AS NOVAS TECNOLOXÍAS DA INFORMACIÓN E DA COMUNICACIÓN. IMPLICACIÓNS LEGAIS

José Pedro Morais Gallego
Centro de Formación e Recursos de Ourense

RESUMO

A aparición das novas tecnoloxías da información e da comunicación, coas súas innegables vantaxes, supón o establecemento de diferentes formas de relacións na sociedade e de novas modalidades de actuación dos individuos tanto no campo do traballo como do mesmo ocio.

Este estudo pretende sinalar as implicacións xurídicas da utilización das novas tecnoloxías desde o punto de vista do usuario, as respostas dos poderes públicos ante os novos métodos delituosos e responder aos interrogantes máis comúns en relación coas actividades que teñen como protagonista a informática.

PALABRAS CLAVE

Novas tecnoloxías, delito informático, *software*, descargas, copia ilegal, políticas de seguridade.

1. INTRODUCIÓN

Cando en 1978 a Constitución española garantía a honra e a intimidade persoal e familiar dos cidadáns e o pleno exercicio dos seus dereitos, facía unha clara referencia á limitación, mediante lei, do uso da informática (artigo 18.4º). Posiblemente, naqueles momentos, ninguén era consciente da repercusión que no futuro ían ter as novas tecnoloxías da información e a comunicación.

A innovación tecnolóxica ía dar lugar a novos problemas sociais e políticos; a revolución informática cambiaría a estrutura interna da sociedade, alterando os métodos para conseguir e tratar a información, así como as técnicas de comunicación e traballo.

Esta nova sociedade, configurada en *redes* de información e máis concretamente en *Internet*, fundaméntase na virtualidade, que lle permite ao usuario o dereito ao anonimato e ao provedor de servizos o deber de dispor de medios para identificar os autores de actos ilícitos.

É innegable o dereito fundamental do usuario de *Internet* á intimidade e ao segredo das comunicacións e este dereito configúrase no anonimato. Non obstante,

as condutas máis danosas realizadas a través de *Internet* e o seu contorno fundaméntanse, precisamente, na capacidade de que unha persoa dixital, por medio dunha identidade virtual xeralmente anónima, vulnere o correo electrónico, os códigos de entrada á información, a protección de programas informáticos, etc., e incluso incorra na realización das ilicitudes penais máis tradicionais (Morón, 2002).

Os poderes públicos tentaron ao longo destes anos dar unha resposta aos cambios introducidos polas novas tecnoloxías no que se refire ao desenvolvemento dunha lexislación propia en materia informática.

No inicio dos anos 70, as primeiras reaccións en materia lexislativa ían en torno á protección da vida privada ante as novas posibilidades de recollida, almacenamento, transferencia e interconexión de datos persoais que propiciaba a informática.

A partir dos anos 80, preténdese combater a delincuencia económica específica derivada das actividades relacionadas coas novas tecnoloxías, observando as dificultades que presentan as disposicións sobre a propiedade para o amparo dunha realidade inmaterial non tanxible. Deste modo, xorden as iniciativas lexislativas en relación coa propiedade intelectual, para a protección dos programas de ordenador por medio do dereito de autor.

Máis adiante, a actividade lexislativa camiñaba cara á introdución de innovacións no campo do dereito procesual, perfeccionando a investigación deste novo tipo de delincuencia para, na actualidade, centrarse no dereito internacional polo feito de que na utilización das novas tecnoloxías as fronteiras desaparecen e a persecución da chamada criminalidade informática ten un carácter supranacional (Lourenço, 2003).

Neste estudo descríbense certas actividades, de dubidosa ou palpable ilicitude, relacionadas co emprego das novas tecnoloxías da información e da comunicación, facendo unha análise das respostas do ordenamento xurídico, ben ante as modernas modalidades delituosas ou ben ante novos modos da realización das figuras máis clásicas.

2. DIFERENTES PROCEDEMENTOS DE ACTUACIÓN POR MEDIO DAS NOVAS TECNOLOXÍAS

Os comportamentos dos usuarios das novas tecnoloxías son variados, estando en continua evolución. Na denominación destas condutas apréciase unha desmesurada proliferación de anglicismos, indicador claro do papel secundario que nestes momentos ten a cultura hispánica no sector das tecnoloxías da información e da comunicación (Tabarés, 2003). Os procedementos máis habituais descríbense a continuación.

2.1. Sniffing

Consiste na utilización de programas rastreadores ou *sniffers*, usados para supervisar o tráfico entre os ordenadores e buscar información. A utilización destes rastreadores pode permitir o control invisible e non consentido do correo electrónico.

2.2. Snooping

Este tipo de acción é similar ao *sniffing*. Ademais de interceptar o tráfico da *rede*, o autor accede aos documentos, correo e outro material gardado, realizando a copia desa información ao seu propio ordenador.

O obxectivo desta conduta pode ser a simple curiosidade, pero tamén pode ser utilizado con fins de espionaxe ou roubo de información ou *software*.

2.3. Spoofing

O *spoofing* é unha técnica para actuar en nome doutros usuarios. Conseguindo o nome e o contrasinal dun usuario lexítimo e ingresando nun sistema, pódense efectuar accións en nome dese usuario, tales como enviar falsos correos electrónicos.

A persoa intrusa utiliza un sistema para obter información e ingresar noutro, desde o que, á súa vez, volve a entrar noutros sistemas. Este proceso é o chamado *looping*, que dificulta a identificación e a localización do atacante, xa que o percorrido excede os límites dun país, e fai a investigación practicamente imposible.

2.4. Rastreo ou monitorización

A monitorización dixital pode ter lugar a través das denominadas *cookies*, pequenos programas ou subrutinas informáticas que identifican o usuario cada vez que entra nun servidor de información e que controlan en certa medida as súas preferencias, constituíndo unha forma de intromisión na privacidade informática dos usuarios.

Os denominados "programas espía" (*spyware, web bugs*), identificadores ocultos e outros dispositivos similares, son outras formas máis graves de intromisión na vida privada. Estes programas introdúcense no terminal dos usuarios sen o seu coñecemento, accedendo aos datos, arquivando información oculta ou rastreando as súas actividades.

2.5. Spaming

O *spaming* consiste no envío non consentido de mensaxes por correo electrónico a unha multitude de particulares, facendo publicidade de produtos ou

servizos comerciais. Deste modo pode chegarse á saturación de calquera caixa de correo electrónico ou incluso ao mesmo bloqueo de todo un sistema informático por medio da execución dun programa de envío masivo de mensaxes.

Como evolución desta técnica, está a conduta dos *hoax*, que perseguen captar enderezos de correo e saturar a *rede* ou un servidor.

2.6. Cracking ou "piratería informática"

As condutas de *cracking* teñen como característica a eliminación ou neutralización dos sistemas de protección que impiden a copia ou utilización inconsentida dunha aplicación informática. Estariamos, polo tanto, nunha copia non autorizada e a posible distribución ilegal de programas informáticos (chamados *warez*, aplicacións comerciais sometidas á acción dun *crack*) con vulneración dos dereitos de autor (Morón, 2002). Estas condutas serían diferentes das condutas de mero intrusismo informático ou *hacking*.

2.7. Condutas de "danos" ou "vandalismo electrónico"

Consisten en asaltos sobre sistemas informáticos para ocasionar perturbacións, modificar ou destruír datos. Estes comportamentos reciben diversa nomenclatura e materialízanse por medio de virus (programas que modifican aplicacións) ou vermes (programas que se autopropagan por medio do correo electrónico). Estas aplicacións aproveitan sistemas mal configurados, a vulnerabilidade de programas ou os fallos de seguridade para a destrución de datos ou perturbación de sistemas, chegando nalgúns casos a permitir o acceso remoto e o manexo do sistema infectado.

Como modalidade destes comportamentos podemos considerar os *troianos*. Trátase de programas informáticos que se instalan no ordenador enmascarados noutros programas executables, de imaxe ou son. Unha vez instalados, poden permitir o acceso remoto ao sistema por medio das chamadas "portas traseiras" (Tabarés, 2003).

De modo similar, as bombas lóxicas, *logic bombs*, consisten na introdución nun programa dun conxunto de instrucións non autorizadas para que, nunha determinada data ou circunstancia predeterminada, se executen de forma automática ocasionando o borrado ou destrución da información almacenada, distorsionando o funcionamento do sistema ou paralizándoo de forma intermitente.

2.8. Intrusismo informático ou hacking

As condutas de *hacking* ou simple intrusismo informático consisten en comportamentos de acceso ou interferencia, sen autorización, nun sistema de tratamento da información.

Pódese clasificar o *hacking* como directo ou indirecto. O primeiro consiste no acceso non autorizado a un sistema informático coa finalidade de obter unha satisfacción persoal ou intelectual polo desciframento dos códigos de acceso ou *passwords*, sen causar danos inmediatos, ou ben pola vontade de curiosear ou divertirse. Tamén é denominado como *joy riding*, ou paseo de diversión, sendo propio de persoas novas, expertas en informática, sen motivación para causar danos (Libano, 2000).

En canto ao *hacking* indirecto, considérase como un medio para a comisión doutros delitos como fraudes, sabotaxes, piratería, etc. Neste caso existe unha intención de danar, defraudar, etc. Estas condutas de intrusismo poden dar lugar a certas especificidades:

- Introdución de datos falsos ou *data diddling*, como por exemplo a manipulación de transaccións de entrada nun sistema informático coa finalidade de ingresar movementos falsos total ou parcialmente, ou eliminar transaccións verdadeiras.
- Redondeo de contas, *salami*, ou *rounding down*, introducindo certas instrucións nos programas para reducir sistematicamente pequenas cantidades e transferilas a contas distintas ou provedores ficticios abertas con nomes supostos e controladas polo defraudador (Blossiers, 2002).
- Recollida de información residual ou *scavenging*, aproveitando as finalizacións das execucións dos programas realizados para a obtención da información residual da memoria ou dos soportes magnéticos; tamén chamado *trashing,* ou busca de directorios e contrasinais rastrexando a *papeleira* do sistema.

2.9. Phreaking

Esta conduta é realizada por persoas con certas ferramentas e coñecementos de hardware e software que manipulan os sistemas informáticos das compañías de telefonía coa finalidade de facer chamadas sen custos.

O *phreaking* comezou como unha actividade intimamente ligada ao *hacking*, posto que un hacker necesitaba facer *phreaking* para poder utilizar moito tempo a liña telefónica de forma gratuíta e, da mesma forma, un *phreaker* precisaba o acceso non consentido a un sistema de comunicacións (Borghello, 2004).

2.10. Phishing

Consiste no envío masivo de mensaxes electrónicas que semellan ser notificacións oficiais coa finalidade de obter datos persoais e bancarios dos usuarios

para facerse pasar por eles en diversas operacións *on line*. Mentres o internauta cre estar dando os datos ao seu banco de confianza, en realidade estallos a facilitar a unha *web* duplicada similar ou igual á verdadeira páxina da entidade bancaria.

2.11. Linking, inlining, deep linking e framing

a) *Linking* é a utilización ilícita de hipervínculos. Prodúcese cando unha páxina *web* reproduce textualmente os títulos dos contidos doutra páxina con enlaces ao correspondente contido.
b) *Inlining* é un comportamento similar ao *linking*, referido ás imaxes (fotografías, debuxos ou pinturas) que circulan libremente pola *rede*. Consiste en copiar nunha páxina *web* propia as imaxes doutras páxinas que pagaron dereitos de autor por elas.
c) *Deep linking*. Este termo fai referencia á introdución na nosa *web* dun *link* (enlace) a outra páxina *web* que non é a páxina de inicio ou "*homepage*". Esta especie de "enlaces profundos" non posúen polo momento implicacións legais claras, pero repercuten nos ingresos por publicidade, xa que os usuarios non pasan pola páxina de inicio (Blasco, 2004).
d) *Framing*. Consiste no establecemento de vínculos por medio de *frames*. A pantalla da páxina *web* orixinal mantense aberta, aparecendo unha pantalla reducida con outra páxina, á que se accede ou se reproduce sen permiso do autor ou autores dela (Miró, 2005).

Como variedade destas técnicas, os *pop ups* son unha forma de bombardear o usuario con publicidade non solicitada a través de ventás emerxentes cada vez que se visita unha páxina *web*.

2.12. Caching e mirroring

O *caching* é unha forma de copia dunha páxina *web* que consiste no almacenamento intermedio e provisional de materiais nun sistema, gardando na memoria RAM dun ordenador, mediante a realización dunha copia, un arquivo ou conxunto de arquivos para a súa posterior recuperación (Garrote, 2001).

O *mirroring* é a creación de sitios idénticos a outros existentes, pero non tan próximos ao usuario. O básico desta conduta reside en copiar de forma exacta unha páxina *web* e colocala noutro servidor máis inmediato, ao que o usuario pode acceder con maior facilidade. Este comportamento afecta claramente aos intereses dos titulares dos dereitos da propiedade intelectual, posto que limitan o acceso á páxina orixinal.

2.13. Softlifting

Trátase da copia en diferentes ordenadores dun mesmo usuario, empresa ou institución dun *software* do que se posúe unha soa licenza de uso. Dentro deste comportamento tamén podería integrarse a adquisición dun programa de ordenador e a súa comunicación pública nunha *rede* interna para a utilización por parte de varios usuarios.

Esta conduta podería considerarse como unha infracción contractual, por incumprimento das condicións dunha determinada licenza de *software*, ademais dunha infracción dos dereitos de explotación exclusiva da propiedade intelectual (Mirón, 2005).

2.14. Downloading e uploading

Basicamente estas actividades consisten na carga e descarga de arquivos dixitais que conteñen obras protexidas polos dereitos de autor.

Downloading sería a conduta do usuario que descarga no seu ordenador unha obra dixitalizada, como pode ser un disco con cancións convertidas en arquivos con formato *Mp3*. Como se trata da simple reprodución dunha obra, estariamos ante unha actividade lícita e permitida, pero sería ilícita a súa posta a disposición do público en xeral e incluso delituosa se concorre ánimo de lucro.

Uploading é a posta a disposición de terceiros dos arquivos dixitais para a posterior descarga por parte doutros usuarios. Este comportamento é claramente ilícito, dado que se trata dunha comunicación pública de obras protexidas polos dereitos de autor.

2.15. Outras condutas

Semella ser interminable o abano de comportamentos, de evidente ilegalidade ou dubidosa legalidade, relacionado co mundo das novas tecnoloxías da comunicación e da información. Para finalizar, podemos considerar:

- Acceso ás áreas non autorizadas ou *piggynbaking*, que consiste no acceso a áreas restrinxidas dentro dos sistemas ou dispositivos periféricos como consecuencia de portas abertas ou dispositivos desconectados.
- Divulgación non autorizada de datos ou *data leakcage*, consistente na subtracción de información confidencial almacenada nun sistema desde un punto remoto.
- Suplantación de personalidade ou *impersonation*, ben mediante utilización de claves alleas de acceso a un sistema, chaves ou tarxetas magnéticas.

- Pinchado de liñas informáticas ou *wiretapping*; trátase de interferir as liñas de transmisión de datos, recuperando a información que circula por elas.
- *Carding,* ou condutas de manipulación de tarxetas de crédito pertencentes a outras persoas coa finalidade de cometer fraudes.
- Roubo de servizos ou de tempo, como utilización sen ningunha autorización dos elementos informáticos da empresa ou organismo para a realización de traballos para terceiros ou para beneficio particular.
- Técnicas de enxeñería social, baseadas na boa fe das persoas que facilitan contrasinais ou claves solicitadas por alguén que se fai pasar por outro.
- Condutas de connotación sexual, especialmente as relacionadas coa pornografía infantil por *Internet*.

3. DELITOS INFORMÁTICOS E DELINCUENCIA INFORMÁTICA

A complexidade de todas estas accións reflíctese, nun primeiro lugar, na dificultade de acadar unha posición doutrinal unánime en canto a unha denominación común. En segundo lugar, e xa desde unha perspectiva xurídica, existen tamén dificultades á hora de encadrar determinadas condutas nun tipo delituoso concreto.

Así, utilízanse os termos de delincuencia informática, criminalidade informática, delincuencia de *guante branco*, abuso informático, *cybercrimen*, delito electrónico, *computer crime* (no ámbito anglosaxón), *computerkriminalität* (expresión xermana).

No ano 1985, un grupo de expertos convocado pola OCDE para analizar este tipo de comportamentos fixo referencia a eles como "delitos relacionados cos ordenadores", integrados por calquera conduta antixurídica, antiética, ou non autorizada, relacionada co procesamento automatizado e/ou transmisión de datos.

Obviamente, non todas as condutas anteriormente descritas, aínda que moitas poden ser socialmente reprochables, constitúen necesariamente un delito. Para que unha acción sexa cualificada como delituosa, é preciso que estea tipificada como tal na lexislación penal correspondente. Neste sentido, o artigo 25.1º da Constitución española establece que "*ninguén pode ser condenado ou sancionado por accións ou omisións que no momento de producirse non constitúan delito, falta ou infracción administrativa, segundo a lexislación vixente naquel momento*". Da mesma forma, o vixente Código Penal de 1995 indica no

seu artigo 10 que "*son delitos ou faltas as accións e omisións dolosas ou imprudentes penadas pola lei*".

Son múltiples as definicións do que pode constituír un delito informático. Así, Davara indica que consiste "en la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, sea hardware o software" (Davara, 1997).

Segundo Gómez Peral, trataríase do "conjunto de comportamientos dignos de reproche penal que tienen por instrumento u objeto los sistemas o elementos de técnica informática, o que están en relación significativa con esta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos" (Gómez, 1994).

O relevante é que, baixo as distintas denominacións, se fai referencia a un tipo de actividades ou comportamentos que teñen como instrumento ou obxecto algún elemento informático e que, o máis importante desde o punto de vista do dereito, reúnen os requisitos que delimitan o concepto de delito.

Non obstante, algúns autores negan a existencia do concepto "delito informático", preferindo denominar as citadas condutas como "delincuencia informática" ou "criminalidade informática", polo feito de que tal fenomenoloxía delituosa non ataca outros obxectos de tutela xa protexidos, tratándose de novos modos de agresión e comisión de actividades ilícitas contra bens xurídicos xa recoñecidos e tutelados (Mata, 2001).

Outros autores, tendo en conta os novos intereses xurdidos dos retos da sociedade actual, consideran que existen outros bens xurídicos a protexer, tales como a información en si mesma e o interese colectivo na seguridade e fiabilidade dos sistemas e *redes* de almacenamento, tratamento, procesamento e transferencia desta. Por este motivo avalan a existencia do concepto de "delito informático" con entidade propia (Rovira, 2002).

De calquera forma, estamos ante o novo reto das novas tecnoloxías que, proporcionando evidentes beneficios, son susceptibles de riscos e inseguridade e obriga os poderes públicos a establecer formas de control destes medios.

4. OS PODERES PÚBLICOS ANTE OS NOVOS FEITOS DELITUOSOS

Considerando a información como ben xurídico a protexer ou o posible ataque aos bens xurídicos tradicionais a través da informática, os poderes públicos recorren ao dereito penal como medio de sanción das novas condutas delituosas.

Este recurso ao dereito penal como resposta á aparición de *Internet* e das novas tecnoloxías, en opinión de R. Mata, presenta tres problemas fundamentais.

En primeiro lugar, hai que determinar a zona punible, decidir os feitos que teñen relevancia penal entre os múltiples comportamentos irregulares derivados das novas tecnoloxías.

Un segundo problema é a individualización da responsabilidade criminal no ámbito dos feitos cometidos a través de *Internet*. É dificultosa a determinación individual da responsabilidade dentro da pluralidade de suxeitos que aparecen no contexto xeral da *rede*.

Ademais, existen certas limitacións na persecución destes feitos motivadas pola fragmentación e aplicación territorial do dereito, pola transnacionalidade dos seus efectos, o que leva a unha necesidade de harmonización da lexislación e a unha maior cooperación internacional (Mata, 2004).

No marco do Consello de Europa, en Budapest, o 23 de novembro de 2001, asinouse o Convenio sobre a Ciberdelincuencia co obxectivo de aplicar, con carácter prioritario, unha política penal común encamiñada a protexer a sociedade fronte ás novas manifestacións da delincuencia, adoptando unha lexislación adecuada e fomentando a cooperación entre os distintos estados.

No preámbulo deste convenio indícase a necesidade de previr os actos dirixidos contra a confidencialidade, integridade e dispoñibilidade dos sistemas informáticos, *redes* e datos informáticos, así como o abuso deses sistemas, *redes* e datos, mediante a súa tipificación para a loita efectiva contra eses delitos, facilitando a súa detección, investigación e sanción, tanto a nivel nacional como internacional.

O convenio, pese a estar asinado por máis de trinta países, non está en vigor por non contar co número necesario de ratificacións; non obstante, representa polo momento o instrumento internacional máis válido para facer fronte ás condutas relativas á chamada *cibercriminalidade* (Mata, 2004).

Este instrumento internacional clasifica en catro grandes grupos as condutas que constitúen ilicitudes penais e que constitúen un referente de cara á adopción de medidas a nivel internacional:

A) Infraccións contra a confidencialidade, integridade e dispoñibilidade dos datos e sistemas informáticos. Dentro destas condutas, figuran:

- acceso deliberado e ilexítimo á totalidade ou parte dun sistema informático,
- interceptación ilícita, por medios técnicos, de datos informáticos comunicados en transmisións non públicas efectuadas a un sistema informático,
- comisión deliberada e ilexítima de actos que causen danos, borren, deterioren ou alteren datos informáticos,

- interferencias nos sistemas que obstaculicen gravemente o funcionamento destes mediante a introdución, transmisión, provocación de danos, borrado, deterioración, alteración ou supresión de datos informáticos,
- condutas abusivas relativas á produción, venda e obtención para a súa utilización de dispositivos informáticos que permitan a realización dos feitos delituosos anteriores.

B) Delitos relativos á falsificación e á fraude informática. Os Estados deberán adoptar as medidas necesarias para tipificar como delito no seu dereito interno as seguintes infraccións:

- introdución, alteración, borrado ou supresión de datos informáticos que dean lugar a datos non auténticos, coa intención de ser tidos en conta ou utilizados a efectos legais como se fosen auténticos,
- condutas de introdución, alteración, borrado ou supresión de datos informáticos ou calquera interferencia no funcionamento dun sistema informático coa intención fraudulenta ou delituosa de obter de modo ilexítimo un beneficio económico.

C) Delitos relativos aos contidos. Neste grupo faise referencia a unha serie de condutas relacionadas coa pornografía infantil:

- produción, oferta ou posta a disposición de pornografía infantil por medio dun sistema informático,
- difusión ou transmisión de pornografía infantil por medio dun sistema informático,
- adquisición de pornografía infantil por medio dun sistema informático para un mesmo ou para outra persoa,
- posesión de pornografía infantil nun sistema informático ou nun medio de almacenamento de datos informáticos.

Para estes efectos, no convenio, enténdese como pornografía infantil todo o material pornográfico que conteña a representación visual dun menor comportándose dunha forma sexualmente explícita, a dunha persoa que pareza un menor comportándose dese modo e incluso as imaxes realistas que representen menores en comportamentos sexualmente explícitos.

D) Delitos relacionados con infraccións da propiedade intelectual e dereitos afíns. Os Estados deberán adoptar as medidas necesarias para tipificar como delito no seu dereito interno as infraccións relativas a:

- a propiedade intelectual, de conformidade coas obrigas da Acta de París de 1971 pola que se revisou o Convenio de Berna para a protección de obras literarias e artísticas, do Acordo sobre os aspectos

dos dereitos de propiedade intelectual relacionados co comercio e do Tratado da OMPI sobre a propiedade intelectual,
- a protección de artistas intérpretes ou executantes, produtores de fonogramas e organismos de radiodifusión (Convención de Roma).

5. A RESPOSTA DO ORDENAMENTO XURÍDICO ESPAÑOL

5.1. Ámbito penal

Segundo o Código Penal de 1995 e a súa modificación pola Lei Orgánica 15/2003, do 25 de novembro, pódense clasificar as condutas delituosas relacionadas coas novas tecnoloxías da comunicación e da información como:

a) Delitos contra a intimidade e a propia imaxe.
b) Delitos contra o patrimonio e a orde socioeconómica (furtos, defraudacións, danos, propiedade intelectual e industrial, mercado e consumidores)
c) Falsidades documentais
d) Outras referencias indirectas (defraudacións de fluído eléctrico e similares, delitos societarios e estragos).

Así, dentro dos delitos contra a intimidade, a integridade e dispoñibilidade de datos e sistemas informáticos, o artigo 197 do Código Penal (CP) castiga con penas de 1 a 7 anos de prisión e multa de 12 a 24 meses o descubrimento e revelación de segredos, como conduta que leva a apoderarse de mensaxes de correo electrónico alleas ou acceso a documentos privados sen a autorización dos seus titulares. O artigo 264.2 CP castiga, como un delito de danos, cunha pena de 1 a 3 anos de prisión e multa de 12 a 24 meses, a destrución, alteración ou dano de programas ou documentos electrónicos alleos contidos en *redes*, soportes ou sistemas informáticos. O artigo 278 CP, en relación co mercado e os consumidores, sinala penas de 2 a 5 anos de prisión e multa de 12 a 24 meses para o que se apodere ou difunda documentos ou datos electrónicos de empresas[1].

En relación cos delitos de estafa e fraude, o artigo 248.2 CP impón penas de 6 meses a 3 anos de prisión para as estafas como consecuencia de manipulacións informáticas, cando o defraudado excede os 400 €. O artigo 255 CP castiga con multa de 3 a 12 meses a defraudación de enerxía ou nas telecomunicacións valéndose de mecanismos, alteración de contadores ou medios clandestinos. Por outra parte, a utilización de calquera equipo terminal de telecomunicación sen consentimento do seu titular, que cause un prexuízo económico superior aos 400 €, está castigada con pena de multa de 3 a 12 meses (artigo 256 CP)[2].

Con respecto aos delitos relacionados coa propiedade intelectual e industrial, o artigo 270 CP sinala a pena de 6 meses a 2 anos de prisión e multa de 12 a 24 meses para a copia non autorizada de programas de ordenador ou de música e para a fabricación, distribución ou posesión de programas que vulneran as medidas de protección anti-piratería. A mesma pena establece o artigo 273 CP para o comercio a través de *Internet* con produtos patentados sen a autorización do titular da patente.

O acceso, sen consentimento do prestador de servizos e con fins comerciais, a un servizo de radiodifusión sonora ou televisiva e a servizos interactivos prestados a distancia por vía electrónica, así como a fabricación, importación, distribución, posta a disposición, venda, alugamento ou posesión de calquera equipo ou programa informático para facer posible o citado acceso, está penado con 6 meses a 2 anos de prisión e multa de 12 a 24 meses (artigo 286 CP). A mesma pena impón este artigo para a alteración do número identificativo dos equipos de telecomunicacións e a subministración, aínda sen ánimo de lucro, de información sobre o modo de conseguir un acceso non autorizado aos citados servizos.

En relación coas condutas de exhibicionismo e provocación sexual, o artigo 186 CP castiga con penas de 6 meses a 1 ano de prisión e multa de 12 a 24 meses a venda, difusión ou exhibición entre menores, por calquera medio, de material pornográfico.

Con penas de 1 a 4 anos de prisión sanciona o artigo 189 CP as condutas de produción, distribución, venda ou exhibición por calquera medio, de material pornográfico que utilice na súa elaboración menores de idade ou incapaces; incluso está penada a simple posesión de material para a realización destas condutas.

5.2. Ámbito civil e mercantil

A problemática que xira en torno ás novas tecnoloxías ten as súas repercusións no campo do dereito privado e, fundamentalmente, no referente á protección xurídica do software, dereitos de autor, copia e distribución de programas, etc.

O artigo 428 do Código Civil (CC) indica que "o autor dunha obra literaria, científica ou artística ten o dereito de explotala e dispor dela á súa vontade", e remite á lexislación especial no sentido de que "a lei sobre propiedade intelectual determina as persoas ás que pertence este dereito, a forma do seu exercicio e o tempo da súa duración. Nos casos non previstos nin resoltos pola dita lei especial aplicaranse as regras xerais establecidas neste Código sobre a propiedade" (art. 429 CC).

Os programas de ordenador considéranse como a consecuencia dunha actividade, cunha notable carga de intelectualidade, que producen obras creativas, orixinais, que, baixo un determinado soporte, realizan certas tarefas coa finalidade básica do manexo da información (Davara, 2004). Así, como un ben inmaterial obxecto do tráfico xurídico, a nosa lexislación non ampara os programas de ordenador baixo a protección da propiedade industrial; a propia Lei de Patentes de 1986 indica no seu artigo 4 que son patentables as invencións novas e susceptibles de aplicación industrial, excluíndo de forma explícita os programas de ordenador.

A normativa española a este respecto segue o camiño emprendido por case todos os países do noso contorno, que é o de asimilar os programas de ordenador ás obras literarias, científicas ou artísticas típicas da propiedade intelectual. De forma inequívoca, o Real Decreto Lexislativo 1/1996, do 12 de abril, Texto refundido da Lei de Propiedade Intelectual (LPI), sinala como obxecto de propiedade intelectual, entre diversas creacións literarias, artísticas e culturais, os programas de ordenador (art. 10).

Internet facilita a copia, distribución e posta a disposición de obras musicais, videográficas, programas de ordenador, etc. As condutas máis conflitivas son as relacionadas coas copias e reproducións non autorizadas desas obras, como, por exemplo, a colocación dun programa de ordenador nun sitio *web* para facer posible a copia a todos os que teñan acceso a el.

Como xa quedou apuntado no tratamento penal destas condutas, a posibilidade do anonimato e a dificultade de probalas complican a aplicación do Dereito.

Os dereitos de explotación dunha obra ou programa de ordenador durarán toda a vida do autor e setenta anos despois da súa morte ou declaración de falecemento (arts. 26 e 98 LPI). Non obstante, unha obra xa divulgada poderá reproducirse sen a autorización do autor, para uso privado e sempre que a copia non sexa obxecto de utilización colectiva nin lucrativa (arts. 31 e 100 LPI).

Para estes efectos, considéranse infractores dos dereitos de autor os que, sen autorización do titular deles, poñan en circulación ou teñan, con fins comerciais, unha ou máis copias dun programa de ordenador coñecendo ou podendo presumir a súa natureza ilexítima. Tamén son infractores dos dereitos de autor os que poñan en circulación ou teñan, con finalidade comercial, calquera instrumento para facilitar exclusivamente a supresión ou neutralización non autorizada de calquera dispositivo técnico utilizado para protexer un programa de ordenador (art. 102 LPI).

O titular dos dereitos de autor, sen prexuízo doutras accións legais que lle correspondan, poderá instar o cesamento da actividade ilícita, a retirada do comercio das copias ilegais e a súa destrución, a inutilización ou destrución dos elementos exclusivamente destinados á reprodución desas copias e de calquera ins-

trumento destinado a facilitar a supresión ou neutralización non autorizada da protección dun programa de ordenador e tamén poderá esixir a indemnización dos danos materiais e morais causados (arts. 139 e 140 LPI).

5.3. Ámbito laboral

Desde o punto de vista deste estudo, a problemática da aplicación das novas tecnoloxías no mundo do traballo garda unha estreita relación co que poderiamos chamar o "uso indebido", é dicir, aquel en que un traballador non utiliza as tecnoloxías que o empresario ou institución pon á súa disposición cunha determinada finalidade, senón cun ánimo lúdico ou baseado en motivacións persoais. Prodúcese, neste caso, un baleiro legal importante no que existe a contraposición dos dereitos de dúas partes: por un lado, o poder de dirección do empresario sobre a actividade dos traballadores ao seu servizo, e, por outro, o dereito á intimidade e o segredo das comunicacións (Segoviano, 2003).

O empresario ten recoñecido o poder de dirección sobre a actividade dos traballadores ao seu servizo, podendo adoptar as medidas que estime máis oportunas de vixilancia e control para verificar o cumprimento por estes das súas obrigas e deberes laborais (art. 20.3º Estatuto dos traballadores –ET–).

O modo de levar a cabo o control das actividades dos traballadores non está establecido de modo expreso. O citado artigo 20 ET indica que na adopción e aplicación das medidas de vixilancia o empresario debe gardar a debida consideración á dignidade humana dos traballadores. Por outra parte, nesta cuestión opera un límite de gran importancia referido a dous dereitos fundamentais: o dereito á intimidade (art. 18.1º CE) e o dereito ao segredo das comunicacións (art. 18.3º CE), que poden ser vulnerados polo empresario na súa actividade de control das obrigas e deberes dos traballadores.

As resolucións dos distintos xulgados e tribunais son dispares en relación coa utilización indebida por parte do traballador de *Internet* e do correo electrónico e tamén á hora de pronunciarse respecto aos poderes de control que ten o empresario dentro deste ámbito (Segoviano, 2003). A liña xurisprudencial maioritaria foi nun principio claramente favorable aos intereses dos empresarios, considerando que o dereito ao segredo das comunicacións non ampara os correos electrónicos enviados polos traballadores empregando os medios informáticos que a empresa pon á súa disposición, posto que non se trata dunha correspondencia privada, senón da utilización indebida de medios e instrumentos da empresa para fins alleos aos estritamente laborais. Igualmente sucede co acceso a *Internet* en xornada laboral cunha finalidade allea á derivada do posto de traballo, onde priman os intereses do empresario ante o dereito á intimidade do artigo 18.1º CE.

Actualmente, na xurisprudencia apréciase un posicionamento máis favorable aos dereitos dos traballadores, prevalecendo o dereito fundamental á intimidade persoal ante o interese empresarial polo feito de obter a proba dun modo ilícito, tal como a utilización de programas espía sen coñecemento dos traballadores ou o rexistro do ordenador sen as garantías que establece o artigo 18 ET de necesidade, respecto á dignidade e intimidade e con asistencia dun representante legal dos traballadores.

Ante este confuso panorama, moitas empresas implantan as chamadas políticas de seguridade, nas que se articulan as obrigas e deberes dos traballadores que dispoñen de acceso aos sistemas informáticos, ben prohibindo o seu uso, filtrando contidos ou vixiando as comunicacións. Nestas políticas establécense as consecuencias que pode ter para os traballadores o incumprimento desas medidas de seguridade en relación co uso de *Internet* e do correo electrónico no ámbito laboral.

6. A MODO DE CONCLUSIÓNS

Logo deste percorrido polas distintas condutas relacionadas coa utilización das novas tecnoloxías e do seu encaixe no ordenamento xurídico, pódese concluír que non todos os comportamentos que teñen como medio ou finalidade elementos informáticos son necesariamente sancionables. Para que isto sexa así deben concorrer certos requisitos que por necesidade teñen que estar establecidos nas leis.

Diariamente, estamos ante situacións que, como consecuencia dun escaso desenvolvemento lexislativo e de decisións xudiciais variadas, poden xerar certa confusión. Preténdese, para finalizar, intentar dar resposta a certas interrogantes que xorden na vida cotiá.

6.1. Copia privada dun CD

Estamos ante un suposto legal no que non é precisa a autorización do autor dunha obra xa divulgada para proceder a unha reprodución desta para o uso privado do copista, sempre que non sexa obxecto de utilización colectiva nin lucrativa. Polo tanto, e tal como se desprende do artigo 31 LPI, facer unha copia dun CD ou DVD para uso privado é un dereito e non constitúe un delito.

6.2. Descargar de Internet *software* desprotexido ou *cracks*

Descargar un ficheiro de música sen ánimo de lucro e para uso privado non é delito; descargar un ficheiro dun libro sen ánimo de lucro e para uso privado tampouco é delito; igual sucede cun ficheiro dunha película, que tampouco é delito sempre que non exista ánimo de lucro e sexa para uso privado.

Descargar un programa informático cuxa distribución non sexa libre nin autorizada polo seu autor ou distribuidor si sería delito porque, a diferenza dos outros tipos de ficheiros, a descarga de *software* non está amparada polo dereito de copia privada (que permite a reprodución de obras xa divulgadas para uso privado do copista) e precisa a autorización do autor ou distribuidor do *software*. Polo tanto, a descarga de *software* tanto a través dunha páxina *web* como por medio das *redes* P2P é ilegal.

O artigo 100 LPI permite facer unha *copia de seguridade* dun programa de ordenador, pero soamente por parte do que ten o dereito a utilizar o programa, é dicir, do seu usuario lexítimo. Polo tanto, é importante a distinción entre copia privada, aplicada a unha obra de audio ou vídeo en formato informático, e copia de seguridade, aplicada exclusivamente aos programas de ordenador, dos que o artigo 99 LPI prohibe expresamente a súa copia incluso para uso persoal, coa excepción vista da copia de seguridade.

En canto aos denominados *cracks*, están prohibidos por toda a lexislación e incluso a súa posesión está penalizada.

6.3. Desprotección de CD e DVD para facer unha copia de uso privado

A desprotección dun CD ou DVD para facer unha copia de uso privado non é un delito. O artigo 270.3º CP, na súa nova redacción segundo a Lei 15/2003, prevé o castigo dos que fabriquen, importen ou simplemente teñan calquera medio especificamente destinado a facilitar a supresión non autorizada ou neutralización da protección dos programas de ordenador ou calquera obra, pero fai unha clara referencia aos termos previstos no apartado 1 do mesmo artigo "con ánimo de lucro e en prexuízo de terceiro". Polo tanto, a desprotección dun soporte coa finalidade de facer unha copia para uso privado e non colectivo non ten carácter delituoso.

6.4. Difusión de obras musicais, literarias ou científicas a través de páxinas *web*

Os usuarios de sistemas similares ao antigo *Napster* realizan reproducións lícitas cando descargan ao seu ordenador obras protexidas para uso privado e non colectivo. Non obstante, podemos considerar que, logo, ao pór á disposición de terceiros esas obras, están facendo comunicacións públicas ilícitas. Este comportamento podería ser sancionable pola vía civil conforme á LPI, pero non por vía penal, a menos que a citada difusión se faga con ánimo de lucro.

Os titulares da páxina *web*, pola súa parte, cometen unha ilicitude civil cando poñen a disposición do público obras das que non son titulares, podendo converterse esta conduta en delito no caso de producirse unha ganancia a cambio, ben directamente, ben indirectamente por medio da publicidade ou polo número de visitas (Miró, 2005).

6.5. Uso das redes P2P (*Peer-to-peer*) na descarga de arquivos

O comportamento dos usuarios destas *redes* é similar ao descrito no punto anterior. No antigo sistema *Napster*, a súa páxina *web* servía como un intermediario que realizaba a posta a disposición do público das obras protexidas polo dereito de autor, existindo unha clara comunicación pública ilícita destas, da que eran responsables os titulares daquela *web*.

O sistema *Peer to peer* está baseado nos mesmos principios. Non obstante, a páxina *web* en ningún momento pon a disposición do público as obras protexidas, senón que a través do *software* permite que os usuarios contacten entre si e, desde os seus propios ordenadores, carguen e descarguen calquera obra.

As condutas dos particulares que acceden a estas *redes* terán a mesma cualificación legal que no caso de *Napster*: a descarga é unha reprodución dunha obra, e dependerá do seu uso (público ou privado) para resultar ilícita. A posta a disposición pode considerarse unha comunicación pública ilícita, xa que lle permite ao público o acceso a obras protexidas polo dereito á propiedade intelectual (Miró, 2005).

A reforma do Código Penal, levada a cabo pola Lei 15/2003, do 25 de novembro, non deu unha resposta clara en torno ao carácter delituoso destas condutas. A esixencia do ánimo de lucro nelas implica delimitar o concepto de lucro; para certos sectores doutrinais o ánimo de lucro e o ánimo de aforro son a mesma cousa, o intercambio de arquivos nunha *rede P2P* é un troco, unha forma de comercio. Ademais, arguméntase que unha copia privada, ao ser distribuída, deixa de ser privada e non está amparada polo dereito de copia privada.

Desde outro punto de vista, unha aplicación literal do Código Penal daría lugar ao seguinte paradoxo: baixar unha canción a través dunha *rede P2P* podería implicar unha pena de prisión de 6 meses a 2 anos (art. 270 CP), pero o furto dun CD enteiro nuns grandes almacéns suporía unha simple multa pola comisión dunha falta (art. 623 CP).

A aplicación do Código Penal nestas condutas semiprivadas é difícil, salvo en casos de gran relevancia.

6.6. Compartir conexións e accesos a sistemas de pagamento

Segundo o artigo 256 CP, a utilización de calquera tipo de terminal de telecomunicación, sen o consentimento do seu titular e que lle ocasione a este un prexuízo superior aos 400 euros, está castigada cunha pena de multa de 3 a 12 meses.

Polo tanto, compartir conexións e accesos a sistemas de pagamento pódese considerar delito sempre que tal práctica estea expresamente prohibida polo prestador deses servizos ou operadora e ocasione un prexuízo de máis de 400 euros (*véxase a Nota 2*).

6.7. Aproveitar unha conexión sen fíos allea

Esta conduta ten un claro carácter delituoso. En primeiro lugar, pódese vulnerar o segredo das comunicacións e a intimidade do titular desa conexión nos termos establecidos no artigo 197 CP. Igualmente, pódese incorrer nun delito de defraudación (art. 255 CP) e, da mesma forma, estaríase cometendo un delito de acceso non autorizado a un equipo de telecomunicación, con independencia da contía da posible defraudación (art. 286 CP).

6.8. Facer público o modo de acceso non autorizado a un servizo de telecomunicacións

O citado artigo 286 CP prohibe, aínda sen ánimo de lucro, facilitarlles a terceiros por medio de comunicación pública información sobre o modo de conseguir o acceso non autorizado a un servizo de radiodifusión sonora ou televisiva e aos servizos interactivos prestados a distancia por vía electrónica.

6.9. Outras actividades relacionadas

Entre outras cuestións relacionadas coas novas tecnoloxías, podemos considerar a descodificación dunha canle de televisión mediante a utilización dun ordenador. Esta conduta constitúe un delito, posto que é preciso o emprego dun *software* especificamente orientado a romper unha protección, con infracción do artigo 286 CP sobre o acceso non autorizado.

Para finalizar, é tamén delituosa a conduta de liberar un teléfono móbil, posto que é preciso dispoñer dunha tecnoloxía (*software/hardware*) especificamente deseñada para a desprotección dos mesmos. Non obstante, o propio usuario pode liberar legalmente un teléfono móbil cando o fai con permiso ou por delegación da operadora correspondente, tecleando os códigos subministrados por ela.

7. BIBLIOGRAFÍA

BLASCO, J. Deep Linking: ¿enlaces a problemas? http://www.infonomia.com [Consulta: 30 abril 2004].

BLOSSIERS MAZZINI, J. J. (2002) *Los delitos informáticos en la banca*. Lima, Rao.

BORGHELLO, C. F. Seguridad informática. Sus implicaciones e implementación. http://www.web.net/seguridad [Consulta: 30 marzo 2004].

DAVARA RODRÍGUEZ, M. A. (2004) *Manual de Derecho Informático*. Navarra, Aranzadi.

GARROTE FERNÁNDEZ-DIEZ, I. (2001) La propiedad intelectual en la sociedad de la información. En BERCOVITZ RODRÍGUEZ-CANO, R. *Manual de propiedad intelectual*. Valencia.

GÓMEZ PERAL, M. (1994) Los delitos informáticos en el Derecho Español. *Actas del III Congreso Iberoamericano de Informática y Derecho*. Vol. I. Mérida. UNED Centro Regional de Extremadura, Aranzadi.

LIBANO MANZUR, C. (2000) Los delitos de Hacking en sus diversas manifestaciones. *Ponencias del VII Congreso Iberoamericano de Derecho e Informática: Al inicio de un nuevo siglo*. Lima. Perú.

LOURENÇO MARTINS, A. G. (2003) Criminalidade Informática. *Direito da sociedade da informação*. Vol. IV. Coimbra, Coimbra Editora.

MATA Y MARTÍN, R. M. (2001) *Delincuencia Informática y Derecho Penal*. Madrid, Edisofer.

MATA Y MARTÍN, R. M. (2004) *Criminalidad informática: una introdución al cibercrimen*. Temas de Directo da Informática e da *Internet*. Porto, Coimbra Editora.

MIRÓ LLINARES, F. (2005) *Internet y delitos contra la propiedad intelectual*. Madrid, Fundación Autor.

MORETÓN TOQUERO, M. A. (2002) *Delitos contra la propiedad intelectual*. Barcelona, Bosch.

MORÓN LERMA, E. (2002) *Internet y derecho penal: hacking y otras conductas ilícitas en la red*. Navarra, Aranzadi.

ROVIRA DEL CANTO, E. (2002) *Delincuencia informática y fraudes informáticos*. Granada, Comares.

SÁNCHEZ ALMEIDA, C. e MAESTRE RODRÍGUEZ, J. (2002) *La ley de Internet*. Barcelona, Servidoc.

SEGOVIANO ASTABURUAGA, Mª L. (2003) Nuevas causas de despido: la inadecuada utilización del correo electrónico y de Internet. *Lex Nova* (32) 25-28.

TABARÉS PÉREZ-PIÑEIRO, R. (2003) Ciberdelincuentes en el Ejido digital. Problemática penal del hacking. *Controversia* (4) 53-72.

8. NOTAS

[1] O sistema de penas "días-multa" consiste no aboamento dunha cantidade fixa de diñeiro diario durante un tempo determinado. A extensión mínima da multa será de 10 días e a máxima de dous anos, en función do delito ou falta e as súas circunstancias. A cota mínima diaria será de 2 euros e a máxima de 400 euros, en relación directa coa situación económica do reo.

[2] Cando a cantidade estafada ou defraudada en relación coa enerxía, comunicacións ou equipos terminais de telecomunicación sexa inferior a 400 euros, non constitúe delito, pero si falta, e será castigada coa pena de localización permanente de catro a 12 días ou multa dun a dous meses.

Data de aceptación definitiva: 23/12/05