la del programador informàtic esmentat anteriorment, crida l'atenció que l'accessòria que sistemàticament s'imposa als ciberdelinqüents sigui la inhabilitació especial per al dret de sufragi passiu.⁵¹

D'altra banda, mancats com estem d'una llei d'execució penal que reguli adequadament la implantació pràctica de les penes privatives de drets, l'execució d'aquestes inhabilitacions es limita a un requeriment al condemnat per tal que s'abstingui d'exercir l'activitat o el dret, sense cap mena de control o seguiment. La seva efectivitat és, per tant, quasi nul·la. Més enllà del compliment voluntari, l'únic efecte que podrien tenir les inhabilitacions professionals en el camp de les TIC seria que, amb ocasió de la comissió d'un nou delictes, es detectés que s'estava realitzant una activitat sobre la qual pesava una inhabilitació i que, per tant, es castigüés pel corresponent delictes de trencament de condemna.

49. *Vid.* el resum de la problemàtica, crític amb la postura restrictiva, de Boldova Pasamar a Gracia Martín, Luis (coord.), *Tratado de las Consecuencias Jurídicas del Delito*, València, Tirant lo Blanch, 2006, p. 137-140, amb moltes referències.

50. Relació que existeix, per exemple, amb les prohibicions de comunicació o amb les inhabilitacions per a activitats per a les quals no cal llicència prèvia establertes expressament al CP.

51. Per comprovar-ho, n'hi ha prou amb consultar en els reculls jurisprudencials les escadusseres condemnes per estafes o danys informàtics (art. 248.3 i 264.2 CP) o per descobriment i revelació de dades de caràcter personal (art. 197.2 CP). És probable, però, que en sigui responsable en bona part una certa deixadesa de les acusacions.

4. Finalment, existeixen altres penes o conseqüències penals que poden incidir en l'ús de les TIC, però de manera tangencial. Aquest és el cas de:

- La prohibició d'entrar en comunicació per qualsevol mitjà amb la víctima, els seus familiars o altres persones, pena utilitzada principalment en els delictes de violència de gènere, domèstica o familiar i que inclou qualsevol mitjà informàtic o telemàtic (art. 48.2 CP).⁵²
- El comís, que permet la confiscació d'ordinadors i tota mena d'equipaments que s'hagin utilitzat com a mitjà o instrument per a la comissió d'un delicte (art. 127 CP).
- La prohibició a una persona jurídica de realitzar activitats en l'exercici de les quals s'hagi comès, afavorit o encobert un delicte (art. 129.1.c CP).⁵³

5. En definitiva, les prohibicions d'ús de les TIC com a pena es mouen en un marc legal discutible i tenen una aplicació pràctica insignificant.

2. Es pot restringir l'ús de les TIC amb motiu de l'aplicació de mesures penals alternatives?

1. Tal com hem vist en l'apartat III d'aquest treball, la prohibició o les restriccions en l'ús de les TIC i la seva vigilància pot trobar un espai d'aplicació en el marc de la suspensió de l'execució de la pena de presó i en la llibertat condicional, que, a grans trets, es pot equiparar respectivament a la *probation* i la *parole* del món anglosaxó.

2. En termes generals, quan una persona ha estat condemnada a una pena privativa de llibertat inferior a dos anys i no té antecedents penals,⁵⁴ l'execució

52. No gens inusual en cas de violència de gènere, domèstica o familiar: *vid.*, per exemple, SAP Cantàbria (Sec. 3a.) de 22 de desembre de 2006, on expressament es condemna un estudiant, que havia enviat frases amenaçadores a la seva xicota a través del *Messenger*, a «una prohibició de comunicar-se amb ella per qualsevol mitjà —incloent-hi Internet—» durant sis mesos (*Diario La Ley*, núm. 6674, 19 de març de 2007, p. 1 i s.).

53. Com seria, per exemple, el cas d'un delicte publicitari a través d'Internet o d'una estafa telefònica mitjançant una línia 900, de manera que es restringís l'ús d'aquests mitjans per part de l'empresa. Cal reconèixer, però, que la posada en pràctica de les conseqüències accessòries aplicables a les persones jurídiques de l'article 129 CP ha estat molt minsa.

54. En el cas dels drogodependents, les penes poden arribar fins a cinc anys i és possible aplicar-ho a persones amb antecedents.

de la pena pot ser suspesa durant un període mai superior als cinc anys, transcorregut el qual queda extingida la responsabilitat penal. Aquesta suspensió resta condicionada, en tot cas, al fet que el reu no torni a delinquir durant el període de suspensió i al compliment d'una sèrie d'obligacions i deures que el jutge sentenciador pot imposar si ho considera necessari. El catàleg d'obligacions, denominades també *regles de conducta*, es concreta a l'article 83 CP, on es preveuen mesures de naturalesa tant assegurativa (per exemple, prohibició d'apropar-se a la víctima) com rehabilitadora (per exemple, participació en programes formatius, laborals, culturals, d'educació vial, sexual i altres de similars). Si no es compleixen aquestes regles, el jutge pot modificar-les, prorrogar el període de suspensió o, fins i tot, revocar la suspensió i procedir a l'execució de la pena de presó. En la pràctica, els jutges solen concedir quasi sempre la suspensió a qui reuneix els requisits per accedir-hi.⁵⁵

D'altra banda, una vegada complertes les tres quartes parts de la pena de presó, els penats que reuneixen una sèrie de requisits –el més important de tots, estar en el tercer grau de tractament penitenciari– poden ser alliberats sota condicions, de manera que compliran el darrer tram de la pena en règim de llibertat. La condició necessària per assolir finalment l'extinció de la pena és no tornar a delinquir durant aquest període. Però, a més, el jutge de vigilància penitenciària pot imposar addicionalment alguna de les regles de conducta de la suspensió de la pena previstes a l'article 83 CP. La manca de respecte a aquestes regles comporta la revocació de la llibertat provisional i el reingrés a la presó. A Catalunya, un 24% dels penats aconseguen extingir la pena en llibertat condicional.⁵⁶

55. Cfr. Cid Moliné, José / Elena Larrauri Pijoan (coords.), *Jueces penales y penas en España. (Aplicación de las penas alternativas a la privación de libertad en los juzgados de lo penal)*, València, Tirant lo Blanch, 2002, p. 104-106, amb algunes matisacions pel que fa a persones sense antecedents penals vigents però amb un cert historial delictiu. Confirma aquesta conclusió les dades de Cid Moliné, José, «La suspensión de la pena en España: descarceración y reincidencia», *Revista de Derecho Penal y Criminología*, núm. 15, 2005, p. 230. Actualment a Catalunya hi ha 3.326 persones sotmeses a mesures penals alternatives (concepte que engloba altres mesures a banda de les «regles de conducta») segons el *Butlletí de dades setmanals de la Secretaria de Serveis Penitenciaris, Rehabilitació i Justícia Juvenil*, 30 de maig 2007 [no publicat]. No es disposa, però, de dades sobre el nombre de suspensions revocades, element que en permetria avaluar el grau de control real, si bé, segons les decisions judicials disponibles, sembla que la revocació no és gens usual.

56. A l'any 2004, segons les dades de Tébar Vilches, Beatriz, «La aplicación de la libertad condicional en España», *Revista de Derecho Penal y Criminología*, núm. 18, 2006, p. 288. Actualment hi ha 9.334 reclusos i 749 alliberats condicionals (*Butlletí de dades setmanals, supra* nota 55). No es disposa de dades sobre el nombre de les revocacions, però la impressió, a la vista de la jurisprudència disponible, és que no són tan excepcionals com en la suspensió de la pena.

3. Així doncs, la possible restricció de l'ús de les TIC que pugui fer una persona en llibertat condicional o amb una pena suspesa s'hauria de plasmar a través de la imposició d'alguna obligació basada en l'article 83 CP. D'entrada, cap d'aquestes expressament sembla aplicable a les TIC.⁵⁷ Ara bé, pel que aquí interessa, cal destacar que el catàleg finalitza amb una clàusula oberta (art. 83.1.6è): aquells deures que el jutge estimi convenients per a la rehabilitació social del penat, amb la conformitat prèvia d'aquest, sempre que no atemptin contra la seva dignitat com a persona. Queda clar que no es tracta de mesures exclusivament asseguratives, però les necessitats dels programes formatius de rehabilitació que també es preveuen com una possible condició de la suspensió o de la llibertat condicional poden requerir l'acompanyament de mesures per controlar el subjecte mentre no s'adquireixen els hàbits o les capacitats que es persegueixen:

Així, per exemple, a la STS 913/2006, de 20 de setembre (ponent Martín Pallín), s'imposa una pena d'un any i sis mesos de presó per un delictes de possessió de pornografia infantil (art. 189.2 CP), que ha estat obtinguda en «comunitats de Microsoft» i en *xats*, i es condiciona la suspensió al seguiment de programes formatius d'educació sexual (art. 83.1.5è). Aquest és un cas en què el jutge podria haver acordat la imposició de mesures de limitació de l'ús de les TIC basades en l'art. 83.1.6è.

Un primer problema seria si aquesta previsió genèrica pot donar cobertura, sense vulneració del principi de legalitat, a mesures restrictives d'ús de les TIC i, sobretot, a les mesures de vigilància que les acompanyen. En qualsevol cas, haurien de quedar clarament fixades a la decisió judicial i no seria admissible que es determinessin en seu administrativa.⁵⁸ Tanmateix, el principal obstacle no està en la regulació legal, sinó que en la pràctica s'imposen poques vegades condicions de l'article 83, almenys en la seva modalitat 6a. I, a més, no

57. De manera indirecta, la prohibició d'acudir a determinats llocs (art. 83.1.1r. CP) també podria tenir alguna virtualitat: per exemple, la prohibició d'entrada a cibercafès, a locutoris o a altres locals on es faciliti l'accés a xarxes d'informació.

58. És a dir que, a l'empara d'una menció genèrica a la sentència, es deixés per als programes i plans d'intervenció, control o seguiment elaborats pels serveis socials penitenciaris la concreció de les regles de conducta i les condicions de control més severes de la suspensió o la llibertat condicional (cfr, respectivament, art. 17 a 20 RD 515/2005, de 6 de maig, i art. 195 i s. Reglament penitenciar). De fet, en el cas de la llibertat condicional, s'ha arribat a qüestionar que aquests serveis puguin realitzar tasques d'investigació i control (*vid.* Vega Alocén, Manuel, *La libertad condicional en Derecho español*, Madrid, Civitas, 2001, p. 321-322).

existeixen prou recursos institucionals, materials i humans per donar un autèntic contingut a aquestes mesures.⁵⁹ Certament, en els darrers temps s'observa una millora en aquest àmbit, especialment a l'Administració catalana, però els esforços en les mesures penals alternatives estan centrats en sectors molt determinats, concretament la deshabitació de drogodependents i les mesures que, imperativament, s'han d'aplicar als autors de violència de gènere, domèstica i familiar.

V. Balanç

1. Per entendre bé la naturalesa i l'autèntic objectiu de les mesures de prohibició i restricció d'ús de les TIC als EUA, cal situar-la en el context de la pràctica penal dominant avui dia. En el seu origen, *probation* i *parole* es van idear com a alternatives a la presó d'inspiració rehabilitadora, però, a partir dels anys vuitanta, la situació va canviar radicalment.⁶⁰ Actualment són més aviat concebudes com a sancions complementàries a la presó⁶¹ i s'orienten de manera prioritària vers la protecció de la comunitat i la incapacitació de l'infractor. Així, s'ha passat a un model de gestió de riscos (el risc que el condemnat torni a delinquir), en què prima la vigilància i la inoqüització.⁶²

Les agències que operen en aquest camp s'han vist desbordades per les demandes socials de seguretat i han abandonat el model ressocialitzador, aparent-

59. Cfr. el diagnòstic de Díez Ripollés, José Luis, «La evolución del sistema de penas en España: 1975-2003», *Revista Electrónica de Ciencia Penal y Criminología*, núm. 8, 2006, p. 22 i s. (disponible a <<http://criminet.ugr.es/recpc/08/recpc08-07.pdf>>). En efecte, existeix un cert acord en que la manca d'organització i de mitjans només permet un «control passiu, administratiu i burocràtic» (Vega Alocén, *supra* nota 58, p. 359-360; *vid.*, també, Tébar Vilches, Beatriz, *El Modelo de libertad condicional*, Cizur Menor, Thomson Aranzadi, 2006, p. 245).

60. La més impressionant descripció i l'anàlisi més lúcida d'aquests canvis és l'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 sentit que cada vegada més les legislacions presenten les formes de llibertat vigilada com una sanció addicional a la pena de presó i no com una alternativa o un substitutiu d'aquesta.

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 i s., amb múltiples referències, entenent que aquest fet és una manifestació de l'«administrativització» del dret penal dins del fenomen més global de la seva expansió.

ment car, lent i de resultats incerts. Opten per «manejar el risc» a través de la detecció, mitjançant formes barates de vigilància, de nous delictes o, sobretot, de simples infraccions tècniques, de manera que la tasca essencial dels funcionaris és la de retornar a la presó les sotmesos a *parole* i *probation*.⁶³ En efecte, en sotmetre a vigilància intensiva persones que estan en situació de risc de tornar a delinquir, s'acaben detectant infraccions, sovint inevitables però que, mal gestionades, impliquen la interrupció del procés rehabilitador i el reingrés a la presó. La conclusió és clara: institucions que, en teoria, són alternatives a la presó, amb l'objectiu de disminuir la reincidència es converteixen en generadores de més reincidència.⁶⁴

Aquesta tendència ha assolit cotes orwellianes en la guerra total iniciada contra la delinqüència sexual (en sentit molt ampli), catalitzat per l'especial problemàtica dels «depredadors sexuals» (agressors sexuals molt violents i tal vegada incorregibles).⁶⁵ No oblidem que les restriccions a les TIC s'han aplicat bàsicament a delinqüents sexuals.

Vist tot això, queda clar que l'objectiu de la imposició de prohibicions d'ús de les TIC als EUA no és donar suport a la rehabilitació, ni tant sols incapacitar completament i constantment el subjecte, sinó limitar simplement les oportunitats delictives i, sobretot, introduir una infracció tècnica susceptible de ser detectada a mitjà termini i que justifiqui la revocació de la mesura i el retorn a la presó.

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. Les dades són significatives: segons les estadístiques oficials (*supra* nota 21), només el 59% dels sotmesos a *probation* la finalitzen amb èxit mentre que, en el cas de la *parole*, només ho fa el 45%. La meitat dels reingressos a presó ho són per infraccions purament tècniques; el paroxisme s'assoleix a Califòrnia, on les tres quartes parts de les persones en règim de *parole* tornen a la presó per aquest motiu (Jakobson, p. 39-40 i 144 i s.).

65. *Doe vs. City of Lafayette*, 377 F.3d 757 (7th Cir. 2004) és il·lustratiu de a quin extrem s'ha arribat: un pederasta sotmès a *probation* reconeix, en una sessió de la seva teràpia de grup, haver-se aturat en un parc i haver estat fantasiant mentre mirava els nens que jugaven. Objecte d'una denúncia anònima, les autoritats locals li prohibeixen l'accés, entre d'altres llocs, als parcs públics del municipi i els tribunals confirmen que és legítim sancionar el fet de fantasiar si s'hi involucraven nens reals. Un resum d'aquest cas i del conjunt de mesures «creatives» (com la rebaixa dels estàndards de la prova, la castració química i els registres públics de delinqüents sexuals) pot veure's a l'inquietant treball de Siverts, Jennifer B., «Punishing Thoughts too Close to Reality: a New Solution to Protect Children from Pedophiles», *Thomas Jefferson Law Review* 27, 2004-2005, p. 393-419.

2. Per contra, la situació al nostre país és l'oposada. Com s'ha vist, el nostre marc legal continua orientat vers un model rehabilitador, en el qual les mesures de control compleixen sobretot una funció auxiliar del tractament i quasi no estan regulades, de manera que seria molt qüestionable un sistema de control del compliment de les condicions tan agressiu com el nord-americà. D'altra banda, malgrat algunes millores els darrers anys, en la pràctica el nostre aparell d'execució penal en l'entorn comunitari és molt feble, amb prou feines pot fer front a les necessitats més urgents i no està en condicions de portar a terme un control intensiu del compliment.⁶⁶ En definitiva, no sé si volem però està clar que no podem portar a la pràctica les prohibicions d'accés a les TIC amb l'abast, la intensitat i el control del «model nord-americà».

Fent de la necessitat virtut, podríem dir que, atès que el model de control penal anglosaxó sembla rebutjable, la impossibilitat d'implantar mesures en el camp de les TIC no és un problema. Però aquesta impossibilitat és també el símptoma de les nostres mancances regulatòries i organitzatives globals per donar un enfocament rehabilitador al sistema penal. Em temo que, finalment, no gestionem ni el risc ni la rehabilitació.

3. Tanmateix, per poc que millori la situació descrita, les restriccions d'ús de les TIC hi poden tenir un –modest– paper.

En tant que pena, ja ha quedat clara la possibilitat d'aplicar inhabilitacions professionals accessòries en el camp de les TIC, la qual es podria aprofitar més, especialment en la cibercriminalitat patrimonial. De fet, les dificultats d'execució i control no serien gaire diferents de les que existeixen amb les inhabilitacions per a professions i activitats no reglades.

Pel que fa a la suspensió i la llibertat condicional, crec que les restriccions (que no les prohibicions absolutes) tenen raó de ser. En efecte, des d'una perspectiva rehabilitadora, s'haurien d'aprofitar els períodes de llibertat supervisada per a l'adquisició d'hàbits d'ús responsable de les TIC.⁶⁷ I s'ha demostrat empíricament que els tractaments «no funcionen» si no van acompanyats d'un

66. Les revocacions de les suspensions de la pena o de la llibertat condicional són escadusseres i sempre vinculades a la comissió de nous delictes.

67. En el mateix sentit, Wiest, *supra* nota 21, p. 847, n. 2.

seguiment i d'una vigilància apreciable.⁶⁸ L'alternativa al model de gestions de riscos no és, doncs, el de la rehabilitació sense control. Segurament el problema no està en el grau de control sinó en la finalitat d'aquest control, així com en les conseqüències dels possibles incompliments. En un model rehabilitador, els dits incompliments s'han de considerar en el si d'un procés de tractament en què la recaiguda és previsible i l'avanç no és lineal, de manera que té sentit evitar sancions automatitzades per infraccions tècniques. Partint d'aquestes premisses, les mesures restrictives i de vigilància de l'ús de les TIC en el marc de les regles de conducta de la suspensió i de la llibertat condicional no només em sembla que poden tenir cabuda legal, sinó que, en certs casos, poden ser recomanables.⁶⁹

Certament, la severitat de les mesures i la necessitat de vigilància són de tal magnitud que, només poden justificar-se en subjectes amb un risc de reincidència molt elevat en la comissió de delictes molt greus (bàsicament, en certs delinqüents sexuals i alguns ciberdelinqüents perillosos) i són desproporcionades en perfils delictius més comuns. Així mateix, caldria donar major cobertura normativa a les eventuais mesures de control de les regles de conducta. D'altra banda, des d'una perspectiva pràctica, les dificultats d'execució són tals que no sembla que tingui sentit preconitzar la seva aplicació general i només paga la pena recórrer a aquestes mesures quan la utilització de les TIC constitueixi la via principal per manifestar la seva perillositat criminal.

En qualsevol cas, el futur d'aquestes possibles penes i mesures està condicionat pel fet que el legislador i el sistema de justícia criminal desenvolupin, legalment i institucionalment, de forma plena un sistema d'execució penal que no estigui basat essencialment en la presó.

68. *Vid.*, en el famós informe encomanat pel Congrés dels EUA, MacKenzie, Doris, «Criminal Justice and Crime Prevention», a Sherman, Lawrence W. i altres, *Preventing Crime: What Works, What Doesn't, What Promising*, National Institute of Justice, 1998, p. 9-26 i s., 9-56 i 9-61 (disponible a <<http://www.ncjrs.gov/works/>>). De la mateixa autora, actualitzant-ne el plantejament, *What works in corrections: reducing the criminal activities of offenders and delinquents*, New York, Cambridge University Press, 2006.

69. Qüestió diferent és si no seria recomanable separar, fins on sigui possible, les tasques de tractament i rehabilitació i les de vigilància i control.

RESUM

Revista catalana de dret públic, 35, ISSN 1885-5709, 2007

Font de la classificació: Classificació Decimal Universal (CDU)

Font dels descriptors: paraules clau facilitades pels autors

004.7

David Felip i Saborit, professor titular de dret penal del Departament de Dret de la Universitat Pompeu Fabra

ca Demandar la lluna en un cove? Sobre la possibilitat de prohibir penalment l'ús de les tecnologies de la informació i la comunicació

p. 307-336

Aquest treball tracta sobre la possibilitat de prohibir o restringir penalment als ciberdelinqüents l'ús d'ordinadors, l'accés a Internet o a d'altres TIC. Amb aquest objectiu, s'analitza l'experiència als EUA, on des de fa més d'una dècada es limita i controla l'ús d'aquestes tecnologies a persones sotmeses a

probation i *parole*. La conclusió és que, si bé aquestes mesures podrien ser acceptables i, fins i tot, aconsellables en certs casos molt concrets com a suport de la rehabilitació, la regulació legal i l'estructura d'execució penal del nostre país són insuficients per implantar-les fora dels establiments penitenciaris.

Paraules clau: ciberdelictes; delictes sexuals; presó; *probation*; control penal; societat de la vigilància.

RESUMEN

Revista catalana de dret públic, 35, ISSN 1885-5709, 2007

Fuente de la clasificación: Clasificación Decimal Universal (CDU)

Fuente de los descriptores: palabras clave facilitadas por los autores

004.7

David Felip i Saborit, profesor titular de derecho penal del Departamento de Derecho de la Universidad Pompeu Fabra

ca Demanar la lluna en un cove? Sobre la possibilitat de prohibir penalment l'ús de les tecnologies de la informació i la comunicació

es ¿Poner puertas al campo? Sobre la posibilidad de prohibir penalmente el uso de las tecnologías de la información y la comunicación

p. 307-336

Este trabajo trata sobre la posibilidad de prohibir o restringir penalmente a los ciberdelincuentes el uso de ordenadores, el acceso a Internet o a otras TIC. Con este objetivo, se analiza la experiencia de los Estados Unidos, donde desde hace más de una década se limita y controla el uso de estas tecnologías a personas sometidas a *probation* y *parole*. La

conclusión es que, si bien estas medidas podrían ser aceptables e incluso aconsejables en ciertos casos muy concretos como apoyo de la rehabilitación, la regulación legal y la estructura de ejecución penal de nuestro país son insuficientes para implantarlas fuera de las instituciones penitenciarias.

Palabras clave: ciberdelitos; delitos sexuales; prisión; *probation*; control penal; sociedad de la vigilancia.

ABSTRACT

Revista catalana de dret públic, 35, ISSN 1885-5709, 2007

Classification source: Universal Decimal Classification (UDC)

Key words source: Key words are given by the authors

004.7

David Felip i Saborit, tenured professor of Criminal Law at the Law Department of the Pompeu Fabra University

ca Demandar la lluna en un cove? Sobre la possibilitat de prohibir penalment l'ús de les tecnologies de la informació i la comunicació

en Asking for the Impossible? On the Possibility of Criminalizing the Use of Information and Communications Technologies

p. 307-336

This paper deals with the possibility of criminalizing or restricting under criminal law the use of computers, the access to the Internet or other communication and information technologies by cybercriminals. Towards this end, the U.S. experience is analyzed. In the U.S., the use of these technologies by persons on probation and parole has been limited for

more than a decade. The conclusion is that although these measures might be acceptable and even advisable in certain very specific cases as a support measure in the rehabilitation process, legal regulations and the structure of the criminal justice system in our country are inadequate for them to be implemented outside the prisons.

Key words: cybercrimes; sex crimes; prison; probation; criminal oversight; surveillance society.