

Les noves tecnologies enfront de la delinqüència, la llibertat i la seguretat

Nous delictes o noves formes de delinquir

**La configuració jurídica actual dels delictes informàtics a
Espanya i la perspectiva de judicialització penal de noves
conductes produïdes per l'ús de la xarxa.**

Joan Josep Martínez Mateos

2007

Projecte MIC

Índex i glossari de termes

Enunciats de l'índex			Pàgina
1.- Introducció			<u>5</u>
<u>Primera part</u>			
2.- Definició i tipologies del delictes informàtic segons el codi penal espanyol.			<u>7</u>
	2.1.- Distribució dels delictes informàtics segons el bé jurídic protegit.		<u>11</u>
		2.1.1.- La intimitat personal i familiar i la pròpia imatge	<u>11</u>
		2.1.2.- La integritat moral	<u>12</u>
		2.1.3.- La llibertat	<u>12</u>
		2.1.4.- La llibertat i indemnitat sexuals	<u>12</u>
		2.1.5.- L'honor	<u>12</u>
		2.1.6.- El patrimoni	<u>12</u>
		2.1.7.- La propietat intel·lectual	<u>13</u>
	2.2.- Anàlisi sobre l'aplicació de les circumstàncies modificatives de la responsabilitat criminal als delictes informàtics.		<u>13</u>
		2.2.1.- Circumstàncies atenuants	<u>14</u>
		2.2.1.1.- La eximent incompleta	14
		2.2.1.2.- La de greu addició a l'alcohol i les drogues	<u>15</u>
		2.2.1.3.- L'estat passional	15
		2.2.1.4.- La confessió espontània	15
		2.2.1.5.- La reparació espontània	15
		2.2.1.6.- L'atenuant d'analògica significació	15
		2.2.2.- Circumstàncies agreujants	<u>15</u>
		2.2.2.1.- La traïdoria	15
		2.2.2.2.- Disfressa, abús de superioritat o aprofitament de les circumstàncies	15
		2.2.2.3.- Preu, recompensa o promesa	15
		2.2.2.4.- Motius discriminatoris	<u>16</u>

		2.2.2.5.- L'acarnissament	16
		2.2.2.6.- L'abús de confiança	16
		2.2.2.7.- Prevaldre's del caràcter públic	16
		2.2.2.8.- La reincidència	16
		2.2.3.- La circumstància mixta de parentiu	16
		2.3.- La practica de probes en el delicte informàtic	16
		2.3.1.- La de declaració d'imputats i coimputats	17
		2.3.2.- La prova de testimonis	18
		2.3.3.- La pericial	18
		2.3.4.- La documental	18
		2.3.5.- La inspecció ocular i reconeixement judicial	20
<u>Segona part</u>			
		3.- La perspectiva de judicialització penal de noves conductes produïdes per l'ús de la xarxa	21
		3.1.- Diferents visions ètiques de l'ús de les noves tecnologies	25
		3.1.1.- La comunicació i l'ètica de les comunicacions	26
		3.1.2.- Diferents visions ètiques	26
		3.2.- Propostes de codis d'ètica	27
<u>Tercera part</u>			
		4.- Conclusions	30
		5.- Webgrafia i bibliografia	33
Glossari de termes per ordre d'aparició al text			
CP	Codi penal espanyol		
NT	Noves tecnologies		
TIC	Tecnologies de la informació i la comunicació		
CE	Constitució Espanyola		
LO	Llei orgànica		
RDL	Reial decret legislatiu		
LECRim	Llei d'enjudiciament criminal		
RD	Reial decret		

[Hipervincles a les pàgines](#)

Nous delictes o noves formes de delinquir

La configuració jurídica actual dels delictes informàtics a Espanya i la perspectiva de judicialització penal de noves conductes produïdes per l'ús de la xarxa

1.- Introducció

Primera part

El tema s'orienta, en la primera part, a fer un petit anàlisi dels delictes informàtics que actualment estan tipificats a Espanya examinant en primer lloc una definició que pugui ser suficientment descriptiva que inclogui el màxim de locucions possibles encaminada encabir tots els delictes habitualment qualificats com informàtics.

En segon lloc cal veure les descripcions i tipologies existents al codi penal, buscant en elles la novetat o la continuïtat, relativa a l'acció que tipifica com antijurídica, per tal de valorar si es tracta d'una nova forma delictiva o d'una adaptació de la tipificació habitual del delictes a una acció amb elements d'execució (d'acció) nous encabible en la delimitació formulada pel Codi Penal.

La classificació dels delictes informàtics segons el bé jurídic que protegeixen, crec que pot aportar és molt orientativa de les

Així mateix, és important conèixer quines són les circumstàncies modificatives de la responsabilitat penal que poden ser aplicables a cada forma delictiva

i la dificultat per a la pràctica de proves que analitzarem en la primera part.

Segona part

La segona part s'orienta a la possibilitat de que noves conductes puguin ser tipificades en un futur o despenalitzades, segons vam poder veure al debat. Un repàs ràpid a les tipologies penals d'altres països ens pot obrir una mica més la nostra opinió pel que fa aquestes formes delictives.

Les diferents visions ètiques i alguns codis ètics tancaran la visió de l'ús de la xarxa i les noves tecnologies que tenen alguns col·lectius i institucions que tenen a veure amb la moral, les lleis i la utilització com usuaris de les NT o les TIC.

Tercera

Respon a les indicacions de l'auditor de l'assignatura.



[Tornar](#)
[índex](#)

Primera part

2.- Definició i tipologies del delicte informàtic segons el codi penal espanyol.

2.- Definició i tipologies del delictes informàtic segons el codi penal espanyol.

Definició

“Els delictes informàtics, en general, són els actes delictius realitzats amb l’ús d’ordinadors o mitjans electrònics, en tant que aquestes conductes constitueixen l’únic mitjà de comissió possible, o el considerablement més efectiu, i els delictes en els quals es produeixen danys en els equips, xarxes informàtiques, o a la informació continguda en ells, amb vulneració de bens jurídics protegits. Es a dir, són els delictes en els que els mitjans tecnològics o són el mètode o són el mitjà de comissió, o la finalitat de la conducta delictiva en sí.” (1)

La codificació actual del codi penal espanyol en relació als delictes derivats de la informàtica i les noves tecnologies de la informació es centra en les formes delictives següents:

Pornografia infantil

Està regulat de forma extensa a l'article [189 del CP](#). L'acció típica d'aquest delictes és molt extensa però bàsicament la forma de producció pot tenir dos besants en relació amb la informàtica i els mitjans informàtics i les TIC. Així la informàtica i els mitjans informàtics poden ser el contenidor del material pornogràfic on hi surtin menors o incapaços. Aquest és el sentit de la locució del primer paràgraf de l'apartat 1 que diu “*cualquiera que sea su soporte*”.

Igualment, les TIC poden ser utilitzades per al propòsit de “*difusión o exhibición por cualquier medio*”, segons el que es regula al paràgraf segon de l'apartat 1 de l'article 189. En aquest cas cal esmentar la facilitat de difusió i anonimat que suposa la tecnologia de les comunicacions a l'actualitat. En aquest sentit, la dificultat de la ubicació del delictes i la situació en un espai temporal és la característica bàsica que incrementa la capacitat investigativa de la policia.

Podem concloure per tant, que les TIC i els mitjans informàtics, en relació als anomenats delictes de pornografia infantil, poden ser contenidors de material il·lícit per una banda i per l'altra, i aquesta és la més greu per les característiques que he anomenat (difusió, anonimat, ubicació i temporalitat), un mitjà de transmissió amb gestos tan senzills com l'enviament de “*simples arxius digitals*”.

L'autoritat dels delictes de pornografia infantil també es concreta en diferents formes, però, encara que totes elles es poden relacionar amb la comissió d'un delictes informàtic de pornografia infantil, sols les formes regulades en el paràgraf segon de l'apartat 1 de l'article que comentem es poden considerar purament d'aquesta classe. Per tant, la venda, la difusió o la exhibició del material pornogràfic; considerant-se autor tant al que cometi l'acció concreta com el que la faciliti.

Com podem veure, el codi penal espanyol, tot i no fer una menció expressa a les noves tecnologies, si ha previst, amb conceptes amplis, la possibilitat d'aplicació dels tipus penals a les persones que puguin fer ús de les TIC per a la comissió de delictes de pornografia infantil, fins i tot tancant el cercle amb la locució del paràgraf segon de punt 1 que diu “*aunque el material tuviere su origen en el extranjero o fuere desconocido*”, en relació a la possessió d'aquest material.

Amenaces

El delictes d'amenaces està regulat en els articles [169 a 171 del CP](#). La seva configuració jurídica no està especialment influenciada per la possibilitat de cometre el delictes per mitjà de les TIC o les NT. Així la regulació prevista en el codi fa esment del mitjans tècnics sols com una de les formes de delictes agreujat quan, en relació a la forma de difusió, diu “*Las penas señaladas en el párrafo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción...*”. Per la qual cosa, les TIC nomes han vingut a ser un mitjà facilitador i/o de gran difusió per la comissió del delictes d'amenaces, d'aquí la qualificació del tipus penal.

Calumnies i injúries

Aquest tipus de delictes està regulat als articles [205 al 216 del CP](#). Respon a una estructura tecnico-jurídica similar al d'amenaces, segons l'article 211 de disposicions generals als dos tipus delictius , “*La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.*” Bé, és notòria l'eficàcia publicitària d'internet o dels missatges de mòbil, encara que aquest no tan visibles públicament, quan es tracta de cometre un delictes d'injúries o calumnies, per això el CP les considera en cada un dels casos com un delictes qualificat pel mitjà de difusió utilitzat.

És discutible la responsabilitat civil solidària a que fa referència [l'article 212](#) entre l'autor i el responsable del mitjà de comunicació emprat per cometre el delictes. En els mitjans de comunicació tradicional el gerent, el director, l'editor, etc, compleixen amb la missió de supervisió del contingut publicat en el seu mitjà. A internet, el propietari d'un entorn web és difícil que se li puguin derivar responsabilitats civils degut a la manca de control. Una altra qüestió és l'administrador de la web, que és en detall el que posa i supervisa els continguts.

Apologia del genocidi

Segons [l'article 18 del CP](#) és apologia: “*la exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor. La apología sólo será delictiva como forma de provocación y si por su naturaleza y circunstancias constituye una incitación directa a cometer un delito.*” ; com es pot veure, no fa una referència expressa a internet o les NT, però generalitza un concepte que les encercla. Si ens centrem en l'apologia del genocidi segons l'article [510 del CP](#), hem de posar-lo en relació amb l'article [607.1](#) relatiu a la difusió en la que es neguin o es justifiquin els delictes tipificats en l'apartat 1 de l'article,

tenen un càstig penal de privació de llibertat, per tant, novament les NT poden ser objecte de comissió d'un delictes, no de forma genuïna, si no com un mitjà més de producció.

Delictes contra la llibertat de consciència i els sentiments religiosos

Regulat a l'article [525 del CP](#) resulta d'aplicació el raonament exposat a l'apartat anterior pel que fa al protagonisme de les TIC i les NT en la comissió del delictes.

Descobriment i revelació de secrets

Aquests tipus de delictes es troba ubicat en el títol X del CP, de l'article [197 fins al 201](#), l'apartat 1 del 197 fa referència a les noves tecnologies de forma expressa quan fa referència al correu electrònic, la intercepció de les telecomunicacions o qualsevol altre senyal de comunicació, per referir-se a la vulneració de la intimitat d'un altre o la revelació de secrets. També l'apartat 2 fa referència a les TIC quan el delictes es cometi per persones que sense estar autoritzats s'apoderin, utilitzin o modifiquin, en perjudici de tercers, dades de caràcter personal o familiar d'un altre que es trobin registrats en suports informàtics, electrònics o telemàtics. Per tant en aquest tipus sí que les NT formes part de l'element objectiu del tipus.

Falsificació de targes de crèdit

L'articulat previst al codi penal per aquest tipus delictiu no conté cap indicació sobre la possibilitat de fer les falsificacions amb els mitjans informàtics i no hi ha cap paraula que ho pugui indicar. No obstant, la redacció fa referència a les targes de crèdit o dèbit a les que qualifica de moneda segons l'article 387. Aquest tipus d'il·lícits respon generalment a autors en xarxes de delinqüència amb una certa formació tècnica i la disposició de mitjans informàtics de lectura i gravació de les bandes o els xips de les targes, constituint aquesta vinculació una qualificació del delictes de falsificació ([article art 386 CP](#)). Els mitjans informàtics utilitzats en el es qualifiquen segons disposa l'article 127 del CP com un efecte del delictes subjecte a comís.

Estafes

L'article [248 del CP](#) comença amb les estafes dient a l'apartat 1 quines són les conductes susceptibles de ser incriminades, essent la seva formulació la tradicional. L'apartat 2 i 3 han estat introduïts com a conseqüència de la irrupció en el mercat audiovisual de software privat per explotar els materials provinents de la indústria d'audiovisuals i per tal de protegir-lo, per això, de forma expressa fa referència als mitjans informàtics: "3. *La misma pena se aplicará a los que fabricaren, introdujeran, poseyeran o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo*". També l'apartat 2, en relació a les estafes per internet diu: "los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero".

Com veiem en aquest tipus penal internet és el mitjà necessari en el cas de l'apartat 2 i en l'apartat 3 les tecnologies que es deriven de la informàtica per mitjà de programes per produir les estafes previstes en l'article als usuaris, tot i que en aquests casos s'ha de demostrar l'ànim de lucre.

Delictes contra la propietat intel·lectual

Estan regulats a [l'article 270 del CP](#). L'apartat 1 pena la conducta per la qual una persona u organització *“reproduzca, plagie, distribuya o comuniqué públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.”*, en aquest tipus delictiu ha de concórrer l'ànim de lucre i el perjudici de tercer. L'apartat 3 del mateix preveu que el que *“ fabrique, importe, ponga en circulación o tenga cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo.”*. Com podem observar, en la vulneració de la propietat intel·lectual els equips informàtics poden ser el contenidor de la propietat segons l'apartat 1 i l'apartat 3 fa referència a la decodificació o de “krac” per desprotegir i fer ús sense llicència de la propietat d'un altre, tot i que en aquest cas s'ha de demostrar l'ànim de lucre i el perjudici de tercers com hem dit.

Delictes relatius al mercat i als consumidors

Regulat als articles [278 al 286 del CP](#) bàsicament el comesos amb connotacions informàtiques o per aplicació de mitjans tecnològics són dos, els regulats a l'article 278 i els de l'article 286. El 278 fa referència als mitjans de suport que suposen els arxius informàtics quan fa referència a l'acció il·lícita d'apoderament per descobrir els secrets de l'empresa i fa una analogia de [l'apartat 1 de l'article 197](#), del descobriment i la revelació de secrets, si els mitjans informàtics són utilitzades segons el propòsit defraudador del 278.

L'article 286 consisteix en l'alteració mitjançant programes, manipulacions i alteracions dels equips i dotar l'accés als programes de radio o televisió sense coneixement del prestador del servei i amb finalitats comercial. En aquest cas podem concloure que és un delictes plenament originat per l'ús de les NT i les TIC. Les NT que es fan servir per a la decodificació i creació de programari capaç de donar accés a televisió codificada i per una altra banda les TIC que s'han fet servir per a indicar les formes d'evitar el pagament i accedir als serveis d'accés condicional.

Danys relatius a la informàtica i al equips informàtics

Aquest és l'últim dels delictes que analitzaré i està regulat a l'article [264.2 del CP](#) que diu que *“...al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.”* En aquest cas queda clar que els danys no és necessari que siguin físicament identificables en els

equips, per això ja està l'apartat 1, si no que la referència és als programes, dades i documents que com ja sabem no són tangibles, per tant el dany que se'ls produeixi ha de ser electrònic o informàtic.

2.1.- Distribució dels delictes informàtics segons el bé jurídic protegit.

El motiu de fer un repàs al bé jurídic que protegeixen els articles que hem relacionat i comentat en l'apartat anterior és per tenir la perspectiva del legislador del codi de 1995 que va agrupar les conductes derivades de l'evolució informàtica al voltant dels bens jurídics coneguts i establerts en la carta magna espanyola. Per tant, pel que sembla, ha estat més fàcil tractar-los com a noves formes de delinquir que no com nous delictes derivats de l'evolució de la societat en relació a la revolució de les comunicacions que estan suposant les TIC i les NT.

Bàsicament els bens jurídics que es protegeixen amb la tipificació penal són els següents:

- La intimitat personal i familiar i la pròpia imatge
- L'honor
- La integritat moral
- La llibertat
- La llibertat i indemnitat sexuals
- El patrimoni
- La propietat intel·lectual

Començarem per veure la relació dels delictes informàtics amb:

2.1.1.- El dret a la intimitat personal i familiar i a la pròpia imatge contemplada a l'article 18 de la CE com una garantia del dret a que ningú vulneri la intimitat de la persona, en qualsevol àmbit, ni la imatge pública. Es tractaria per tant de la intromissió en la vida de les persones o el deteriorament públic de la imatge personal i familiar.

- a. La intimitat personal.- Es pot veure vulnerada de diverses formes en la xarxa o amb l'ús de sistemes informàtics. La tipificació en el CP correspon al TÍTOL X "*Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*" CAPÍTOL I "*Del descubrimiento y revelación de secretos*" regulat com hem vist a l'article 197 i següents. Algunes formes de producció del mateix pot ser: la intromissió de hackers en el nostre sistema, la intercepció del correu electrònic, l'apoderament d'arxius informàtics personals.
- b. La imatge personal i familiar si es deteriora a s'atempta contra ella pot ser motiu d'un delictes d'injúries dels articles 205 al 216 del CP. Tot i que en aquest cas també és un atemptant contra l'honor com a bé jurídic.

2.1.2.- La integritat moral es recull a [l'article 16 de la CE](#) la garantia que l'Estat ha d'exercir sobre la llibertat religiosa, ideològica i de culte no sols de l'individu, també de les comunitats. La [LO 5/1980 de 5 de juliol de llibertat religiosa](#) ve a confirmar i reforçar l'emparament legal en relació a la integritat de la moral. No obstant, el CP regula a [l'article 525](#) les accions ofensives contra les creences morals, els sentiments, de membres de confessions religioses mitjançant publicació escrita feta pública. En aquest tipus penal no fa una referència expressa a les TIC o NT, però com hem dit abans per als delictes contra l'honor, no deixen de ser un mitjà molt eficaç per fer públics els escarnis contra dita confessió religiosa.

2.1.3.- La llibertat, que en aquest cas no es tracta de la llibertat física, de moure's, si no, de la llibertat de decidir, de la voluntat. De la voluntat de decidir que pot ser disminuïda o anul·lada per una altre. [L'article 17 de la CE en l'apartat 1](#) diu: Que tota persona té dret a la llibertat i a la seguretat.

Estem per tant en els delictes d'amenaques i de coaccions que es regulen als [articles 169 a 172 del CP](#), en aquest cas, com en els dos últims es facilita la possibilitat de comissió també com un mitjà més.

2.1.4.- La llibertat i indemnitat sexuals les hem de posar en relació amb el dret a la intimitat personal i familiar i a la pròpia imatge i el dret a la llibertat en el sentit que hem exposat, per tant els delictes que podem associar aquesta contravenció penal és el regulat a [l'article 197](#) “*Del descubrimiento y revelación de secretos*”, i, segons el cas als [articles 169 a 172 del CP](#), d'amenaques i coaccions.

Tornen a ser, en aquest tipus criminal, les noves tecnologies i internet facilitadors per a la comissió del delicte.

2.1.5.- El dret a l'honor està recollit també a l'article [18.1 de la CE](#) “Es garanteix el dret a l'honor...”, segons doctrina constitucional el dret que es tracta de protegir amb la regulació penal és el dret a ser respectat, a no se humiliat ni escarnit. És un dret sense el qual no es pot entendre la dignitat de la persona inherent a la dignitat humana. Tot i tractar-se d'un dret inherent a la persona individual, també és transfereix a les associacions, agrupacions polítiques i religioses, la família, etc de les que la persona individual forma part. Com he dir en l'apartat anterior, els atemptats contra l'honor poden ser objecte d'un delictes d'injúries dels articles [205 al 216 del CP](#) i respon a conductes com: publicació a internet o difusió per correu electrònic de fotos íntimes, fotos trucades on surti la persona en actituds o posicions compromeses essent fàcil el reconeixement, etc, rebre insults per mitjà de qualsevol foro i finalment ser calumniat pels mitjans anteriors.

Com podem observar és un dels delictes en què les NT faciliten la comissió, obrint-se també la possibilitat als missatges des de telèfons mòbils.

2.1.6.- El patrimoni o la propietat està recollit a [l'article 33 de la CE](#) que reconeix el dret a la propietat privada. La protecció d'aquest bé jurídic, en relació a les NT i les TIC, tant com a mitjà per a cometre accions delictives com a objecte de conductes il·lícites es veu reflectida, novament en el CP, de diferents formes segons si són l'objecte o si són el mitjà.

- a. Si són l'objecte el delicte, quan es produeix en el programari o arxius, danys o modificacions, per invasions de virus o altres programes estem davant d'un delicte de danys dels que es regula a l'article 264.2 del CP. En aquest cas, és de suposar que el mitjà de comissió del delicte és: per una banda internet, que ha servit per transmetre els programes, i, per una altra, l'ordinador del creador del programa, el que en la majoria dels casos queda indemne.
- b. Si són el mitjà de comissió com hem vist anteriorment, estaríem davant de dos formes delictives: les estafes i la falsificació de targes de crèdit.
- c. També hem de classificar en aquest apartat els delictes relatius al mercat i als consumidors dels articles 278 al 286 del CP, encara que amb relació al l'apartat 1 de l'article 197 de la revelació de secrets.

2.1.7.- La propietat intel·lectual no té un reconeixement específic a la CE. L'article 149.9 de la mateixa fa referència a la propietat intel·lectual com una competència de l'Estat en relació a la seva regulació legal. No obstant, l'Estat, fent ús d'aquesta norma, ha dictat la llei de la propietat intel·lectual amb l'última redacció per RDL 1/1996 de 12 d'abril.

El nou CP ha recollit de forma expressa una protecció penal, com a norma negativa, encara que la Constitució, com a norma positiva, no l'hagi recollit com un bé jurídic reconegut.

Menció diferenciada mereix els **delictes comesos per apologia**, en els que la regulació penal pretén la defensa dels bens jurídics de la llibertat i la igualtat. L'apologia del genocidi què el que fa és la justificació o la negació de l'holocaust s'ha recollit com hem vist al CP article 607.1.

2.2 Anàlisi sobre l'aplicació de les circumstàncies modificatives de la responsabilitat criminal als delictes informàtics.

En el delicte informàtic pur ens troben amb la dificultat de graduació de la punibilitat i l'antijuridicitat, segons el que es preveu al CP, amb les circumstàncies modificatives de la responsabilitat penal, degut a la distància normalment que es produeix, tan en temps com en espai, des de la comissió del delicte fins que es descobreix, l'anonimat i l'emascarament que suposa internet i les noves tecnologies també se sumen a les dificultats d'aplicació. No obstant, mirarem de fer una aproximació a dites possibilitats de modificació i discernir, en funció dels delictes que hem vist, susceptibles de ser qualificats com "informàtics", a quins podrien ser aplicables, pensant també en algunes possibilitats casuístiques.

Les circumstàncies modificatives de la responsabilitat penal estan regulades als articles 20, 21, 22 i 23 del CP, i, com podem observar la seva concepció està orientada a la modificació la responsabilitat dels delictes, podríem dir tradicionals, que es cometen i s'ubiquen en llocs específics, en espais socials clarament delimitats i significatius, amb freqüència amb noms, amb la possibilitat de ser assenyalats en un mapa, es poden deduir escenaris del crim, es poden trobar proves físiques que qualsevol persona pot reconèixer, es pot obtenir un perfil psicològic de la víctima i el delinqüent, la comunitat els coneix, etc.

2.2.1.- Circumstàncies atenuants

L'article 21 del CP preveu les següents:

2.2.1.1- La eximent incomplerta: És la que es recull a l'apartat 1 i fa referència a les atenuants, de forma que si alguna d'elles no concorren els requisits necessaris en cada una seran atenuants. Si fem un repàs a l'article 20, les eximents, observem que són difícils d'aplicar als delictes informàtics, degut a que la comissió d'aquest s'ha de fer amb molta consciència dels que es fa, sols el els casos de ininputables (menors de 18 anys i incapaces) són aplicables per aplicació de l'article 19, i que tampoc poden actuar com atenuants incomplertes degut a que ambdues són taxades no hi ha termes mitjos en l'edat de 18 o en la incapacitat. Veiem però la resta:

“1.- El que al tiempo de cometer la infracción penal, a causa de cualquier anomalía o alteración psíquica, no pueda comprender la ilicitud del hecho o actuar conforme a esa comprensión.

El trastorno mental transitorio no eximirá de pena cuando hubiese sido provocado por el sujeto con el propósito de cometer el delito o hubiera previsto o debido prever su comisión.”

Com es pot apreciar, les característiques del delictes informàtics fa que sigui difícil la seva aplicació.

“2.-El que al tiempo de cometer la infracción penal se halle en estado de intoxicación plena por el consumo de bebidas alcohólicas, drogas tóxicas, estupefacientes, sustancias psicotrópicas u otras que produzcan efectos análogos, siempre que no haya sido buscado con el propósito de cometerla o no se hubiese previsto o debido prever su comisión, o se halle bajo la influencia de un síndrome de abstinencia, a causa de su dependencia de tales sustancias, que le impida comprender la ilicitud del hecho o actuar conforme a esa comprensión.”

Es torna apreciar la dificultat d'aplicació de la eximent en un delictes informàtics per les raons comentades al primer paràgraf, difícilment un ciberdelinqüent s'alienarà per cometre el delictes, però ni que estigui en aquest estat, com es podrà saber si no hi ha testimonis ?.

El punt 3, relatiu a l'alteració en la percepció per naixement, difícilment una persona amb aquesta afecció podrà cometre un delictes informàtics. El mateix passa amb el punt 4, “*El que obre en defensa de drets propis o aliens*”, amb els requisits de: Patir una agressió il·legítima, la necessitat racional del mitjà de defensa utilitzat i la manca de provocació suficient del defensor.

En aquests supòsits **el denominador comú és la presència física entre el subjecte actiu i el subjecte passiu** o els bens objecte del delictes, situacions que en el delictes informàtics no es donen i si es donen és mitjançant els xats o les videoconferències.

Els punts 5, 6 i 7, l'estat de necessitat, la por insuperable i el compliment d'un deure respectivament, poden ser aplicables als delictes informàtics en general, més amb els que tenen a veure amb l'honor, la intimitat personal i familiar i la pròpia imatge i la llibertat, més susceptibles de ser executats amb coaccions.

2.2.1.2.- La de greu addició a l'alcohol i les drogues: Continguda a l'apartat 2 de l'article 21, també com les anteriors, no és fàcil trobar una relació amb el delinqüent informàtic, plenament conscient del delicte que està cometent i també per la dificultat de relacionar el moment i el lloc de producció de l'acció delictiva i l'atenuació per l'addicció.

2.2.1.3.- L'estat passional: De l'apartat 3 que podria ser d'aplicació, encara que costaria la justificació, al delicte d'amenaques, calumnies i injúries o, de forma més general, als bens jurídics de l'honor, la intimitat personal i familiar i la pròpia imatge.

2.2.1.4.- La confessió espontània: Aplicable a qualsevol delicte.

2.2.1.5.- La reparació espontània: Igual que l'anterior.

2.2.1.6.- L'atenuant d'anàloga significació: Els comentaris fets de cada una de les anteriors val per aquesta general que obra les possibilitats a altres circumstàncies que tinguin un significat anàleg a les que regula l'article.

2.2.2.- Circumstàncies agreujants

L'article 22 del CP preveu les següents:

2.2.2.1.- La traïdoria: Regulada a l'apartat 1, des del meu punt de vista, i segons la redacció del CP, és una circumstància que podríem considerar que forma part del propi delicte informàtic. La referida redacció diu: " empleando en la ejecución medios, modos o formas que tiendan directa o especialmente a asegurarla, sin el riesgo que para su persona pudiera proceder de la defensa por parte del ofendido.". La impunitat i la manca de risc físic i de possibilitats d'identificació dels autors que proporciona la comissió de delictes per internet és indiscutible i, per això, aquesta circumstància, caldria que es considerés integrada en la acció delictiva Informàtica.

2.2.2.2.- Disfressa, abús de superioritat o aprofitament de les circumstàncies: En aquesta, aplicaria el mateix raonament que l'anterior, en algun dels conceptes. La disfressa, considerant que internet permet disfressar-se mitjançant pàgines web suposades o suplantant personalitats d'altres, per exemple en les estafes o en la falsificació de targes o apoderament dels codis de comptes bancaris.

L'aprofitament de les circumstàncies de temps i lloc, considero que en gran part dels delictes que hem comentat, produïts mitjançant les TIC, aquesta circumstància és inherent al tipus.

L'abús de superioritat i la utilització de persones per obtenir la impunitat o debilitar la defensa de l'ofens crec que han de ser elements a determinar en cada cas concret, ja que, la utilització de persones, per exemple menors, per cometre el delicte informàtic podria donar lloc a l'aplicació d'aquesta agreujant.

2.2.2.3.- Preu, recompensa o promesa: Aquest és un agreujant perfectament aplicable a tots els delictes informàtics.

2.2.2.4.- Motius discriminatoris (raça, sexe, religió, etc): Aquesta és l'agreujant 4 de l'article que comentem i és la més susceptible de ser aplicada a delictes que tenen a veure amb el racisme o la xenofòbia, l'apologia i contra els sentiments religiosos. Fets delictius que fan servir internet i la facilitat de difusió que té.

2.2.2.5.- L'acarnissament, tal i com està concebut a l'agreujant 5 s'orienta a l'acarnissament físic o psíquic però crec que és necessària la presència física entre subjecte actiu i passiu, per tant, buscar una aplicació al delictes informàtic és poc menys que difícil.

2.2.2.6.- L'abús de confiança, de l'apartat 6, és plenament aplicable a delictes com el de revelació de secrets, els relacionats amb la propietat intel·lectual, les estafes i al mercat i els consumidors.

2.2.2.7.- Prevaldre's del caràcter públic el culpable és aplicable a tot tipus de delictes.

2.2.2.8.- La reincidència, també és aplicable a tot tipus de delictes inclosos els informàtics.

2.2.3.- La circumstància mixta de parentiu

Aquestes circumstàncies poden agreujar o atenuar la penalitat del delictes segons el que disposa l'article 23 del CP que diu: "*Es circumstància que puede atenuar o agravar la responsabilidad, según la naturaleza, los motivos y los efectos del delito, ser o haber sido el agraviado cónyuge o persona que esté o haya estado ligada de forma estable por análoga relación de afectividad, o ser ascendiente, descendiente o hermano por naturaleza o adopción del ofensor o de su cónyuge o conviviente.*" Com es pot apreciar té un ascendent familiar o afectiu en les dos direccions d'atenuació o agreujament.

Alguns delictes informàtics que hem vist que podria aplicar-se com agreujant: el de pornografia infantil i el de descobriment i revelació de secrets, imaginem que una parella es separa i una de les parts, per despit, publica a internet fotos íntimes. Podria aplicar-se a les estafes i a la falsificació de targes i no s'ha de descartar en els delictes contra la propietat intel·lectual.

En relació a la possibilitat d'atenuar algun dels tipus delictius que tractem no es veu cap possibilitat d'aplicació. Sols de forma remota en els delictes que es puguin produir contra l'honor com a bé jurídic i contra la llibertat de consciència i els sentiments religiosos com a delictes específic reculat a l'article 525 del CP.

2.3 La practica de probes en el delictes informàtic

En tot procés penal la practica de la prova és el moment més significatiu i transcendental per a inculpar del fet delictiu al fins aquell moment presumpte autor. Les dificultats de portar-les a terme impregna tots aquest tipus delictius, segons una fulla explicativa de la unitat especialitzada de la Guàrdia Civil, el comandant Juan Salom Clotet posa com a dificultats de la investigació policial les següents:

- Conservación de datos de tráfico.
- Imposibilidad de identificación del **usuario**.
- Virtualidad de la prueba informática
- Determinación espacial de la Ley penal
- Mundo digital desconocido. Judicatura

En base aquestes primeres consideracions hem d'analitzar les formes probatòries previstes a la legislació criminal. Cal remarcar, però, que l'expressió "**d'usuari**", l'hem de canviar per la de **presumpte autor** i posteriorment imputat en la causa. A més no farem referència a la determinació espacial de la llei penal per no ser un tema objecte d'aquest estudi.

En relació al món digital desconegut per la judicatura, és un fet comentat en els debats de l'aula i que com va quedar bastant remarcant, aquest fet impregna totes les formes probatòries relacionades amb aquests tipus delictius, sobre tot els que la única prova possible és la pericial, documental o la inspecció ocular, prova aquesta última que la sol practicar la policia judicial especialitzada amb la comissió judicial constituïda a l'efecte i per això amb més garanties d'èxit processal.

La importància o les deficiències de practicar proves no ajustant-se als procediments i les lleis, pot avocar a sentències absolutòries de l'imputat per manca de proves o de proves realitzades amb vulneració de drets.

2.3.1.- La de declaració d'imputats i coimputats

La primera dificultat investigativa és la identificació dels autors i coautors, que si hi ha indicis racionals de la comissió dels delictes passaran a ser declarats per l'autoritat judicial imputats i coimputats respectivament. Segons el tipus de procediment, ordinari o abreuja, es fa per interlocutòria de processament ([Art 384 paràgraf 1º de la LECrim](#)), o, en la primera compareixença ([Art 775 de la LECrim](#)), respectivament. La dificultat prové, com ja hem comentat, de l'anonimat que suposen la infinitat de terminals i accessos a la xarxa a disposició del públic en establiments de pública concurrència que han proliferat amb la evolució tan espectacular que tenen les NT i les TIC; pensem en cibercafés, campus universitaris, aeroports, hotels, zones d'esbarjo, etc.

És la primera prova de la fase del judici oral i la primera pregunta que fa el president del tribunal a l'imputat és si està conforme amb la pena més alta sol·licitada, si presta la seva conformitat pot derivar en una sentència de conformitat si es compleixen els requisits legals, en cas contrari es continua amb l'interrogatori.

La pràctica d'aquesta prova no planteja especials dificultats ni processals ni pericials, ja que es tracta d'obtenir una versió dels imputats i coimputats dels fets dels quals són acusats, i que la seva versió, emparada en el dret de defensa i no declarar contra sí mateixos, pot ser falsa o de negativa a declarar, les proves inculpatòries, per tant, s'han d'obtenir amb els altres mitjans de prova.

2.3.2.- La prova de testimonis

Un altre característica del delictes informàtic és que la comissió es fa de forma virtual, per mitjà de la xarxa, on no hi ha testimonis, o els que puguin haver la voltant de l'escenari, o són coautors o no saben què s'està fent, precisament, per no mostrar-se cap interacció amb la víctima, que encara que virtualment estigui present es imperceptible per qualsevol observador que no participi de l'acció. Per això la prova de testimonis en aquest tipus de delictes estarà més encaminada a establir la personalitat de l'autor/s, la presència del mateix/os en llocs i hores concretes o les manifestacions que l'autor/s, amb ànim de notorietat, pugui haver fet a amics i coneguts de les intencions de comissió del delictes.

En relació a la pràctica de la prova ens hem de remetre a la regulació extensa que ha fet la LECRim que s'estén de [l'article 701 al 722](#).

2.3.3.- La pericial

L'alta qualificació tècnica que es necessita per esbrinar l'iter criminis seguit pels imputats fa d'aquesta prova una de les més difícils de portar a terme i, al temps, és de les més rellevants de la instrucció policial i judicial. La dificultat de trobar la informació necessària i les tècniques seguides pels autors és evident per, com hem dit, la comissió virtual de crim, que pot ser descobert després de molts dies d'haver estat comés. Aquesta primera dificultat hem de sumar la que esmenta el Comandant de la Guàrdia Civil en relació al poc coneixement que tenen els òrgans jutjadors de les xarxes i internet. En aquest punt hem de recordar que la prova, actualment en el nostre sistema, és de lliure apreciació del tribunal que recolza la seva decisió en les màximes d'experiència, el coneixements personals i el convenciment que li aportin les proves pericials, les quals queden sotmeses a les parts, tant pel que fa a la proposició com la defensa i qüestionament.

Una altra dificultat de la prova pericial radica en que en molts casos s'ha de fer amb urgència, pels funcionaris de la policia judicial o en presència del jutge instructor perquè se sospiti que pugui desaparèixer o sigui d'impossible reproducció en l'acte de judici oral. Aquestes proves són les que s'anomenen preconstituïdes i anticipades. Normalment solen tenir un marcat caràcter inculpatori, però també és aquí on es pot caure en la possibilitat d'incórrer en la formulació de proves il·lícites per manca de requisits legals, com pot ser el cas d'entrada i registre sense autorització judicial en un domicili o local per obtenir les proves dels disc dur del presumpte delinqüent.

Segons la doctrina, les proves que es fonamenten en una perícia que s'hagin de preconstituir o anticipar es consideren documentals en la vista del judici oral, per la raó que queden registrades en l'informe del pèrit.

Queda recollida la seva regulació en la LECRim en els [articles 723-725](#).

2.3.4.- La documental

La prova documental no suposa cap més problema que en qualsevol altre tipus delictiu en relació a l'obtenció, requisits de fons i de forma i valoració judicial. Pot ser que, com hem dit abans, pel

llenguatge utilitzat s'hagi de fer una interpretació pericial per al bon enteniment de l'òrgan judicial, però amb aquesta excepció, no té una especial dificultat de formulació. Està recollida a [l'article 726 de la LECRim](#).

2.3.5.- La inspecció ocular o reconeixement judicial

El reconeixement judicial està previst en la fase de judici oral segons el que disposa [l'article 727 de la LECRim](#). La consideració que la jurisprudència té d'aquesta prova en aquesta fase és d'excepcional segons les sentències d'1 de juliol de 2003 RJ 2003/6258, de 6 de febrer y 13 de novembre de 2002, entre d'altres. Segons aquestes sentències, l'aparició de la fotografia com a element descriptiu d'escenaris de crims fa innecessària aquesta prova en la fase del judici oral i la trasllada a les fases prèvies d'investigació i d'instrucció, per la qual cosa, entraran en el judici oral per la via de la prova documental en qualitat de prova preconstituïda.

Per això, en quant als requisits i formalitats de la inspecció ocular s'han de complir els que es regulen als [articles 326 a 333 de la LECRim](#) relativa a la inspecció ocular en la fase d'instrucció. No obstant, com he dit en el cas de la prova pericial, de la que per aquesta podríem dir el mateix, la realització de la inspecció ocular també suposa, en cas de delictes informàtics, l'actuació d'experts per a realitzar-la, ja que no consisteix "solsament" en la capacitat d'observació forense de l'entorn, que té les seves dificultats, si no que és necessària la manipulació minuciosa i cauta del sistema informàtic objecte d'investigació, sobre tot quan es tracta de delinqüents experts en informàtica.



[Tornar](#)
[índex](#)

Segona part

3.- La perspectiva de judicialització penal de noves conductes produïdes per l'ús de la xarxa.

3.- La perspectiva de judicialització penal de noves conductes produïdes per l'ús de la xarxa. (2)

Les diferents societats del món i els dirigents que les governen a l'actualitat s'estan trobant amb un nou escenari que fa tan sols 10 o 15 anys no existia ni es podia imaginar amb la incorporació a la nostra vida quotidiana d'internet i les noves tecnologies de la informació. Els canvis que les NT i les TIC estan generant no és un fenomen local, l'abast és mundial. La rapidesa amb que la informació es propaga per internet és un dels exemples, al que s'ha de sumar, el nombre immens de receptors de la informació propagada i la llibertat per accedir, tres factors que estan provocant reaccions legislatives de diversa magnitud en els diferents estats, que varia segons el règim de govern.

No obstant el règim de govern, també s'està produint una acceleració de la implantació i un intent per a la igualtat d'oportunitats d'accés de totes les societats i cultures. Les NT, permeten la formació, el comerç, activitats recreatives i lúdiques, la comunicació entre grups d'amics, jocs en línia, i tantes d'altres activitats present i per descobrir, que també està generant el que s'està anomenant la cibersocietat, no tant com un grup humà diferent dels altres humans, si no com totes aquelles persones que són capaces de fer ús i aprofitar-se de les oportunitats que ofereixen les NT i les TIC.

És en aquest conjunt d'oportunitats on s'està experimentant el major canvi de la mentalitat del "ciberciudadà", que està sent capaç d'assumir un vocabulari propi, uns hàbits de consum de "ciberproductes", però també, a mesura que les possibilitats i la cibersocietat s'amplien també s'amplien o es generen els ciberdelinqüents.

El ciberdelinqüent ho és per vulnerar bens jurídics com hem vist abans. De forma simple, els dos bens jurídics bàsics són: els que vulneren drets personals i els que atempten contra la propietat de les persones físiques o jurídiques. Un tercer, que separo dels dos anteriors, és aquell conjunt de delictes que cada estat, particularment, considera contraris al propi estat.

Observem com estan tractant alguns països la vulneració dels seus bens jurídics per mitjà de la legislació penal en relació al delictes informàtics.

Estats Units

Actualment als EEUU regeix la "Computer Fraud and Abuse Act de 1986", En ella es fa referència en la seva major part als delictes següents: abús o frau contra empreses financeres, registres mèdics, ordinadors d'institucions públiques financeres, tràfic de claus amb intenció de cometre frau, declara il·legal l'ús de passwords alienes o propies en forma inadequada. Però sols és aplicable en els casos en els que hi hagi danys superiors a mil dòlars. L'any 1994 es va publicar l'Acta Federal d'Abús Informàtic que modificava la de 1986 afegint: la contaminació de sistemes amb qualsevol classe de virus o instruccions que facin fer als ordinadors aliens coses que no han produït els seus usuaris, contaminar les seves bases de dades o modificar els programes, modificar, destruir, copiar,

transmetre dades o la simple alteració d'ordinadors o xarxes. En tots aquests casos s'han formulat els delictes corresponents.

Es pot dir que tots els comentaris sobre la legislació d'EEUU la titllen de pròxima i realista amb el problema del delictes cibernètic i com hem pogut veure de la primera a la segona Acta (lleis), que és específica per als delictes informàtics, s'han afegit noves accions de qualificació criminal. Aquest comentari es confirmen amb la proliferació de més normativa relacionada amb les conductes de l'ús d'internet com veurem a continuació.

- Ús d'identitats fraudulent en línia, de 3 de febrer de 2004 "*Fraudulent Online Identity Sanctions Act*".
- Protecció dels infants a internet de 15 de desembre de 2000 "*Children's Internet Protection Act*".
- Llei de protecció del frau i activitats relacionades amb la connexió d'ordinadors a la xarxa de 1 de maig de 1999 "*Fraud and related activity in connection with computers.*"
- Llei de Prevenió de Cyberpirateria de Marques de 6 d'octubre de 1999 "*Trademark Cyberpiracy Prevention Act*".
- Protecció infantil contra els depredadors sexuals de 27 de gener de 1998 "*Protection of Children From Sexual Predators Act of 1998*".
- Protecció del joc a internet de 3 de setembre de 1997 "*Internet Gambling Prohibition Act*".
- Llei de decència en les comunicacions de 31 de desembre de 1995 "*Communications Decency Act of 1995*".

Xina

El règim de l'estat xinès va anunciar el 23 de gener de 2001 que mitjançant el Tribunal Suprem castigaria amb pena de mort l'espionatge per internet. Així, d'aquesta manera, totes les persones implicades en activitats d'espionatge poden ser condemnades penes que oscil·len de 10 anys de presó a la de mort. Per espionatge s'entén qualsevol activitat relacionada amb el robatori, descobriment o divulgació de secrets d'Estat.

El tribunal determina que hi ha tres tipus d'activitats on la vigilància i el càstig seran extrems: les accions relatives a la vulneració de secrets qualificats d'alta seguretat, els secrets d'estat, informacions de produeixin danys seriosos a la seguretat de l'estat o als seus interessos. Es consideren també il·legals les infiltracions de documents relacionats amb l'estat i la defensa, les tecnologies punta i la difusió de virus informàtics.

Es pot deduir que l'estat xinès està més preocupat per la seguretat de l'estat que de la protecció dels bens jurídics de les persones, que no fa una llei, si no que es limita a anunciar pel Tribunal Suprem les accions i conductes que es consideraran delictes, fent especial menció a les que es deriven de l'espionatge a la que asseguren la condemna de la pena de mort.

França

La llei sobre el frau informàtic 88/19 de 5 de gener de 1988 preveu entre d'altres les següents conductes: Accés utilitzant frau a un sistema d'elaboració de dades, graduant les penes en funció del resultat com la modificació o la destrucció de dites dades.

El sabotatge informàtic és la conducta de falsejament d'un sistema de tractament de dades. I en relació a la destrucció d'informació es sanciona al que intencionadament i amb menyspreu dels drets dels demés introdueixi dades en un sistema de tractament automatitzat, supprimeixi o les modifiqui així com l'alteració del sistema de tractament o de transmissió.

La falsificació de documents informatitzats també la recull en quan es facin amb la intenció de causar perjudici a un altre.

És un sistema que no contempla un ventall ampli de conductes delictives

Alemanya

La reforma del codi penal alemany operada per la segona llei contra la criminalitat econòmica de 15 de maig de 1986 ha criminalitzat les següents conductes:

- Espionatge de dades
- Estafes informàtiques
- Falsificació de dades probatòries i falsedat de documents.
- Alteració, cancel·lació o inutilització de dades, fins i tot la temptativa és punible
- Sabotatge informàtic
- Utilització il·lícita de targes de crèdit
- Estafes informàtiques

Holanda

L'1 de març de 1993 va entrar en vigor la llei de delictes informàtics. La llei contempla específicament com a conductes il·legals el Hacking, relatiu a l'ús i manipulació de sistemes informàtics i el Phreaking, relatiu a la manipulació de sistemes telefònics. Com a fets punibles es trobem tipificats:

- Entrar en un ordinador en el qual no es té accés legal
- Ús d'un ordinador hackead per accedir a un altre, en aquest cas agreuja la pena privativa de llibertat de sis mesos de màxim de l'anterior a quatre anys.
- Copiar arxius de la màquina o sistema hackeads o processar dades d'ella
- Publicar la informació obtinguda si les dades devien romandre en secret. No obstant si són d'interès públic no és il·lícita aquesta publicació.
- Danys a sistemes informàtics amb una pena màxima de 15 anys de privació de llibertat si amb els danys al sistema s'ha causat la mort alguna persona.

- Alterar, afegir o esborrar dades d'un sistema informàtic, amb el tipus agreujat si l'acció es fa de forma remota.
- La infecció de virus informàtic intencionada.
- El Phreaking i la venda d'elements que permetin el Phreaking.
- La falsificació de targes de crèdit.

Anglaterra

A l'agost de 1990 va entrar en vigor la Computer Misuse Act, llei d'abusos informàtics, per la qual, qualsevol intent, consumat o no d'alteració de les dades informàtiques amb intencions de caràcter criminal es podia castigar amb penes de privació de llibertat de fins a cinc anys.

Les conductes típiques en aquesta llei són:

- L'accés no permès ni autoritzat a un.
- Realitzar fets delictius amb una computadora hackeada
- Realitzar qualsevol modificació en el sistema que permeti la còpia de dades o manipulació de programes i la contaminació amb virus

Xile

Xile va ser el primer país iberoamericà que va emetre una llei en relació a la cibercriminalitat, la llei 19223 de 7 de juny de 1993 "*Ley Contra Delitos Informáticos*".

Les conductes típiques en aquesta llei són:

- La destrucció o inutilització d'un sistema de tractament de la informació
- L'accés a sistemes aliens sense autorització amb afectació de les dades del mateix. Inclosos els autors dels virus als quals és aplicable aquest tipus.
- El hacking, amb ànim d'apoderament de la informació per usar-la o conèixer-la indegudament.
- Donar a conèixer la informació emmagatzemada en un sistema.
- És delictes qualificat, en el cas anterior, si el que ho fa és el responsable del sistema.

Àustria

La llei per a la reforma del Codi Penal de 22 de desembre de 1987, preveu les següents accions delictives:

- Destrucció de dades que inclou les dades personals, les no personals i els programes.
- Estafa Informàtica que tipifica les accions de:
 - El perjudici patrimonial dolós

- Confeccionar programes per a la influència en el resultat d'elaboració de dades automàtica
- Introduir, cancel·lar o alterar dades d'un sistema informàtic
- Actuar sobre el processament de dades. En aquest cas qualifica el delicte per aquells que s'aprofitin de la seva professió.

Com es pot veure en la majoria dels estats dels països del nostre entorn cultural i polític les conductes previstes a la legislació criminal són similars, destaca la d'Estats Units amb un sistema de legislació molt dirigit a la limitació de la informació ofensiva, les conductes relatives a les aberracions sexuals i la protecció de la propietat intel·lectual. Amb tot, Espanya és un dels països en el que més conductes s'han tipificat, en defensa dels bens jurídics que protegeix la Constitució. La Xina es troba en l'altre part de la balança amb la màxima preocupació estatal en una direcció: el control sobre la xarxa i la preservació dels secrets d'estat, que arriba a la imposició de la pena de mort, imagino per delictes que ells consideren molt greus, gravíssims diria jo.

(2) La informació relativa a les legislacions dels diferents països està sintetitzada de la pàgina web <http://www.segu-info.com.ar/delitos/delitos.htm>.

3.1 Diferents visions ètiques de l'ús de les noves tecnologies

La paraula ètica prové de grec "Ethikos" que significa caràcter. L'ètica tracta de l'estudi de la moral i l'acció humana. Que està bé o malament en un determinat entorn social ens ho mana la moral de dita societat, formada pel conjunt de creences elaborada a través de segles de formació i evolució. L'ètica respon allò que està bé i el que no i accepta o prohibeix accions i decisions humanes segons els dictats dels seus principis.

Històricament s'ha vingut confonent la moral i l'ètica, considerant l'una i l'altra de forma separada i indistinta, cal dir però que en l'actualitat, la moral respon a un conjunt de valors que mollegen el sentir de cada moment social, valors que han vingut donats per les organitzacions religioses dominants, en part també provocat per estar la vida quotidiana de les famílies centrada en la senzillesa que provoca l'aïllament al que estaven sotmeses les societats. Es pot dir que actualment el valors derivats de la moral del moment estan experimentant un canvi en relació a la font d'emissió, i ja hi ha diverses entitats, poders públics, mitjans de comunicació, religions, etc que doten el concepte de moral de valors que l'ètica converteix en la prohibició i permissió d'accions o decisions. Però la diferència amb aquella ètica històrica està en la sortida de l'aïllament, la comunicació, l'element disruptor d'aquella ètica relict, que proporciona la discussió i el canvi i incorporació constant de valors ètics, segons l'entorn on es comuniqui. Internet, les NT i les TIC, són capaces de donar-nos escenaris ètics diferents en qüestió de segons, on es pot ofendre, sense que necessàriament sigui delicte o es pot delinquir, sense saber que ho fem segons les nostres conviccions ètiques i jurídiques.

La violació al respecte interpesonal derivat de l'anonimat ha fet que algunes empreses incloguin en el seu contracte de serveis d'internet clàusules per les quals els usuaris contractants es comprometin a evitar activitats que puguin causar situacions desagradables, és el cas de l'empresa AOL.

3.1.1.- La comunicació i l'ètica de les comunicacions

Com he dit, el plantejament ètic de la comunicació "a gran escala" com representa internet està fent que totes les institucions reaccionin a la corrupció del mitjà. Un mitjà que a l'hora es veu extremadament útil per al desenvolupament humà, gairebé des de totes les institucions polítiques, socials i econòmiques.

Veiem com les institucions elaboren quins han de ser els valors de les coses. En l'actualitat, les institucions polítiques elaboren els "Llibres verds", que són un recull d'indicacions per al bon ús d'allò que tracta.

La Unió Europea, en el [Llibre verd sobre la protecció dels menors i la dignitat humana en la comunicació](#) planteja a grans trets tres propostes de conducta als estats membres, en relació a les comunicacions i internet, però en relació a les restriccions a la llibertat d'expressió que es fonamentin en la defensa [dels drets dels menors i la dignitat humana](#) que condiciona a tres exigències acumulatives:

- 1) *Prohibició de l'arbitrarietat*, que implica que cada restricció he d'estar prevista per llei;
- 2) *Necessitat social imperiosa* de garantir els valors i els drets de les societats democràtiques;
- 3) *Legitimitat dels objectius*, enumerats de forma limitada i entre els que la defensa de la moralitat i la salut públiques s'estimen particularment adequats per a protegir als menors i la dignitat humana.

És en aquest àmbit dels drets dels menors i la dignitat de la persona que s'ha de conjuminar el dret a la llibertat d'expressió, en relació a les comunicacions.

La violació al respecte interpesonal derivat de l'anonimat ha fet que algunes empreses incloguin en el seu contracte de serveis d'internet clàusules per les quals els usuaris contractants es comprometin a evitar activitats que puguin causar situacions desagradables, és el cas de l'empresa AOL, que ha imposat en els seus contractes un codi de conducta i comportament.

3.1.2.- Diferents visions ètiques

La facilitat amb que internet i els nous continguts i activitats que es poden realitzar està proposant una nova corrent de pensament en relació a l'ètica i la legislació que reguli tot aquest món d'oportunitats i a la vegada de riscos per als menors i la dignitat de les persones. Altres límits que proporcionen les qüestions purament econòmiques per a l'ús de la xarxa com la propietat intel·lectual no són menys importants, encara que des del meu punt de menor transcendència humana. Aquestes

noves corrents són les que aposten per sistemes d'autoregulació, en consonància a la complexitat de regulacions i d'ètiques que es barregen entre usuaris de la xarxa. El que es proposa amb l'autoregulació és un sistema basat en valors, amb insistència per la responsabilitat social, que permeti la flexibilitat que exigeix internet i que es completi per les legislacions locals orientades a facilitar l'adequació constant.

El 22 de febrer de 2002, el “Pontificio Consejo para las Comunicaciones Sociales” va publicar a la Ciutat del Vaticà un document denominat “*Ética en Internet*”. El document situa Internet com a l'últim i més poderós dels mitjans de comunicació, afavorint l'eliminació progressiva del temps i l'espai en la comunicació entre persones. El document planteja que per a l'ús correcte d'internet, s'han de tenir en compte dos elements importants: actuar a favor de la dignitat de la persona humana i la llarga tradició de saviesa moral.

Entre les qüestions ètiques que planteja estan les següents:

- *Individualismo exagerado (modelo neoliberal), convirtiendo Internet en un lugar apto para cualquier tipo de expresión en detrimento de la dignidad y respeto de las personas y los pueblos.*
- *Peligro de división por ideologías, políticas, etnias, etc., convirtiéndose en un potencial escenario de conflictos internacionales.*
- *La denominada «brecha digital», que es la discriminación de personas, grupos o naciones al acceso de las nuevas tecnologías, y así participar de los beneficios propios de este instrumento en el desarrollo humano.*
- *Transmisión de una cultura dominante de falsos valores.*
- *La cuestión de la libertad de expresión queda en suspenso cuando las autoridades públicas bloquean el acceso a la información, siendo las personas sujetas a la manipulación o a la desinformación.*
- *La ideología de la libertad radical no legitima la libre expresión al servicio de la verdad.*

3.2 Propostes de codis d'ètica



El 28 de novembre de 2002 es va aprovar el [Codi Ètic del Comerç Electrònic i la Publicitat Interactiva](#) que va entrar en vigor al gener de 2003, modificat en novembre de 2004 i 2005 amb la finalitat d'adaptar-lo al RD 292/2004 pel qual es crea el Distintiu Públic de Confiança en els Mitjans Electrònics.

Aquest codi planteja un conjunt de normes deontològiques en tres grans àrees: les comunicacions comercials i el comerç electrònic, la protecció de dades de caràcter personal i la protecció dels menors.

En un altre context, el professor Titular d'Ética i Deontología de la Informació de la facultat de Ciències de la Informació de la Universitat Complutense de Madrid, i Professor de Deontologia Informática en la Facultat i Escola d'Informàtica de la Universitat Pontificia de Salamanca en Madrid [Porfirio Barroso Asenjo](#), després d'un estudi entre professionals de la informàtica fa una proposta de codi ètic que és el següent:

“Propuesta de Código Deontológico de Internet

1. Todo usuario de la red de Internet ha de considerar la libertad de expresión como un bien máximo y procurar evitar en lo posible la censura.
2. El intercambio de información en la red se regule por criterios de verdad, exactitud y objetividad.
3. Respetar la necesaria protección y seguridad en la información.
4. Primacía del servicio al bien común, público y social.
5. Respetar la intimidad y vida privada de las personas y la confidencialidad de la información cuando la hubiere.
6. Defender el derecho de autor y la propiedad intelectual evitando toda forma de plagio.
7. Evitar toda forma de piratería.
8. El acceso a Internet de forma no discriminatoria.
9. Evitar el fomento y distribución de material obsceno, erótico y pornográfico.
10. Todo usuario de Internet deberá asumir las responsabilidades éticas y legales a las que el uso que hace de la red diere lugar.”

També estan proliferant normes de conducta per a l'ús dels serveis web, com a exemple i per a finalitzar exposo la de e-México.

“El uso que usted haga de los servicios proporcionados en este sitio, es condicionado a la aceptación del siguiente Código de Ética. e-México se reserva el derecho de prohibir o suspender a cualquier persona, por comportamiento inapropiado en Internet o por quebrantar el Código de Ética.

1. **USO DEL LENGUAJE.-** Al utilizar los foros, salones de charla y al enviar sugerencias, peticiones y comentarios o bien, al publicar material, queda estrictamente prohibido el uso de palabras altisonantes, lenguaje soez o inapropiado, blasfemias así como todo tipo de palabras ofensivas, muestras de odio o amenazas de violencia, que dañen la integridad moral de las personas o instituciones públicas y privadas.
2. **CONTENIDOS DISCRIMINATORIOS (RAZA, GÉNERO, RELIGIÓN, IDEOLOGÍA).-** Queda estrictamente prohibido subir contenidos de carácter discriminatorio, que pretendan atacar a personas o grupos raciales, religiosos, minorías sexuales, o bien, en razón de su género o ideología. Además, queda prohibido subir contenidos difamatorios o constitutivos de calumnia, amenaza o coacción. Cabe señalar que todo contenido que contravenga lo anterior será eliminado y al responsable le será prohibido el acceso y en su caso, la información será puesta a disposición de la autoridad competente.
3. **CONTENIDOS OBSCENOS E ILEGALES.-** Queda estrictamente prohibido publicar contenidos que vayan en contra de la ley y las buenas costumbres, que afecten al pudor y la moral así como los que presenten información tendenciosa, pornográfica, racista, fundamentalista o que afecte el orden público, ético y moral. Cabe señalar que todo

contenido que contravenga lo anterior será eliminado y al responsable le será prohibido el acceso y en su caso, la información será puesta a disposición de la autoridad competente.

4. **BENEFICIO DE COMUNIDADES.-** Queda prohibida la publicación de material que, de uno u otro modo, incumpla los valores de la comunidad o las condiciones de uso, ya que dichos contenidos deberán enfocarse en beneficio de la comunidad correspondiente. e-México se reserva el derecho de prohibir o suspender a los miembros.
5. **COOPERACIÓN, PARTICIPACIÓN O APRENDIZAJE.-** Los contenidos del portal deberán ser informativos y útiles para la comunidad a la cual están dirigidos. Deberá fomentarse la participación, cooperación y retroalimentación entre los miembros de las comunidades.
6. **TRANSPARENCIA.-** Los miembros de cada comunidad deberán actuar en forma transparente en los procedimientos involucrados para el buen funcionamiento de la comunidad, en la toma de decisiones y votaciones sobre asuntos de interés para su comunidad, así como en la elección del líder de su comunidad.
7. **DERECHOS DE AUTOR.-** Queda prohibida la publicación de material con registro de derechos de autor, ya sea contenido textual o bien imágenes, gráficos, dibujos comerciales, emblemas, slogans, distintivos, logotipos y todo elemento con derechos reservados, sin el permiso expreso y por escrito del titular del mismo, así como copiar imágenes, sonidos y/o software propiedad del portal sin consentimiento de e-México. En el supuesto de que algún usuario viole esta prohibición, le será prohibido el acceso y será remitido a las autoridades competentes.
8. **MARCO LEGAL.-** El usuario deberá cumplir con todas las leyes y normas de igual rango, ordenanzas y reglamentos, nacionales e internacionales, que fueran aplicables en relación con el uso del portal e-México, así como en el uso y transferencia de información en el citado portal
9. **NO SABOTEAR EL PORTAL.-** Queda prohibido publicar o compartir información dentro del portal, que contenga intencionalmente algún virus u otras herramientas de programación informática que puedan dañar, interferir perjudicialmente o expropiar sistemas, datos o informaciones personales. Todo contenido que contravenga lo anterior será eliminado y al responsable le será prohibido el acceso.
10. **HONESTIDAD.-** El objetivo del portal es fomentar la comunicación abierta y honesta entre todos sus miembros, quienes deben ser respetados como individuos con el fin de lograr un entorno cálido, armonioso y de respeto. Cualquier acoso o abuso verbal o escrito hacia otros usuarios o miembros del personal de e-México, resultará en la cancelación de los servicios de e-México a la comunidad como grupo y a sus líderes. “

Tercera part

4.- Conclusions.

5.- Bibliografia i webgrafia.

4. Conclusions

La pregunta nous delictes o noves formes de delinquir la hem de buscar crec jo en el següent raonament:

Crec que els nous delictes responen a la criminalització de conductes que fins el moment no han estat considerades com un delicte, per què atenen a la protecció d'interessos econòmics d'uns i altres. En canvi les noves formes de delinquir les hem de posar en relació als delictes que afecten bens jurídics bàsics, detectant-se, això si, dins el mateix tipus delictiu noves formes de cometre'l.

No obstant, a l'inici del treball em feia unes preguntes que havia de ser capaç de respondre sintèticament. Després de totes les consideracions, cites, enunciats i conclusions parcials fetes al llarg del treball, dites preguntes, que reproduïxo a continuació queden ser contestades com segueix:

1.- A Espanya s'estan produint **nous delictes o noves formes de delinquir**?

S'estan produint les dos coses, en primer lloc perquè els nous delictes atenen a conductes que no estaven prohibides que es movien en el context de l'il·lícit civil i que ara, per pressions de les grans empreses s'han criminalitzat, i, en segon lloc, noves formes de delinquir amb l'ús de les NT i les TIC com a mitjà i contenidor del delicte clàssic que fa que s'incrementi l'eficàcia de la comissió i l'anonimat, amb un alt component d'impunitat i carència de risc físic per al delinqüent.

2.- És **suficient la legislació actual** espanyola per a la persecució dels delictes que es produeixen a la xarxa ?.

Com hem pogut apreciar, la legislació espanyola és de les més complertes en matèria de delictes en el que es faci ús de les NT i les TIC pel que fa a la tipificació de les conductes criminals. En canvi, pel que fa a les circumstàncies modificatives de la responsabilitat penal, gairebé no s'han modificat de les que existien pels delictes clàssics construïdes sobre la base de la presència del subjecte actiu en el lloc de comissió del delicte o trobant-se cara a cara amb el subjecte passiu.

Així mateix, la legislació processal no s'ha ajustat als nous temps en relació a la pràctica de les proves, que fan de la investigació un camp abonat per a l'error i la il·legalitat en la obtenció de les mateixes, amb grans possibilitats de sentències absolutòries.

3.- Quines són les **mancances principals** si es que existeixen ?.

L'adaptació de la legislació processal.

4.- Cap a on van les **tendències mundials en relació al delicte informàtic** practicat mitjançant l'anomenada societat de la informació ?.

Com hem vist en la tercera part, bàsicament les tendències mundials fan referència a la **protecció dels menors, de la dignitat humana i de la propietat intel·lectual**. Però també hem vist que els interessos econòmics dels grans monopolis o grans empreses poden fer que els estats penalitzin accions que fins al moment eren discutibles en l'àmbit civil i ara són delictes.

5.- Podria influenciar aquesta tendència a Espanya i fer canviar substancialment la normativa actual ?.

La normativa actual espanyola és de les més complertes i està adaptada a les directives comunitàries per la qual cosa no és que es pugui influenciar per les tendències, està en sintonia amb elles.

6.- La concepció ètica-delicte a internet, com la podríem qualificar en relació a Espanya ?.

A Espanya, la regulació constitucional dels diferents bens jurídics que el codi penal protegeix, és la mesura ètica de referència. No responen a conceptualitzacions morals derivades de raonaments religiosos socialment acceptats ni a prejudicis polítics dels governants, per això podem concloure que és una concepció moderna o actual.

7.- Quines són les opinions dels diferents grups interessats en el desenvolupament de la societat de la informació en relació a les formes d'ús ?.

La tendència més pronunciada en l'actualitat és l'anomenada autoregulació. L'ètica moral de componen religions també intenta fer-se un recó com a grup d'interès. La cibersocietat en general propugna la llibertat d'expressió i d'ús. I algunes webs tenen el seus codis de conducta o normes d'utilització.

8.- Podem concloure normes d'ètica per a l'ús de la xarxa d'internet ?.

És evident que si, la qüestió serà quina de les tendències tindran les normes d'ètica i el més important, que es facin llei, ja que d'un altra manera, són simples llistats d'intencions o de lectures per a la sensibilització.



[Tornar](#)
[índex](#)

5.- Webgrafia i bibliografia

A més de les webs que he anat linkant al llarg del text, el quadre següent reflecteix la majoria de les que he fet servir per treure conclusions i efectuar els redactats.

Quadre de Webs

https://www.gdt.guardiacivil.es/ GDT Grupo de delitos telemáticos	Cos de la Guàrdia Civil especialitzat en delictes informàtics. Descriu algunes formes noves de delictes.
http://www.iabogado.com/esp/guialegal/guialegal.cfm?IDCAPITULO=18050000 iAbogado	Què són els delictes informàtics i algunes tipologies delictives
http://www.bufetalmeida.com/56/delitos-informaticos Bufet Almeida Abogados asociados	Definicions i links a la legislació espanyola sobre les tipologies regulades i els noms vulgars amb els que es coneixen les noves formes delictives per internet.
http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico Wikipedia, la enciclopedia libre	Definició de delictes informàtics molt resumida.
http://www.rediris.es/cert/doc/reuniones/af05/delitos-telematicos.pdf GDT Grupo de delitos telemáticos	Esquema de la investigació policial.
http://www.guardiacivil.org/telematicos/formatos/ciberdelincuencia.pdf	Conveni sobre la ciberdelinqüència del Consell d'Europa de 23/11/01 signat a Budapest
http://dialnet.unirioja.es/servlet/oaiart?codigo=198394 Dialnet	Petit plantejament de les avantatges i inconvenients a la xarxa.
http://www.bvs.sld.cu/revistas/aci/vol11_3_03/aci06303.htm#cargo Acimed	Alguns dels principals problemes ètics que plantegen les noves tecnologies.
http://www.20minutos.es/noticia/133327/0/descargas/p2p/pirateria/ 20 minutos.es	Nota de premsa en relació a les descàrregues P2P.

http://www.consumer.es/web/es/tecnologia/2006/06/22/153236.php Consumer.es	Nota de premsa per la detenció d'un internauta que posava partits de futbol gratuïts a la seva pàgina web.
http://cibersociedad.rediris.es/congreso/ Cultura & politica @ciberespacio	Pàgina del primer congrés ONLINE de l'observatori per a la cibersocietat. 110 ponències i comunicacions relacionades amb les TIC, la societat, l'ètica, la legalitat, etc
http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_ethics-internet_sp.html PONTIFICIO CONSEJO PARA LAS COMUNICACIONES SOCIALES	Plantejament de l'ètica d'interner des de el sector eclesiàstic.
http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo18.htm mailxmail.com	Estadístiques de delictes informàtics.
http://www.delitosinformaticos.com/estafas/estadisticas_2002.shtml delitosinformaticos.com	Estadístiques del 2002 de denúncies i un recull de delictes mes habitual amb links a notícies de premsa.
http://www.monografias.com/trabajos6/delin/delin.shtml monografias.com	Treball sobre els delictes informàtics.
http://www.unav.es/penal/iuspoenale/ Iuspoenale 1.3 Universitat de Navarra	Diferents treballs i material sobre dret penal
http://www.ehu.es/zer/zer3/2artbarr.html Universitat Complutense Madrid	Quatre principis d'ètica a Internet, pel professor Porfirio Barroso Asenjo de deontologia de la informació de la U. Complutense de Madrid
http://noticias.juridicas.com/base_datos/ Notícies jurídiques	Base de dades gratuïta a la que he dirigit els links a articles als que faig esment al llarg del text.

Bibliografia

- Derecho penal español, Rodriguez Devesa, Alfonso Serrano Gómez parte general
- Derecho penal español, Rodriguez Devesa, Alfonso Serrano Gómez parte especial, editorial DYKINSON.