DELITOS CONTRA MENORES EN INTERNET

TRABAJO FINAL DE GRADO
GRADO EN CRIMINOLOGÍA Y SEGURIDAD 2015/2016

ALUMNO: **Marta Martínez Amorós**
TUTOR: **Manuel Mollar Villanueva**

ÍNDICE:

Extended Summary

The emergence of ICT, Information and communications technology, has opened the door to new forms of cybercrime because of the deepest changes caused by the digitalization, the convergence and the continuous globalization of computer network, this causes the came up of new typology of cybercrime and the consequent increase in the next years.

The term cybercrime can get two meanings, a typological meaning, to referring the cybercrime to a determined behaviour that meets a number of criminology and legal features related with the cyberspace, and a normative meaning, to identify a determined penal type with their assumption and their sanction, pretending to prevent the realization of behaviour in the cyberspace that can affect to legal interests that deserves protection. It's important the fact of knowing when we face a cybercrime, because it isn't enough to eject the criminal behaviour the using of ICT, also it will require the same use of ICT that has to do with some essential factor of the crime.

In English there isn't two terms to referring cybercrime, in Spain it's different, we have two terms to mention cybercrime: *cibercrimen* and *cibercriminalidad*.

The Spanish Constitution in their 39 article refers the figure of child as particularly vulnerable individuals, with we have to bring special social, economic and legal protection expected in the international agreements like the Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, the first instrument that recognize that childhood is entitled to special care and assistance.

The Internet crimes against children are:

Child pornography:

Is a criminal offense and is defined as any visual depiction involving the use of a minor, or one appearing to be a minor, engaging in sexually explicit conduct. Visual depictions include photographs, film, video, pictures or computer-generated images of pictures, whether made or produced by electronic, mechanical, or other means. Child pornography has become particularly problematic with the rise of the Internet and its ability to both transmit data far and wide and provide a level of anonymity (specially in web servers like TOR, but they use other ways like FTP servers or P2P) to its users and the victims depicted in images of child pornography.

Cyberbullying:

Is when a child, preteen or teen is tormented, threatened, harassed humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet,

interactive and digital technologies or mobile phones. It has to have a minor on both sides, or at least have been instigated by a minor against another minor. Once adults become involved, it is plain and simple cyber-harassment or cyberstalking. Adult cyber-harassment or cyberstalking is never called cyberbullying.

In Spain the social preoccupation for this type of violence (minor against minor) has increased in the last years. Causing social alarm and putting this type of cases on the principal Spanish newspapers and news, making with this a greater diffusion and knowledge about this issue in society. However, Spain has a lack of an integral dealing on the fight against all forms of violence in childhood like cyberbullying, resting efficacy to the measures that could take.

Childgrooming or sexual grooming:

Is one of the most dangerous cybercrimes because attempts directly against the child's right to liberty and sexual indemnity. It consists when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse or exploitation. Using in this case to find possible victims social media sites, instant messaging apps including teen dating apps, or online gaming platforms to connect with a young person or child. Once they have established trust, childgroomers will exploit the relationship by isolating the child from friends or family and making the child fell dependent of them.

Sexting

Is the act carry out by children to sending sexually explicit photos, messages, voicemails, videos, etc., either via phone, computer, webcam or other device. Sending suggestive and explicit content has been done for hundreds of years, what's different now is the combination of technology that can broadcast this information instantly and virally, and the permanence of sending and storing this content on digital media. We can discern two types of risky behaviours:

- Active sexting: The sending of selfies or videos on a sexy, provocative or inappropriate attitude.
- Passive sexting: The receiving of selfies or videos on a sexy, provocative or inappropriate attitude.

Sexting requires:

- The voluntariness of the subject.
- The using of ICT
- Sexual content.
- Age.

Cyberstalking:

Is a crime in which the attacker harasses, stalks or threatens a victim using electronic communication, such as e-mail or instant messaging, or messages posted to a web site or a discussion group. A cyberstalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected. It isn't a conduct that affects exclusively to child, it can be made by adults.

This behaviour involves using electronic means, including the Internet, to stalk or harass a person or group of people. Cyberstalking can include many things including threats, solicitation for sex, false accusations, defamation, slander, libel, identity theft, and vandalism. Cyberstalking is often used in conjunction with offline stalking, as both are an expression of a desire to control, intimidate or manipulate a victim. However, many authors are discussing yet the idea of a connection between cyberstalking and offline stalking.

We have to consider the importance of prevention, how? through the labour of the police forces, Internet service provider (ISP) and education.

The role of the police in prevention:

In Spain we have two forces: *la Guardia Civil* and *el Cuerpo de Policía Nacional*. They work in special groups like the *Grupo de Delitos Telemáticos* and the *Brigada de Investigación Tecnológica.* They cooperate with EUROPOL and INTERPOL in order to disbanding organized cybercrime groups.

We can ask how act the police to catch this type of illegal content. There are three types of actuations:

- Tracking system, in which various file channel sharing are unceasingly monitored. For example: P2P networks.
- Interception of communications with programs like SITEL.
- With Trojan programs, police agents will be able to use spyware programs. However, this type of actions requires judicial authorisation.
- The figure of undercover agent, that can exchange or sending illicit files in order to identify the subjects that are sending illegal content in chat rooms, closed forums or P2P networks. That actuation requires judicial authorization.

The role of Internet Service Provider in prevention:

ISPs are a company that provides Internet services, including personal and business access to the Internet. The service provider usually provides a software package, username, password and access phone number.

ISPs have a central role to play in combating Internet child pornography. The structure of the Internet makes control of child pornography very difficult. The Internet is a decentralized

system with no single controlling agency or storage facility. Consequently, if one website or newsgroup is closed down, there are many others that can instantaneously take its place. ISPs in object to combat Internet child pornography may:

- Report known illegal activity on their sites, blocking the access of child pornography users and the retirement of this type of content.
- ISPs may collaborate with the police.

The role of education in prevention:

The education takes an important place to affront cybercrime against children. Children are naturally trusting, especially with adults. It's difficult for parents to teach children to balance this trust with caution. Today, children need to learn how to react to dangerous situations on the Internet using common sense to keep them safe. They should be reinforced in a gentle manner and be provided with effective rules to avoid some tough situations.

The guidelines to achieve an effective prevention are:

- Establish of suitable levels of interfamilial education.
- Education in sensibility.
- Information management.
- Collaboration between family and schools to resolving problems.
- Education in digital skills.
- Establishment of rules and supervision based on age.
- Familiar and school education in relation to preserve and educate about managing privacy, law and protection of it and respecting self and others image.
- Concept of crime: Improve child sensitization about the actions that can cause sanctions in familiar, school and penal areas.

On the other hand, we have to speak about school and teacher's strategies to prevent:

- Measures related to self-affirmation.
- Organizational measures.
- Curricular insertion measures.
- Measures associated with the adequate management of cases.
- Measures related to risk avoidance.
- Finding help measures.

Finalizing, the dark figure of crime is a term that is used by crime experts to illustrate the number of committed crimes that are never reported or are never discovered and this puts into doubt the effectiveness and efficiency of the official crimes data. Among the crimes that take place in any given place at a given period of time, some of them are never reported to the

police, and some are reported but never recorded by the police officers. The phenomenon of the dark figure of crime occurs for many reasons:

- In many occasions the criminal behaviour passes directly unnoticed by the victim, not reported in that case although this action has committed and even the criminal effect was done.
- The victim is aware of the attack but he or she reports it late when the crime has prescribed, or when the own victim thinks that is illogical to presenting the demand because thinks that are a few possibilities that police was able to identify, arrest and prosecute the cyber delinquent.
- The victim aware of cybercrime rest value of the act and don't report it.
- The reason why the victim doesn't complaint is because the lack of confidence in judicial system, generally because the conviction to the difficulty that involve the identification of the responsible person of acts.
- The called "silence law", when bullying occurs through electronic communication, there is an additional obstacle to reporting, the fear of not being accepted between equals if they report.
- Perhaps the greatest fear that restrains students from reporting abusive online behaviour is that adults will restrict the reporting child's digital access.

Conclusions

It's impossible to eliminate completely problems caused by cybercrime, because the Internet is a technology that is evolving incredibly fast causing the emergence and improvement of new and old criminal behaviours.

Levels of cybercrime will be increase in the next years because we are living in a society completely dependent of technologies.

We have to insist in the idea of prevention as instrument to fight against cybercrime.

Total security in Internet doesn't exist. It's impossible to decrease child pornography content in web servers like TOR because their policies of anonymity.

It's problematic the lack of attention that shows some parents not educating their sons in the risks that can cause the bad using of ICT, being this a factor for their sons to become a potential victims of cybercrime.

Resumen: El objeto de estudio de este trabajo es, como bien dice el título, los delitos contra menores cometidos a través de Internet, para ello elaboraré un listado acerca de los delitos más relevantes basándome en la legislación vigente sobre esta materia en España, realizando además un análisis exhaustivo de cada modalidad delictiva, extrayendo el perfil del sujeto infractor, así como el de la víctima, presentando estadísticas del número de delitos de este tipo cometidos en territorio español, aportando casuística y describiendo la actuación policial que se realiza en cada tipo delictivo. Previamente, analizaré la figura del menor como víctima y el papel que poseen tanto los padres como las instituciones a la hora de preservar al menor de este tipo de delitos. Asimismo, haré referencia a la prevención, donde uno de los puntos que cobra más importancia en la defensa de la indemnidad sexual del menor será la educación y la aplicación de programas de actuación vigentes, por parte de las Fuerzas y Cuerpos de Seguridad del Estado. Finalmente haré mención a la llamada cifra negra y concluiré dicho estudio bajo mi criterio personal, basándome en todo momento en los datos y la información extraída y expuesta anteriormente en el trabajo.

Palabras clave: Delitos contra menores, Internet, menor como víctima, perfil víctima y agresor, prevención, cifra negra.

Abstract: The objective of this project is to analyse Internet crimes against children, doing a list of relevant cybercrime based in Spanish current legislation and explaining it, obtaining offender's and victim's profile, presenting statistics of cybercrime happened in Spain. Previously analysing the figure of minor as victim. Then explaining the dark figure of crime and the important role that takes prevention (role of police, ISPs and education). Finishing with my personal criteria based in the information exposed along the project.

Keywords: Crimes against children, Internet, minor as victim, offender's and victim's profile, prevention, the dark figure of crime.

1 Introducción

La aparición de las TIC, acrónimo de Tecnologías de la Información y la Comunicación, ha abierto la puerta a nuevas formas de cibercrimen debido a los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas[1], hecho que provoca que vayan surgiendo nuevas tipologías de cibercriminalidad, lo que supone que esta siga expandiéndose y evolucionando en las próximas décadas.

Podemos hacer un seguimiento cronológico para visualizar como es de cambiante el mundo de las tecnologías y como este ha introducido nuevas formas de criminalidad: La aparición de la figura del hacker que atenta contra la intimidad de la persona al aparecer los primeros sistemas informáticos [2] que contenían información personal. Cuando esta

[1] Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

[2] Entiéndase por "sistema informático", todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento

información personal pasó a tener además un valor económico y a utilizarse o servir para la realización de transacciones económicas dio lugar a la aparición de varias formas de criminalidad económica relacionadas con los ordenadores, como es el fraude informático, evolucionando con la aparición de Internet en scam, phishing, skimming o carding, ransomware, etc. Posteriormente la universalización de la Red y la constitución del ciberespacio dio lugar a nuevas conductas delictivas que aprovechaban la referida universalización para atacar intereses patrimoniales y personales de usuarios concretos o para atentar contra intereses colectivos a través del ciberterrorismo o ciberracismo. En la actualidad con la entrada en juego de redes sociales como Facebook, Twitter, Instagram o Tumblr, multitud de programas de mensajería instantánea, invadiendo todos los ámbitos sociales, como lo son WhatsApp, Line o Telegram, y la aparición de aplicaciones que particularmente "sirven para todo", conocer gente nueva y ligar, Tinder, Badoo; viajar en coche de forma compartida como Blablacar, car2go, etc. Esto ha dado pie de forma positiva a la creación de relaciones a través del ciberespacio pero con ello también se ha dado lugar a nuevas conductas delictivas precisamente al ceder voluntariamente esferas de la intimidad del sujeto como son el grooming, sexting, ciberbullying, etc. Consecuentemente ha provocado además la evolución del perfil del ciberdelincuente, y el de la víctima.

Ese carácter cambiante y novedoso del cibercrimen será lo que le dé mayor dificultad desde una visión político criminal, por la obligación de adaptar todas las estructuras políticas, jurídicas y sociales a la necesidad de protección de nuevos y viejos intereses frente a nuevas formas delictivas que son cambiantes porque lo sigue siendo el ámbito social en el que las mismas se producen[3].

1.1 Concepto de cibercrimen y cibercriminalidad

Es necesario hablar por tanto de los conceptos de cibercrimen y cibercriminalidad ya que es el objeto de estudio que nos hemos planteado en este trabajo.

En un principio se empleaba el término delitos informáticos para referirse a "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos", esta definición fue realizada por SIEBER junto a otros expertos de la materia en la Organización de Cooperación y Desarrollo Económico (OCDE) en 1983 París, Francia. Sin embargo aunque esta descripción fuese concebida por sus autores como una primera aproximación con gran amplitud que permitiría

automatizado de datos en ejecución de un programa. Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

[3] MIRÓ, F., El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Ed. Marcial Pons. 2012. p. 28.

el tratamiento de las mismas hipótesis de trabajo para distintas disciplinas, tanto en análisis económicos, penales, sociológicos, etc.[4] Esto conllevaba a que formasen parte de dicha definición tanto aquellos comportamientos realizados a través de procesos electrónicos, como aquellos otros delitos tradicionales que recaían sobre bienes que presentaban una configuración específica en la actividad informática, de hecho la clasificación realizada por SIEBER de los delitos informáticos era de: Una primera categoría de contenido patrimonial, formada por el fraude informático, espionaje informático y sabotaje informático; una segunda categoría de delitos cometidos por medio de sistemas informáticos contra derechos de la personalidad, como la intimidad o libertad sexual y una tercera categoría de delitos informáticos que afectan a bienes supraindividuales o bienes sociales[5]. No obstante, esta clasificación se refería exclusivamente a tipologías de conductas y no a tipos penales, lo que provocó que se replantease el concepto de delitos informáticos y se sustituyese por los términos cibercrimen y cibercriminalidad, la evolución de este término se debe a la preocupación legal que comienza a surgir con respecto al desarrollo de nuevos comportamientos ilícitos en la Red, la preocupación por la información contenida en los sistemas informáticos pasa a un segundo plano; el riesgo se centra ahora en las redes telemáticas[6] a las que estos sistemas informáticos empezaron a estar conectados, poniendo en peligro los intereses personales y sociales que se producen a través de esta conexión. De hecho el Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, se decanta como bien dice el título por el término ciberdelincuencia y no por el de delito informático, este último concepto únicamente será utilizado para clasificar los delitos estrictamente informáticos, como lo son la falsificación informática y los fraudes informáticos.

El término cibercrimen puede tener dos sentidos, un sentido tipológico, para referirnos a un comportamiento concreto que reúne una serie de características tanto criminológicas, como legales relacionadas con el ciberespacio[7]; y un sentido normativo, para tratar de identificar un

[4] SIEBER, U., The International Handbook on Computer Crime: Computer-related Economic Crime and the Infringements of Privacy, Ed. Wiley, 1986.
[5] SIEBER, U., Informationstechnologie und Strafrechtsreform, Köln/Berlin/Bonn/München, ed. Carl Heymanns, 1985, pp.14 y 15.
[6] Entenderemos por "redes telemáticas", el grupo de protocolos TCP/IP que se ha convertido en el estándar de la industria de los protocolos de transferencia de datos para los niveles de red y de transporte del modelo OSI (Open Systems Interconnection o Interconexión de Sistemas Abiertos). Ya que son los protocolos utilizados en Internet. ZACKER. C., Redes. Manual de referencia, ed. McGraw-Hill. Osborne Media, 2002.
[7] El término ciberespacio fue acuñado por el escritor de ciencia ficción GIBSON, W., en su obra Neuromante, Barcelona, ed. Minotauro, 1984, pero aparece por primera vez en Quemando Cromo, 1981, este se refiere al ciberespacio como *"una representación gráfica de los datos extraídos por bancos de cada ordenador en el sistema humano. Complejidad impensable. Líneas de luz trazadas en el no-espacio de la mente, cúmulos y constelaciones de datos. Como luces en la ciudad, alejándose"*, como vemos es un concepto muy abstracto, básicamente el autor describía en su obra una sociedad muy avanzada tecnológicamente en la que las personas accedían a un mundo virtual separado del mundo real.

tipo penal concreto con un presupuesto y una sanción, que pretende prevenir la realización de conductas en el ciberespacio que afectan a bienes jurídicos que merecen protección. Es importante el hecho de saber cuándo nos encontramos ante un cibercrimen, ya que no bastará con que se utilicen las TIC para ejecutar el comportamiento criminal, se exigirá que el mismo uso de las TIC tenga que ver con algún elemento esencial del delito.

En cuanto al concepto de cibercriminalidad, diremos que se establece una relación directa con el concepto de cibercrimen ya que el concepto cibercriminalidad se entiende como fenómeno de la criminalidad en el ciberespacio en general y el término cibercrimen por tanto, para situar dentro de ese fenómeno de la criminalidad a un tipo de comportamiento concreto.

2 El menor como víctima en el ciberespacio

La Constitución Española en su artículo 39 hace referencia al menor elevándolo a la categoría de sujeto especialmente vulnerable, el cual se le deberá ofrecer una especial protección, tanto social, económica como jurídica prevista en los acuerdos internaciones donde se encuentra entre ellos la Convención sobre los Derechos del Niño, de 20 de noviembre de 2006, primer instrumento creado que reconoce a los niños y niñas como agentes sociales y titulares activos de sus propios derechos.

Hemos dicho que en la Convención sobre los Derechos del Niño se garantiza el que los menores sean titulares de sus propios derechos, es decir puedan tomar sus propias decisiones de forma autónoma. Pero para ello se exigirá que el menor tenga el suficiente discernimiento para comprender la acción que realiza, a esto se le llama “capacidad natural”, es decir se presupone que es capaz de valorar las consecuencias tanto positivas como negativas de la decisión que adopte en un determinado momento, valorando por tanto las ventajas, inconvenientes y posibles riesgos.

Pero debemos tener en cuenta que cada acto tiene un alcance y trascendencia que influenciará de diferente manera en el desarrollo futuro del menor, provocando una serie de consecuencias que podrían ser perjudiciales para su mencionado desarrollo.

Para intentar salvar esto se estableció un límite de edad generalizado para el ejercicio de determinadas conductas que pudiesen conllevar el riesgo de afectar al desarrollo del menor. En estos casos se da por hecho que superado ese límite el menor tiene la capacidad natural para realizar la conducta.

Algunas conductas que se encuentran limitadas al ejercicio por la edad, serían:

- Consentimiento sexual, ahora establecido a los 16 años.
- Donación de órganos, se requiere la mayoría de edad, establecida en 18 años.

- Técnicas de reproducción asistida, establecida también en 18 años, además se requiere la "plena capacidad de obrar".
- La conducción de vehículos a motor, establecida en 18 años.
- Solicitud de la nacionalidad española, establecida a los 14 años.

Por tanto, cuanto más graves sean las consecuencias que pueden resultar del ejercicio de un determinado derecho mayor será el grado de exigencia de capacidad natural, es decir de capacidad de discernimiento y madurez que se requiera para ejercer dicha conducta.

En muchas ocasiones además del consentimiento del menor se requerirá del consentimiento de los padres o tutores del menor.

Ahora bien, esa capacidad natural como hemos dicho viene delimitada por la edad del sujeto, habrá casos en los que aunque el sujeto cumpla con la edad establecida para ejercer un determinado derecho, no se encuentre capacitado para ello dificultando por tanto la tarea del legislador a la hora de desarrollar normativa nueva.

Esta problemática es la que se encuentra en el punto de mira en estos momentos en cuanto a los delitos cometidos en medios informáticos contra menores, ¿hasta qué punto el menor que publica datos personales o imágenes propias en Internet es consciente de los riesgos que con ello van asociados? Poniendo un ejemplo, en la red social Facebook[8] en sus condiciones de servicio exige al usuario que sea mayor de 13 años para poder acceder a esta, sin embargo no existe ningún mecanismo para evitar que este menor se registre falsificando su fecha de nacimiento, acción que es muy habitual, con esta se está poniendo en peligro el derecho a la intimidad del menor que no es consciente de las consecuencias o el riesgo que podría conllevar la subida desafortunada de una imagen propia aun siendo mayor de 13 años, poniendo en duda por tanto su capacidad natural para realizar este tipo de conducta.

Como curiosidad debemos apuntar que, anteriormente el acceso a la red social Facebook en España estaba permitida a mayores de 12 años igual que en los demás países, pero debido a la labor de la Agencia Española de Protección de Datos (AEPD) se elevó el límite a 14 años, adaptándose pues a la exigencia de la legislación española. ¿Por qué 14 años y no 16, por ejemplo?, según la AEPD "el menor de 14 años tiene condiciones suficientes de madurez para prestar su consentimiento al tratamiento de los datos, ya que en nuestro ordenamiento jurídico viene a reconocer a los mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solos determinados actos de la vida civil". También añade que, "la minoría de edad no supone una causa de incapacitación por lo que aquella habrá de ser

[8] En la página web de Facebook dentro del apartado condiciones del servicio habla de que *"Los usuarios de Facebook proporcionan sus nombres e información reales y necesitamos tu colaboración para que siga siendo sí. Estos son algunos de los compromisos que aceptas en relación con el registro y mantenimiento de la seguridad de tu cuenta"*, uno de ellos es *"no utilizarás Facebook si eres menor de 14 años"*. Únicamente recomienda que no utilicen la red social los menores de 14 años.

analizada en cada caso concreto a los efectos de calificar la suficiencia en la prestación del consentimiento en atención a la trascendencia del acto de disposición y a la madurez disponente", básicamente viene a decir que el ser menor de edad no quiere decir que no pueda o este incapacitado para realizar determinadas conductas, que deberán ser estudiadas para decidir si pueden ser ejercidas o no por el menor.

Debemos tener en cuenta que aunque no se requiera el consentimiento parental para estos casos dejando la decisión a merced del menor a la hora de acceder a determinadas redes sociales o a Internet en general, los expertos recomiendan la supervisión de los padres sobre las conductas que realiza el menor en la red, de hecho una de las causas que más preocupa a los padres es el que sus hijos menores sean contactados por extraños en Internet o que puedan cometerse delitos contra ellos en Internet[9] seguido de que sean maltratados o vejados por otros niños y de que vean material inapropiado en Internet. Sin embargo, un 54% depositan bastante confianza en Internet, un 53,3% y un 53,9% autorizan a sus hijos/as a utilizar Messenger, WhatsApp y a navegar por Internet o ver videoclips por Internet. Un 88,6% no tienen conocimiento de que sus hijos hayan accedido a alguna página web con contenido inapropiado o perjudicial.

En cuanto a la misma encuesta realizada a los menores[10], un 58,8% utiliza Internet todos los días dedicándole entre una y dos horas (41,9%), un 70,3% están autorizados por sus padres a navegar en Internet en cualquier momento sin su supervisión, seguido de ver videoclips en Internet (67,3%) y utilizar plataformas de mensajería instantánea tipo WhatsApp o Messenger (66,7%). Un 88,6% recibieron alguna vez información de cómo utilizar Internet de forma segura a manos de su padre, madre o tutor, sin embargo un escaso 34,4% y 13,9% recibieron información respectivamente por parte de la Policía Nacional, Guardia Civil o Policía Local o por parte de los medios de comunicación.

Un 82,7% no ha tenido una experiencia desagradable con alguien que le haya podido provocar desagrado o haberle herido, frente al 12,9% que sí la ha experimentado, de estos 12,9% un 55,9% le sucedió a través de plataformas de mensajería instantánea y un 39% a través de las redes sociales, ¿de qué forma experimentaron esto? a través del envío de mensajes desagradables por Internet (43,6%), seguido de un 21% que indicaron que le enviaron o *postearon* públicamente en Internet mensajes desagradables o hirientes sobre él.

[9] Según la encuesta sobre hábitos de uso y seguridad de Internet de menores y jóvenes en España de junio de 2014 realizada por el Ministerio de Interior. En esta se realizaron 1006 entrevistas a través de una web, a padres con hijos/as de edad comprendida entre los 10 y 17 años y residentes en territorio nacional.

[10] Se trata de la encuesta sobre hábitos de uso y seguridad de Internet de menores y jóvenes en España de junio de 2014 realizada por el Ministerio de Interior. Se efectuó a 1506 menores y jóvenes con edades comprendidas entre los 10 y 17 años residentes en territorio nacional, a través de una entrevista realizada por página web.

Un 42,3% visualizaron alguna vez material hiriente o grotesco en Internet a través de pop-up o ventanas emergentes[11] que aparecían accidentalmente (47,1%) y en páginas de vídeos (33,1%).

En cuanto a mensajes recibidos o vistos por menores con contenido sexual en Internet un 36,4% los recibió a través de plataformas de mensajería instantánea, un 32,5% a través de las redes sociales y un 31,2% a través de pop-up o ventanas emergentes.

Debemos destacar que un 22,2% añadió a gente a su lista de amigos o libreta de contactos a los que nunca ha conocido en persona, y un 42,2% alguna vez tuvo contacto en Internet con alguien a quien no había conocido en persona frente a un 53,9% que no. De ese 42,2%, un 54,8% no tuvo contacto en persona con quien conoció por Internet pero sí un 41,7%.

Por otro lado, según datos del Instituto Nacional de Estadística del año 2015[12], prácticamente toda la población escolar entre 10 y 15 años (por encima del 90%, concretamente 93,6%) tiene acceso a Internet, y un porcentaje muy alto (en torno al 90%, concretamente 90,9%) de alumnos de entre 12 y 16 años tiene su propio teléfono móvil. Además, diversos estudios realizados en España demuestran que los adolescentes usan principalmente las TIC para comunicarse con sus amigos especialmente a través de las redes sociales.

3 Clasificación de delitos contra menores en Internet

3.1 Pornografía infantil

3.1.1 Regulación en materia de pornografía infantil

Es mucha la materia legislativa que se ha escrito a cerca de la pornografía infantil debido al incremento de esta práctica, en la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989 se añadió un Protocolo facultativo relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía infantil, a través de la Resolución A/RES/54/263 del 25 de mayo de 2000 que entró en vigor el 18 de enero de 2002, en ella se amplían las medidas que debe adoptar los Estados que forman parte de la Convención con el fin de garantizar la protección de los menores contra estas conductas, además se define el término pornografía infantil como “toda representación, por cualquier medio, de un niño

[11] Una ventana emergente o pop-up es una ventana que aparece automáticamente mientras se navega por Internet sin ser solicitada y que tiene como fin desplegar publicidad, dirigir tráfico de Internet a ciertas páginas o recopilar direcciones de correo electrónico. Causando una molestia para los usuarios de Internet. Además de mostrar contenidos sexuales que pueden ser inapropiados para el usuario que se encuentra en ese momento navegando por Internet.

[12] Instituto Nacional de Estadística (2015): Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares.

dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales".

Por su parte a nivel europeo el asunto se ha tratado en el Convenio sobre Cibercriminalidad de Budapest de 2001[13] y el Parlamento Europeo y el Consejo de la Unión Europea que elaboraron la Directiva 2011/92/UE de 13 de diciembre de 2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, sustituyendo a la Decisión marco 2004/68JAI del Consejo; en esta se realiza un concepto más elaborado de pornografía infantil como:

i) todo material que represente de manera visual a un menor participando en una conducta sexualmente explícita real o simulada,
ii) toda representación de los órganos sexuales de un menor con fines principalmente sexuales,
iii) todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita real o simulada o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, o
iv) imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales.

También establece en su calidad de instrumento de aproximación del Derecho Penal, el límite máximo de la pena a alcanzar que deberían tener las diferentes conductas relacionadas

[13] El artículo 9 del referido Convenio tiene por nombre "delitos relacionados con la pornografía infantil", en este específica las conductas que serán constitutivas de pornografía infantil como es:

a) la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;
b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;
c) la difusión o transmisión de pornografía infantil por medio de un sistema informático,
d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;
e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

El apartado 2 establece además un concepto de pornografía infantil, como todo material pornográfico que contenga la representación visual de:

a) un menor comportándose de una forma sexualmente explícita;
b) una persona que parezca un menor comportándose de una forma sexualmente explícita;
c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

En el apartado 3 establece lo que se entiende por "menor" toda persona menor de dieciocho años, aunque se podrá establecer un límite de edad inferior, que será como mínimo de dieciséis años.

Finalmente el apartado 4 da a los Estados miembros libertad para reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2, del referido artículo 9.

con la pornografía infantil y que debería aplicar cada Estado perteneciente a la Unión Europea, las conductas que concretamente hace referencia son:

- La adquisición o la posesión de pornografía infantil
- El acceso a sabiendas a pornografía infantil por medio de las tecnologías de la información y la comunicación.
- La distribución, difusión o transmisión de pornografía infantil.
- El ofrecimiento, suministro o puesta a disposición de pornografía infantil.

Sin embargo, quedará a opción del Estado castigar o no cuando la persona que parezca ser un menor resulte tener en realidad 18 años o más en el momento de obtenerse las imágenes y cuando el material pornográfico ha sido producido y está en posesión de su productor estrictamente para su uso privado, siempre que para su producción no se haya empleado material pornográfico en los términos que establecen los apartados i), ii) y iii), y que el acto no implique riesgo de difusión del material.

Como vemos ha habido un gran esfuerzo por parte de los poderes públicos por concretar y definir con claridad qué se entiende por pornografía infantil, existiendo aun dudas sobre lo que es y no es.

A nivel estatal esta controversia no ha quedado del todo zanjada con la nueva redacción del artículo 189.1 del Código Penal introducida por la Ley Orgánica 1/2015, de 30 de marzo, en vigor desde el 1 de julio de 2015, que modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal y que específica lo que se entiende por pornografía infantil a través de la directiva 2011/93/UE, anteriormente mencionada.

En el artículo 189.1 contempla una serie de conductas típicas relacionadas con la explotación sexual y la corrupción de menores, se castigará en su apartado a) al que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas; en su apartado se castigará b) al que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

El legislador como vemos ha querido abarcar todas las conductas posibles con la intención de castigar todo lo relacionado con la pornografía infantil.

Seguidamente introduce una definición de pornografía infantil, que se consideraría:

a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada.
b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales.
c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.
d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales.

Algunos sectores se muestran reticentes con esta definición, resumidamente exigen la necesidad de fijar el significado que debe atribuirse a las palabras "representación" y "representar", para poder completar las conductas típicas, ya que consecuentemente una interpretación literal del precepto conduciría a resultados constitucionales y político-criminales inaceptables.[14] Concluyen además que las definiciones comentadas son válidas para aclarar qué es genéricamente pornografía infantil, pero no para establecer un componente esencial de unos tipos de acción, si no es a costa de burlar la Constitución Española. Una representación en la que no intervienen personas reales no lesiona bien alguno. Además, el material pornográfico escrito y el de audio quedarían excluidos del radio típico, este último se consideraba hasta ahora incluido dentro de las conductas típicas pero con la nueva definición quedaría fuera del concepto de material pornográfico infantil según el informe del Consejo Fiscal de 8 de enero de 2013, no obstante las pistas de audio podrían ser de interés a la hora de deslindar la naturaleza pornográfica o no del material de video.

[14] Concretamente en el manual GONZÁLEZ, J. L., VIVES, T. S., BUJÁN, C. M., ORTS, E., CUERDA, M. L., CARBONELL, J. L., BORJA. E., Derecho Penal Parte Especial, ed. Tirant lo Blanch, Valencia, 2015., con respecto a la definición de pornografía infantil realizada por el legislador se dice que se ha elaborado una descripción de las conductas típicas muy difusa o genérica, provocando que en el concepto de pornografía encajen conductas sin la menor importancia como por ejemplo, quienes pintan, dibujan o elaboran virtualmente a través del ordenador mediante un programa informático imágenes con apariencia de personas menores de edad o con discapacidad reales o imaginadas, participando en una conducta sexualmente explícita, real o simulada; o hacen lo propio con los órganos genitales, etc. Si las imágenes recogen solo los órganos genitales, ¿como se sabrá si son de un menor, salvo si es muy pequeño, o de una persona con discapacidad?. Y si son reales y son fotografiados o filmados sin que haya actividad sexual alguna, nos encontraremos con un desnudo y esto por sí solo no es pornográfico, por tanto no se castigaría ya que no va dirigido a fines principalmente sexuales. Los autores del manual se preguntan, ¿en qué consistiría por tanto la finalidad sexual?, ¿en el soporte en que se publique?, ¿si se publica una fotografía de los genitales de un menor en un libro serio sobre sexualidad infantil no es pornográfico y en una revista porno si?.

En el artículo 189.2 establece una serie de agravantes aplicadas a las conductas anteriormente mencionadas, como son:

a) Cuando se utilice a menores de dieciséis años.
b) Cuando los hechos revistan un carácter especialmente degradante o vejatorio.
c) Cuando el material pornográfico represente a menores o a personas con discapacidad necesitadas de especial protección que sean víctimas de violencia física o sexual.
d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.
e) Cuando el material pornográfico fuera de notoria importancia.
f) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.
g) Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho, aunque fuera provisionalmente, o de derecho, del menor o persona con discapacidad necesitada de especial protección, o se trate de cualquier otro miembro de su familia que conviva con él o de otra persona que haya actuado abusando de su posición reconocida de confianza o autoridad.
h) Cuando concurra la agravante de reincidencia.

El artículo 189.3, agravará la pena cuando hubiera mediado violencia o intimidación en los hechos a los que se refiere la letra a) del párrafo primero del apartado 1.

El artículo 189.5 castiga el auto-consumo y la posesión de pornografía infantil, el hecho imputable, consiste en la adquisición de material pornográfico de menores de edad, con independencia de que se obtenga o no mediante una contraprestación económica, no es necesario que el autor tenga ánimo de lucro[15]. Deberíamos plantearnos aquí que con las nuevas tecnologías se ha transformado el concepto de posesión, puesto que el aumento de la velocidad de Internet significa que ya no sería necesario descargar imágenes, porque pueden verse en línea. Por tanto, ¿sería la conducta de visualizar contenido en línea sin descargar reprochable penalmente?.

Además el mismo artículo castiga a quien acceda a sabiendas a pornografía infantil, por medio de las tecnologías de la información y la comunicación. Vemos que aquí el legislador

[15] Según la Sentencia núm. 105/2009 de 30 de enero, se exige para el tipo penal de la posesión que concurran tres elementos:

1. una posesión de material pornográfico, en cuya elaboración se hubieren utilizado menores o incapaces.
2. que este material se tenga para uso personal de quien lo almacene, excluyéndose cualquier actividad que suponga producción o difusión, es decir, alguna de las modalidades de producir, vender, distribuir, exhibir o facilitar estas actividades por cualquier medio, o la mera posesión para esos fines.
3. un elemento subjetivo, constituido por el dolo del agente, que aquí bastará con la conciencia de que se posee en su sistema o terminal, tales archivos que constituyen pornografía infantil.

añade el medio por el cual se accederá a tal material, las tecnologías de la información y la comunicación, esto entraña graves dificultades probatorias ya que la necesidad de que el acceso a este tipo de contenido sea "a sabiendas" impone la exigencia de un dolo directo, requiriendo por tanto que para ser responsable de este tipo penal, la persona deberá de tener la intención de acceder a un sitio de Internet en el que haya pornografía infantil y, a su vez, saber que es posible hallar en él este tipo de imágenes. No deberán aplicarse penas a las personas que accedan sin intención a sitios que contengan pornografía infantil. Podrá deducirse el carácter intencionado de la infracción cuando el sujeto acuda con frecuencia a consultar en la red dicho material o si lo hace a través de recurrir a los servicios de pago[16]. En definitiva, con este artículo lo que se pretende es proteger la indemnidad, la seguridad y la dignidad de la infancia en abstracto, adelantando las barreras de protección y atacando el peligro inherente a conductas que pueden fomentar prácticas pedofílicas sobre menores concretos, siendo el objeto material del delito el material pornográfico.[17]

Por último, en el artículo 189.8, debido a que las nuevas tecnologías constituyen una vía principal de acceso a los soportes de la pornografía infantil, los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de Internet que contengan o difundan pornografía infantil o, en su caso para bloquear el acceso de dichas páginas web o aplicaciones a los usuarios de Internet que se encuentren en territorio español, que podrán ser acordadas con carácter cautelar a petición del Ministerio Fiscal.

3.1.2 Etapas en la utilización de Internet como medio de acceso

A lo largo del tiempo, con la irrupción de las Tecnologías de la Información y Comunicación y su evolución, se ha ido transformado completamente el modo de producir y difundir el material pornográfico, podemos distinguir por tanto una serie de fases:

- El traficante disponía el contenido pornográfico infantil en páginas web alojadas en servidores de Internet, los usuarios de estas páginas web pagaban una determinada cantidad económica proporcionando su número de tarjeta de crédito para efectuar el pago. Tenemos dos modalidades conductuales, la del usuario que conoce de este tipo de páginas web y accede a sabiendas, y la conducta del sujeto que crea la página web. Este sistema que se vino utilizando durante un tiempo se reveló como muy vulnerable a las denuncias penales y a las acciones de piratas informáticos, por tanto se pasó a otras modalidades conductuales más discretas.
- Los chats desarrollados en tiempo real donde los pedófilos dialogan entre sí y acuerdan intercambiarse a través del correo electrónico el material pornográfico, la compra directa

[16] Preámbulo de la Directiva 2011/93/UE
[17] Audiencia Provincial de Pontevedra (Sección 5ª) Sentencia núm. 84/2013 de 26 febrero. ARP 2013\222

de este material por alguna página web o la simple descarga de archivos, en los que el intercambio de fotografías de pornografía infantil es inmediato. Estas salas de chat han sido evitadas posteriormente por los pedófilos al cerciorarse de que podrían estar infiltradas por agentes encubiertos, aunque se siguen utilizando no para intercambiar contenido ilícito si no para establecer contacto entre usuarios interesados en este tipo de material intercambiando para ello sus direcciones de correo electrónico, ampliando el círculo de intercambio. Por lo tanto, la figura del traficante de pornografía infantil es sustituida por la de los consumidores que se asocian entre ellos de forma informal y sin ánimo de lucro. Estos socios, actuando coordinadamente pueden descargarse en su ordenador en poco tiempo a través de técnicas de intercambio por medio de correo electrónico o de métodos como el send to receive[18], multitud de fotografías de contenido ilícito. Debemos de hacer especial referencia a la técnica de intercambio mediante correo electrónico, la doctrina ha planteado la posibilidad de imponer a los servidores de correo electrónico la práctica de un exhaustivo seguimiento en relación con el contenido que transmiten, esto sería muy complicado de llevar a cabo en la práctica, por una parte porque se estaría vulnerando el principio de intervención mínima del Derecho Penal, además de la vulneración del derecho a la intimidad del usuario, por otra parte sería imposible este control por el hecho de que la mayoría de estos servidores de correo electrónico ofrecen cuentas gratuitas con el simple relleno de un formulario, cuyos datos pueden ser totalmente falsificados.

- Los grupos de noticias y foros como medio de comunicación.
- El ocultamiento de las páginas web de pornografía infantil, no accesibles a través de buscadores y localizables únicamente por expertos en esta materia. Podemos incluir en este método el acceso en busca de este tipo de contenido a través de la llamada freenet.
- A raíz de la creación de programas de globalización de archivos individuales que permiten al usuario compartir parte del contenido de su ordenador con los sujetos que se encuentren conectados a la Red utilizando el mismo programa, por lo tanto no se entabla contacto directo ni se mantiene conversación alguna con el sujeto que originariamente tiene el material pornográfico, se convertirá de este modo en una tarea más difícil para la

[18] La expresión *send to receive* (manda y recibirás), es una técnica muy utilizada para iniciar una sesión de intercambio sin ni si quiera dar una dirección de correo electrónica o física, será habitual en esta el cambio de una foto por otra, aunque los términos se modifican cuando se intercambian vídeos, que suelen valorarse en cinco o seis fotografías cada uno. Como hemos hecho referencia anteriormente, se ha cambiado la figura del traficante por la del usuario, ya que una de las consecuencias a parte de la que hemos dicho anteriormente es que a través de estas técnicas los traficantes no pueden hacer nada más que afrontar el descenso de sus ventas, conscientes de que el material por el que recibían dinero es posteriormente intercambiado entre particulares, reduciendo significativamente su beneficio económico.

policía, la determinación del sujeto que ha enviado dicho contenido y el sujeto que lo ha recibido. Los pedófilos se sirven para lograr su cometido de varias herramientas:

a) Servidor FTP: Se trata de un programa especial que se ejecuta en un equipo servidor (siguiendo el modelo cliente-servidor[19]) normalmente conectado a Internet. Su función es permitir el intercambio de datos entre diferentes servidores/computadores que están actuando en un momento dado como servidores FTP. Este sistema ofrece la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza sin ningún cifrado estando demasiado expuestos, con lo que es posible que el material pornográfico pueda ser interceptado en este caso por la policía[20], simplemente a través del conocimiento de la IP del usuario realizando un rastreo si se conoce el servidor y se tiene constancia del contenido ilícito que podría albergar.
b) Red P2P o *peer-to-peer*, es una red que no tiene clientes ni servidores fijos, sino que está formada por una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red. Es un medio ideal para la distribución o facilitación de material pornográfico infantil, si hemos dicho que no hay ni servidores ni clientes fijos, esto querrá decir que se podrán compartir archivos ubicados en los ordenadores de usuarios de todo el mundo que se conecten a dicha red, si bien el sujeto deberá instalar antes un programa cliente como uTorrent, eMule o Ares. Podríamos hablar aquí sobre la problemática al descargar un archivo pornográfico por error, muchas veces estos archivos van camuflados bajo nombres de por ejemplo películas infantiles que provocan que el usuario que realmente quiera obtener la película se encuentre con que se ha descargado un archivo de contenido ilícito, esta conducta no sería en principio reprochable penalmente, se debería denunciar este hecho a la policía aportando todos los datos que el sujeto pueda dar, como su identidad, su domicilio, la conexión con la que se ha producido la descarga, el titular de la conexión a Internet, el nombre del archivo, el tamaño, los minutos de duración, una breve referencia a al contenido y, si es posible, el enlace ed2k[21] o el

[19] Una persona desde su ordenador invoca un programa cliente FTP para conectar con otro ordenador/servidor, que a su vez tendrá instalado el programa FTP. Una vez establecida la conexión y debidamente autenticado el usuario con su contraseña, se pueden empezar a intercambiar archivos de todo tipo.

[20] Véase el caso http://www.abc.es/hemeroteca/historico-02-04-2004/abc/Tecnologia/cuatro-detenidos-por-distribuir-pornografia-infantil-por-internet_962766538455.html

[21] El enlace ed2k, es un hiperenlace utilizado para localizar archivos dentro de la red Edonkey, en el que se conectan programas como eMule. Cada archivo que se encuentra en esta red dispone de un enlace que lo diferencia del resto de archivos disponibles. Por tanto, aunque este archivo tenga distintos nombres dentro de la red P2P, podrá ser localizado y descargado.

código hash[22], que permita solicitar la descarga sin tener que realizar el proceso de búsqueda. Lo que nunca se deberá hacer será el compartir este tipo de archivos, aunque sea únicamente para mostrar repulsa e indignación ya que estaríamos difundiendo material ilícito tipificada esta acción por tanto, penalmente. Entre enero y septiembre de 2010 la Fundación Alia2, desarrolló un programa informático llamado Florencio que rastreaba este tipo de redes para identificar los archivos que contenían pornografía infantil. En total el programa Florencio encontró 421.368 archivos de pornografía infantil, de los que Estados Unidos ocupaba el primer puesto, con 86.767 (un 21% del total), España, el segundo puesto con 47.742 (11%) y en tercer lugar, México, con 31.433 (7%).

c) Servidor web: Últimamente, el tráfico de pornografía infantil se está convirtiendo en una conducta cada vez más complicada de detectar por parte de la policía debido al uso de la llamada free-net o Internet invisible. Para poder acceder a este tipo de redes, es necesario el uso de programas como TOR, la diferencia entre una conexión por Internet visible y una conexión a través de la Internet invisible radica en la forma en que se establece dicha conexión, la primera habitualmente se realiza a través del modelo cliente-servidor donde un usuario utiliza un programa cliente (Internet Explorer, Google Chrome, Mozilla Firefox) para acceder a Internet, en este se introduce una URL de la que se interpretan una serie de peticiones a través del llamado puerto 80, el destinatario de estas peticiones será el servidor que ofrecerá la petición que el usuario ha realizado estableciéndose, una comunicación bidireccional y directa entre el servidor y el cliente, por tanto será más fácil la interceptación en un punto intermedio de las peticiones que nosotros enviamos al servidor quedando estas visibles para el sujeto que haya interceptado estos datos. En cambio, la conexión a través de la Internet invisible es totalmente diferente, hay varios modos de acceder a ella. En este caso explicaremos el modelo utilizado por el programa TOR que es el que nos interesa, este se basa en una cebolla, formada por varias capas o nodos. La petición lanzada por el cliente pasa por estos nodos que se encuentran cifrados hasta llegar al servidor final el cual se encargará de desencriptar la petición del cliente para acceder. De esta forma al pasar los datos por varios nodos siendo este camino aleatorio, la comunicación no es directa y por tanto será imposible saber qué datos se han transmitido, así como el origen o el destino, convirtiendo al usuario en totalmente anónimo. A pesar de que el programa TOR fue diseñado en principio como herramienta de ayuda a los ciudadanos de países con gobiernos demasiado entrometidos en sus vidas como herramienta de expresión garantizándoles su

[22] El código hash, es un algoritmo matemático que identifica al archivo como si fuese una huella digital. Sirve para corroborar que el contenido del archivo no ha sido cambiado por otro.

privacidad y anonimato, lo cierto es que ha dado pie con ello a otra clase de fines ilícitos como el tráfico de drogas, anabolizantes o medicamentos ilegales, la contratación de servicios a sicarios, la utilización de esta red por parte del grupo terrorista ISIS como herramienta para difundir su contenido a través de revistas, vídeos, imágenes con el fin de que captar adeptos y de que se conozcan sus fines, o el tráfico de pornografía infantil. Centrándonos en la pornografía infantil, es relativamente fácil encontrar este tipo de contenido en la red TOR a pesar de ser distinta la forma de buscar contenido respecto a los navegadores convencionales de la Internet visible, en estos el contenido se encuentra indexado[23] y puede ser buscado a través de los distintos motores de búsqueda como Google, Yahoo! , etc. En cambio, en la red TOR este proceso de búsqueda se realiza de diferente manera, el contenido no se encuentra indexado y no se pueden utilizar los motores de búsqueda tradicionales. Para realizar una búsqueda se deberá acudir a foros o páginas web de la Internet visible en el que se proporcionan enlaces con dominios .onion que serán los que nos permitirán acceder a la verdadera Internet profunda, algunos de estos enlaces actuarán como una especie de base de datos en la que se hará una recopilación y clasificación según la temática del contenido de los enlaces. Igualmente, esto no quiere decir que a la primera que accedamos a alguna de estas bases de datos encontremos fácilmente el contenido al que queremos acceder, debido a que muchos de estos enlaces se encontrarán rotos o no disponibles, habiéndose traspasado el contenido a otro enlace quizás como método de seguridad ante hackers u otras fuerzas, se necesitará además paciencia para encontrar cualquier contenido en TOR, ya que no se caracteriza por ser un servicio rápido. Pero no quiere decir que sea imposible, la mayoría de contenido pornográfico infantil se encuentra en enlaces directos .onion o en foros cerrados los cuales se necesitará para acceder una contraseña proporcionada a través del registro en el foro.

3.1.3 Otras conductas realizadas por los pedófilos

Además de las formas de difusión de pornografía infantil anteriormente nombradas, podríamos hablar de otras conductas como las grabaciones caseras o la mera tenencia de material pornográfico infantil para su uso, y la problemática de determinar la edad de la víctima o víctimas que aparecen en el contenido ilícito ya que la mayoría de este contenido ha podido ser filmado en otro país y, por lo tanto no se podrá hacer que la víctima se encuentre presente en el proceso judicial.

[23] Se refiere al proceso de recolectar y almacenar páginas web por parte de un buscador de Internet en su base de datos, con el fin de que estas aparezcan en los “resultados de búsqueda” del referido buscador.

3.1.4 Perfil del consumidor y la víctima de pornografía infantil

No existe un perfil como tal ni del consumidor, ni de la víctima, pero si podemos afirmar que algunos sujetos cumplen las siguientes características.

Se trata de personas generalmente varones de entre 25 y 50 años que han perdido interés en la pornografía tradicional y buscan nuevos estímulos inclinándose por material con escenas de violencia real, la zoofilia o la pornografía infantil aprovechándose de la gran oferta que les ofrece Internet. Son experimentados usuarios de Internet y plenamente conscientes de sus acciones.

Son personas generalmente de un poder adquisitivo medio-alto. Psicológicamente con severas dificultades para relacionarse socialmente, con poca capacidad de empatizar y sentir que los sujetos expuestos en el contenido ilícito son menores.

La gran mayoría nunca pasa de la etapa de observación, es decir su disfrute solo se da con la visualización de ese material y la satisfacción con ello de sus necesidades sexuales; por lo tanto no llegarán a la comisión de agresiones sexuales a menores. Aunque siempre existirán sujetos que rompan esta regla.

Anesvad, una ONG que trabaja contra la explotación sexual de niños y mujeres, entre otras áreas, creó una página web en la que supuestamente se ponía a la venta una muñeca hinchable con el aspecto de una niña de 12 años. Esta página fue visitada por 1.981 consumidores, en los tres meses que duró la investigación, la entidad introdujo diferentes preguntas con las que realizó una encuesta con una muestra de 168 usuarios, de la que se extrajo una serie de conclusiones:

- El 14% de los encuestados confirmó que había mantenido relaciones sexuales con menores y todos ellos señalaron que les gustaría repetir.
- Un 12% dijo que estaría dispuesto a mantener relaciones sexuales con menores.
- Un 6% afirmó buscar en este tipo de webs sexo sin límites con niños.
- En cuanto a las motivaciones, el 35% confesó que le daba mucho morbo, el 27% declaró que estas acciones le suponían algo diferente, el 20% expresó que es una forma legal y fácil de tener sexo con un menor y el 18% explicó que quería probar algo nuevo.
- El 23% manifestó su deseo de concertar una cita virtual o un encuentro real con un menor.
- El 78% de los encuestados mostró interés por adquirir la falsa muñeca hinchable.

En cuanto al perfil de la víctima, no existe uno en concreto pero sí podemos hacer una aproximación a este, generalmente provienen de países con grandes dificultades económicas, esta procedencia también dependerá del medio o vía de difusión del material pornográfico, como ejemplo podemos hacer referencia a la pornografía infantil que se difunde a través de DVD en video-clubs protagonizada normalmente por menores pertenecientes al Tercer Mundo

y Asia o a la que se difunde a través de Internet en los que estarán protagonizados normalmente por menores de nacionalidad tailandesa o procedentes de algún país asiático.

3.1.5 Dimensión del problema de la pornografía infantil en España

En España afecta tanto a niños como a niñas, especialmente a menores de 13 años. Todos los años son desarticuladas redes de explotación sexual infantil, a quienes les son incautadas miles de fotografías y videos de menores, producidos para la venta entre particulares o mediante catálogos, normalmente en países diferentes al de procedencia de las víctimas para evitar su identificación.

Como hemos comentado anteriormente gracias a un estudio de 2010 realizado por la fundación Alia2, España fue el segundo país del mundo en visitas a páginas web de pornografía infantil y el primero en Europa en consultas a cualquier tipo de páginas con contenidos pornográficos. Otro estudio internacional de 2009 situaba a España como el quinto país del mundo en contener páginas web con material pornográfico infantil, con un 3,4% sobre el total mundial. La pornografía se ha convertido en el delito informático online más denunciado, según un estudio del Observatorio Español de Internet de 2003.

La pornografía en España está muy relacionada con Internet, el 89% de los delitos usan Internet según la asociación Protégeles. En esta se indicó que, del millar de pederastas que fueron detenidos entre 2005 y 2007, únicamente una treintena acabaron cumpliendo condena.

Según la Memoria de la Fiscalía General del Estado correspondiente al año 2011, un 12,52% de los procedimientos judiciales incoados en España por conductas asociadas al uso de las TIC tuvieron por objeto delitos de pornografía infantil o en relación con personas discapacitadas y el número de acusaciones presentadas por el Ministerio Fiscal por hechos ilícitos de esta naturaleza fue de 368 en el mismo periodo anual.

3.1.6 Casuística

Para profundizar más en el tema, podríamos hacer referencia a varios casos ocurridos en España en cuanto a la pornografía infantil, tanto desde el punto de vista de la víctima como sería el caso del usuario @indignado7777[24] como desde el punto de vista del profesional perito encargado de la investigación por parte de la Policía Nacional[25]

3.2 Ciberbullying

3.2.1 Concepto de ciberbullying

[24] https://indignado7777.wordpress.com/
[25] http://conexioninversa.blogspot.com.es/

Este tipo de violencia tiene importantes consecuencias para las personas y la sociedad en su conjunto. A parte de los riesgos físicos que se sufren, las consecuencias psicológicas a veces son más graves aún que las físicas, yendo desde la depresión, abandono escolar, absentismo por miedo a acudir a la escuela hasta provocar el suicidio en los casos más graves.

El ciberbullying es una variante del ciberacoso[26], en la que "un niño, adolescente o preadolescente es atormentado, amenazado, acosado, humillado y avergonzado por otra persona desde Internet, mediante medios interactivos, tecnologías digitales y teléfonos"[27].

Por tanto, la definición de ciberbullying consta de varios elementos que deben cumplirse:

- Se trata de un acoso entre iguales, ya que tanto la víctima como el agresor serán menores de edad.
- Aunque la víctima y el agresor sean menores, existirá un desequilibrio de poder.
- Utilización del ciberespacio a través de las TIC.
- Al igual que el ciberacoso, la realización de forma repetida o reiterada en el tiempo de las conductas típica.
- La intencionalidad por parte del agresor de causar daño.
- Las conductas empleadas en este tipo de acoso, causan no como en el caso del bullying un daño físico sino más bien psicológico, a través de amenazas, vejaciones, humillaciones, etc. Independientemente de que de forma posterior el menor víctima se cause a sí mismo daño físico (autolesiones, intentos de suicidio, etc.) consecuencia del acoso sufrido.

Junto con el concepto de ciberbullying debemos hacer dos aclaraciones:

La primera aclaración es que, se ha venido discutiendo el ciberbullying como mera modalidad del bullying o de otra forma, como un fenómeno con identidad y características propias, en cuanto al tipo de agresor y víctimas. Descartaríamos esta opción ya que se dice

[26] El ciberacoso según MARCO, J.J., <<Menores, ciberacoso y derechos de la personalidad>>, en J. García González (dir.), Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet, ed. Tirant lo Blanch, 2010., sería "la amenaza, el hostigamiento, la humillación o la molestia que una persona ejerce sobre otra, haciendo uso para ello de diferentes tecnologías, como pueden ser el correo electrónico, los chats, páginas web, la telefonía móvil, las cámaras digitales, las videoconsolas, etc.".

Otros autores amplían el concepto de ciberacoso, añadiendo dos características:

PARDO, J., <<Ciberacoso: Ciberbullying, grooming , redes sociales y otros peligros>>, en J. García González (dir.), Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet, ed. Tirant lo Blanch, Valencia, 2010, p. 54., el ciberacoso iría dirigido a "un individuo o grupo de personas, a través de ataques personales u otros medios".

Según CHACÓN, A., <<Una nueva cara de Internet: el acoso>>, RE, 2003, pp. 1 y ss., el ciberacoso se trataría de una "conducta repetitiva de acercamiento, acoso y/o amenazas a otra persona".

[27] MARCO, J.J., <<Menores, ciberacoso…>>, cit., p. 56.

que a pesar de que esta modalidad comparte características con el bullying, el ciberbullying tiene una autonomía propia, ya que atiende a otras causas, se manifiesta de formas distintas y difieren además tanto sus estrategias de abordamiento y las consecuencias de estas.

Por otro lado, otros autores consideran que no es que el ciberbullying sea una modalidad del bullying sino que existen varios tipos de ciberbullying:

- El realizado en el marco de una actividad de bullying, en el que se suma el acoso presencial al ejercido posteriormente en el ciberespacio, actuando como reforzador. Se acude al ciberbullying cuando las formas tradicionales de acoso ya no son eficientes o satisfactorias para el acosador, utilizando por tanto el ciberespacio para amplificar los efectos sobre la víctima.
- El llamado ciberbullying puro, en este no existen antecedentes de una situación de bullying (acoso presencial), en esta modalidad se ejercería entre menores, en el que el agresor no conocería anteriormente de forma física a la víctima, o bien la conoce pero no ha realizado antes un sobre el ningún acto de acoso en el espacio físico.

La segunda aclaración del concepto de ciberbullying es que se excluyen tanto el acoso de índole sexual[28] como el de los casos en los que intervienen personas adultas como víctimas o como agresores[29].

3.2.2 Regulación en materia de ciberbullying

Es necesario aclarar que al ser un acoso entre iguales, tratándose en este caso de menores de edad, se debería aplicar la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores[30]. Esta nos hace alusión al Código Penal, en cuanto a que será el instrumento que deberemos tomar como referencia para castigar las conductas tipificadas como delitos o faltas[31] realizadas por los menores. Sabiendo esto, no existe el tipo penal de ciberbullying como tal, ya que se trata de un fenómeno relativamente moderno y España es uno de los países en el que menos situaciones de ciberacoso se producen (13,3%

[28] Debemos hacer una pequeña matización en este caso y es que, en muchas ocasiones se produce el ciberbullying como consecuencia de otros fenómenos, como el sexting que explicaremos posteriormente (caso Amanda Todd), empleándose en este caso las fotografías realizadas por parte de menores, de desnudos completos o partes desnudas, como medio de presión, chantaje, explotación y/o ridiculizaron contra el menor fotografiado.

[29] A este fenómeno se le denomina ciberbating, consiste en que los menores adoptarían el papel de acosadores, siendo en este caso las víctimas los profesores, que serían sometidos a injurias, vejaciones, amenazas, fotomontajes, insultos y todo tipo de burlas que, después de ser grabados con los smartphones, aparecerían en Internet, atentando contra el honor y la intimidad de las víctimas.

[30] Concretamente en el título preliminar, en su artículo 1.1 establece que, "esta ley se aplicará para exigir la responsabilidad de las personas mayores de catorce años y menores de dieciocho por la comisión de hechos tipificados como delitos o faltas en el Código Penal o las leyes penales especiales"

[31] Como vemos la Ley Orgánica 5/2010 no ha sido modificada posteriormente a la última reforma del Código Penal, de ahí que aún se haga referencia a delitos o faltas, en vez de a delitos graves y leves.

frente al 37% de Rumanía)[32], pero sí que podemos castigar algunas de las conductas típicas que se dan en el ciberbullying, como serían:

- Delitos contra la libertad: Las amenazas y coacciones.
- Delitos contra la intimidad, concretamente el descubrimiento y revelación de secretos.
- Delitos contra el honor: La calumnia y la injuria.
- Delito de torturas, uno de los elementos que se exige es que al sujeto pasivo de la conducta se le menoscabe gravemente su integridad moral, se requiere por tanto un nivel de gravedad[33], muy difícil de determinar en este tipo de casos. De todas formas, en el caso de que pueda aplicarse tendremos que tener presente la posibilidad de aplicar la regla concursal del art. 177[34], ya que los atentados a la integridad moral de una persona vienen habitualmente acompañados de la lesión de otros bienes jurídicos personales y el legislador ha querido dejar claro que el bien jurídico de la integridad moral tiene su propia autonomía[35].

3.2.3 Tipos de ciberagresiones

Las conductas de ciberbullying pueden ser muy diversas, podemos clasificarlas en varios grupos:

- Insultos directos como indirectos: El hecho de provocar a la víctima en servicios web que cuentan con una persona responsable de vigilar o moderar lo que ocurre, con el fin de conseguir una reacción violenta por parte de la víctima, que una vez denunciada o evidenciada, le suponga a esta la exclusión.
- Amenazas: Enviar mensajes amenazantes vía redes sociales o mensajería móvil.
- Excluir, aislar o ignorar: Hacerle a la víctima vacío en los foros, canales de chat o mensajería móvil con el objetivo de que se sienta incómodo o culpable.

[32] Según el II Plan Estratégico Nacional de Infancia y Adolescencia (II PENIA), en este se deja entrever la justificación de por qué no tenemos regulado como tal el ciberbullying y si otras conductas de índole sexual cometidas contra menores de edad, como puede ser el childgrooming. Es debido a que existe un mayor impacto de este tipo de conductas que no de las relacionadas con el acoso.

[33] Según el auto de la sección 5ª de la Audiencia Provincial de Madrid 3234/2010, de 24 de septiembre, el delito de torturas consiste en conductas de trato degradante, que en su individual consideración no son calificables de graves, pero que al ser reiteradas terminan menoscabando gravemente por erosión la integridad moral. […] No todas las manifestaciones de acoso tienen acomodo típico, pues tanto en el caso del mobbing como en el de bullying estas conductas pueden proyectarse en un amplio elenco de acciones y omisiones que en algunos casos no suponen, como consecuencia necesaria, la intervención penal, regida por las exigencias de tipicidad, y por los principios de lex cerca y lex estricta, teniendo presente el carácter fragmentario del derecho penal.

[34] El artículo 177 del Código Penal viene a decir, si en los delitos descritos en los artículos precedentes (delitos que atentan a la integridad moral), además del atentado a la integridad moral, se produjere lesión o daño a la vida, integridad física, salud, libertad sexual o bienes de la víctima o de un tercero, se castigarán los hechos separadamente con la pena que les corresponda por los delitos cometidos, excepto cuando aquél ya se halle especialmente castigado por la ley.

[35] MUÑOZ, J., Los delitos contra la integridad moral, ed. Tirant lo Blanch, Valencia, 1999.

- Difundir rumores sobre alguien: Hacer circular rumores en los que a la víctima se le suponga un comportamiento reprochable, ofensivo o desleal, de forma que sean otros quienes, sin poner en duda lo que leen, ejerzan sus propias formas de represalia o acoso.
- Retocar fotos o videos de alguien que estaban colgados en Internet: Colgar en Internet una imagen comprometida (real o efectuada mediante fotomontajes) que pueda perjudicar o avergonzar a la víctima y darlo a conocer en su entorno de relaciones.
- Suplantación de la identidad: Crear un perfil falso en nombre de la víctima, en redes sociales, foros o páginas de contactos, donde se escriban a modo de confesiones en primera persona, determinados acontecimientos personales o se realicen demandas explícitas de contactos sexuales.
- Subida de información personal o comprometida que afecte a la intimidad: Con intimidad nos referimos al conjunto de manifestaciones, actividades y aspectos más privados de la vida de una persona, que esta desea desarrollar y conservar de forma reservada, para que no sean conocidas por los demás[36].
- Robo de información e identidad: Dar de alta la dirección de correo electrónico en determinados sitios para que luego sea víctima de spam, de contactos con desconocidos o usurpar su clave de correo electrónico para, además de cambiarla de forma que su legítimo propietario no lo pueda consultar, leer los mensajes que a su buzón le llegan violando su intimidad.

3.2.4 Dimensión del problema del ciberbullying en España

En España la preocupación social por los actos de violencia entre iguales ha aumentado en los últimos años, sobretodo en el ámbito escolar. Ha generado tal alarma social que estos casos han estado en las portadas de los principales periódicos y telediarios, provocando con ello una mayor difusión y conocimiento del problema por parte de la sociedad. Sin embargo, España carece de un abordamiento integral de lucha contra todas las formas de violencia en la infancia, entre ellas el ciberbullying, lo cual resta eficacia a las medidas que puedan tomarse. Pese a haberse realizado diversos estudios al respecto, no se ha dado suficiente importancia a estas formas de violencia, ni se ha reconocido su gravedad. Las políticas públicas no han abordado suficientemente la realidad del ciberbullying, y cuando lo han hecho ha sido sin el necesario enfoque de derechos que requiere un asunto que implica a menores de edad tanto cuando se trate de víctimas como de perpetradores de violencia. De hecho, casi siempre las respuestas han surgido como reacción a casos de acoso grave que han tenido repercusiones mediáticas. Sin embargo las situaciones de acoso cotidianas

[36] ORTS, E., GONZÁLEZ, J.L., MATALLÍN, A., ROIG, M., VII Esquemas de Derecho Penal Parte Especial, ed. Tirant lo Blanch, 2010.

permanecen invisibles ante la falta de registro y la escasez de datos, así como la ausencia de respuestas institucionales sistemáticas.

En la línea de Atención sobre ciberbullying, dependiente del Centro de Seguridad en Internet para España del Safer Internet Programme de la Comisión Europea (Protégeles), se produjeron 435 y 363 casos durante 2011 y 2012 respectivamente. No obstante, según el estudio anteriormente citado sobre conductas adictivas, de los siete países de la UE estudiados, España es el país en el que menores situaciones de ciberbullying se producen (13,3% frente al 37% de Rumanía).

En una encuesta más reciente[37] realizada a 21.487 estudiantes entre 12 y 16 años de 1º a 4º de Educación Secundaria Obligatoria que asisten a centros educativos públicos en España, un 6,9% (un 5,8% de forma ocasional, una o dos veces y un 1,1% frecuentemente, una o dos veces al mes o más de una vez por semana) ha sufrido ciberbullying en los últimos dos meses. En cambio, un 3,7% de los estudiantes habrían sido víctimas tanto de acoso tradicional como de ciberbullying. En cuanto al sexo de los estudiantes víctimas de ciberbullying se destaca la prevalencia de victimización en chicas con un 8,3% y un 5,3% en chicos.

Haciendo referencia al tipo de conductas que se perpetran durante el proceso de ciberbullying, las más recurrentes entre estudiantes son los insultos tanto directos como indirectos, concretamente más de un tercio de los encuestados (36,3%) reconoce que alguien le ha dicho palabras ofensivas usando el móvil o Internet en los últimos dos meses de forma ocasional y uno de cada diez de forma frecuente.

Dos de cada diez estudiantes (19,2%) ha difundido rumores sobre su persona a través de Internet o el móvil, un 6,3% de manera frecuente. Un 17,9% ha recibido amenazas a través de mensajes de forma ocasional y un 5,3% frecuentemente. Un 11,8% ha sido excluido aislado o ignorado en una red social o chat. Un 8,9% afirma que le han colgado en Internet videos o fotos comprometidas sobre él o ella. Por último, un 6,3% indica que le han pirateado su cuenta y la han utilizado para suplantar su identidad a través de mensajería instantánea o redes sociales.

En cuanto al victimario que comete este tipo de conductas, el porcentaje entre el número de chicas y chicos que reconocen haber cometido algún acto de ciberbullying no se distancia mucho, concretamente un 3,5% son chicos y un 3% chicas.

3.2.5 Perfil del ciberacosador y víctima del ciberbullying

[37] CALMAESTRA, J., ESCORIAL, A., GARCÍA, P., DEL MORAL, C., PERAZZO, C., UBRICH, T., Yo a eso no juego. Bullying y ciberbullying en la infancia, ed. Save the Children, España, 2016.

En cuanto al perfil del ciberacosador o ciberbully, es el joven capaz de navegar y dominar el mundo electrónico, el que está en una posición de poder en relación con una víctima y puede utilizar las TIC para acosar a sus víctimas. No presenta un perfil único ni especialmente perturbado desde el punto de vista psicológico.

Los ciberacosadores suelen ser sujetos que no tienen una escala de valores conforme a un código moralmente aceptable y en el que se instalan sin demasiada dificultad constantes como el abuso, el dominio, el egoísmo, la exclusión, el maltrato físico, la insolidaridad. Muchos de ellos se han socializado en entornos familiares sin pautas de educación moral, con modelos de ejercicio de autoridad desequilibrados, autoritarios, inexistentes o permisivos, o, incluso, en modelos en los que los propios menores han sido la autoridad, y que han generalizado alusivamente a otras situaciones.

Como hemos dicho se encuentran en una posición de poder en relación con la víctima. Muchas características como la popularidad, la fuerza física o la imagen, la competencia social, seguridad en sí mismo, extroversión, inteligencia, edad, genero, raza, etnia y el estatus socioeconómico pueden afectar a la percepción del poder que ejerce el agresor sobre la víctima.

El autor Mason[38] indica que existen varios roles que se establecen en una situación de ciberbullying:

- Los ciberbullies proactivos o ciberacosadores por derecho: Son aquellos que creen ser superiores y tener el derecho de acosar o degradar a los demás, cometen la acción de acoso para conseguir un fin. Las víctimas de este tipo de ciberacosadores son aquellas escogidas por ellos por el simple hecho de creer que son diferentes o inferiores a los demás.
- Los ciberbullies reactivos o vengadores: Son aquellos que han sido acosados por otras personas y utilizan los medios tecnológicos para vengarse del maltrato sufrido en el pasado, agreden por tanto, como respuesta a una provocación, agresión o amenaza. Las víctimas de los vengadores son los individuos que han acosado a otros a través del bullying tradicional, y ahora reciben de su propia medicina a través del ciberespacio.

Otro punto conflictivo es el hecho de que muchas veces el ciberacoso se realiza públicamente, como son las conversaciones en grupo en aplicaciones de mensajería instantánea, donde un número de personas (más de dos) se une en una conversación para tratar un tema, en este caso muchas veces el acosador que se dedica a insultar a otro miembro no lo hace solo, se ayuda de los demás miembros del grupo que reaccionarán en contra de la víctima o a favor de esta, son los llamados espectadores, existen dos tipos; los

[38] MASON, K. L., <<Cyberbullying: A preliminary Assessment for School Personnel>>, PS, 2008.

espectadores de apoyo, son los individuos que apoyan y animan el acoso a otro compañero o los que simplemente se dedican a observar la situación de acoso y quedarse impasibles, no ayudando a la víctima. Por otro lado, tenemos a los espectadores que sin ser las víctimas del acoso tratan de detener este acoso, protestando y prestando ayuda a la víctima.

Respecto a las víctimas, gran parte de estas son menores que presentan dificultades para defender sus propios derechos, con escasa red social y pocos amigos, bajo concepto de sí mismos y con dificultades de interacción social.

También existen otros perfiles:

- El alumno seguro y brillante con el que termina metiéndose un agresor/a o un grupo, virtual o presencialmente.
- Los alumnos/as víctimas resultantes de alianzas y emparejamientos cambiantes dentro de un mismo grupo.
- El alumno/a irritante para el grupo que termina siendo objeto de sus agresiones, conocida como víctima provocativa.
- El alumno/a descolocado en el grupo que ocupa cualquier papel que se le deje con tal de ser aceptado en su seno aunque pague un precio alto por ello como ser sometido a maltrato o humillación, muy típico en los grupos de chicas.

Las formas de interacción virtual han facilitado en algunas víctimas la reacción agresiva a través de estas vías. Algunas de ellas, que no reaccionarían ante los agresores presencialmente, aprovechan la desinhibición y el supuesto anonimato que proporciona la red para canalizar sus respuestas de forma agresiva también.

3.3 Childgrooming

3.3.1 Concepto de childgrooming

El childgrooming está relacionado con la pornografía infantil, según el FBI[39] se diferencian dos tipos de pedófilos online:

- Los sujetos que coleccionan de forma anónima imágenes de pornografía infantil compartiéndolas o destinadas para uso propio.
- Los sujetos que con intenciones sexuales, buscan un encuentro cara a cara con los menores.

Este último tipo es el llamado childgrooming o ciberacoso sexual a menores, es uno de los ciberdelitos más peligrosos ya que atenta contra el derecho a la libertad e indemnidad sexual de los menores, se trata del sujeto adulto que trata de contactar con menores por medio de

[39] http://ciberdelitos.blogspot.com.es/2011/05/el-fbi-explica-el-proceso-del-grooming.html

las redes sociales o de otras formas de comunicación como salas de chat, canales de mensajería instantánea o similares, para obtener fotografías o videos de contenido íntimo, en ocasiones, con el propósito de acercarse a ellos e intentar posteriormente un contacto sexual. Así pues, el grooming abarcaría todas las conductas preparatorias (el proceso de seducción) llevadas a cabo por el abusador sexual hasta lograr el encuentro con la víctima.

3.3.2 Regulación en materia de childgrooming

El Código Penal regula de forma íntegra el delito de cibergrooming en su artículo 183 ter.[40] En este artículo castiga dos conductas:

- El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento.
- El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor.

Además el legislador prevé una agravación de la pena cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.

Hablando de la modificación que sufrió este precepto, se han realizado críticas a la nueva redacción de este ya que aunque comúnmente el legislador español se ampara en Directivas europeas para introducir cambios, existe una falta de rigor legislativo al no realizar estudios propios de una política criminal racional obedeciendo por tanto ciegamente a las directrices europeas y desconociendo el sentido o rigor de estas, a continuación haremos una comparación entre la Directiva[41] y el precepto encargado de castigar el grooming en el Código Penal:

- Diferente sujeto activo: La Directiva hace referencia al embaucamiento de menores con fines sexuales como una amenaza en el contexto de Internet, ya que este medio ofrece un anonimato sin precedentes a los usuarios puesto que pueden ocultar su identidad y las

[40] Este artículo fue reformado con la llegada de la Ley Orgánica 1/2015, de 30 de marzo, la cual reformaba el Código Penal. En esta reforma se elevó la edad en materia de consentimiento sexual de los menores, de 13 a 16 años esto fue resultado de las sugerencias que el Comité de la Organización de las Naciones Unidas sobre Derechos del nido hizo a España en esta materia, e introdujo la conducta de embaucación que el sujeto utiliza para que el menor le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca el menor en cuestión.

[41] Directiva 2011/92 del Parlamento Europeo y del Consejo del 13 de diciembre de 2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.

circunstancias personales, tales como la edad. Esta además no regula las políticas de los Estados miembros contra los actos de carácter sexual consentidos en los que puedan participar menores, añadiendo además que los Estados que hagan uso de las posibilidades que se ofrecen en la presente Directiva lo harán en el marco del ejercicio de sus propias competencias. En este caso la reforma del Código Penal plantea una extensión en el sujeto activo. Quitándole la categoría de delito especial, referido solo a adulto y ampliando a menores, desnaturalizando con ello la motivación de su introducción.

- Ausencia del elemento finalístico del delito y amplitud en el material que se solicita al menor: La Directiva establece un acto preparatorio, estableciendo solo la facilitación o suministro de pornografía infantil en la que se represente al menor. La reforma del Código Penal no define lo anterior, puesto que se penaliza la conducta del sujeto que realice actos dirigidos a embaucar a un menor para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca dicho menor.
- No existe la penalización de conductas cara a cara o el llamado grooming tradicional: La Directiva en su artículo 19 hace referencia tanto al embaucamiento a través de las nuevas tecnologías como al realizado al margen de estas. En cambio en el artículo que regula el Código Penal sobre esta materia no existe ni una referencia al grooming tradicional[42], dándole más importancia al realizado a través del ciberespacio, un error, puesto que el grooming tradicional es el más peligroso.
- Exigencia de actos dirigidos a embaucarle para que se configure el delito: El artículo 183.2 ter. exige que el sujeto activo realice actos dirigidos a embaucar al menor. En el texto de la Directiva en inglés se hace referencia a “solicitation for sexual purposes” en cambio en la versión de la Directiva traducida al español se hace referencia al “embaucamiento del menor”. El término “solicitation"[43] y “embaucamiento”[44] como podemos comprobar no significan lo mismo.

3.3.3 Dimensión del problema del childgrooming en España

Según un estudio[45] realizado el riesgo de grooming es uno de los que presenta menores tasas de incidencia reconocida en comparación con otros riesgos, con las cifras que ofrecen otras fuentes y con la repercusión mediática de estas situaciones. Más de la mitad de los

[42] El grooming tradicional según MIRÓ, F., El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. cit, p. 99., consiste en la propuesta realizada por parte de un pedófilo sobre un menor de doce años existiendo un contacto directo y no virtual entre ellos.

[43] Según http://dictionary.cambridge.org/es/diccionario/ingles/solicitation El término “solicitation” significa: A request for money, information, or help. Es decir, una petición de dinero, información o ayuda.

[44] El término embaucar sin embargo según http://www.rae.es/ significa: Engañar o alucinar, prevaliéndose de la inexperiencia o candor del engañado.

[45] Guía de actuación contra el ciberacoso. Ministerio de Industria, energía y turismo en colaboración con red.es.

padres y menores entrevistados son conscientes de que existe el riesgo de sufrir acoso sexual en el uso de las TIC, y son más los padres que los hijos lo que manifiestan conocer la amenaza. Existiendo un nivel del conocimiento del peligro más alto entre las niñas (62,2%) que entre los niños (39,7%). El 60% de los padres consideran de mucha o bastante gravedad si les ocurriese una situación de este tipo.

Un 2,1% de los padres y un 1,3% de los hijos afirman que los menores han estado expuestos a situaciones que consideran como grooming o acoso sexual.

En este estudio se destaca la divergencia entre las opiniones de padres e hijos siendo más estricta en el caso de los padres y menos en la de los hijos indicando por tanto la diferencia de percepciones entre unos y otros en cuanto a qué se considera acoso sexual.

3.3.4 Perfil del childgroomer y de la víctima de childgrooming

Con la llegada de Internet se ha cambiado considerablemente el perfil del childgroomer, han aumentado las posibilidades de que potenciales abusadores sexuales lleguen a serlo, incrementando con ello el número de posibles víctimas.

Los estudios de profiling criminológico de los ciberdepredadores sexuales aseguran que el perfil del agresor en el ciberespacio es significativamente distinto, e incluso como ya mencionamos anteriormente desde una perspectiva preventivo-especial, menos peligroso, que el del abusador sexual clásico o tradicional. Según YOUNG[46], a diferencia del depredador tradicional que suele llevar a cabo sus ataques contra niños como forma de auto-gratificación, debido a una necesidad de ejercer poder, dominio, control o rabia, sin ser consciente en ningún momento del daño infligido, el ciberabusador que realiza conductas de grooming en los chats deriva sus fantasías sexuales de los desórdenes psicológicos motivados por la necesidad de escapar de la soledad, de la dificultad de las relaciones personales, de su baja autoestima, por lo que sí es consciente del significado de su conducta y del daño que puede infligir. Por tanto estableciendo una comparación psicológica entre los agresores sexuales clásicos y los agresores online, estos últimos tendrán mayor nivel de empatía con las víctimas, menor índice de desviación sexual y menos distorsión cognitiva que los agresores sexuales clásicos. Implicando por tanto que para un ciberagresor será más difícil acabar cometiendo el ataque sexual, que para el agresor sexual tradicional, dado que el primero tiene más mecanismos inhibitorios, un mayor autocontrol y menor impulsividad, que este último[47].

[46] YOUNG, K. S., <<Profiling online sex offenders, cyber-predators, and paedophiles>>, JBP, 2005.
[47] BABCHISHIN, K. M., HANSON, R. K., HERMANN, C. A., <<The characteristics of online sex offenders: a meta-analysis>>, SA, 2011.

Es importante saber que el sujeto que utiliza Internet para molestar y hacer proposiciones a menores no es generalmente un pedófilo, puesto que sus objetivos no son niños, sino adolescentes, en general, y chicas que ya han tenido experiencias sexuales y que estén dispuestas a tenerlas, en particular. El objetivo por tanto y que se relaciona con la cuestión de la edad desde la que se debe sancionar el delito[48], no será tanto el abusar de menores de dieciséis años, como el mantener relaciones sexuales consentidas con menores de edad de dieciséis a dieciocho años.

En cuanto al perfil de las víctimas de childgrooming, un estudio[49] indica que son más las chicas victimizadas por este tipo de conductas que los chicos, concretamente un 60% y un 40% respectivamente. En cuanto a la edad no parece ser determinante a efectos de victimización por grooming, muestra de menores comprendida entre 14 y 18 años. Siendo cierto que el grupo mayoritario de víctimas se concentra en los 15 y 16 años. Generalmente resultan más victimizados los menores a través del empleo del móvil que del empleo de otro tipo de aparato, como el ordenador fijo o el portátil. La mayor parte de las víctimas del estudio se conectan a Internet en su habitación, frente a las 44% que lo hacen en estancias comunes, no es así cuando el grooming escala hasta pedir al menor que realice alguna conducta sexual que no quiera, en que el 69,2% de las víctimas se conecta habitualmente en zonas comunes.

Por otro lado, la víctima del childgrooming es normalmente seleccionada por el abusador[50], quien busca a los menores más débiles, especialmente aquellos con vulnerabilidades relacionadas con la incomprensión familiar o social como son al tratarse de menores con necesidades especiales y problemas de aprendizaje, menores en entornos familiares muy conflictivos donde hay un traumático proceso de separación, donde la madre está enferma o tiene problemas con las drogas, o también menores solos sin un entorno familiar protector, para centrar en ellos el ataque.

3.3.5 Fases del childgrooming

Dividiremos la actuación del childgroomer en varias fases:

1. Fase de inicio: El childgroomer se registrará en una red social frecuentada por adolescentes, generalmente con una identidad falsa aparentando una edad similar a la media de los menores usuarios de la red.

[48] Actualmente la edad de consentimiento sexual se encuentra en dieciséis años. Se elevó de catorce a dieciséis con la última reforma del Código Penal.
[49] ESTIARTE, V. C., ADILLÓN, Mª. J., <<Nuevas tecnologías y victimización sexual de menores por online grooming>>, RECPC, 2016, pp. 1-27.
[50] MCALINDEN, A. M., <<Setting "Em Up": Personal familiar and Institutional Grooming in the sexual Abuse of Children>>, SLS, 2006, pp. 339 y ss.

2. Fase de contacto: El childgroomer contactará con los menores y seleccionará a los que vea más vulnerables.
3. Fase de ganancia de confianza: El childgroomer se irá ganando la confianza del menor, comenzando a obtener fotografías y datos personales de este como la edad, domicilio, si sus padres están cerca cuando navegan por Internet y otros datos que posteriormente servirán para el chantaje o la sextorsión.
4. Fase de seducción: El childgroomer enviará al menor imágenes con contenido pornográfico de otros menores con la finalidad de convencerle de que se trata de algo normal para que la víctima acceda a desnudarse delante de la webcam y/o que se hagan fotografías o videos mostrando las partes íntimas.
5. Fase de chantaje o sextorsión: Una vez que el childgroomer obtenga las imágenes del menor, exigirá que le envié nuevo material con contenido sexual e incluso planteará un encuentro físico con el menor para abusar sexualmente de este. Para conseguirlo utilizaran en algunos casos cualquier tipo de amenaza, coacción o engaño, sirviéndole de ayuda toda la información que ha recabado del menor en las anteriores fases. Es habitual que amenace con publicar el material obtenido de la víctima en las redes sociales donde esta puede ser reconocida e incluso mandar este material a otros contactos, o informar a los padres de la víctima sobre lo que ha hecho su hijo/a con el fin de atemorizarle y que acceda a sus peticiones. Algunos childgroomers llegan hasta a amenazar al menor con causar daño físico a sus familiares.

3.4 Sexting

3.4.1 Concepto de sexting

Se trata de la realización, por parte de menores, de fotografías propias de desnudos completos o parciales y su envío, normalmente por medio del teléfono móvil, a otros, junto con textos obscenos y con la finalidad de conocer personas o de enviar mensajes de amor o de odio[51]. Distinguiremos dentro del sexting dos tipos de conductas:

- Sexting activo: Realización de autofotos/videos en una postura sexy, provocativa o inapropiada.
- Sexting pasivo: Recepción de fotos/vídeos de personas del entorno en una postura sexy, provocativa o inapropiada.

Para que se dé un caso de sexting se deben cumplir una serie de requisitos[52]:

[51] LENHART, A., <<Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging.>>, PIALP, 2009.
[52] Guía sobre adolescencia y sexting: qué es y cómo prevenirlo. Observatorio de la seguridad de la información. INTECO, PANTALLAS AMIGAS, 2011.

- Voluntariedad del sujeto: Generalmente esta conducta se realiza de forma voluntaria o bajo el consentimiento del protagonista ya que son contenidos creados como regalo para su pareja, utilizados como herramienta de flirteo, realizados simplemente por diversión o para impresionar a alguien, no es necesaria por tanto la coacción ni la sugestión para el envío del contenido. El propio protagonista será el productor de los contenidos y el responsable del primer paso en su difusión.
- Empleo de las TIC: Se requiere la utilización de dispositivos tecnológicos como son el teléfono móvil o la webcam para la existencia y difusión del sexting, facilitando de este modo su envío a otras personas; haciendo incontrolable su uso y redifusión a partir de ese momento.
- Contenido sexual: Para que exista una situación de sexting el contenido del posado enviado por el protagonista debe ser sexualmente explícito. Quedarán fuera del ámbito del sexting las fotografías enviadas que simplemente resultan atrevidas o sugerentes. Resultando muchas veces complicado discernir la línea que separa la carga erótica o sexual de un contenido atrevido o sugerente.
- Edad: Las conductas del sexting pueden realizarlas tanto adultos como menores, en este caso nos interesan las cometidas por menores ya que concurren una serie de circunstancias que exigirán un tratamiento especial desde el punto de vista jurídico.

Como vemos, el peligro no se encuentra en el envío de contenido como tal si no en que esta conducta puede provocar la difusión de manera muy fácil y amplia, de forma que el remitente inicial pierde totalmente el control sobre la difusión. Por tanto, el sexting no deviene exclusivamente de la propia violación del proceso de formación de la sexualidad, sino más bien de la utilización posterior de las imágenes para otros ataques más graves y para los que ya no habrá consentimiento. El sexting puede ser perfectamente el primer paso para posteriores conductas como el ciberbullying, un abuso o corrupción del menor o la exposición a un chantaje sexual relacionado con el grooming. Además la difusión a terceros de las imágenes pueden desencadenar en conductas de pornografía infantil e incluso suponer una presión de tal magnitud en el menor que se ha relacionado con conductas de intento de suicidio y suicidio consumado. Y no siempre el que realice esas conductas será un menor, sino que es perfectamente posible que sea ya un adulto quien acceda a ellas y las utilice con ánimo delictivo.

3.4.2 Modalidades conductuales del sexting

Según LEARY[53] existen varios comportamientos en el sexting:

[53] GRAW, M., <<Sexting or Self-Produced Child Pornography? The Dialogue Continues. Structured Prosecutorial Discretion within a Multidisciplinary Response>>, VJSPL, 2010.

- El menor que manda una imagen a alguien importante para él.
- El menor que hace y/o distribuye imágenes de sí mismo y otros participando en conductas sexuales explícitas.
- El menor que transmite o difunde una imagen desnuda de otro joven sin su conocimiento.
- El menor que publica dichas imágenes en un sitio web.
- El adolescente mayor que pide o coacciona a otro joven por tales imágenes.
- La persona que se hace pasar por un compañero de clase para engañar y chantajear a otros para que le envíen imágenes.
- Los adultos que envían fotos o videos a menores de edad o poseen imágenes sexualmente explícitas de menores de edad.
- Adultos que envían mensajes de texto con imágenes sexualmente sugerentes a otros adultos.

3.4.3 Regulación en materia de sexting

En España la figura específica del sexting no se encontraba regulada en el Código Penal. Por tanto, para castigar esta conducta era preciso recurrir a figuras de diferentes delitos en función de la casuística que se diese en cada situación. Con la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal se ha añadido algo parecido[54] a la figura delictiva del sexting[55], se encuadra dentro del Título X referente a los Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio concretamente el articulo 197.7[56], en este se exigen una serie de requisitos para castigar la conducta:

[54] En el artículo 197.7 del Código Penal en ningún punto se exige que el contexto de la difusión sea sexual.

[55] Según el punto XII del Preámbulo de la Ley Orgánica 1/2015, de 30 de marzo, "se modifican los delitos relativos a la intromisión en la intimidad de los ciudadanos, con el fin de solucionar los problemas de falta de tipicidad de algunas conductas. El vigente artículo 197 contempla como delito, por un lado, el apoderamiento de cartas, papeles, mensajes de correo electrónico o cualesquiera otros documentos de naturaleza persona de la víctima y, por otro lado, la interceptación de cualquier tipo de comunicación de la víctima, sea cual fuere la naturaleza y la vía de dicha comunicación interceptada. Ambas conductas exigen la falta de consentimiento de la víctima. Por tanto, los supuestos a los que ahora se ofrece respuesta son aquellos otros en los que las imágenes o grabaciones de otra persona se obtienen con su consentimiento, pero son luego divulgados contra su voluntad, cuando la imagen o grabación se haya producido en un ámbito personal y su difusión, sin el consentimiento de la persona afectada, lesione gravemente su intimidad".

[56] Este artículo castiga "el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquella que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad persona de esa persona.

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa".

- Falta de autorización de la persona afectada, en este caso la víctima o el sujeto pasivo del delito. El tipo penal especifica que las imágenes o grabaciones hayan sido obtenidas con la anuencia, es decir con el consentimiento de la propia víctima, lo que no da derecho a la libre difusión de dicho material por parte del sujeto activo.
- Se exige la existencia de una difusión, revelación o cesión de esas imágenes o grabaciones audiovisuales a terceros, haciendo referencia a las nuevas tecnologías empleadas a este fin, como es a través de Internet, email, SMS y aplicaciones de mensajería instantánea.
- Que la divulgación de esas imágenes o grabaciones audiovisuales menoscaben gravemente la intimidad personal del sujeto afectado.

Además se contemplan una serie de agravaciones en la pena, en el caso de que:

- Los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia.
- La víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección.
- Los hechos se hubieran cometido con una finalidad lucrativa.

Como hemos dicho anteriormente, el sexting puede ser la puerta de entrada a conductas como el ciberbullying, un abuso (art. 183 del CP) o corrupción del menor (art. 189 del CP) o la exposición a un chantaje sexual relacionado con el grooming (art. 183.2 ter. del CP). Pudiendo llegar al límite de desencadenar en conductas de pornografía infantil (art. 189 del CP) e incluso provocar en la víctima menor conductas de intento de suicidio y suicidio consumado (art. 143 del CP).

3.4.4 Dimensión del problema del sexting en España

El fenómeno del sexting comienza a tener una repercusión importante en España. En el año 2011 se realizó un estudio[57] en el que se extraen resultados importantes:

Respecto al sexting activo, un 69,2% no conoce el riesgo que conlleva, frente a un 30,8% que sí que lo conoce. En cambio haciendo referencia al sexting pasivo, un 61,0% declara que no conoce la existencia de riesgo, con respecto a un 39,0% que sí que lo conoce. Por tanto, los menores son más conscientes de los riesgos asociados al sexting pasivo que al sexting activo (39,0% frente a un 30,8%).

El conocimiento del sexting activo como el pasivo se incrementa con la edad. El 14,4% de los menores de 10 a 12 años conoce el riesgo existente en el hecho de hacerse fotos o videos

[57] Estudio sobre hábitos seguros en el uso de smartphones por los niños y adolescentes españoles. Observatorio de la Seguridad y de la Información. INTECO, ORANGE, 2011.

en posturas provocativas (sexting activo), conocimiento que se eleva hasta llegar al 40,8% entre los menores de 15 a 16 años. Igualmente el 23,4% de los menores de 10 a 12 años conoce el riesgo de recibir fotos o videos provocativos de chicos o chicas de su entorno (sexting pasivo), alcanzando el 52,9% entre los adolescentes de 15 a 16 años.

El sexting activo es más practicado por chicas (2,2%) que por chicos (0,9%). Ocurre lo contrario cuando hablamos del sexting pasivo los chicos (5,1%) reciben más fotografías de carácter sexual de personas conocidas que las chicas (3,3%).

La realización de estas conductas se incrementan con la edad. Así, el 0,9% de los menores de 10 a 12 años reconoce hacerse fotos o videos en posturas provocativas o sexualmente inapropiadas, llegando al 2,5% entre los menores de 15 a 16 años. En el sexting pasivo, es reconocido por el 3,6% de los menores de 10 a 12 años y alcanza el 6,4% entre los menores de 15 a 16 años.

El conocimiento por parte del menor de otras personas de su entorno que realizan este tipo de conductas (incidencia indirecta) es mayor que las conductas realizadas por los propios menores encuestados (incidencia directa). Mientras que el 1,5% reconoce haber practicado sexting activo, el 13,8% afirma que conoce a personas de su entorno que lo practican. Frente a un 4,3% que reconoce haber recibido fotos o videos provocativos de chicos o chicas de su entorno, el 16,5% declara conocer casos de este comportamiento entre sus amigos y compañeros.

3.4.5 Factores que propician el sexting

Para entender el fenómeno del sexting podemos hacer referencia a varios factores que propician su aparición[58]:

- Falta de cultura de la privacidad: El menor no percibe amenaza alguna contra su privacidad, ni es consciente de las implicaciones que sus conductas pueden conllevar desde el punto de vista de la seguridad. No ven riesgos en la exposición de datos personales, privados e íntimos, a través de las TIC, y por ellos los difunden. Colocándose a sí mismos en una situación de vulnerabilidad, ya que ese contenido puede llegar a ser difundido y consecuentemente ser conocido de forma masiva.
- Necesidad de reconocimiento y sentido de pertenencia: Realizan este tipo de conductas para tratar de encajar socialmente, a pesar de no tener experiencia ni poder medir el impacto de sus acciones, actuando sin consultar a nadie.

[58] MARTÍNEZ, J. M., BOO, A., El fenómeno del sexting en la adolescencia: descripción, riesgos que comporta y respuestas jurídicas, Universidad CEU - Cardenal Herrera.

- Adolescencia: etapa de despertar sexual: Los adolescentes son más propensos a situaciones de sobreexposición en temas sexuales, especialmente en el entorno cercano entre iguales, ya que son quienes consideran importantes para su definición (necesidad de autoafirmación y definición sexual) y encaje social o pertenencia a un grupo.
- Inmediatez de comunicaciones: Muchas de las características de las nuevas tecnologías como son la disponibilidad, omnipresencia, sencillez, portabilidad, potencia o inmediatez, facilitan que un impulso inmediato de los menores pueda convertirse en una realidad imposible de revertir. Este factor puede afectar a cualquier grupo de edad, pero entre los adolescentes su incidencia es mayor, debido a que por su madurez son menos propensos a controlar sus impulsos y a actuar con prudencia. Provocando las ventajas de las nuevas tecnologías en potenciales riesgos para los adolescentes.
- La brecha tecnológica: Este término hace referencia al desconocimiento existente entre las generaciones sobre el uso de las tecnologías. Desencadenándose con ello la incapacidad de los padres para enfrentarse a situaciones de este tipo frente a las que no tienen conocimientos suficientes, no pudiendo aconsejar a sus hijos menores porque no comprenden a fondo la problemática deriva de un uso inapropiado de las tecnologías.

3.5 Ciberstalking

3.5.1 Concepto de ciberstalking

El ciberstalking sería el uso de Internet u otra tecnología de comunicación para hostigar, perseguir o amenazar a la víctima menor[59]. Anteriormente a la expansión de las nuevas tecnologías ya se hacía referencia al término stalking como las conductas obsesivas dirigidas a esperar a la víctima todos los días en un lugar, en llamar repetidamente por teléfono cuando se tiene consciencia de que se encuentra en casa, el envío de regalos, cartas, la escritura del nombre de esta en lugares públicos y, en casos más extremos las amenazas y la comisión de actos violentos contra ella. Estas conductas en el ciberstalking se sustituyen por el envío de decenas de correos o de mensajes de acoso, amenaza, odio, obscenos o incluir imágenes hirientes a través de las redes sociales, la puesta a disposición del público de fotos, mensajes o correos de la víctima en páginas web, instar a otros usuarios de Internet a acosar o amenazar a la víctima mediante foros o chat, enviar archivos infectados con la intención de dañar el sistema informático de la víctima y el robo de identidad siempre que el objetivo del agresor sea intimidar a la víctima.

[59] BASU, S., JONES, R., <<Regulating Cyberstalking>>, JILT, 2007, p.13.

Muchos autores se plantean si el ciberstalking es una extensión del stalking tradicional o si debe ser entendido como un fenómeno diferente. Los autores que se encuentran a favor[60] de que estos términos son completamente diferentes argumentan:

- Porque los gobiernos y los medios de comunicación así lo entienden.
- Hay ciberacosadores que no podrían acosar en el mundo físico.
- Porque las nuevas tecnologías traerán siempre nuevos delitos.
- Se hace referencia a la proximidad física entre víctima y victimario. En el stalking tradicional agresor y víctima deben estar en el mismo espacio físico, en el ciberstalking no es necesario.
- Factor tiempo relacionado con la proximidad, en el stalking la conducta se realiza de forma simultánea cuando existe proximidad, en cambio en el ciberstalking el tiempo de comisión puede ampliarse, ya que el agresor puede enviar un mensaje amenazante pero pueden pasar varios días hasta que la víctima lo lea.
- Los llamados elementos de protección eficaz, son cualquier medio del que dispone una persona con el objetivo de protegerse contra uno o varios riesgos que puedan amenazar a su integridad, tanto física como psíquica. En este caso los elementos de protección eficaz serán diferentes dependiendo de si se da un caso de stalking o de ciberstalking. En el stalking existen elementos tanto físicos como sociales que actúan como sistema de seguridad como el hogar, los amigos y los familiares, mientras que en el ciberstalking la seguridad viene dada por elementos electrónicos como cortafuegos o las conductas de autoprotección realizadas por la víctima, como no hacer publica determinada información o privatizar las cuentas en las redes sociales.

En contraposición, se dan argumentos en contra[61] de que el stalking y el ciberstalking sean conductas diferentes:

- El proceso de acoso es el mismo, tanto en el stalking como en su modalidad cibernética.
- El efecto sobre las víctimas y terceros es similar.
- Ambos procesos vienen alimentados por la rabia, el poder, el control y la ira.

3.5.2 Regulación en materia de ciberstalking

[60] MCFARLANE, L., BOCIJ, P., <<An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers>>, FM, 2003.
Autores como: BOCIJ, P., <<Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet>>, FMPRJI, 2003., o BOCIJ, P., MCFARLANE, L., <<Seven fallacies about ciberstalking>>, PSJ, 2003.
[61] Argumentos dados por autores como SHERIDAN, L., GRANT, T., <<Is cyberstalking different?>>, PCL, 2007., o PITTARO, M. L., <<Cyberstalking: An Analysis of Online Harassment and Intimidation>>, IJCC, 2007.

Anteriormente la conducta de ciberstalking no se contemplaba en el Código Penal, con la entrada de la Ley Orgánica 1/2015, de 30 de marzo, por la que reforma el Código Penal, esto ha cambiado. Se introduce un nuevo tipo penal de acoso o ciberstalking, es el art. 172 ter.[62]. En la exposición de motivos de esta Ley define este tipo de conductas como "todos aquellos supuestos en los que, sin llegar a producirse necesariamente el anuncio explícito o no de la intención de causar algún mal (amenazas) o el empleo directo de violencia para coartar la libertad de la víctima (coacciones), se producen conductas reiteradas por medio de las cuales se menoscaba gravemente la libertad y sentimiento de seguridad de la víctima, a la que se somete a persecuciones o vigilancias constantes, llamadas reiteradas u otros actos continuos de hostigamiento". El precepto engloba conductas como vigilar, contactar y atentar contra la libertad o el patrimonio, por lo que también se pueden tener en cuenta conductas realizadas por el acosador con el fin de lograr la vigilancia y seguimiento de la víctima, como sería el realizado vía GPS, programas localizadores en PC's y smartphones, cámaras especiales y cualquier tecnología dirigida a la consecución de este fin.

Para que este delito sea castigado se exige una serie de requisitos:

- Estos hechos solo serán perseguibles mediante la denuncia de la persona agraviada o de su representante legal.
- Esta conducta debe ser una acción que no debe estar legítimamente autorizada por la víctima.
- Se debe demostrar que estas conductas han alterado la vida cotidiana de la víctima, el acoso es un delito de resultado.
- Se ha de demostrar que el acoso es reiterado e insistente conllevando con ello una situación de desgaste y angustia por parte de la víctima.

3.5.3 Perfil del ciberstalker y de la víctima de ciberstalking

Los ciberstalkers suelen ser hombres, con una edad media de 41 años aunque el rango de edad puede variar de 18 a 67 años. La mayoría suelen estar solteros aunque también se

[62] Este artículo se encuentra en el título VI que engloba los delitos contra la libertad, en el capítulo III referido a las coacciones. En él se castiga al que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

1ª La vigile, la persiga o busque su cercanía física.
2ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.
3ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.
4ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se agravará la pena.

pueden dar en menor medida casos de agresores casados. Suelen tener conocimientos informáticos. Respecto a la ocupación laboral suelen ser estudiantes.

Se trataría de una persona fría, con poco o ningún respeto por los demás. Es un depredador que puede esperar pacientemente conectado a la red, participar en chats o en foros hasta que entabla contacto con alguien que le parece susceptible de molestar, en este caso menores; y que disfruta persiguiendo a una persona determinada, ya tenga relación directa con este o sea un completo desconocido. Sintiéndose en una posición de poder desde el anonimato, se encargará de recabar toda la información posible proveniente de la víctima para iniciar posteriormente su acoso. Su motivación para el acoso girará en torno al acoso sexual, la obsesión amorosa, el odio o la venganza.

Se pueden clasificar en cuatro tipos[63]:

- El ciberstalker vengativo: Es el tipo más violento que generalmente presenta antecedentes delictivos. Suele tener un nivel alto de manejo de las tecnologías y usa una amplia gama de métodos para acosar a sus víctimas como será el envío de correos masivos, troyanos, el robo de identidad, etc. Podrían presentar este tipo de ciberstalkers algún tipo de enfermedad mental debido al tipo de mensajes que envían a sus víctimas.
- El ciberstalker integrado: A diferencia del ciberstalker vengativo no suelen tener antecedentes delictivos ni padecer ninguna enfermedad mental. Tienen como objetivo molestar e irritar a sus víctimas sin intención de mantener algún tipo de relación sentimental con ellas. Presentan un nivel alto de manejo de Internet.
- El ciberstalker íntimo: El nivel de manejo de Internet de este tipo varía desde el que apenas tiene conocimientos hasta el que tiene conocimientos altos. Tienen como objetivo establecer una relación íntima con sus víctimas y el medio que suelen contactar con ellas es el correo electrónico y las webs de citas.
- El ciberstalker colectivo: Se trata de cuando dos o más personas se unen para acosar a una misma víctima a través de medios tecnológicos. Este tipo de agresores se caracterizan por tener conocimientos amplios de informática y de emplear técnicas muy variadas para acosar a sus víctimas.

En cuanto a la víctima, la población que tiene más probabilidad de sufrir ciberstalking son las mujeres al igual que los menores porque se encuentran constantemente conectados a una variedad de medios electrónicos para comunicarse. Curiosamente la víctima más probable será el agresor. Ya que es el que realiza más comportamientos desviados por Internet como contactar con alguien en repetidas ocasiones cuando le han pedido que pare, acosar o molestar a alguien por Internet, solicitar sexo a alguien que no quiere, amenazar por Internet,

[63] MCFARLANE, L., BOCIJ, P., <<An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers>>, FM, 2003.

descargar música o películas piratas y enviar o recibir imágenes de contenido sexual, es decir realiza más conductas de riesgo que pueden llegar a la propia victimización. Como vemos las actividades cotidianas realizadas en el ciberespacio pueden ser predictores significativos de la victimización.

4 La prevención como pilar fundamental

4.1 El papel de las Fuerzas y Cuerpos de Seguridad del Estado

A nivel policial, tanto la Guardia Civil como el Cuerpo de Policía Nacional trabajan a través de determinados grupos especiales como son el Grupo de Delitos Telemáticos y la Brigada de Investigación Tecnológica, respectivamente. Colaboran además con la Europol y la Interpol a la hora de la desarticulación de grandes redes internacionales dedicadas a este tipo de delitos. Una de ellas fue la denominada Operación Carrusel realizada en colaboración con la Policía Federal de Brasil entre 2007 y 2008 en la que se localizaron más de 18.000 conexiones en 75 países diferentes, motivando a la Brigada de Investigación Tecnológica a que centrase sus pesquisas en España a través de 1.600 conexiones P2P que intercambiaban archivos clasificados como pre-teen o pre-teen hard core, como resultado se realizaron 210 registros a domicilios en 42 provincias, incautando en ellos 347 discos duros, 1.186 CDs y DVDs, 36 ordenadores portátiles, dos cintas VHS y siete tarjetas de almacenamiento, produciéndose la detención de 121 y la imputación de otras 96 personas por tenencia y distribución de material pedófilo en Internet.[64]

Otra operación más reciente a nivel estatal fue la macro operación realizada por la Brigada de Investigación Tecnológica en la que se realizaron un total de 80 registros domiciliarios incautando 96 discos duros, 58 ordenadores, 68 pendrives, cuatro tabletas, 195 CDs y DVDs, 18 teléfonos móviles, 25 tarjetas de memoria, una consola, un MP4, una videocámara y dos cámaras fotográficas, saldándose con la detención de 82 personas por intercambiar a través de Internet mediante las redes P2P, vídeos y fotografías sexuales protagonizadas por menores de edad.[65]

Podemos preguntarnos como actúa la policía para intervenir este contenido, puede realizarlo a través de tres actuaciones:

- El rastreo o ciberpatrullaje en la que se vigilan continuamente diversos canales de intercambio de archivos, entre ellos las redes P2P. Los agentes ejecutan su versión de eMule y leen metadatos públicos existentes en este tipo de redes.
- La interceptación de comunicaciones a través de programas como SITEL (Sistema Integrado de Interceptación Telefónica), es uno de los numerosos sistemas existentes

[64] Noticia extraída de http://elpais.com/elpais/2008/10/01/actualidad/1222849019_850215.html
[65] Noticia extraída de http://www.policia.es/prensa/20151017_1.html

para el control de las comunicaciones telefónicas, permiten a parte del acceso a datos como las llamadas, posicionamiento, uso de terminales, localización, determinación de la identidad, contenido de las conversaciones o los mensajes SMS, también permiten acceder a los mensajes de correo electrónico cuando se envían desde un ordenador a otro y el conocimiento de las páginas de Internet y la hora en que un usuario las ha visitado. Para ello se requerirá autorización judicial ya que el artículo 18.3 de la Constitución Española garantiza el secreto de las comunicaciones.

- Troyanizar, con la Reforma del Código Penal de 2015 y de la Ley de Enjuiciamiento Criminal se permitirá a los agentes la instalación remota de programas espías, requiriendo para ello autorización judicial.[66]

Podemos añadir a estas actuaciones la figura del agente encubierto informático en el que podrá bajo una identidad supuesta, intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de estos archivos, todo ello con la correspondiente autorización judicial y en comunicaciones que se mantengan en canales cerrados de comunicación como pueden ser los chats, foros cerrados ubicados en la freenet, etc.[67] Con el objetivo precisamente, de acceder a los ámbitos ocultos y más difíciles de acceder donde tienen lugar los intercambios de contenidos más violentos y graves.

4.2 El papel de los proveedores de servicios de Internet

Un proveedor de servicios de Internet es una compañía que ofrece acceso a Internet, normalmente pagando una cuota económica. Muchos de estos proveedores ofrecen servicios adicionales como son cuentas de correo electrónico, exploradores web y espacios para crear un sitio web propio.

En la lucha contra la lacra de la pornografía infantil estos proveedores juegan un papel muy importante, y es que es donde se encuentran la mayoría de material con contenido ilícito y donde se cometen la mayoría de delitos relacionados con la pornografía infantil, como hemos

[66] El artículo 588 septies a. de la Ley de Enjuiciamiento Criminal dice, el juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telepática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:

a) Delitos cometidos en el seno de las organizaciones criminales.
b) Delitos de terrorismo.
c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.
e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

[67] Artículo 282 bis. de la Ley de Enjuiciamiento Criminal.

dichos anteriormente, en concreto el 89% en España. Estos proveedores por lo tanto, con el objeto de evitar la circulación de este tipo de contenido por Internet, deberán:

- Profundizar en la actuación referente al bloqueo de acceso al usuario y la retirada de este tipo de contenido.
- Colaborar activamente en la detección, información rápida a las Fuerzas y Cuerpos de Seguridad y la retirada de dicho contenido.

En este aspecto, se realizó una cumbre respaldada por el Primer Ministro del Gobierno Británico el 18 de noviembre de 2013, con los principales proveedores de servicios de Internet, para promover tanto el bloqueo del acceso a contenidos de pornografía infantil y su retirada, como el bloqueo a contenidos nocivos. Como resultado de esta cumbre, Google y Microsoft introdujeron cambios en sus motores de búsqueda a escala mundial, para impedir que el uso de determinados términos (hasta un total de 100.000 combinaciones) pueda conducir a imágenes de pornografía infantil. Google anunció que los cambios se irían introduciendo en 159 lenguas en un período de 6 meses. Esta iniciativa entre estas dos compañías comprende también la introducción de mensajes de advertencias claves que aparecerán siempre que alguien utilice una de las 100.000 combinaciones de términos incluidas en la lista negra, informando al usuario de las consecuencias de sus acciones y remitiéndole a organizaciones de ayuda, así como cambios en la función de predicción de textos para evitar sugerencias que conduzcan a búsquedas relacionadas con la pornografía infantil.

Microsoft por su parte desarrolló la herramienta PhotoDNA consistente en la creación de identificadores que permiten retirar las imágenes de abuso de menores y cualquier copia de las mismas en todo Internet, esta tecnología ha sido aceptada para compartirse por otras compañías.

4.3 El papel de la educación

La labor de padres, madres, tutores y educadores es un factor clave y primordial en el diagnóstico, prevención y actuación ante este tipo de situaciones, debiendo tener un papel protagonista en la lucha contra este tipo de conductas.

Programas de capacitación como el puesto en marcha por el Ministerio de Industria, Energía y Turismo, a través de la página web red.es que tiene como objetivo dotar de habilidades a padres, madres, tutores y educadores, con el propósito de que sean capaces de acompañar a los menores de edad en el uso de las TIC de una forma responsable. Es decir, que conozcan los principales riesgos a los que los menores se pueden enfrentar en el ciberespacio, y tengan capacidad para guiarles acerca de cómo minimizarlos y cómo reaccionar ante ellos, son una herramienta eficaz para prevenir este tipo de conductas.

La prevención de este tipo de situaciones deben partir como bien se dice desde la propia educación a los menores en los riesgos vinculados con el uso de las nuevas tecnologías. A continuación se expondrán una serie de pautas a seguir para lograr una prevención eficaz ante este tipo de conductas[68]:

Respecto a los padres y educadores de los menores:

- Establecer niveles adecuados de comunicación intrafamiliar: Dialogar y establecer una comunicación positiva sobre los riesgos asociados a estas conductas debe configurarse como uno de los primeros pasos a seguir. Los niveles adecuados de comunicación no se construyen cuando se necesitan, sino que han de estar consolidadas para que se puedan utilizar ante la aparición de la problemática.
- Educación en sensibilidad: Importante el hecho de hacerles comprender tanto el derecho y el respeto a la víctima como el ponerse en las situación de este para evitar que se llegue a situaciones de violencia o incluso de aislamiento de determinados menores.
- Gestión de la información: Es importante que los menores aprendan tanto en la línea con la información que se recibe, qué información es creíble y cual no, como el que aprendan a analizar las consecuencias de la información que se publica.
- Colaboración entre familia y escuela para la resolución de problemas: En los casos de ciberbullying, sexting, ciberstalking que generen posteriormente una situación de acoso en el centro educativo.
- Educación en competencias digitales: Darles a conocer a los menores, los riesgos, las herramientas de protección y las buenas prácticas de uso como puede ser el proteger el ordenador con contraseña, no contratar servicios de proveedores de Internet que le proporcionen una dirección IP fija, ya que esto hará fácil localizar al menor cuando está navegando u obtener datos importantes sobre él, la instalación de un software antivirus de calidad y que se actualice automáticamente a diario, etc.
- Establecer reglas y supervisar en base a un criterio de edades: Los menores se comportan de manera diferente cuando sienten que alguien está prestando atención a lo que están haciendo. Se deberá por tanto ajustar el nivel de supervisión a la edad del menor. Debiendo evolucionar estos niveles hacia la generación de autonomía, de modo que vaya aprendiendo a gestionar las situaciones por sí mismo.
- Educación familiar y escolar con respecto a la preservación y educación de la gestión de la privacidad, el derecho y la salvaguarda de la intimidad y el respeto a la imagen de uno mismo y de los otros.

[68] Monográfico ciberacoso escolar (ciberbullying). Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad. red.es

- Concepto de delito: Sensibilización a los menores sobre las conductas que puedan llevar a consecuencias en el ámbito familiar (castigos), en el ámbito escolar (sanciones) o, en casos más graves, incluso penales (delitos).

Por otra parte, deberíamos hablar de las estrategias de prevención que deberían establecer por su parte, los centros educativos y sus educadores:

- Medidas relacionadas con la autoafirmación, es decir el convencimiento que una persona tiene de sus propias capacidades, habilidades y virtudes como sería en el alumnado que aprenda a responder asertivamente ante el abuso y en la comunidad educativa, formada por familias y el profesorado, la utilización de programas o protocolos de actuación previstos para cuando ocurra una situación de estas.
- Medidas organizativas: Como sería la disposición de sistemas anónimos y seguros de comunicación de los casos que se diesen de ciberbullying, etc., o el contar con grupos de personas con una estructura estable que trabajen contra este tipo de conductas.
- Medidas de inserción curricular: Adoptar metodologías como el roleplay, las técnicas narrativas o el análisis de casos para facilitar la interiorización de este tipo de conductas y las consecuencias que pueden causar por parte del alumnado.
- Medidas que tienen que ver con la gestión adecuada de los casos: Como es el establecer pautas educativas de reacción, es decir el qué hacer y qué no hacer cuando esto pueda suceder, tanto por parte del alumnado como de sus familias o dar información y formación al profesorado, familias y alumnado de una correcta gestión de las emociones en el ciberespacio.
- Medidas referidas a la evitación del riesgo: Implementar acciones que dificulten el que lleguen a los menores personas con no muy buenas intenciones instruyendo al menor para que conozca los riesgos de estas conductas o educando al menor en lo que tiene que ver con la gestión de la comunicación, de sus datos personales, imagen e intimidad; que sepa reaccionar y a quien acudir ante una sospecha, por otra parte la utilización de mecanismos físicos y técnicos en la red y en los aparatos para dificultar el acceso fácil al menor.
- Medidas de búsqueda de ayuda: Realización de reuniones de familias que aborden estos temas, elaboración de una red en la comunidad escolar que haga tareas preventivas contra este tipo de conductas o el asesoramiento en instancias superiores o de fuera de la escuela.

5 La cifra negra

Denominamos cifra negra a la tasa de delito desconocido y que, en consecuencia, no aparece reflejada en las estadísticas. En esta se incluyen dos grupos, la tasa de delitos que,

habiendo sido cometidos, no se han descubierto por la falta de denuncias por parte de las víctimas y aquellos en los que no se ha dictado una sentencia condenatoria, por falta de pruebas. El fenómeno de la cifra negra muchas veces ocurre por diversas razones:

- En muchas ocasiones la conducta criminal pasa directamente desapercibida por la víctima, de modo que no es denunciada aunque haya sido consumada e incluso se hayan logrado los efectos criminales de la misma.
- La víctima si es consciente del ataque pero lo hace tarde, cuando el delito ha prescrito o cuando ya valora absurdamente el presentar demanda judicial dado que según esta piensa que habrá pocas posibilidades de que la policía llegue a identificar, detener y procesar al delincuente.
- La propia víctima consciente del ciberataque, le resta valor a la conducta, por lo que no procede a denunciarlo.
- La razón de la no denuncia es precisamente la falta de confianza en el sistema judicial para la averiguación de los hechos, generalmente por la convicción de la dificultad que conllevará la identificación de los responsables.
- La denominada “ley del silencio” relacionada con el ciberbullying, por la que la víctima y el resto de menores que presencian las conductas de acoso no denuncian esta situación por miedo al rechazo social que puede implicar, suponiendo que en muchas ocasiones estas conductas sean muy difíciles de detectar.
- La víctima menor no denuncia los hechos para evitar que se les prohíba el acceso al ciberespacio que es para ellos un nuevo y prioritario espacio de socialización.

CONCLUSIONES

CONCLUSIONES GENERALES

PRIMERA: Hemos observado que existe un consenso mundial al penar este tipo de conductas. No obstante, a pesar de todo esfuerzo realizado por parte de los organismos internacionales y estatales, es imposible eliminar de raíz el problema debido a que estamos hablando de Internet, una tecnología que va avanzando increíblemente rápido y con ella la aparición y perfeccionamiento de nuevas y antiguas conductas delictivas. Por tanto, deberá ser necesario que al menos la normativa se encuentre continuamente actualizada en este tipo de materia, razón de peso será el hecho de que la víctima sea un menor de edad.

SEGUNDA: En España hemos observado que la incidencia de delitos como el ciberbullying, sexting, ciberstalking o childgrooming es ínfima en comparación con otro tipo de delitos o países, a pesar del despunte que ocasionan en las estadísticas los casos de pornografía infantil. Esto podría cambiar en los próximos años debido a que nos encontramos en una sociedad dependiente totalmente de la tecnología.

TERCERA: Algunas conductas delictivas como el sexting, ciberstalking o ciberbullying llegan a producir importantes consecuencias psicológicas en la víctima menor, concluyendo en algunos casos en el suicidio de esta. Será necesario por tanto insistir en la prevención y no actuar posteriormente cuando el daño ya ha sido cometido.

CUARTA: Internet es imposible de controlar. En el caso por ejemplo de la pornografía infantil no se puede erradicar al 100%, pero sí que se se puede reducir lo máximo posible la presencia de material pornográfico infantil en Internet a través de la utilización de medidas de prevención adecuadas. Cosa distinta será la reducción del contenido pornográfico infantil en la Internet invisible, siendo imposible debido al mecanismo que se utiliza en esta para anonimizar al usuario, que generará grandes dificultades a las Fuerzas y Cuerpos de Seguridad.

CONCLUSIONES PERSONALES

PRIMERA: Dado que son conductas cuyo medio de comisión es el espacio cibernético se debería exigir al legislador un mínimo de conocimientos en el manejo de las TIC o que a la hora de legislar estuviese auxiliado en todo momento por un perito informático.

SEGUNDA: Es preocupante la falta de interés que demuestran algunos padres o educadores no educando eficientemente a sus hijos/as en cuanto al peligro que entraña el mal uso de las TIC, muchas veces siendo este el factor detonante para que sus hijos/as se conviertan en potenciales víctimas de dicho tipo de delitos.

BIBLIOGRAFÍA

- MIRÓ, F., El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio, ed. Marcial Pons, Madrid, 2012.
- CERVANTES, P., TAUSTE, O., Internet negro. El lado oscuro de la red, ed. Planeta, 2015.
- SIEBER, U., The International Handbook on Computer Crime: Computer-related Economic Crime and the Infringements of Privacy, ed. Wiley, 1986.
- SIEBER, U., Informationstechnologie und Strafrechtsreform, Köln/Berlin/Bonn/München, ed. Carl Heymanns, 1985.
- ZACKER. C., Redes. Manual de referencia, ed. McGraw-Hill. Osborne Media, Madrid, 2002.
- GONZÁLEZ, J. L., VIVES, T. S., BUJÁN, C. M., ORTS, E., CUERDA, M. L., CARBONELL, J. L., BORJA. E., Derecho Penal Parte Especial, ed. Tirant lo Blanch, Valencia, 2015.
- MUÑOZ, J., Los delitos contra la integridad moral, ed. Tirant lo Blanch, Valencia, 1999.
- MARCO, J.J., <<Menores, ciberacoso y derechos de la personalidad>>, en J. García González (dir.), Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet, ed. Tirant lo Blanch, 2010.
- PARDO, J., <<Ciberacoso: Ciberbullying, grooming , redes sociales y otros peligros>>, en J. García González (dir.), Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet, ed. Tirant lo Blanch, Valencia, 2010.
- CHACÓN, A., <<Una nueva cara de Internet: el acoso>>, RE, 2003.
- ORTS, E., GONZÁLEZ, J.L., MATALLÍN, A., ROIG, M., VII Esquemas de Derecho Penal Parte Especial, ed. Tirant lo Blanch, 2010.
- CALMAESTRA, J., ESCORIAL, A., GARCÍA, P., DEL MORAL, C., PERAZZO, C., UBRICH, T., Yo a eso no juego. Bullying y ciberbullying en la infancia, ed. Save the Children, España, 2016.
- MASON, K. L., <<Cyberbullying: A preliminary Assessment for School Personnel>>, PS, 2008.
- YOUNG, K. S., <<Profiling online sex offenders, cyber-predators, and paedophiles>>, JBP, 2005.
- BABCHISHIN, K. M., HANSON, R. K., HERMANN, C. A., <<The characteristics of online sex offenders: a meta-analysis>>, SA, 2011.
- ESTIARTE, V. C., ADILLÓN, Mª. J., <<Nuevas tecnologías y victimización sexual de menores por online grooming>>, RECPC, 2016.
- MCALINDEN, A. M., <<Setting “Em Up”: Personal familiar and Institutional Grooming in the sexual Abuse of Children>>, SLS, 2006.
- LENHART, A., <<Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging.>>, PIALP, 2009.
- GRAW, M., <<Sexting or Self-Produced Child Pornography? The Dialogue Continues. Structured Prosecutorial Discretion within a Multidisciplinary Response>>, VJSPL, 2010.
- BASU, S., JONES, R., <<Regulating Cyberstalking>>, JILT, 2007.
- MARTÍNEZ, J. M., BOO, A., El fenómeno del sexting en la adolescencia: descripción, riesgos que comporta y respuestas jurídicas, Universidad CEU - Cardenal Herrera.
- BOCIJ, P., <<Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet>>, FMPRJI, 2003.
- BOCIJ, P., MCFARLANE, L., <<Seven fallacies about ciberstalking>>, PSJ, 2003.
- SHERIDAN, L., GRANT, T., <<Is cyberstalking different?>>, PCL, 2007.
- PITTARO, M. L., <<Cyberstalking: An Analysis of Online Harassment and Intimidation>>, IJCC, 2007.
- MCFARLANE, L., BOCIJ, P., <<An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers>>, FM, 2003.
- JIMÉNEZ, J., <<Tráfico de pornografía infantil: dinámica, roles y prevención>>, GICF, 2012.

- Sentencias núm. 105/2009 de 30 de enero; 84/2013 de 26 de febrero y 3234/2010, de 24 de septiembre.
- Ley de Enjuiciamiento Criminal y Código Penal.
- Directiva 2011/93/UE y Directiva 2011/92 del Parlamento Europeo y del Consejo del 13 de diciembre de 2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.
- Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.
- II Plan Estratégico Nacional de Infancia y Adolescencia (II PENIA)
- Instituto Nacional de Estadística (2015): Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares
- Monográfico ciberacoso escolar (ciberbullying). Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad. red.es
- Guía de actuación contra el ciberacoso. Ministerio de Industria, energía y turismo en colaboración con red.es.
- Guía sobre adolescencia y sexting: qué es y cómo prevenirlo. Observatorio de la Seguridad de la Información. INTECO, PANTALLAS AMIGAS, 2011.
- Estudio sobre hábitos seguros en el uso de smartphones por los niños y adolescentes españoles. Observatorio de la Seguridad y de la Información. INTECO, ORANGE, 2011.
- http://elpais.com/elpais/2008/10/01/actualidad/1222849019_850215.html
- http://www.policia.es/prensa/20151017_1.html
- http://www.abc.es/hemeroteca/historico-02-04-2004/abc/Tecnologia/cuatro-detenidos-por-distribuir-pornografia-infantil-por-internet_962766538455.html
- https://indignado7777.wordpress.com/
- http://conexioninversa.blogspot.com.es/
- http://ciberdelitos.blogspot.com.es/2011/05/el-fbi-explica-el-proceso-del-grooming.html
- http://dictionary.cambridge.org/es/diccionario/ingles/solicitation
- http://www.rae.es/
- http://www.elmundo.es/elmundo/2010/02/18/navegante/1266493878.html
- http://www.rtve.es/noticias/20100218/facebook-acata-ley-espanola-sube-edad-para-entrar-su-red-13-14/318732.shtml
- https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Consentimiento-otorgado-por-menores-de-edad.pdf
- http://www.ciberbullying.com/cyberbullying/
- http://www.seguridadpublica.es/2015/09/el-nuevo-delito-de-sexting-tras-la-reforma-del-codigo-penal/
- http://www.ecpat-spain.org/
- https://www.microsoft.com/es-es/
- https://www.gov.uk/government/news/internet-safety-summit-at-downing-street-communique
- http://www.delitosinformaticos.com/10/2007/noticias/pornografia-infantil-e-internet-una-problematica-social
- http://www.libertaddigital.com/nacional/sistel-un-sistema-sin-garantias-judiciales-1276373292/
- http://www.elconfidencial.com/sociedad/2007-03-06/anesvad-denuncia-la-gran-produccion-y consumo-de-pornografia-infantil-en-espana_493944/
- http://web.archive.org/web/20140814025634/http://www.rtve.es/noticias/20091105/sitel-doce-preguntas/299489.shtml
- http://www.ciberfamilias.com/ciberdelitos/el-menor-como-victima-de-delitos/
- http://www.protegeles.com/index.asp
- http://www.anesvad.org/es/anesvad/
- http://forum.emule-project.net/index.php?showtopic=155939
- http://asteriskmx.org/restringe-el-acceso-a-carpetas-especificas-usando-apache/
- https://httpd.apache.org/docs/2.0/es/sections.html