EL “CYBERSTALKING” EN LAS REDES SOCIALES

Daniel Amat Huerta

Tutor: Roger López Ayala

9 de junio de 2023

ÍNDICE

“*El progreso no es un accidente, es una necesidad, una parte de la naturaleza”*

(Herbert Spencer, 1820-1903).

1– INTRODUCCIÓN

1.1– Contextualización e impacto del ciberespacio en las sociedades actuales

La humanidad tiende a avanzar hacia el progreso para reducir sus necesidades y mejorar las condiciones de vida, generando como resultado modificaciones en los elementos estructurales de las sociedades de cada época.

Es un hecho que las sociedades actuales no son equiparables con las de los siglos pasados, ya que estas se fundamentan en un elemento que cambia con el tiempo, el conocimiento.

Un ejemplo que demuestra este hecho consiste en observar cómo ha cambiado el concepto de Estado. Max Weber, a principios del siglo pasado, definió el Estado como una entidad política caracterizada por ostentar una población, una capacidad de soberanía o toma de decisiones, unas instituciones político-administrativas, el monopolio del uso la fuerza legítima, y un territorio delimitado por fronteras naturales o artificiales en el espectro físico. (Weber, 1993)

Esta definición, con el conocimiento y el contexto de la época, se ajustaba en gran medida a la realidad, pero, hoy en día aspectos como la territorialidad se han ido difuminando debido a la aparición del ciberespacio y a la globalización, y, con ello el modelo de autoridad que ha estado establecido durante décadas, ya que, en el ciberespacio, aunque las autoridades tienen una cierta relevancia en este campo a la hora de garantizar la seguridad de los usuarios, han dejado de ser los principales suministradores de esta.

La globalización, entendida como “un proceso de transformación social basado en la integración e interconexión, creciente en el tiempo, a nivel económico, político y cultural entre los diferentes países del mundo” por el sociólogo Ulrich Beck (1986/2006), ha sido el último gran suceso que ha generado un cambio en la estructura de la sociedad.

El mismo autor, en su obra “La Sociedad del Riesgo” ya vislumbró que, aunque en primera instancia esta globalización traería consigo una infinidad de ventajas en todos estos ámbitos, a largo plazo traería nuevos riesgos y desafíos globales, como la desigualdad económica o el cambio climático, debido al alto nivel de interdependencia entre los Estados globalizados. Y, con los sucesos de estos últimos años como la pandemia del COVID-19 o la inflación mundial posterior a esta, podríamos estar de acuerdo con que acertó en este aspecto, demostrando lo vulnerable que es la sociedad actual debido a esta (Beck, 1986/2006).

Para hacer frente a estas vulnerabilidades, las sociedades y estados deberían tener estructuras sólidas y estables que se focalicen en convertirlas en fortalezas. No obstante, tal y como Zygmunt Bauman (2003/2022) expone en su obra “Modernidad líquida”, ambos conceptos se caracterizan justamente por lo contrario, por ser elementos que están constantemente en movimiento y en procesos de cambio, provocando que las vulnerabilidades existentes persistan, pero también que surjan de nuevas por los avances de la sociedad o la toma de decisiones de los estados.

Una vez expuesto esta primera parte, cabe mencionar que todos estos autores no han sido elegidos de manera arbitraria, sino para cumplir un propósito: demostrar que las sociedades han cambiado y, con ello, la forma de relacionarse, ya que, con la creación de Internet y de las redes sociales, las personas podemos interactuar en un espacio digital, independientemente de la distancia física que exista entre estas.

Como veremos en el presente informe, por las características de las redes sociales, este aspecto puede ser favorable o desfavorable para la seguridad de las personas dependiendo de las intenciones que tengan. Sin embargo, todo esto, nos lleva a un dilema que existe desde los orígenes de las sociedades humanas y que hoy en día aún persiste en estas: el dilema libertad-seguridad.

Los dos elementos, que en un principio son inversamente proporcionales, y el debate que se crea entorno a estos, así como determinar cómo deberían de darse las relaciones sociales en la sociedad de cada época, han sido materia de estudio por varios pensadores a lo largo de los siglos, de los cuáles cabe destacar a los siguientes:

Hobbes (1651/2003), en su obra “Leviatán” se mostró partidario de la necesidad de garantizar un determinado nivel de seguridad a costa de reducir las libertades que hagan falta de las personas que conforman la sociedad mediante la creación de un contrato social entre estas y el estado, que sería el encargado de garantizar su seguridad. Esto debido a la creencia de que las sociedades que carecen de uno estarían en un estado de naturaleza donde cada persona haría lo necesario para garantizar su seguridad y reinaría el caos y la guerra.

Locke (1689/1988), al contrario que Hobbes, creyó que el estado de naturaleza de las sociedades que no tienen un contrato social establecido está basado en la paz y la igualdad, no en la guerra. No obstante, también expone la necesidad de que exista un contrato social entre el estado y su población para evitar la exposición a la incertidumbre y a la amenaza de ser invadido por otros existente en el estado de naturaleza, siempre y cuando este garantice un determinado grado de libertades que el estado no puede llegar a transgredir.

Y, Mill (1859/2008), en su obra “Sobre la Libertad” coincide mayoritariamente con Locke, sobre todo en determinar que el aspecto más importante de los dos es la libertad, concretamente la individual, y el Estado, aunque es la figura que tiene que proteger a las personas de daños externos, no debe transgredir esta sin que exista una necesidad y una justificación

Las aportaciones de cada uno de los anteriores autores fueron de suma importancia en su época, pero, la realidad actual, no se basa en ningún pensamiento anterior en concreto, sino que se trata de una combinación de varios elementos que se expusieron en estos junto con los nuevos temas de interés propios de las sociedades del siglo XXI, ya que sigue siendo necesario un contrato social, pero se debe añadir aspectos como el respeto a los derechos humanos, tanto en la esfera pública como en la privada, la no asignación de roles de género a la sociedad o la participación de esta sociedad en los procesos políticos de decisión (Martí, 2005).

Todo ello, con el fin de que este contrato social sea igualitario y respetuoso con todos los géneros/razas y las formas de relacionarse existentes hoy en día, es decir, que se adapte a las necesidades de la sociedad actual, aunque éstas cambien parcialmente según el sistema político de cada estado.

Asimismo, también se debería integrar en este contrato los nuevos avances tecnológicos del momento, sin que se pudiera producir una limitación de estos, debido a que el ciberespacio, y más concretamente, las redes sociales, son otros ámbitos actuales donde la integridad del usuario puede verse afectada. Por este motivo, como se tratará posteriormente, la eliminación del anonimato y la identificación mediante algún mecanismo son los objetivos para conseguir el objetivo tan ansiado de este debate: conseguir la máxima libertad con un nivel de seguridad aceptable (González, 2015).

En este contexto general es donde surge la investigación del presente informe, que consiste en determinar qué cambios se deben llevar a cabo urgentemente en una actualización del contrato social vigente para integrar tanto todas estas nuevas prácticas que han aparecido recientemente, como el “cyberstalking”, como todo lo relativo al nuevo campo donde estas se dan, el entorno virtual, haciendo especial énfasis en las redes sociales, y, con ello, poder establecer nuevas medidas que permitan garantizar la seguridad de los usuarios en el ciberespacio.

Para ello, como hay múltiples redes sociales en la actualidad, este trabajo estará acotado a tres de las principales redes sociales de los últimos 10 años: Facebook, Twitter e Instagram.

Como último dato antes de pasar al marco teórico, me gustaría mencionar brevemente que las motivaciones que me llevaron a elegir este campo en concreto fueron que, por una parte, tiene una repercusión mediática menor respecto a otras prácticas similares como el “cyberbullying”, y, por otra parte, que está relacionado con el ciberespacio y la ciberseguridad, los cuáles son campos que siempre me han suscitado un gran interés.

2 – Marco teórico y conceptual

El internet, las redes sociales, los sistemas de programación…Todos ellos son elementos que fueron creados con una finalidad diferente. No obstante, tienen un aspecto común: son concepciones relativamente nuevas que traen riesgos y amenazas que no se habían planteado hasta el momento, como es el caso del “cyberstalking”.

Antes de la revolución industrial de los años 50-70, era descabellado pensar en un escenario de amenaza que consistiera en que una persona nos vigilara desde su casa, mediante un anonimato que dificultara su identificación y sin estar físicamente presente donde nos encontremos, pero, actualmente, es una realidad.

Por este motivo, es de especial relevancia definir el “cyberstalking” y todos los elementos que le rodean de la manera más clara y concisa como sea posible según los conocimientos actuales que se tenga sobre la materia.

2.1 – Internet

2.1.1 – Resumen histórico de su creación

Internet, también conocido como ”red de redes”, nació con la tercera revolución industrial que se llevó a cabo durante los años 1950 y 1970 con la idea de reemplazar el sistema de comunicación de datos existente de la época a través de la creación de un nuevo sistema de comunicación que fuera capaz de soportar un mayor tráfico de datos y que dotará de mayores capacidades a los usuarios (Coffman & Odlyzko, 2001).

Según Coffman & Odlyzko (2001), su origen proviene de la creación de la Agencia de proyectos de investigación avanzada (ARPA) por parte del gobierno de los Estados Unidos de América durante la Guerra Fría con el objetivo de convertirse en el país “líder” en cuanto a avances tecnológicos y científicos se tratara, y, a su vez, por la época histórica en la que se da, ostentar una mayor capacidad defensiva y de disuasión frente al bloque soviético. En esta agencia es donde se empezaron a llevar a cabo pruebas piloto para convertir la idea de Licklider, un estudioso del MIT, que consistía en crear un mecanismo de interconexión entre ordenadores de forma global donde se pudiera intercambiar y acceder a la información independientemente del lugar del planeta, a una realidad.

Sin embargo, no era una tarea sencilla teniendo en cuenta que los conocimientos sobre telecomunicaciones y electrónica habían surgido recientemente. Por ello, trabajaron por fases para crear el Internet que conocemos hoy en día.

Lo primero que hicieron fue trabajar sobre la idea de Leiner de crear una red cooperativa donde los usuarios fueran capaces de compartir sus ordenadores. Con este fin, y después de haber creado todos los elementos necesarios, en 1969 se llevó a cabo una prueba piloto que consistió en la instalación de cuatro dispositivos, uno que funcionara como “host” y tres que funcionaran como nodos, interconectados mediante una red inalámbrica en diferentes estados de los Estados Unidos.

Este hecho, permitió que se diera el primer envío de un mensaje digital entre ordenadores localizados en diferentes estados, creando la primera versión en miniatura de Internet, la cual fue nombrada como “ARPANET”, y marcando así el nacimiento de Internet (Coffman & Odlyzko, 2001).

La segunda fase, tal y como mencionan Coffman & Odlyzko (2001), se dio un año más tarde del suceso anterior, el año 1970, en el que, por fin, se pudo crear una conexión entre hosts y permitir la comunicación entre estos.

A partir de esta última fase, por cada año que pasaba, se iban añadiendo más hosts y nodos para expandir la red que conformaba ARPANET y se empezó a trabajar en otros elementos destinados a facilitar la comunicación como fue la aplicación de mensajería “Email”. Todo ello, hasta que en 1973 se realizó la primera conexión internacional entre dos dispositivos: uno ubicado en Estados Unidos y otro en Inglaterra.

Este hecho generó que el proyecto tuviera cada vez más popularidad entre la población y se fuera desvinculando de su propósito inicial militar/de defensa militar, hasta que en 1978 se creó la primera versión de ARPANET con un fin comercial, es decir, con el objetivo de crear una forma de negocio donde las empresas ISP pudieran obtener beneficios económicos a cambio de dotar a unos usuarios de la capacidad de comunicarse mediante esta red (Coffman & Odlyzko, 2001).

Por último, Coffman & Odlyzko (2001) mencionan en su investigación que, en los años posteriores, se fueron creando otras versiones de redes de este estilo como MILNET o NSFNET, hasta que, finalmente, en el 1996, la red se convirtió de “dominio público” para cualquier persona, creando así, Internet.

2.1.2 – Definición del concepto

Una vez expuesto un breve resumen de la historia de cómo se originó el elemento que nos atañe en esta sección del trabajo, se puede llegar a la conclusión que, al igual que el elemento y la tecnología que lo envuelve han ido evolucionando con el tiempo, el concepto en sí mismo también ha ido sufriendo varias transformaciones.

Sin embargo, aunque actualmente Internet está fuertemente integrado en nuestras vidas, definirlo por su multiplicidad de funciones y usos es una tarea compleja en la que se han embarcado varios autores y organizaciones de renombre.

Por una parte, una posible definición del concepto es la que realizó el Tribunal Supremo de los Estados Unidos en 1997. En este caso, el tribunal lo definió como “una red global de ordenadores interconectados que permite a millones de personas comunicarse entre sí y acceder a fuentes inacabables de información”, incluyendo una perspectiva que conforma el aspecto diferenciador con otros autores, la cual consistió en describirlo como “un modo de comunicación humana totalmente nuevo y único que interconecta personas del mundo entero” (Reno, et al.1997).

Por otra parte, otra posible aproximación al concepto es la que hacen Lee Sproull y Samer Faraj en su aportación al libro “Cultura de Internet” de Sara Kiesler, donde exponen que la función de cualquier red es permitir acceso a la información o el intercambio de esta entre usuarios (Lawrence Erlbaum Associates, Inc., 2014).

Sin embargo, los autores en cuestión no limitaron la concepción que tenían sobre Internet a un aspecto tan limitado como sería el decir que este fuera una “red” más, sino que lo definieron como “una tecnología social que permite encontrar, interactuar, y mantener una relación prolongada en el tiempo con personas con gustos similares, así como informar y prestar servicios comerciales” (Lawrence Erlbaum Associates, Inc., 2014).

Como he mencionado anteriormente, existen una multiplicidad de actores que han definido el concepto desde su creación, pero, como el presente trabajo de investigación no se va a centrar en este elemento, estos dos ejemplos descritos nos aportan suficiente información como para concluir que, aunque cada autor lo define según sus conocimientos y le da más énfasis a una función en concreto que a otra, todos coinciden en la esencia de lo que es Internet, la cual consiste en ser un mecanismo social en forma de red que habilita la comunicación interpersonal del mundo entero y permite acceder a una fuente infinita de información

2.1.3 – Descripción de las características de Internet

La invención de Internet y su expansión a la población a partir del 1978 ha traído consigo una inmensidad de ventajas para la sociedad. Algunas de ellas que cabe mencionar son las siguientes:

-Dota de una mayor comodidad para el usuario. Con la comercialización de Internet y la posibilidad de adquisición por parte de la población a los servicios que presta este, la comunicación se ha vuelto más sencilla, ya que, aunque ya existía el teléfono fijo y las cabinas telefónicas para acortar la distancia en la comunicación y poder contactar con una persona que estaba lejana físicamente, permite que se pueda hacer en cualquier lugar y en cualquier momento de forma "segura" (López, 2019).

-Permite conocer gente nueva. Una de las utilidades que tiene Internet es que permite conectar con personas con las que, en un primer momento por la barrera del espacio, sería imposible.

-Mejora la socialización. Con las capacidades que tiene internet, este aporta la posibilidad de relacionarse fácilmente con cualquier persona, sin necesidad de que exista algún tipo de vínculo entre las dos, permitiendo encontrar e interactuar con personas con los mismos gustos y aficiones (Medina, 2003).

-Aporta la posibilidad de pertenecer a una comunidad. Todo ser humano tiene la necesidad de formar parte de "algo", de una familia, de un círculo de amistad…Por este motivo, una de las grandes ventajas de Internet es que, al proporcionar la capacidad de que una persona se pueda relacionar con gente considerada como "igual", permite pertenecer a una comunidad virtual de ámbito mundial y generar vínculos afectivos entre sus miembros (Medina, 2003).

-Anonimato. En términos generales, en el presente trabajo, me referiré a este aspecto en su versión negativa, como una desventaja/inconveniente, pero no por ello hemos de dejar el lado positivo que este aporta esta característica de Internet a los usuarios, ya que, esta capa de anonimato existente, aporta seguridad a aquellas personas que son introvertidas, permitiendo que incluso estas que les cuesta socializar en la vida real puedan hacerlo en el ciberespacio sin importar sus preocupaciones o sus miedos (Medina, 2003).

Cabe mencionar que esta última característica, que es la más controversial de todas, representa a todos los elementos mencionados y que se mencionarán a posteriori, ya que, todos y cada uno de ellos, dependiendo de la perspectiva que la persona les dé, pueden ser un aspecto positivo o negativo para el usuario.

No obstante, aunque como podemos observar de estos ejemplos y otros no mencionados existen muchos aspectos positivos que nos aportado Internet, hay un multitud de elementos negativos que comportan riesgos para los usuarios y propician el surgimiento de ciber amenazas, entendidas como tal, “todas aquellas actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula por el mismo, para la comisión de distintos delitos mediante su utilización, manipulación, control o sustracción”. (Díaz, 2016).

Los aspectos negativos de Internet más relevantes para nuestro caso de estudio son los siguientes.

-Es un medio sincrónico, es decir, Internet es un espacio donde se mueven cantidades desorbitadas de datos personales debido a que cada usuario ha decidido voluntariamente, o en casos minoritarios, bajo amenaza, compartir cierta información personal con el resto de internautas o con ciertas entidades para poder acceder a diferentes funciones dentro de Internet, como hacer uso de una red social. Todas estas acciones se derivan a una única consecuencia que define lo consiste un “medio sincrónico”, y es que estos datos personales quedan registrados en un determinado lugar de Internet y perduran en el tiempo (Cornejo, M., & Tapia, M. L., 2011).

-A su vez, también es un medio acrónico, en otras palabras, tal y como he mencionado, los datos perduran en el tiempo, y eso se traduce en que muchas personas pueden llegar a acceder a esta información tiempo después con el objetivo de utilizar para conseguir un determinado fin, como, por ejemplo, desprestigiar a una persona célebre o a una multinacional (Cornejo, M., & Tapia, M. L., 2011).

-Enfatiza la introversión. Actualmente, un gran número de usuarios consumen Internet y los contenidos que hay en este de manera significativa y prolongada en el tiempo (Cornejo, M., & Tapia, M. L., 2011).

Esto conlleva un problema intrínsecamente relacionado con la personalidad del usuario, ya que, si este utiliza Internet para todo y únicamente se relaciona a través de Internet, provocará que no busque relacionarse con nadie físicamente o que, cuando se tenga que relacionar porque no haya otra opción, le cueste más que a una persona que consume Internet de manera moderada (Cornejo, M., & Tapia, M. L., 2011).

-Anonimato. Esta característica, aunque forma parte de la esencia de Internet, es una de las mayores amenazas para gran parte de los usuarios, ya que, la red en cuestión es un espacio difícil de controlar, que no forma parte de ningún gobierno y donde fácilmente una persona puede falsificar su información personal (nombre, apellidos, ubicación, hobbies…) y hacerse pasar por una persona que no es para conseguir un objetivo concreto.

Normalmente este aspecto se da más en aquellos espacios integrados dentro de Internet que se especializan en la interacción entre los usuarios tales como foros o, el espacio acotado del presente trabajo, las redes sociales.

2.2 – Redes sociales

2.2.1 – Historia y definición de las redes sociales

Las redes sociales, tal y como las conocemos hoy en día, son el producto de un proceso evolutivo que ha sufrido durante los años.

Aún en estas condiciones, cabe mencionar que su finalidad, la cual consiste en complementar la capacidad social innata de las personas creando espacios públicos que les permitan socializar aunque las condiciones físicas no sean favorables, se ha mantenido intacta, ya que, a día de hoy, ninguna red social busca sustituir la interacción física entre las personas (Danah & Nicole, 2007).

Según Danah y Nicole (2007), el origen de las redes sociales se remonta al 1997 con el lanzamiento de la red social “SixDegrees.com” que ya contenía elementos característicos de estas, como son la opción de la creación de un perfil y la capacidad de tener una lista de amigos. No obstante, lo que realmente es relevante es que, en un principio, las redes sociales como la anteriormente expuesta o una que hablaremos posteriormente en el informe, Facebook, fueron diseñadas para un uso meramente académico. No fue hasta 2005 que se originó la idea de expandir las capacidades que estas aportaban a la población en general y llegar a la concepción de red social que tenemos hoy en día.

Actualmente, la definición más completa del concepto de “red social”, es la elaborada por Boyd y Ellison, en la cual se expone que una red social, es un servicio prestado por una web que permite a los individuos: crearse un perfil público o semipúblico sin un sistema delimitado, construir una lista de otros usuarios con los que compartes algún tipo de relación, y ver e indagar en la lista de relaciones que tienen otros usuarios dentro del sistema (Danah & Nicole, 2007).

Cabe destacar que, a diferencia de otros elementos del presente informe, la definición de red social anteriormente expuesta está bastante delimitada debido a su alta aceptación por parte de la comunidad de expertos y de la población en general.

Expuesta esta introducción al concepto y a su origen para entender el elemento en cuestión, pasamos a describir las tres redes sociales/ámbitos a analizar en este informe.

2.2.2 – Descripción de las redes sociales: Facebook

La red social conocida como “Facebook” fue fundada por la empresa que compartía el mismo nombre que la red de Mark Zuckenberg el año 2004 con el objetivo de aportar a los estudiantes de Harvard una opción alternativa, y en parte, innovadora, de interactuar con otros estudiantes de la misma institución (Brügger, 2015).

Con el paso del tiempo, Facebook fue ganando popularidad y se fue expandiendo a otras instituciones académicas hasta que, como se ha mencionado anteriormente, eventualmente se permitió el acceso a toda la población mundial, siempre y cuando los estados no lo prohibieran, como es el caso de Canadá, donde su gobierno prohibió a los militares usar Facebook (Danah & Nicole, 2007).

Con este cambio, la empresa actualizó su misión empresarial y su objetivo con la red social[1] a "aportar a las personas una opción alternativa, y en parte, innovadora, de interactuar con personas conocidas o desconocidas de cualquier parte del mundo", ampliando su "público objetivo" (Meta, 2023).

A partir de este momento, Facebook se fue convirtiendo en la red social más famosa del mundo hasta la actualidad, donde, según los últimos datos recogidos en enero de 2023, con un total de 2,9 billones de usuarios activos mensuales, sigue manteniendo el liderazgo en este ámbito respecto al resto de redes sociales (Fernández, 2023).

2.2.3 – Descripción de las redes sociales: Twitter

Twitter es una red social que fue creada el año 2006 a partir de un proyecto de investigación y desarrollo llamado como "Status" o "Twttr" que llevó a cabo la empresa "Obvious LLC" en base a una idea que aportó Jack Dorsey.

Durante los años posteriores, el servicio recibió un gran apoyo y popularidad por parte de los usuarios de Internet, que estaba en auge, y eso favoreció a la plataforma social para recibir inversores y poder mejorar los servicios que prestaba esta según su objetivo de crear un espacio para contribuir al aumento de la salud colectiva, la apertura y las conversaciones públicas civilizadas, y para responsabilizarnos públicamente del progreso (Falcón, 2011) (Twitter, 2023).

1. La actualización de los objetivos de la empresa también produjo un cambio en la nomenclatura de esta, pasando de "Facebook" a "Meta", como se la conoce actualmente.

En este contexto, la red social ha ido creciendo a lo largo de los años en todos los aspectos, hecho que no ha dejado indiferente a organizaciones multimillonarias y personas con grandes fortunas para comprar las acciones necesarias para poder tener y controlar la empresa, como ha sido el caso reciente de Elon Musk.

En cuanto a la cantidad de usuarios activos mensuales, desafortunadamente para la red social, según los últimos datos disponibles, que son de enero de 2023, muestran un decrecimiento de usuarios activos hasta 556 millones, muy por debajo de las cantidades que presentan las otras dos redes sociales del presente informe (Fernández, 2023).

2.2.4 – Descripción de las redes sociales: Instagram

Como tercera y última red social que se tendrá en cuenta en la presente investigación tenemos Instagram. Instagram fue lanzada en un dominio web y en dispositivos móviles para el público general en el año 2010 por Systrom y Krieger.

La idea de crear una aplicación centrada en una característica en concreto, que era compartir fotos y videos, surgió de una aplicación más general llamada “Burbn” que estaba trabajando Systrom desde antes de solicitar la colaboración de Krieger en su construcción. Cuando esta fue lanzada en el 2010, vieron que la mayoría de los usuarios hacían uso de la característica de compartir fotos y, viendo la popularidad de esta mecánica, decidieron crear una nueva aplicación centrada en este aspecto, Instagram.

El objetivo principal que se buscaba con esta red social era que los usuarios de Internet tuvieran un lugar donde pudieran compartir fotos y videos de su día a día y de temas diversos con sus personas relativas y, al mismo tiempo, estas pudieran comentarlas, habilitando una interacción continua entre ambas partes: creador-seguidor (Mattern, 2017)

Dicho esto, aunque en 2012 Facebook compró esta red social porque veía su potencial, cabe mencionar que el objetivo principal se ha mantenido intacto hasta la actualidad, incluso se ha ido mejorando los servicios que aporta la red social con el tiempo para fomentar esta conexión digital (Meta, 2023).

Actualmente, tomando como referencia los últimos datos disponibles de enero de 2023, la red social se posiciona como la tercera en el “ranking” de redes sociales con mayor número de usuarios activos a nivel mundial, compartiendo su posición con WhatsApp, con un total de 2 billones de usuarios activos mensualmente (Fernández, 2023).

Por último, en lo referido a las redes sociales, se presenta a continuación una tabla comparativa de las características principales a nivel funcional y de seguridad de las tres redes sociales expuestas, con especial énfasis en la facilidad que tiene los agresores de acosar a las víctimas en estas, siendo 3 posibles escenarios:

-Baja. Se requiere de varias acciones por parte de la víctima para que la persona pueda entrar en contacto directo con ella.

-Media. Requiere que la víctima lleve a cabo una acción para que este pueda monitorizarla o acosarla.

-Alta. No es necesario que la víctima lleve a cabo una acción, la persona generalmente tiene acceso libre para llevar a cabo el acoso.

	Utilidad principal	Privacidad	Seguridad de cifrado de la información	Tipo de comunicación	Facilidad de acosar
Facebook	Conocer gente nueva	Depende de la información que el usuario decida compartir	-Autentificación por correo electrónico -Método de autentificación 2FA: SMS al móvil y correo electrónico (opcional)	Principalmente sincrónica.	Media. Requiere que la víctima acepte su "follow".
Twitter	Conocer gente nueva con gustos similares e informar a los usuarios de los acontecimientos que suceden en el mundo	Depende de la información que el usuario decida compartir	-Autentificación por correo electrónico -Método de autentificación 2FA: SMS al móvil y correo electrónico (opcional)	Principalmente sincrónica.	Media. Requiere que la víctima acepte su "follow".
Instagram	Colgar fotografías	Depende de la información que el usuario decida compartir	-Autentificación por correo electrónico -Método de autentificación 2FA: SMS al móvil y correo electrónico (opcional)	Principalmente asincrónica.	Alta. Cualquier persona puede mandar un mensaje directo a otra persona.

Tabla 1. Elaboración propia.

2.3 – Definición y características del "cyberstalking"

La exposición de las anteriores áreas, siendo estas las principales donde se dan la mayoría de las prácticas nos llevan al elemento central de nuestro campo de estudio, el "cyberstalking".

Este fenómeno, como todo lo relacionado con el campo de la ciberseguridad y del ciberespacio, es relativamente reciente y tiene dificultades añadidas para definirlo correctamente.

Primeramente, observamos que al igual que la tecnología, esta práctica sufre una evolución constante respecto a las formas en la que se lleva a cabo. Actualmente se considera "cyberstalking" las siguientes conductas: creación de webs o foros con el fin de incluir información e imágenes privadas sobre la víctima, suplantación de identidad para solicitar que sea acosada, envío de malwares tipo spyware, "keylogger" o troyanos mediante técnicas como el "phishing" o el "spear phishing" a la víctima para que el acosador pueda obtener el control del dispositivo o de un activo de valor, como las contraseñas de sus cuentas de las redes sociales, y poder monitorizar sus movimientos, entre otras; pero en un futuro, con los avances tecnológicos, aparecerán más.

Y, en segundo plano, tenemos que, aunque el ciberespacio abarca prácticamente todo el mundo, no hay una norma jurídica internacional para definir y penar esta clase de conductas, y tenemos que remitirnos a las normas internas de cada estado, en el caso que vean esta práctica como una amenaza y tengan estas conductas penadas jurídicamente.

Aún con las dificultades expuestas anteriormente, varios autores han intentado realizar diferentes aproximaciones al concepto con el fin de definirlo de manera precisa.

> En el momento que surgió, varios expertos dieron una definición de "cyberstalking" muy básica, la cual consistió en "el uso de internet para contactar con alguien o encontrar información sobre las víctimas de una manera molesta o aterrorizante". Esta es la que podemos encontrar en la actualidad en los diccionarios populares como el Collins (2023).
>
> En 2002, Bocij y McFarlane, a partir del análisis de los elementos que contienen las diferentes legislaciones del mundo, crearon una definición eficaz a nivel internacional para el fenómeno. Esta consistió en definir el "cyberstalking" como "un grupo de conductas individuales o grupales, ya sea en forma de grupo u organización, que usa las TIC para acosar a uno o más individuos. Algunas de estas conductas que podríamos incluir dentro de este delito podrían ser la transmisión de mensajes amenazadores o acusaciones infundadas, el robo de identidad con una finalidad de extorsión de la víctima a atender las demandas, el robo de información, la monitorización del dispositivo de la víctima, entre otros".
>
> Un año más tarde, en 2003, Robert d'Ovidio, M.S. y James Doyle definieron el "cyberstalking" como "el uso repetido de Internet, aplicaciones como el correo o dispositivos electrónicos similares para molestar, asustar o amenazar una persona o grupo de persona con un fin".
>
> Y, en 2010, Javier García González, investigó el ámbito y expuso un listado de características técnicas que estaban estrechamente relacionadas con el fenómeno, las cuales son:

1.Invisibilidad. Al ser una práctica propia de un entorno como Internet que aporta anonimato, entre otros aspectos anteriormente mencionados en su apartado, provoca que se le dote al acosador de unas capacidades de protección que con el “stalking” no existirían, dificultando la tarea de las autoridades para conocer la identidad de este.

2.Ausencia de contacto directo con la víctima. El acosador, al realizar la práctica por medio de dispositivos electrónicos, tiene una percepción del daño distinta al del “stalking”, provocando que no sienta que sus actuaciones estén generando graves daños y, por tanto, le cueste empatizar más con la víctima.

3.Invade ámbitos de privacidad aparentemente seguros. Algunas de las conductas que pueden considerarse como “cyberstalking” pueden ser el hostigamiento a la víctima y la humillación ante la familia mediante envío de información o imágenes comprometidas, produciendo una ruptura con la esfera privada de la víctima que es el hogar/la familia.

4.Proyección pública. La práctica del “cyberstalking”, al darse en Internet, donde confluyen todo tipo de personas, produce que el acoso sea público y fácilmente perceptible por cualquier usuario en la red, provocando, en ocasiones, que otras personas se sumen a esta, o, por el contrario, la defiendan.

5.Facilidad de difusión, reproducción y accesibilidad. Internet siempre está disponible y está al alcance de cualquiera que tenga acceso a un dispositivo electrónico, provocando que la gravedad de los actos de “cyberstalking” sea igual o mayor que la de otras prácticas que no exploten las capacidades que aporta Internet.

Sin embargo, en la actualidad, aún con todos los intentos expuestos, sigue sin haber una definición conceptual clara. Por este motivo, y siendo este fenómeno un aspecto central en la presente investigación, veo la necesidad de definirlo de la siguiente manera:

El “cyberstalking” es un fenómeno conductual constitutivo de delito que utiliza el uso de las TIC y las características técnicas que estas aportan, como el anonimato o la facilidad de difusión de información, para monitorizar y acosar intencionadamente a una persona o grupo de personas adultas, conocidas o desconocidas, de forma reiterada en el tiempo, produciendo como resultado un efecto psicológico adverso y una alteración en la vida cotidiana de la/s víctima/s.

No obstante, aun teniendo esta definición y habiendo expuesto el fenómeno en sí, sigue existiendo un problema con la terminología que normalmente se hace uso, ya que se puede llegar a confundir con otra práctica con la que comparte ciertas características y elementos: el “cyberbullying”.

Por este motivo, aunque esta no conforma el aspecto central de la presente investigación, es esencial aportar un pequeño espacio en esta para definirla brevemente y, con ello, evitar una posible confusión en futuros apartados del informe.

El “cyberbullying” es un fenómeno que, al igual que el “cyberstalking”, ha sido estudiado por varios expertos y se han llegado a algunas posibles aproximaciones.

Una de ellas es la que hacen Patchin y Hinduja, que definen el “cyberbullying” como “la voluntad de acosar a un/a menor de edad de forma reiterada a través del uso de dispositivos electrónicos”.

Por otro lado, tenemos a Kowalski que, de forma conjunta con otros autores, ha definido el “cyberbullying” como “el acto de realizar bullying a menores mediante el uso de las TIC cuya finalidad, generalmente, consiste en humillar a alguien para conseguir algo”, es decir, como una extensión del “bullying” tradicional. Sin embargo, todos coinciden en que los comportamientos que se dan en este fenómeno son los insultos, las amenazas, el acoso y, el más importante en este fenómeno, la humillación y que la víctima objetivo tiene el estado civil de menor de edad (Elizabeth, et al, 2017).

Por tanto, aunque las herramientas para llevar a cabo estas prácticas (humillación, amenazas, coacción…) pueden llegar a ser más o menos comunes en ambos y los dos requieren de un componente de "reiteración" para ser usados, el aspecto diferenciador principal que existe entre este y el "cyberstalking" reside en la edad de la víctima, ya que el término de "cyberbullying" solo se haría uso en casos de menores de edad y el "cyberstalking" solo entre adultos (Ramírez, 2019).

A su vez, en la actualidad, existe otro concepto que no he nombrado anteriormente debido a que no es equiparable a estos dos, pero que guarda una fuerte relación, ya que engloba ambas prácticas en determinadas circunstancias, este es el conocido ciberacoso. Este concepto se utiliza únicamente cuando las conductas propias del acoso en la red suceden de forma puntual por uno o varios sujetos contra una víctima en concreto, sin importar la edad de la víctima (Llinares, 2013).

Conductas	Menor-Menor		Adulto-Menor		Adulto-Adulto	
	Reiterada	Puntual	Reiterada	Puntual	Reiterada	Puntual
Cyberbullying	X		X			
Cyberstalking					X	
Ciberacoso		X		X		X

Tabla 2. Elaboración propia.

Dicho esto, y volviendo al tema central de la investigación, con toda la información expuesta anteriormente, tanto a nivel textual como gráfico, ha quedado acotado el "qué" se entiende por "cyberstalking" y el "cuándo" se debe de utilizar este término para evitar disonancias cognitivas.

No obstante, por las conductas habituales expuestas en el presente apartado, se muestra que estas prácticas pueden llegar a generar graves consecuencias físicas y psicológicas en la víctima. Por este motivo, es imperativo que existan normas de rango de ley que castiguen punitivamente la realización de estas.

3 – Marco normativo

Expuesta una definición técnica lo más completa posible sobre el fenómeno para entender todas las actuaciones que son consideradas como tal, delimitaré el concepto a lo que está integrado en el Código Penal español.

No obstante, antes de ello, cabe mencionar la Declaración de Monterrey del 2009 sobre los derechos emergente y el desarrollo económico y social en los países emergentes que, aunque no trata este tipo de prácticas de forma directa en su contenido, indirectamente los aspectos que promueve dicha declaración pueden tener un impacto en la educación de las personas para prevenir y hacer frente esta tipología de acoso, es decir, en la promoción de los derechos individuales en el ciberespacio (Andreu, 2009).

Dicho esto, como se ha mencionado anteriormente, el "cyberstalking" es un tipo de acoso relativamente reciente, ya que hasta finales del siglo pasado no se podía llevar a cabo por los requisitos tecnológicos necesarios, pero la legislación española sobre esta es aún más reciente, concretamente del 30 de marzo 2015 (Sánchez, 2016).

Antes de la anterior fecha, no existía un tipo penal específico para castigar estas prácticas y las víctimas de "cyberstalking" se aferraban a los efectos que esta producía, centrándose en que era un tipo de acoso que afectaba bienes jurídicos como la libertad de obrar, el honor, la integridad moral o la intimidad y que menoscababa el sentimiento de seguridad, que comprende el derecho al sosiego y tranquilidad personal, de la víctima (Llinares, 2013).

Por tanto, apelaban al delito de coacciones, al delito de vejaciones leves o amenazas, al delito contra la integridad moral, al delito de injurias y/o al delito de calumnias contenidas en los artículos 172.2, ex artículo 620/artículo 169, 173, 208 y 205 respectivamente. No obstante, como estos tipos penales no fueron creados pensados en un tipo de práctica delictiva como es el "cyberstalking", en algunos juicios les castigaron levemente por alguno de estos delitos, y en otros casos los acosadores quedaban impunes (Sánchez, 2016).

Un ejemplo de esta se muestra en la sentencia “SAP de Madrid n.º 407/2006, de 21 de noviembre de 2006, en la que se condenó al acusado como autor de una falta de amenazas por el envío reiterado de correos electrónicos a la víctima, con la que tuvo una relación sentimental, en los que le advertía que no podría ir tranquila por la calle y que tenía la intención de lesionar a su novio actual (Llinares, 2013).

Por este motivo, el 30 de marzo de 2015, a partir de una decisión político criminal de garantizar la protección de los bienes jurídicos de las personas ante estas conductas, se llevó a cabo una reforma del código penal español mediante ley orgánica en la cual se integraron, en el Título VI: Delitos contra la Libertad, las nuevas prácticas delictivas relacionadas con el acoso que fueron surgiendo, una de ellas el stalking, en el artículo 172 ter (Sánchez, 2016)

En dicho artículo se especifican varios aspectos importantes que son importantes para la presente investigación:

1.Lo primero es que, en 2015, como ya se había dado la expansión mundial de Internet, ya observaron que podría llegar a existir un “cyberstalking” y extendieron todos los requisitos y conductas tipificadas del “stalking” expuestas en dicho artículo al campo de las TIC/del ciberespacio. Por ello, hoy en día, se utiliza este como principal delito para castigar a los acosadores.

2.El precepto expone que, para que una conducta de “cyberstalking” sea entendida y penada como tal, debe cumplir 3 requisitos:

1.El acoso, independientemente de la naturaleza, debe darse de forma continuada, insistente y reiterada. El significado de “reiterado” varía según el autor, pero, a nivel general, se acepta lo que expusieron Pathé y Mullen en 1999, que consiste en que la conducta o la comunicación/intromisión no deseada se debe dar al menos diez veces en un período de al menos 4 semanas (Ginner & Delgado, 2017).

2.Ha de existir una falta de consentimiento por parte de la víctima en torno a la realización de esta conducta.

3.Estas acciones de acoso deben alterar gravemente el desarrollo de la vida cotidiana de la víctima mediante la provocación de miedo razonable. Para corroborar lo anterior en casos que no sean visibles las alteraciones, será necesario el informe de un psicólogo (Sánchez, 2016).

3.Y, por último, determina las conductas integradas y, por tanto, tipificadas penalmente, en este artículo, que son las siguientes:

-Vigilar, perseguir o buscar la cercanía física.

-Establecer o intentar establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

-Usar indebidamente los datos personales, adquirir productos o mercancías, contratar servicios o hacer que terceras personas se pongan en contacto con ella.

-Atentar contra su libertad, contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella (Rupérez, 2023).

No obstante, cabe mencionar que el origen de la decisión político criminal de introducir el delito de “stalking” y sus variantes en el código penal español, se vio influenciada por la iniciativa que llevó a cabo la legislación de California en el 1998, en la cual se modificó la terminología del apartado principal del artículo 646.9 de su código penal de “amenaza creíble” a “amenazas mediante comunicaciones electrónicas” con el objetivo de incluir la prohibición de las actuaciones consideradas como “cyberstalking” (Shouse Law Group, A.P.C., 2023).

4 – Preguntas de investigación y metodología

4.1 – Preguntas de investigación

El presente trabajo de investigación, tal y como he mencionado anteriormente en la introducción, tiene como objetivo determinar qué cambios se deben llevar a cabo urgentemente en una actualización del contrato social vigente para integrar tanto todas estas nuevas prácticas que han aparecido recientemente, como el “cyberstalking”, como todo lo relativo al nuevo campo donde estas se dan, el entorno virtual, haciendo especial énfasis en las redes sociales, y, con ello, poder establecer nuevas medidas que permitan garantizar la seguridad de los usuarios en el ciberespacio.

Por este motivo, la pregunta de investigación que conforma el elemento central de la investigación es: “¿Qué aspectos deben de ser redefinidos a nivel sistémico-social para se lleve a cabo una adaptación a las nuevas necesidades y se pueda llegar a garantizar un cierto nivel de seguridad y libertad a las personas ante prácticas como el cyberstalking en el entorno digital?”

No obstante, a partir de esta, se derivarán 2 preguntas de investigación secundarias para observar algunos aspectos directamente relacionados con la principal.

La primera pregunta de investigación secundaria consiste en “¿Qué medidas de protección física existentes hoy en día son extrapolables al entorno digital?”. Esta nos permitirá conocer si hay alguna medida propia del entorno físico que se puede utilizar de la misma manera o de una manera adaptada en el ciberespacio para poder proteger a los usuarios.

Y, siguiendo la misma línea de investigación, la segunda sub pregunta es “¿Quiénes son los encargados de garantizar la seguridad de los usuarios en las principales redes sociales de los últimos 10 años, como son Facebook, Twitter e Instagram, y qué medidas existentes o innovadoras podrían proporcionar seguridad frente a fenómenos emergentes como el cyberstalking?”.

En esta última se tratará de exponer si la función asociada a la figura de la “autoridad”, como es la policía en el espacio físico, se ha desplazado a un ámbito privado o, por el contrario, sigue siendo una función de una entidad pública; y, a su vez, qué medidas se han implantado o se podrían implantar en las redes sociales para dificultar y hacer frente al “cyberstalking”.

4.2 – Metodología de investigación

El diseño metodológico de la presente investigación consistirá en una metodología mixta, ya que emplearé tanto técnicas cualitativas como cuantitativas para poder llevar a cabo un análisis lo más completo posible que permita responder las preguntas de investigación expuestas en el apartado anterior y poder alcanzar los objetivos del trabajo.

Por ello, por un lado, utilizaré técnicas cualitativas como el análisis documental de datos secundarios extraídos a partir de fuentes académicas como Cercabib, Dialnet y otras obras accesibles mediante Google Scholar para obtener la información que permitirá construir la base de pensamiento de este trabajo.

Y, por otro lado, haré uso de una técnica cuantitativa, la encuesta, para poder obtener datos primarios interpretativos de varios aspectos relevantes para poder responder la segunda sub pregunta de investigación, como la opinión general sobre las medidas que hay actualmente implantadas en las redes sociales o el grado de uso de las medidas opcionales que tienen las redes sociales para proteger al usuario.

La encuesta en cuestión se realizará en formato digital y mediante un enlace de “Google Forms” a través de Instagram, Twitter y Facebook durante un periodo de tiempo delimitado.

Y, por último, la muestra tendrá por objetivo las personas mayores de 16 años que accedan desde estas redes sociales. Esto es debido a que el “cyberstalking”, como se ha explicado anteriormente, es un fenómeno que solo se da entre adultos. Cabe mencionar que el análisis será interpretativo y no se podrán extraer conclusiones verídicas debido a las razones que se expondrán en su debido momento del informe.

5 – Revisión del sistema político-social establecido

En la introducción de este trabajo se ha expuesto que el debate entre la libertad y la seguridad está directamente ligado con el concepto y la esencia del contrato social, y, aunque tiene una antigüedad considerable, sigue siendo el pilar fundamental que sustenta la estructura de las sociedades actuales.

Sin embargo, no se ha mantenido intacto a lo largo de la historia, sino que, al igual que las sociedades han ido cambiando y evolucionando, las normas para garantizar la seguridad/protección de la población y los márgenes delimitadores de la libertad se han ido ajustando al estilo de vida y de gobierno de cada momento histórico.

Por ello, debido a los cambios que han sufrido las sociedades en las últimas décadas se ha producido una necesidad urgente de redefinir el contrato social establecido con el fin de integrar todos los aspectos nuevos o temáticas de interés para la sociedad del siglo XXI.

Como se ha podido observar en el presente trabajo, algunas autoras como Martí (2005) ya han realizado algunas aproximaciones introduciendo algunos elementos del espectro físico y de la vertiente plenamente social que cumplen con esta descripción, como pueden ser la igualdad de género, la igualdad de participación en la toma de decisiones, entre otros.

No obstante, en los últimos años, la sociedad ha cambiado drásticamente con la aparición de las nuevas tecnologías, el entorno digital, etc. generando nuevas prácticas peligrosas para la integridad de las personas como el “cyberstalking” y provocando que, la acción de añadir aspectos relevantes actuales como la igualdad de género, no sea suficiente como para actualizar el contrato y conseguir que este se adapte a la realidad actual.

Este hecho es debido a que, anteriormente, Hobbes expuso en su obra “Leviatán” (1651/2003), que el contrato se fundamentaba en la existencia y la relación entre dos figuras principales con unas obligaciones definidas de forma clara:

-El Estado, cuya obligación es la de proteger a la población de posibles amenazas contra su integridad.

-La población, cuyo deber era dar cierto grado de libertad al Estado para que se pudiera dar esta transacción.

Pero, con el surgimiento del entorno digital, si bien los Estados siguen teniendo un cierto grado de influencia en este, el papel de autoridad que originalmente ostentaban los Estados se ha ido difuminando a causa de que el ciberespacio está controlado de forma directa por empresas multinacionales de carácter privado y/o por magnates multimillonarios.

En este contexto, el poder de influencia que un Estado puede tener es variable según algunos factores como:

-La tipología de sistema político que esté vigente en él. En la actualidad hay una gran variedad de sistemas políticos: democracias directas, democracias representativas, dictaduras…y, según el sistema que tenga, cada Estado tomará unas decisiones que pueden ir encaminadas a tener más o menos control sobre las actividades que realizan sus ciudadanos en la red y, por lo tanto, controlar de cierta manera esta red.

Mayoritariamente, el mundo actual está compuesto por democracias de algún tipo y siguen la regla general de tener un cierto grado de influencia, pero sin llegar a controlar una parte de Internet, ya que el acceso a cualquier rincón de Internet se suele entender como una extensión de la propia libertad, mientras no contraten o compren bienes o servicios ilegales según la legislación del Estado.

No obstante, hay excepciones, y el ejemplo por excelencia es el caso de China. El sistema político chino actual consiste en una dictadura comunista donde se busca controlar a sus ciudadanos en cualquier espectro de la realidad, incluido el digital. Por ello, el gobierno chino cataloga qué dominios webs son afines al régimen comunista y son accesibles por la población china, y cuáles no lo son y los ciudadanos tienen el acceso vetado, controlando así una parte de Internet.

-La posición que ostente en el plano internacional. La posición mundial de un Estado no se limita meramente al porcentaje del PIB mundial que representa, sino que también es el cómputo de un conjunto de elementos propios del “soft power” que describe Nye (2006), como las victorias/medallas en competiciones multifacéticas a nivel regional o mundial o el nivel educativo de un estado comparado con el resto.

Todo ello dota de un mayor estatus al Estado en cuestión para poder tener más influencia sobre las multinacionales que controlan el ciberespacio como Google, Meta, entre otros.

Sin embargo, la pérdida de la función protectora por parte del Estado y la adquisición de esta por parte del ámbito privado puede llevar consigo un conjunto de problemáticas como las siguientes:

-Su objetivo discrepa del objetivo propio de una figura autoritaria. Las empresas privadas como las nombradas, a diferencia de organismos de la realidad física como los cuerpos policiales, no fueron creadas entorno a la idea de proteger, sino que fueron creadas con el objetivo último de obtener el máximo beneficio económico posible, a veces, sin importar los medios legales que se hagan uso y si los usuarios están satisfechos.

Esto conlleva un riesgo debido a la indiferencia que pueden llegar a tener sobre la aplicación de nuevas medidas de seguridad que dificulten las prácticas como el “cyberstalking” debido a que, a nivel general, no existe una obligación normativa de implementar una medida especifica contra este tipo de fenómenos, y que la elaboración e implantación de medidas en una red social u otra aplicación/dominio web conlleva destinar una cierta cantidad de recursos.

-La cantidad de recursos disponibles destinados a aumentar la seguridad. Las entidades privadas nombradas, en un principio, no son reacias a aplicar medidas de seguridad, ya que eso lo pueden llegar a ver como una oportunidad de obtener prestigio en un mercado que es competitivo, pero esto se da siempre y cuando la elaboración e implementación no traiga consigo un coste económico muy elevado, ya que en el caso que así fuera, esta acción pasaría a segundo plano debido a su objetivo principal.

Aún con estas problemáticas, la situación actual es que la figura que ostenta el papel de "autoridad" en el entorno cibernético no está del todo definida y consistiría en un papel compartido entre los Estados y las empresas privadas.

Con todo lo expuesto hasta el momento, se puede observar que un cambio de un aspecto tan concreto como es la "figura" que tiene el papel de autoridad y, por tanto, la obligación de proteger a los ciudadanos, o usuarios en el entorno digital, cambia enormemente los fundamentos del contrato social.

Por ello, es de vital importancia realizar/añadir cambios sustanciales a su esencia mediante el establecimiento de nuevos elementos relacionados con la tecnología actual y las nuevas formas que tiene la población de relacionarse.

A continuación, se procederá a determinar las directrices generales de los cambios que se deben llevar a cabo:

-Añadir una nueva figura: las empresas privadas. Tal y como se ha explicado a modo de razonamiento anteriormente, se debe llevar a cabo una ruptura de la idea preexistente de que la única figura que debe tener la obligación y función de proteger a las personas sea el Estado, ya que, en los entornos digitales, las empresas privadas pueden reemplazar a este en su papel/posición dentro del contrato y, por lo tanto, deberían estar sujetas a las mismas condiciones que tiene el Estado.

-Extensión de la protección/seguridad. Una pieza del contrato social original consistía en que, la autoridad, representada por la figura del Estado, garantizara la protección de la integridad física y moral de las personas que estuvieran dentro de su territorio, que estaba delimitado por fronteras.

Sin embargo, ya en la introducción se ha mencionado que el elemento de la territorialidad que expuso Max Weber (1993) en su definición de Estado se ha difuminado a causa de la globalización y la aparición del ciberespacio, ya que el entorno digital no tiene unos límites del todo definidos, aunque cada dominio web pertenece a una entidad pública o privada/persona física o jurídica y podría ser una forma de delimitación de Internet, pero no es la materia principal de esta investigación.

Por este motivo, el cambio respecto a la seguridad y la obligación de la autoridad de proteger a las personas debería extenderse, en la medida de lo posible, al entorno digital con el fin de que los usuarios puedan sentirse seguros ante prácticas como el “cyberstalking”.

-Extensión del entorno donde garantizar la libertad. Tal y como expuso John Stuart Mill en su obra “Sobre la libertad” (1859/2008) mediante la redacción de la frase “Mi libertad acaba cuando empieza la tuya”, es vital que dentro de un entorno donde nos relacionamos constantemente con otras personas, como son la sociedad o el ciberespacio, se determinen unos límites de la libertad individual con el fin de conseguir una coexistencia lo más pacífica posible.

No obstante, la presente aproximación de Mill que ha tenido una función ejemplificadora para expresar la necesidad de delimitar la libertad individual de las personas únicamente conforma una de las múltiples aproximaciones realizadas durante la historia sobre el contrato social.

Otra de ellas es la aproximación de Hobbes en su obra Leviatán (1651/2003), donde se especifica que el límite de la libertad individual de una persona reside en la capacidad de agresión o de amenaza a la seguridad pública que traiga asociada su comportamiento o las acciones que lleve a cabo. Es decir, si a partir de una acción que quiera realizar una persona se puede esperar que se genere un daño a otra persona o plantee un problema de seguridad para las demás personas, no se le permitirá que la haga.

A partir estas aproximaciones, el cambio que se debería realizar para actualizar el contrato social y poder garantizar un cierto grado de libertad y seguridad a las personas, consistiría en, al igual que el aspecto de la seguridad, ampliar el campo de limitación de libertades al ciberespacio, sobre todo en las partes de Internet donde se relacionan la mayoría de los usuarios como las redes sociales.

Cabe mencionar que, aunque se ha mencionado que los estados tienen cierta influencia en este entorno, los organismos responsables de delimitar los márgenes de las libertades individuales en este tipo de entornos serían las empresas privadas, ya que son las que llevan las redes sociales en el día a día.

Respecto a cómo deben fijarse estos márgenes, cada empresa puede decidir qué comportamientos son aceptables o inaceptables, pero, en cualquier caso, una vez realicen esa distinción, deberán notificarlo a todos los usuarios de alguna manera. Un ejemplo factible sería integrar estas reglas de conducta en la política de Términos y condiciones de uso que los usuarios deben aceptar antes de hacer uso de la red social.

Con estos cambios, el contrato social quedaría redefinido a nivel tecnológico y no estaría dirigido exclusivamente a un entorno físico, sino que pasaría a contemplar también el entorno digital.

La gran relevancia de incluir esta temática en el contrato se fundamenta en que, desde la creación de ARPANET, la expansión de Internet a la población, y la creación de las redes sociales, gran parte de la sociedad pasa un tiempo considerable en el campo digital diariamente, aunque este puede variar debido a factores como el tiempo libre disponible o la edad, pero, en cualquier caso, se le ha dotado de una gran importancia a todos los niveles del sistema (Coffman & Odlyzko, 2001).

Esto puede representar un problema debido a que todos estos avances tecnológicos son relativamente recientes y carecen de una delimitación social o normativa que abarquen todas las problemáticas que han surgido en el entorno digital.

Por este motivo, la actualización del contrato social en cuestión también debe ir dirigida a la vertiente tecnológica, ya que es vital que se establezcan unos límites a las libertades individuales, concretamente, a la libertad de acción, es decir, a la capacidad que tienen las personas para poder realizar acciones, y unas medidas de seguridad que protejan, en la medida de lo posible, a los usuarios de prácticas que puedan producirles efectos adversos de algún tipo.

Para llevar a la práctica los cambios de seguridad anteriormente expuestos, existen tres métodos de trabajo que están diferenciados por el "destino" al que deben ir encaminados y los esfuerzos que son necesarios aportar para reducir lo máximo posible la incidencia de fenómenos como el "cyberstalking" y/o proteger a los usuarios, y estos son los siguientes:

-Actuar en las causas. Incidir en el razonamiento psico-social que lleva a las personas a realizar este tipo de prácticas y generar el problema, centrarse en el "Por qué" el agresor decide llevar a cabo tales acciones, normalmente suele ser la opción más eficaz para acabar con este tipo de problemáticas. Sin embargo, teniendo en cuenta que los recursos que la figura que tiene el papel de autoridad son limitados y que las causas pueden ser muy variadas porque dependerán de la personalidad y las experiencias vividas de cada persona, este enfoque, aunque es el ideal, no es el más óptimo ni realista desde un punto de vista objetivo.

-Actuar en los efectos. El impacto que pueden provocar las prácticas que consisten en acosar a una persona por medio de un entorno digital, como es el caso del tema del presente trabajo: el “cyberstalking” en las redes sociales, son principalmente psicológicos, aunque, en determinadas ocasiones que el acosador tenga acceso a la información que comparte la víctima por Internet o al dispositivo de la víctima mediante la inyección de un malware tipo troyano, puede acabar trasladando el problema a un espectro físico, como es el “stalking” y un posterior abuso sexual.

Aunque reducir y/o evitar los efectos deben ser dos objetivos que tener en mente, incidir y destinar recursos a este enfoque no puede ser en ningún caso la solución para dificultar las praxis de estos fenómenos y proteger a los usuarios, ya que, si bien es cierto que destinar una cierta cantidad de recursos psicoterapéuticos puede ser de gran ayuda para estas víctimas, el daño, que es lo que se intenta evitar, ya habrá sido causado.

-Actuar en aspectos del entorno. Anteriormente, en el marco teórico, se ha expuesto los dos entornos donde suceden los casos de este tipo de prácticas: Internet y las redes sociales.

Internet, la “red de redes” como se ha podido ver, tiene la capacidad de interconectar todos los dispositivos del mundo de manera simultánea. No obstante, no es en esta donde principalmente se produce la interacción entre las personas, sino que es en unas aplicaciones web integradas dentro de la red que conocemos como redes sociales.

Incidir y destinar recursos, por una parte, a las redes sociales para que tengan las capacidades necesarias, tanto a nivel de conocimiento técnico como humano, económico, etc., y puedan poner “obstáculos” a los posibles acosadores en forma de medidas de seguridad, y, por otra parte, a los estados para que determinen los elementos que debe tener cada práctica adversa para que constituya un delito y se considere como tal, es otra forma a tener en cuenta.

Una vez descritos los tres enfoques y a partir de la información expuesta, la opción por la que este trabajo se inclinará de ahora en adelante consiste en la de actuar en el propio entorno, ya que, desde una perspectiva subjetiva, esta es donde existe una mayor capacidad para incidir y, por tanto, es la óptima para conseguir un mayor grado de protección para los usuarios respecto a fenómenos como el “cyberstalking”.

6 – Medidas “anti-cyberstalking”

Como bien se ha mencionado en el apartado anterior y a lo largo del informe, el entorno donde se materializa la temática principal de la presente investigación, el “cyberstalking", y el destino de los cambios que se han expuestos corresponde al ciberespacio, más concretamente, a las redes sociales ubicadas en una porción de Internet.

Aunque en términos generales, se ha expuesto que lo que permite el funcionamiento de las redes sociales es, por consecuencia, la existencia de Internet, esta red tiene unas proporciones inmensas. Por este motivo, en un principio, se crearon aplicaciones web como Email o WeChat para acotar unas regiones en Internet que estuvieran destinadas a permitir la interacción entre personas, y, más adelante, estas mismas se convirtieron, mediante un avance tecnológico y una sofisticación de los procesos, en las redes sociales que conocemos actualmente (Coffman & Odlyzko, 2001).

Con esta idea, desde inicios del siglo XXI, han ido surgiendo una gran variedad de redes sociales, cada una centrada en algún aspecto o funcionalidad concreta que les permitía destacar sobre el resto, pero la última década, han destacado tres sobre el resto: Facebook, Twitter e Instagram.

No obstante, si bien aportan grandes beneficios sociales a los usuarios que las utilizan, varios pueden hacer uso de las capacidades integradas en estas para llevar a cabo acciones de acoso a otras personas. Y, siendo estas, los principales lugares de interacción entre las personas en el entorno digital, es necesario que se tomen medidas para evitar o impedir, en la medida de lo posible, que se lleven a cabo este tipo de prácticas. De ahí la importancia de esta investigación

La creación de medidas de seguridad en estos entornos no es tarea fácil, ya que quienes dirigen las redes son empresas privadas y no quieren que se vean afectados sus beneficios. Por tanto, para que estas se acaben aplicando y se mantengan en el tiempo deberán cumplir diferentes condiciones como:

-La transacción de libertad por seguridad debe ser “justa”. Algunas medidas de seguridad pueden afectar parcialmente a la libertad de los usuarios. Por este motivo, al momento de aplicar una medida, la empresa deberá pensar si la medida puede afectar a la libertad en un grado aceptable por un “bien mayor” como es la seguridad, o, por el contrario, sería demasiado restrictiva y perderían una parte de los usuarios, ya que, en la actualidad, hay muchas otras redes sociales en el mercado.

-No deben suponer un problema para la utilidad de la red social. Las medidas de seguridad que se decidan implantar de forma voluntaria o por influencia de la normativa legislativa de algún estado con buena posición a nivel mundial, no deben impedir que se utilice la red social para la finalidad con la que se creó.

Esta finalidad puede variar según la red social, como bien se específica en la tabla 1 elaborada en el apartado 2.2.3 del marco teórico del presente trabajo.

-Deben ser aceptadas por la mayoría de los usuarios. Los usuarios son el eje central que hacen posible conseguir los objetivos tanto de las empresas privadas como de los organismos de seguridad. Por este motivo, es necesario contar con su apoyo con el fin de que se pueda implementar correctamente y se obtengan los resultados esperados.

Para ello, es necesario que la empresa exponga las razones por las que han decidido elaborar y aplicar cada medida de seguridad en concreto a través de, no solo una actualización del texto de los “Términos y condiciones de uso” que cada usuario deberá aceptar, sino también mediante un comunicado a través de su cuenta oficial y/o una notificación de alerta a los usuarios en la pantalla principal de la red social la primera vez que accedan desde que se implementó la medida.

El sentido de todas estas acciones es crear una interconexión perceptible por los usuarios entre la empresa que lleva cada red social y ellos, ya que tendrán la sensación de que sus opiniones son relevantes y que participan parcialmente en la decisión de implementar las medidas de seguridad en este entorno. Hecho que generará un mayor grado de comprensión/aceptación entre los usuarios por el bien mayor que corresponde a la seguridad.

-Deben salir acabadas en la versión oficial de la aplicación web. Uno de los grandes problemas actuales que tienen varios tipos de industrias que se dedican al entorno digital, consiste en que, por varias razones no accesibles a través de fuentes OSINT[2], las medidas o los cambios, incluidos los de seguridad, llegan a la versión pública con errores o vulnerabilidades en su código informático.

Este hecho representa un gran problema técnico de seguridad para todos los intervinientes, tanto para la empresa como para los usuarios, ya que, si una medida de seguridad se implementa con una vulnerabilidad y un ciberdelincuente llegara a descubrir y explotar esa vulnerabilidad, tanto los sistemas como la información que está almacenada en estos, que es un activo de alto valor, podrían llegar a quedar comprometidos.

Por este motivo las empresas deberían probar las medidas en un simulador o entorno controlado antes de lanzarlo a la versión pública, ya que elaborar medidas de seguridad que tienen el objetivo de dificultar prácticas como el “cyberstalking” puede ser una forma correcta de incidir sobre el problema de la investigación, pero, si durante el proceso, se crean vulnerabilidades a nivel de código informático que faciliten la materialización de otros ciberdelitos como el robo de información sensible, no sería factible su implementación.

Estas serían todas las condiciones a nivel general que deberían cumplir las medidas de seguridad para que se acabarán instalando en las redes sociales de forma duradera.

2. OSINT. Tipología de fuente de información utilizada en el campo de la investigación/inteligencia para referirse a aquella información disponible/accesible por cualquier persona.

Como se ha podido observar en la tercera condición, el grado de aceptación por parte de los usuarios tiene una gran relevancia a la hora de la verdad. Por ello, para complementar esta idea, he elaborado y distribuido una encuesta en inglés y en formato Google Forms por las tres redes sociales anteriormente expuestas, Facebook, Twitter e Instagram, para conocer la opinión de otros usuarios sobre las medidas que hay actualmente implantadas en estas.

Cabe mencionar, antes de comenzar el análisis de las respuestas recogidas que, los resultados y las conclusiones a las que se lleguen a continuación están afectadas por circunstancias limitantes.

Una de ellas es la existencia de un conjunto de factores que impiden que se pueda demostrar la veracidad y fiabilidad de los datos que se recogen, como pueden ser:

-La elección de un medio como Internet para llevar a cabo la encuesta, que ya trae consigo unos sesgos de veracidad asociados.

-La distribución y alcance de la encuesta, ya que, mayoritariamente, la habrán realizado personas cercanas a mi círculo social.

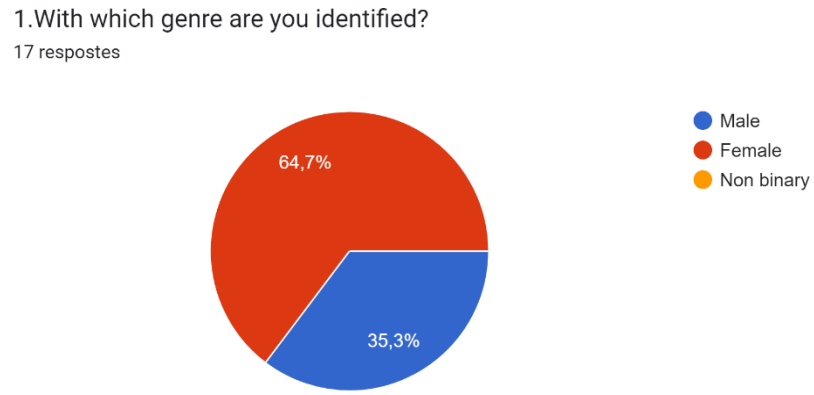
Y, la otra es la capacidad para ejecutar una encuesta a gran escala, ya que trae asociado un coste económico significativo que no poseo actualmente. Por ello, el análisis siguiente se llevará a cabo con el material que se ha podido recoger en vista a un mejor análisis en el futuro con el financiamiento necesario.

Hechas estas aclaraciones, los primeros aspectos que se expondrán son los aspectos generales relativos a esta.

Como primer elemento para tener en cuenta está el género de los usuarios de estas redes sociales que han realizado la encuesta.

El motivo por el cual se ha preguntado este aspecto a los usuarios es debido a la voluntad de buscar una equidad en las respuestas, ya que existe la creencia generalizada de que las mujeres son las víctimas principales de prácticas como el “cyberstalking”, y, añadiendo los diferentes géneros, puede ayudar a contemplar el fenómeno desde varias perspectivas diferentes.

Y tal y como podemos observar, a grandes rasgos, se ha cumplido el objetivo, ya que, de las 17 personas que han realizado la encuesta, un 64,7% de los encuestados se identifican como género femenino y un 35,3% como masculino, estando relativamente cerca de un 50-50.



Gráfica 1. Género de los encuestados.

El segundo elemento relevante para la investigación que se preguntó a los encuestados es la edad.

Existen 2 razones principales por la que se añadió esta pregunta a la encuesta:

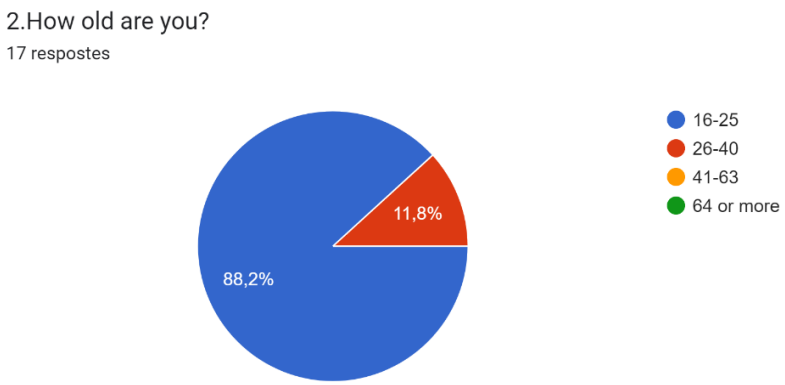
-La primera de ellas reside en una característica que tienen las redes sociales en general, y es que, para que una persona pueda crearse una cuenta en uno de estos entornos de interacción, es necesario tener un correo electrónico y, si vamos al dominio web de creación de correos electrónicos de Google, para crearse una cuenta, es necesario que, o bien la persona tenga una edad igual o superior a 16 años, o bien el menor esté supervisado/tenga el consentimiento de los padres.

-Y la segunda es que, tal y como se ha mencionado en el marco teórico del presente trabajo, el cyberstalking o su terminología está asociada a un tipo de acoso reiterado en el tiempo donde tanto el acosador como la víctima son personas adultas, es decir, mayores de 18 años aquí en España (Ramírez, 2019).

Sin embargo, como con la encuesta se buscaba tener un alcance global, se redujo a 16 años debido a que, en ciertos países del mundo, con 16 años la persona ya es considerada como mayor de edad y Google utiliza esta edad.

Por estos motivos, la encuesta tenía como población objetivo las personas iguales o mayores de 16 años.

En los resultados podemos observar uno de los factores que ya había mencionado anteriormente como posibles inhibidores de la veracidad de la encuesta y es que, mayoritariamente, un 88,2% de los encuestados tienen una edad comprendida entre los 16 y los 25 años, siendo esta delimitación la edad de gran parte de mi círculo social cercano. Mientras que un 11,8% corresponde a personas que tienen entre 26 y 40 años.

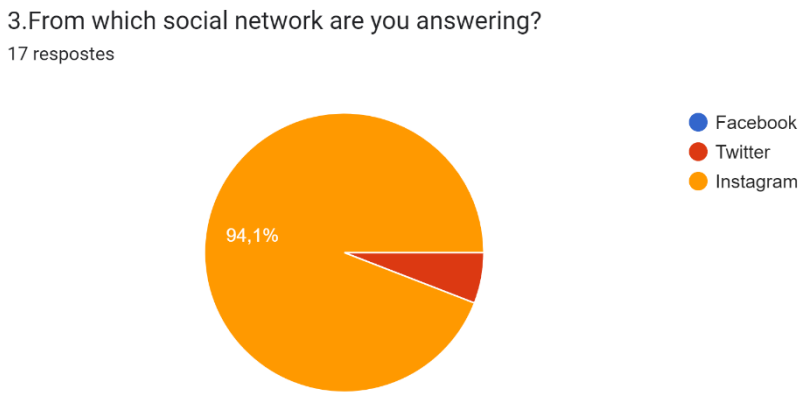


Gráfica 2. Edad de los encuestados.

La tercera pregunta genérica que se preguntó a los encuestados concierne al aspecto relativo a desde qué red social de las tres que se tratan en esta investigación han accedido a la encuesta.

Este aspecto es relevante debido a que, cuantas más respuestas obtengamos de una red social en concreto, más capacidad de análisis tendremos respecto a la situación de seguridad y la efectividad de las medidas de seguridad implantadas en esta.

Como podemos observar en el gráfico 3 un 94,1% de los encuestados han respondido desde Instagram y un 5,9% desde Twitter. Por desgracia, no ha habido ningún usuario de Facebook que la haya realizado, pero aún en esta situación, como se trata de ver las medidas existentes actualmente y proponer nuevas que ayuden a proteger a los usuarios de prácticas como el "cyberstalking", no es un impedimento para el resto del trabajo.



Gráfica 3. Orígenes de las respuestas.

Hasta aquí sería la parte de los aspectos que, en términos generales, se preguntan en encuestas de múltiples vertientes académicas o de investigación para conocer un poco de la persona respetando el anonimato prometido a los encuestados en la descripción de esta.

A continuación, se procederá a analizar las preguntas más específicas del presente estudio y las más importantes para conseguir responder las preguntas de investigación planteadas en este.

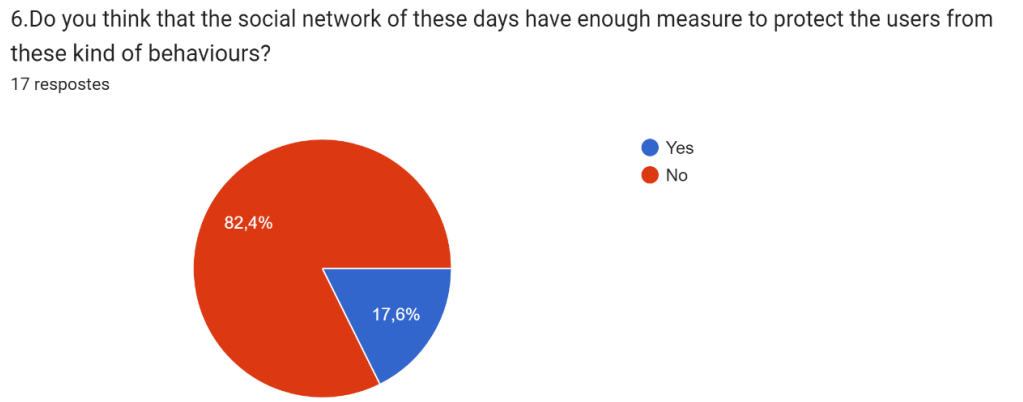
La primera pregunta técnica de la investigación trata de observar el grado de satisfacción de los usuarios de Facebook, Twitter e Instagram sobre las medidas de seguridad implantadas actualmente y si creen que estas son suficientes para hacer frente a la práctica delictiva centrada en esta investigación: el "cyberstalking".

Ya se ha mencionado la importancia de este aspecto a la hora de implementar de forma efectiva y duradera las medidas. Por ello, los resultados de esta pregunta, aunque la encuesta sea interpretativa debido a los sesgos existentes, es de vital importancia para la investigación.

Tal y como podemos observar en el gráfico 4, el pensamiento, a nivel general, concretamente el de un 82,4%, es que, actualmente, las medidas de seguridad implantadas en las redes sociales son ineficaces para protegerse de este tipo de prácticas y es necesario que se apliquen nuevas que sí lo hagan.

Este resultado respalda la idea principal de este trabajo sobre la existencia de una necesidad de hacer cambios en lo establecido en el momento y elaborar nuevas medidas de seguridad que sean eficaces.

Por otro lado, aunque sean la minoría, cabe mencionar que, un 17,6% de los encuestados creen que las medidas implantadas y accesibles para los usuarios son suficientes para protegerse de fenómenos como el “cyberstalking”.



Gráfica 4. Opinión de los encuestados sobre las medidas de seguridad actualmente implantadas en Facebook, Twitter e Instagram.

Para comprender las opiniones de los encuestados que han respondido negativamente en esta pregunta, se han de exponer cuáles son las medidas de seguridad implantadas actualmente. Y estas son las siguientes:

-Opción de restricción de contenido/cuenta. La presente opción, que dota la capacidad de bloquear a una persona por la voluntad del usuario sin que sea necesario argumentar esta acción, constituye una de las medidas más difundidas y ampliamente implantadas en el entorno de las redes sociales.

Esta opción tiene una eficacia "relativa" en una situación de "cyberstalking", ya que, si esta se da mediante el envío reiterado de mensajes públicos o directos, la víctima puede utilizar esta opción para bloquear al acosador y este que no le pueda escribir o no le lleguen sus mensajes.

Más adelante se tratará el motivo por el cuál su utilidad depende es considerada como "relativa".

-Opción de denuncia. Otra medida que tiene como fin proteger a los usuarios y que ha sido implementada en un elevado número de redes sociales consiste en dotar a los usuarios de la capacidad de denunciar o "reportar"[3] a otro usuario de la plataforma social por uno o varios mensajes.

Las tres redes sociales en las que se centra el presente estudio, tal y como se ha expuesto en los apartados 2.2.2, 2.2.3 y 2.2.4, tienen una gran cantidad de usuarios mensuales, hecho que provoca que, diariamente, los sistemas de las redes sociales destinados a este ámbito reciban una cantidad variable de denuncias por parte de los usuarios.

No obstante, tanto los sistemas que reciben y analizan todos los informes de denuncia como los procedimientos en sí, en términos generales, tienden a estar automatizados mediante el uso de la IA.

-Uso de la Inteligencia artificial (IA) como sistema de detección. En la actualidad, muchos aspectos de la sociedad comienzan a complementarse con la IA por múltiples motivos: reducción de la plantilla y, con ello, de la masa salarial, distribución de recursos a otros proyectos de la empresa…, y uno de ellos son las redes sociales.

3.Reportar. Jerga utilizada en el ciberespacio proveniente del verbo inglés "report".

La IA, en estos entornos, tienen unas funciones de detección y análisis de la información que sube a las redes sociales, es decir, por un lado, detectan palabras que se suelen utilizar en prácticas como el “cyberstalking” a partir de una lista predefinida por un/os trabajador/es de la empresa con antelación, y, por otro lado, registran la cantidad de veces que estas se han utilizado para ver si puede haber un componente de reiteración que corresponda a este fenómeno o si es una conversación entre amigos.

Sin embargo, aunque el uso de la IA puede traer beneficios, la automatización de los procesos de análisis pueden conllevar ciertas problemáticas como la falta de “humanidad”, es decir, el grado de avance que tienen las IA actuales no son capaces de discernir unos insultos según el contexto, y eso puede derivar en falsas alarmas de “cyberstalking”.

-Opción para silenciar a un cierto usuario o palabras clave. Otra opción que también tiene una eficacia “relativa” contra prácticas como el “”cyberstalking” es la que consiste en silenciar los mensajes de un cierto usuario o ciertas palabras que el usuario considere como ofensivas.

-Opción de solo poder mandar mensajes directos (MD) a seguidores de tu cuenta. El sistema de solo poder hablar en privado con usuarios que te siguen, no con los que el acosador sigue, es de los mecanismos más eficaces para dificultar el “cyberstalking”, pero, por motivos desconocidos, está poco extendido entre las redes sociales. Tal y como se ve en la tabla 3, de las tres redes sociales que se tratan en esta investigación, solo Twitter la tiene implantada.

Esta consiste en que, para que un usuario “A” pueda mandar un mensaje directo por un chat privado a un usuario “B”, el usuario “B” debe seguir al “A”.

Si la situación anterior la extrapolamos al campo de estudio de la presente investigación, podemos observar que, para que el "cyberstalker" haga contacto con la víctima y la acose por medio de chats privados/mensajes directos, la víctima tendrá que seguir al acosador, cosa que es muy complicado que suceda a menos que esté llevando a cabo un método de "follow-back"[4]. Por este motivo, aunque no sea una opción infalible, es bastante eficaz para impedir este tipo de prácticas.

-Vincular un número de teléfono a una cuenta. La presente opción, que consiste en preguntar al usuario su número de teléfono para que lo asocie a su cuenta de la red social en cuestión, es una medida de seguridad cuya función/finalidad es la de disuadir al acosador, ya que, si se le obliga a asociar su número, estará parcialmente identificado.

Sin embargo, las tres redes sociales no exigen que se vincule un número de teléfono a cada cuenta, sino que es algo opcional y dan la alternativa de asociar una dirección de correo electrónico.

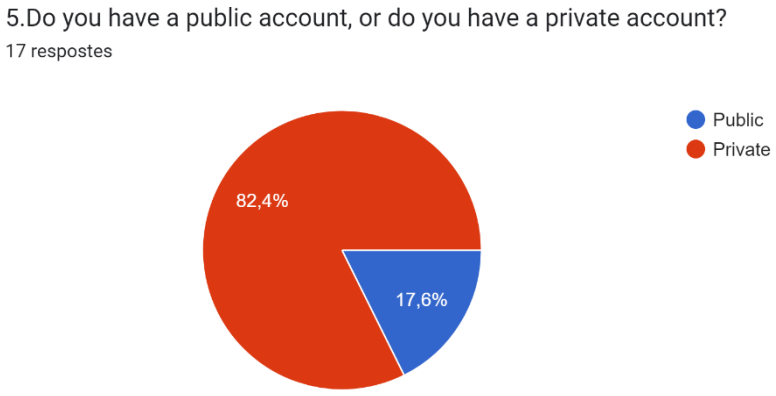
-Opción de privacidad. Como última opción está la que aporta a los usuarios la capacidad de configurar sus cuentas, que, de forma predeterminada están "públicas", como privadas.

La presente opción fue diseñada por las empresas para dar a la posibilidad de dotar de más privacidad y proteger mejor la información del usuario que está expuesta en las redes sociales, y a su vez, su integridad.

No obstante, esta opción, aunque aporta aspectos como el hecho de que los usuarios no puedan ver las fotografías ubicadas en el perfil de otro usuario, en el caso de Instagram, o no puedan reaccionar a sus comentarios, como pasa en Twitter, no es una opción obligatoria y solo se puede activar si el usuario así lo desea.

4. Follow-back. Técnica social utilizada en algunas redes sociales consistente en seguir a personas desconocidas con el fin de que le devuelvan el gesto y le sigan para subir su número de seguidores.

Como podemos observar en el gráfico 5 de la encuesta que trata sobre el grado de cumplimiento/uso de la medida relativa a la privacidad, de los 17 encuestados, el 82,4% tienen su cuenta en privada, pero el 17,6% sigue teniéndola pública, con los problemas de seguridad que eso conlleva y con la posibilidad de llegar a ser víctima de fenómenos como el “cyberstaking”.



Gráfica 5. Configuración de privacidad de los encuestados.

Los motivos pueden ser muy variados, algunos a destacar son los siguientes:

-Moda/movimiento “influencer”[5]. En las últimas décadas, con el surgimiento de las redes sociales, una parte de la población mundial invirtió en lo que podían ofrecer las nuevas tecnologías y empezaron a hacer contenido de entretenimiento. Con el tiempo, empezaron a tener más seguidores/números y a obtener financiación de otras empresas, lo conocido como “sponsors”[6], y, con ello, vieron que podrían vivir de esto.

A partir de ese momento, muchas personas, aún en la actualidad, piensan que se podrán ganar la vida de este modo, pero la verdad es que solo un porcentaje muy reducido lo consigue, como pasa en el mundo de la música.

5. Influencer. Persona famosa por el contenido que crea en las redes sociales con capacidad para movilizar a un gran número de personas.
6. Sponsor. Empresa del mismo sector o de un sector diferente que remunera a una persona con un número de seguidores aceptable por la empresa para que publicite su marca en los contenidos que elabore.

El problema recae en que, para poder ser famoso/a y poder vivir de ello, se olvidan de la seguridad y solo les importan los números y que su contenido tenga el máximo alcance posible, y, para ello, es necesario tener una cuenta pública, provocando que compartan mucha información privada, un elemento clave para poder llevar a cabo el "cyberstalking".

-Pasotismo/Indiferencia. El motivo actual no suele representar un problema de seguridad para el usuario, ya que suele darse en personas que no utilizan las redes sociales para compartir información personal ni ganar seguidores, simplemente hacen uso de las redes sociales para estar "conectados" con lo que está pasando en el mundo y con su círculo social cercano, y visualizar "memes"[7].

Por ello, a este tipo de usuario le es indiferente tener su cuenta en pública o en privada, porque prácticamente no hay información sobre él que puedan recoger los potenciales acosadores.

-Falsa sensación de seguridad. En algunas ocasiones, los usuarios observan por algún medio de comunicación que otro usuario ha sufrido "cyberstalking", pero tienen la convicción de que no les pasará a ellos. Esta mentalidad del "no me pasará a m" supone un problema para la seguridad del usuario.

-Por el trabajo o los estudios. Otro motivo factible podría consistir en que un usuario lo deba tener público por contrato porque representa la imagen pública de una empresa o que temporalmente lo deba tener para llevar a cabo algún proyecto académico o laboral, como ha sido el caso de esta investigación para que pudiera ser accesible para cualquier persona de las tres redes sociales en cuestión.

7. Memes. Nomenclatura utilizada para referirse al contenido audiovisual distorsionado con fines caricaturescos. RAE. <https://dle.rae.es/meme>

Las anteriormente expuestas representan las opciones más generales que deberían tener todas las redes sociales, aunque se pueda observar en la tabla 3 que no es así.

	Facebook	Twitter	Instagram
Opción de restricción de contenido/cuenta	✓	✓	✓
Opción de denuncia	✓	✓	✓
Uso de IA-Detección	✓	✓	✓
Opción de silenciar palabras o cuentas	✓	✓	✓
Opción de solo poder mandar mensajes privados a seguidores	✗	✓	✗
Asignación de número de teléfono a una cuenta	✓	✓	✓
Opción de privacidad -configuración de cuenta a privada	✓	✓	✓
✓ Lo tienen implantado. ✗ No lo tienen implantado			

Tabla 3. Elaboración propia

Con esto, se finalizaría la exposición de la opinión sobre las medidas de seguridad que hay implantadas en las Facebook, Twitter e Instagram que se ha podido reflejar, de manera interpretativa, en la encuesta.

Sin embargo, se puede observar que, aunque en la actualidad hay una gran variedad de medidas que buscan proteger a los usuarios de prácticas como el “cyberstalking”, aún hay espacio para mejorar.

Por ello, a continuación, se plantearán qué aspectos deberán tratarse en futuras medidas de seguridad que se implanten en las redes sociales para mejorar la protección de los usuarios a este tipo de prácticas:

-Reducir el anonimato. Como ya se ha mencionado en el apartado 2.1.3 de la presente investigación este conforma una de las características que aporta Internet de forma predeterminada, pero, a su vez, por los problemas de identificación que están asociadas a este aspecto, representa un aspecto que hay que reducirla teniendo en cuenta el debate libertad-seguridad.

Para ello, una de las posibles opciones que se podrían plantear es la de obligar a los usuarios a vincular un número de teléfono a su cuenta y exigirlo cada vez que acceda a esta.

Anteriormente se ha expuesto que las redes sociales tienen la opción de que los usuarios puedan vincular sus cuentas a un correo electrónico o a un número de teléfono.

El problema reside en que, para crear un correo electrónico, no es necesario poner ninguna información real de la persona que está detrás de la pantalla, por lo tanto, es una opción ineficaz para disuadir a los acosadores, debido a que no facilitará su identificación.

En cambio, si las empresas que llevan estas tres redes sociales exigieran a los usuarios asignar un número de teléfono a sus cuentas, sí que tendría un efecto disuasorio, ya que, en el caso que haya una actuación considerada como delictiva, las autoridades podrían pedir a la empresa de la red social el número del acosador y, posteriormente, contactar con las compañías del proveedor de servicios de telefonía móvil para pedir los datos de ese número.

A su vez, siguiendo con esta opción, sería muy práctico para identificar a los “cyberstalkers” que hacen uso de herramientas o redes especializadas en el anonimato como la red TOR[8], que:

> -Cada vez que el usuario quiera acceder a su cuenta desde un nuevo dispositivo deba identificarse con su número de teléfono.
>
> -Y poner un temporizador de inactividad, para que, si el usuario quiere acceder a un dispositivo ya registrado en los sistemas de la red social, también deba ir poniendo su número de teléfono periódicamente.

Ambas tienen la finalidad de establecer un “control de acceso” para poder tener identificado al usuario en todo momento y desde cualquier dispositivo.

Y, la otra posible opción consiste en cambiar el número de teléfono por el número de identificación del estado en cuestión, como el DNI en el caso del estado español, en todas las situaciones anteriormente planteadas, aunque, para llevar esto a cabo, se tendría que realizar una colaboración público-privada con todos los Estados donde está disponible la red social en cuestión con el fin de cumplir con las políticas de privacidad y sería muy complejo (González, 2015).

- Prohibir las multicuentas o la creación de cuentas secundarias. Una gran problemática que provoca que algunas medidas de seguridad como la opción de restricción/bloqueo de cuentas sean “relativamente eficaces” es que, si un usuario/a es acosado/a y bloquea al acosador, este, siempre y cuando el usuario tenga más de un correo electrónico y no haya un sistema como el de solo poder mandar mensajes privados a seguidores, podrá hacerse otra cuenta para evadir este bloqueo y seguir acosando a la víctima desde otra cuenta.

8.Red TOR. Es una red de routers voluntarios que encaminan el tráfico de datos de una manera en específico, habilitando anonimato al usuario y confidencialidad a la información que se transmite por esta.

La solución para que no se den este tipo de “maniobras de evasión” es implantar la otra medida anteriormente expuesta y programar las cuentas de tal manera que solo se pueda asociar un número de teléfono a una cuenta.

-Extender la medida de seguridad de solo poder mandar mensajes directos (MD) a los seguidores implantada en Twitter, Facebook e Instagram para dificultar que el “cyberstalker” pueda actuar.

-Llevar a cabo campañas de concienciación destinadas a todos los usuarios para que vean los peligros asociados a tener cuentas públicas.

Con estas medidas, se podría proteger mejor la integridad de los usuarios de estas redes sociales ante prácticas como el “cyberstalking”.

No obstante, no todo recae en el papel que juegan las empresas que llevan las redes sociales, sino que los usuarios también jugamos un papel importante a la hora de configurar nuestras cuentas para tener estas medidas de seguridad activadas, en el caso que no lo estén de forma predeterminada.

Y, por último, cabe aclarar que las medidas expuestas pueden ser útiles si se implantan en la actualidad, pero, al ser un ámbito que está en constante evolución, es necesario que se vayan actualizándolas periódicamente, ya que, el fin último siempre debe ser la protección/seguridad de los usuarios.

7 – Conclusiones

Con ello, llegaríamos al tramo final de la presente investigación sobre el “cyberstalking” en las redes sociales descritas.

A lo largo del trabajo se ha expuesto la situación que existe en la actualidad entorno a esta práctica de forma pragmática para que se pudiera percibir que, a causa de los avances constantes de la humanidad, era necesario una redefinición de las figuras que ostentan los papeles principales de las sociedades y de las formas en la que estas se relacionan.

A su vez, también se ha enfatizado a partir de la materialización del “cyberstalking”, que el producto de esta redefinición debía contemplar obligatoriamente el espectro tecnológico, no solo el sociopolítico, debido a su creciente importancia en todos los ámbitos de la sociedad y, sobre todo, en el peligro que puede llegar a suponer para la seguridad/integridad de las personas.

Para ello, es esencial definir de forma clara qué se cataloga como “conducta aceptable” y “conducta inaceptable”, aspecto que las normativas cada vez más están tratando de normativizar, y, aún más importante, que diferencia una práctica como el “cyberstalking” de otras similares, como el “cyberbullying”.

Esta ha sido otra materia que se ha tratado en la primera parte de la investigación, pero, debido a la dificultad que traen asociados todos estos elementos novedosos, no existe una diferencia clara.

En el presente trabajo se ha optado por la aproximación relativa a 2 variables: la edad de la víctima y si existe un componente de repetición o no, definiendo así el “cyberstalking” como “un fenómeno conductual constitutivo de delito que utiliza el uso de las TIC y las características técnicas que estas aportan, como el anonimato o la facilidad de difusión de información, para monitorizar y acosar intencionadamente a una persona o grupo de personas adultas, conocidas o desconocidas, de forma reiterada en el tiempo, produciendo como resultado un efecto psicológico adverso y una alteración en la vida cotidiana de la/s víctima/s”.

Asimismo, en la última parte, a partir de las medidas de seguridad que tienen implantadas Facebook, Twitter e Instagram y de la opinión de algunos usuarios que realizaron la encuesta, que sería más representativa con la financiación económica adecuada, se han propuesto unas posibles medidas para dificultar que se lleven a cabo y, por consecuencia, para proteger mejor a los usuarios antes estas prácticas.

No obstante, estas medidas propuestas son óptimas para conseguir este fin en la situación actual, ya que, como se ha mencionado durante el trabajo, la tecnología avanza constantemente y, con ello, van surgiendo nuevas maneras de evadir las medidas de seguridad establecidas. Por este motivo, siempre es necesario actualizarse constantemente para adaptarse a la realidad de cada momento.

8 – Bibliografía

Bauman, Z. (2022). *Modernidad Líquida.* Editorial. Fondo de cultura económica de España. 232 p. (Primera edición lanzada en el 20 de octubre de 2003). [Tapa blanda, en castellano] ISBN: 9789505575138.

Beck, U. (2006, 1 de mayo). *La sociedad del riesgo: Hacia una nueva modernidad* (Navarro, J., Jiménez, D. y Borrás, M. R. Ed.). Republicado por Editorial Paidós Iberica. 400 p. (Obra original publicada por la editorial Suhrkamp en 1986) [Tapa blanda, en castellano] ISBN: 9788449318924.

Falcón, J. A. C. (2011, 24 de febrero). Twitter. Marketing personal y profesional. RC Libros. 76 p. [Tapa blanda, en castellano]. ISBN: 9788493831226.

González, J. G. (2010). *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet.* Tirant lo Blanc, Valencia. 220 p. [Idioma: español]. ISBN: 9788498768350.

Hobbes, T. (2003, 20 de octubre). *Leviatán* (Escohotado, A. Ed.). Editorial Losada. 570 p. (Obra original datada del 1651). [Tapa blanda, en castellano]. ISBN: 9789500392532.

Locke, J. (1988, 28 de octubre). *Locke: Two Treatises of Government.* (Laslett, P. Ed.). Editorial Cambidge University Press; Edición estudiante. 176 p. (Obra original datada del 1689). [Idioma: inglés]. ISBN: 1453857710

Mill, J. S. (2008, 22 de septiembre). *Sobre la libertad.* (Braun, C. R. Ed.). Editorial Tecnos. 272 p. (Obra original datada del 1859). [Tapa dura, en castellano]. ISBN: 9788430947058.

Nye, J. (2006, 18 de abril). *Soft power: the means to success in the world politics*. (2005 Ed.). Editorial Public Affairs. 208 p. [Tapa blanda, en inglés]. ISBN: 9781586483067.

Spencer, H. (1820-1903). *Estática Social.* Editorial INNISFREE. 1 MAR 2017, 446 p. [En Castellano]. ISBN: 9781005692438 | ISBN-10: 1005692432.

Weber, M (1993, 1 de enero). *Economía y sociedad*. Editorial: Fondo de cultura económica de España. Madrid, 1993. 1246 p. [Tapa Blanda, en Castellano]. ISBN: 9788437503745.

9 – Webgrafía

Andreu, A. S. (2009, junio). *Declaración Universal de derechos humanos emergentes.* Institut de Drets Humans de Catalunya. Primera edición. <https://www.idhc.org/arxius/recerca/1416309302-DUDHE.pdf>.

Bocij, Paul & McFarlane, L.. (2002). Online harassment: Towards a definition of cyberstalking. Prison Service Journal. 139. 31-38. <https://www.researchgate.net/publication/284807346_Online_harassment_Towards_a_definition_of_cyberstalking>.

Brügger, N. (2015, 4 de mayo). *A brief history of Facebook as a media text: The development o fan empty structure.* First Monday, Volumen 20, Número 5. <http://dx.doi.org/10.5210/fm.v20i5.5423>.

Coffman, K. G. & Odlyzko, A. M. (2001, 6 de julio). *Growth of the Internet*. AT&T Labs. Version preliminar. <https://www-users.cse.umn.edu/~odlyzko/doc/oft.internet.growth.pdf>.

Collins (2023). *Cyberstalking.* Diccionario Collins. <https://www.collinsdictionary.com/es/diccionario/ingles/cyberstalking>.

Cornejo, M., & Tapia, M. L. (2011). *Redes sociales y relaciones interpersonales en internet.* Fundamentos en Humanidades, XII(24), 219-229. <https://www.redalyc.org/articulo.oa?id=18426920010>.

Danah m. boyd & Nicole B. Ellison (2007, 1 de octubre*). Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication*. Volumen 13, pág. 210–230. <https://doi.org/10.1111/j.1083-6101.2007.00393.x>.

Díaz, J. R. (2016, 19 de agosto). *Ciberamenazas: ¿el terrorismo del futuro?* Instituto Español de Estudios Estratégicos. Documento de opinión 86/2016.

Elizabeth E., Edward D., Robin K., Carolyn A. L., Katalin P. (2017, 1 de noviembre) *Defining Cyberbullying.* Pediatrics. 140 (Supplemento_2). < https://publications-aap-org.sire.ub.edu/pediatrics/article/140/Supplement_2/S148/34183/Defining-Cyberbullying>.

Fernández, R. (2023, 25 de mayo). *Ranking mundial de redes sociales por número de usuarios en 2023.* Statista. <https://es.statista.com/estadisticas/600712/ranking-mundial-de-redes-sociales-por-numero-de-usuarios/>.

Ginner, C. A. & Delgado, J. J. (2017, 16 de octubre). *Consideraciones criminológicas sobre el perfil del stalker y el acecho mediante ciberstalking*. Estudios en Seguridad y Defensa, 12(24), 19-35. <https://esdegrevistas.edu.co/index.php/resd/article/view/250/353>.

González, J. G. (2015, octubre). *Oportunidad criminal, internet y redes sociales*. Revista para el análisis del derecho InDret. Universidad CEU. <https://indret.com/wp-content/themes/indret/pdf/1172.pdf>.

Lawrence Erlbaum Associates, Inc. (2014, 4 de febrero) (Kiesler, S. Ed.) *Culture of Internet*. Google books (Primera publicación datada del 1997) < https://www.google.es/books/edition/Culture_of_the_Internet/bJvKAgAAQBAJ?hl=ca&gbpv=0>.

Llinares, F. M. (2013, junio). *Derecho penal, cyberbullying y otras formas de acoso (no sexual) en el ciberespacio.* Revista de Internet, Derecho y Política. UOC. <https://dialnet.unirioja.es/servlet/articulo?codigo=4477372>.

López, E. V. (2019, 4 de enero). *Las ventajas y desventajas del internet en la sociedad*. Conciencia Digital. <https://doi.org/10.33262/concienciadigital.v2i1.928>.

Martí, F. P. (2005). *Libertad y seguridad en un nuevo contrato social.* Anuario de filosofía de derecho págs. 83-112. Universidad Autónoma de Barcelona. <https://dialnet.unirioja.es/servlet/articulo?codigo=2220953>.

Mattern, J. (2017). *Instagram.* Abdo Publishing. Google books <https://books.google.es/books?hl=ca&lr=&id=0BvPDAAAQBAJ&oi=fnd&pg=PP1&dq=instagram+history&ots=Ay3PlNlNJv&sig=I0byEbr0PY5Tqc17jCvcDfmxlds&redir_esc=y#v=onepage&q&f=false>.

Medina, A. C. (2003, julio). *Una nueva cara de Internet: el acoso.* Etic@ net: Revista científica electrónica de Educación y Comunicación en la Sociedad del Conocimiento. Universidad de Granada. ISSN: 1695-324X.

Meta (2023). Página oficial de la compañía propietaria de Facebook. <https://about.meta.com/company-info/>.

Ovidio, R., S.M., Doyle, J. (2003). *A Study on Cyberstalking. Understanding Investigative Hurdles.* Heinonline. 72 FBI L. Enforcement Bull. 10. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/fbileb72&div=20&id=&page=>.

Ramírez, V. (2019, 22 de febrero). *Las diferencias clave entre Ciberacoso, Cyberbullying y el Grooming.* Cyberpedia. <https://cybersecuritynews.es/las-diferencias-clave-entre-el-ciberacoso-cyberbullying-y-grooming/>.

Reno, J. Attorney General of the United States, et al., Appellants v. AMERICAN CIVIL LIBERTIES UNION et al. (1997, 26 d junio). *Sentencia 521 U.S. 844.* Tribunal Supremo de los Estados Unidos. <https://www.law.cornell.edu/supremecourt/text/521/844>.

Rupérez, H. A. (2023). *Artículo 172 ter del Código Penal.* Mundo Penal. <https://mundopenal.es/codigo-penal/articulo-172-ter/>.

Sánchez, M. T. M. (2016, 29 de noviembre). *Incidencia de la última reforma del Código Penal por LO 1/2015, de 30 de marzo, en materia de violencia de género. Especial referencia a la agravante de género y a los nuevos delitos de stalking y sexting.* ELDERECHO.COM. <https://elderecho.com/incidencia-de-la-ultima-reforma-del-codigo-penal-por-lo-12015-de-30-de-marzo-en-materia-de-violencia-de-genero-especial-referencia-a-la-agravante-de-genero-y-a-los-nuevos-delitos-de-stalking-y-sex>.

Shouse Law Group, A.P.C. (2023). *California Cyberstalking Laws.* Criminal Defense Division. <https://www.shouselaw.com/ca/defense/laws/cyberstalking/>.

Twitter (2023). Página oficial de la red social. <https://about.twitter.com/es>.