Problemáticas derivadas del uso malintencionado de las redes sociales

El ciberacoso como punto de partida

Trabajo Final de Grado

Grado Multimedia

Comunicación y cultura digital

Autor: Alex Silva Fernández

Consultor: Pere Báscones Navarro

Profesor: Antonio Laiz Triana

13/01/2020

Índice

Figuras y tablas

Índice de figuras

Índice de tablas

Capítulo 1: Introducción

Introducción, justificación y validez

El desarrollo de las Tecnologías de la Información y de la Comunicación (TIC) ha supuesto una auténtica revolución para la humanidad aportándonos numerosos beneficios, conocidos por todos; sin embargo, también han supuesto importantes ventajas para usuarios malhechores, los cuales, mediante la aparición de las redes sociales, han visto la posibilidad de perpetrar acciones criminales a cientos de kilómetros, pudiendo utilizar identidades supuestas, cuentas anónimas y todo ello con el fin de dificultar su identificación.

Las redes sociales e Internet también han traído la aparición de nuevas conductas ilícitas que, por su gravedad, merecen un reproche penal y no estaban hasta escasos años recogidas como tales en nuestra legislación: intrusiones ilegales en sistemas informáticos, daños informáticos, nuevas problemáticas a nivel social y educativo como el ciberacoso, la usurpación de la privacidad y las sensación de inseguridad en las redes, la desinformación y el espionaje…

Esta nueva presencia de amenazas en las redes sociales y nuevos medios han supuesto un incremento de la preocupación de los usuarios que emplean este tipo de redes, además de padres preocupados por las conductas que llevan a cabo sus hijos en este tipo de entornos. Cabe destacar que desde el punto de vista de la tecnología y las aplicaciones multimedia, todavía hay un desconocimiento generalizado por parte de las víctimas y sus allegados a cerca de qué herramientas existen como método de ayuda y prevención a estas problemáticas.

Es por esto que mediante este Trabajo de Fin de Grado se quiere llevar a cabo un estudio, análisis e investigación a cerca de las redes sociales y las problemáticas que envuelven a estas. Como demuestran numerosos estudios, la problemática social y educativa más relevante en estos entornos es el ciberacoso, debido, en gran parte, a las características citadas con anterioridad y a la relación que este puede tener con el entorno en el mundo físico de la víctima.

Por lo tanto, y una vez habiendo entrado en contexto, el trabajo se centrará en el ciberacoso y en las demás problemáticas que están relacionadas a este derivadas de un mal uso de las redes sociales. Será indispensable analizar e investigar en profundidad cada una de ellas dando una gran importancia a todos los individuos partícipes. El análisis de las causas y las consecuencias en el ámbito educativo, social y clínico y su relación con estas problemáticas será de alta importancia para llegar a conclusiones contundentes.

Además del estudio de las problemáticas relacionadas al ciberacoso, no se debe de pasar por alto analizar la legislación y la normativa a la que están sujetas este tipo de actos en la actualidad, tanto a nivel nacional como europeo.

Finalmente, se debe de llevar a cabo un análisis de las herramientas con las que contamos hoy en día en el mercado que nos ayudarán a prevenir y detectar en mejor manera el ciberacoso y las conductas delictivas relacionadas con el mismo, pudiendo así, tras haber estudiado todo tipo de posibilidades, incluir en este Trabajo de Fin de Grado mi propia aplicación multimedia interactiva como herramienta de lucha contra este tipo de actos delictivos, según las deficiencias o novedades que pueda aportar en base a lo analizado e investigado.

Es por tanto, que este documento va enfocado tanto a receptores que quieran ser informados a cerca de problemáticas como el ciberacoso y otras relacionadas al mismo como a aquellos que quieran conocer la actualidad en cuanto a normativa y herramientas que podemos emplear para prevenir, detectar, evitar y combatir el ciberacoso y otros fenómenos de persecución virtual. A su vez, éste podrá ser de gran ayuda tanto para víctimas, familias, testigos e incluso agresores, los cuales, podrán encontrar aquí la razón por la cual deben de reflexionar en cuanto a su reinserción y concienciarse de todas aquellas consecuencias que pueden acarrear los actos que estos llevan a cabo.

Marco teórico

A día de hoy, vivimos en un mundo en el que la evolución constante de la tecnología juega un papel determinante. La sociedad ha pasado a estar conectada de manera instantánea y sin tener que hacer ningún esfuerzo. Las comunidades virtuales ya no son una novedad, pero sí han supuesto un gran cambio hacia una nueva estructura social, integrada por personas, organizaciones y entidades conectadas entre sí: La Red Social. Tal ha sido este cambio que Zuckerberg[1], creador de la red social *Facebook*, llegó a manifestar que "*Facebook es ya el tercer país más grande del mundo, si consideramos su población, por lo que es capaz de mover más información que cualquier gobierno*" (Zuckerberg, 2010).

Las redes sociales tienen su origen con la creación de *Classmates.com* (1995) y *SixDegrees.com* (1997). Este segundo espacio virtual ofrecía básicamente la posibilidad de la creación de un perfil de usuario y la confirmación de una lista de amigos. Con el paso del tiempo, esta red fue mejorando y ofreciendo nuevas prestaciones en cuanto a la comunicación de los usuarios y la interacción de los mismos con el entorno, ampliando el abanico de posibilidades y las herramientas a emplear. A partir de esto, comenzaron a surgir otras redes sociales como *MySpace* (2003), *Facebook* (2004) y *Twitter* (2006). No obstante, pese a la aparición de nuevas redes sociales y el incremento de usuarios, con el paso de los años, no todas han evolucionado de la misma manera (Figura 1).

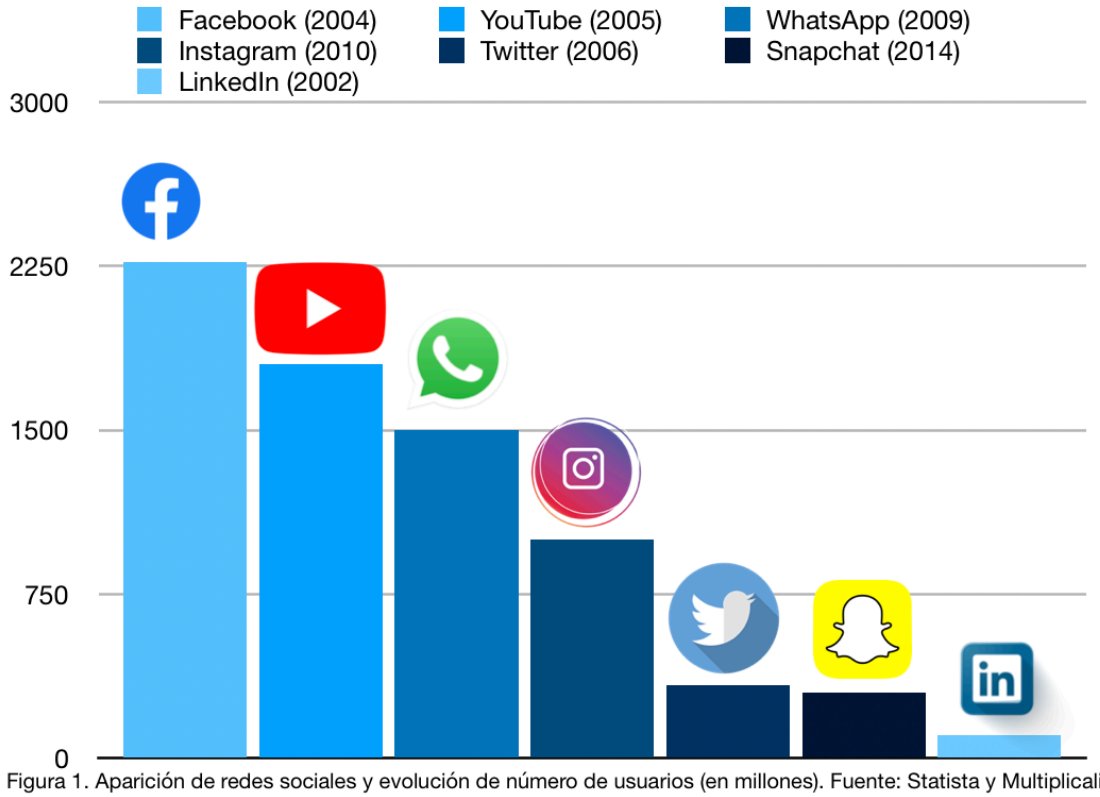

Figura 1. Aparición de redes sociales y evolución de número de usuarios (en millones). Fuente: Statista y Multiplicalia (2019)

[1] Creador y fundador de *Facebook*, la red social con más usuarios a nivel mundial.

Sin lugar a dudas, podemos afirmar que las redes sociales son un fenómeno social que permite un gran desarrollo para la humanidad, pues las redes, por naturaleza, son formas de interacción social, establecidas como un intercambio muy activo entre personas, comunidades e instituciones. "*Tengamos en cuenta que el hombre desde sus orígenes ha dado vida a sistemas de comunicación que recaen en la conformación de círculos humanos y hoy en pleno siglo 21, la composición de estos tejidos sociales, se encaminan a ser uno de los retos más relevantes de su historia*" Figueroa[2] (2010). Más aún, Brian Solis[3] (2013) afirma que el *Social Media* "*se trata de sociología y psicología más que de tecnología*".

Todos hemos sido testigo del crecimiento de estas y los beneficios que ha dado a la sociedad de las últimas generaciones, no solamente ha logrado formar y brindar un gran crecimiento en el ámbito empresarial, ya que permite el incremento de la globalización y poder crear lazos entre otras empresas y otros países para tener una buena relación mediante las redes sociales, sino también en el aspecto personal del ser humano, que, como ya se ha mencionado, tienen la necesidad de relacionarse con otras personas.

Sin embargo, pese a todos los beneficios que las redes sociales aportan a la sociedad, no todos los usuarios de estas hacen un buen uso de las mismas. "*Existe un peligro latente ya que al haber tantos menores utilizando las redes sociales y al estar relacionándose con personas que no conocen personalmente, están expuesto a que les pueda ocurrir algo. Puede ser muy alarmante este aviso debido a que tanto personas mayores, jóvenes y niños utilizan las redes sociales también las pueden utilizar personas con malas intenciones como pedófilos, acosadores, psicópatas, etc.*" Biesot[4] (2011).

A partir de la evolución de las redes sociales, también se ha visto incrementado un problema dentro de las mismas y es que, los actos delictivos, llevados a cabo por parte del mal uso de estas, son una realidad. Además, muchos de estos actos delictivos se cometen contra usuarios menores (Figura 2). Esto se debe en gran medida a que los autores de estos actos son usuarios que se aprovechan de la inofensividad de estos jóvenes y del anonimato que les proporciona las redes. Es más, el sociólogo y filósofo Bauman[5] (2016) apoyó en una de sus últimas tesis que "*Los seres humanos del siglo XXI son de dos mundos*". Dos mundos en los que, según analiza Bauman (2016), "*cada persona adopta unos preceptos, reglas, fronteras, vocabularios y códigos de conducta distintos*" y que, en conjunto con "*la ilusión de totalitarismo que te aporta la red y el anonimato*" ha desembocado en "*prácticas de aislamiento, separación, exclusión, enemistad y*

[2] Cesar Falla Figueroa es Licenciado en Ciencias de Comunicación en Perú. Experto en análisis e investigación en redes sociales, cuenta con gran reconocimiento en su país natal debido a sus relevantes trabajos.

[3] Especialista en marketing digital, sociólogo y analista que ha ocupado cargos de gran importancia como el de director de *Altimeter* y desempeños como la fundación de *FutureWorks*.

[4] Angela Biesot es una periodista española especializada en investigación. Realizadora de diversos estudios relacionados con los usuarios de las redes sociales. Ganadora del Premio de Periodismo Rey de España (2013).

[5] Zygmunt Bauman es un sociólogo, filósofo y ensayista de lo más destacados del pensamiento crítico moderno. Entre sus numerosos galardones, cuente con el premio Príncipe de Asturias de Comunicación y Humanidades (2010).

conflictividad" lo que relaciona directamente a los "numerosísimos casos de ciberacoso y difamación".

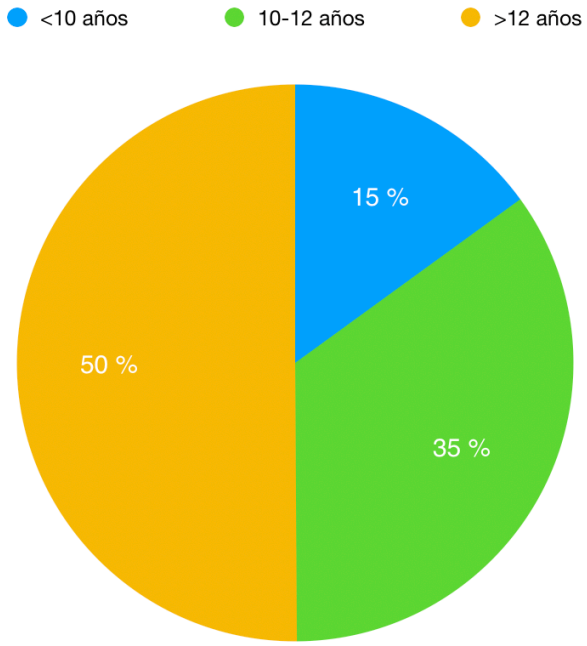

Figura 2: Ciberacoso en edades.
Fuente: elaborada a partir de estudios realizados por ANAR en colaboración con Mutua Madrileña y Stadista (2017)

Más aún, el perfil de este tipo de usuarios es variado y los hay desde acosadores en redes, pasando por perfiles más criminalísticos como los pedófilos hasta las campañas de desprestigio y el espionaje hacia usuarios más reconocidos o con cierta influencia social. Pese a la existencia de un marco legal un tanto escueto, España, uno de los primeros países que empezó a notar las consecuencias de estas problemáticas, creó una ley. "*La ley española dicta que la edad mínima para obtener de manera legal una cuenta en una red social es de 14 años. Sin embargo, la veracidad de los datos que se introducen al crear un perfil es incontrolable*", Biesot (2011).

Esto es lo que dice la propia normativa y marco legal en territorio español. En España, el acceso a estas plataformas está regulado en el art. 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que establece que "*podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores*". Por ello, no es legal el uso de estas redes sociales por parte de menores de 14 años y está prohibido que se registren sin el consentimiento previo de sus tutores legales.

Pese a la normativa existente a nivel nacional, es prácticamente imposible saber qué se esconde detrás de un perfil falso. Más aún, solo podemos tener constancia de un perfil real cuando estos están verificados y, a día de hoy en redes sociales, esto es un privilegio que solo poseen empresas de alta reputación y celebridades (Tabla 1). Por esto, es imprescindible analizar el *software* y las herramientas tecnológicas que disponemos a día de hoy y, llevar a cabo un buen uso de las mismas para evitar ser víctimas de las problemáticas existentes. Esto nos permitirá mejorar el nivel de seguridad que tenemos a la hora de navegar por las redes, e incluso, podremos burlar posibles ataques de otros internautas y, mantener a su vez, un alto nivel de privacidad.

Redes sociales	**Actualidad**	**¿Quién puede ser verificado?**	**¿Cómo sé que una cuenta ha sido verificada? Logotipos junto a nombre del perfil**
Twitter	Es la primera red social que comenzó a usar perfiles verificados. *Twitter* lleva sin verificar perfiles desde 2018 (están mejorando el programa de verificación)	A día de hoy, nadie.	
Facebook	A día de hoy, la red social más grande del mundo tiene implantando un sistema de verificación. Se debe de rellenar un formulario para tener acceso a dicha verificación.	Personajes públicos, perfiles destacados, usuarios que demuestren mediante el formulario y cumplan ciertos requisitos, empresas	
Instagram	Lanzo su programa de verificación a mediados de 2018. Cualquiera puede solicitar ser verificado, siempre que mantenga una reputación dentro de la misma	Se debe de cumplir con alguno de los siguientes requisitos: figura pública, celebridad o gran marca para ser aprobado.	

Tabla 1: Verificación en redes sociales. Fuente: *Socialreport*

Del Mundo Analógico al Mundo Digital

El ser humano es un ser social por naturaleza, y gracias a este carácter social se ha conseguido evolucionar a lo largo de la historia como sociedad y dar lugar a la creación y desarrollo de comunidades. A partir de la aparición de Internet y de la Web 2.0 (O'Reilly[6], 2005), se han formado redes sociales digitales que han evolucionado hacia lo que conocemos como comunidades virtuales. Es así como vivimos en lo que el sociólogo Castells[7] (1996) denomina "*la Sociedad Red*". Podríamos decir sin ningún tipo de reparo que Castells (1996), en muchas de sus teorías y afirmaciones, fue un visionario a cerca del papel que jugarían las nuevas tecnologías y las redes en un futuro que ya ha llegado.

Por una parte, la globalización ha permitido crecer a numerosos países y por ende a muchas organizaciones, mucho más rápido que en otras épocas. A su vez, ha permitido, igualmente, que un número mayor de personas tengan en la actualidad un mayor nivel adquisitivo y un nivel de vida superior nunca visto con anterioridad, brindado así a un mayor número de personas el acceso a un grado de conocimientos que sólo hace un siglo no era alcanzable.

Además, las tecnologías de la información juegan un papel importante para que una empresa sea productiva, pues hoy en día todo se maneja a través de las TIC y una organización que se quede estancada tiende sencillamente a fracasar o desaparecer. Cada vez es más evidente la convergencia entre el mundo analógico y el digital permitiéndonos mantener una comunicación sincrónica y asincrónica independientemente del espacio-tiempo en que nos encontremos. La cibercultura y la cultura de la participación son dos características del S. XXI que están transformando el sentido de la comunidad tradicional dando paso a comunidades interconectadas.

En estas comunidades, a las que se las denominará comunidades virtuales, surgen problemas de índole social y educativo, al igual que en las comunidades análogas. Las problemáticas sociales y educativas visibles dentro de las redes sociales no siempre tienen su origen en las mismas, sino que, son acciones o sucesos que pueden haberse extrapolado desde el mundo real al mundo digital, en gran parte, gracias a la evolución tecnológica. Poniendo el centro de atención en estas problemáticas, como el ciberacoso, cabe destacar que "*uno de cada dos casos de ciberacoso en España lo provoca un compañero de clase del afectado*", según la última encuesta realizada por *Ipsos Global Advisor*[8] (2018). Esto quiere decir, más concretamente, que en el 56% de los casos, el acoso ya se ha dado en el mundo real y, prosigue sus pasos más allá, entre las comunidades virtuales.

---

[6] Fundador y presidente de O´Reilly Media. Fuerte impulsor de movimientos de *software* libre y código abierto así como uno de los autores del concepto web 2.0 y participante en el desarrollo del lenguaje *Perl*.

[7] Sociólogo, economista y profesor. Desarrolló el libro "La Sociedad Red", gran influyente en su análisis de la aparición de los nuevos medios.

[8] Grupo especializado en investigación, análisis y estadísticas.

Por otra parte, existen otras problemáticas relacionadas con el ciberacoso que también surgieron, en un primer momento, en el mundo analógico, pero que posteriormente han sido avistadas en redes debido a la digitalización. Un claro ejemplo es el del espionaje. Numerosos han sido los métodos y las técnicas empleadas por diversas entidades para conseguir información a cerca de un hecho o de ciertos personajes. Desde Gengis Kan[9], el conquistador mongolo, que desarrolló un sistema de comunicaciones llamado *yam*, hasta el peculiar Richebourg[10], un espía de 60 centímetros de altura que se hacía pasar por un bebé. Actualmente, repasamos el panorama y vemos cómo las redes sociales tienen un papel fundamental en el espionaje. Incontables son las denuncias que le llegan a diario a la red social *Facebook* y su fundador, Mark Zuckerberg, acusado (y afirmado por altos cargos que lo filtraron) de espiar y seguir a la población mundial y vender todo tipo de información de los usuarios a gobiernos y servicios secretos. En su día, nadie entendió porqué Zuckerberg decidió comprar el servicio de mensajería *WhatsApp* por 21.800 millones de dólares, pero, atendiendo a la información anterior, se puede confirmar que el creador de *Facebook* tiene ahora en su poder todo tipo de datos y acceso a más de 2.271 millones de cuentas de usuarios que emplean sus redes sociales en la actualidad, tal y como afirma la revista Muy Interesante[11] (2016). Más aún, seguimos en la misma línea cuando hablamos de campañas de desprestigio, persecución en redes o de la desinformación.

Ahora bien, estas problemáticas, al igual que las que ocurren en el mundo análogo, deben de contar con una serie de soluciones para lograr contrarrestarlas y reducirlas. Hasta el siglo XIX, en España, no hubo un sistema educativo claramente definido. Esto provocaba una diferencia abismal en cuanto a condiciones de vida, nivel social, cultural y educativo. Con el paso del tiempo, en 1857 se promulgó la Ley de Instrucción Pública, generando un gran cambio a nivel nacional. Esta ley se fue modificando, pasando por la Ley General de Educación, La Ley de Ordenación General del Sistema Educativo (LOGSE) y, la ley que rige el ámbito en nuestros días reformando a la anterior, la LOE. El empleo de un sistema educativo por ley ha conseguido que a día de hoy podamos vivir en una sociedad en la que cada uno de sus integrantes puede adaptarse en mejor manera a la civilización, ofreciéndole desde su nacimiento el derecho a tal enseñanza y, apoyando a su vez, la inclusión social.

Esto lo que nos viene a ofrecer es una perspectiva de cómo un nivel educativo puede influir en mejor manera en el nivel social pues, como afirmaba Mandela[12] (1994), "*La educación es el arma más poderosa que puedes usar para cambiar el mundo*". Más aún, la ONU (s.f.)[13] afirma que "*La educación es un derecho de todas las mujeres y los hombres, ya que nos proporciona las*

[9] Conquistador mongolo que desarrolló un nuevo sistema postal denominado *Yam*.

[10] Richebourg, un espía de 58 centímetros de altura que influyó en el desarrollo de la revolución francesa.

[11] Revista de prestigio que actúa y realiza sus publicaciones en el ámbito nacional.

[12] Nelson Mandela, activista, abogado y político sudafricano de los siglos XX y XXI conocido mundialmente por su lucha pacífica contra la segregación racial en Sudáfrica

[13] Organización de Naciones Unidas.

capacidades y conocimientos críticos necesarios para convertirnos en ciudadanos empoderados, capaces de adaptarse al cambio y contribuir a la sociedad". Por lo que, "*Una sociedad educada tiene muchos beneficios, entre los que destacan menores tasas de mortalidad infantil, menos infecciones por enfermedades venéreas, tasas menores de contaminación y mayor inclusión social, tolerancia y respeto por los demás"*[14].

Aplicando estos aspectos de cara al ámbito de las redes sociales y nuevas tecnologías, las problemáticas podrían ir evolucionando y descendiendo su actividad. Es decir, ante un fenómeno tan reciente como es el de las comunidades virtuales, lo ideal es inculcar un mínimo de educación, conocimientos y aspectos normativos a los nuevos "habitantes" de las comunidades virtuales, queriendo así formarles en mejor manera en el ámbito digital con el objetivo de crecer, al menos, mínimamente en cultura digital y, más importante aún, a nivel social, pues no se debe de olvidar que de aquí en adelante tanto las comunidades análogas como las virtuales vivirán mano a mano. Una de las claves a nivel educativo es "*transmitir a los menores que se tienen que aplicar los mismos valores en el mundo real y en el digital*", Perazzo[15](2017).

Tal es la relación entre ambas comunidades y "mundos paralelos" que contamos con datos ofrecidos por un estudio llevado acabo por UNICEF[16] (2019) en España que revela que uno de cada cinco niños y una de cada siete niñas de entre 12 y 16 años están implicados en algún caso de ciberacoso. Más aún, este tipo de actos, según dicho estudio, suelen ser llevados a cabo paralelamente en el mundo digital como en el análogo, pues los ciberacosadores suelen pertenecer al mismo centro que la víctima. Estas cifras concluyen con un dato estremecedor: al menos dos estudiantes en cada clase sufren ciberacoso.

Esto lo que pretende es dar un golpe de realidad a los usuarios, pues el mundo analógico y el digital no son tan distantes y en ellos interactúan seres del mismo tipo. La naturalización del mundo digital y un empleo de herramientas de protección que favorecerán a nuestra seguridad terminarán con el ciberacoso y problemáticas relacionadas. Lo indispensable es hacer saber al malhechor que, aunque esté sentado frente a una pantalla, detrás de ella hay otras personas y que, además, existe una ley con prestaciones que le castigará según sus actos. No podemos tomarnos la red como una comunidad a su libre albedrío, pues si esto se diera, las problemáticas aumentarían y las consecuencias para muchos usuarios serían nefastas.

---

[14]Declaración llevada a cabo por la Organización de las Naciones Unidas.

[15] Catalina Perazzo Aragoneses es la Directora de Sensibilización y Políticas de Infancia en Save the Children España.

[16] Fondo de las Naciones Unidas para la Infancia.

Capítulo 2: Ciberacoso

Ciberacoso

Como se ha venido comentando, a pesar de los beneficios infinitos de las nuevas tecnologías de la información y de la comunicación, no podemos olvidar los riesgos que las TIC presentan a los usuarios. El ciberacoso o acoso en línea es uno de ellos. El Centro de Investigación de Ciberacoso de Estados Unidos lo define como un daño intencionado y repetido perpetrado a través de ordenadores, teléfonos móviles y otros aparatos electrónicos. Esto incluye amenazas, intimidación u hostigamiento a través de emails, chats, mensajes de texto y páginas web. También abarca acciones como la difamación, exclusión o rechazo de compañeros, suplantación de identidades, publicación no autorizada de información o imágenes privadas y manipulación.

A su vez, el ciberacoso puede tener connotaciones sexuales a través de insultos con elevada carga sexual o mediante la distribución de fotos y vídeos de sexualidad explícita con el fin de avergonzar o causar angustia emocional a la víctima. Si bien el ciberacoso puede manifestarse aisladamente, muchas de sus víctimas también han sufrido acoso tradicional, de manera directa y no en línea. Este acoso en línea puede darse entre amigos y compañeros, así como en el contexto de relaciones amorosas entre adolescentes, pudiendo estar en ambos casos solapado. En cualquier caso, en base a los últimos documentos ofrecidos por UNICEF y la Asociación Española de Pediatría (2015), se ha descubierto que la mayor parte de los perpetradores son adolescentes o usuarios con temprana edad. Por último, un rasgo único de esta modalidad de acoso es que su perpetrador permanece en el anonimato.

El centro de *EU Kids Online Survey* (2011-2012) recabó datos sobre la utilización de Internet y las experiencias digitales de niños en 25 países europeos, entre 9 y 16 años. De un total de 25.000 niños encuestados, el 6% declaró haber sufrido ciberacoso y solo un 3% admitió haber acosado a otros. Sin embargo, las cifras eran mayores en lo que se refería al acoso tradicional y es que 1/5 de los niños declaró haberlo sufrido alguna vez en su vida. Se encontró además una relación entre ambos tipos de acoso. La mitad de las víctimas de ciberacoso denunciaron haber sufrido también acoso en persona. Al mismo tiempo, la mayoría de los niños que admitieron haber perpetrado acoso online, también admitieron haberlo hecho en persona. Otro de los datos destacados que señala el estudio es que la mitad de los niños que admitieron ser perpetradores de ciberacoso, también fueron víctimas.

La encuesta arroja respuestas diferentes sobre la percepción de las propias víctimas sobre el daño que habían sufrido. Más de la mitad indicaron que el ciberacoso les había afectado mucho o bastante, mientras que el 15% declaró no haberse visto afectado en absoluto. En cuanto a las diferencias por sexo, las adolescentes manifestaron haber sufrido más que los adolescentes. El 37% de ellas alegaron haber estado muy afectadas en comparación con el 23% de ellos. Por otro lado, algo más de 3 de cada 4 niños expresó haber hablado de su experiencia -con un amigo o familiar-, casi la mitad bloqueó el contacto online con la persona acosadora y alrededor de un tercio expresó haber tratado de arreglar el problema.

A nivel Europeo, estos fueron los últimos años en los que se recabaron datos de manera tan global. Sin embargo, a nivel nacional, contamos con recientes datos ofrecidos por el Observatorio Español de Delitos Informáticos (2019) en los que se afirma que en 2017 fueron denunciados 81.307 casos de ciberacoso. Entre las tipologías en el que se manifiesta este contamos con el *Happy Slapping*, el *Grooming* y el *Sexting* que posteriormente analizaremos. Además, el ciberacoso escolar es el que peor sale parado (Figura 3).

Figura 3. 7 de cada 10 jóvenes ha sufrido ciberacoso en España. Fuente: Observatorio Español de Delitos Informáticos (2019)

Ahora bien, ¿Que lleva a estos usuarios a realizar este tipo de acciones? Las causas para que se den estos actos son muy variadas y pueden diferir dependiendo de la tipología del autor. Los estudios llevados a cabo por ANAR y Mutua Madrileña (2016-2018), confirman que los acosadores son personas con baja autoestima que solo se sienten bien cuando hacen daño a los demás pues este hecho les hace sentirse más fuertes. También, este suele carecer de todo respeto por sus semejante y no conoce los límites éticos básicos necesarios para la convivencia en sociedad. Más aún, el agresor se aprovecha de una determinada situación de inferioridad de la víctima, ya sea por temor, escasa comunicación de esta con sus allegados o la existencia de varios acosadores simultáneos. Otra de las causas de esta problemática a destacar es que en la mayoría de casos, el acosador cree erróneamente que quedará impune ante la ley al realizar estas acciones a través de las TIC por una falsa creencia de anonimato.

Cuando el ciberacoso se da en el entorno escolar, según la Guía de Actuación contra el Ciberacoso (s.f.), cabe destacar que el tutor debe establecer un proceso de recogida y triangulación de información que sirva de fundamento para la valoración del supuesto caso, e incluso, valorar la posibilidad de conseguir pruebas de las acciones de intimidación que está padeciendo la víctima. Este proceso debe caracterizarse por la actuación comedida, pausada y ajustada a las circunstancias. Las prisas no deben caracterizar el proceso, pero la diligencia y la prontitud son buenas aliadas de éste, debido a las consecuencias que podría tener un caso de este tipo.

Por otra parte, cabe destacar la importancia de apoyarse sobre el resto de equipo docente e incluso en consultores y orientadores del centro. Más aún, es imprescindible aguardar en todo momento la privacidad y confidencialidad de la víctima y el caso y pasar a entrevistarse con víctima, agresores y tutores legales de ambas partes. Finalmente, tras la recogida de información y concluidas las entrevistas, el tutor deberá de elaborar un informe en el se valorará la existencia o no de una situación de ciberacoso escolar y, habiendo estudiado la situación, se propondrán las acciones inmediatas a llevar a cabo.

Ahora bien, comparando el acoso tradicional con el ciberacoso, llegamos a ciertas conclusiones a cerca de los riesgos que el acoso, a través de las comunidades virtuales, puede acarrear. En primer lugar, la víctima no deja de ser acosada una vez se encuentra en su domicilio, sino que puede recibir las amenazas 24 horas al día, 365 días al año, siempre que esté conectada (*Smartphone*, Internet, etc), por lo que la prevalencia en el tiempo a través de las TIC aumenta su grado de incidencia en la víctima. Otro riesgo diferencial con el acoso escolar tradicional, es que la audiencia del acoso ya no es local (el grupo de clase, el colegio, la comunidad educativa, el vecindario, etc.) sino global, por lo que la víctima se siente perseguida allá donde vaya, lo que le provoca una sensación muy grande de indefensión y puede llegar a provocar la exclusión social de esta. En suma, no se debe de olvidar el riesgo en cuanto a las consecuencias legales para el acosador o para sus padres, cuando es un menor el que acosa.

Víctimas	¿Dónde son acosadas ?	¿Testigos, "audicencia" del acoso?	Medio de acoso	Responsable legal
Acoso tradicional	La víctima es acosada en el lugar físico en el que mantiene contacto con el acosador.	La audiencia del acoso es local, es decir, visualizan el acoso aquellas personas que pertenecen a dicha clase, colegio, vecindario, etc.	Análogo (acoso verbal, físico, etc)	Padre, madre o tutores legales al tratarse de un menor.
Ciberacoso	La víctima es acosada en cualquier momento del día.	La víctima se siente perseguida allá por donde va. La audiencia se extiende a través de la red. Posibilidad de hacerse viral.	Digital (por medio de Smartphones, Internet, redes sociales)	Padre, madre o tutores legales al tratarse de un menor.

Tabla 2. Comparativa del acoso tradicional y el ciberacoso en el ámbito escolar.

Ambos tipo de acoso pueden llegar a ser comparables, porque en la mayoría de ocasiones están relacionados entre sí, pero, como dice Ciruelos[17] (2016) "*Las consecuencias de la violencia digital para un usuario nativo digital son más graves que la violencia real. La repercusión de su imagen en las redes sociales tiene gran importancia entre su círculo social, que se vea dañada puede suponer su muerte en el entorno digital, y en ocasiones, en la vida real*".

Cabe destacar a su vez, por otra parte, los efectos del ciberacoso. Es una problemática que puede llegar a afectar a las víctimas en distintos ámbitos, como la personalidad. Muchos de los afectados, se tornan especialmente inquietos nervioso cuando recibe un mensaje de texto (*WhatsApp*, SMS, chat) o un *email*. Además, se refugian en sí mismos y la relación con terceros queda rota, pues temen a la gente que les rodea, se vuelven antisociales y no ven la necesidad de quedar con gente, ir a la escuela o el trabajo o, simplemente, salir a la calle, pues su casa es su refugio. Otro de los efectos del ciberacoso es el cambio que sufren estos sujetos en cuanto al uso de las TIC. Se sienten enfadados o frustrados después de utilizar el ordenador, la *tablet* o el *Smartphone* y, otras veces, puede dejar de usar las TIC de forma brusca e inesperada. Aún así, lo más preocupante es el cambio radical que se da en relación con la familia, pues se muestra tímido y distante con sus allegados mas cercanos.

Tras todos estos ámbitos en los que interviene el ciberacoso, cabe destacar las principales consecuencias tanto para las víctimas de estas problemáticas como para los acosadores. Entre estas, podemos diferencias las consecuencias psicológicas y las consecuencias físicas. Por una parte, las consecuencias psicológicas se producen debido a que el ciberacoso está presente las 24 horas del día. Siempre está en línea. Incluso si se apaga el ordenador la víctima sabe qué página web está accesible, o qué personas están propagando ese rumor sobre ti. La dureza de esto es psicológicamente devastadora.

Por otra parte, entre las consecuencias físicas, aparecen entre las víctimas síntomas como el estrés, humillación, ansiedad, ira, impotencia y fatiga. Más aún, el conjunto de todos estos factores hacen que se de un brusco cambio de personalidad en el acosado, tales como la resignación (como se ha venido comentando con anterioridad, la víctima no se siente parte de la sociedad, por lo que opta por aislarse de manera voluntaria), la aparición de rasgos obsesivos (cambio hacia una actitud hostil y suspicacia, sentimiento crónico de nerviosismo, hipersensibilidad con respecto a las injusticias) y aparición de rasgos depresivos (la víctima desarrolla un sentimiento de indefenso, junto a la incapacidad de disfrutar y sentir placer), tal y como afirma la Guía Clínica sobre el Ciberacoso para profesionales de la salud (2015), elaborada por el Gobierno de España en colaboración con instituciones como Hospital Universitario La Paz, según el estudio de casos de diversos pacientes[18]. Además, todos estos datos son respaldados

[17] Marta Ciruelos, responsable de Marketing en *Always On*, empresa especializada en protección digital.

[18] Guía Clínica sobre el Ciberacoso para profesionales de la salud.

por estudios psicológicos elaborados por el equipo técnico de Sanitas[19] (s.f.), el equipo de psicólogos de Lomber[20] (2018) y estudios realizados por distintas Universidades como por ejemplo la UNIR[21] (2018).

Pese a todos los ámbitos vistos, no debemos olvidarnos de los casos más extremos que han estado relacionados con el ciberacoso. Las consecuencias de estos, han sido fatales, llegando incluso a la pérdida de víctimas de esta problemática. Por ejemplo, el caso de Romina Perrone, difundido en medios como La Nacion (2010), una estudiante de 10 años que tuvo que soportar que una compañera de clase creara un grupo de *Facebook* "porque la odiaba". La página de *Facebook* llegó a sumar 5.000 fans y la madre de Romina se vio en los juzgados con *Facebook* por no acceder a borrar dicho evento. Y es que el ciberacoso es una práctica que la lleva a cabo la misma persona que acosa en la vida real. Esa persona que abusa de su poder y pretende elevar su estatus denigrando a otros. El efecto del ciberacoso puede llegar a ser devastador y, en ocasiones, incluso mortal. Como por ejemplo, el caso de Brandy Vela, que se hizo viral en EEUU y medio mundo a través de medios como CNN (2016). "*La adolescente de 18 años sufría acoso escolar y el maltrato llego también al entorno digital. La joven decidió poner fin a su vida ante los ojos de su familia, que la reclamaban que no lo hiciera*".

[19] Expertos en asistencia sanitaria.

[20] Un equipo variado de profesionales entorno al ciberacoso.

[21] Universidad Internacional de La Rioja.

Tipos de ciberacoso

El ciberacoso, es una problemática que puede manifestarse de diferentes maneras. Es por esto que hay distintas categorías y tipologías del mismo, dependiendo de las acciones e intenciones que tenga el acosador con la víctima. De manera general, podemos diferenciar o clasificar el ciberacoso en tres categorías. En primer lugar, el ciberacoso en sentido estricto, es decir, aquel que se produce entre adultos, en el que tanto la víctima como el acosador son mayores de edad. En segundo lugar, nos encontramos con el ciberacoso sexual, cuya finalidad no es otra que la de obtener algún tipo de beneficio sexual de la víctima. En tercer y último lugar, nos encontramos con el *ciberbullying*, que engloba todas aquellas acciones en las que se producen situaciones de acoso entre menores (Figura 4) [22].

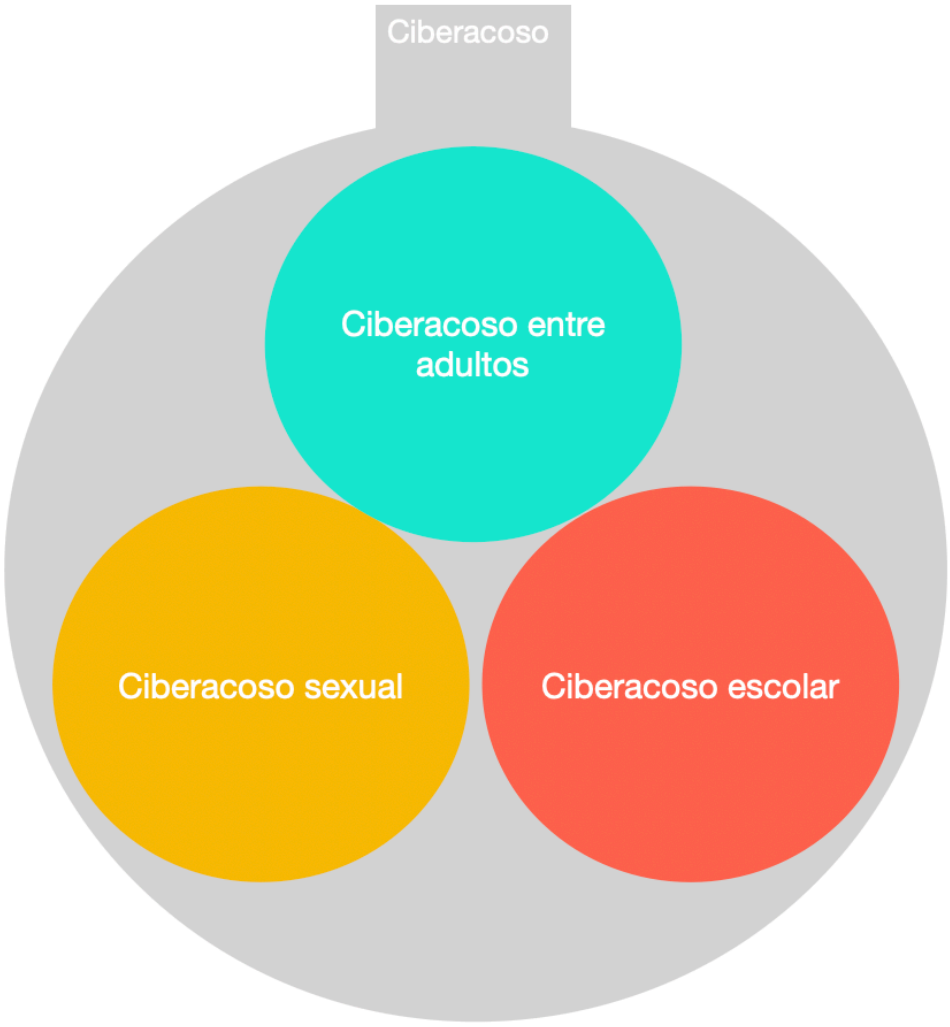

Figura 4. Ciberacoso y sus tipologías. Fuente: elaboración propia a partir de lo analizado.

[22] Clasificación llevada a cabo por especialistas en el tema como Ciberacoso.net, Pantallas Amigas y medios como El Periódico.

Ahora bien, partiendo de esta base de “tres categorías de ciberacoso”, nos encontramos con otras acciones o tipologías que están directamente relacionadas con las mismas. En primer lugar, dentro de lo que conocemos como ciberacoso en sentido estricto, podemos encontrarnos con diferentes acciones como el ciberacecho o C*yberstalking*, el cual implica aquellos seguimientos vía online que realiza el acosador a la víctima. Dentro de esta categoría también podemos encontrar tipologías como el *Flame*, mediante el cual el acosador provoca mediante un mensaje incendiario enviado a un foro o lista de correo con la finalidad de incitar reacciones airadas de sus participantes (suele contener insultos u ofensas y puede estar dirigido a todos en general, a un grupo de usuarios o a alguien en particular) y la guerra de notificaciones, que es un método empleado a veces en caso de ciberacoso para implicar a un proveedor de servicio contra la víctima.

En segundo lugar, el ciberacoso sexual cuenta también con distintas tipologías. Una de ellas es el *grooming*, mediante el cual, se produce el acoso por parte de un adulto hacia menores de edad con intenciones sexuales. Más aún, relacionado con el *grooming* nos encontramos con la sextorsión, qué, como la misma palabra indica, se trata de la extorsión realizada con intenciones sexuales a través de contenido de índole sexual de la víctima. En muchas ocasiones, detrás de estos tipos de acosos también se pueden esconder otros casos de pedofilia y pederastia. A su vez, este tipo de acosadores suelen emplear cebos (*Luring*) para atraer a niños a encuentros fuera de la red. Según cifras del Instituto Nacional de Estadística (2019), el *grooming* ha aumentado un 410% en los últimos años y, un dato relevante como causa de este hecho, es que casi el 90% de los menores de 10 años dispone de acceso a Internet y 1 de cada 4 tiene un móvil, lo que quiere decir, que las redes de pederastas y pedófilos han visto como los usuarios a los que acceder o engañar han aumentado en número.

En tercer lugar, el *ciberbullying* se centra en el ciberacoso entre menores. Como hemos visto en el punto anterior, el caso de Romina Perrone se corresponde con un tipo de *ciberbullying* denominado “web apaleador”. Es decir, la creación de una página web o social creada para hacer *ciberbullying* sobre algún menor, metiéndose con él/ella de manera pública y ridiculizándolo/la, destacando que, a menudo, se anima a otros internautas a participar en el abuso. Más aún, cabe destacar otro tipo de conducta dada en el ciberacoso entre menores y, esta, es la ciberviolencia de género, que se corresponde con todos los tipos de actos (insultos, ataques, chantajes, control…) por parte de una persona o un grupo de personas a otra u otros del sexo opuesto, jugando las nuevas tecnologías un papel central. Concluyendo, cabe destacar una tipología relacionada a este ámbito que ha surgido muy recientemente. Se trata del *Happy Slapping*. Esta acción se basa en gravar una agresión para posteriormente hacerla pública en las redes (también puede ser llevada a cabo por adultos).

Cabe destacar, que aunque las tipologías de acoso suelen afectar en mayor medida a dichas categorías con las que se ha relacionado, puede haber excepciones, pues el ciberacoso por género también puede producirse entre adultos. Además, estas tipologías pueden darse a través

de distintas acciones y comportamientos, como demuestra la encuesta realizada por *Statista* (2016), (Figura 5).

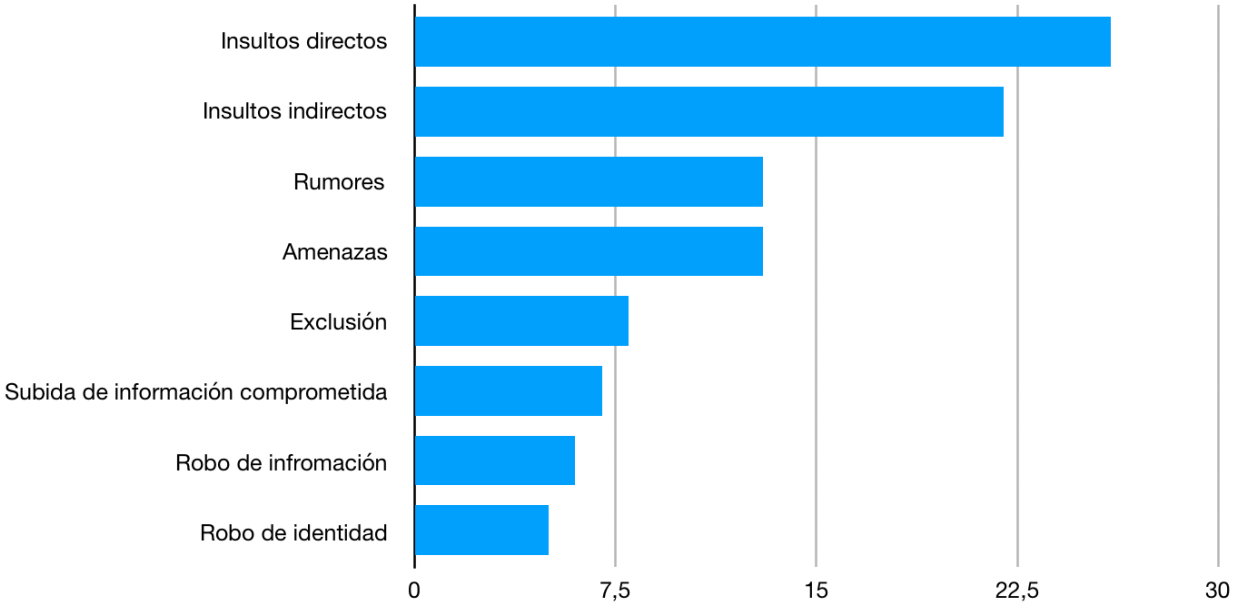

Figura 5. Conductas llevadas a cabo para desarrollar las tipologías estudiadas. Fuente: Statista

Finalmente, cabe destacar las víctimas más comunes dentro de esta problemática. Según un estudio llevado a cabo por la fundación ANAR (2016-2018), las chicas son las víctimas del 70% de los casos del ciberacoso escolar y, este tipo de acoso en línea representa ya uno de cada cuatro casos. Estos datos además, son respaldados por un estudio reciente llevado a cabo por Amnistía Internacional (2019) que llega a la misma conclusión en cuanto al ciberacoso escolar y, además, afirma que 1 de cada 5 mujeres adultas (18-55 años) sufren acoso en las redes sociales en España. Profundizando, un 19% de las encuestadas aseguró haber experimentado situaciones de acoso en *Facebook*, *Instagram* u otras redes sociales como *WhatsApp*. Aún más lejos, añade este informe que el 27% de las mujeres españolas vivieron amenazadas de agresiones físicas o sexuales a través de esos canales. Y es que, como muestran los estudios y estadísticas, el ciberacoso también es una cuestión relacionada con la violencia de género.

Además, corren especial riesgo de convertirse en víctimas los más jóvenes que navegan por las redes sociales (75%). Finalmente, hacer mención una vez más de la extrapolación del mundo "real" al "virtual" en el que, grupos discriminados, como los usuarios pertenecientes a colectivos LGBTI[23], siguen sufriendo acoso y persecución. Así lo afirma un estudio realizado por COGAM (2015-2016) en España durante los, en el cual se afirma que "*la LGBTI-fobia sigue campando*

[23] Estas siglas hacen referencia al colectivo formado por Lesbianas, Gays, Bisexuales, personas Transgénero e Intersexuales.

libremente en los centros de estudio donde el 60% del alumnado ha sido testigo de agresiones LGBT-fóbicas sufridas tanto por adolescentes LGBT como por todas aquellas personas que no reproducen los estereotipos de género de masculinidad y feminidad tradicional" y, además, recalca en la influencia de las tecnologías, pues "*el 15% del alumnado LGBTI padece ciberacoso por su orientación sexual y/o identidad de género, y entre ellos muy especialmente el alumnado trans; que más del 52% ha sido testigo de ciberacoso por ser o parecer LGBTI; y que el 24,11% del alumnado declara conocer a alguna persona que haya sufrido este tipo de abuso*". Una realidad alarmante sabiendo que el 11% del total del alumnado es LGBTI y el 0,1% es transexual.

Figura 6. Colectivos con más riesgo de sufrir ciberacoso.

El perfil de los acosadores en la red

Siguiendo con lo expuesto con anterioridad, podemos diferenciar distintos tipos de perfiles de acosadores según la tipología de acoso que estos ejerzan. Centrándonos en primer lugar en el ciberacoso escolar, cabe destacar que en España, según el último estudio realizado a nivel nacional por la ONG *Save the Children* (2017), se recogen datos como que un tercio de los alumnos reconoce haber agredido físicamente a otro compañero; uno de cada diez, haberlo amenazado, y el 50 %, haberlo insultado cara a cara y el 25 %, por las redes.

Específicamente en el acoso a través de la red, el perfil de estos agresores suele ser de un chico de entre 14 y 15 años (49 %), que se caracteriza por empezar a hacer uso de internet antes de lo habitual sin mediación de sus padres y por tener un control muy alto y rigidez familiar en el resto de aspectos y un autoconcepto emocional bajo. “El 67 % de los ciberacosadores o troles han sido víctimas de ciberacoso”, alerta Montiel[24] (2017), doctora en Psicología y profesora del Grado de Criminología de la UOC. “En la mayoría de casos, pues, los jóvenes que presentan comportamientos agresivos en línea necesitan recibir tratamientos adecuados no solo por su comportamiento disruptivo, sino también en la gestión de sus propias experiencias como víctimas", añade la experta.

Más aún, cobra una gran importancia el perfil del espectador del acoso, pues tiene un papel clave en la dinámica de la victimización, es mucho más heterogéneo: «Su actitud, desde el apoyo, la aceptación sin intervención o la defensa de la víctima, puede mantener o romper el acoso», especifica Montiel (2017).

En segundo lugar, tenemos el perfil del ciberacosador sexual. Es un usuario que agrede a otros y que suele iniciar su acercamiento a estos mediante la empatía y/o engaños para pasar al chantaje más cruento. La finalidad de estos suele ser la obtención de imágenes íntimas de las víctimas y, en casos extremos y si la distancia lo permite, un encuentro en persona. Los acosadores son en mayoría hombres de cualquier edad y condición social y económica. Esto lo confirman los últimos datos ofrecidos por el Ministerio del Interior y el Sistema Estadístico de Criminalidad (2017), en el que se afirma que el 94% de delitos sexuales en línea registrados fueron causados por un hombre. De los 4.912 casos, 291 los cometieron chicos menores de edad (de 14 a 17 años) y 77 chicas.

“Son personas aparentemente normales e integradas socialmente, habitualmente hombres, pero cada vez más mujeres, de casi cualquier edad y ubicación geográfica, con acceso a internet y que se saben mover por el ciberespacio. Forman redes virtuales donde intercambian técnicas y

[24] Irene Montiel, profesora de Criminología en la UOC y experta en psicología.

materiales visuales de los abusos cometidos. Con internet todo es más fácil para ellos", afirma Montiel (2017).

En tercer lugar, vamos a dar paso a hablar a cerca del perfil de los casos de acoso entre adultos. Cabe destacar, que se sigue la corriente dada en los otros tipos de acoso, en los que el índice de victimización es mayor entre las mujeres. Como se ha venido analizando, el conjunto de conductas y ataques que se pueden realizar, son tan amplios y variados como posibilite el uso de la tecnología, los medios utilizados y, por supuesto, los conocimientos y habilidades del agresor. A su vez, podemos distiguir dos tipos de perfiles completamente distintos a la hora de acosar según el sexo del acosador, el masculino y el femenino.

El perfil de un acosador masculino se caracteriza porque emplean un acoso más directo, lo que a la larga se traduce en conductas agresivas contra las propiedades de la víctima. Además, estos desarrollan actitudes despectivas (insultos, burlas, etc) que vuelvan a través de internet y las redes sociales.

Por otra parte, el perfil de un acosador femenino se caracteriza por el empleo de un acoso social caracterizado por aislar a la víctima, es decir, mediante las redes, intentan utilizar la marginación y la exclusión grupal de la víctima para adentrar a esta en la soledad. Esto lo hacen mediante la ayuda de la difusión de mentiras o rumores falsos. Como es obvio, todo esto tiene una especial gravedad cuando se comete a través de internet y las redes sociales, dado el efecto viral y de expansión, lo que provoca que el daño psicológico a la víctima sea muy superior al acoso tradicional.

De manera general para ambos perfiles, cabe destacar que son usuarios con una escala de valores que no se corresponde con los valores normativos o socialmente aceptables, entre los que se incluyen la violencia, la insolidaridad, la transgresión de las normas sociales o el egoísmo. Además, suelen proceder de entornos familiares donde se han socializado sin referentes morales claros, con estilos educativos autoritarios, inexistentes o permisivos, carentes de normas claras, donde los padres ejercen un escaso control sobre los hijos y donde se potencia el uso de la violencia.

Según la Fundación CSZ (2016, 2017), son diversos los motivos que pueden llevar a estos usuarios a actuar como acosadores, entre los que se incluyen la rabia, la envidia, los celos, el sentimiento de venganza, la inmadurez, el aburrimiento, la imitación de los modelos de los adultos, la necesidad de escenificar su posición de poder o liderazgo, los prejuicios raciales o sexuales, etc. En este tipo de acciones, también pueden actuar movidos por las emociones negativas tras las rupturas personales, en especial las de tipo sentimental o de pareja. Con frecuencia el ciberacoso es un modo (inadecuado) de afrontar la frustración.

Cabe comentar, a su vez, que, la plataforma preferida empleada por los acosadores es *WhatsApp* (81%) frente al resto de redes sociales y *apps* (36,2%), y que las víctimas de estos usuarios suelen ser mujeres (un 70%). Además, la mayoría de casos suele darse con algún joven "de por medio" (87%) y la víctima suele pertenecer a una familia convencional (85,9%) y sin problemas económicos (81,8%). Finalmente, para terminar de conocer conforme a la realidad el género de los acosadores según el tipo de víctima, es recomendable visualizar la Figura 7 y 8 basadas en un estudio llevado a cabo por la fundación ANAR (2016-2018)[25].

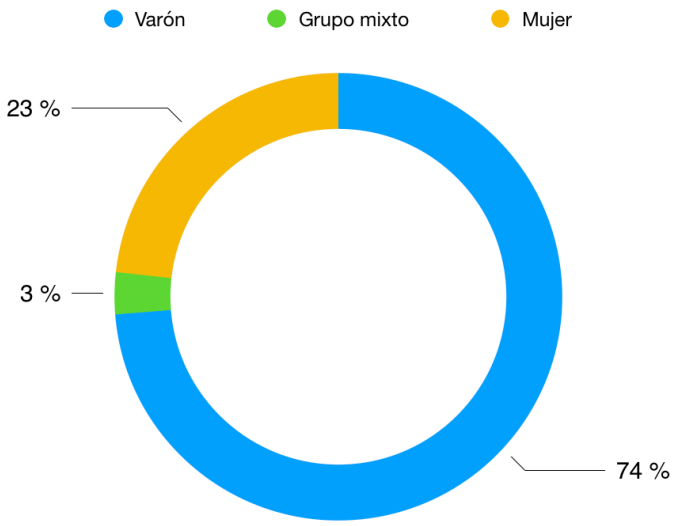

Figura 7. Cuando la víctima es mujer. Fuente: Fundación ANAR (2016-2018)

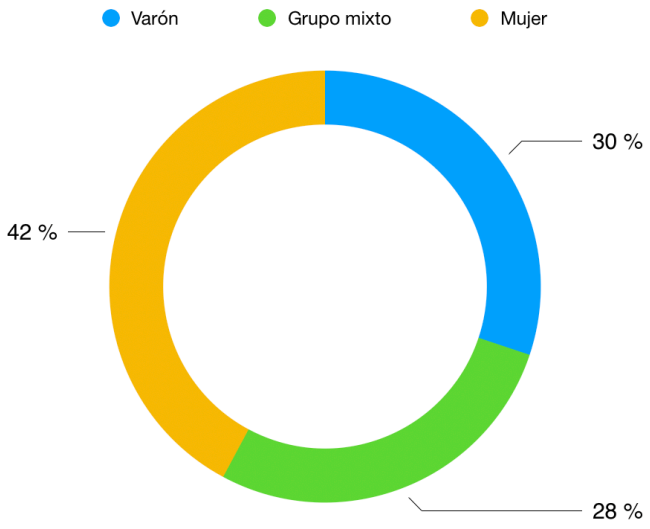

Figura 8. Cuando la víctima es hombre. Fuente: Fundación ANAR (2016-2018)

[25] I y II Estudio sobre ciberacoso y ciberbullying publicado por ANAR (2016-2018).

Detección

Cuando nos encontramos ante un caso relacionado con el ciberacoso, los profesionales que trabajan en este ámbito tendrán que llevar a cabo ciertos procesos que facilitarán el diagnóstico final de la víctima para conocer el punto en el que esta se encuentra. En general, esta identificación y procesos se llevarán a cabo de manera clínica. La intención de estos es ofrecer un pronóstico y valorar la gravedad y el riesgo del paciente, así como valorar la necesidad de derivación a salud mental urgente, pues en casos extremos de ciberacoso la idea del suicidio puede llegar a darse en víctimas.

Siguiendo la Guía del Ciberacoso para Profesionales de la Salud (2015) deberá de procurarse llevar a cabo una buena coordinación entre familia, víctima, responsables clínicos y/o ayudantes externos (asociaciones, cuerpos de seguridad del estado) y colegios o instituciones académicas (en caso de darse el ciberacoso en este tipo de entornos, en víctimas menores de edad), pues se deberá de dar rienda suelta al rápido cese del ciberacoso, mediante la búsqueda de apoyos, A su vez, se deberá de valorar y asesorar la necesidad de denuncia inmediata (según gravedad y tipología del caso) y prevenir paralelamente que la víctima sufra un nuevo ciberacoso (educando al menor y a los padres en el uso adecuado de las TIC) .

¿Cómo actúa la víctima? Para contrarrestar el ciberacoso, es esencial “pillarlo” desprevenido. Cabe destacar, que hay algunas conductas y comportamientos de las víctimas que ayudarán a sus allegados a darse cuenta de que algo inusual le sucede al acosado.

La observación va a ser una de las acciones fundamentales a la hora de detectar el ciberacoso. Gracias a esto, podremos reconocer cambios de humor o comportamiento, cambios en la motivación para realizar actividades comunes o quejas espontáneas, como por ejemplo, en caso de ciberacoso escolar, mostrarse reacio a ir a la escuela por ningún motivo aparente.

Otro de los factores de gran importancia es la comunicación. En una sociedad dominada por las nuevas tecnologías y las redes sociales, es de gran importancia mostrarnos abiertos al diálogo y a la conversación “cara a cara”, ya que, de esta manera, se estará naturalizando un hábito que poco a poco va siendo cada vez menos inusual y, en ocasiones, la víctima se olvida o carece de empatía con sus seres más directos.

Este último factor, el de la comunicación, es de gran importancia pues, la víctima tiende a dejar de socializarse y a abandonar las relaciones personales en el “mundo real”. Pasar por este tipo de problemáticas es sinónimo de cambios y los usuarios pueden querer aislarse de la familia pero si también se separan de su círculo de amistades y se recluyen en su habitación –sin interactuar tampoco en redes sociales-, tal vez merezca la atención de sus más allegados.

A su vez, cabe destacar que otro de los factores importantes es la aparición de cambios físicos inesperados en la víctima tales como pérdida de peso, estrés, o falta de sueño. Estos síntomas pueden representar que algo no va bien. Más aún, si la víctima es sospechosa de de fingir enfermedades para no llevar a cabo su rutina diaria o se desconecta por completa de las redes (hábito extraño), puede indicar que ésta esté evitando a sus acosadores, tanto en el ámbito digital como en el físico. Todo esto, respaldado por *Internet Segura for Kids* (s.f.).

Como se puede ver, son muchos los handicaps existentes para poder conocer con la suficiente antelación cuándo un usuario está siendo víctima de ciberacoso: en general, el agredido no comunica la situación y predomina la ley del silencio por los espectadores pasivos. Ello trae como consecuencia que en un porcentaje muy elevado de los casos son las familias quienes tienen mayor capacidad de detección de las agresiones sufridas por las víctimas. A su vez, cabe destacar que debido a esta pasividad por parte de terceros y la asocialización de la víctima, en muchas ocasiones estas problemáticas se detectan demasiado tarde, cuando la víctima lleva ya mucho tiempo sufriendo los ataques, las agresiones o las humillaciones y no se ha actuado con la celeridad que el asunto requiere.

Ahora bien, por otra parte, tras la detección e intervención del ciberacoso, la siguiente actuación por la que hay que apostar es la recuperación de las víctimas. Se trata de restaurar el daño ocasionado facilitando a las víctimas todas las herramientas y recursos necesarios para superar la situación vivida. Resulta, por lo tanto, esencial que las víctimas reciban protección y un seguimiento especializado tanto en el ámbito educativo, social o sanitario, evitando por supuesto la revictimización.

En ese proceso de recuperación se ha de tener presente asimismo al agresor. Se deben de buscar las razones que motivan su comportamiento, poniendo en marcha mecanismos de justicia restaurativa encaminados su educación y estudiando, con la ayuda de especialistas, el grado de criminalización del acto que ha llevado a cabo. No es infrecuente, como ha ocurrido en diversos casos, que el agresor repita un comportamiento que ha llevado a cabo de manera frecuente y que éste sea, a su vez, víctima de violencia en otro escenario. Tampoco hay que descartar que el agresor padezca una patología no diagnosticada o no tratada (Figura 9).

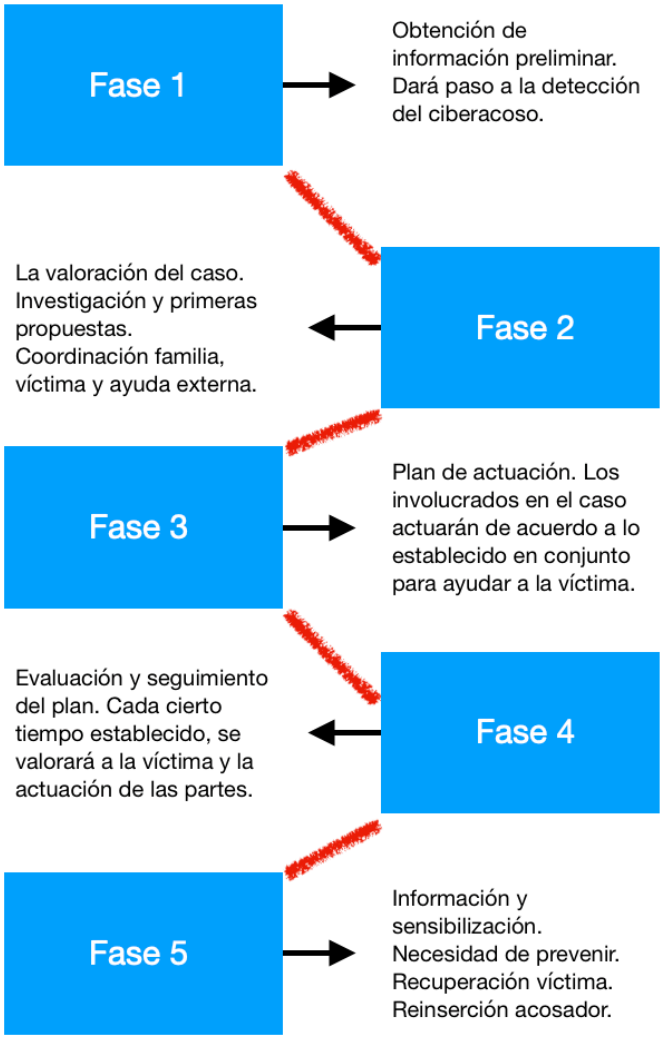

Figura 9. Fases del proceso en la detección del ciberacoso. Fuente: basado en los estudios analizados.

Capítulo 3: Fenómenos relacionados con el ciberacoso

Espionaje

Uno de los fenómenos relacionados con el ciberacoso es el espionaje a través de las redes sociales. A nivel doméstico, para que un amigo o un desconocido pueda espiar tu móvil necesita instalar una aplicación de *spyware* en él. Para ello, va a necesitar tener acceso físico a tu teléfono y ser capaz de desbloquearlo para instalar algún tipo de aplicación “APK”, las cuales además siempre suelen ser de pago, por lo que tendrá que “rascarse” el bolsillo y querer saber realmente sobre ti. Este fue el método que empleo una mujer condenada a un año de prisión y 1.080 euros de multa por espiar a su pareja, pues ésta leyó unos sms que su ex se había intercambiado con su vecina (cabe destacar que este tipo de acciones es ilegal en el ámbito español), Barrera (2015)[26].

Esta normativa está recogida en el artículo 197.1 del Código Penal, tal y como recoge Del Rosal (2018), en el cual se recoge que este tipos de delitos (interceptar telecomunicaciones ajenas sin consentimiento, norma aplicable también en el ámbito familiar) están castigados con penas de cárcel de uno a cuatro años, además de sus respectivas multas económicas dependiendo de la gravedad de los delitos[27].

Otra alternativa es hacer que nosotros mismos nos instalemos la aplicación mediante la técnica del *phishing*. Estos espías cibernéticos actúan de tal manera que mandan un mensaje de tipo "oye prueba esta app", o enviando un correo electrónico en el que se hacen pasar por otra persona o empresa para lo mismo, para que nos descarguemos una app concreta y la instalemos en nuestro móvil.

Son varias las aplicaciones que nos pueden afectar para conseguir tal fin, pero por lo general, la mayoría funciona de forma parecida. Su función suele ser la de actuar como un virus informático, escondiéndose en nuestro móvil y obteniendo información y grabaciones que luego envían por Internet a quien nos las haya instalado y la esté controlando. Algunas de las aplicaciones más conocidas y utilizadas son, por ejemplo, *XNSPY*, *Spyzie* y *Flexispy*, entre otras. Estas cuentas con muchas de las características citadas, aplicaciones capaces de visionar el contenido al que accede un usuario (tanto en el propio dispositivo como en redes sociales), rastrear posición geográfica, contactos e historial de llamadas, entre muchas otras funcionalidades.

La buena noticia respecto a este tipo de espionaje es que vamos a poder prevenirlo e incluso contamos a nuestra disposición con aplicaciones específicas *anti-spyware* que van a detectar este tipo de aplicaciones y software malicioso y que van a evitar a su vez que estos se instalen en nuestros dispositivos (ver Capítulo 5). Por otra parte, si desconocemos estas aplicaciones o

[26] Silvia Barrera, investigadora y redactora de la cadena de televisión y comunicaciones La Sexta.

[27] Pedro del Rosal, investigador y redactor del periódico y publicación El País.

métodos preventivos, cuando detectamos este tipo de problemáticas en nuestro dispositivo podemos acceder a su vez a restablecer nuestro móvil a sus valores de fábrica para que elimine todas las aplicaciones incluidas en él, pudiéndolo así, una vez restablecido y reiniciado, detectar cualquier *software* o aplicación "impostora", pues todas las demás (benignas se eliminarán).

Más aún, cabe destacar que la intención de estos "espías" no siempre es el mero espionaje, si no que debido a toda la información que recaban y a la que acceden estos, surgen nuevos delitos como la suplantación de identidad. Estos usuarios aprovechan los datos para crear perfiles falsos en redes sociales u otro tipo de plataformas para hacerse pasar por ella pudiendo incluso acceder a más información aún para posteriormente amenazar a la víctima de esta suplantación o extorsionarla (acceso a conversaciones privadas, fotos personales, etc). A su vez, también surgen nuevos comportamientos ilícitos como usar esa identidad para atentar contra el honor de una tercera persona o cometer un delito de calumnia a través de las redes sociales. Si llegados a este punto una víctima no ha podido prevenir o detectar mediante los métodos citados con anterioridad estos delitos (ya es tarde), deberá de denunciar estos hechos ante las Fuerzas y Cuerpos de Seguridad del Estado.

Será de vital importancia recabar pruebas de la suplantación (por ejemplo, mediante capturas de pantalla), avisar a nuestros contactos de que se está teniendo un problema de este tipo y pedirles que denuncien dicho perfil para que los gestores de las redes sociales lo eliminen cuanto antes.

Destacar a su vez que dicha acción puede encuadrarse perfectamente en el delito de usurpación del estado civil tipificado en el artículo 401 del Código Penal, que dice que "*El que usurpe el Estado Civil de otro será castigado con la pena de prisión de seis meses a tres años*", tal y como informa Perito Informatico (2016).

Espionaje, empresas y la falta de ética

Por otra parte, cuando se habla de espionaje, no se hace referencia únicamente al hecho de que un usuario ande "husmeando" en el perfil o dispositivo de otro, sino que la problemática va más allá de lo que nosotros, como usuarios, podemos apreciar.

El empleo de las redes sociales a través de dispositivos electrónicos, como los *smartphones* o las tabletas, ha hecho que nuestros datos sean mas vulnerables. Tal y como recoge el diario 20minutos (2013), Edward Snowden evidenció a la población mundial de este hecho, filtrando a los medios el espionaje masivo de la NSA[28], marcando un punto de inflexión. Las filtraciones realizadas por este ex de la NSA causó un revuelo mundial y una guerra diplomática de la que

[28] Agencia de Seguridad Nacional (Estados Unidos)

salió muy mal parada EEUU, destapada y acusada de espiar a más de 35 líderes mundiales y de tener además acceso a millones de datos de los usuarios.

Ahora bien, este tipo de casos no solo se han dado con agencias de inteligencia globales de por medio, sino que, las propias redes sociales, han sido acusados en innumerables ocasiones de "jugar" con nuestros datos. "*Son grandes agencias multinacionales de recopilación de datos que construyen una nueva lógica de acumulación*". Así define a las redes sociales el máster en Derecho Administrativo Castro[29] (2017), con *Facebook* y sus 2.250 millones de usuarios a la cabeza, para advertir sobre el cuidado que se debe tener al navegar por ellas.

La empresa creada por Mark Zuckerberg para comunicarse internamente con sus compañeros universitarios que se popularizó a partir de 2004, se ha convertido, junto con *Google*, en actor clave del orden mundial establecido. Saben todo de nosotros y lo usan con fines comerciales, empresariales y políticos. *Facebook* facturó 26.000 millones de dólares en 2016. Tiene 2.250 millones de usuarios, a los que se suman los 2.500 millones que le aportan sus empresas asociadas *Whatsapp* e *Instagram*. En esta etapa de masificación total de las redes, los algoritmos permiten descifrar gustos alimenticios, opciones sexuales e ideologías. Por eso, se han convertido en un arma para orientar consumos, definir campañas e incidir en elecciones.

"Ellos juegan con estas ideas y fantasías que venden —inclusive Mark Zuckerberg- de que vivimos en una comunidad global, en un plano en el que estamos todos igualados para producir y acceder a la información. No es así de ninguna manera, porque los algoritmos y programas digitales a través de los cuales reciben o transmiten tus intimidades, están destinados a lograr las informaciones consideradas importantes por las empresas que contratan estas redes para llegar a tu persona en tanto consumidor", opinó Castro (2017) .

De hecho, uno de los casos mas sonados relacionados con *Facebook* es el caso de *Cambridge Analytica*. La red social se vio envuelta en una serie de escándalos de obtención de los datos personales de sus usuarios sin su consentimiento explícito. En abril del 2018, el fundador de *Facebook*, Mark Zuckerberg, testificó ante el Congreso de EEUU acerca del marco en el que la consultora británica *Cambridge Analytica* accedió a datos de por lo menos 87 millones de usuarios de la red social y supuestamente los utilizó en campañas políticas —en particular, para manipular la opinión pública a favor del *Brexit* en el Reino Unido y en la candidatura de Donald Trump en las presidenciales de EEUU— a través de la aplicación T*his Is My Digital Life*.

Más aún, la veracidad del caso y la culpabilidad de esta multinacional fue totalmente confirmada cuando el 12 de julio, la Comisión Federal de Comercio de EE.UU aprobó de aproximadamente 5.000 millones de dólares con *Facebook* por haber violado la privacidad de sus usuarios, tal y como lo confirman diversos medios como Europa Press (2018).

[29] Fredes Castro, máster en Derecho Administrativo y especialista colaborador en la web "Sputnik Mundo" (2017).

Este hecho, el espionaje que las propias redes sociales hacen a sus usuarios y el intercambio de datos e información entre las distintas instituciones, fue confirmado en una entrevista por el ex asesor en tecnología de Barack Obama[30], Andrew McLaughlin (2011), que afirma que "*son una fabulosa fuente de información para los que espían a sus ciudadanos*" y que "*el espionaje en redes sociales es la forma más efectiva de control estatal en Internet*".

Pero no solamente nos vigilan y emplean los datos para los fines analizados con anterioridad, sino que también son capaces de regular nuestro consumo. En determinadas ocasiones, cuando por ejemplo hablamos por *WhatsApp* con nuestro mejor amigo de la PS4, posteriormente, cuando navegamos por la red nos encontramos con anuncios de la consola de *Sony*. ¿Magia o… ingeniería social? Un estudio realizado por *Ghostery* (2017) muestra las empresas que más seguimiento hacen a sus usuarios. *Google* se lleva el premio a la compañía que más seguimiento realiza en la red o, dicho de otro modo, la compañía que más espía la actividad de los internautas (Figura 10).

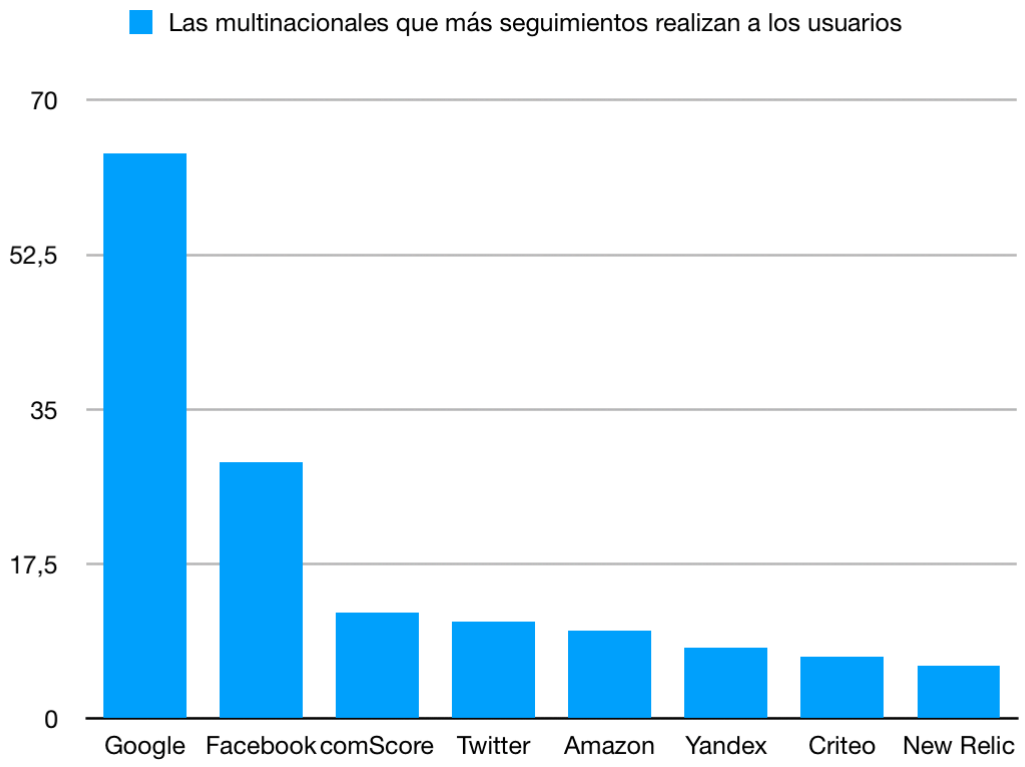

Figura 10. Las empresas que más nos espían mediante redes sociales y las nuevas TIC. Fuente: *Ghostery*

[30] Ex-Presidente de Estados Unidos.

Desinformación y Fake News

En la actualidad, es evidente que la sociedad esta viviendo una era en la que los datos y la información viajan de una manera nunca antes vista en la historia de la humanidad. Esto a permitido que muchas personas alrededor del mundo estén informadas de todo tipo de acontecimientos a nivel global y, a su vez, se ha creado una democratización que antes no existía en diferentes temas. Sin embargo, este fenómeno también tiene un efecto colateral, pues la información falsa, sensacionalista y sin fundamentos también se propagada rápidamente y sin fronteras.

La rápida propagación de la información (tanto verídica como falsa) es en gran parte a las redes sociales, pues son herramientas que nos ofrecen datos de manera instantánea a nivel global e incluso la posibilidad de seguir acontecimientos en tiempo real. Solo en Estados Unidos, estadísticas reales (únicas conocidas de un territorio concreto) que afirmó el CEO de *Facebook* Mark Zuckerberg (2016) afirman que "*más de un 44% de la población usa las redes sociales como fuente de noticias*". Además, *Twitter* es una de las redes sociales mas utilizadas por los usuarios para este tipo de ámbito, debido a la posibilidad de emplear mensajes cortos y concisos.

Hay mucha información falsa que se propaga a la población mediante las redes sociales. *Facebook*, que es la red social con el mayor numero de suscriptores, cuenta con numerosas noticias que contienen bulos y mala información. La creación de páginas falsas y la generación de noticias inciertas nace de la necesidad de ciertas páginas de prensa amarillista cuyo objetivo es beneficiarse o lucrarse o bien económicamente o bien mediante nuevos seguidores. El *modus operandi* de este tipo de páginas se basa en el empleo de titulares llamativos y exagerados (e inventados) para atraer la atención de los usuarios.

Estos bulos con contenido un tanto controversial y escandaloso suelen propagarse a gran escala, lo que influye directamente en la opinión de muchos de los usuarios y puede causar un gran daño a muchos otros. De hecho, antes de las elecciones de EEUU circularon por *Facebook* noticias falsas y titulares tales como "*Agente del FBI sospechoso de dar conocer los correos de Hillary Clinton fue encontrado muerto en un aparente asesinato*" lo que, claramente, afectó a la candidata a la presidencia, pues finalmente perdería las elecciones presidenciales.

Desafortunadamente, cada vez es más difícil identificar las noticias falsas distribuidas por las redes sociales. Esto se debe a que la prensa amarilla sabe como crear unas buenas cuentas de usuario, empleando nombres y métodos parecidos a los de medios de comunicación de prestigio. Más aún, prosiguiendo con el caso anterior (Hillary Clinton) hay un análisis realizado por *BuzzFeed* (2017) el cual encontró que, durante los últimos tres meses de la carrera presidencial,

las noticias falsas atrajeron más visitas y fueron compartidas más que reportajes legítimos del *New York Times, The Washington Post* y CNN.
Además de *Facebook*, hay usuarios de otras redes sociales que se están lucrando mediante la desinformación. Esta red social es *YouTube*, la cual cuenta con un sistema de pago a los creadores de contenidos según las visitas y los ingresos que generen por publicidad. Muchos de estos canales emplean el *clickbait*, que, similar a la prensa amarilla, consiste en emplear un título atractivo para que el usuario se meta en el vídeo. Cuando este accede al mismo, se siente engañado, pues el titulo por el que ha entrado al vídeo es totalmente engañoso en relación al contenido que se puede visualizar.

¿Cómo actúan las empresas y los buscadores respecto a este tema? Pues bien, el tratado de la desinformación y de las *fake news* no es un tema sencillo como dice Nayak (2019), vicepresidente del departamento de *Google* que se encarga de la herramienta de búsqueda: "*Es duro decirlo, pero no creo que se puedan crear algortimos que identifiquen qué información es falsa y cuál no*", explica. Además afirma que *Google* mejora día a día en este aspecto y en el refinamiento del motor de búsqueda más famoso del mundo. La mejor solución para el vicepresidente pasa por "*posicionar mejor la información relevante que procede de fuentes autorizadas*", afirma Nayak (2019).

Paralelamente a la actuación de estas empresas vinculadas con los motores de búsqueda y las redes sociales, puedo afirmar que en España contamos con una herramienta de prevención, más concretamente una aplicación, que ha lanzado *Maldita.es*, la cual, mediante un estructurado grupo de trabajo detrás de ésta, opta por mostrar a los usuarios que naveguen por ella noticias que ya han sido desmentidas y bulos o prensa amarilla verificada por sus propios trabajadores (ver Capítulo 5).

En definitiva, la desinformación es una problemática que ayuda a generar beneficios económicos y a manipular a las masas. A su vez, cabe destacar que no es una problemática emergente a raíz del nacimiento de internet y las redes sociales. Sí es verdad que a partir de la aparición de estas, como se ha comentado con anterioridad, la globalización y difusión de datos ha crecido exponencialmente y a día de hoy vemos con mayor continuidad todo tipo de casos de desinformación y bulos. Pero el origen de esta desinformación se remonta mucho tiempo atrás, empleada en medios de comunicación tradicionales como periódicos, televisión, radio y revistas. Sin ir más lejos, pese a la globalización que vivimos hoy en día, hay países como Corea del Norte y China donde no existe la libertad de expresión. Los medios son controlados por el estado y, siempre han sido empleados para desinformar a la población, ganar influencia política y mantener una imagen de su gobierno que los beneficie (Figura 11).

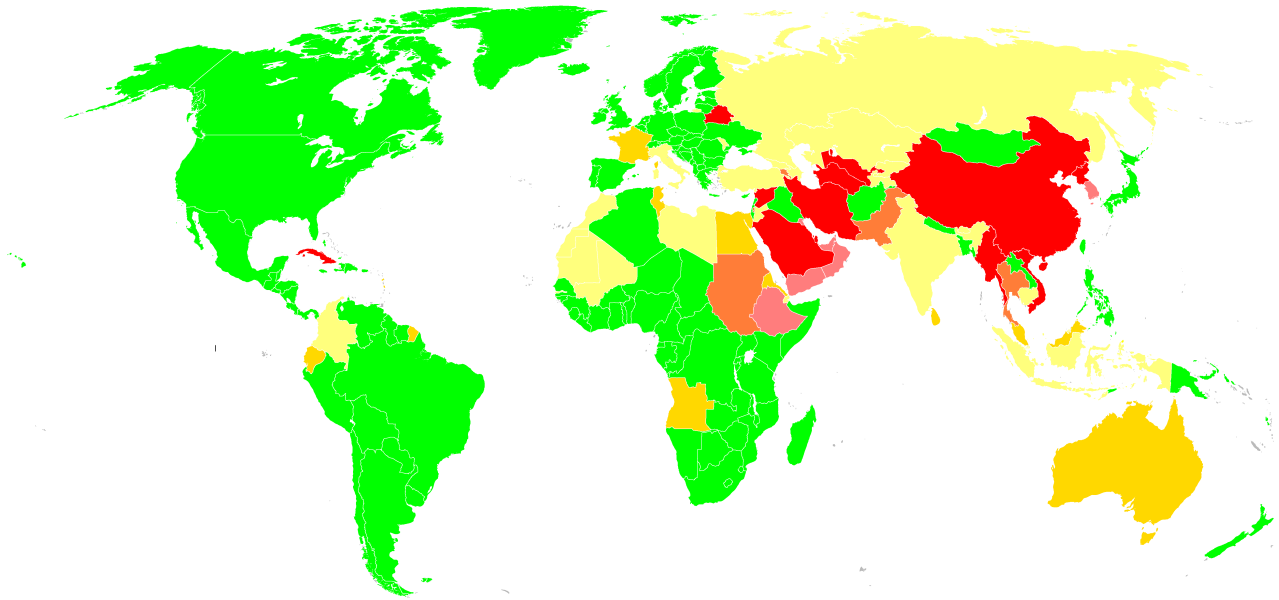

Figura 11. Mapa mundial a cerca de la censura y el acceso a internet. El color verde representa la libertad de expresión, el rojo la restricción. Fuente: LE-VPN (2016). La situación actual es la misma.

Campañas de desprestigio

Hay una sección de usuarios en redes sociales que bien porque tienen un ego muy frágil o bien porque no han sido educadas en la generosidad, creen que dañar a los demás les da más poder. Son personas tóxicas que lejos de alegrarse de que a las demás personas les vaya bien, intentan contaminar su entorno, manipular a la gente y hacer una campaña de desprestigio social. Para ellos utilizan las redes sociales y las conexiones como armas arrojadizas, intentando generar imágenes alteradas de las personas a la par que intentando que su imagen quede inmaculada.

Según la psicóloga especialista Alcaide[31] (2019), muchas personas, "*especialmente aquellas con trastornos de la personalidad - es decir, que no pueden adaptarse y ser flexibles sino que siempre siguen una pauta de conducta rígida -, pueden hacer una proyección de la culpa en alguien y chantajear emocionalmente o atacar a la persona que hacen responsable. Normalmente la persona atacada es aquella que les ha generado algún tipo de frustración, envidia o que ha dejado al descubierto su frágil ego*".

Es imprescindible que los usuarios que sufran este tipo de conductas las identifiquen como un maltrato psicológico en toda regla. El acosador, la persona que inicia esta campaña de

[31] Paula Alcaide. *Psicóloga, terapeuta y profesora experta.* Comparte sus experiencias a través del blog Paula Alcaide "Mujeres libres de estigma".

desprestigio o difamación, tiende además a convencer al entorno de la víctima para que se aleje de ella y de “echarla la culpa” de la situación. Alcaide (2019) asegura que ha recibido además pacientes que han sufrido estas campañas de desprestigio con claros síntomas de ansiedad, debido al “*machaque al que se ven sometidos*”.

Hay varias pautas para combatir estas campañas de desprestigio. Lo mejor que podemos hacer de cara a estas difamaciones, según la psicóloga experta, es no picar en el anzuelo y “*seguir el rollo al acosador*”, apoyarnos en nuestros allegados y no asumir una culpa que ha sido inventada y no nos corresponde. Esto lo podemos conseguir emitiendo un comunicado objetivo sobre los hechos ocurridos aclarando así la situación y sin tener que contactar o responder de manera directa al difamador (además podríamos incluso rogarl la lucha contra este usuario y la denuncia conjunta vía redes sociales, pues estas se encargarían automáticamente de comprobar la situación y cerrar el perfil del acosador). Así podremos protegernos e incluso, si la cosa fuera a más, podríamos poner en marcha medidas legales, pues nos encontramos a su vez ante un delito de injurias y/o calumnias.

Estas acciones se recogen clasificadas en los artículos 208 y 205 del código penal, dentro de los delitos contra el honor. En cuanto a la pena tipificada, en el caso del delito de calumnias, la normativa española recoge que serán castigadas con las penas de prisión de seis meses a dos años o multa de 12 a 24 meses, si se propagaran con publicidad y, de lo contrario, con multa de seis a 12 meses. La pena para el delito de injurias graves hechas con publicidad será de multa de seis a 14 meses y, en otro caso, con la de tres a siete meses, tal y como afirma Legalitas (2019).

Desde el punto de vista de las TIC no contamos con una solución o aplicación definitiva o explícita a día de hoy para resolver dicha problemática, pues no hay posible solución inmediata para un usuario que emplea un perfil y que de un momento a otro opta por difamar o iniciar campañas de desprestigio contra otras personas. Las propias redes sociales cuentan con el “botón Denuncia” mediante el cual podremos dar nuestros propios motivos y hacer ver a los gestores de la misma el mal comportamiento que tiene ese usuario en la red social para que opten por cerrarle el perfil. También contamos con el apoyo de otros usuarios que pueden ponerse a nuestro favor viendo la injusticia que se comete contra nuestra persona. No olvidar tampoco que dependiendo de la tipología de gravedad del asunto, los cuerpos de seguridad del estado y su sección especializada en actividades telepáticas estarán dispuestos a escuchar nuestro caso.

No obstante, cabe destacar al igual que en el punto anterior la aplicación lanzada por *Maldita.es*, pues si somos testigos de una campaña de desprestigio hacia algún personaje famoso o político, dicha aplicación tratará de estar actualizada al día y determinar si dicha noticia es verídica o si se trata de desinformación, una *Fake New* o bien, una campaña de desprestigio (pues una campaña de desprestigio, en la mayoría de ocasiones, trata con información manipulada y mentiras).

Campañas de desprestigio y empresas

Sin razón ni motivo aparente, cuando una empresa o emprendedor está en redes sociales, es muy posible que alguien intente crear una campaña de desprestigio en su contra. Manejar esa situación imprevista y nada agradable puede ser difícil y si no se toman las medidas adecuadas, quizás sea peor el remedio que la enfermedad.

Pueden darse comentarios negativos en las redes sociales de restaurantes, hoteles, tiendas de ropa, y otro tipos de negocios; como también publicaciones, imágenes o videos que afectan la reputación online de estos, ya que gracias a la inmediatez de los medios digitales este tipo de opiniones llegan a miles de personas en muy poco tiempo, afectando severamente el prestigio de éstas.

Cuando los usuarios observan este tipo de acciones en las redes sociales de los negocios en los que consumen regularmente los toman muy en cuenta y dudan en volver a consumir en ese lugar, dependiendo del comentario, los usuarios condenan a las empresas. En muchos casos, los comentarios son falsos, historias a medias o comentarios muy bien elaborados (fundamentados) con la finalidad de causar desprestigio; es muy importante gestionar este tipo de información y saber tomarles partido de manera positiva.

Hay que darle una gran importancia a esto. Es decir, no se puede ignorar la poderosa influencia que tienen las redes sociales en prácticamente todas las esferas de la sociedad. En el ámbito comercial han llegado a modificar gustos y comportamientos de los consumidores hasta tal punto que actualmente “7 de cada 10 consumidores consultan opiniones y recomendaciones en las redes sociales antes de adquirir un producto”, según señala un estudio de la firma *Deloitte* (2013).

La primera pregunta que puede venir a la mente es ¿por qué? Puede ser una de mil razones, desde un cliente insatisfecho hasta la aparición de la figura del *hater*. Hay que saber diferenciar entre estos dos tipos de usuarios, pues un cliente insatisfecho probablemente también desprestigie en mayor o menor medida a la entidad, pero se debe de prestar atención a los reclamos o peticiones de los mismos, pues mediante esa crítica la empresa podrá mejorar sus servicios. Sin embargo, los *haters* son usuarios que navegan a sus anchas por las redes sociales y que se dedican a despreciar, difamar o criticar destructivamente a una persona, a una entidad, a una obra, a un producto o a un concepto en particular, por causas poco racionales o por el mero acto de difamar.

La marca Nutella conoce desde hace un tiempo el efecto *hater*. Como informa *Antevenio* (2016), queriendo mejorar su estrategia de Marketing y Comunicación, la empresa inició la campaña *Dites-le-avec Nutella* (dilo con *Nutella*), que se centraba en la personalización de la etiqueta de los envases. Es decir, *Nutella* solicitaba a sus usuarios que compartieran mediante las redes sociales

su etiqueta virtual que incluía un mensaje personalizado. Sin embargo, algunos usuarios lo aprovecharon para incluir mensajes que atacaban a la marca. Nutella por su parte vetó una serie de términos en los que se encontraban: obesidad, diabetes, boicot, palabras sexistas, términos racistas u homófobos o ataques directos a la empresa. El viral que buscaba la marca se produjo pero con el efecto contrario.

En contraposición, *McDonald´s* lanzó también hace dos años una campaña por *Twitter* con el *hashtag #McDStories*, con el fin de que los clientes compartieran experiencias positivas con los productos de la marca. Pero los internautas en vez de hablar sobre los servicios o actos positivos de la empresa (tal y como esperaba *McDonald´s*), utilizaron el *hashtag #McDStories* para criticar a la compañía. Malestares estomacales, pelos, uñas y hasta ratones acompañaron los mensajes dirigidos con dicho *hashtag*. En total fueron más de 72.000 *tweets*, la gran mayoría negativos, según la firma *Business Insider* (2012).

Ante este escenario, los directivos de la empresa no tuvieron más remedio que admitir la veracidad de ciertas críticas y el rotundo fracaso de la campaña en redes sociales. “Aprovecharemos las nuevas oportunidades publicitarias ofrecidas por las redes sociales y aprenderemos de esta experiencia”, agregó Rick Wion (2012), director de medios digitales de McDonald’s en EE. UU.

Capítulo 4: Las leyes y las redes sociales

Privacidad y seguridad

Como se ha venido diciendo, una red social es una aplicación de internet que permite crear contenidos y compartirlos con otros usuarios. Precisamente ese carácter comunitario de la aplicación es el que hace que nos aventuremos a crear perfiles en los que recogemos nuestros hobbies, intereses o incluso nuestras actividades cotidianas. De forma habitual compartimos y publicamos fotos, comentamos la información publicada por otras personas e interactuamos con ellas proporcionándoles datos personales.

A día de hoy, todos accedemos a diario a *Facebook*, *Twitter* o *Instagram* sin preocuparnos demasiado por la protección de nuestra privacidad en Internet. Y es que podemos definir como privacidad el nivel de protección de que disponen todos los datos e informaciones que una persona introduce en una red social, en cuanto al grado de accesibilidad a ellos que otros usuarios o internautas pueden tener.

En muchas ocasiones estos usuarios se adentran en el mundo de las redes sociales de manera "ciega" sin tener en cuenta que la clave del negocio de las redes sociales es la información personal que tú mismo les facilitas a través de tu perfil. Esto les permite, por ejemplo, hacerte llegar publicidad altamente personalizada y maximizar así la eficacia de las campañas de sus anunciantes. Al mismo tiempo, una excesiva exposición en redes sociales puede hacernos más vulnerables frente a todo tipo de delincuentes o estafadores que quieran sacar partido de la información que conocen de nosotros.

Más aún, los riesgos que asumimos los usuarios al compartir datos personales pueden ser incontables. Por definición una red social implica compartir. Un concepto que es completamente opuesto a mantener la privacidad. La información que publicamos en redes sociales dice mucho de nosotros y puede ser utilizada para definir, por ejemplo, perfiles de personalidad, afinidades políticas, contactos, localización, etc. Solo a modo enumerativo podríamos mencionar la posibilidad de conocer nuestra geolocalización a través de los parámetros de las fotografías que subimos, nuestras rutinas diarias a través de los cambios de estado que reflejamos en nuestras cuentas, los amigos (incluso "no amigos") que añadimos (o bloqueamos) a grupos de confianza, la conexión que hacemos con otras aplicaciones (por ejemplo, financieras), etc. Todo ello permite no solo hacer perfiles sociológicos de grupos o de personas sino incluso proporcionan información útil para deducir, por ejemplo, contraseñas que utilizamos en las cuentas que tenemos asociadas.

Ahora bien, ¿Cómo nos informan las redes sociales? Las condiciones de uso de las redes sociales forman parte de los pasos previos que debemos aceptar para hacer uso de los servicios que nos ofrecen. Sin previa aceptación de dichas condiciones, no formaremos parte de la red. Estamos condenados a decidir si admitimos, o no, las reglas que definen qué datos recopilarán, con qué fin los utilizarán, con quién estarán autorizados a compartirlos, etc. Se trata de los

habituales “Términos y Condiciones de uso” que —y aquí viene por qué no estamos debidamente informados— mayoritariamente aceptamos sin siquiera leer. Esto lo afirma la Organización de Consumidores y Usuarios (2018) que realizó una encuesta mediante la cual llegó a la conclusión de que el 88% de los usuarios las aceptan sin leer, frente a un 12% que si sigue la lectura de los términos y condiciones.

La reglamentación vela por que seamos informados adecuadamente y por que los datos se utilicen de forma correcta, pero nosotros mismos debemos conocer qué datos estamos dispuestos a proporcionar para que sean recogidos por terceras partes. Y con ello debemos ser conscientes del riesgo. Una inmensa mayoría de la sociedad confía en las redes sociales de forma casi ciega. Quizás cuando utilicemos este tipo de redes deberíamos pensar en cuestiones como quién puede acceder a nuestra información, qué información pueden pasar nuestros contactos a terceras personas, qué confianza nos transmiten aquellos con los que estamos conectados… Si después aceptamos esos riesgos será otra cuestión.

Una vez decidimos aceptar estas condiciones, podremos acceder a dichas redes sociales. ¿Que nos ofrecen éstas de manera interna en cuanto a la configuración de nuestra privacidad?
Todas las redes sociales están “estandarizadas” a día de hoy en cuanto a lo que plantea esta cuestión. El usuario puede disponer de acceso a la configuración de privacidad de la red social, mediante la cual podrá comprobar el nivel de privacidad de su cuenta, configurar la privacidad de las publicaciones, modificar los parámetros del perfil y comprobar cómo los otros usuarios ven el perfil. Estas opciones nos permitirán administrar opciones tales como quién puede ver nuestras publicaciones, la información que muestras en tu perfil y muchos otros aspectos.

Precauciones

A pesar de las posibilidades en cuanto a las diferentes configuraciones en redes sociales, también existen otros parámetros de gran importancia que caben a tener en cuenta para maximizar la protección de nuestra privacidad en estas. Estos cuentan con el respaldo de empresas de seguros como *Allianz* (2019). Uno de ellos es el de limitar la información personal que se proporciona en redes sociales. Por ejemplo, no es necesario completar absolutamente todos los datos de nuestro perfil en *Facebook*, *Instagram* o *Twitter*. La mayoría de campos acerca de intereses, creencias, familia o relaciones son opcionales. Del mismo modo, se debe de intentar no compartir fotos u otra información que pueda afectar a nuestra reputación profesional, facilitar la localización de nuestro domicilio o comprometer a terceras personas.

Otra de las recomendaciones a emplear es la de utilizar contraseñas seguras. Aunque ya conocemos esta recomendación, no está de más repetirla. Bien sea por desconocimiento, bien por simple comodidad, muchas veces utilizamos contraseñas muy sencillas que, además, reutilizamos

en diferentes aplicaciones. Es recomendable seguir unas buenas medidas de uso de contraseñas (Tabla 3) y, más aún, si queremos elevar la protección, podemos utilizar la opción de verificación en dos pasos de las mismas.

Buen uso de contraseñas
No utilizar palabras “lexicalizadas”, nombres propios u otras combinaciones como por ejemplo: 1234567, dragón.
No usar palabras extranjeras como por ejemplo en inglés. Los hackers cuentan con diccionarios especiales que contienen estas combinaciones, por lo que este método no es seguro.
Es recomendable memorizar las contraseñas y, para ello, emplear símbolos o cifras que signifiquen algo de manera personal es una buena solución.
Cuanto más rápido escribamos la contraseña, mejor, pues cualquier persona que podamos tener a nuestro alrededor no dispondrá de tiempo para espiarnos y retenerla en su memoria.
Una buena contraseña siempre debe de tener cifras, caracteres especiales, mayúsculas y minúsculas.
Bajo ningún concepto debemos compartir nuestra contraseña.
En caso de compartir dispositvos, es recomendable crear distintos perfiles de usuario para que cada uno tenga su contraseña personal.
Utilizar distintas contraseñas seguras para cada una de nuestras cuentas (correo electrónico, banca electrónica, redes sociales).
Como alternativa a memorizar nosotros mismos nuestras contraseñas, podemos emplear un software especial gestor de contraseñas como Kaspersky Total Security o Password Manager, los cuales, las almacenarán de forma segura.

Tabla 3. Recomendaciones para gestionar con seguridad nuestras contraseñas.

Mediante esta serie de medidas conseguiremos evitar un posible “*hackeo*” de nuestras contraseñas pero, no obstante, según un estudio elaborado por *Google* (2017) el *Phising* es el modelo más seguido por los malhechores para robar contraseñas en las red. Estos actúan de tal manera que se hacen pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. Actuando de esta manera, consiguen ganarse la confianza de los usuarios, los cuales, acaban facilitándole datos personales como contraseñas y, más aún, datos bancarios o personales.

Más aún, hay otros factores a tener en cuenta. No debemos de olvidar de cerrar nuestra sesión en redes sociales, especialmente cuando utilizamos ordenadores compartidos o redes wifi abiertas y de desactivar las opciones de geolocalización que incorporan éstas. Es preferible

además tener precaución con las aplicaciones propias y relacionadas a las redes que solicitan acceso a nuestros datos. Por ejemplo, en *Facebook* muchas aplicaciones exigen acceder a nuestro perfil para poder utilizarlas. De hecho, se han descubierto muchos casos en que este tipo de aplicaciones, aparentemente inofensivas y divertidas, hacían un uso fraudulento de datos privados (de hecho, aplicaciones propias de *Facebook* como *Onavo Protect* o F*acebook Research* tuvieron que ser retiradas por la propia multinacional ya que accedían a los dispositivos de los usuarios, incluidos menores de edad, con la finalidad de recopilar datos, hecho que los alertó y llevo a denunciar a la red social).

También deberemos de tener en cuenta otros factores como asegurarnos de que las redes utilizan una url del estilo *https://* (esta "s" al final asegura un mayor nivel de encriptación y de seguridad de los datos). De la misma manera, tenemos que tener cuidado con las personas con las que nos relacionamos en la red y evitar aceptar solicitudes de amistad de usuarios desconocidos y, ante una situación de acoso o persecución por parte de estos, siempre podemos emplear una de las opciones que nos ofrecen a día de hoy todas las redes sociales que es la de bloquear, denunciar o reportar, que nos permitirán que este usuario no se pueda poner en contacto de nuevo con nosotros de ninguna manera y que, si más personas se suman a nuestra denuncia, pueda ser baneado (expulsado) de esa red social.

Finalmente, destacar que la mejor recomendación en sí es utilizar el sentido común. Con esto me refiero a que quizás más que una recomendación esta sea la medida más importante. No hay razón para que en las redes sociales bajemos la guardia y tengamos comportamientos temerarios que no tendríamos en otras circunstancias. Así, debemos de tener precaución ante posibles estafas (como premios millonarios o regalos inesperados), no aceptar solicitudes de amistad de perfiles sospechosos (frecuentados por acosadores en línea), no compartir datos sensibles, etc. Y, ante cualquier problema importante, informar a los administradores o, si es necesario, buscar ayuda legal.

Normativa nacional e internacional

Edad mínima de acceso

Dentro de la propia normativa y legalidad en territorio español, cabe destacar que en cuanto a redes sociales, hay establecida una edad legal de acceso a las mismas. En España, el acceso a estas plataformas está regulado en el art. 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que establece que "*podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela.*

En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores". Por ello, no es legal el uso de estas redes sociales por menores de 14 años y está prohibido que se registren sin el consentimiento previo de sus tutores legales.

Pese a esto, debido a la facilidad de acceso y al anonimato que pueden contar los perfiles de las redes sociales, es muy fácil que adolescentes menores a esta edad ya tengan una cuenta en una red social. Así lo demuestra el estudio *Menores e Internet: la asignatura pendiente de los padres españoles* elaborado por *Qustodio* (2019), plataforma de seguridad y bienestar digital para familias. Según estos datos, 2 de cada 3 menores españoles de entre 15 y 17 años utiliza *Instagram*, cifra muy superior al 44% de Estados Unidos. Además, casi la mitad (49%) de los niños entre 12 y 14 años utiliza esta *app* en España pese a que, según la ley española y la normativa de la red social, los menores de 14 años no pueden registrarse. Por si eso fuera poco, un 4% de los niños españoles de 5 a 8 años utiliza *Instagram* pese a las restricciones de edad.

A nivel legislativo, poco se puede recurrir para que los adolescentes y niños no se introduzcan a edades tan tempranas en redes sociales, aunque sí podemos encontrar soluciones desde un entorno más cercano, como sus familiares más cercanos. Según Guerrero[32] (2019), psicóloga experta de *Qustodio*, "*Las redes sociales son como cualquier otra aplicación o servicio de internet, si se usa sin ningún control puede derivar en problemas de autoestima por la falta de 'me gustas', desconexión con la familia y adicción" y, además, "La prohibición no es la solución, ya que es mucho más efectivo seguir las recomendaciones de uso de la app, hablar con los hijos y contar con herramientas de gestión y control*".

Protección de datos

Ahora bien, habiéndonos adentrado en las edades mínimas requeridas por la ley para emplear las redes sociales, cabe destacar que dice la normatividad a cerca de la ley de protección de datos. El 25 de mayo de 2018 entró en vigor el Reglamento Europeo de Protección de Datos (RGPD), tal y como lo reafirma INCIBE[33] (2019) y, como consecuencia de ello, las legislaciones de los Estados de la Unión Europea se están adaptando. Este ha sido el caso de la Ley Orgánica 3/2018 de Protección de Datos, que entró en vigor el 5 de diciembre. El derecho fundamental que la protección de datos persigue es garantizar y proteger el tratamiento de los datos personales y los derechos fundamentales de las personas físicas; especialmente el derecho al honor e intimidad personal y familiar.

Más aún, para los menos familiarizados con el ámbito hay que diferenciar el RGPD como el Reglamento Europeo de Protección de Datos frente a la Ley Orgánica de Protección de Datos,

[32] María Guerrero, psicóloga experta de *Qustodio*.

[33] Instituto Nacional de Ciberseguridad.

que actúa a nivel nacional. Este RGPD actúa directamente sobre los reglamentos establecidos en los estados miembros de la Union Europea, definiendo derechos y obligaciones comunes a todos estos países y ciudadanos europeos. Hay que recordar que los datos personales afectan a nuestra intimidad, nuestra privacidad y a nuestra seguridad; por esa razón, se exige a todos los que tratan datos personales de terceros, que cumplan con una serie de requisitos que garanticen que estos tratamientos no vulneren derechos y libertades.

A su vez, este nuevo RGPD ha instaurado nuevos cambios en cuanto a la protección de datos de los usuarios, entre los cuales, tal y como afirma la Oficina de Seguridad del Internauta (2018), "*podremos solicitar que nuestros datos desaparezcan de la base de datos de determinados registros cuando éstos ya no sean necesarios para la finalidad con la que fueron recogidos o cuando éstos hayan sido recogidos de forma ilícita. Además, podremos solicitar que se bloqueen en las listas de resultados de los buscadores enlaces a información obsoleta, incompleta, falsa o irrelevante. Por otro lado, también tendremos derecho a solicitar la recuperación de los datos para poder ser transferidos a otro responsable*".

La aprobación de estas leyes están haciendo a día de hoy que redes sociales como *Facebook*, *Instagram*, *Twitter* o multinacionales como *Google* estén teniendo que implementar cambios profundos en sus políticas de privacidad y habilitar nuevos mecanismos de control para que los ciudadanos europeos podamos ejercer nuestros derechos. Esto era algo impensable antes del *RGPD*; estas empresas se escudaban en países con regulaciones más laxas y convenientes. Ahora, deberán acatar el *RGPD* siempre mientras traten datos de ciudadanos europeos.

Normativas que rigen el ciberacoso y las problemáticas relacionadas a este

Por otra parte, no debemos dejar de analizar la normativa en cuanto a las relaciones de los distintos usuarios entre sí. El ciberacoso y la victimización en redes ha crecido a un ritmo creciente desde la aparición de las redes sociales. Cabe destacar la publicación científica por parte de *BMC Public Health* (2018) que ha compartido los resultados de una investigación sobre cibervictimización realizada con adolescentes de entre 14 y 17 años en diferentes países europeos. Aunque España ha quedado bien parada dentro de la comparativa, queda mucho trabajo por hacer y la investigación sobre el *ciberbullying* es creciente.

Siete han sido los países participantes en el estudio comparativo sobre el *ciberbullying* en Europa: Alemania, Grecia, Islandia, Holanda, Polonia, Rumania y España. Para llevar a cabo la investigación con adolescentes, se hizo uso de cuestionarios anónimos con datos sociodemográficos, características de uso de Internet, logros escolares, control parental, así como una prueba de Adicción a Internet y la Escala *Achenbach* para evaluar problemas emocionales y conductuales.

Los investigadores encontraron que una proporción relativamente alta de niños en edad escolar en Rumania (37.3%), Grecia (26.8%), Alemania (24.3%) y Polonia (21.5%) han sido intimidados *online*, mientras que una menor proporción experimentan acoso cibernético en los Países Bajos (15.5 %), Islandia (13,5%) y España (13,3%). En resumen: los resultados mostraron la tasa más alta de victimización cibernética en Rumanía y la más baja en España, siendo el tiempo dedicado a las redes sociales uno de los factores más influyentes para que se sucedan episodios de *ciberbullying* e intimidación *online*. Aunque, según determinan los autores del estudio, de la Universidad Kapodistrian de Atenas, no es el único.

Bajo estos datos, algunos países cuentan con una tasa de ciberacoso más preocupantes que otros pero, aún así, España, el país con la tasa de ciberacoso más baja de este estudio, es el único que cuenta con una normativa a nivel legal a cerca de este tipo de conductas en redes. De hecho, un informe de la Comisión de Libertades Civiles del Parlamento Europeo evidencia las carencias comunitarias a la hora de abordar este fenómeno, y resalta que España es el único país que criminaliza este tipo de delito.

El ciberacoso lleva tipificado en el Código Penal en España desde 2013, fecha en la que se incluyó un artículo específico para regular cualquier tipo de acoso sexual en internet. Aunque sí es cierto que las leyes del Código Penal respecto al ciberacoso no son lo suficientemente completas, ya que se tipifican más concretamente aquellos actos que tienen finalidades sexuales. El artículo 131 de la Ley 26.904 del Código Penal dice: "*Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma*". Con este artículo, se penaliza especialmente el acoso sexual a menores de edad a través de medios cibernéticos.

Relacionado con estos, en el artículo 183 ter de la Ley Orgánica 10/1995 de 23 de noviembre, del Código Penal, se sostiene que: "*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, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.*" y, más aún, "*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, será castigado con una pena de prisión de seis meses a dos años.*".

Posteriormente, en 2016, se hizo una reforma del Código Penal, incluyendo en la Ley Orgánica 1/2015 la regulación del *ciberstalking* y el *sexting*. El *ciberstalking* (vigilancia de una persona, contacto o intento de contacto con la misma, uso indebido de los datos personales de un tercero o un atentado contra la libertad personal) queda regulado en el artículo 172 ter, que sanciona estos actos con una pena de 3 meses a 2 años de prisión, o una multa de 6 a 24 meses.
Por su parte, las graves consecuencias del *sexting* (envío de contenidos sexuales que posteriormente son difundidos sin consentimiento) quedan tipificadas en el artículo 197.7, al atentar contra el derecho a la intimidad de la persona y su dignidad. La pena para estas acciones va de 3 meses a un año de prisión, o una multa de 6 a 12 meses, pena que se amplía de 2 a 5 años de prisión en los casos de difusión de imágenes que se hayan obtenido sin el consentimiento de la víctima.

Actualidad

Como se puede apreciar, las leyes que regulan este tipos de actos a nivel nacional están un tanto incompletas ya que como hemos ido analizando a lo largo de los apartados, hay distintos tipos de ciberacoso, víctimas, acosadores y diversas formas y tipologías de manifestación del mismo. Claramente, es un paso adelante que España sea pionero en tomar este tipo de medidas hacia estas conductas inaceptables por parte de ciertos usuarios, aunque me temo que dentro de poco tanto a nivel nacional como europeo la normativa será más estricta e influirá a todos los estados miembros.

Esto lo confirma el Parlamento Europeo, quién presentó a principios de 2017 un informe de urgencia ante la Comisión Europea ante la necesidad de crear un marco legal específico en el que se defina claramente el *cyberbullying*, con el objetivo de que pueda ser abordado de igual manera por todos los Estados miembros, y se sienten las bases de protección a las víctimas y acciones preventivas que puedan reducir un fenómeno en aumento en la Unión Europea.

A este respecto, el Parlamento sugiere a la Comisión la adopción de una definición oficial de acoso cibernético con el fin de garantizar una comprensión común y proporcionar así orientación jurídica a los países miembros. El informe señala que, si bien los vínculos del cyberbullying están relacionados con los de la intimidación tradicional, el ciberacoso debe ser considerado y abordado por sí mismo. Por otro lado, el Parlamento insta a la Comisión a "*introducir instrumentos jurídicos no vinculantes como directrices dirigidas a los proveedores de acceso a Internet sobre la forma de detectar, supervisar y notificar eficazmente los incidentes de intimidación electrónica*".

Bajo estas últimas novedades, podemos anticipar un futuro esperanzador en cuanto a la reducción del ciberacoso y todo tipo de actos delictivos en redes sociales. Como hemos visto, España sale “vencedor” en el estudio analizado con anterioridad y, estos datos, como país más bajo en

ciberacoso en Europa (respecto a los estados analizados), seguro que tiene un fuerte respaldo gracias a la ley vigente en el ámbito nacional, que trata de contrarrestar este tipo de conductas. Si un país puede reducir a esos extremos la tasa de ciberacoso, hay que confiar en que la unión de los estados miembros por una misma causa y estableciendo unas normativas y leyes comunes, lograrán decrecer este tipo de actos delictivos en las redes sociales y regular la situación, al menos, a nivel europeo.

CASOS	Ley	Pena
Edad mínima	Articulo. 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre	Necesaria la intervención de padres y tutores
Protección de datos	España: Ley Orgánica de Protección de Datos. Europa: Reglamento Europeo de Protección de Datos	Poder de reclamo para los usuarios frente a compañías e invasión de privacidad y seguridad (datos).
Normativas que rigen el ciberacoso y las problemáticas relacionadas a este	Artículo 131 de la Ley 26.904 del Código Penal (ciberacoso). Artículo 183 ter de la Ley Orgánica 10/1995 de 23 de noviembre, del Código Penal (*grooming*). Artículo 172 ter y artículo 197.7 regulan el *ciberstalking* y el *sexting*, respectivamente.	*Ciberacoso*: *prisión 6 meses-4 años-* *Grooming*: prisión 6 meses-3 años *Ciberstalking*: 3 meses-2 años *Sexting*: *prisión 3 meses-6 años* *Europa: no penado*
Actualidad	En espera de reformas por parte del Parlamento y la Comisión Europea (ciberacoso y problemáticas, elaboración de marco teórico y contextualización).	A la espera

Tabla 4.Resumen de leyes y normativas.

Capítulo 5: Herramientas preventivas

Ámbito doméstico

A día de hoy, las problemática sociales y educativas en las redes sociales son un hecho que no pasa desapercibido. El avance tecnológico y la creación de las comunidades virtuales trajeron consigo un gran cambio y progreso cultural, pero algunos factores como las problemáticas que se han estudiado con anterioridad no entraban dentro de las predicciones de los creadores de las redes sociales. No obstante, a día de hoy y ante el panorama de un crecimiento progresivo de estos contratiempos, han surgido un gran número de herramientas que tienen como objetivo ayudar a los usuarios a contrarrestar dichas problemáticas existentes en las redes sociales.

Comenzando, cabe prestar atención a los más pequeños de la casa. Como se ha venido analizando, los casos de ciberacoso y las problemáticas relacionadas con las nuevas tecnologías y redes sociales provienen, en gran parte, por la falta de una educación o iniciación más controlada de estos nuevos usuarios más jóvenes. Es por ello que, para niños de 5-6 a 10-12 años, es recomendable comenzar a educarles dentro del ámbito de las nuevas tecnologías y de las comunidades virtuales.

Sistemas operativos y control parental

Microsoft Windows

Si lo que queremos es tener un control parental en *Windows 10*, debemos de crear una nueva cuenta de usuario y pulsar sobre la opción Agregar Familiar, recalcando posteriormente que este se trata de un mejor. Una vez habiendo finalizado el proceso, podremos administrar y controlar los pasos que los menores llevan a cabo con el dispositivo en la sección Restricciones de contenido (Tabla 5)

Apple

Si lo que queremos es tener un control parental en *iOS*, deberemos de dirigirnos a la sección Tiempo de uso, en Ajustes. Una vez habiendo accedido, deberemos de establecer que dispositivo es el parental y cual es el del niño. Tras esto, deberemos de establecer un código de seguridad para poder manipular el dispositivo del menor desde el nuestro y al fin conectar ambos. Una vez llevado a cabo este proceso, deberemos de dirigirnos a la sección Restricciones de contenido y privacidad, desde la cual, configuraremos las distintas opciones a nuestra disposición (Tabla 6).

¿Que configuraciones podemos llevar a cabo?
Se podrá establecer que un adulto tenga que autorizar compras en *Microsoft Shore*.
Recibir notificaciones de la realización de una descarga.
Bloquear aplicaciones, juegos y contenido multimedia no adecuado.
Establecer permiso de acceso a aplicaciones y juegos clasificados según edad.
Bloquear sitios web inadecuados (incluso se puede establecer que sitios no pueden visitar o qué sitios son los únicos que si pueden).
Establecer límites de tiempo.

Tabla 5. Configuraciones control parental *Microsoft Windows*.

¿Que configuraciones podemos llevar a cabo?
Establecer restricciones de contenido y privacidad.
Impedir compras en *iTunes* y *App Store*.
Permitir *apps* y funciones integradas.
Impedir contenido explícito o con calificaciones concretas.
Impedir contenido web.
Restringir la búsqueda web de *Siri* y *Game Center*.
Realizar cambios en ajustes de privacidad y funciones.

Tabla 6. Configuraciones control parental *Apple* (*iOS*).

Famisafe

Una herramienta que sería de gran ayuda para los tutores de cada uno de estos usuarios es *Famisafe*. Mediante esta, podremos crear una zona segura en el dispositivo para niños. A estas edades tan tempranas los niños y adolescentes comienzan a desarrollar cierto grado de independencia, por lo que para llevar un control de los mismos y seguir su educación tanto en el mundo físico como en el digital, esta aplicación es una de las mejores alternativas.

Por una parte, usando la información de ubicación GPS de su dispositivo, podremos rastrear la ubicación en tiempo real de nuestros hijos en un mapa satelital. Es decir que podremos ver exactamente dónde están nuestros niños y dónde ha estado.También se puede usar la función geo-cercados para establecer límites virtuales en el mapa. Si un niño se mueve por fuera de estos límites, recibiremos una notificación indicándonos lo que ha ocurrido, por ejemplo, si se va de la escuela (Figura 12).

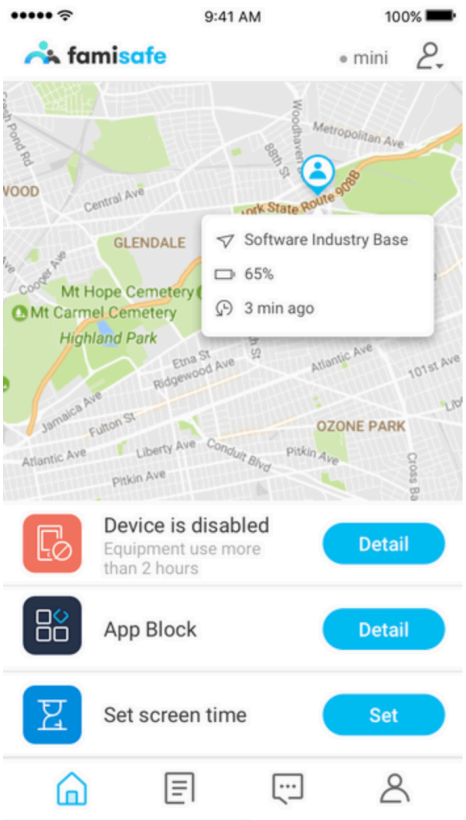

Figura 12. *Famisafe*, geolocalización.

Otras de las funciones disponibles en la aplicación, que vela por la privacidad y la seguridad de estos menores, es el empleo y la personalización del monitoreo y el filtrado web. Al usar esta función, se pueden activar y desactivar ciertos tipos de contenido a los que nuestro hijo puede tener acceso mientras navega por Internet. También se podrá bloquear el acceso a ciertos tipos de sitios web, hacer excepciones a los bloqueos y recibir notificaciones cuando nuestro hijo intente acceder a un sitio web bloqueado (Figura 13).

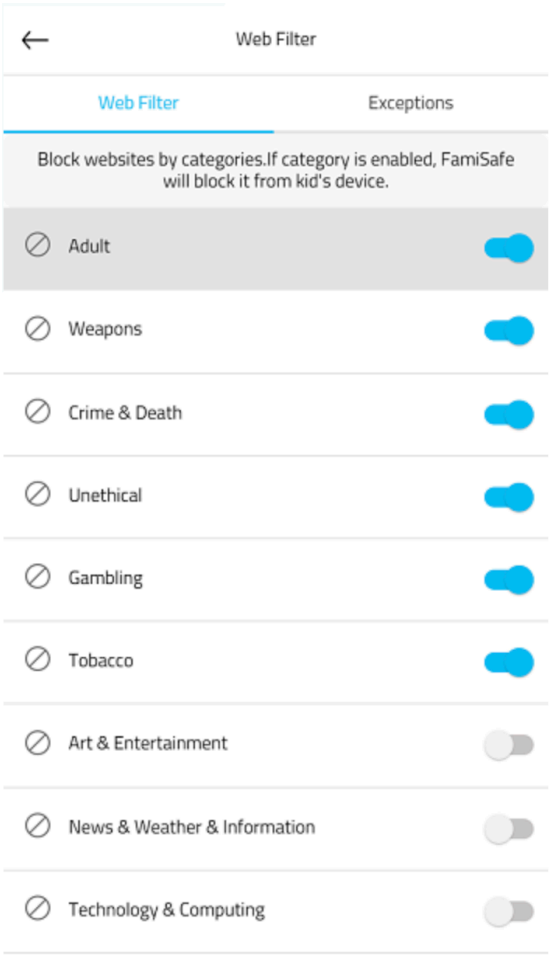

Figura 13. *Famisafe*, configuraciones filtrador web.

Conjuntamente a estas funcionalidades, también se puede llevar a cabo el rastreo de la actividad del dispositivo. Es decir, utilizando *Famisafe*, se puede ver exactamente cómo los niños usan sus dispositivos. Se puede ver por cuánto tiempo está usando su dispositivo, a qué aplicaciones está accediendo con mayor frecuencia y en qué momento está usando las aplicaciones. En este sentido, podremos tomar las decisiones correctas cuando se trata de permitir que nuestros hijos estén en sus dispositivos, para que puedan disfrutar de un balance en la tecnología (Figura 14).

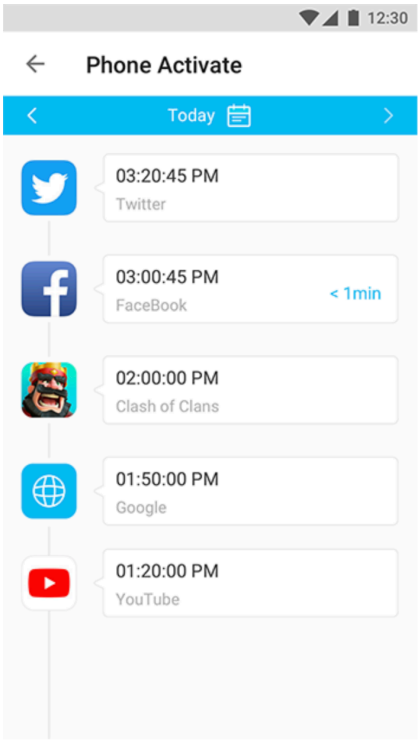

Figura 14. *Famisafe*, actividad en aplicaciones.

Por otra parte, cabe destacar que podremos emplear la aplicación de forma totalmente remota. Esto se podrá llevar a cabo mediante la descarga de una copia de la aplicación en nuestro dispositivo, desde el cual podremos realizar cambios. Cuando llevemos a cabo estos cambios en nuestro dispositivo, supondrá el cambio instantáneo de la configuración en el teléfono del niño (Figura 15).

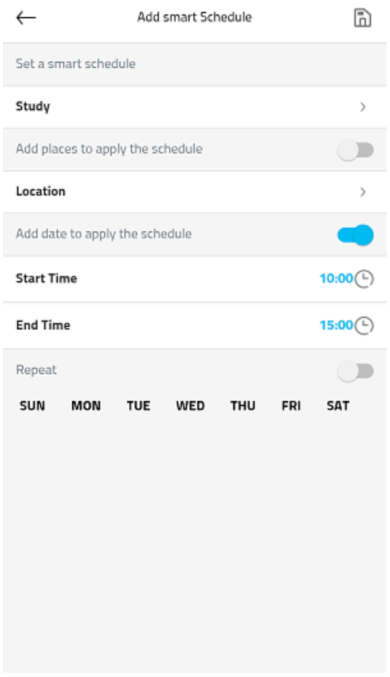

Figura 15. *Famisafe*, configuraciones control parental.

Finalmente, cabe destacar que dentro de todas las funcionalidades analizadas, más aún podremos personalizar la experiencia de los más pequeños en sus respectivos dispositivos, principalmente, mediante la administración del acceso a las aplicaciones. Esto quiere decir que, al usar esta aplicación, podremos monitorear el tiempo en el que nuestro hijo usa su dispositivo y cómo está usando sus aplicaciones. Podremos ver qué aplicaciones se están instalando o desinstalando. De esta manera, se pueden establecer límites de tiempo para cada aplicación, elegir a qué horas del día se puede acceder a la misma o bloquear el acceso a éstas por completo.

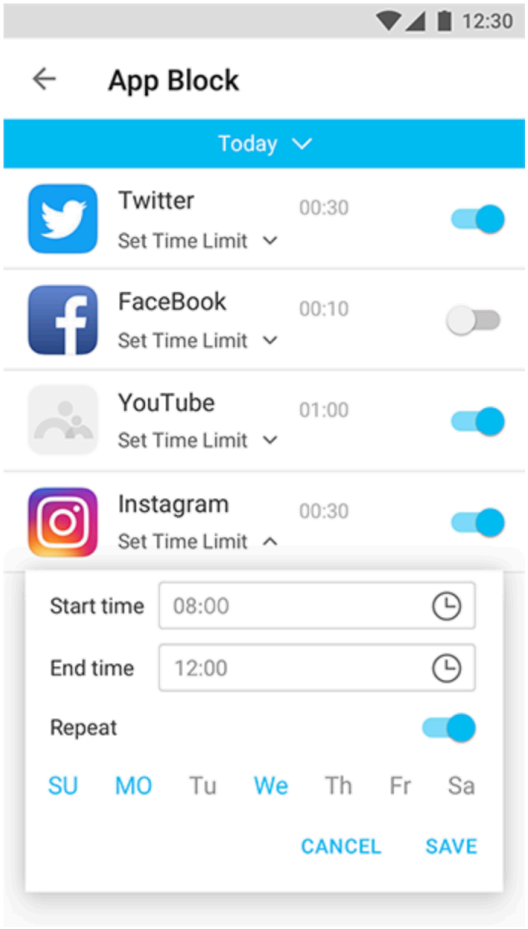

Figura 16. *Famisafe*, control de aplicaciones.

En resumen, como se puede ver, *Famisafe* permite a nuestros hijos aprender a usar sus dispositivos de la manera más natural, al mismo tiempo en el que bloquea ciertas funciones que pueden dañar su bienestar. Sin lugar a dudas, es una de las aplicaciones más efectivas en cuanto a control, lo que nos permitirá introducir a los más pequeños de la casa de una manera más guiada y educándoles de cara a identificar e interactuar en ciertas páginas, redes sociales y webs en las que intervienen otros usuarios. Ahora bien, pese a que *Famisafe* es una de las aplicaciones más completas en el mercado, también podremos emplear otras alternativas como *Qustodio*, que, sumando todas las funcionalidades de la aplicación anterior, también cuenta con un “botón del pánico”, mediante el cual, los niños/as que utilicen un dispositivo protegido por *Qustodio* podrán

enviar una alerta rápida y directamente desde su teléfono a contactos de emergencia. Finalmente, tampoco cabe pasar por alto *ParentalClick*, una aplicación que promueve la educación frente a la prohibición de los menores en Internet. Mediante esta, los padres pueden llevar a cabo un control consentido y consensuado de los hijos y, en el caso de producirse un hecho denunciable, la aplicación permitirá presentar pruebas legales y legítimas en un proceso judicial.

Ámbito escolar

El empleo de *Famisafe* y sus distintas alternativas puede ser de gran ayuda para inicializar y proteger a los más pequeños de la casa en las redes sociales y entornos virtuales. Es la mejor opción a emplear de manera particular, es decir, cuando unos padres o tutores bajo su propia decisión deciden emplearla y tomar medidas para mejorar la educación de sus sucesores en las redes. Pero, ¿Qué ocurre fuera de casa? ¿Cómo se debe de seguir fomentando esta educación fuera de nuestra zona de confort y en convivencia con otros niños o adolescentes?

Dinantia

Para este tipo de casos, existen otras posibilidades y herramientas como *Dinantia*, una plataforma de comunicación web y móvil dirigida a colegios, profesores, padres y alumnos. Cabe destacar que a día de hoy, es empleada tanto en colegios como institutos y universidades, por lo que puede abarcar un gran rango de edades. Entre sus múltiples funcionalidades, *Stop Bullying* permite a los alumnos reportar casos de todo tipo de ciberacoso de forma anónima y segura.

Entre las principales características de la aplicación, cabe destacar que hace un buen uso de la comunicación. Permite a los centros y profesores mandar mensajes y notificaciones tanto a padres como a alumnos en tiempo real, sin compartir el número de móvil (protegiendo así la privacidad de los usuarios). Además, los padres podrán activar las notificaciones *push* que les saldrá en la pantalla principal de su dispositivo para así no perderse ninguna noticia relacionada con el centro. Además, los profesores podrán comprobar si los padres y/o alumnos han recibido dichos mensajes. Está aplicación incrementa por tanto la comunicación e interacción entre padres, alumnos y profesores, un factor de gran importancia de cara a si se diera alguna tipología de acoso (tanto analógico como digital) en el centro o entre los alumnos del mismo (Figura 17).

Más allá de las distintas funcionalidades que ofrece, cabe destacar la implementación de *Stop Bullying* dentro de la propia aplicación, lo que permite a los distintos usuarios de la misma denunciar o bien mediante su identificación o bien mediante el anonimato casos de acoso, el procedimiento, como se puede ver a continuación, es el siguiente.

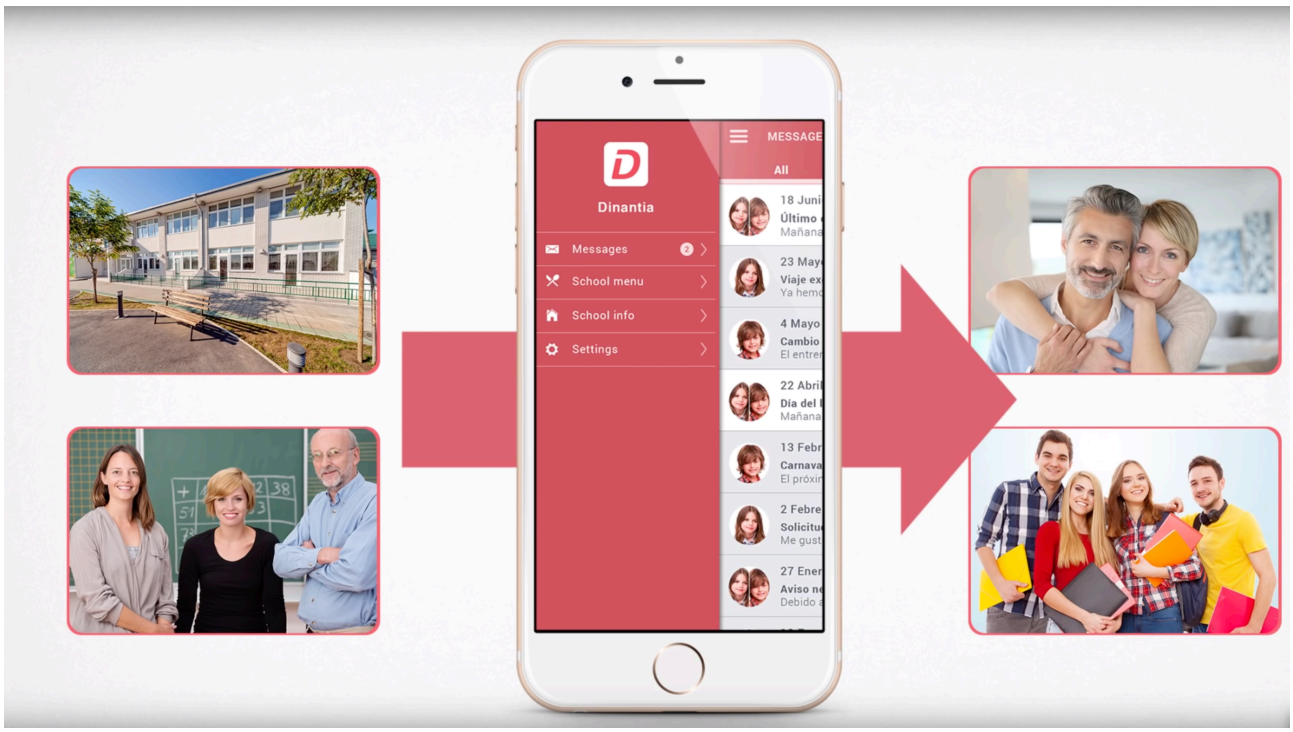

Figura 17. *Dinantia*, funcionamiento.

Los usuarios de la aplicación dispondrán de un número PIN que le ofrecerá un mayor anonimato en caso de denuncia. La información que contenga la denuncia será trasladada a los altos cargos del centro educativo y, dependiendo de la gravedad del asunto, posteriormente esta información podrá ser trasladada a las autoridades correspondientes (Figura 18).

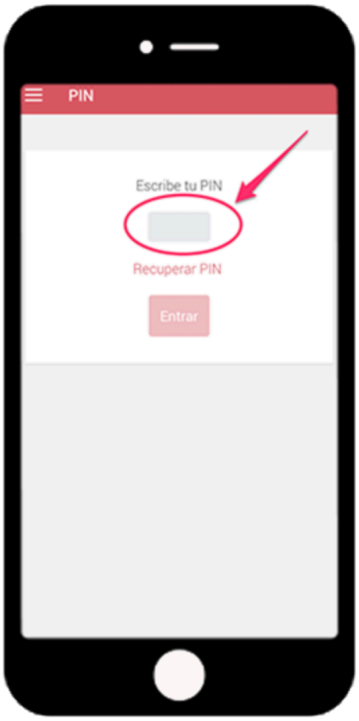

Figura 18. *Dinantia*, *Stop Bullying* y número PIN.

Una vez accedamos, se deberá de pulsar el botón “nuevo caso”, en el que escribiremos el mensaje que se desea transmitir (Figura 19).

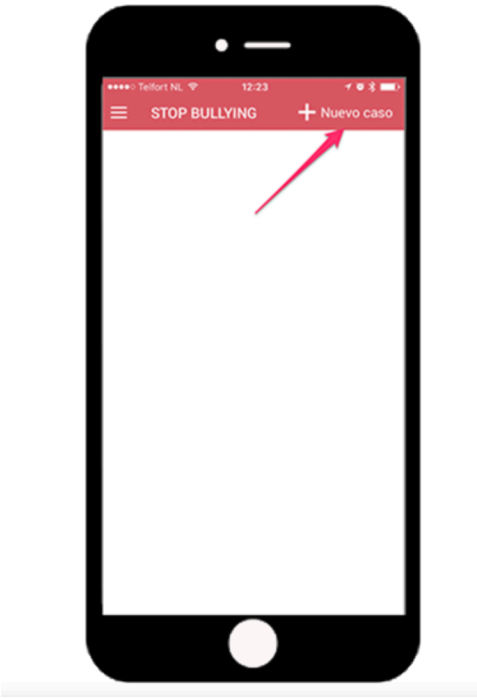

Figura 19. *Dinantia*, denuncia.

El mensaje por defecto se enviará de forma anónima, aunque si lo deseamos, se podrá revelar nuestra identidad. En este mensaje, a su vez, podremos adjuntar pruebas en el caso de tenerlas, tales como fotos, vídeo, documentos, etc (Figura 20).

Figura 20. *Dinantia*, denuncia anónima o identificada.

Finalmente, comentar que entre las posibles alternativas a esta aplicación, cabe destacar *AppVise*. De nuevo, una aplicación que apuesta por la interacción, comunicación y cooperación entre profesores, padres y alumnos, para fomentar la educación de éstos y el buen uso de redes sociales y los distintos entornos digitales, excluyendo, por supuesto, las distintas tipologías de acoso de estos (Figura 21).

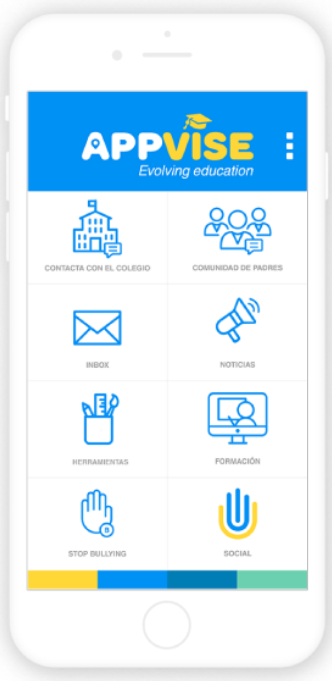

Figura 21. *AppVise* como alternativa.

Ámbito de la desinformación y de las campañas de desprestigio

En muchas ocasiones, navegamos por la web y las redes sociales viéndonos expuestos a encontrar mucha información. En algunas de ellas, sin apenas percatarnos, leemos noticias falsas o bulos que emplea una parte de la prensa y de los usuarios con la necesidad de generar visitas para ganar afiliados y ganancias económicas mediante la publicidad. La peor parte de esta desinformación en la que nos vemos involuntariamente involucrados es que, con posterioridad, solemos compartir este tipo de noticias en nuestras redes y éstas tienden expandirse entre las largas listas de usuarios amigos que, a su vez, siguen expandiendo este tipo de contenidos por sus redes y así sucesivamente.

Maldita App

Mediante esto, lo que se consigue es difundir difamaciones, bulos, información falsa y, a la larga, esto a su vez puede acabar convirtiéndose en una campaña de desprestigio, según el contenido de dicha noticia. Para evitar esto, *Maldita.es* ha lanzado una aplicación que “batalla contra la

mentira”. Mediante esta, innovan ofreciendo la primera aplicación móvil capaz de avisarnos cuando estamos entrando en una web o página con este tipo de contenidos.

Ahora bien, ¿Cómo funciona la aplicación de *Maldita*? Mediante una notificación *push*, la app nos dirá si la web en la que estamos navegando desinforma de manera habitual, si es una web satírica o si el contenido al que estás accediendo ya está desmentido (Figura 22).

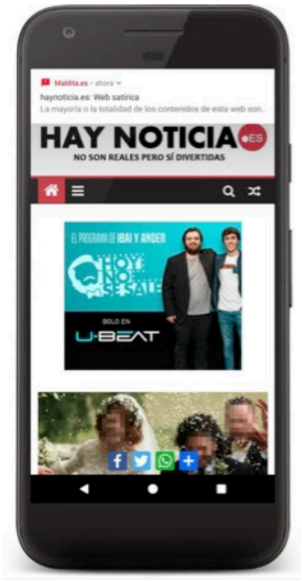

Figura 22. *Maldita*, notificación *Push* y página inicio.

Con la *app* de *Maldita* también se podrán buscar bulos ya desmentidos a través del buscador integrado y subir imágenes desde nuestro smartphone para comprobar si han sido desmentidas por *Maldito Bulo* (Figura 23).

Figura 23. *Maldita*, buscador de bulos.

Más aún, en caso de no encontrar el desmentido que estamos buscando, pues creemos que es un contenido sospechoso, también podremos enviar enlaces e imágenes para su verificación. Incluso podremos filtrar contenidos que ya han sido desmentidos (Figura 24).

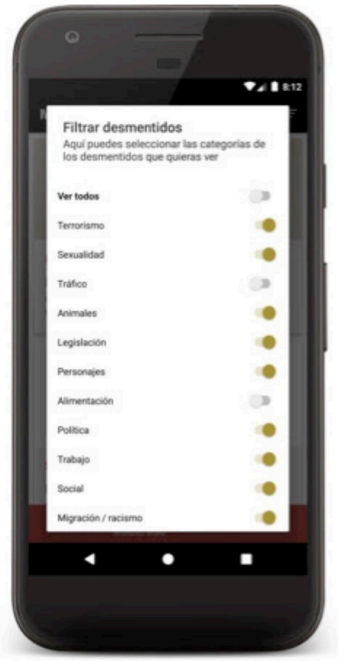

Figura 24. *Maldita*, filtrador de bulos.

Ámbito del espionaje

En la actualidad, hay diversas aplicaciones y medios mediante los cuales unos usuarios pueden espiar móviles de otros. Entre estas espías destacan acciones como escuchar nuestras llamadas en tiempo real, acceso a nuestro historial de llamadas, correos electrónicos y búsquedas, envío y recibo de mensajes, información de localización y rastreo, actividad en redes sociales y hasta acceder a vídeos, fotos y registros bancarios o médicos. Entre estos medios, sin llegar al *hackeo* más profesional, nos encontramos con que usuarios “a pie de calle” pueden acceder a este tipo de información mediante la descarga de aplicaciones como *XNSPY* o *Spyzie*. Éstas, permiten realizar muchas de las acciones comentadas con anterioridad y atravesar las barreras de privacidad y seguridad de nuestros dispositivos, más aún, están al alcance de cualquier perfil de usuarios, pues pese a que distintas funcionalidades de las mismas no son gratuitas, tienen un precio muy asequible.

Incognito AntiSpy Scanner

Para contrarrestar este tipo de aplicaciones intrusas, paralelamente han surgido y han ido evolucionando las denominadas aplicaciones “anti-espionaje”, las cuales, son capaces de analizar nuestro dispositivo y encontrar en este todo tipo de amenazas. Una de las más destacadas es *Incognito AntiSpy Scanner* (Figura 25), una aplicación desarrollada por un equipo de profesionales cibernéticos con más de 50 años de experiencia en la lucha contra el *malware* y *software* espía. Son conocedores del mercado y de las aplicaciones mencionadas con anterioridad, las cuales, fueron creadas en un principio como una herramienta de control parental y, en ocasiones, también empleadas por las empresas para vigilar a sus empleados. No obstante, con el paso del tiempo y la globalización de estas aplicaciones, a día de hoy son empleadas de forma siniestra.

Figura 25. *Incognito*, *App* anti-espionaje.

A todo esto, ¿Cómo es capaz *Incognito* de devolvernos nuestra privacidad y eliminar todo tipo de *software* espía en nuestro dispositivo?

La aplicación realiza un análisis exhaustivo de nuestro dispositivo (Figura 26). El equipo que creó la app actualiza de manera constante la aplicación incorporando cada vez mejores herramientas de *software* anti espía. Esto lo consiguen mediante el estudio de las aplicaciones espía que salen al mercado y las mejoras que incorporan a las mismas. Es decir, el algoritmo mediante el cual perciben este tipo de *software* espía es modificado de forma periódica según las novedades que aporten los *software* espía, para así lograr en el dispositivo del usuario un análisis de lo más completo y que le liberará de dichas amenazas, devolviéndole así su privacidad y seguridad.

Figura 26. *Incognito* analiza nuestro dispositivo.

Como se puede apreciar, una vez realizado el análisis, este nos informará de los resultados del mismo, incluyendo el *software* intruso que está espiándonos o vigilándonos. Por el contrario, si nuestro dispositivo está limpio de este tipo de *software*, también nos lo notificará.

Cabe destacar que *Incognito AntiSpy Scanner* no es la única aplicación que nos puede ayudar, si no que hay muchas otras, tanto para *Android* como para *iOS* que tienen las mismas características y funcionalidades y que nos pueden servir como buenas alternativas. Entre ellas, cabe destacar *Anti Spy Mobile Free* (Figura 27). que, aunque funcionando prácticamente de la misma manera que *Incognito*, esta nos ofrece además la posibilidad de conocer, dentro de las apliaciones que contenemos en nuestro dispositivo, las vulnerabilidades y permisos a los que afectan.

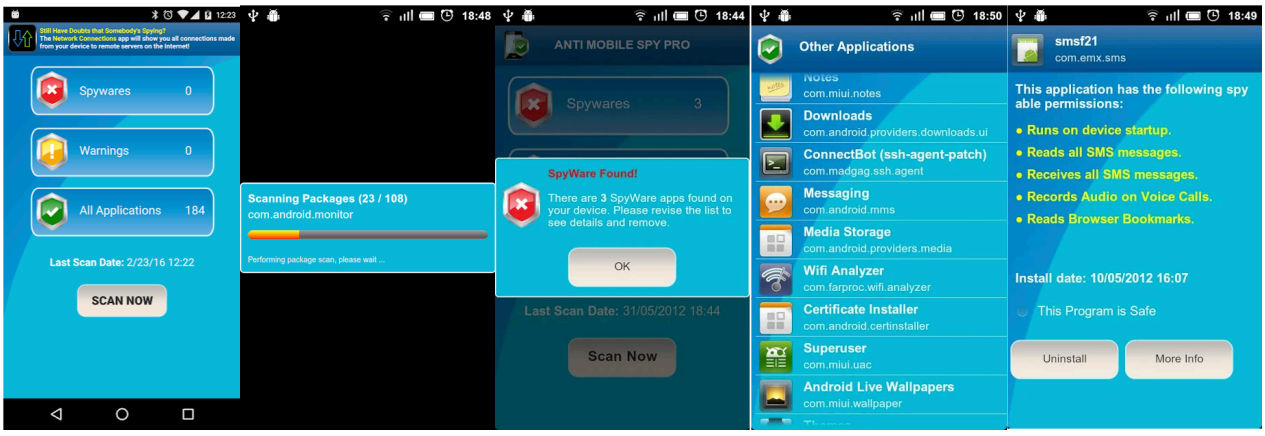

Figura 27. *Anti Spy Mobile Free* como alternativa.

Ámbito de la privacidad y seguridad

A partir del incremento del ciberacoso y de la sobreexposición de nuestra información a otros usuarios, han surgido también herramientas y aplicaciones específicas que nos van a ayudar a personalizar y gestionar nuestra privacidad en las redes sociales, incrementando así nuestra seguridad frente a otros usuarios.

Jumbo

Entre ellas, cabe destacar *Jumbo*, una aplicación disponible para todas las plataformas que ayuda a los usuarios de las distintas redes sociales a ajustar las configuraciones de privacidad de las mismas. A su vez, posibilita bloquear el seguimiento no deseado.

Jumbo deja en evidencia y nos ayuda a cubrir las áreas donde considera que se puede filtrar nuestra información. Entre otras de sus funcionalidades, cabe destacar que la aplicación nos ayuda también a limpiar nuestros perfiles sociales y blinda la privacidad para evitar situaciones comprometidas, como por ejemplo, la reaparición de un tuit traicionero publicado años atrás o la aparición de una fotografía que quizás no queremos que ahora salga a la luz. También, por ejemplo en lo referente a *Facebook*, la aplicación pasa por las 40 configuraciones de la compañía y las cambia para limitar la visibilidad de nuestras publicaciones. *Jumbo* ofrece una configuración de privacidad “débil”, “media” y “fuerte”. La configuración del medio hace que la mayoría de la información de nuestro perfil esté disponible solo para amigos; la configuración fuerte hace que la mayoría de esa información sea visible solo para nosotros (Figuras 28 y 29).

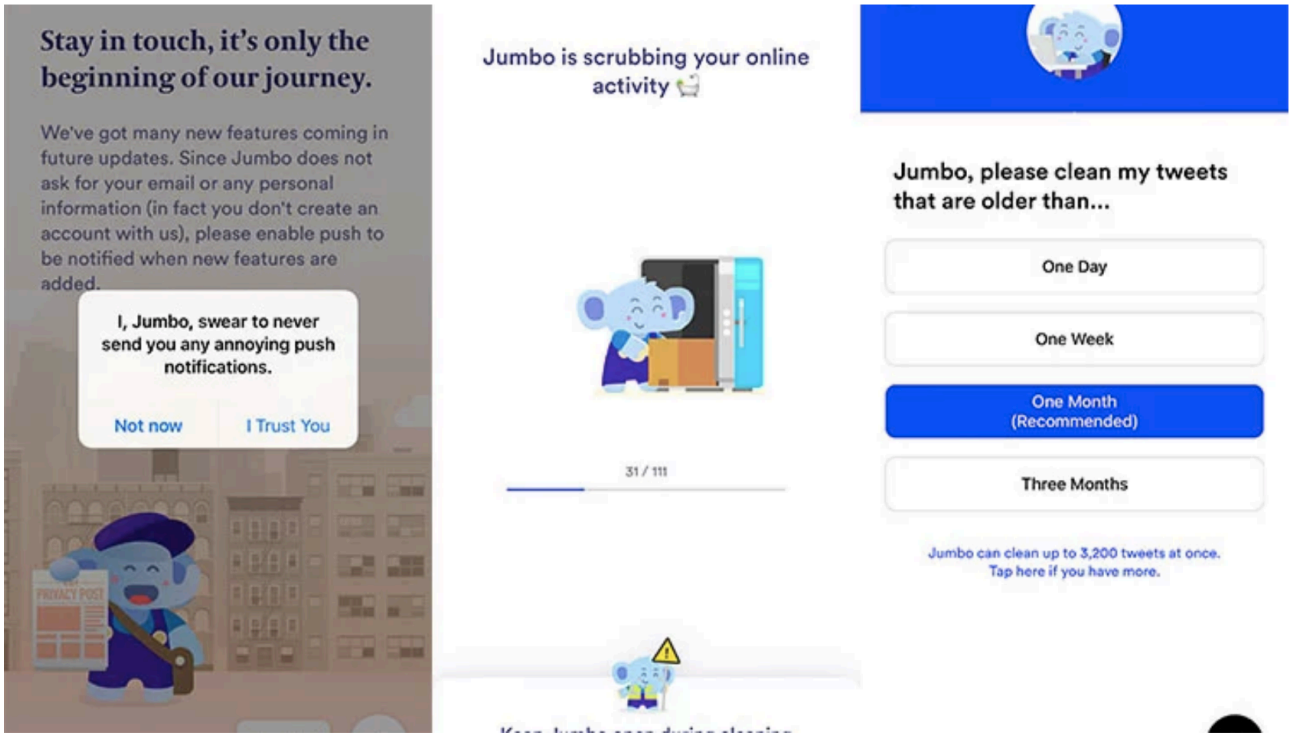

Figura 28. *Jumbo*, privacidad y seguridad.

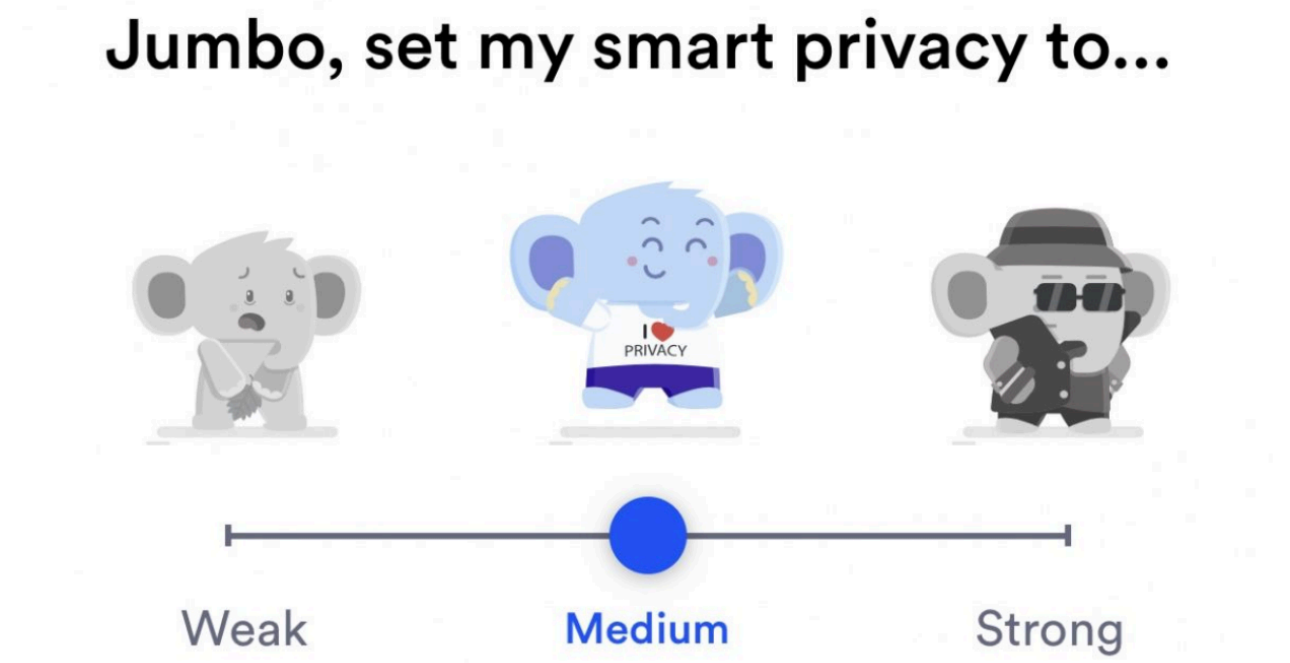

Figura 29. *Jumbo*, privacidad y seguridad.

Además, dependiendo de esta configuración y el nivel de privacidad seleccionado, *Jumbo* podrá acceder, además de a redes sociales, a medios como el motor de búsqueda de *Google*, en el que podrá encargarse de borrar nuestro historial cada día, semana, mes o de manera trimestral y a *Alexa*, el asistente de *Amazon*, del que se hará cargo de eliminar el historial que contiene grabaciones de nuestra voz para hacer búsquedas o activar funciones.

En relación a esta aplicación, cabe comentar una alternativa a la misma como puede ser *AVG PrivacyFix*. Tiene funcionalidades similares a *Jumbo*, pero cuenta con características particulares como la posibilidad de recorrer sus opciones de manera individual y, además, nos otorga un puntaje para medir el nivel de seguridad que poseemos en nuestros perfiles. Constantemente interpela al usuario, con consejos sobre los pros y los contras de aumentar la privacidad, que deben ser leídos con atención para tener un total manejo de la información que se desea preservar y de la que se puede publicar.

Como complemento a estas aplicaciones, podemos a su vez utilizar alguna del estilo de *LogDog*, la cual se encarga de explorar indicadores de acceso no autorizado y cuando encuentra algo que no está bien emite una alerta de intrusión y permite a los usuarios recuperar el control de sus cuentas. Sin lugar a dudas, una buena opción para mejorar la administración y evitar intrusos.

¿Cómo son de válidas estas aplicaciones?

A raíz de los análisis y las investigaciones realizadas en los anteriores apartados podemos llegar a ciertas conclusiones a cerca de las herramientas existentes hoy en día que velan por contrarrestar el ciberacoso y las distintas problemáticas relacionadas con el mismo.

Por una parte, el ámbito doméstico cuenta con numerosas aplicaciones que cuentan con funciones similares a las analizadas. Éstas funcionan como un “conector” entre padres e hijos para que los progenitores ayuden a los más pequeños de la casa a introducirse en el mundo de las redes sociales y de los distintos entornos digitales. Mediante este tipo de aplicaciones, inexistentes al comienzo de la evolución tecnológica y digital, se conseguirá educar en el ámbito de la red a los más pequeños de la casa, fomentándoles desde edades pequeñas un buen uso de las mismas, la privación de contenidos inadecuados y la capacidad de poder convivir en sociedad mediante, como se ha dicho con anterioridad, la educación y la tolerancia. Estas aplicaciones, por lo tanto, conseguirán que de cara a generaciones futuras decrezca el ciberacoso y muchas de las problemáticas del mismo, pues poco a poco se estará construyendo una nueva red de usuarios “preparados” para participar en la misma.

Por otra parte, en el ámbito escolar, también se han visto incrementadas las herramientas que ayudan a mejorar la relación hijos-padres-profesores. Sin lugar a dudas, estas aplicaciones ayudan a mejorar la comunicación y la interacción entre las tres partes implicadas, lo que implica que de cara a cualquier tipo de acto relacionado con el acoso y sus diferentes tipologías sufrido por cualquier alumno pueda ser revelado por este mismo de manera inmediata o, incluso, si algún compañero de este supiera de la existencia de estos hechos, también pueda manifestarlo incluso de manera anónima. Mediante esto, se consigue que cualquier problemática relacionada con el ciberacoso sea parada y detectada a tiempo sin que llegue a pasar mala factura a la víctimas.

Más aún, también se ha analizado el empleo de aplicaciones en favor de problemas más concretos como el de las campañas de desprestigio y la desinformación. Mediante este tipo de herramientas, conseguiremos estar seguros de que cualquier información que se exponga a nuestros ojos tanto en redes sociales como en la web sea verídica pues, cualquier información de tipo sensacionalista y falsa quedará señalada. Esta aplicación, si fuese empleada por todos los usuarios, borraría cualquier campaña de desprestigio y de desinformación de la web pues, la torpeza de esta problemática, es que los usuarios tienden a compartir información, noticias y cadenas de opiniones a cerca de actos de personas que no han llegado a validar. Es, por lo tanto, necesario el uso de estas aplicaciones, pues se logrará terminar con la prensa amarilla, los usuarios dañinos y el *clickbait* o información sensacionalista.

Además, también nos encontramos con aplicaciones que remedian el espionaje al que, en ocasiones a través de las redes y en muchas otras a través de la web, nos vemos sometidos mediante nuestro smartphone. A través del uso de esta aplicación vemos como podemos hacer un

uso más eficaz y seguro de nuestro dispositivo móvil. Es más, las aplicaciones anti-espionaje están muy relacionadas con el incremento de nuestra seguridad y nuestra privacidad, por lo que, en parte, pese ser un *software* explícito para denegar entradas a agentes externos que pudieran usar y manipular nuestros datos, también podemos considerarla como una herramienta en favor de nuestra seguridad y privacidad que, de emplearse al mismo tiempo con las aplicaciones específicas en este ámbito, darían lugar a un *smartphone* altamente impenetrable. Esto se debe a que mediante el empleo de este tipo de aplicaciones tendríamos cubierto en seguridad y privacidad tanto el propio sistema del *smartphone* como las distintas aplicaciones y, en especial, las redes sociales y la lucha contra el ciberacoso y demás problemáticas, mediante el empleo de aplicaciones como *Jumbo*.

¿Qué se podría mejorar?

Como se ha podido apreciar en los análisis y en las concusiones a las que se ha llegado a cerca de las distintas herramientas y aplicaciones preventivas existentes en el mercado a día de hoy, se puede decir que en los distintos ámbitos estudiados, estas cumplen con sus principales funciones a rajatabla logrando minimizar las distintas problemáticas relacionadas con el ciberacoso y éste en si mismo. Eso sí, esto se seguirá cumpliendo siempre y cuando estas aplicaciones permanezcan actualizadas y sigan al tanto de la evolución tan rápida que sufren las redes sociales y los distintos entornos digitales, pudiendo seguir así estando preparadas ante cualquier amenaza.

Cabe destacar, por otra parte, que las aplicaciones funcionan de manera en sí mismas y bajo su propia interfaz, por lo que, tras el análisis e investigación realizado debo desde un punto de vista personal retirar mi idea inicial de proponer una aplicación híbrida, la cual, recogería, las principales funciones de las herramientas ya analizadas creando una aplicación nueva más completa y que incluiría todas y cada una de estas. Esto se debe a que como es lógico, una aplicación no puede incluir una función de control parental junto a un apartado dedicado al ámbito escolar, sumándole más aún, un *software* dedicado a rechazar el espionaje y a mejorar nuestra privacidad y seguridad en redes sociales.

Las aplicaciones de manera individual cuentan con funcionalidades muy explícitas propias de las mismas, las cuales en cuanto a contenidos sería erróneo mezclarlas y, desde un punto de vista técnico y programático, prácticamente imposible. Es por esto que lo más adecuado es emplear la aplicaciones como independientes pues en sí mismas desarrollan correctamente su función y, en su conjunto, relacionadas unas con otras y empleándolas paralelamente (según la necesidad del usuario podrá emplear unas u otras) podremos decir que tenemos un *smartphone-fortín*, altamente impenetrable, salvaguardador de nuestra seguridad y privacidad y fomentador de una mayor relación usuario-entorno que lucha en conjunto contra el ciberacoso y las problemáticas relacionadas con el mismo.

No obstante, pese a estas reflexiones a cerca de las aplicaciones analizadas, bajo mi punto de vista, el elenco de herramientas disponibles en las tiendas y mercados digitales podría ser ampliado. Durante la investigación, he echado en falta una aplicación concreta que se centre únicamente en dar soporte a todas las víctimas. Es cierto que tanto en el ámbito doméstico como en el escolar se nos presentan una aplicaciones muy correctas de cara a detectar el acoso y sus diferentes tipologías pero, si lo analizamos bien, éstas están enfocadas a víctimas más jóvenes propias de la infancia o adolescencia, además de abordar la formación de estos. Es decir, son aplicaciones mediante las que se verán resultados en la reducción de dichas problemáticas y en usuarios a la larga, pues se les forma dentro del contexto cultural, social y educacional, para evitar dichos comportamientos cuando estos vayan adquiriendo cierta independencia. Pero, ¿Qué pasa con las víctimas en la actualidad? ¿Acaso no hay víctimas de todo tipo de sexo y edad? Como se ha estudiado a lo largo del documento la respuesta es sí. Por lo tanto, en el siguiente apartado, se tratará de abordar, mediante la propuesta de una aplicación, estas cuestiones.

Capítulo 6: Propuesta de aplicación

Descripción de la actividad del proyecto

Este proyecto tiene por objeto ofrecer una alternativa a todos aquellos usuarios afectados por las distintas tipologías del ciberacoso. Tras todo el análisis e investigación que se ha llevado a cabo, es necesaria la implementación de una aplicación móvil de esta tipología; abierta a todas las edades, usuarios de cualquier sexo y terceras personas que pudieran denunciar actos delictivos de los que han sido testigos en la red. Contamos a día de hoy con herramientas que ciertamente muestras una consistente utilidad, pero éstas están enfocadas en un público sin contar, como se ha dicho con anterioridad la gran variedad que hay de usuarios distintos. Bajo mi punto de vista, crear una aplicación móvil para contrarrestar el ciberacoso y ofrecer una ayuda y/o salida a las víctimas, es la manera más óptima de combatir este frente, pues gracias a los nuevos medios este tipo de herramientas logran llegar a un gran número de usuarios debido a la fácil difusión y alcance de las mismas, pues a día de hoy, la mayoría de los usuarios cuentan con un *smartphone* o tableta electrónica que les mantiene siempre al tanto de este tipo de novedades.

Por otra parte, cabe destacar que esta aplicación tendrá cuatro páginas principales que tendrán una función bien distinta cada una de ellas. Entre estas, podemos diferencias la página de “Inicio”, que nos ofrecerá una breve presentación de la aplicación y de los órganos que colaboran en ella, la página “Denuncia”, mediante la cual un usuario, ya sea víctima o testigo, podrá denunciar hechos relacionados con el ciberacoso y las distintas problemáticas, la tercera página, “Protégete”, desde la cual se ofrecerán ciertas herramientas y aplicaciones relacionadas con la prevención y detección del ciberacoso y algún que otro ámbito, todas ellas relacionadas con lo analizado en el apartado anterior y, finalmente, cabe destacar la página “Últimas noticias”, en la que se compartirán artículos actualizados de prensa y propia elaboración relacionados con el ciberacoso y las distintas problemáticas relacionadas a este, los cuales se podrán compartir y difundir para tratar de llegar a un elevado número de usuarios y concienciar a las masas de la importancia de colaborar y ser intolerante ante este tipo de situaciones.

Objetivos

Este proyecto tiene como objetivo la implementación de una solución tecnológica para una de las problemáticas más presentes en nuestras redes desde que estas se inauguraron: el ciberacoso. El principal objetivo de la aplicación es el de ayudar a las víctimas que sufren este hecho y el de concienciar a los distintos usuarios de la importancia de participar a favor de las víctimas mediante la defensa de éstas y la no tolerancia a acosadores. Es importante destacar que uno de los principales problemas relacionados con el ciberacoso es que tanto víctimas como testigos, por miedo al contraataque o a volverse (más) víctimas suelen sufrir este tipo de situaciones en silencio, sin contar con la ayuda de profesionales o de su propio entorno y esta es una de las finalidades de la aplicación, dar un revés a la situación y poder reducir con el tiempo el número de acosadores. Como “sub-objetivos” tenemos todos aquellos mencionados en la descripción tales

como la difusión de las distintas herramientas de protección o la compartición de novedades los cuales, en conjunto, harán que finalmente se pueda cumplir el objetivo y finalidad principal.

Ahora bien, por otra parte cabe destacar que la aplicación tiene una finalidad puramente social y educativa, es decir, no está orientada a ser empleada como una herramienta mediante la cual obtener beneficios económicos, si no que es una aplicación sin ánimo de lucro. A nivel personal, mi mayor obtención a partir de esta aplicación sería la satisfacción de saber que llega a un elevado público obteniendo así un incremento de víctimas ayudadas haciendo así que decrezca el ciberacoso. Finalmente, cabe destacar que uno de los objetivos de la aplicación es el de colaborar con entidades como la Guardia Civil, Policía Nacional y la asociación Protégeles. En relación a estos, lo que se quiere facilitar con esta aplicación son los trámites y la identificación de las distintas tipologías de ciberacoso o problemáticas relacionadas. Se les facilitará a los cuerpos de seguridad del estado todas las denuncias delictivas clasificadas por tipología, sexo y edad, lo cual facilitará las fluidez con la que podrán actuar los distintos departamentos. Además, estos ofrecerán apoyo psicológico a las víctimas. Por otra parte, la asociación protégeles actuara de guía y orientador de cara a los más jóvenes y niños.

Especificaciones técnicas

La *App* a desarrollar estará disponible para descargar en tabletas y smartphones, mediante servicios de distribución como *Google Play* o *App Store*. Para poder acceder a descargar la aplicación será necesario tener acceso a internet en un principio, aunque después, una vez obtenida la aplicación, podremos visualizar aquellos contenidos vía *offline*.

La aplicación se podrá obtener de manera gratuita, aunque previamente el usuario deberá registrarse en los distintos servicios de distribución y en esta misma para dejar constancia de su adquisición. Además, se valorará que, dependiendo del dispositivo en el que sea descargada la *App*, determinará que esta sea más o menos interesante y variará su funcionalidad (no todos los dispositivos tienen la misma potencia).

La aplicación destacará por el valor de su contenido, una correcta usabilidad (se facilitará un uso sencillo e intuitivo mediante una buen diseño e interfaz de usuario) y, dando una gran importancia al soporte web.

A su vez, el contenido de la aplicación se irá actualizando temporalmente según vaya surgiendo novedades y se vayan consiguiendo ciertos objetivos dentro de la temática que se abarca.

Contenidos y estructura

Páginas	Contenido
Registro	En esta primera página, la cual aparecerá antes de acceder al propio contenido de la App, deberemos registrarnos para poder acceder a la misma.
Inicio	Esta es la primera página a la que accederemos una vez habiendo iniciado sesión. En ella se podrá observar una breve introducción al contenido y funcionamiento de la App. A su vez, aparecerán las instituciones que colaboran con la misma.
Denuncia	En esta página, los usuarios deberán, primeramente, indicar el tipo de ciberacoso que sufren y posteriormente rellenar un formulario. Una vez habiendo realizado esto, será imprescindible que se acepte una afirmación de veracidad para presentar la denuncia pues, si una vez estudiado el caso este se tratase de una broma o de una mentira, el peso de la ley podrá caer sobre el usuario que ha formalizado la denuncia. Habiendo completado todos los campos, la denuncia es presentada.
Protégete	Esta página, en relación a lo estudiado y analizado en el Capítulo 5, ”Herramientas preventivas”, se presentarán aquellas herramientas o sistemas que ayudarán a prevenir o detectar cualquier problemática relacionada con el ciberacoso o relacionadas con este, según lo investigado y las conclusiones extraídas.
Últimas noticias	“Últimas noticias” es una página en la que se presentan noticias, artículos, guías y consejos de manera actualizada. Es decir, en esta sección, podremos encontrar tanto noticias a cerca de sucesos relacionados con el ciberacoso como avisos a cerca de nuevas normativas aprobadas o nuevas aplicaciones o sistemas software nacidos con la intención de derrotar este tipo de problemáticas.

Tabla 7. Contenidos App.

Las operaciones asociadas a la interfaz (alta, baja, gestión de contenidos) cumplirán el diagrama de flujo siguiente de alto nivel (Figura 34).

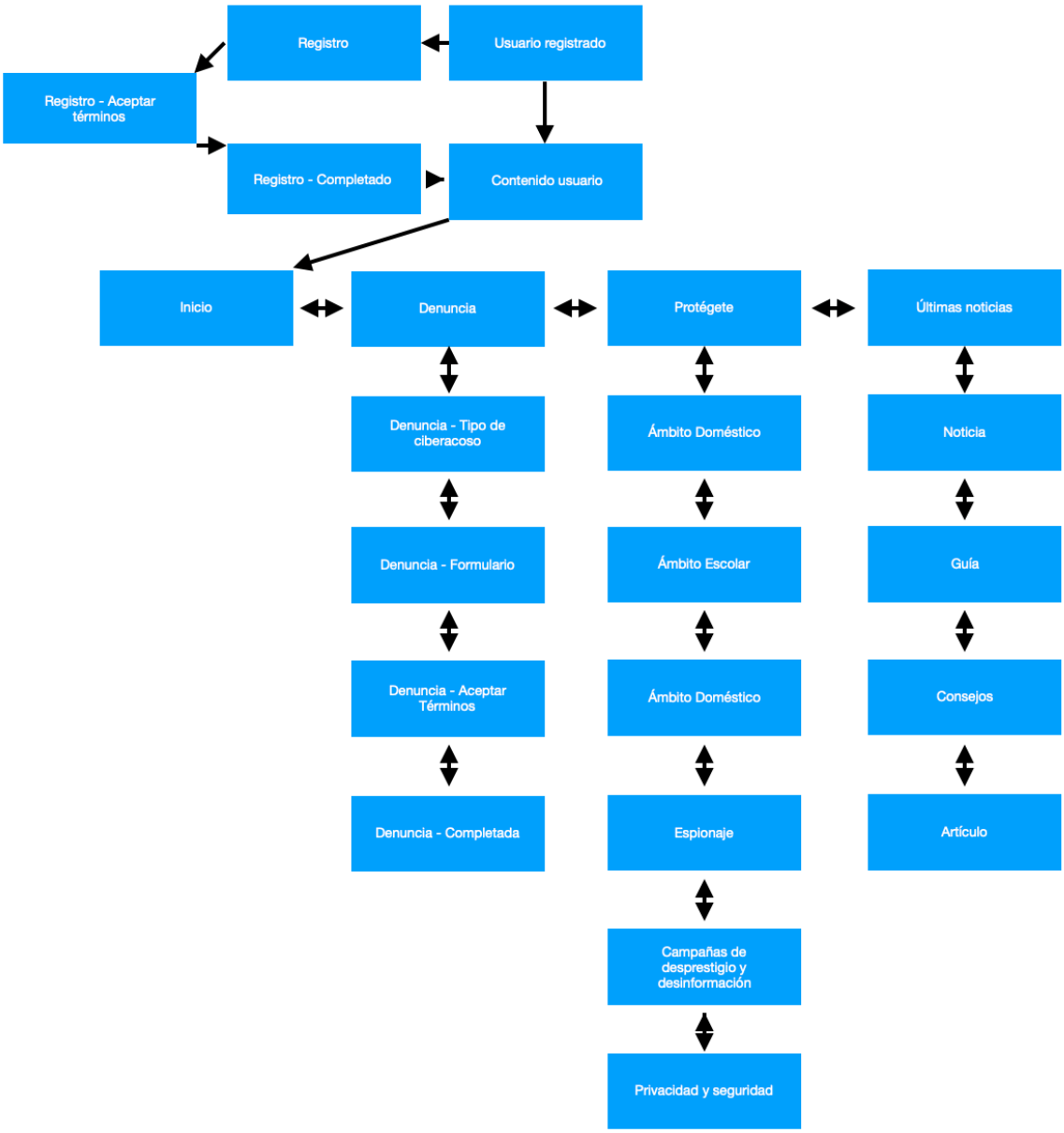

Figura 30. Estructura App.

Look and Feel

El diseño que se plasmará en la aplicación estará basado en el empleo de una paleta de colores simples para poder resaltar en mejor manera los distintos elementos textuales y gráficos, como la introducción de la página inicio o los logos de los colaboradores. El objetivo mediante esto es conseguir una sensación de naturalidad y una interfaz intuitiva y, evitar así complicados menús.

Más concretamente, se empleara una imagen de fondo transparente casi blanca, que aportará un tono azulado formando siluetas generando así una mayor armonía y manteniendo un buen contraste, lo que llamará la atención del usuario. En cuanto a las gráficas e imágenes a emplear, estarán relacionadas con imágenes representativas de la página noticias, logotipo, logos de colaboradores y herramientas de descargas en la página “Protégete”. Se utilizará una calidad óptima de las mismas. Más aún, la tipografía a emplear será *Gill Sans*, debido a que se le quiere dar un toque de actualidad, elegante y selecto en conjunto al contenido de la aplicación/contenido.

Finalmente, comentar que lo que se pretende es ofrecer una alta accesibilidad en relación a todos los componentes dinámicos (acceso a distintas páginas, menús desplegables, botones, formas e imágenes) ofreciendo así una mayor naturalidad e interactividad al usuario.

Creación de Logotipo

El logotipo se basará en una señal de tráfico como la de “Stop” o “Prohibido el paso”. Mediante esto se conseguirá representar la idea de “hasta aquí hemos llegado”, “no más ciberacoso”, “ciberacoso, no puedes pasar”, representando así la temática y el contenido que trata el proyecto y la propia aplicación. Básicamente, se partirá de 0 y con la ayuda de un programa de diseño se crea la señal. Siguiendo nuestro referente, esta portará tonalidades rojas. A su vez, se incrustará la tipografía “NE. Nueva Era” de manera original en el centro de la señal. ¿Por qué Nueva Era? Porque queremos que este trabajo transcienda y se difunda y la aplicación sea referente de cara a instaurar nuevos tiempos en los que la interacción a través de los entornos digitales se lleva a cabo de manera “sana”.

Representación gráfica

Ver Anexo 1 y 2.

Conclusiones

Dando por finalizado el desarrollo del análisis e investigación y habiendo propuesto el desarrollo de una nueva aplicación para combatir el ciberacoso y las problemáticas relacionadas a este, toca dar paso a las conclusiones.

Por una parte, cabe destacar que el ciberacoso y las problemáticas relacionadas a este provocan, a día de hoy, una dificultad de cara a la convivencia en el mundo digital que no para de crecer y que no remite, tanto a nivel nacional, en España, como a nivel internacional, centrándonos en el ámbito europeo. Este problema se encuentra directamente relacionado con dos factores.

El primero de ellos es el de la falta de la educación digital. Con esto nos referimos a que muchos de los usuarios que emplean las redes sociales y se introducen al mundo digital creen que por el mero hecho de interaccionar con otros a través de una pantalla pueden actuar malintencionadamente bajo su libre albedrío, pues o bien consideran que están respaldados por un falso anonimato, o bien consideran que a nivel legislativo nada les puede ocurrir y, estas creencias, unidas a ciertas características relacionadas con la personalidad y el entorno de estos, les lleva a delinquir. A su vez, cobra gran importancia el hecho de que la educación que se nos ha sido inculcada en el mundo analógico no traspasa al mundo digital, pues esa sensación de libertad y de encontrarnos en otro mundo nos hace olvidarnos de ella.

El segundo de ellos es el del desconocimiento de herramientas preventivas que pueden servir para prevenir, detectar y combatir el ciberacoso o problemáticas relacionadas a este. Es decir, al igual que en el mundo analógico contamos con una alarma en nuestra casa por si nos entran a robar e intentan invadir nuestra privacidad y seguridad, también debemos de contar con ciertas herramientas o soluciones para actos de este tipo similares que se dan en el mundo digital. Al igual que cuidamos de nuestros hijos pequeños en el mundo analógico y les intentamos ayudar ante todo tipo de situaciones que transcurren en el día a día y llevamos un control de su actividad diaria, esto también debe de extrapolarse y llevarse a cabo en el entorno digital.

Para poder eliminar estos factores relacionados directamente con la aparición del ciberacoso y otras problemáticas relacionadas a este, se deberá de llevar a cabo una colaboración mutua entre ambos. Es decir, para poder conseguir que estas problemáticas disminuyan será indispensable la aplicación de un incremento de la educación en el entorno digital y el empleo de herramientas o aplicaciones de prevención (al igual que ocurre en el entorno analógico). La educación a la que nos vemos inculcados en el mundo analógico debe de ser extrapolada al mundo digital y esto, en el caso de menores y jóvenes, puede llevarse a cabo mediante la ayuda de soluciones tecnológicas (como el empleo de herramientas de control parental) que nos ayudarán a controlar y educar de manera remota y a asegurarnos de que el comportamiento y conductas de este tipo de usuarios en la red es el adecuado, pudiendo así disminuir este tipo de problemáticas en un futuro. A su vez, podremos ayudarnos de otro tipo de herramientas (contra el espionaje, privacidad y seguridad…) para así defendernos de otros tipos de usuarios problemáticos.

Más aún, cabe destacar que la propuesta de aplicación da solución tanto de cara a la denuncia por parte de víctimas o testigos de un caso de ciberacoso o problemáticas relacionadas a este como a los agresores. Esto se debe principalmente a que los usuarios adultos que cometen este tipo de actos delictivos ya no pueden ser educados digitalmente de la misma manera que un usuario mejor o joven, el cual, todavía esta “a tiempo”. Es por esto que mediante la ayuda de la aplicación y de su función “Denuncia” se podrá poner en manos de las autoridades como la Guardia Civil, Policía Nacional o la asociación Protégeles casos relacionados con este tipo de problemáticas y, de esta manera, ayudar a víctimas y a su vez, tratar de reinsertar digitalmente a los agresores de cara a futuras reincorporaciones a las redes.

Por otra parte, cabe destacar el sorprendente escaso marco normativo y legislativo que se da en España y, más aún, en territorio europeo. Se puede llegar a entender desde el punto de vista de que las problemáticas analizadas se pueden considerar recientes dentro del entorno digital, pues la evolución tecnológica y la aparición de las comunidades virtuales ha sido rápida y la aparición de dichas problemáticas también. No obstante, pese a que a nivel nacional contamos con penalizaciones de cara a los ciberagresores (está penado el ciberacoso, *grooming*, *ciberstalking*…) es de necesidad que el Parlamento Europeo y la Comisión Europea se pongan de acuerdo y terminen de formalizar un marco y contexto respecto al ciberacoso y problemáticas relacionadas a este, pues estoy convencido de que establecer una normativa general a nivel europeo en la que todos los estados miembros estén involucrados hará que estos y las instituciones relacionadas con las redes sociales modifiquen sus normativas y términos de uso y se centren en la consecución de decrementar todas las problemáticas definidas con anterioridad. Me apoyo en esto gracias a los resultados que ha dado la implantación en 2018 del nuevo RGPD, en el que se han visto involucrados en su implantación tanto los estados miembro como instituciones relacionadas directamente con las redes sociales.

Finalmente, comentar que, sin lugar a dudas, este es uno de los proyectos (sino el que más) más ambiciosos que he desarrollado tanto en mi vida profesional/académica como personal. La parte de análisis e investigación y la recuperación de datos actualizados y contrastados ha sido complicada, puesto que hay muchos estudios a cerca del ciberacoso y problemáticas relacionadas a este, por lo que, utilizar las más precisas y actuales ha sido la prioridad. En cuanto al trabajo más profesional, considero que me he involucrado en desarrollarlo al máximo detalle, empleando así, todo tipo de recursos diferentes necesarios para llevarlo a cabo. Me llevo un gran aprendizaje de cara al futuro, el cual, quiero formar a partir de la disciplina, el trabajo, el esfuerzo, la constancia y la motivación, cualidades básicas que han sido vitales para llevar a cabo este Trabajo de Fin de Grado.

Anexos

Anexo 1: Representación gráfica de la propuesta de aplicación

Figura 31. Página Registro (1).

Figura 32. Página Registro (2).

Figura 33. Página Registro (3).

Figura 34. Página Inicio.

Figura 35. Página Denuncia (1).

Figura 36. Página Denuncia (2).

Figura 37. Página Denuncia (3).

Figura 38. Página Denuncia (4).

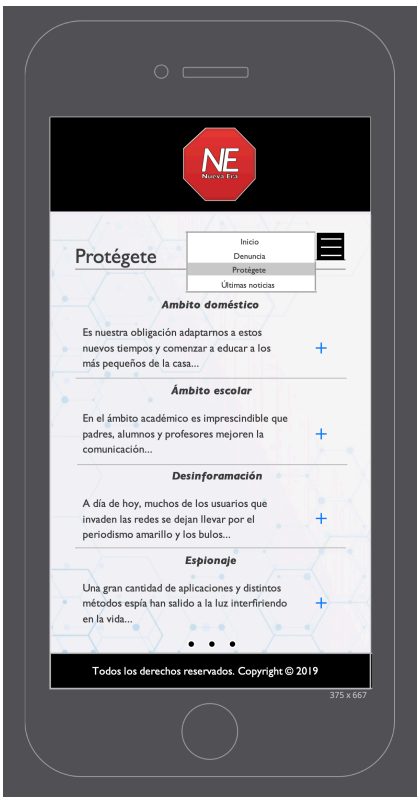

Figura 39. Página Protégete (1).

Figura 40. Página Protégete (2).

Figura 41. Últimas noticias (1).

Figura 42. Últimas noticias (2).

Anexo 2: Logotipo

Versión tienda

Figura 43. Logo versión tienda.

Versión Encabezado App

Figura 44. Logo versión App.

Versión Original

Figura 45. Logo versión original (alternativa).

Referencias

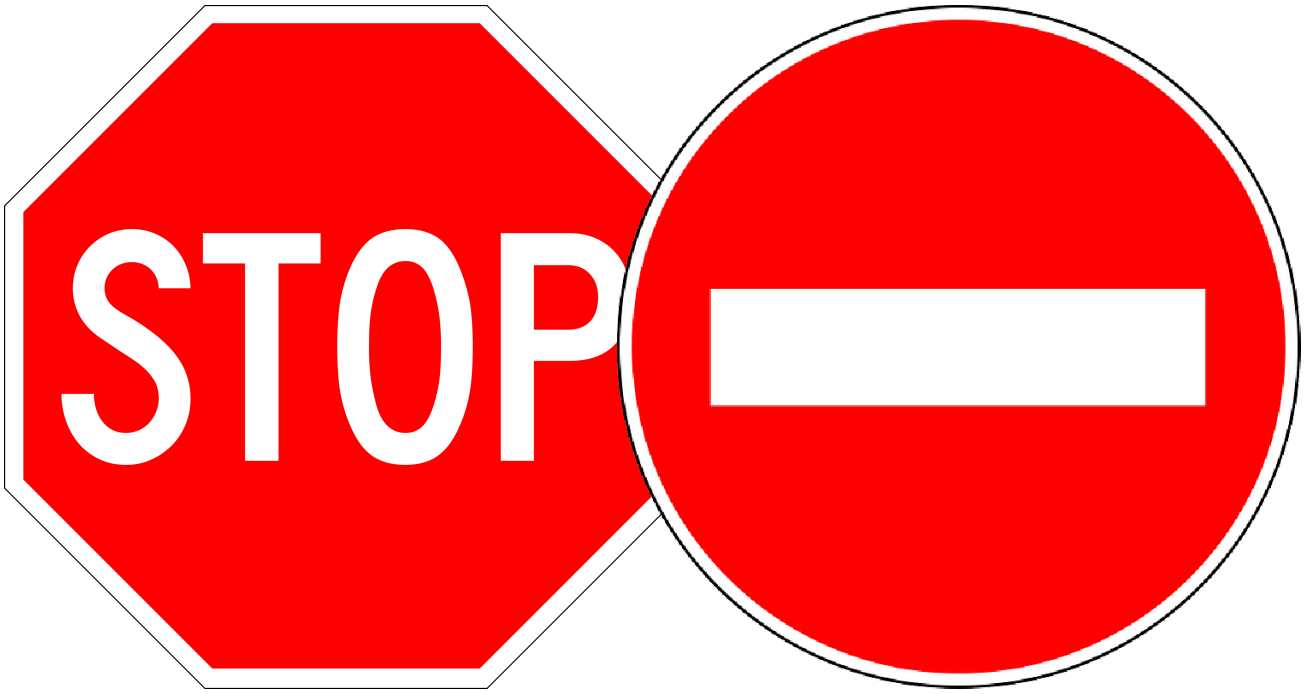

Figura 46. Referencia logotipo.

Bibliografía

Documentación y referencias en orden de aparición

-Redacción Multiplicalia (2019). Redes Sociales más usadas en 2019
Lugar de publicación: *Multiplicalia [artículo en línea]. Recuperado de:* http://evoredessociales.blogspot.com/2011/05/marco-teorico.html

-Arias, S. (2019). Las mejores frases sobre Social Media y Marketing Digital
Lugar de publicación: *Digitalist Hub [artículo en línea]. Recuperado de:* https://digitalisthub.com/las-mejores-frases-sobre-social-media-y-marketing-digital/

-López, C.A. (2019). Trabajo De Investigacion Meto. Lugar de publicación: *Calameo [documento en línea]. Recuperado de:* https://es.calameo.com/books/004797995b35320d73dbf

-Suarez, G. (2018). Bauman: "Internet es un mundo de ciberacoso y difamación"
Lugar de publicación: *El Mundo [artículo en línea]. Recuperado de:* https://www.elmundo.es/papel/lideres/2018/01/28/5a6a113fca4741dd3f8b45ec.html

-Fernández,R. (2017). Distribución porcentual de los estudiantes víctimas de ciberbullying en España en 2017, por edad de inicio. Lugar de publicación: *Statista [artículo en línea]. Recuperado de:* https://es.statista.com/estadisticas/608487/porcentaje-de-estudiantes-victimas-de-ciberacoso-por-edad-de-inicio-en-espana/

-Social Report Blog (2018). ¿Cómo ser verificado en todas las redes sociales en 2019?. Lugar de publicación: *SocialReport [artículo en línea]. Recuperado de:* https://es.socialreport.com/insights/article/360019252852-C%C3%B3mo-ser-verificado-en-todas-las-redes-sociales-en-2019-

-Castells, M. (1996). *La sociedad red*. Madrid: Alianza

- Redacción ABC (2018). Uno de cada dos casos de ciberacoso en España lo provoca un compañero de clase. Lugar de publicación: *ABC [artículo en línea]. Recuperado de:* https://www.abc.es/familia/educacion/abci-cada-casos-ciberacoso-espana-provoca-companero-clase-201806270224_noticia.html

- Wikipedia (s.f.). Yam (sistema postal). Lugar de publicación: *Wikipedia [documento en línea]. Recuperado de:* https://es.wikipedia.org/wiki/Yam_(sistema_postal)

- López, A. (2015). Richebourg, un curioso espía de 58 centímetros de altura. Lugar de publicación: *20 minutos [artículo en línea]. Recuperado de:* https://blogs.20minutos.es/yaestaellistoquetodolosabe/richebourg-un-curioso-espia-de-58-centimetros-de-altura/

- Sabadell, M.A. (2016). Así nos espían en las redes sociales. Lugar de publicación: *Muy interesante [artículo en línea]. Recuperado de:* https://www.muyinteresante.es/revista-muy/noticias-muy/articulo/asi-nos-espian-en-las-redes-sociales-951474008569

- Redacción crónicas africanas (2015). La educación es el arma más poderosa que puedes usar para cambiar el mundo. Lugar de publicación: *Crónicas Africanas [artículo en línea]. Recuperado de:* http://cronicasafricanas-matildegp.blogspot.com/2015/09/lo-dijo-mandela-en-su-discurso.html

- Palacio, A. (s.f.).12 grandes frases sobre educación. Lugar de publicación: *serPadres [artículo en línea]. Recuperado de:* https://www.serpadres.es/3-6-anos/educacion-desarrollo/fotos/8-grandes-frases-sobre-educacion/la-educacion-ayuda-a-la-persona-a-aprender-a-ser-lo-que-es-capaz-de-ser

- Chueca, I. G. (2017).Cómo evitar y combatir el cyberbullying. Lugar de publicación: *La Vanguardia [artículo en línea]. Recuperado de:* https://www.lavanguardia.com/vida/20171115/432884519381/todas-las-claves-para-evitar-el-cyberbullying-love-brl.html

- Redacción RTVE (2019).Al menos dos estudiantes en cada clase sufren ciberacoso escolar en España. Lugar de publicación: *RTVE [artículo en línea]. Recuperado de:* http://www.rtve.es/noticias/20190205/menos-dos-estudiantes-cada-clase-sufren-ciberacoso-escolar-espana/1879262.shtml

- UNICEF y AEP (2019). Nueva era del Bullying: Ciberacoso. Lugar de publicación: *AEP [documento en línea]. Recuperado de:* https://www.aeped.es/sites/default/files/documentos/entrega4_aep_ciberacoso.pdf

- Redacción La Sexta (2019). Aumentan las cifras de ciberacoso: conoce cómo detectarlo y cómo pararlo. Lugar de publicación: *La Sexta [artículo en línea]. Recuperado de:* https://www.lasexta.com/programas/arusitys/mejores-momentos/aumentan-las-cifras-de-ciberacoso-conoce-como-detectarlo-y-como-pararlo_201909185d81f8960cf26d238d595bc0.html

- ANAR (2016). I Estudio sobre acoso escolar y ciberbullying según los afectados. Lugar de publicación: *ANAR [documento en línea]. Recuperado de:* https://www.observatoriodelainfancia.es/ficherosoia/documentos/4998_d_I-Estudio-Cyberbullying.pdf

- ANAR (2017). II Estudio sobre acoso escolar y ciberbullying según los afectados. Lugar de publicación: *ANAR [documento en línea]. Recuperado de:* https://www.anar.org/wp-content/uploads/2017/04/INFORME-II-ESTUDIO-CIBERBULLYING.pdf

- ANAR (2018). II Estudio sobre acoso escolar y ciberbullying según los afectados. Lugar de publicación: *ANAR [documento en línea]. Recuperado de:* https://www.anar.org/wp-content/uploads/2018/09/III-Estudio-sobre-acoso-escolar-y-ciberbullying-seg%C3%BAn-los-afectados.pdf

- Gobierno de España e INTECO (s.f.). Guía de actuación contra el ciberacoso. Lugar de publicación: *Xuventude [documento en línea]. Recuperado de:* http://xuventude.xunta.es/uploads/Gua_de_actuacin_contra_el_ciberacoso.pdf

- Cabañas, A.L. (2016). Ciberacosado, ¿qué puedo hacer?. Lugar de publicación: *e-volucion [artículo en línea]. Recuperado de:* http://www.e-volucion.es/2016/09/ciberacosado-que-puedo-hacer

- Gobierno de España, Red, Sema, Hospital Universitario La Paz (2015). El ciberacoso para profesionales de la salud. Lugar de publicación: *Adolescencia Sema [documento en línea]. Recuperado de:* https://www.adolescenciasema.org/usuario/documentos/Guia_Ciberacoso_Profesionales_Salud_FBlanco.pdf

- Redacción Sanitas (s.f.). ¿Qué es el ciberacoso?. Lugar de publicación: *Sanitas [artículo en línea]. Recuperado de:* https://www.sanitas.es/sanitas/seguros/es/particulares/biblioteca-de-salud/psicologia/ciberacoso.html

- Administrador (2018). Las consecuencias psicológicas del ciberacoso: Análisis desde la perspectiva psicológica. Lugar de publicación: *Lomber [artículo en línea]. Recuperado de:* http://lomber.es/las-consecuencias-psicologicas-del-ciberacoso-analisis-desde-la-perspectiva-psicologica/

-UNIR (2018). UNIR elabora el primer estudio sobre acoso y ciberacoso en alumnos con altas capacidades. Lugar de publicación: *UNIR [artículo en línea]. Recuperado de:* https://www.unir.net/vive-unir/noticias/unir-elabora-el-primer-estudio-sobre-acoso-y-ciberacoso-en-alumnos-con-altas-capacidades/549203614418/

-La Nacion (2010). Una niña, insultada en Facebook. Lugar de publicación: *La Nacion [artículo en línea]. Recuperado de:* https://www.lanacion.com.ar/sociedad/una-nina-insultada-en-facebook-nid1261618

-Hassan, C. (2016). Una joven víctima de ‘bullying’ se suicidó en frente de su familia. Lugar de publicación: *CNN [artículo en línea]. Recuperado de:* https://cnnespanol.cnn.com/2016/12/02/una-joven-victima-de-bullying-se-suicido-en-frente-de-su-familia/

-Calvo, M. (2018). Qué es el acoso en internet y cuándo es delito. Lugar de publicación: *El periódico [artículo en línea]. Recuperado de:* https://www.elperiodico.com/es/extra/20180212/acoso-internet-delito-6618285

-Ciberacoso.net y Pantallas Amigas (s.f.). Tipos de ciberacoso. Lugar de publicación: *Ciberacoso.net [artículo en línea]. Recuperado de:* https://ciberacoso.net/

-ABC Familia (2019). Qué es el «grooming» y por qué ha aumentado un 410% en los últimos años. Lugar de publicación: *ABC [artículo en línea]. Recuperado de:* https://www.abc.es/familia/padres-hijos/abci-grooming-y-aumentado-410-por-ciento-ultimos-anos-201903081632_noticia.html

-Jupsin (2016). Infografía del ciberbullying en España. Lugar de publicación: *Jupsin [artículo en línea]. Recuperado de:* https://jupsin.com/noticias/el-ciberbulllying-en-espana/

- Redacción ABC (2019). El ciberacoso también es una cuestión de género. Lugar de publicación: *ABC [artículo en línea]. Recuperado de:* https://www.abc.es/contentfactory/post/2017/11/23/el-ciberacoso-tambien-es-una-cuestion-de-genero/

-COGAM (2015-2016). Ciberbullying LGTB-Fóbico. Lugar de publicación: *CogamEduca [documento en línea]. Recuperado de: https://cogameduca.files.wordpress.com/2016/03/4-ciberbullying-lgbt-fc3b3bico-informe-completo-web.pdf*

-Escriche, E. (2017). El perfil del acosador escolar: entre la angustia y la crueldad. Lugar de publicación: *UOC [artículo en línea]. Recuperado de:* https://www.uoc.edu/portal/es/news/actualitat/2017/014-bullying.html

-Formatjé, N.B (2018). Agresiones sexuales en internet: el perfil de la víctima y del agresor. Lugar de publicación: *UOC [artículo en línea]. Recuperado de:* https://www.abc.es/contentfactory/post/2017/11/23/el-ciberacoso-tambien-es-una-cuestion-de-genero/

-Pardo, L.S *et* al (2016-2017). Los adolescentes y el ciberacoso. Lugar de publicación: *Fundación CSZ [documento en línea]. Recuperado de:* http://www.fundacioncsz.org/ArchivosPublicaciones/292.pdf

-Internet Segura for Kids (s.f.). Ciberacoso escolar. Lugar de publicación: *Internet Segura for Kids [artículo en línea]. Recuperado de:* https://www.is4k.es/necesitas-saber/ciberacoso-escolar

-Barrera, S. (2015). ¿Cómo puedo darme cuenta de que me espían a través del móvil?. Lugar de publicación: *La Sexta [artículo en línea]. Recuperado de:* https://www.lasexta.com/tecnologia-tecnoxplora/internet/ciudad-con-ley/como-puedo-darme-cuenta-que-espian-traves-movil_2015060157f794e20cf2a2e945b3dc36.html

-Del Rosal, P. (2018). Espiar el móvil de tu hijo, reenviar un vídeo sexual y otros delitos de privacidad que puedes cometer sin saberlo. Lugar de publicación: *El Pais [artículo en línea]. Recuperado de:* https://elpais.com/economia/2018/05/22/mis_derechos/1526987320_921066.html

-Perito Informatico (2016). Pericia en la suplantación de identidad en Redes Sociales. Lugar de publicación: PeritoInformático *[artículo en línea]. Recuperado de:* https://peritoinformatico.es/blog/como-defenderse-legalmente-suplantacion-redes-sociales/

-EFE/20MINUTOS (2013). Cronología del 'caso Snowden', el joven que reveló el espionaje masivo de Estados Unidos. Lugar de publicación: *20minutos [artículo en línea]. Recuperado de:* https://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/

-Telescopio (2017). Las redes sociales: ¿agencias de espionaje?. Lugar de publicación: *Mundo sputnik news [artículo en línea]. Recuperado de:* https://mundo.sputniknews.com/radio_telescopio/201706221070167302-redes-sociales-espionaje/

-Europa Press. (2018). Cierra Cambridge Analytica, la empresa que usó datos de Facebook para influir en el «brexit» y en el triunfo de Trump. Lugar de publicación: *La voz de asturias [artículo en línea]. Recuperado de:* https://www.lavozdeasturias.es/noticia/actualidad/2018/05/02/cierra-cambridge-analytica-empresa-uso-datos-facebook-influir-brexit-triunfo-trump/000315252863140217627 72.htm

-Moral, M.M. (2017). Estas son las compañías que más te “espían” en la Red. Lugar de publicación: *AS [artículo en línea]. Recuperado de:* https://as.com/meristation/2017/12/13/betech/1513156162_469107.html

-Fierro, J. C. (2016). Desinformación y las redes sociales. Lugar de publicación: *También Somos Americanos [artículo en línea]. Recuperado de:* http://tambiensomosamericanos.com/desinformacion-y-las-redes-sociales/

-Sanhueza, P.M. (2017). “Medios de comunicación y posverdad: Análisis de las noticias falsas en elecciones presidenciales de EE. UU. de 2016”. Lugar de publicación: *TFG Universidad Autónoma de Barcelona [documento en línea]. Recuperado de:* https://ddd.uab.cat/pub/trerecpro/2017/hdl_2072_293813/TFM_Priscilla_Munoz.pdf

-Sierra, C. (2019).¿Puede identificar Google las noticias falsas?. Lugar de publicación: *Diario Información [artículo en línea]. Recuperado de:* https://www.diarioinformacion.com/vida-y-estilo/tecnologia/2019/01/19/identificar-google-noticias-falsas/2109060.html

-Alcaide, P. (2019). *Campañas de desprestigio de gente tóxica*. Lugar de publicación: *Palcaide [artículo en línea]. Recuperado de:* https://www.palcaide.com/campanas-de-desprestigio-de-gente-toxica/
-Camilo, P.G. (2013). Historias de desprestigio contra marcas de prestigio. Lugar de publicación: *Camilo Perez García [artículo en línea]. Recuperado de:* https://camiloperezgarcia.wordpress.com/2013/07/18/historias-de-desprestigio-contra-marcas-de-prestigio/

-Antevenio Redacción. (2016). 7 ejemplos de crisis en redes sociales mal gestionadas . Lugar de publicación: *Antevenio Anticipation e-Marketing [artículo en línea]. Recuperado de:* https://www.antevenio.com/blog/2016/10/crisis-en-redes-sociales-mal-gestionadas/

-Jimenez, Eva. (2018). El 88% de los usuarios acepta los términos y condiciones en internet sin leerlos, según OCU. Lugar de publicación: *OCU [artículo en línea]. Recuperado de:* https://www.ocu.org/organizacion/prensa/notas-de-prensa/2018/privacidad070318

-Álvarez, E. (2017). Estas son las formas más fáciles de hackear contraseñas, según Google. Lugar de publicación: *Computer Hoy [artículo en línea]. Recuperado de:*https://computerhoy.com/noticias/software/estas-son-formas-mas-faciles-hackear-contrasenas-segun-google-71487

- Redacción ABC (2019). La mitad de los menores españoles de entre 12 y 14 usa Instagram siendo la edad mínima 14 años. Lugar de publicación: *ABC [artículo en línea]. Recuperado de:* https://www.abc.es/familia/padres-hijos/abci-mitad-menores-espanoles-entre-12-y-14-instagram-siendo-edad-minima-14-anos-201907270209_noticia.html

-Peyró, P. (2018). Así es el ciberbullying en Europa en 7 distintos países. Lugar de publicación: *Control-parental [artículo en línea]. Recuperado de:* http://www.control-parental.es/asi-es-el-ciberbullying-en-europa-7-distintos-paises/

-Redacción Incibe (2019). Leyes en ciberseguridad que afectan a tu empresa. Lugar de publicación: *Incibe [artículo en línea]. Recuperado de:* https://www.incibe.es/protege-tu-empresa/blog/leyes-ciberseguridad-afectan-tu-empresa

-Redacción Incibe (2019). Cumplimiento legal. Lugar de publicación: *Incibe [documento en línea]. Recuperado de:* https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_cumplimientolegal.pdf

- Redacción OSI (2019). Protección de datos, ¿qué novedades se avecinan?. Lugar de publicación: *OSI [artículo en línea]. Recuperado de:* https://www.osi.es/es/actualidad/blog/2018/01/30/proteccion-de-datos-que-novedades-se-avecinan

Herramientas preventivas

-Google (2008). Google Play (17.9.17) [Aplicación Móvil]. Descargado de: https://play.google.com/store

-Apple (2008). App Store (Versión 3.0 “1003.3”) [Aplicación Móvil]. Descargado de: https://www.apple.com/es/ios/app-store/

-Wondershare Software Co., Ltd (2018). Famisafe (Versión 3.2.0) [Aplicación Móvil]. Descargado de: https://www.apple.com/es/ios/app-store/ y https://play.google.com/store

-Qustodio (2017). Qustodio Control Parental (Versión 180.39.0) [Aplicación Móvil]. Descargado de: https://www.apple.com/es/ios/app-store/ y https://play.google.com/store

-ParentalClick (2017). ParentalClick (Versión 2.0) [Aplicación Móvil]. Descargado de: https://www.apple.com/es/ios/app-store/ y https://play.google.com/store

-Dinantia (2017). Dinantia (Versión 2.0.20) [Aplicación Móvil]. Descargado de: https://www.apple.com/es/ios/app-store/ y https://play.google.com/store

-AppVise Spain SL. (2017). AppVise (Versión 3.3) [Aplicación Móvil]. Descargado de: https://www.apple.com/es/ios/app-store/ y https://play.google.com/store

-Maldita.es (2019). Maldita.es - Periodismo para que no te la cuelen (Versión 1.0.10) [Aplicación Móvil]. Descargado de: https://www.apple.com/es/ios/app-store/ y https://play.google.com/store

-Incognito - Spyware Removal by Arcane Solutions (2019). Eliminador de software espía GRATIS (Varía según dispositivo) [Aplicación Móvil]. Descargado de: https://www.apple.com/es/ios/app-store/ y https://play.google.com/store

-Anti Spy Mobile (2017). Anti Spy Mobile FREE (Versión 1.9.10.46) [Aplicación Móvil]. Descargado de: https://www.apple.com/es/ios/app-store/ y https://play.google.com/store

-2121 Atelier, Inc (2019). Jumbo: Privacy + Security (Versión 1.31.0) [Aplicación Móvil]. Descargado de: https://www.apple.com/es/ios/app-store/ y https://play.google.com/store

Glosario

Términos

Android: sistema operativo móvil desarrollado por *Google*, basado en *Kernel* de *Linux* y otros *software* de código abierto. Fue diseñado para dispositivos móviles con pantalla táctil, como teléfonos inteligentes, tabletas, relojes inteligentes, automóviles y televisores.

Anti-Spyware: es una tecnología de seguridad que ayuda a proteger a un equipo contra *spyware* y otro *software* potencialmente no deseado (generalmente malicioso).

APK: un archivo con extensión .apk contiene una aplicación para el sistema operativo *Android*. Es un acrónimo de su nombre en inglés *Android Application Package*. Es muy parecido a los archivos ejecutables que tenemos en *Windows* (.exe o .msi) desde los que instalamos *software*. El formato APK es básicamente un formato de compresión parecido al ZIP y que dentro contiene todos los archivos necesarios para que funcione una aplicación en *Android*.

Aplicación híbrida: en el contexto en el que se ha desarrollado el trabajo, una aplicación híbrida es un sistema desarrollado para teléfonos móviles que recoge todas aquellas funcionalidades cualificadas para combatir contra las problemáticas existentes en redes sociales.

Artículo: parte de un tratado, ley o documento oficial que forma con otras iguales una serie numerada y ordenada.

Banear: en la jerga informática, se llama *ban* o baneo a una restricción; ya sea total, parcial, temporal o permanente, de un usuario dentro de un sistema informático, generalmente una red.

Bulos: noticia falsa que se difunde, generalmente, con el fin de perjudicar a alguien.

Campaña de desprestigio: plan deliberado y malintencionado para acabar con la buena fama o nombre de una persona o institución.

Cebos: ver *Luring*.

CEO: es el máximo ejecutivo de la empresa y sobre él recaen grandes responsabilidades, como tomar las decisiones más importantes y dirigir las estrategias que llevarán a la empresa a conseguir sus objetivos.

Ciberacecho: es un tipo de acoso que se da por medio del uso de algunas tecnologías, principalmente Internet. Se caracteriza por el seguimiento e investigación constante de información sobre una persona o empresa. Es un acto premeditado, repetitivo, obsesivo, y sobre todo, no deseado.

Ciberacoso: también denominado acoso virtual, es el uso de redes sociales para acosar a una persona o grupo de personas, mediante ataques personales, divulgación de información confidencial o falsa entre otros medios.

Ciberacoso sexual: es la persecución de un indivíduo a otro a través de mensajes, fotografías o videos de carácter sexual. La finalidad de acosador puede ser el abuso sexual en persona, la explotación pornográfica de la víctima o la extorsión.

Ciberbullying: es el acoso, amenaza, molestia, persecución o incordio realizado a través de cualquier dispositivo móvil, como puede ser el caso de teléfono móviles, *tablets*, videoconsolas, ordenadores, etc., realizado por parte de un menor hacia otro menor.

Cibercultura: es la cultura que surge, o está surgiendo, del uso del ordenador para la comunicación, el entretenimiento y el mercado electrónico. Es una cultura nacida de la utilización de las nuevas tecnologías de la información y comunicación como internet.

Ciberstalking: ver Ciberacecho.

Ciberviolencia de género: es aquella violencia desarrollada frente a la mujer que se sustancia en el mundo virtual, utilizando las nuevas tecnologías como medio paran ejercer daño o dominio.

Clickbait: es un neologismo en inglés usado de forma peyorativa para describir a los contenidos en Internet que apuntan a generar ingresos publicitarios usando titulares y miniaturas de maneras sensacionalistas y engañosas para atraer la mayor proporción de clics posibles.

Comunidad virtual: una comunidad virtual es un espacio digital diseñado para que un grupo de personas compartan sus intereses, opiniones y establezcan nuevas relaciones interpersonales.

Control parental: en el ámbito tecnológico y de las telecomunicaciones, es un sistema en formato de aplicación o interfaz que consiste en impedir, o limitar el acceso al manejo de los mismos, o a su contenido a menores de edad.

Cultura de la participación: en el entorno de la web 2.0, nos referimos con este término al modelo de interacción entre las personas que permite una participación en igualdad de condiciones y trabajo colaborativo.

Cultura digital: es un término que hace referencia a los cambios culturales que se producen a partir del desarrollo y la difusión de las TIC y, en particular, de internet y la web.

Código penal: conjunto de documentos que recoge la leyes que afectan a las faltas y delitos.

Desinformación: es la acción y efecto de procurar en los sujetos el desconocimiento o ignorancia y evitar la circulación o divulgación del conocimiento de datos, argumentos, noticias o información que no sea favorable a quien desea desinformar.

Difamación: es la comunicación a una o más personas, de una acusación que se hace a otra persona física o moral de un hecho, determinado o indeterminado, que pueda causar o cause a ésta un menoscabo en su honor, dignidad o reputación; siempre que no esté fundamentada en pruebas fehacientes.

Digitalización: supone la acción y efecto de digitalizar, en donde digitalizar significa registrar datos en forma digital o, en su segunda acepción, convertir o codificar en números dígitos datos o informaciones de carácter continuo, como por ejemplo una imagen fotográfica, o un documento, o un libro.

Encriptación: es un procedimiento mediante el cual los archivos, o cualquier tipo de documento, se vuelven completamente ilegibles gracias a un algoritmo que desordena sus componentes. Así, cualquier persona que no disponga de las claves correctas no podrá acceder a la información que contiene.

Especificaciones técnicas: es un documento en el que se prescriben los requisitos técnicos que debe reunir un producto, proceso, servicio o sistema.

Espionaje: es el acto o práctica de obtener secretos sin el permiso del poseedor de la información (personal, sensible, propietaria o de naturaleza clasificada), de individuos, competidores, rivales, grupos, gobiernos y enemigos para ventaja personal, económica, política o militar usando métodos en la Internet, redes o computadoras individuales a través del uso de técnicas de *software* maliciosos y *spyware*.

Fake news: son un tipo de bulo que consiste en un contenido seudoperiodístico difundido a través de portales de noticias, prensa escrita, radio, televisión y redes sociales y cuyo objetivo es la desinformación.

Fans: conjunto de personas que sienten gusto y entusiasmo por algo.

Flame: consiste en un mensaje deliberadamente hostil o insultante enviado sin ningún propósito constructivo.

Geolocalización: es la capacidad para obtener la ubicación geográfica real de un objeto, como un radar, un teléfono móvil o un ordenador conectado a Internet.

GPS: es un sistema que permite determinar en toda la Tierra la posición de cualquier objeto con una precisión de hasta centímetros, aunque lo habitual son unos pocos metros de precisión.
Grooming: serie de conductas y acciones deliberadamente emprendidas por un adulto, a través de Internet, con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de disminuir las preocupaciones del menor y poder abusar sexualmente de él.

Hackear: acción de comprometer los dispositivos digitales, como ordenadores, teléfonos inteligentes, tabletas e incluso redes enteras.

Happy Slapping: consiste en la grabación de una agresión física, verbal o sexual y su difusión online mediante las tecnologías digitales (páginas, blogs, chats, redes sociales, etc.). Lo más común es que esta violencia se difunda por alguna red social y, en ocasiones, puede hacerse viral.

Hater: hace referencia a un término empleado en Internet para denominar a los usuarios de la red que difaman, desprecian o critican destructivamente a una persona, a una entidad, a una obra, a un producto o a un concepto determinado, a causas poco racionales o tan sólo por el acto de difamar.

Hobby: es una actividad productiva cuyo valor reside en que la persona que la ejecuta lo hace por su interés hacia la actividad en sí misma y sus frutos intelectuales, artísticos, deportivos o materiales.

Internet: red informática de nivel mundial que utiliza la línea telefónica para transmitir la información.

iOS: es un sistema operativo móvil de la multinacional *Apple Inc*. Originalmente desarrollado para el *iPhone*, después se ha usado en dispositivos como el *iPod touch* y el *iPad*. No permite la instalación de *iOS* en *hardware* de terceros.

Look and Feel: es el conjunto de propiedades y características que le dan una identidad visual única a una interfaz gráfica y pueden ser percibidos de manera diferente de acuerdo con cada usuario.

Luring: es el uso de engaños que utilizan los pedófilos en la red o internet en el fin de llevar a los niños y niñas a tener encuentros personales con ellos.

Marketing: conjunto de técnicas y estudios que tienen como objeto mejorar la comercialización de un producto.

Modus operandi: expresión latina que significa ‘modo de obrar’ y se usa para referirse a la manera especial de actuar o trabajar para alcanzar el fin propuesto.

Motor de búsqueda: es un sistema informático que busca archivos almacenados en servidores web gracias a su araña web. Un ejemplo son los buscadores de Internet cuando se pide información sobre algún tema.

Notificación “push”: son mensajes instantáneos que recibimos en nuestros dispositivos. Los mensajes de *WhatsApp*, por ejemplo, son mensajes *push*. También lo son los SMS de promociones, las notificaciones que recibimos en nuestro navegador web o las notificaciones de aviso de un nuevo email.

Número PIN: es un número de identificación personal utilizado en ciertos sistemas, como el teléfono móvil o el cajero automático, para identificarse y obtener acceso al sistema. El PIN es un tipo de contraseña. Sólo la persona beneficiaria del servicio conoce el PIN que le da acceso al mismo; esa es su finalidad.

Offline: es un estado respecto a nuestra presencia en redes sociales o en la web. *Offline* hace referencia a estar desconectado de la misma.

Online: es un estado respecto a nuestra presencia en redes sociales o en la web. *Online* hace referencia a estar conectado en la misma.

Phising: es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta.

Prensa amarilla: es un tipo de periodismo que presenta noticias con titulares llamativos, escandalosos o exagerados para tratar de aumentar sus ventas, aunque por lo general estas noticias no cuenten con ninguna evidencia y sin una investigación bien definida.

Redes sociales: son estructuras formadas en Internet por personas u organizaciones que se conectan a partir de intereses o valores comunes. A través de ellas, se crean relaciones entre individuos o empresas de forma rápida, sin jerarquía o límites físicos.

Sexting: se refiere al envío de mensajes sexuales, eróticos o pornográficos, por medio de teléfonos móviles. Inicialmente hacía referencia únicamente al envío de SMS de naturaleza sexual, pero después comenzó a aludir también al envío de material pornográfico a través de móviles y ordenadores.

Sextorsion: es una forma de explotación sexual en la cual una persona es chantajeada, generalmente por aplicaciones de mensajería por Internet, con una imagen o vídeo de sí misma desnuda o realizando actos sexuales que generalmente es compartida con fines de que se haga viral mediante *sexting*.

Smartphone: es un teléfono inteligente que cuenta con la capacidad de llevar a cabo diversas funciones además de las convencionales como llamadas telefónicas y envío de mensajes. Algunos ejemplos son la navegación en internet e instalación de aplicaciones.

Social Media: es un término en ingles que significa medios sociales. Es un sistema de plataformas donde la gestión de la información es creada y visualizada por los usuarios mediante la tecnología web 2.0, donde además pueden compartir y transferir textos, fotografías, audio y vídeo, entre otros.

Software: soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados *hardware*.

Software espía: es un *malware* (programa malicioso) que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

Soporte web: es una asistencia que brindan los propietarios de las webs para que sus clientes puedan hacer uso de sus productos o servicios. La finalidad del soporte técnico es ayudar a los usuarios para que puedan resolver ciertos problemas.

Spyware: Ver *Software* espía.

Stalking: es el término usado para referirse al trastorno que tiene una persona que lo lleva a espiar a su víctima.

Status: Posición social que una persona tiene dentro de un grupo o una comunidad.
Suplantación de identidad: ver *Phising*.

Tablet: es una computadora portátil de mayor tamaño que un teléfono inteligente. Se trata de una sola pieza que integra una pantalla táctil (sencilla o multitáctil) que emite luz y con la que se interactúa primariamente con los dedos o un estilete (pasivo o activo), sin necesidad de teclado físico ni ratón.

Tableta electrónica: ver *Tablet*.

TIC: conjunto de tecnologías desarrolladas en la actualidad para una información y comunicación más eficiente, las cuales han modificado tanto la forma de acceder al conocimiento como las relaciones humanas. TIC es la abreviatura de Tecnologías de la Información y la Comunicación.

Tuit: es el nombre que reciben las publicaciones en la red social *Twitter*. Los tuits constan de una extensión máxima de 140 caracteres. Son de carácter público (salvo que se cree una cuenta privada) y aparecen automáticamente en el timeline de los usuarios que siguen al tuitero que ha publicado el mensaje, es decir, que ha tuiteado.

Virus informatico: es un *software* que tiene por objetivo de alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo.

Web 2.0: comprende aquellos sitios web que facilitan el compartir información, la interoperabilidad, el diseño centrado en el usuario y la colaboración en la *World Wide Web*. Web 2.0 permite a los usuarios interactuar y colaborar entre sí, como creadores de contenido.

Web apaleador: es una página web creada para hacer acoso a un usuario por parte de su acosador o agresor, metiéndose con él/ella de manera pública y ridiculizándolos/las. A menudo se anima a otros internautas a participar en el abuso.