# REFLEXIONES SOBRE CIBERDELINCUENCIA Y REDES SOCIALES DIGITALES

# CYBER CRIME AND DIGITAL NETWORKS REFLECTIONS

**MANUEL OLLÉ SESÉ**[1]



Summary: I. SOCIAL NETWORKS: FROM THE EXCLUSIVE HUMAN FACTOR TO THE (IN ADDITION) IMPERSONAL AND DANGEROUS TECHNICAL FACTOR. II. PROBLEMS FROM THE PERSPECTIVE OF CRIMINAL LAW. III. SOME SPECIFIC CONDUCTS: 1. IDENTITY THEFT OR PERSONALITY USURPATION. 2. PHISHING. 3. CYBERBULLYING.

## I. REDES SOCIALES: DEL EXCLUSIVO FACTOR HUMANO AL, ADEMÁS, IMPERSONAL Y PELIGROSO FACTOR TÉCNICO

Las redes sociales no es un fenómeno aparecido en los últimos años. Las redes sociales *digitales*, sí. Desde siempre, hemos creado y formado parte de redes sociales en el que el factor fundamental, por no decir exclusivo, era la persona humana en sí misma considerada, que participaba físicamente presente en las actividades de un grupo humano mínimamente organizado. En aquel entonces, e incuso hoy, lejos de denominarlas redes sociales, las tildábamos, entre muchos ejemplos, como tertulias, de amigos o de profesionales, reuniones, asambleas, clubes, círculos recreativos, casinos, agrupaciones profesionales, grupos de trabajo o guateques.

Estos vínculos esencialmente personales demuestran que el fenómeno de las redes sociales humanas no es un invento de la tecnología sino que la humanidad, desde el mismo momento de su existencia, ha gozado de las habilidades necesarias para satisfacer sus necesidades de relación o interrelación, de sociabilidad, de intercambio presencial de información y de alcanzar objetivos e intereses comunes de ocio o profesionales.

Estas redes humanas y sociales, ajenas a las nuevas tecnologías, han estado presididas por la idea de la confianza recíproca entre los miembros del grupo, en el que las personas que lo integran, por lo general, son todos conocidos y todos generan y comparten información, desde la amistad o compañerismo y bajo el paraguas de la

[1] Profesor de Derecho penal de la Universidad Complutense de Madrid y Abogado.

intimidad o de confidencia de aquellos datos que no pueden superar los muros propios que delimita ese círculo social.

Esta idea y no otra, este factor humano y no otro, es el que preside también, desde la vertiginosa evolución de las nuevas tecnologías, las redes sociales *digitales*, sin embargo a ese elemento personal o humano, ahora, se añade otro material: "lo digital", esto es, la sustitución presencial y física de los miembros de la red por la presencia "virtual" a través de internet, gracias a las empresas que facilitan los llamados servicios de redes sociales. Estos grupos o grandes comunidades digitales gozan de las características citadas para los no digitales, con la única diferencia de que las relaciones del grupo se desarrollan en la red y a través de internet. Se sustituye la presencia física y palpable de nuestros compañeros de red, por la presencia virtual.

En la primera, todos los componentes del grupo nos olemos, nos oímos y nos palpamos en un mismo local de cemento y ladrillos o en un espacio natural. En la virtual nos leemos, en el mejor de los casos nos vemos y oímos a través de un dispositivo, pero ni nos olemos ni nos palpamos y los muros de la intimidad, de la confidencia, y del riesgo de no ser objeto de un designio criminal están en constante riesgo de desvanecerse.

## II. PROBLEMÁTICA DESDE LA PERSPECTIVA DEL DERECHO PENAL

Las redes sociales digitales ofrecen indudables ventajas y bondades para los usuarios de los mismos, como, por ejemplo, la obtención y compartición de información para la diversión o para el trabajo. Sin embargo, las peculiaridades propias de lo digital llevan en ocasiones a lamentables consecuencias, convirtiéndose en un instrumento para la comisión de diferentes delitos.

La criminalidad de antaño propia del viejo ladrón de gallinas ha experimentado en y con las redes sociales nuevos problemas delincuenciales, de difícil solución en ocasiones. Por un lado, internamente, los propios miembros de las comunidades digitales utilizan éstas para vulnerar derechos constitucionales de terceros, como pueden ser el derecho al honor, a la intimidad o a la imagen. La calumnia, la injuria o la revelación de secretos son delitos de frecuente comisión por parte de usuarios de las redes sociales digitales, a los que se añaden, igualmente otros ilícitos penales como, y sin ánimo exhaustivo, las amenazas, coacciones o la difusión de pornografía infantil. Nuestro Código penal no es precisamente ejemplo de tipificación de este tipo de conductas cometidas a través de internet. La ausencia de tipos específicos y la sujeción al principio de legalidad impiden en ocasiones la persecución penal de estos hechos. Y, por otro lado, externamente, la ciberdelincuencia, que evoluciona al mismo ritmo que las nuevas tecnologías, se vale de estas plataformas universales, como herramientas necesarias, para la comisión delictiva[2].

[2] Véase un amplio estudio de sobre este tipo de delincuencia en E. VELASCO NUÑEZ, *Delitos cometidos a través de internet,* La Ley, Madrid, 2010.

Por ejemplo, según los datos del informe del Instituto Nacional de Tecnologías de la Comunicación (en adelante, INTECO[3]) de 2012 sobre el fraude a través de internet, en España, durante el primer cuatrimestre del año 2012, se produjeron dos ataques importantes. Uno basado en la imagen de la Agencia Tributaria con el siguiente mensaje: "después de los cálculos anuales pasados de su actividad fiscal hemos determinado que usted es elegible para recibir un reembolso de impuestos de 223,56 Euros". Si la víctima visitaba el enlace, era conducido a una supuesta web donde se le solicitaban los datos bancarios. Este mensaje tuvo una alta difusión durante los meses de febrero a abril de 2012. Y el otro fue el conocido como "virus de la policía", en el que en nombre de la Policía Nacional, se han infectado los equipos de los receptores. La tasa de infección de este virus fue muy elevada.

Precisamente la protección de estos derechos de los usuarios de los sistemas de internet, ha llevado a la Sala Segunda del Tribunal Supremo, de forma innovadora, a ampliar la protección penal a lo que ha denominado el derecho al *entorno digital*. La interesante sentencia 342/20013, de 17 de abril, lo interpreta desde "la multifuncionalidad de los datos que se almacenan" en un dispositivo, y establece que el derecho al entorno digital "se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos". Añade la cita sentencia del Tribunal Supremo que "incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria" porque "existe un derecho al propio entorno virtual".

La indicada delincuencia informática aprovecha las fisuras propias de estas comunidades digitales, como la negligencia de los propios usuarios a la hora de registrase y crear sus propios perfiles digitales, normalmente al aceptar alegremente todos y cada uno de los términos de esa compañía digital que les va servir de soporte para su interrelación grupal. También, la despreocupación de los usuarios en el *modus operandi* de sus servicios técnicos y deficientes medidas de vigilancia que evidencian gritas de seguridad coadyuva a la comisión delictiva.

La aportación masiva de datos por los interesados es otro factor de elevado riesgo, al salir los mismos de su esfera de control. La información de todo tipo que por parte de los usuarios se pone a disposición de un grupo determinado, bajo un teórico principio de confianza, muchas veces ingenuo, puede quebrarse al circular la información *colgada* por ese espejo público *on line* de fácil acceso para terceros ajenos ase grupo inicialmente cerrado y no abierto, lo que facilita el acceso a datos e informaciones que son expuestas por el usuario. Y la no menos preocupante presencia de menores en las redes sociales digitales con la consiguiente vulnerabilidad en la que

[3] Véase http://www.inteco.es/

se auto exponen, igualmente se convierte en otro elemento de desconfianza hacia las redes digitales.

Las conductas negligentes deben valorarse también en su justo término a lo hora de determinar la existencia o no de hechos con relevancia penal y determinar, consecuentemente, y en su caso, el reproche penal, de acuerdo con la estructura de la teoría del delito, tomando como elementos valorables, por un lado, las condiciones personales del sujeto vulnerado en sus derechos, como su edad, situación, cultura, posible déficit intelectual; y, por otro lado, la medidas de diligencia y autoprotección que ese usurario adoptó como factor de defensa ante las debilidades técnicas de la red. Al usuario le deben ser exigibles, al menos, mínimas medidas de diligencia en su aventura informática.

Es notorio que el usurario que introduce datos en al red debe ser consciente de las consecuencias positivas y negativas que le puede acarrear esa publicación, de la cómoda accesibilidad a la que pueden acceder terceros propios o ajenos a ese grupo virtual y, desde luego, y muy especialmente, de la fragilidad técnica de los servicios informáticos.

En el ámbito de la *ciberdelincuencia* el uso por parte de estos criminales cibernéticos de programas *malaware* y de virus informáticos convierten hábilmente a los usuarios digitales en víctimas de aquéllos. La técnica se maneja y desarrolla por personas que también, en ocasiones, anidan motivaciones malignas que se ponen al servicio no del bien común y del leal desarrollo tecnológico sino de la maldad, del crimen.

En el ámbito de la investigación criminal, la averiguación de los responsables de estas conductas no es especialmente fácil, sino todo lo contrario. A pesar de los grupos especializados existentes en los cuerpos y fuerzas de seguridad, estatales y autonómicos, incluso hasta municipales en algunas capitales españolas, la investigación de este tipo de delincuencia no suele ser efectiva por diferentes factores.

Entre otros elementos distorsionadores de este tipo de investigación se pueden evidencias los siguientes: las dificultades en determinar la jurisdicción y competencia de los tribunales cuando los hechos, por ejemplo, se cometen desde diferentes países. Los obstáculos que se presentan en la necesaria cooperación judicial internacional en materia penal[4]. La ausencia de legislaciones uniformes respecto de los tipos penales relacionados con la ciberdelincuencia. La desaparición de datos en la red y en ordenadores o la imposibilidad legal de obtención de los mismos por el transcurso del tiempo[5]. La coautoría o coparticipación de pluralidad de personas operando en varios

[4] *Vid.* por ejemplo el Convenio sobre la Ciberdelicuencia de 23 de noviembre de 2001, que fue ratificado por España el 20 de mayo de 2010 (BOE núm. 226, de 17 de septiembre de 2010).

[5] En España, por ejemplo, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, establece en el artículo 5 que "La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación".

lugares geográficos nacionales y/o internacionales. Y las facilidades para cometer el crimen desde el anonimato que facilita la red y el hecho de poder conservar esa invisibilidad indefinidamente.

## III. ALGUNAS CONDUCTAS CONCRETAS

Las amenazas cibernéticas se han multiplicado en los últimos años y últimamente presentan un elevado grado de sofisticación provocado por el mayor conocimiento de los cibernautas y por el uso masivo de las redes sociales que propician el alimento necesario para el ciberdelincuente. Algunas de estas conductas a las que me voy a referir, entre otras, son: la suplantación o usurpación de identidad, el *phising* y el *ciberbullying*.

### 1. La suplantación o usurpación de identidad

La suplantación de identidad es un fenómeno que ha experimentado un aumento importante en los últimos tiempos. Las compañías distribuidoras de los servicios de internet facilitan esta práctica ante la inexigencia de requisitos a la hora de registrar un perfil en la red que permita identificar fielmente quién es ese usuario. Un simple ejemplo que se ofrece todos los días facilita la comprensión: Pablo y Gonzalo crean un perfil falso en Google suplantando a su amigo Carlos con la finalidad de injuriar a Manuel y a una organización a la que este pertenece.

La dinámica comisiva para los sujetos activos del ilícito es perfecta: suplantan la personalidad de Carlos, mediante la creación de un perfil falso en Google, lo que contribuye a mantener el anonimato. Desde un lugar público, como es un cibercafé o locutorio, remiten diferentes emails a múltiples destinatarios para injuriar a Manuel y la organización a la que pertenece. De esta forma, además, Pablo y Gonzalo se garantizan que no se serán descubiertos al ser tanto el ordenador, como la IP[6] desde la que se han lanzado esos emails, de un establecimiento público (cibercafé o locutorio).

En cualquier caso, siempre que se pueda determinar la autoría de estas acciones, lo que no siempre será factible, en principio, la conducta se subsumiría en el artículo 401 del Código penal -y más allá de la interesante discusión entre los conceptos de usurpación y suplantación de identidad- como delito de usurpación del estado civil o incluso de un delito de revelación de secretos del artículo 197 del Código penal según el supuesto concreto que se plantee. Desde luego, lo deseable es que este ilícito tuviera una precisa tipificación en el ámbito penal que ofreciera la imprescindible seguridad jurídica.

[6] *Internet Protocol.*

## 2. El *phising*

La nueva categoría de amenazas producidas a través de internet se denomina APTs (*Advanced Persistent Threats*) o Amenazas Persistentes y Avanzadas[7]. Estos ataques normalmente comienzan con la recopilación y obtención ilegal de la información del objetivo -a través de redes sociales como *Facebook, Twitter* o *Linkedln* o correo electrónico, entre otros muchos- para introducirse en la red. Para ello utilizan técnicas de ingeniería social[8]. Una de ellas es la conocida como *phishing*, técnica por la que los ciberdelincuentes se aseguran una comunicación continua con los equipos de las víctimas, instalando un malware o software malicioso que puede permanecer oculto durante días sin ser detectado. Este malware explora a través de la red los equipos que almacenan información sensible y, de este modo, y por medio de diversas técnicas, obtiene las credenciales de los usuarios y sus claves.

Según el citado informe sobre detección de APTs de 2013 del INTECO, la forma más común de estos ataques dirigidos es el *Phishing.* Consiste en el envío de correos electrónicos donde el remitente suplanta la identidad de alguna entidad o persona conocida por la víctima. En este tipo de ataque, el correo suele llevar incorporado un enlace a un sitio malicioso para que la víctima lo visite, comprometiendo de este modo el equipo desde el que se conecta. En otros casos, en el email remitido se adjunta un archivo malicioso que infecta el equipo al ser abierto.

Los correos electrónicos enviados tienen una imagen familiar para la víctima: suelen provenir "aparentemente" de una entidad financiera u otro tipo de organización fácilmente identificable para el destinatario del correo. En el texto de dichos correos, por lo general, se explica que, por motivos de seguridad, mantenimiento o mejora del servicio al cliente, se deben actualizar los datos de la cuenta, imitando, en todo el mensaje, la imagen corporativa de la entidad (logo, color, formato del texto, etc.). En caso de que la víctima sea cliente de esa entidad financiera o miembro de esa organización, es muy común que admita como fiable el contenido del mensaje, se meta en la web e introduzca sus claves y firma electrónica en la misma, obviando que está siendo víctima de una estafa. La apariencia y diseño de la web a la que accede la víctima es exacta a la de la entidad a la que está suplantando. Este tipo de ataque es conocido como *spoofing*.

Como he señalado, otro modo de obtener las claves y credenciales de la víctima es por medio del envío de software maliciosos, que captan la información cuando el ingenuo y confiado usuario se introduce en las páginas web de las entidades financieras u otro tipo de organización. Para ello utilizan programas específicos que captan las pulsaciones en el teclado.

---

[7] Véase el Informe de Detección de APTs de 2013 (http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf).

[8] Según el INTECO las técnicas de ingeniería social son todas las prácticas llevadas a cabo a través de engaños o manipulaciones para obtener información privilegiada, haciendo que la víctima ejecute sin conocimiento determinadas acciones que le pueden perjudicar.

Los medios necesarios para ejecutar el *phishing* son, habitualmente, materiales y humanos. Dentro de los materiales, es necesario contar, lógicamente, con un ordenador con conexión a internet, que normalmente están ubicados en lugares muy distintos a los de los organizadores del fraude y el de la eventual víctima. Normalmente son lugares públicos como cibercafés, espacios culturales, etc.

Los medios humanos, a modo de sociedad criminal, se estructuran de la siguiente forma. En primer lugar, aparecen los miembros de la organización diseñadora y ejecutora del plan delictivo. Normalmente se trata de personas de la misma nacionalidad o zona de influencia de la organización. Viajan al país donde se va a cometer el fraude por un tiempo limitado con el objetivo de aperturar cuentas corrientes para recibir las transferencias, reembolsar el dinero y enviarlo a otros lugares por medio de agencias especializadas de remisión de dinero.

En segundo lugar, los gestores de pago. Por lo general, se trata de ciudadanos de los países de la organización, pero que residen o se encuentran en el país donde se va a producir el fraude. Y, en tercer lugar, los captados, también denominados como "muleros". En este grupo se encuentran todas las personas que, independientemente de su nacionalidad, responden a una oferta de trabajo que les llega, normalmente, a su correo electrónico como SPAM, acceden a las condiciones y ejecutan las instrucciones que reciben, en muchos casos de forma inconsciente y sin conocer que son elementos necesarios para la ejecución del delito.

Los muleros contribuyen a la comisión delictiva de la siguiente forma: i) cuando la organización se lo indica -normalmente el contacto se efectúa por correo electrónico- debe abrir una cuenta bancaria en una entidad concreta para facilitar inmediatamente a ese remitente o peticionario el número de cuenta, los datos del titular, los códigos de acceso online y el código IBAN; ii) posteriormente los miembros de la organización contactan con el mulero, indicándole que retire el dinero de la transferencia que ha recibido, obteniendo el mulero, como ganancia, un porcentaje del importe total de la transferencia que oscila entre el 10 y el 15%, remitiendo el resto al extranjero a través de las empresas especializadas en envíos de remesas de dinero al lugar y beneficiario que le indican; y iii) cuando se realiza el envío, el mulero notifica, por medio de un correo electrónico, que ha realizado el envío y remite el código identificador del mismo[9].

[9] La sentencia de la Audiencia Provincial de La Rioja, de 21 de diciembre de 2011, sintetiza de forma didáctica en qué consiste el *phishing*: "es un concepto informático que denomina el uso de un tipo de fraude caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como "phisher", envía a numerosas personas correos electrónicos masivos en los que se hace pasar por una empresa de confianza (por ejemplo, una entidad bancaria, o una compañía telefónica, etc.); otras veces lo hace mediante la creación de páginas "web" que imitan la página original de esa entidad bancaria o empresa de reconocido prestigio en el mercado; en ocasiones también se realiza por medio de llamadas telefónicas masivas realizadas a numerosos usuarios en las que se simula ser un empleado u operador de esa empresa de confianza. En todo caso, siempre se trata de una aparente comunicación "oficial" que pretende engañar al receptor o destinatario a fin de que éste le facilite datos bancarios o de tarjeta de crédito, en la creencia de que es a su entidad bancaria o a otra empresa

La relevancia penal del *phishing* sí está contemplada en el Código penal, de tal suerte que estas conductas se subsumen en el tipo del artículo 248.2 del Código penal, sin perjuicio de aplicar el subtipo agravado del artículo 250 si concurre alguno de los supuestos allí contemplados[10].

### 3. El *ciberbullying*

Es frecuente que niños y jóvenes en edad escolar sufran, acoso, vejaciones y amenazas continuadas por parte de compañeros, producidas también a través de redes sociales digitales, como twitter, que menoscaban, a menudo, la integridad moral, y atentan contra el honor y dignidad personal de quien sufre esos ataques y, a veces, también de sus familiares.

La Audiencia de Ávila estableció que el acoso escolar, también conocido como *bullying* "comprende un catálogo de conductas, en general permanentes o continuadas en el tiempo, susceptibles de provocar en la víctima sentimientos de terror, de angustia e inferioridad idóneos para humillarle, envilecerle y quebrantar, en su caso, su resistencia física y moral"[11].

---

igualmente solvente y conocida a quien está suministrando dichos datos. Finalmente, en otras ocasiones el sistema consiste simplemente en remitir correos electrónicos que inducen a confianza (simulando ser de entidades bancarias, etc) que cuando son abiertos introducen "troyanos" en el ordenador del usuario, susceptibles de captar datos bancarios cuando este realiza pagos en línea. En todo caso, fuere cual fuere el "modus operandi"elegido, el objetivo son clientes de banco y servicios de pago en línea. A su vez, entidades ficticias de "phishing" intentan captar tele-trabajadores (mediante un método conocido usualmente como " scam") por medio de e-mails, chats, y otros, ofreciéndoles no solo trabajar desde casa (desde su ordenador), sino también otros importantes beneficios, normalmente consistentes en cuantiosas comisiones por prácticamente "no hacer nada": efectivamente, las personas que aceptan la oferta se involucran obligándose a facilitar una cuenta bancaria y a transferir el dinero que su "empleador" le ingrese en esa cuenta (obviamente está implícito que sin hacer preguntas después), transferencia que siempre se realiza a destinatarios en el extranjero (por lo general a países del Este de Europa y por medios como "Western Union" "MoneyGram" y otros semejantes), previa detracción de una comisión porcentual que se queda el trabajador captado y que oscila entre el 5 y el 10%. Es decir, si cada transferencia es, por ejemplo, de 3.000 euros, el "tele- trabajador reclutado" se queda con una comisión entre 150 y 300 euros por transferencia; y lo único que tiene que hacer es recibir el dinero en su cuenta y efectuar una transferencia electrónica a la cuenta que le facilita quien le "contrató". Si multiplicamos esto por varias transferencias, obviamente esta persona recibe una importantísima retribución a cambio de una actividad de nula complejidad y menor esfuerzo. Huelga decir que las sumas trasferidas a las cuentas de estos "tele-trabajadores" (que son conocidos a veces como "muleros" o " mulas" en argot informático) son las que el "phisher" previamente ha obtenido fraudulentamente a través del "phishing"; y que este dinero, previo paso fugaz por la cuenta del tele-trabajador y previa detracción por éste de su comisión, acaba en la cuenta extranjera del mencionado "phisher". En definitiva, y sin perjuicio de la actividad fraudulenta del "phisher" (muchas veces se trata delincuencia organizada extranjera), en cada acto fraudulento de phishing el trabajador captado o reclutado recibe el ingreso en su cuenta bancaria y la empresa le notifica del hecho, una vez recibido este ingreso, se queda un porcentaje del total del dinero como comisión de trabajo y el resto lo reenvía a través de sistemas de envío de dinero como MoneyGram, Wester Union, etc. a los destinatarios indicados por la seudoempresa contratante" (FJ 1).

[10] El Acuerdo adoptado en Sala general, por el Pleno de la Sala Segunda, en su reunión de 31 de marzo de 2009 concluyó que: "A los efectos del art. 250.1.4 del CP, la utilización de las claves bancarias de otro no es firma".

[11] Sentencia 146/2008, de 20 de octubre.

El *bullying* se integra en el tipo del artículo 173 del Código penal, como delito contra la integridad moral, que, además, de acuerdo con la conducta desplegada por el sujeto activo y de sus efectos puede estar en relación concursal con los delitos o faltas de lesiones, amenazas o coacciones.

La jurisprudencia del Tribunal Supremo ha definido este delito como el tipo básico de las conductas incluidas dentro del Título VII del Libro II del Código penal como delitos contra la integridad moral de las personas configurando el bien jurídico protegido por el tipo (la integridad moral), como una categoría conceptual propia, como un valor de la vida humana independiente del derecho a la vida, a la integridad física, a la libertad en sus diversas manifestaciones o al honor[12].

El concepto de la integridad moral aparece así definido desde el artículo 15 de la Constitución Española que reconoce el derecho a la vida y a la integridad física y moral, interpretando la jurisprudencia constitucional el mismo, desde la idea de la inviolabilidad de la personalidad humana, es decir, el derecho a ser tratado como persona y no como cosa, refiriéndose a "sensación de envilecimiento", "humillación, vejación e indignidad" y a "padecimientos físicos o psíquicos ilícitos e infligidos de un modo vejatorio para quien los sufre y con esa propia intención de vejar y doblegar la voluntad del sujeto paciente[13].

Desde esta perspectiva, el Tribunal Supremo señala que la integridad moral estaría compuesta por vía negativa por elementos subjetivos, tales como los constituidos por la humillación o vejación sufrida por la víctima que se ve tratada de forma instrumental y desprovista de su dignidad, pudiendo además concurrir la nota del dolor físico y también por elementos objetivos en referencia a la forma y modo en que se produce el ataque. Asimismo, la Sala Segunda del Tribunal Supremo añade que la nota que delimita y sitúa a la conducta típica dentro de la órbita penal radica en un límite que es a su vez difuso, refiriéndose a la nota de la gravedad ("menoscabando gravemente su integridad moral" dice literalmente el artículo 173 del CP), exigencia de gravedad que deja claro que no todo trato degradante será típico conforme al citado precepto, sino sólo los más lesivos.

Por tanto, los elementos que conforman el concepto de atentado contra la integridad moral de las personas que sufran este acoso informático son los siguientes: i) un acto de claro e inequívoco contenido vejatorio para el sujeto pasivo; ii) la concurrencia de un padecimiento físico o psíquico; y iii) que el comportamiento sea degradante o humillante con especial incidencia en el concepto de dignidad de la persona-víctima.

Las expresiones y actuaciones proferidas en este tipo de acoso escolar cibernético, de forma continua, reiterada y persistente en el tiempo, crean en los menores un sentimiento de angustia e incluso de inferioridad susceptible de humillarles y de quebrantar su resistencia moral. Estas conductas de naturaleza degradante o humillante que inciden

[12] Entre otras, SSTS de 29 de septiembre de 1993; 3 de octubre de 2001; 8 de mayo de 2002; 2 y 16 de abril de 2003; 824/2003, de 5 de junio; 22 de febrero de 2005 y 31 de enero de 2007.
[13] SSTC 120/90, 137/90 y 57/94.

directamente en el concepto de dignidad de la víctima es el *bullying*, que cuando se practica a través de plataformas digitales se le denomina *ciberbullying*.