ASPECTOS PROCESALES DE LA INVESTIGACIÓN Y DE LA DEFENSA EN LOS DELITOS INFORMÁTICOS

1.-CONCEPTO Y CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN NUESTRO CÓDIGO PENAL:

En la Dogmática Penal española actual se incluye en el *concepto* de Delito Informático tanto el delito tradicional cometido a través de ordenador o Internet (v. gr.: injurias a través de correo electrónico) como el propiamente tal, Delito contra la Informática, por atacar los datos o sistemas informáticos o las vías telemáticas de comunicación, especialmente a través de Internet (v. gr. daños informáticos causados mediante un virus).

Dentro de ese concepto tan amplio , a su vez, se ha admitido como más adecuada, desde un punto de vista expositivo, la *clasificación* tripartita de los delitos informáticos que pasamos a desarrollar a continuación , relacionándola con su calificación jurídico penal en el actual Código Penal español:

A) Delitos económico patrimoniales vinculados a la informática: *ciberdelincuencia económica.*

Se trata de los ataques al bien jurídico patrimonio ajeno, vehiculizados a través de la Informática, siempre realizados con la intención, por cualquier medio, de consumar apoderamientos o beneficios económicamente evaluables sobre el patrimonio de terceras personas.

Estos tipos penales, que suponen cerca del 70% de los delitos informáticos que se denuncian, se pueden encontrar en nuestro Código Penal principalmente, entre otros, en:

- Art. 238.5 CP.-*Robo inutilizando sistemas de guardia criptográfica*.
- Art. 248.2 CP.-*Estafa informática*, en su doble modalidad de :

-Estafa por *ingeniería social*: a través de engaño a personas (como ocurre con el phising tradicional, o las cartas nigerianas, las estafas de ONGs, el timo del Gordo o de la Lotería, las ventas de segunda mano, las falsas subastas E-bay, etc)

-Estafa por *ingeniería informática*: a través de manipulación informática o artificio semejante, descartando el engaño sobre máquinas o dispositivos técnicos (como el carding y las apropiaciones económicas por manipulación informática)

- Art. 255 CP.- *Defraudación de telecomunicaciones informáticas.*
- Art. 256 CP.- Hurto de tiempo informático, o *Uso no autorizado de terminales informáticos.*

- Art. 264.2 CP.- Virus o *Daños informáticos,* cuando se produce sobre datos. Cuando los daños persiguen más que un ataque a los datos, a los sistemas informáticos, nos hallaríamos ante el *Sabotaje Informático* , a penar conforme al delito de Estragos (art. 346 CP) o , si fuera con intencionalidad terrorista, a través de tal delito (art. 571 CP)
- Art. 270.3 CP.- *Contra la Propiedad Intelectual Informática,* en cualquiera de sus múltiples modalidades creativas reguladas, como puede ser la protección con entidad penal de la creación y explotación antiplagio de programas de ordenador, los intercambios masivos de productos intelectuales vehiculizados a través de la Informática o Internet, etc.
- Art. 273-275 CP.- *Contra la Propiedad Industrial Informática,* en cualquiera de sus modalidades protegidas siempre que tengan entidad penal.
- Art. 278-280 CP.- *Espionaje informático de secretos de empresa.*
- Art. 282 CP *Publicidad engañosa,* Art. 283 CP *Manipulaciones en aparatos en perjuicio del consumidor* o Art. 286 CP *Contra el Mercado Informático*
- Art. 301 CP *Blanqueo informático de capitales*
- Art. 390 CP *Falsedad documental* , cuando el soporte sea de naturaleza informática (art. 26 CP)

B) Atentados por medios informáticos contra la intimidad y la privacidad: *ciberdelincuencia intrusiva.*

Se trata de los ataques al bien jurídico privacidad como un concepto que incluyendo el de intimidad, va más allá, pues abarca todas las modalidades protegidas en el art. 18 CE (el honor, la intimidad personal, la familiar, la propia imagen, el domicilio, el secreto de las comunicaciones, o el uso correcto de la informática)

Suponen el 25 % aproximado de los delitos que se denuncian, y entre otros, se encuentran tipificados en el Código Penal en:

- Art. 169 y 172 CP.- *Amenazas y Coacciones Informáticas*.
- Art. 186-189 CP.- *Distribución de material pornográfico y Pornografía Infantil*
- Art. 197-200 CP.- *Descubrimiento y Revelación de secretos,* que es delito informático intrusivo por excelencia.
- Art. 205-216 CP.- *Injurias y Calumnias Informáticas* , con el art. 211 CP que eleva a las que se hacen a través de Internet al rango de delictivas , excluyendo la falta, por la propia difusión plural del mismo.
- Art. 417,418 y 423 CP.- *Cesión inconsentida de datos ajenos,* a través de la infidelidad en la custodia de documentos y violación de secretos para su venta, hecha por funcionario, que la tiene funcionalmente prohibida.

C) Ataques por medios informáticos contra intereses supraindividuales: *ciberespionaje y ciberterrorismo.*

Se trata de los ataques más graves, que afectan indiscriminadamente a intereses generales de la población, con la intención de crear pánico y terror, para subvertir el sistema político o de convivencia generalmente aceptado.

Apenas tiene incidencia estadística, pero su realización, por afectar a la masa genera mucha intranquilidad y desasosiego.

Algunas de sus modalidades en nuestro Código Penal pueden ser:

- Art. 402 CP.- *Usurpación de funciones públicas* mediante correo electrónico
- Art. 598 y 603 CP.- *Descubrimiento y Revelación de secretos relativos a la Defensa nacional.*

Por otra parte ,sociológicamente, estos delitos tienen una *enorme proyección de futuro,* ya que, por un lado crecen desmesuradamente año a año (por ejemplo, los delitos de Pornografía a través de Internet se han multiplicado por 4 en España entre 2004 y 2005),

sus autores en la mayor parte de los casos conocidos son personas jóvenes que no alcanzan la media de los 40 años , y en muchos casos ni siquiera llegan a la mayoría de edad , a ellos se incorporan altos profesionales cualificados del mundo de la ciencia y la tecnología (ingenieros, informáticos, físicos, etc) que incluso no rehuyen la delincuencia grupal organizada, y además, año a año, evolucionan en cuanto al uso de las últimas tecnologías de la comunicación y la informática de manera que obligan a quienes los combaten a tener que actualizarse constantemente.

2.-CARACTERÍSTICAS ESPECÍFICAS PROPIAS DE LA INVESTIGACIÓN EN LOS DELITOS INFORMÁTICOS:

Pese a la heterogénea variedad de delitos que hemos visto se recogen bajo la denominación de Informáticos, la preparación de la fase previa a juicio que conocemos como instrucción presenta en ellos una serie de características comunes o especificidades propias en su investigación que los singulariza de la que se realiza respecto de otros y que pueden enumerarse en los siguientes rasgos:

2.1 LA UBICUIDAD COMO TEORÍA PARA DETERMINAR SU COMPETENCIA:

Dado el carácter itinerante de la comisión de este tipo de delitos, que numerosas veces incluso afecta al territorio de diversos países o al mundo entero (en los supuestos de los delitos por Internet) y la diferente ubicación del lugar desde donde se dirige el ataque informático y el de aquel donde éste despliega su resultado, se vino planteando tradicionalmente cuál era el foro y el Juez competente para el conocimiento e investigación de cualquier delito informático con efectos en más de un partido judicial, pues un sector doctrinal abogaba por la teoría de la acción , y otro, descontento con los grados de ejecución que ello determinaría , por la del resultado.

Para evitar esas discusiones sobre foro (que sólo favorecen el anonimato delincuencial y la demora en la persecución de estos delitos, que por su naturaleza precisan de la rápida actuación del investigador), el Tribunal Supremo, ha considerado que el delito informático, de tracto mutante e itinerante, y que establece sus efectos en múltiples ubicaciones geográficas, se produce (y por lo tanto es competente) en todos y cada uno de los sitios donde se manifiestan sus efectos, lo que incluye tanto el lugar de la acción como el del resultado.

Esa opción por el llamado principio de la ubicuidad, se reflejó a partir del acuerdo no jurisdiccional del pleno del Tribunal Supremo de fecha 3/02/2005, según el cual:" el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa" Ello no implica más que una regla inicial muy operativa para la determinación de una eventual competencia instructora, porque, llegado el caso, si de la investigación se determina el lugar geográfico de comisión, porque se conociera el momento de la inclusión en la red de la información o comunicación origen de la causa –A TS 22/07/2002 y 19/01/2004 -(donde está el ordenador que contiene las pruebas del delito,

y desde el que se ha realizado la principal acción comisiva), cabe la inhibición a favor del Juez así determinado, ahora sí, conforme al general criterio del forum delicti comisi (art. 14 LECrim).

2.2.-LA UNIVERSALIDAD:

Decíamos igualmente que otra característica propia de los delitos informáticos es que generalmente traspasan las barreras geográficas de las realidades estatales e internacionalizan, o en el caso de Internet, universalizan, sus consecuencias.

Ello obliga a tener en cuenta ciertas reglas propias del Derecho Procesal Penal Internacional, de entre las que las más importantes afectan a la competencia, pues dada la multiplicidad de ubicaciones internacionales donde pueden hallarse los autores, las víctimas, o las pruebas de este tipo de delitos, principios fundamentales como el del derecho al juez predeterminado por la ley, o el de a un juicio justo ,obligan, ante todo, a prohibir la posibilidad del castigo por lo mismo en más de un ordenamiento jurídico distinto, , aún teniendo en cuenta incluso criterios respetabilísimos de soberanía, y a la interdicción del doble enjuiciamiento, evitando en todo caso el "bis in idem", lo que no supone, que mientras ello se dilucida, los Juzgados españoles no puedan investigar un delito que no haya sido enjuiciado en ningún otro país, procediendo la acumulación en fase posterior a favor del país que tenga mejor foro.
Dicho de forma resumida, primero es investigar, y lo último coordinarse para que el enjuiciamiento sea sólo uno.

2.3.-DELITOS MASA:

Por afectar a delitos difusos en que se suele atacar a múltiples víctimas desconocidas, ubicadas en distintos territorios de diferentes partidos judiciales, y aun de diferentes países (delitos masa), como hemos dicho, en muchos de ellos procederá la acumulación de delitos (art. 300 LECrim) para ser enjuiciados en una única causa que permita:
-evitar la *desaparición de pruebas* a que la investigación de un hecho atomizado suele llevar.
-por un lado aplicar las *agravaciones genéricas*, principalmente la aplicación del delito continuado –art. 74 CP-(v. gr: las múltiples diferentes estafas por importes a veces inferiores a los 400 euros de las estafas telefónicas o del phising)
-por otro para posibilitar *agravaciones específicas* (v. gr: estafa de especial gravedad en atención al valor de la defraudación del art.250.6 CP, actuación en pornografía infantil perteneciendo a asociación o agrupación delictiva del art. 189.3 e CP)
-y por otro para un correcto conocimiento de la dinámica comisiva del delito informático, que sólo se aprecia cuando aparece su reiteración sobre múltiples víctimas con un *modus operandi* delincuencial semejante, que entre otros extremos, nos permita confirmar que nos hallamos ante una actuación en grupo o una fuga de propiedad intelectual o industrial a favor de empresa de la competencia, o un intercambio organizado de pornografía infantil.

Lo anterior, además ,evita ciertos plazos cortos de prescripción en ciertos delitos con baja pena, y resuelve la competencia dentro de la conexidad delictiva (art. 17 LECrim) a favor del que primero conociere del asunto (art. 18.2 LECrim) , sin romper la continencia y unidad de la causa.

2.4.-INVESTIGACIÓN ACELERADA:

En otro orden de cosas y en lo que hace a la temporalidad delictiva, los informáticos, son delitos de pena no muy elevada (en torno a los tres años de privación de libertad máxima) y que por ello, prescriben con cierta rapidez.

Ello tiene incidencia no sólo en la *celeridad* a que obliga de por sí su persecución delictiva, sino repercusiones en cuanto a que para su investigación es precisa la urgente puesta en marcha de la misma.

- pues los *rastros y pistas técnicas* que dejan se desvanecen y difuminan enseguida,
- los *datos de tráfico* de las comunicaciones que encierran desaparecen con gran prontitud, pues la obligatoriedad de su conservación por parte de los ISPs no es igual en todos los países (en España , 12 meses de máximo, ex art. 12 Ley 34/2002 y en la Unión Europea , para el ámbito material de la Propuesta de Directiva que el Consejo de Ministros de Interior y Justicia de la UE aprobó el 21/02/2006, de entre 6 a 24 meses) y
- la otra gran dificultad, la de *averiguar la autoría* de quien se prevale de las técnicas informáticas para delinquir, igualmente cada vez que el tiempo avanza, se hace mayor.

  Además suele ser necesaria y habitual *la prueba pericial* (pantallazos, volcados de disco duro, análisis de los archivos, confección de la pericia en sí misma, etc) que tiende a alargarse en el tiempo, y que contribuye poco a la celeridad precisa en este tipo de investigaciones, razón por la que se suele encomendar judicialmente a los Organismos oficiales (Departamento de delitos Telemáticos de la Guardia Civil o Brigada de Investigación Tecnológica de la Policía judicial),quienes gozan, prima facie, de presunción de neutralidad e imparcialidad y que por contar con todas las garantías técnicas, siempre que se hagan por técnicos ingenieros o informáticos distintos de los que han hecho la intervención del material operativa, se tienen presuntivamente por veraces, salvo prueba en contra.

  Para garantizar la contradicción, (s TS 2/12/1992,5/02/1991 y 22/04/1991) la defensa puede proponer:
  - la oportuna contra pericia, en su caso,
  - la impugnación explícita en su escrito de calificación, lo que conllevaría examinar al perito en el plenario (s TS 5/09/1991,1/03/1994 y 1/02/1995)

  Caso de no optar por ninguna de estas dos líneas de defensa, los informes provenientes de organismos oficiales (igual que los análisis de drogas, huellas, balística, etc.), pueden ser traídos al proceso para ser valorados por el órgano fallador como prueba documental (s TS 1/03/1994 y 11/03/1994)

2.5.-INVESTIGACIÓN RESTRICTIVA DE DERECHOS FUNDAMENTALES:

Los ordenadores, que de común suelen estar en lugares cerrados (domicilios, empresas, Dependencias de la Administración, etc.) encierran información en forma de escritos, fotografías, filmaciones o sonidos y archivos que muchas veces desarrollan secretos y son puras manifestaciones de la *vida íntima y privada*, y a su vez sirven de vehículo de expendición y recepción de *comunicaciones* uni o multilaterales (correo-e, chats, foros, etc.) , cuya aprehensión o conocimiento afecta la esfera de privacidad que la ley reserva

al dominio de cada cual, y por ello, sólo pueden ser ingeridas, observadas o interceptadas con mandamiento judicial, si su titular no las permite, o no concurren situaciones de flagrancia delictiva (art. 553 LECrim)

Nos encontramos en la investigación de los delitos informáticos, como en pocos otros supuestos, ante el área de protección constitucional más sensible de los derechos fundamentales de la persona del investigado y por ello, dentro de la esfera de defensa más garantista posible , donde debe el Juez , como en ningún otro campo, preservar su imparcialidad y sólo permitir el avance de medidas tan intrusivas de la privacidad en la investigación, cuando la pulsión entre los intereses sociales y los individuales se decanten especialmente por los primeros.

Por la dinámica de la comisión y rastro probatorio que dejan, los delitos informáticos suelen acabar afectando tanto activa (en los de la víctima por parte del infractor) como pasivamente (en los del infractor por parte de la acción de la Justicia) bien el derecho a la protección de sus datos personales (art. 18.4 CE), bien los de a su intimidad personal y familiar y a la propia imagen (art. 18.1 CE) , bien al secreto de sus comunicaciones (art. 18.3 CE) o finalmente a su inviolabilidad domiciliaria (art. 18.2 CE).

So pena de nulidad probatoria cuando la obtención y consecución de prueba vulnere derechos fundamentales, (art. 11 LOPJ) y como garantía de la regularidad a la hora de conseguir la prueba que afecte a los mismos (art. 53 CE), cuando del investigado se trata, el legislador debe protegerlos bajo reserva legal y al ingerirlos, encomendarlos a la excepcional intervención razonada y proporcional del Juez (art. 18 CE).

Por eso, en la investigación de los delitos informáticos, ha de ponerse especial énfasis en que la *judicialización de la protección de los derechos de la privacidad* en que suele envolverse la actuación del investigado, revista todas las garantías y cautelas que hacen excepcional su ingerencia y que resumidamente son:

- la incoación del oportuno proceso judicial- que evita investigaciones genéricas o prospectivas (art. 558 LECrim) -,
- auto judicial razonado que explique hechos, sus tipificaciones jurídicas y sobre todo los indicios (no meras sospechas) que hacen imprescindible y proporcionado vulnerar alguno de los derechos de la privacidad del investigado para culminar la instrucción procesal
- una ejecución de la diligencia restrictiva de derechos -entrada y registro con ocupación de cuerpo delictivo, intervención u observación de comunicaciones privadas, etc – bajo la fé del secretario judicial, y con la participación, cuando sea posible del investigado
- un control final de la labor garantista judicial, que comienza por la notificación de la práctica de la diligencia restrictiva de derechos, y que se ejerce a través del oportuno sistema de recursos.

De entre todas las diligencias restrictivas de derechos fundamentales, la de *entrada y registro en lugar cerrado,* (donde de común se encuentran los ordenadores desde los que se comete la presunta acción delictiva) es la diligencia más usual a practicar en todos los supuestos de investigación de delitos informáticos, pues no en vano los ordenadores a través de los cuales se ejecutan suelen estar en lugares de esa naturaleza.

Sin embargo lo anterior no implica que en todo caso se ingiera y afecte a derechos fundamentales del investigado y por ello, no siempre procede su acuerdo o ingerencia judicial, y por lo tanto no todos los supuestos precisan de la necesidad de ejecutarse amparados en un mandamiento.

Se plantea la duda de si es necesario el mandamiento judicial en la entrada y registro que se haga en una empresa, despachos de profesionales amparados en el secreto o en dependencias de la Administración.

Para resolverla, hay que tener en cuenta que la diligencia de entrada y registro en lugar cerrado cuenta con la garantía de la intervención del Juez cuando en su interior se desarrolla vida privada.

Se suele entender que las *empresas*, al desarrollar actividades mercantiles, no son entornos lógicos de despliegue de vida íntima o familiar, por lo que en principio, para la entrada en empresas no es preciso mandamiento judicial.

Sin embargo, en los registros en delitos informáticos (espionaje empresarial, plagio, contra las propiedades industrial e intelectual, etc.), actos como la aprehensión de discos duros de ordenador o los vistazos a la pantalla del escritorio (pantallazos) o a las carpetas de archivos de los mismos, así como a la verificación de las últimas actuaciones hechas con el mismo, realizadas en el lugar sin presencia o bajo mandato judicial, pueden rozar la inmisión en la privacidad del usuario del ordenador ,y afectar a revelar datos de terceros que se relacionan con la empresa en aspectos no siempre mercantiles, por lo que lo aconsejable es que los funcionarios que registren acudan amparados en un mandamiento judicial basado en un auto que lo autorice e indique los delitos que se investigan y el objeto e indicios en que se fundan, ya por lo tanto dentro de una auténtica investigación judicial.

Dicho de otra forma, no es estrictamente necesario, salvo que conste el desarrollo en su interior de vida privada (lo que puede ocurrir en los despachos, zonas no abiertas al público, reservados, privados o trastiendas) pero sí aconsejable.

Es cierto que sobre los mismos registros en soportes más convencionales (como el papel y archivos de este material) tampoco es preciso el mandamiento si se trata de documentación estrictamente mercantil, pero, y en cualquier caso y soporte, los archivos y datos informatizados se deben registrar con las mismas garantías que los arts. 573 y ss LECrim establecen, lo que incluye la posibilidad de que esté presente el imputado o su representante (art.576, in fine y 569 LECrim), y ello salvo que el Juez acuerde la apertura o el registro en secreto, lo que no suele ser muy habitual en este tipo de procedimientos.

En lo que hace a los *despachos de profesiones liberales* no deberán ser entrados sin mandamiento judicial en aquellos casos en que sus profesiones se hallen amparadas por el secreto profesional (v. gr: despachos de abogados, periodistas, eclesiásticos, médicos, etc…), dado que como decimos, lo protegido bajo la garantía de la imparcialidad judicial son las intimidades que, en este caso, pueden ser conocidas por razones profesionales por los responsables de esas actividades.

Respecto del *registro de dependencias públicas* donde se ejerce la función pública a través de funcionarios (Ayuntamientos, Delegaciones, Consejerías, Ministerios, etc.), habituales lugares de custodia de datos íntimos ciudadanos recogidos a los solos efectos de posibilitar las funciones propias del Estado, igualmente es necesario el mandamiento judicial, que deberá ser notificado y cuyo registro deberá ser presenciado (art. 564 LECrim) por la Autoridad o Jefe de la dependencia registrada, o su superior , si se tratase de registro sobre aquel.

Por otra parte, los *elementos que convenga ocupar en un registro* por delitos informáticos dependen del tipo delictivo investigado.

En general, tras la realización del oportuno “pantallazo” sobre el que el secretario judicial dé fe, formando parte del contenido del acta, y cuya impresión puede adjuntarse para verificar los archivos obrantes con cargo al disco duro (art. 572 LECrim), procede realizar el volcado y copia del mismo y la aprehensión de los restantes archivos extraíbles en las distintas unidades de almacenamiento a analizar (en disquete, c-d, dvd, usb, etc.), procurando inspeccionar sólo lo conducente a la investigación en curso, hacerlo sin perjudicar e importunar a los interesados más de lo necesario y sin

comprometer su reputación y respetando los secretos que no interesen a la instrucción (art. 552 LECrim), debiendo devolver lo que no se relacione con la causa (art. 587 LECrim) lo más inmediatamente posible.

La aprehensión de los ordenadores, pantallas, impresoras, teclados y accesorios, sólo procede si se trata de una ocupación de material a efectos de garantizar la pena de decomiso o para garantizar las oportunas responsabilidades civiles que puedan derivarse del ilícito investigado, a través del correspondiente embargo.

Por otro lado, las concretas garantías judiciales necesarias para llegar al contenido de un ordenador ubicado en un domicilio privado se resumen exclusivamente el *auto de autorización de entrada y registro,* pues con él se permite lícitamente:

-la *entrada* en un lugar cerrado en que se desarrolle vida privada, aun contra la voluntad de su ocupante

-el *registro* de todas sus dependencias y pertenencias

-la *ocupación* de las conducentes y determinantes para la investigación de las supuestas infracciones perseguidas con la apertura y desprecinto de lo ocupado y el precintaje y ocupación de lo necesario y conducente a la investigación autorizada por el Juez

-las *comunicaciones pasadas y los documentos escritos, gráficos, o audiovisuales necesarios,* en cualquier tipo de soporte que se hallen.

Jurídicamente , la aprehensión bajo las instrucciones del secretario judicial y los comisionados policiales del Juez, se hace bajo la cobertura de la resolución judicial de entrada y registro que supone la autorización de la ocupación de cuantos cuerpos delictivos referidos a lo investigado se encuentren en el lugar cerrado, por lo que no es necesaria más cobertura judicial (s AP Cáceres 2º, de 17/06/2004) que en los casos de "hallazgos casuales", de objetos de otras infracciones delictivas heterogéneas, no relacionadas con las autorizadas en el auto, y que dan lugar a que, avisado el Juez , se complementen con una nueva autorización, en su caso.

Finalmente, para la apertura de comunicaciones no conocidas, y por ello ignoradas por el destinatario, salvo secreto del sumario, se deberá contar con la presencia del imputado, si no está en ignorado paradero y quiere venir a conocerlas.

Para esta diligencia, nuevamente, es precisa la presencia judicial (art. 576 LECrim)

El resto de garantías procesales se consiguen con la neutral intervención del fedatario público que es el secretario judicial y con la presencia del imputado o quien le represente al momento de hacer la entrada y registro (y no de su letrado), y en su caso los testigos, para hacer posible la contradicción, que posibilite la defensa.

Por otro lado, como la apertura de archivos del disco duro o de unidades externas (disquetes, cds, usbs, etc.) no es correspondencia privada detenida, y como cualquier otro archivo en soporte convencional (en papel, fotografías, grabaciones, filmaciones, etc.), simplemente constituye el cuerpo de los delitos informáticos, no es necesario hacerla a presencia judicial , por lo que (art. 334 LECrim y ss) puede hacerla la policía en presencia del imputado y del secretario judicial, o de testigos en su caso, sin necesidad de acudir al Juez, para acompañarle los de contenido delictivo, como tal cuerpo del delito, junto con el atestado, en su caso.

Sólo si se tratara de correspondencia (v.gr: correos-electrónicos) no abierta e ignorada por el imputado, es de aplicación la obligatoriedad de ser citado para darle la oportunidad a él o a quien le represente, de presenciar su apertura ante el Juez (art. 584 LECrim) y en ese caso no lo pueden abrir por su cuenta para su estudio las Fuerzas y Cuerpos policiales u otros comisionados judiciales, al tratarse de una diligencia de estricta naturaleza judicial.

En todos los demás casos la correspondencia ya abierta, por conocida y pasada por parte del investigado, deja de serlo a los efectos del título VIII del Libro II de la LECrim, y se

transforma en mera prueba documental –contenga o no información íntima.-que puede perfectamente aprehenderse tras su visionado en el lugar del registro (pues es en el auto que lo autoriza donde se ha ponderado y admitido su ingerencia) o posterior estudio en dependencias policiales por los comisionados del juez ordenante del registro.

Otra de las excepciones, o mejor puntualizaciones, se halla en el tratamiento procesal de *los "hallazgos casuales"*.

Cuando el Juez en su mandamiento autoriza la entrada y registro (o la ingerencia de las comunicaciones) para la investigación de un determinado tipo delictivo (se busca pornografía infantil, por ejemplo), y en el curso de su ejecución, aparecen evidencias de la comisión de otro u otros entre los que no hay homogeneidad delictiva (principio de especialidad) –en el sentido del art. 553.1 LECrim de "guardar relación con el delito perseguido"- , (se descubre la tenencia ilícita de un arma) por la flagrancia patente (sTS 4/10/1996 y 4/03/2003) y por la regla de la conexidad de los arts 17.5 y 300 LECrim , y al no haber "novación" del objeto de la investigación, sino simplemente "adición" ,debe procederse evitando la continuación de la existencia del nuevo delito hasta entonces ignorado, pero la ocupación debe interrumpirse también , ponerse en comunicación de la autoridad judicial ordenante , y en su caso, conseguir de ella un complemento de mandamiento razonado, que puede ordenarse de forma oral, s TS 3 /07/2003 (que debe unirse de forma razonada a autos con posterioridad) para proceder también contra el delito casualmente descubierto y con ello conseguir que la aprehensión del "hallazgo casual" tenga la cobertura necesaria de la garantía constitucional que supone la intervención judicial .

Como señala la s TS 29/12/1997 "el descubrimiento casual de indicios de otro delito distinto del investigado durante un registro domiciliario o una intervención telefónica no implica vulneración de los derechos fundamentales garantizados por el art. 18 CE, siempre que se cumpla el requisito de proporcionalidad y que la autorización y práctica del registro o de la intervención se ajusten plenamente a las exigencias y prevenciones legales y constitucionales" (s TC 24/02/1998 y s TS 18/02/1994, 28/04/1995, 7/07/1995,1/12/1995,4/10/1996 , 26/09/1997 ,30/03/1998, 1/02/1999 ,21/07/2000 y 21/01/2005).

La LECrim, con no prohibirlo (s TS 12/12/2000), parece ordenarlo de la nota consustancial de la flagrancia, pues como establece la s TS 3/07/2003, que específicamente se dedica al análisis de los "hallazgos casuales", los mismos "se instalan en la nota de flagrancia por lo que producida tal situación la inmediata recogida de los mismos no es sino consecuencia de la norma general contenida en el art. 286 de la Ley procesal ".

Todo lo contrario a lo que ocurrirá (y será invalidada) cuando se trate de usar medidas restrictivas interpuestas con el espurio fin de aparentar un descubrimiento que a priori se sabe " no casual", pues el ordenamiento jurídico no puede prestar protección a las conductas que tratan de violentar los derechos y libertades fundamentales (art. 11.1 LOPJ) y además , estas deben ser declaradas nulas para al mismo tiempo ejercer un efecto disuasor de conductas torticeras, espurias, no éticas y prohibidas por anticonstitucionales en los agentes encargados de la investigación criminal.

En este sentido, la s TS 3/07/2003 indica que "tan sólo si se advirtiera que todo ello pueda responder, en realidad, a un designio intencionado de los funcionarios solicitantes del registro que fraudulentamente hubieran ocultado al juez autorizante ,por las razones que fueren ,el verdadero motivo de su investigación ,la violación del domicilio habría de ser considerada nula".

Por otra parte, como a través del ordenador igualmente pueden realizarse *comunicaciones privadas,* es igualmente posible ingerirlas en el curso de una investigación judicial, pero por afectar al secreto de las mismas (art. 18.3 CE) su ejecución se rige por los mandatos constitucionales y se complementa por las normas de apertura de la correspondencia privada (arts. 584 y ss. LECrim) si la correspondencia, ya pasada, (principalmente correos electrónicos o archivos intercambiados) no ha sido abierta y es por ende ignorada por su destinatario, y por la de la intervención de las comunicaciones (arts 579 LECrim), si se trata de conocerlas a la vez que se van produciendo.

Todo lo demás, incluidas las comunicaciones ya pasadas, guardadas o no borradas por su destinatario, son prueba documental, cuerpo del delito, en su caso, que se aprehenden conforme las normas de detención de la correspondencia ya abierta (arts. 574 y ss LECrim)

Por otro lado, y por su frecuencia se plantea el problema de la necesidad o no de *mandamiento judicial para las intervenciones en cybercafés.*

En principio, como los Cybercafés no dejan de ser establecimientos públicos, no es necesario el mandamiento judicial para su entrada y registro, salvo que se pretenda en zonas donde, dentro de él, se desarrolle vida privada (reservados, despachos, etc),

Por el contrario, las comunicaciones que los usuarios, sus clientes, realizan en ellos son todas privadas, y por ello, para la interceptación e intervención de su contenido siempre será necesario mandamiento judicial, en el curso de una investigación que por ello se halle judicializada, y que por lo tanto no puede ser prospectiva.

Por otro lado, acudir a un Cybercafé y, desde un ordenador, observar sin mandamiento judicial, lo que se transmite desde otro ordenador, según un sector de la doctrina supone una vulneración del derecho al secreto de las comunicaciones del espiado, y por ello opinan que la información así obtenida, es nula jurídicamente.

Así, la s AP 3ª Asturias de 29/11/2004 establece que observar las comunicaciones ajenas es una facultad que sólo corresponde al instructor judicial en el marco de un procedimiento penal abierto, y que por ello, se vulnera el derecho al secreto de las comunicaciones y constituye prueba prohibida la conseguida por detectives privados que ,siguiendo al sospechoso hasta un cybercafé, se sitúan en el ordenador contiguo y mirando por encima del hombro lo que escribía en su pantalla el investigado, le observan el nombre de usuario, el del destinatario y cómo envía cierta cantidad de correos electrónicos de contenido injurioso contra personas de la empresa en la que él resultó ser sindicalista.

Según esta teoría el acceso por la vía descrita a datos que identifican el autor de la remisión de los correos electrónicos injuriosos, “se encuentra protegido por el secreto a las comunicaciones, y llevada a efecto en la forma reseñada, sustrayendo la intervención judicial, implica una obtención inconstitucional de la prueba pretendida”, pues para la AP 3ª Asturias, “el concepto de secreto que aparece protegido en el art. 18.3 CE , no cubre sólo el contenido de la comunicación , sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales” y cita en su apoyo la s TEDH 2/08/1984 , caso Malone, que da por violado el art.8 CEDH por el uso de la técnica “comptage” que es el empleo de un artificio técnico que permite registrar cuáles han sido los números telefónicos marcados sobre un determinado aparato, sin conocimiento del contenido de las conversaciones efectuadas -lo que se dice un auténtico mero dato de tráfico-.

Sin embargo, no sólo por la antigüedad y el contexto en que se dictó tal sentencia, sino por su fondo también, no podemos compartir el criterio indicado -muy discutible-en cualquier contexto comunicativo ,por cuanto la identidad del comunicante hecha en

lugares públicos como cybercafés no es un dato protegido , mientras que sí lo es el contenido en sí mismo, y la prueba evidente es que basta con mirar por encima del hombro –algo que ni es subrepticio, ni sofisticado ni ingerente, pues no necesita de la intermediación de ningún instrumento distinto a la vista , propiamente dicha -para saber la identidad subjetiva del autor de la comunicación , que bien pudo entrar a valorarse como prueba testifical no prohibida en el caso de autos, ya que la protección del derecho a la intimidad debe valorarse en cada caso concreto en función de la efectiva y objetiva protección que su titular da a la reserva de los extremos de su comunicación y al contenido de la misma.

De lo contrario, en los seguimientos policiales en que se revela con quién se comunica oralmente una persona vigilada , cuando lo hace en lugares públicos, constituiría la prueba prohibida que no compartimos concurra en los casos de observación de la identidad subjetiva de los comunicantes , cuando las comunicaciones ocurren en espacios no privados.

Por eso, los datos de tráfico, adjetivos al contenido de la comunicación, únicamente tendrán la misma protección que el contenido comunicado en sí mismo considerado, cuando la protección y reserva que les dispense su titular sean cruciales, determinantes en sí mismos y de tanta intensidad como el dispensado a aquel, y obviamente, no es indiferente el lugar desde donde se comunica, público o privado, pues es uno de los principales indicativos objetivos para fijar en el caso concreto este criterio de extensión del concepto de “intimidad “ o “privacidad”- (¿privacidad en espacios no privados por ser públicos?)-

En otro orden de cosas se plantea el problema jurídico de si existen o no *comunicaciones secretas en el seno de las relaciones familiares efectivas,* (principalmente entre esposos y padres e hijos).

Nuestro sistema constitucional parece optar por una concepción individualista, de modo y manera que los derechos fundamentales de la persona se le conceden a esta por el mero hecho de serlo y no en consideración a su pertenencia a grupos (matrimonio, familia, etc.) que igualmente cuentan con protección constitucional.

Por ello, las conversaciones y comunicaciones que un cónyuge tenga con terceras personas, no pueden ser injeridas lícitamente por el otro esposo, sin consentimiento de este, y si se hace la intromisión es ilícita, y su uso como prueba debe estar prohibido (art. 11.1 in fine LOPJ), además de ser delictivas por atacar el art. 197 CP (s TS 20/06/2003)

Lo mismo ocurre respecto de las comunicaciones privadas de los descendientes o ascendientes o familiares de quien las observa sin su autorización o consentimiento, con independencia de quién sea el titular del medio de telecomunicación a través del cual las conversaciones injeridas tengan lugar, y por lo tanto de quien las costee (que puede tener su importancia a la hora de prohibirlas, pero no es disculpa para injerirlas).

Sólo en los supuestos de personas o familiares dependientes, singularmente menores de edad o enfermos psíquicos, y constando motivo legítimo (deber de corrección, defensa del crecimiento equilibrado del menor, evitación de abusos en su contra, evitar la captación por una secta, etc.), podría entenderse legitimada la observación de comunicaciones privadas.

Finalmente, se plantea el problema de si hace falta o no mandamiento judicial para la *observación de los datos de tráfico de las comunicaciones privadas*, o exclusivamente y sólo para el conocimiento de su contenido

En el ámbito de la interferencia de los meros datos en las comunicaciones por soportes tradicionales como el papel, la información no protegida, como pueda ser la persona y dirección a que se remite la carta o el conocimiento de la fecha en que ha llegado a su

destino, es decir de los datos adláteres, adjetivos o no de fondo y contenido de las comunicaciones privadas, se han considerado informaciones no susceptibles del amparo judicial (v. gr: cartero o portero que informa a la policía de la fecha y destinatario y remitente de una carta que ha tenido que repartir), por lo que con más razón, dada la multitud de comunicaciones electrónicas que se practican actualmente, en principio tampoco los llamados datos de tráfico de estas (número o clave identificadora, aparato emisor, receptor, titulares de los mismos , duración y fecha y hora de establecimiento y fin de la comunicación, localización física o destino del usuario , etc.) , deben conseguirse bajo el amparo de un mandamiento judicial y su correspondiente auto razonado, porque si bien es cierto que la información que desprenden los datos de tráfico , bien estructurada, puede arrojar información susceptible sobre el investigado, no lo es menos que la policía siempre ha contado con registros a esos solos fines de investigación criminal y de protección ciudadana (principalmente el DNI, los antecedentes policiales, etc.), y el hecho de que ahora los datos de telecomunicaciones los custodien empresas privadas , no es óbice para que sólo a la policía, por escrito y a esos efectos, se pueda dar la información sobre los datos de tráfico, tan numerosos ,y conducentes a centrar la investigación y autoría definitiva, que el contenido (con intervención judicial) , puede además probar o esclarecer.

La protección que dispensa la Constitución en su art. 18.3 a las comunicaciones privadas, y la limitación expresa a que se refiere el art. 18.4 sobre el uso de la Informática ,como reservada a la ley , deben entenderse referidas exclusivamente a los datos principales , sustantivos o de contenido y no a los de tráfico.

Así se interpreta en algunos países expresamente (v. gr: República Dominicana)
Sin embargo, y como decíamos supra respecto de las entradas y registros en empresas, aunque no es obligatorio, es aconsejable para forzar la intervención judicial, el nacimiento de un proceso penal y la propia garantía de neutralidad que es en sí la propia jurisdicción.

En contra, no obstante, se posiciona la doctrina de la Consulta de la Fiscalía General del Estado 1/1999, de 22 de enero, sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones, según la cual, todas las comunicaciones, y en especial las postales, telegráficas, y telefónicas son secretas, salvo resolución judicial, por así deducirse de los arts. 18.3 CE y 8.1 del CEDH que declara el derecho de toda persona al respeto de su correspondencia y con cita de la jurisprudencia del TEDH en los casos Amman, Malone y Dugdeon, se centra en la s TEDH 30/07/1998, caso Valenzuela Contreras, cuando califica como ingerencia de la autoridad pública en el ejercicio del derecho al respeto de la vida privada y de la correspondencia, el registro mediante aparato contador de los números de teléfono marcados desde un determinado aparato, aun cuando este tipo de vigilancia no implique acceso al contenido de la conversación, ya que desde la perspectiva de los derechos fundamentales, lo inviolable no sólo es el mensaje, sino todos aquellos datos relativos a la comunicación que permitan identificar a los interlocutores o corresponsales o constatar la existencia misma de la comunicación, su data, duración, y todas las demás circunstancias concurrentes, útiles para ubicar en el espacio y en el tiempo el hecho concreto de la conexión., lo que supone en definitiva que no cabe disociar sin merma relevante de garantías , realidades tan sustancialmente integradas como son el mensaje y su proceso de transmisión.

Sin embargo no podemos compartir esta obsoleta doctrina, primero, porque el derecho a la intimidad se debe graduar en función de lo que es lo íntimo (no se puede proteger igual el contenido que su vía de transmisión en todo caso), y en segundo lugar, de la protección concreta que hace su titular del mismo, que no es idéntica si se hace en lugares públicos , al acceso libre de la ajena discreción , que en privados ,y que sólo

afectará a los datos de tráfico si los considera tan esenciales al secreto y los protege con la misma intensidad que el propio contenido, de lo contrario se puede llegar al absurdo de proteger el contenido de las comunicaciones escritas más que las orales en función de la peculiaridad de sus modos de transmisión y no de dónde y cómo hayan sido transmitidas.

2.6.-DIFICULTADES PARA APRECIAR LA AUTORÍA DELICTIVA:

Si hay alguna característica singular de la delincuencia informática, más que la de su sofisticación tecnológica, es la de que el infractor suele ser un delincuente cobarde, que "tira la piedra y esconde la mano", actuando casi sin riesgo y a distancia, utilizando bien *técnicas humanas de anonimato* mediante las correspondientes suplantaciones de la personalidad, uso de "nicks" o apodos, delinquiendo desde cybercafés , cyberuniversidades , blogs, foros, chats, etc, o *técnicas propiamente dichas que la Informática enseña* y que prácticamente hacen anónima su utilización , como pueden ser los proxys, anonimizadores Web, servidores de correo Web, remailers, dialers, o técnicas de por sí delictivas como cierto tipo de malware, como los Keyloggers.

La determinación de la autoría concreta del real infractor en los supuestos del uso de técnicas de ingeniería social o informática anonimizadoras , y en su caso , en los supuestos de uso compartido del ordenador, no es diferente en las investigaciones por delitos informáticos que en las de delitos tradicionales, pudiendo utilizarse cualesquiera medios de prueba legalmente admitidos, empezando por los que aporta la propia técnica como instrumento al servicio de la investigación procesal misma.

Y si no fuese posible mediante la oportuna prueba técnica pericial para la detección de las señas IP del usuario o el rastreo de las cuentas bancarias asociadas o por la documental , y el conocimiento de la clave de usuario y contraseña de cada cual pudiese ser conocida por terceros, cabe la determinación de la convicción judicial por la testifical (uso del ordenador por el inculpado en exclusiva ,utilización de apodos , seudónimos o "nicks" , descartes de la coartada indicada por el imputado , testimonio no espurio del co-imputado , etc.), confesión del inculpado e incluso por determinación indiciaria siempre que convincentemente se razone (v. gr: analizando a quién le llega el dinero, quién tiene un móvil espurio, a quién le beneficia, los conocimientos informáticos del inculpado ,demostrando la mentira de la declaración del imputado , probando que no es posible la infiltración en el uso del ordenador por terceras personas , no dando el acusado explicación satisfactoria de la posesión (s AP 2ª Madrid de 6/05/2004) etc.)

En la consecución probatoria es crucial el papel de las *empresas de telecomunicaciones y servidoras de Internet (ISPs)* que deben colaborar con la Justicia rápida, leal y eficazmente y que deben tratar de compatibilizar el desarrollo de la legítima libertad de expresión, comercio, conocimientos y comunicación que potencia Internet a través de sus múltiples mecanismos y posibilidades, y en lo que se basa principalmente su negocio, con la exclusión de ellos, sin embargo, del mayor número de contenidos ilícitos posible.

Como las empresas dedicadas a la provisión de contenidos en Internet no los pueden controlar (pues meramente juegan el papel técnico de ser intermediarios de la circulación de información), y sería exacerbado imponerles su vigilancia, se les ha exigido (art. 11 Ley 34/2002) un carácter de *custodia pasiva*, de modo y manera que responderán penalmente, en su caso, no por no haber detectado en sus páginas la

existencia de contenidos ilícitos, sino si una vez hecho, notificado , ordenado o sabido, estos no los retiran (comisión por omisión) , además de en los supuestos en que ellos sean los propios creadores directos o cooperadores necesarios en la difusión del contenido ilícito o asuman el papel de moderadores o gestores responsables , por ejemplo de foros de debate.

No le son de aplicación los criterios de autoría en cascada fijados en el art. 30 CP para los delitos de difusión mecánica, pues amén de parecer pensados para la prensa, son más delitos, los informáticos, de difusión telemática y, en cualquier caso, la capacidad de control sobre la introducción de contenidos presuntamente ilícitos en el proveedor es inexistente.

Vulneraría el principio de culpabilidad hacer recaer responsabilidad penal en los prestadores de servicio y proveedores de Internet, pues ellos no originan, ni modifican, ni seleccionan, ni destinan información de contenido ilícito en el hecho de acceder o transmitir la que hayan hecho sus usuarios, y no tienen sobre los mismos, mientras dure esta ignorancia, ningún poder de dirección, autoridad o control.

2.7 ESCASO DESPLIEGUE NORMATIVO ESPECFICO:

Finalmente acabar indicando que en España, todavía la delincuencia informática encuentra espacios de impunidad, que suman a la posible ineficacia de medios policiales y judiciales, un escaso despliegue normativo de instrumentos que no se entiende por qué no se desarrollan, como es el hecho paradigmático de no haber ratificado España el Convenio del Cybercrimen del Consejo de Europa, o no haber desarrollado reglamentariamente la Ley 3472002, de 11 de julio, de Servicios de la Sociedad de la Información, creando, por ejemplo, procedimientos monitorios para la retirada de contenidos nocivos y/o delictivos sin autor de Internet, tanto para los supuestos de simple denuncia como para aquellos en que por haber oposición, necesariamente hayan de dirimirse en algún procedimiento judicial acelerado en la vía penal o en la contenciosa, o , yendo más allá, complementando el actual Código Penal, contemplando como delitos, realidades ahora atípicas, (la suplantación informática e inconsentida de personalidades ajenas, el acoso informático que bloquee o empeore el normal uso de la Informática y sus comunicaciones, etc) o modalidades complejas como el phising o el sabotaje informático para reducir sus problemas concursales.