Universidad Internacional de La Rioja
Escuela Superior de Ingeniería y Tecnología

Máster Universitario en Seguridad Informática

Recolección y admisión de evidencias en redes sociales

Trabajo fin de estudio presentado por:	Jesús Sánchez de Lechina Tejada
Tipo de trabajo:	Desarrollo de metodologías
Director/a:	Juan José Delgado Sotes
Fecha:	21/07/2022

Resumen

La delincuencia ha avanzado a la par que la tecnología. Hoy en día, uno de los escenarios del crimen más frecuentes son las redes sociales, y es un problema el desafío tecnológico que presenta a nivel forense la obtención de evidencias en estos entornos emergentes que sufren cambios continuos, pero también un desafío social la infravaloración del riesgo que entrañan este tipo de redes debido a la mala percepción de un entorno aparentemente inocuo, pero potencialmente hostil.

Para facilitar el análisis forense que sigue a este tipo de ciberdelitos, se propone una metodología cuyo objetivo es asegurarse la máxima calidad y veracidad de las evidencias a recabar de manera que sean admisibles en un litigio a la vez que se optimiza el tiempo de investigación.

Palabras clave: Redes sociales, peritaje, forense, delitos informáticos, evidencias.

Abstract

Crime has evolved hand in hand with technology. Nowadays, one of the most frequent crime scenes are social networks. These kinds of networks hold two major challenges: A technological one, where everchanging and emerging networks complicate their forensic analysis; and a social one, in which society is not able to perceive the hazards these apparently unharmful scenarios might imply.

In order to ease the forensic investigation that follows this kind of cybercrime, a new methodology is suggested with the goal of accelerating forensic processes while, simultaneously, obtaining the best results in terms of quality and authenticity, which are requirements for evidence to be accepted in a trial.

Keywords: Social networks, forensics, cybercrime, evidence.

Índice de contenidos

Índice de figuras

1. Introducción

En este trabajo se desarrollará una metodología para la recolección eficaz y eficiente de evidencias provenientes de redes sociales y servicios de mensajería de manera que tengan la validez y rigurosidad necesarias para ser admitidas en un litigio.

1.1. Motivación

La delincuencia ha evolucionado siempre de la mano de la tecnología y los escenarios de crímenes tradicionales han seguido este curso. Uno de los nuevos marcos que se presentan son las redes sociales, donde, entre usuarios legítimos, se encuentran individuos que aprovechan las posibilidades de interacción que estas redes ofrecen para perpetrar una amplia gama de delitos.

La justicia, por su parte, ha de estar al día con este nuevo medio de comisión de delitos con la dificultad técnica intrínseca que aporta la informática a este tipo de casos. La evidencia en las redes sociales adquiere una capa de complejidad que la justicia aún está en proceso de asimilar.

Un ejemplo de esto ocurrió en el Tribunal Supremo de Georgia, Estados Unidos, en enero de 2017. Ramel Brown fue acusado de asesinato y pertenencia a bandas criminales en instancias judiciales inferiores en base a evidencias clave que incluían unas capturas de pantalla recortadas de diversas redes sociales. El acusado apeló al Tribunal Supremo y este anuló la sentencia librándose de los cargos de pertenencia a banda criminal basándose en la falta de medios que soportaran la autenticidad de esa evidencia clave (*Brown v. State*, 2017).

Ese mismo mes, en Estados Unidos más de 1200 casos públicamente accesibles involucraron de algún modo las redes sociales. Entre estos procesos se pueden encontrar más ejemplos donde se puede apreciar la relevancia de las pruebas en estas redes: Evidencias adquiridas con malas prácticas, publicaciones que indicaban que se excedieron los plazos para presentar reclamaciones o calumnias que fueron desestimadas por su naturaleza subjetiva hiperbólica son meros ejemplos de que las redes sociales están a la orden del día en el ámbito judicial (Patzakis & Carpenter, 2017).

El problema que se vislumbra aquí es que un hecho que se pretende probar puede ser rechazado por la justicia por la ausencia de rigurosidad y seguimiento de metodologías que

garanticen que el hecho sea demostrado de manera fehaciente. Esta respuesta, además, debe realizarse en un tiempo inferior a los plazos de caducidad que puedan estar asociados a las acciones legales correspondientes.

Esta situación tiene su origen en un conjunto de factores:

En primer lugar, el desconocimiento por la parte que pretende probar un hecho relativo a una red social sin un asesoramiento experto puede llevar a infravalorar la complejidad de los procesos necesarios para demostrar la autenticidad en las redes sociales. Por supuesto, un segundo puede ser una mala praxis de mano de estas entidades (como abogados o peritos) que han de asesorar a una de las partes o la ausencia de una metodología eficiente a seguir pueden influir en el proceso. Adicionalmente, más allá del ámbito de este trabajo, el continuo devenir de las redes sociales, medios de comunicación y nuevas tecnologías influyen en que sea complicado uniformizar el criterio de admisibilidad a lo largo de las diferentes instancias judiciales.

En honor a la justicia, ningún delincuente debería quedar impune de sus delitos, y ningún inocente debería ser condenado por delitos que no cometió. Por esto, es necesario proporcionar unas herramientas que simplifiquen el proceso de recolección de evidencias en redes sociales y sistemas de mensajería para que sean admisibles como pruebas concluyentes de manera ágil y eficaz.

1.2. Planteamiento del trabajo

Ante la vorágine de redes sociales que se popularizan hoy en día, se propone una metodología que aglutine las redes sociales en cuanto a su tipología y ofrezca un flujo de actuación en las diferentes categorías de delitos que se analicen.

Si se dispusiera de un procedimiento para catalogar un hipotético delito y actuar con las herramientas adecuadas y compatibles con cada una de las redes sociales más usadas en la actualidad, se podría llevar a cabo la adquisición de evidencias con garantías de autenticidad y rapidez, dando respuesta a los problemas que han servido para motivar esta investigación.

Este desarrollo implicaría una mejora en la calidad de procesos judiciales en este tipo de casos desde las primeras instancias, pues una inequívoca presentación de pruebas supondría que los fallos que se pronuncien en base a estas evidencias serán irrevocables en cualquier recurso que se quisiera presentar. Lo cual podría incluso llegar a aliviar la presión en el sistema judicial.

Por supuesto, esta metodología también mejoraría los procesos de investigación periciales en el contexto de los quebrantamientos de la ley en redes sociales, mejorando la calidad de las evidencias y reduciendo los tiempos de trabajo.

1.3. Estructura del trabajo

Tras esta introducción, se explicarán a continuación los temas que se abordarán en los sucesivos capítulos:

En el segundo capítulo se hará una revisión sobre el estado del arte de esta casuística. Un repaso a las principales recomendaciones que existen hoy en día acerca de las adquisiciones de pruebas en redes sociales analizando las carencias que puedan tener y examinando con perspectiva la aportación de todas ellas en conjunto para comenzar a trazar el esquema de una metodología que parta del conocimiento existente para abordar estos mismos problemas.

En el tercer capítulo se presentan los objetivos generales y específicos del proyecto, así como una descripción de la metodología de trabajo que se empleará durante la elaboración de este trabajo.

En el capítulo cuarto, se presentará un estudio de los delitos más frecuentes cometidos que involucren de algún modo a las redes sociales. También se realizará otro estudio de las redes sociales más populares, estableciendo una categorización de delitos y redes sociales en tanto a la naturaleza de los delitos y sus vías de investigación en redes sociales determinadas. Esto servirá de base para identificar los requisitos a los que deberá hacer frente la metodología.

Respecto al quinto capítulo, en esta sección se hará una descripción detallada de la metodología, estableciendo un punto de partida y estableciendo en cada paso las posibilidades de actuación, clarificando los procedimientos en cada uno de los casos y redes sociales posibles hasta llegar a la elaboración de un informe final.

En el sexto capítulo, se realizará una evaluación de esta metodología, estudiando su desempeño en comparación con casos conocidos y analizando cuáles han sido los beneficios obtenidos de la aplicación de esta metodología. Adicionalmente, se presenta un modelo de entrevista con el fin de hacer uso de conocimiento experto para validar esta metodología.

Finalmente, el trabajo se cerrará con una conclusión en el séptimo capítulo poniendo en perspectiva los resultados e indicando la vía que se abre para trabajos futuros.

2. Estado del arte

2.1. Peritaje en la actualidad

Hoy en día existen metodologías y estándares para la recolección de evidencias digitales, siendo una de las más relevantes la normativa ISO/IEC 27037, que propone unas líneas de partida en el manejo de las evidencias digitales en tanto a identificación, recolección, adquisición y preservación en los casos de dispositivos de almacenamiento, sistemas de navegación móviles, videocámaras, redes y otros con propiedades similares (ISO, 2012).

Otra norma que es relevante en el peritaje es la norma UNE 197010, sobre la elaboración de informes periciales, pues toda prueba incriminatoria ha de ser debidamente presentada. De este modo, cualquier metodología que se desarrolle en el ámbito del peritaje y las redes sociales, debe partir de una referencia como esta para el tramo inmediatamente posterior a la fase de investigación (AENOR, 2015).

La trascendencia de estas normas se aprecia de manera sencilla en las metodologías forenses que se han ido elaborando a posteriori. Por ejemplo, en el boletín de abogados de Estados Unidos, se define la metodología forense en ordenadores como un conjunto de pasos que comienza con la preparación y extracción de información para proceder con la identificación de evidencias para descartar la información irrelevante y clasificar la información útil de cara al análisis, su última etapa, donde se recopilan los hallazgos junto con las conclusiones (Carroll et al., 2008).

2.2. Peritaje en redes sociales

Sin embargo, en relación al tema de las redes sociales las metodologías no se encuentran tan desarrolladas como para el caso del análisis forense en general. En 2014, Keil Hubert, en el seno del *SANS Institute,* publicó un artículo sobre cómo la evidencia en computadores puede llegar a resolver o destruir un caso. Dada esta relevancia, propone unas recomendaciones básicas sobre buenas prácticas a la hora de identificar, recolectar, adquirir y preservar evidencias (Hubert, 2014). En otro artículo más reciente se otorga esta misma importancia a las evidencias en redes sociales y se ofrecen mecanismos de automatización de su adquisición (Arshad et al., 2022).

En ámbitos más transversales encontramos estudios acerca del estado del arte del análisis forense en *cloud* (Almulla et al., 2014), el marco de trabajo del que disponen las organizaciones para este mismo medio (Alenezi et al., 2019) y la adquisición de evidencias en dispositivos móviles (Aji et al., 2020).

En conjunto, estos estudios dejan ver la relevancia de la identificación, recolección, adquisición y preservación de evidencias que todo proceso que involucre evidencias digitales deberá de abordar, así como también muestra la magnitud de este problema y cómo pueden ser necesarias profundas investigaciones para indagar en evidencias situadas en dispositivos o medios concretos.

La mira de este trabajo se encuentra en el espacio que queda entre unas recomendaciones básicas para la adquisición de evidencias, buscando unas indicaciones más adecuadas para cada caso, y la aplicación generalista de una metodología al mayor número de supuestos posibles.

2.3. Delitos en redes sociales

La delincuencia ha sido siempre un problema de la sociedad. Con el paso del tiempo y los avances de tecnología, la delincuencia ha evolucionado a su par. Con la cerradura se creó la ganzúa, con el dinero *fiat* (basado en la promesa de pago, introduciendo los primeros billetes), las falsificaciones, y con los ordenadores e internet, los ciberdelitos. Los delitos en las redes sociales son una rama de estos que se particularizan por tener un componente fuerte de apoyo en las redes sociales para la comisión del hecho delictivo.

Aquí se presenta un estudio de los delitos más frecuentes cometidos que involucraran de algún modo a las redes sociales. Más adelante, se realizará otro estudio de las redes sociales más populares, estableciendo una categorización de delitos y redes sociales en tanto a la naturaleza de los delitos y sus vías de investigación en redes sociales determinadas. Esto servirá de base para identificar los requisitos a los que deberá hacer frente la metodología que desarrollemos a posteriori.

- **Delitos de odio**: Las manifestaciones de opiniones en la red pueden llegar a polarizarse y llegar al punto en el que se incite al odio y la violencia de determinados grupos en situación de discriminación. Cuando la libertad de expresión garantizada en la

Constitución Española sobrepasa los límites del odio, entra en acción el artículo 510 del Código Penal para garantizar el bienestar (Marabel Matos, 2021).

- **Estafa y fraude**: Destacando redes como Twitter y Facebook, donde es frecuente que los usuarios no hayan restringido la interacción a una «red privada» de conocidos y se encuentren millones de usuarios expuestos de manera sencilla. Además, es frecuente que los usuarios se agrupen en cuanto a intereses y localización, lo que facilita la elaboración de *phishing* con una capa adicional de sofisticación (UNODC, 2013, p.9).
- **Difamación y calumnias**: Atentar contra el honor, reputación o imagen de una persona faltando a la verdad con conocimiento de la misma es delito, pues en una sociedad en la que la viralización de las «*fake news»* están a la orden del día, se puede causar un perjuicio en una persona inocente (UNODC, 2013, p.36).
- **Infracción de copyright** (UNODC, p.36): Todas las creaciones del intelecto humano están protegidos por sus derechos de autor. Frecuentemente los derechos de explotación de esta creación están limitados y no pueden ser accedidos, usados o distribuidos entre otros, por tanto, la vulneración de estos derechos supone un delito. Son frecuentes las páginas de enlaces y el *peer-to-peer*, pero en redes sociales y servicios de mensajería es frecuente encontrar grupos donde se distribuye este material o el acceso al mismo.
- **Pornografía infantil** (Jaishankar, 2011): La capacidad de difusión de internet y las facilidades de interacción de las redes sociales y los sistemas de mensajería han permitido que se creen redes de contactos organizados interesados en la compartición de material pedófilo, que es también un delito en España.
- **Enaltecimiento y humillación de las víctimas del terrorismo** (Moro Díaz, 2017): De acuerdo con el código penal, alentar, premiar y, en definitiva, enaltecer los actos, grupos y organizaciones terroristas constituye un delito. En la misma línea, también es delictivo el abuso, mofa, discriminación y, en definitiva, humillación de las víctimas de estos actos terroristas.
- **Amenazas y coacciones**: El hecho de intimidar a un individuo para privar de alguna libertad o exigiendo algún tipo de beneficio bajo amenaza de sufrir un perjuicio.
- **Delitos sexuales**: *Cyberstalking, online grooming, sexting y sextortion.* Un conjunto de actividades que se relacionan con el ámbito sexual y que consisten en acercamientos a menores con la intención de obtener algún tipo de favor sexual, intercambiar

material íntimo propio y propiciar algún tipo de extorsión o proferir amenazas de revelar estas imágenes si no se proporcionan más, que pueden llegar a constituir un delito.

- **Cyberbullying:** El hecho de acosar de manera sistemática a un individuo con diversos fines. Trato difamatorio, vejatorio y humillación entre otros, se da principalmente entre menores y el uso de las redes sociales es un componente de difusión muy fuerte.

La Oficina de Naciones Unidas contra la Droga y el Delito, (UNODC, en inglés) presentó en febrero de 2013 un estudio comprensivo acerca de los ciberdelitos más frecuentes en la actualidad. Para ello, recolectó datos de las fuerzas y cuerpos de seguridad nacionales de diversos países a lo largo de todo el mundo, como se puede ver en la Ilustración 1, los resultados de estos cuestionarios aglomeran en un único estudio este tipo de comportamientos:

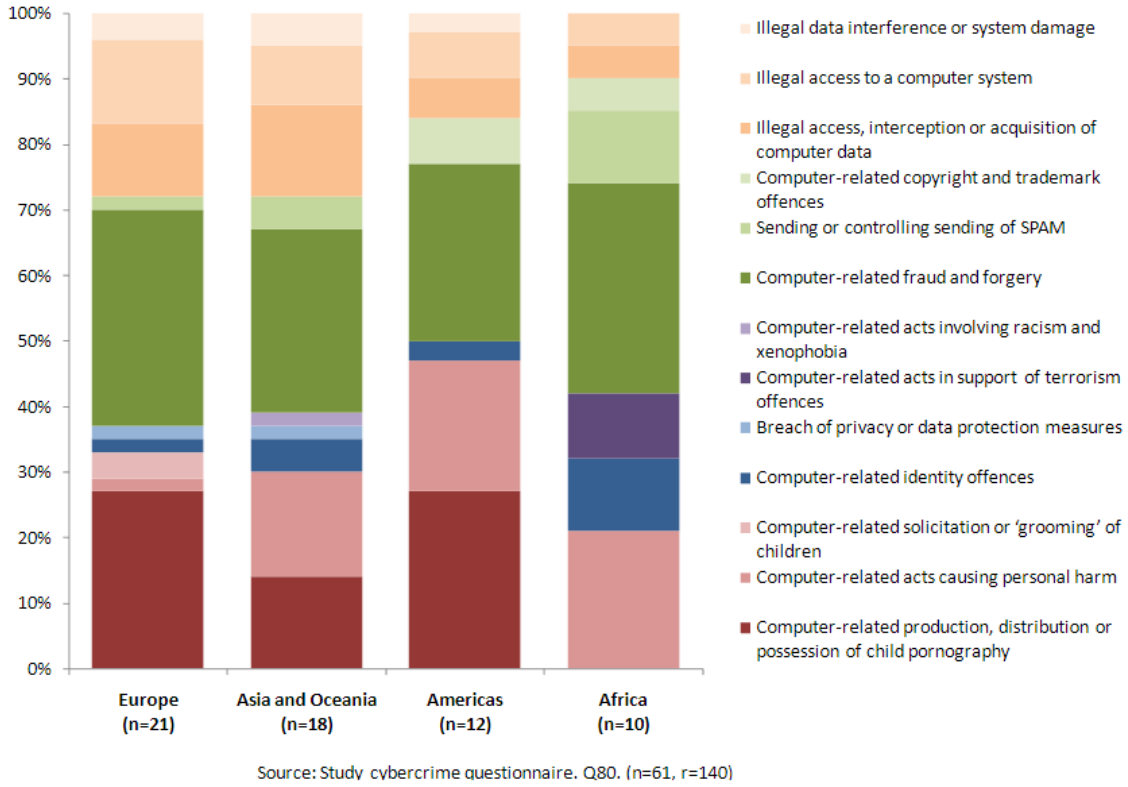

Ilustración 1, Delitos más comunes encontrados por los cuerpos de policía nacionales de países por continentes (UNODC, 2013)

2.4. Redes sociales y uso

El medio de comisión de los delitos informáticos frecuentemente involucra de algún modo las redes sociales. Por este motivo, es interesante realizar un estudio de cuál es el estado del arte de estas redes sociales, pues como resulta lógico, a mayor volumen de usuarios y negocio, mayor cantidad de potenciales víctimas.

Recientemente, Statista publicó un informe acerca de las redes sociales más utilizadas a nivel global, de este estudio se destaca el número de usuarios activos en redes sociales:

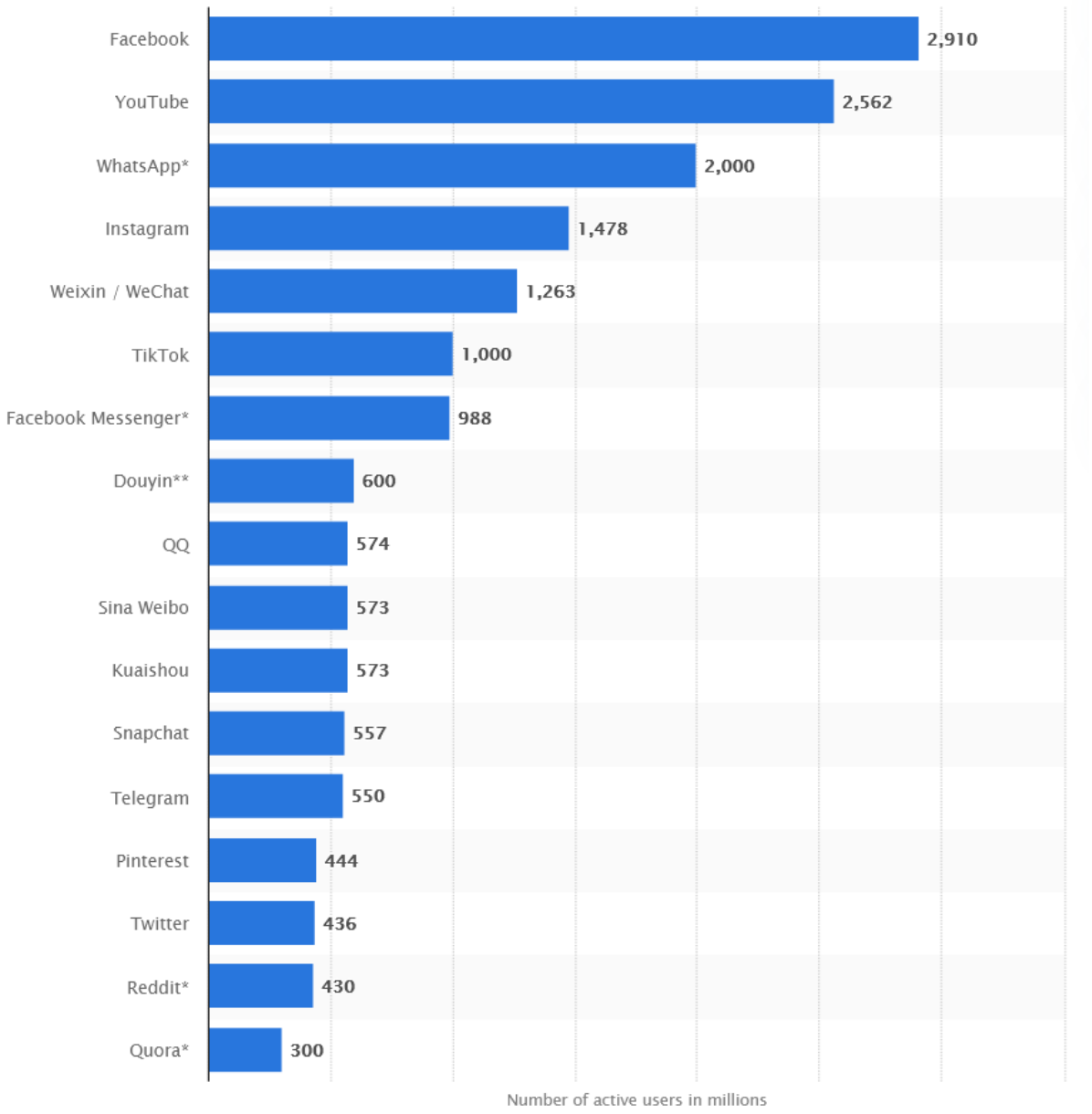

Ilustración 2, Redes sociales a nivel global ordenadas por millones de usuarios activos (Statista, 2022)

Más de un tercio de la población mundial se considera usuario activo de redes sociales como Facebook o YouTube. Teniendo en cuenta que el total de individuos con acceso a internet se estima en 4.300 millones de personas (El Orden Mundial, 2021), más de la mitad de los usuarios de internet usan Facebook, YouTube y, en torno a un cuarto de esta población usa otras redes como Instagram, TikTok o WeChat.

Otro factor a destacar de la extensión de estas redes a lo largo del globo es que la interacción internacional hace que se solapen legislaciones y se añadan capas de complejidad a la hora de realizar análisis periciales y seguir procesos judiciales.

En España también se encuentran estadísticas que se ajustan a estos datos e incluso acentúan el alto porcentaje de acceso a internet de un país moderno. Del estudio de *We Are Social* observamos lo siguiente:

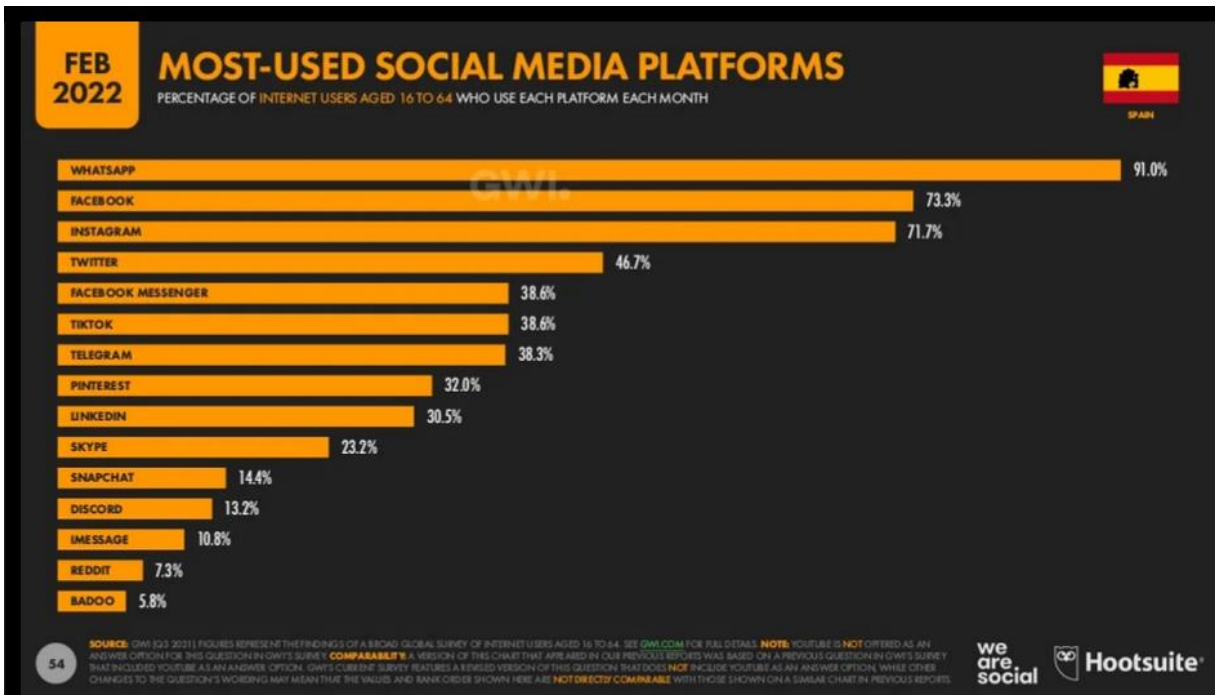

Ilustración 3, Redes sociales más usadas en España (Moreno, 2022)

Acentuando las estadísticas globales, se puede ver como WhatsApp, Facebook e Instagram son las líderes, seguidas de lejos por Twitter, TikTok y Telegram. No es de extrañar, por tanto, que en las consultas periciales estas redes sean también las principales protagonistas.

Este conjunto de información sirve como motivación para comprender estas redes sociales y conocer sus puntos de análisis junto a los problemas más frecuentes que pudieran encontrarse durante la investigación de la comisión de delitos.

3. Objetivos concretos y metodología de trabajo

3.1. Objetivo general

El principal objetivo de este trabajo es el siguiente:

Mejorar la calidad y reducir el tiempo de los procesos de investigación de delitos perpetrados bajo el amparo de las redes sociales **mediante la propuesta de un plan de actuación generalista** que permita la **recolección de evidencias para su debida admisión** en procesos judiciales.

3.2. Objetivos específicos

Para la consecución del objetivo principal, se deberán alcanzar una serie de objetivos específicos. Estos son:

- Determinar cuáles son los delitos más habituales en los cuales las redes sociales jugaron un papel determinante en su comisión o investigación.
- Describir las redes sociales más populares en la actualidad y su interacción y relación con los delitos previamente descritos.
- Catalogar las redes sociales en función del poder de actuación y el margen de maniobrabilidad en la investigación de un delito.
- Desarrollar un flujo de trabajo para la investigación forense de esta combinación de delitos y redes sociales.
- Validar la metodología anteriormente propuesta en tanto a la capacidad de dar respuesta problema a resolver, su eficiencia y la comparación del beneficio adquirido frente a las disponibles en el estado del arte.

3.3. Metodología de trabajo

Partiendo de los conocimientos adquiridos en las asignaturas «Análisis Forense» y «Delitos Informáticos» sea realizado una introducción a una amplia gama de delitos y redes sociales mediante una documentación previa basada en el estudio del marco legal de los primeros en España, estudios publicados acerca de la frecuencia de uso de las redes de acuerdo con estadísticas y una categorización propia de ambos en base a las características percibidas.

Posteriormente, se procedió al desarrollo de la propia metodología, comenzando con el establecimiento de un punto de partida y estableciendo un flujo de actuación hasta llegar al objetivo final que sería la presentación del informe con los hallazgos y evidencias.

Este mismo proceso ha seguido un desarrollo iterativo, incluyendo las propuestas de mejora de las correcciones que se realizaran sobre la versión previa de trabajo.

4. Identificación de requisitos

4.1. Roles en el proceso de investigación

Durante la realización de una investigación forense existen diversos actores que participan de manera activa o pasiva en la misma. La metodología que aquí se presenta, por ser un caso particular de este tipo de investigación, comparten los mismos actores. Estos son:

- **El solicitante**: Generalmente, el conjunto formado por la víctima y, si procede, representantes o consejeros legales. Tiene un rol principalmente pasivo durante la mayor parte de la metodología, pero es el detonante del proceso de investigación y su principal función en la metodología es proporcionar la información que necesite el investigador.
- **El investigador**: Encargado de gestionar la metodología de principio a fin. Desde el momento en el que se pide por parte del solicitante hasta que se presente en un informe apto para ser admitido en un proceso legal. Entre sus aptitudes se encuentra estar capacitado para esclarecer los hechos a investigar tanto a nivel tecnológico como legal.
- **El investigado**: Variable en función del caso. En ocasiones será una persona física o jurídica identificada de la cual se querrá probar la autoría o inocencia de algunos hechos en un contexto tecnológico. En otros casos, puede ser una persona desconocida que se busca desenmascarar. Por la naturaleza descrita de este actor, es un rol pasivo, pero que motiva el proceso de investigación.

4.1.1. Requisitos en el rol del investigador

Dado el propósito de la metodología, en esencia servir de apoyo a los investigadores, es conveniente describir este perfil de investigador, de modo que se puedan definir los requisitos que debe tener esta figura.

Características del investigador:

- Es un **experto**, bien sea en alguna cuestión técnica, en forense, en materia judicial, o en todas ellas a la vez.

- Cual perito, **servirá de apoyo al juez** cuando las evidencias se presenten. Por tanto, debe ser **capaz de transmitir** la información de manera comprensible para el juez, en particular, **las conclusiones**.
- No necesita titulación específica ni estar colegiado, pero el respaldo que ofrecen estos incrementa la credibilidad en la pericia. Además de proporcionar medios y recursos para los procesos de análisis.
- Debe ser **imparcial**, su objetivo es esclarecer los hechos, no dar la victoria a una de las partes en un proceso judicial. De hecho, la falta de imparcialidad está penada legalmente en la justicia y disciplinariamente en los colegios.
- **Ha de estar actualizado**. Las redes sociales cambian continuamente, nuevas redes surgen cada día, algunas alojadas en países donde la legislación complica los procesos de investigación, y, en todas, se modifican los términos y condiciones con frecuencia, así como el modus operandi de los delincuentes se encuentra en un proceso recurrente de mejora y cambio. No actualizarse implica estar un paso por detrás de los sujetos investigados.

4.2. Tecnologías involucradas

Esta metodología está pensada para facilitar la tarea del investigador, y con este mismo fin se describen algunas de las tecnologías que son convenientes o incluso necesarias para el desempeño de su actividad.

A nivel general necesitará algunos medios elementales para el trabajo, algún dispositivo sobre el cual se puedan llevar a cabo labores ofimáticas estándar y software apropiado para la elaboración de este tipo de tareas (como elaboración de informes, almacenamiento de información o correo electrónico).

A nivel específico será necesario disponer de software y hardware dedicado para las labores forenses concretas. A continuación, se proporciona una lista de herramientas que cubren algunas de las necesidades más frecuentes de este tipo de investigaciones:

- **Clonadoras y creadores de imágenes forenses:** Para cuando sea necesario obtener la información de un dispositivo físico, donde frecuentemente se guardan los datos de las aplicaciones de redes sociales y mensajería. Esta categoría incluiría tanto a clonadoras como a protectores contra escritura que usados con suites de creación de imágenes forenses como FTK Imager pueden permitir la copia de estos dispositivos para su análisis.
- **Soportes de almacenamiento:** Para soportar las copias de dichos dispositivos y para otras labores de propósito general.
- **Herramientas y suites forenses para recuperación y análisis de evidencias:** Que proporcionen funcionalidades genéricas de análisis forense, extracción de metadatos, recuperación de archivos borrados o clasificación y etiquetado de evidencias. Si bien existe una amplia gama de herramientas que cumplen estas especificaciones algunas que ofertan estas capacidades son Autopsy, exiftool, FOCA y photorec.
- **Otras herramientas que puedan circunstancialmente ayudar a la investigación:** Como es el caso de herramientas de OSINT (Maltego, theHarvester e incluso *dorks*, atajos de buscadores), software de reconocimiento facial o clasificación de imágenes que permitan automatizar las tareas de investigación, el trazado de conexiones en redes sociales a través de búsquedas específicas o incluso el reconocimiento automático de actividades delictivas preservando la intimidad de la víctima siempre que fuera posible.

4.3. Contexto de uso

La extracción de información en base a los contenidos disponibles en redes sociales y servicios de mensajería es una actividad que se ajusta a un amplio rango de interesados. Un usuario no especializado puede acceder de manera legítima a la información pública que le sea accesible, de hecho, este es el fin esperado de las redes sociales, pero también un usuario con más experiencia podría usar estas mismas herramientas para un informe de inteligencia que pudiera preceder la comisión de un delito. Puede incluso que una persona con los debidos recursos económicos encargue a un experto este tipo de investigación.

No solo se puede usar esta extracción de información a nivel personal, es frecuente que, a nivel judicial o institucional sea necesaria la intervención de un experto que clarifique unos hechos o incluso, por ejemplificar, que una empresa contrate los servicios de un investigador privado para desenmascarar un fraude.

Por tanto, se puede comprobar que el análisis en redes sociales es un proceso que abarca lo individual, lo institucional y la empresa privada, pero cuando se habla de delitos se está refiriendo directamente a la Ley y de un modo u otro están involucrados en el contexto judicial.

Bien sea una solicitud por un individuo víctima de un delito o una investigación llevada a cabo en el seno de una empresa, todas están abocadas a servir como prueba fehaciente en un proceso judicial. Por tanto, se puede afirmar que el contexto final de uso es el de expertos en procesos de investigación de cara a un real o hipotético litigio.

5. Descripción de la metodología

En esta sección se hará una descripción detallada de la metodología, estableciendo un punto de partida y estableciendo en cada paso las posibilidades de actuación, clarificando los procesos en cada uno de los casos y redes sociales posibles.

La idea base de la metodología es calificar el delito a investigar, identificar el tipo de pruebas necesarias que demuestren o soporten la comisión de un delito, identificar la red social en la que se apoya para su comisión y, por último, seguir el proceso de actuación para recolectar, adquirir y certificar evidencias en dicha red social de cara a su presentación.

5.1. Esquema de la metodología

Puesto que el objetivo de la metodología es ser capaz de recolectar de manera fidedigna y eficiente un conjunto de evidencias que constaten un hecho en el cual se vean involucradas las redes sociales, es necesario definir el proceso desde el momento en el que se introduce el caso hasta el momento en el que se presentan las evidencias con sus correspondientes conclusiones. El flujo de la metodología se define así:

En primer lugar, se presenta el caso a estudiar del cual se tienen indicios de que puede haberse cometido a través de redes sociales, haberse apoyado en ellas de algún modo para su comisión o, incluso, pudieran alojar alguna evidencia para el trabajo de investigación. Se recaba toda la información del caso: implicados, hechos verificados, hechos por verificar y similares. En el caso de formar parte de una solicitud de peritaje en un proceso judicial ya existente, se destacará la sección de los supuestos sobre los cuales el perito deberá pronunciarse para centrar el foco de la investigación.

Una vez recabada la información inicial, esta ha de analizarse para determinar si efectivamente se trata de un posible delito admisible como punto de entrada en esta metodología, si se confirma que las redes sociales no han sido involucradas en el caso se desestimará la aplicación de esta metodología y se orientará el peritaje hacia otra metodología distinta que sea aplicable para este caso o si, alternativamente, la información proporcionada

inicialmente fuera insuficiente para determinar si este delito puede ser investigado con la presente metodología y debiera solicitarse más información para llegar a una conclusión.

En el momento en el que se confirmase la implicación de las redes sociales en el caso, se procedería al siguiente paso de la metodología: Identificación de delito en base a los indicios, pruebas y testimonios existentes, verificando que concuerde con el delito que se quería probar en la solicitud inicial o si hubiera indicios de cualquier otro tipo de actividad criminal adicional.

Con el delito o delitos identificados, el siguiente paso es identificar el tipo de pruebas que pueden constatar la comisión del delito o ayudar en este proceso. Según el acto que se investigue, las evidencias a buscar cambiarán, de este modo podrán ser objeto de la búsqueda imágenes, vídeos, mensajes de texto o *logs* entre otros.

El siguiente paso es identificar las redes sociales que se han visto implicadas en la comisión del delito. Para hacer esto en primer lugar se tomará de la documentación del caso todo indicio inicial sacado de testimonios y evidencias previamente existentes que hubiera como punto de partida. Después, se realizará una investigación de tipo *OSINT* para extraer posibles redes o medios en los que se pudiera encontrar más información de la presentada en el dosier inicial, siendo el objeto de esta búsqueda parámetros como nombres de usuario, mensajes o imágenes que pudieran llevar a encontrar relaciones en fuentes abiertas.

Con las redes sociales involucradas identificadas y el tipo de pruebas que identifican al delito a investigar concretadas se pasa al proceso de extracción de pruebas en dichas redes sociales. Esta metodología propone el mecanismo de recolección de un tipo determinado de prueba para una red social concreta o que, por su naturaleza, se acoja a una categoría de redes sociales para las que se ofrecen procedimientos más generales de extracción. Esta metodología busca hacer especial hincapié en la importancia de los mecanismos de adquisición de manera que se garantice la validez de estas evidencias de cara a un proceso judicial.

La fase final de la metodología es la presentación de las pruebas. Recopilar las evidencias encontradas y exponerlas en conjunto con las conclusiones que se han encontrado. Puesto que el objetivo de este es ser admisible para un proceso judicial, la presentación final deberá acogerse a los principios de la elaboración de informes periciales la norma UNE 197010.

En las secciones que se encuentran a continuación, se procede a dar una explicación en profundidad de las fases de esta metodología con el fin de poder llevar a cabo su ejecución.

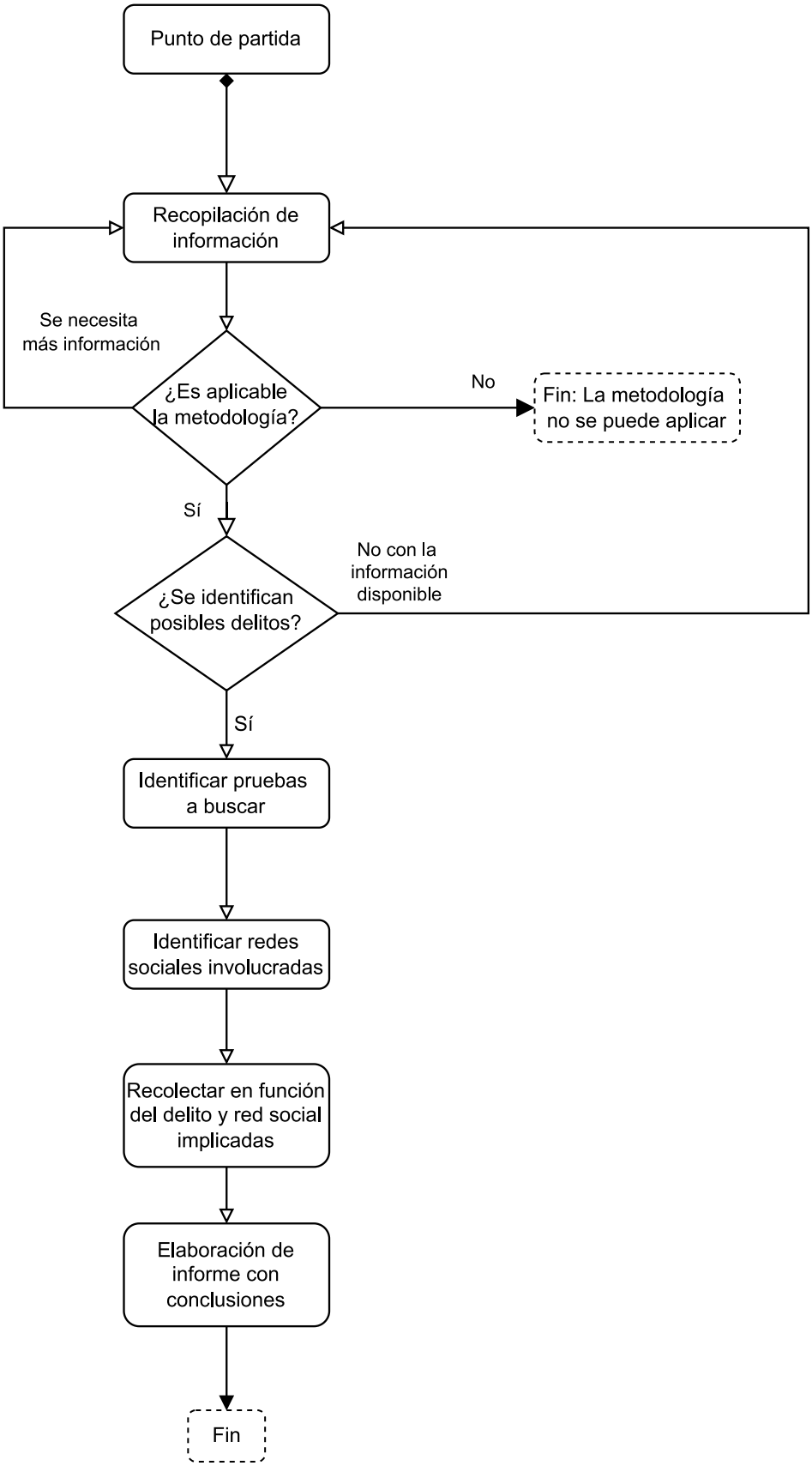

Ilustración 4, Esquema de la metodología

5.2. Primer paso: Recopilación de la información inicial del caso

Todo caso parte de una situación inicial, cuando el perito o investigador reciba el caso será acompañada de algún tipo de información ya sea en formato escrito u oral. La primera tarea de la persona que siga esta metodología será documentar formalmente el caso, adecuando la información recibida a un formato ordenado y elegante donde se recopilarán los datos de partida.

Este primer *documento de presentación* contendrá la siguiente información:

1. **Título**: Frase corta que resuma el caso presentado.
2. **Breve descripción**: Resumen del presunto hecho delictivo y la información clave que se disponga hasta el momento para identificar rápidamente el caso. La extensión será de un solo párrafo.
3. **Actores**: Conjunto de individuos que se han visto envueltos en el suceso. Esta lista comprenderá tanto al subconjunto de víctimas como al sospechoso e hipotéticos cómplices. Es posible que la identidad de algunos de estos actores sea desconocida por la naturaleza de internet, por lo que deberán ser identificados durante la investigación en caso de que sea necesario revelar su identidad.
4. **Redes sociales implicadas**: Conjunto de redes sociales y servicios de mensajería implicados en la comisión del delito a investigar según la información proporcionada. Puede que durante la investigación se descubran medios adicionales o se descarten algunos de los presentados inicialmente.
5. **Sucesos conocidos y probados**: Lista de sucesos probados de interés para la investigación. Por lo general, esta sección solo existirá cuando el caso provenga de una investigación judicial donde se hayan admitido previamente como evidencias estos hechos o cuando el documento inicial sea la continuación de una investigación pericial que se haya adecuado a unas buenas prácticas de recolección de evidencias.
6. **Sucesos a investigar**: Conjunto de sucesos sobre los cuales el encargado de la investigación deberá pronunciarse. Serán el eje central de la investigación y servirán como objetivos de la misma.

Este documento será de uso exclusivamente auxiliar para la investigación, por lo que no deberá presentar un formato específico estricto y puede adaptarse a las necesidades de su

usuario. Sin embargo, es determinante la calidad, exactitud y veracidad de los datos incluidos, pues servirán para realizar múltiples tomas de decisiones a lo largo de la aplicación de la metodología.

5.3. Segundo paso: Decidir si la metodología es aplicable

Con el *documento de presentación* conformado se dispondrá de una colección de información relativa al caso, en el siguiente paso se ha de proceder a tomar la decisión de si la metodología es aplicable al encontrarnos ante un caso relacionado con las redes sociales, si no es aplicable o si no se puede tomar la decisión con la información disponible.

La pregunta que debe responder el investigador, por tanto, es: **¿Es posible aplicar la metodología en este caso?** Las posibles respuestas a esta pregunta son las siguientes:

1. **Sí.**

   Cuando se tenga claro que la comisión del delito involucra a las redes sociales y que existe la posibilidad de que una investigación más profunda pueda esclarecer los hechos, el responsable de la aplicación de la metodología determinará que la presente metodología es aplicable y pasará al siguiente paso de la misma.

   El investigador puede realizar algunas preguntas para ayudarse en la toma de esta decisión: ¿Existe alguna publicación actual o pasada que suponga un indicio o pista? ¿Existe algún mensaje que pueda estar relacionado con el caso? ¿Algún documento delatador? ¿Hay indicios de que existe una entidad atacante? Si la respuesta a estas preguntas o a otras similares es afirmativa se puede decantar hacia el uso de la metodología.

2. **No.**

   Si por el contrario se determina de manera clara que no se han involucrado las redes sociales en el presunto delito o que el mismo hecho no supone un delito no se podrá aplicar la metodología. En su lugar se orientará a la persona solicitante, indicando cómo debiera proceder, asistiendo con otro tipo de servicios periciales si le fuera necesario y se terminaría con la actuación de la presente metodología.

   Del mismo modo al caso afirmativo se pueden hacer algunas preguntas que ayuden a determinar la negativa a la aplicabilidad de la metodología. Algunas de estas preguntas que ha de hacerse el investigador son: ¿Es el acto a investigar un hecho delictivo? Por

ejemplo, la publicación de la agenda de un político en una red social podría no suponer ninguna afrenta a la intimidad por su carácter político. ¿El hecho se sostiene en las redes sociales, o simplemente se ha hecho eco en ellas sin que haya ningún indicio de su comisión a través de las mismas? Por ejemplo, cuando se utiliza una red social para difundir y denunciar un hecho y en sí mismo compartir este suceso no constituye un delito. Además, si las respuestas a las preguntas que se planteaban en el caso afirmativo tienen una respuesta negativa entonces se puede decantar a la no aplicabilidad de la metodología.

3. **No es posible determinarlo con la información actual.**

   Se puede dar la casuística en la que, por la información presentada o por la manera en la que esta se ha ofrecido, no se pueda determinar si las redes sociales toman un papel relevante en el caso y se puede aplicar la metodología. En este caso, es tarea del investigador recabar una lista con los datos que fueren necesarios para tomar una decisión, proporcionársela a la fuente original y volver al primer paso de la metodología con las nuevas respuestas que haya proporcionado.

   En el caso de que no se pudiera conseguir la información restante la investigación deberá suspenderse hasta que no se adquieran datos que permitan avanzar.

   Esta respuesta tiene lugar cuando falta algunos de los elementos clave de la investigación. Algunos casos de ejemplo son: Cuando el hecho a estudiar supone un delito, pero no es posible identificar actores, cuando se omite información relativa a los sucesos ocurridos de tal manera que no se pueda determinar si el hecho es delictivo o no se proporcionan los medios de comisión involucrados.

5.4. Tercer paso: Identificar el delito o delitos a investigar

Cuando se ha determinado que el caso a estudiar es susceptible del uso de esta metodología, la siguiente acción natural es proceder a la propia investigación. Concretamente, se comienza con la identificación del delito o delitos que se sospechan que hayan sido cometidos por el objetivo de la investigación.

Previamente, en este trabajo, se ha hecho una introducción a los delitos informáticos que se apoyan en redes sociales más frecuentes. Para este paso de identificación se tomará como referencia la clasificación de ciberdelitos del Observatorio Español de Delitos Informáticos (OEDI, 2016).

De este modo, el supuesto se clasificará en alguna de las siguientes categorías según corresponda:

1. **Acceso e interceptación ilícita**: Aquellos relacionados con el descubrimiento y revelación de secretos (artículos 197 a 201 del Código Penal) o relativos al mercado y los consumidores (artículos 276 a 286), popularmente conocidos como espionaje industrial.

   Este tipo de delitos comprenden aquellos que vulneren la intimidad de las personas, tanto físicas como jurídicas. Para considerarse delito, los artículos 197 a 201 precisan la denuncia de la persona agraviada o su representante legal (salvo cuando sea cometido por un funcionario público prevaliéndose de su cargo) y el perdón de esta persona detiene los procesos judiciales subsecuentes.

   Los hechos que se aglomeran en esta categoría son: Descubrimiento y revelación de secretos, acceso ilegal informático y otros relativos al mercado y consumidores (incumplimiento de acuerdos de confidencialidad, alegaciones falsas y características inciertas en publicidad que puedan causar un perjuicio grave o falseamiento de información financiera en publicaciones).
2. **Amenazas y coacciones:** Aquellos que profirieran algún tipo de amenaza con o sin condición, hacia una persona o sus allegados o le impidieran violentamente realizar algo que la ley no prohíba (artículos 169 a 172 del Código Penal). Las coacciones leves solo serán perseguibles previa denuncia.

Los tipos de delito que pertenecen a esta categoría son: Amenazas a individuos, amenazas a grupos étnicos, culturales o religiosos o coacciones.

3. **Contra el honor:** Cuando se impute la realización de un delito con conocimiento de su falsedad o con un claro desprecio a la verdad o cuando se atenta gravemente contra la dignidad de otra persona con el objetivo de mermar su imagen pública (se considera grave cuando en el concepto público se tiene como tal).

   Los hechos que encajan en esta categoría son: Calumnias e injurias (artículos 205 a 210 del Código Penal).

4. **Contra la propiedad industrial e intelectual:** Explotar cualquier creación del intelecto humano protegida por las leyes de propiedad intelectual con el ánimo de obtener un beneficio económico directo o indirecto y suponga un perjuicio para el titular de los derechos (artículos 270 al 272 del Código Penal). Es igualmente aplicable para patentes o similares en el contexto industrial donde un tercero, con fin comercial o industrial y sin consentimiento, se aproveche de este tipo de creaciones (art. 273 a 277 del Código Penal).

   En esta categoría se encuentran: Delitos contra la propiedad industrial (uso no autorizado de patentes, modelos de utilidad para extraer un beneficio) y delitos contra la propiedad intelectual (uso no autorizado de creaciones literarias, artísticas o científicas para beneficio propio en perjuicio de un tercero).

5. **Contra la salud pública:** Aquellos en los que se elaboren, intermedien o almacenen sustancias nocivas para la salud por su naturaleza o por la falta de controles exigidos (artículos 359 al 371 del Código Penal).

   En esta categoría se agrupan: Tráfico de drogas y otros contra la salud pública. Ajustándose al contexto de las redes sociales, se buscará en mayor medida todo acto de difusión, distribución o incluso cualquier indicio sobre elaboración o almacenamiento.

6. **Delitos sexuales:** Relacionados con los actos sexuales sin consentimiento entre ambas partes, obligación a la participación o visualización de actividades de carácter sexual u otras obscenidades, solicitud de favores sexuales conllevando una situación intimidatoria o humillante, distribución de material pornográfico entre menores o discapacitados con necesidades especiales, o induzca a la prostitución a una tercera

persona lucrándose de esto o si esta persona fuera menor de edad (artículos 181 a 189 del Código Penal).

En esta categoría se encuentran los siguientes hechos: Exhibicionismo, provocación sexual, acoso sexual, abuso sexual, corrupción de menores o incapacitados, pornografía de menores o delito de contacto mediante tecnologías con menores de 13 años con fines exclusivamente sexuales.

7. **Interferencia en los datos y en el sistema:** Daños provocados por otras causas varias, siendo destacables los daños que de manera grave dañen datos o programas informáticos, obstaculizasen el funcionamiento normal de un sistema ajeno o incluso daños causados por imprudencia grave (en este último caso solo es perseguible ante una denuncia y el perdón finaliza la actuación judicial).

   Los hechos que entran en esta categoría son: Daños y ataques informáticos. Que en redes sociales se pueden manifestar de diversas maneras, por ejemplo, el uso no autorizado de alguna funcionalidad que implique un perjuicio para una tercera persona (artículos 263 a 267 del Código Penal).

8. **Fraude informático:** Más popularmente conocido como estafa, consiste en conducir con ánimo de lucro a que alguna persona realice un acto en perjuicio propio o ajeno, así como el acto de conseguir alguna transferencia patrimonial de manera no consentida con un programa informático o la mera creación, posesión o distribución de programas que permitan esta actividad (artículos 248 a 251 del Código Penal).

   Los hechos que se incluyen en esta categoría son: Estafa bancaria, estafa con tarjetas de crédito, débito o cheques de viaje y otras estafas y fraudes (que involucren otro tipo de bienes patrimoniales).

9. **Otros delitos:** Dada la naturaleza de internet y las redes sociales, cabe la posibilidad de que salgan a la luz nuevas modalidades de delito que no estén contempladas actualmente en el Código Penal, por lo que es tarea de la pericia del investigador determinar si el acto que se quiere estudiar constituye un delito fuera de esta tipificación.

Con la información recopilada en el segundo paso y la aplicación de la categoría del delito en este paso se puede proceder a la recopilación de tipos pruebas a buscar en el siguiente paso. En el caso en el que no se ajustase a ningunos de los delitos expuestos en esta fase se

deberá volver al segundo paso de la metodología para identificar posibles errores en la determinación de la viabilidad de la existencia de una actividad delictiva en el caso que se presenta.

5.5. Cuarto paso: Determinar tipo de pruebas relacionadas con el delito a investigar

Una vez categorizado el delito, es necesario saber qué tipo de pruebas sirven para demostrar que el sospechoso es el autor de algún hecho delictivo para posteriormente buscar esas evidencias en las redes sociales que se vieran envueltas en la investigación.

Este paso de la metodología se centra en definir qué tipo de evidencias pueden ayudar a dilucidar los sucesos ocurridos en el caso de estudio. El investigador hará una lista de tipos de pruebas a recabar que estará compuesta por un conjunto base de evidencias asociadas a delitos concretos y otro conjunto que se elaborará en base a las particularidades del caso, por ejemplo, si la víctima denunció el uso de una imagen o archivo concreto durante una estafa se podría añadir a la lista de indicios a buscar tanto las posibles pistas inherentes a una estafa como la búsqueda de dicho archivo o imagen para conducir la búsqueda.

A continuación, se ofrece una enumeración de posibles evidencias a buscar organizadas por tipo de delito para que sean añadidas a la lista de búsqueda:

1. **Acceso e interceptación ilícita:** Publicaciones en formato texto, imagen o vídeo del secreto o secretos revelados o la información falseada, tanto en publicaciones vigentes como en borradas siempre que existiera el medio de certificación. Registros y logs en dispositivos físicos o en la propia red social que demuestren el acceso a estos secretos o la transferencia de los mismos.
2. **Amenazas y coacciones:** Se buscarán mensajes directamente dirigidos a la víctima donde se exprese directa o insinúe la amenaza, coacción, se exijan condiciones o se manifieste la intención de inhibir a la víctima. También se buscarán publicaciones que pudieran hacer referencia a la amenaza sin estar expresamente dirigidas a la víctima, con el fin de generar una situación hostil, intimidante o humillante. En el caso donde no exista una víctima particular, sino que esté dirigido a un grupo de personas, se podrá investigar la participación del agresor en colectivos de odio en foros o grupos de redes de mensajería.
3. **Contra el honor:** Para el caso de las injurias y calumnias es necesario aportar pruebas acerca de publicaciones o mensajes de carácter público y difamatorio. El tipo de prueba a buscar coincide en el formato, que puede ser de texto o multimedia, pero el

medio no es un ámbito privado sino uno que sea públicamente accesible por cualquiera.

4. **Contra la propiedad industrial e intelectual:** En este caso no solo se busca la posesión del archivo que aloje el objeto protegido con propiedad intelectual o industrial, sino que se ha de demostrar su implicación en su distribución, transferencia o lucro. La compartición de ficheros con estos contenidos vía transferencia directa o el envío de enlaces a servicios *peer-to-peer* pueden ayudar en la investigación. Por supuesto, la publicación directa de contenido protegido por propiedad intelectual es una prueba clara a seguir en el estudio del delito.
5. **Contra la salud pública:** Puesto que es complicado demostrar la elaboración de alguna sustancia o su almacenamiento, la investigación para este tipo de delito se centrará en la intermediación. Por tanto, la búsqueda comprenderá tanto los indicios sobre la distribución de la mercancía (mensajes directos o publicaciones con mensajes ocultos en el uso de alguna jerga o registros de transacciones de criptomonedas entre otros) como en la posible adquisición de material para la fabricación de dicha sustancia. Se podrá adicionalmente extraer datos sobre la ubicación en los casos en los que se pueda asociar al sospechoso con la situación geográfica de algún alijo o elemento que pudiera ser delatador.
6. **Delitos sexuales:** Se buscará la existencia de mensajes de índole sexual que fueran recibidos por la víctima o envíos de archivos de este tipo que no fueran solicitados por la misma o cuando estos fueran dirigidos a menores fuera de la edad de consentimiento. Del mismo modo se investigará cualquier tipo de intercambio que se perciba como una invitación a algún tipo de actividad sexual.
7. **Interferencia en los datos y en el sistema:** Se investigará la actividad del sospechoso en la aplicación, prestando especial atención a las acciones que haya realizado sobre la misma y que pudieran apuntar a algún posible tipo de perjuicio intencionado. Este tipo de información será más propensa a ser encontrada en registros de la aplicación o sistema.
8. **Fraude informático:** Para supervisar la realización de una estafa el medio más común es el uso de mensajes a través de servicios de mensajería o correo, por lo que será de interés todo intercambio de comunicaciones entre víctima y sospechoso. También puede ser de interés datos acerca de la ubicación del sospechoso y cualquier otro dato

que permita identificar al malhechor, que es frecuente en este tipo de delitos que se mantenga en el anonimato e incluso se encuentre fuera del alcance legal físico.

9. **Otros delitos:** De nuevo, por el dinamismo y la evolución de las redes sociales, es factible que se produzcan nuevos tipos de pruebas que pudieran apoyar el proceso de investigación, podría ser el caso de un modelo 3D usado por un actor malicioso en una red social basada en realidad virtual que permitiera identificarle unívocamente. Por lo tanto, es tarea de la pericia del investigador determinar si este nuevo tipo de delito se ampara bajo algún tipo de prueba existente en la actualidad o si nuevas tecnologías implican nuevos tipos de características que empiezan a extenderse en las redes sociales y empiezan a ser admitidos como pruebas en procesos judiciales.

Con el delito identificado y un conjunto de evidencias como objetivos de búsqueda es posible pasar al siguiente paso para identificar las redes sociales implicadas y proceder a la búsqueda de estos indicios en dichas redes.

5.6. Quinto paso: Identificar las redes sociales involucradas

El otro factor clave para la aplicación de esta metodología aparte de la existencia de un delito es que se soporte en alguna red social. Es importante determinar qué redes sociales se han visto envueltas en la comisión del supuesto delito ya que cada red social (y cada tipo de red social) tendrá una manera determinada de adquirir las pruebas que demuestren su comisión.

Este paso consiste precisamente en esto. Identificar qué redes sociales se involucraron en el acto a investigar y analizar el tipo de red social para, en el siguiente paso, saber qué procesos serán necesarios seguir para la obtención de evidencias.

A continuación, se ofrece una categorización de algunas de las redes sociales más extendidas, estas categorías no son mutuamente excluyentes y algunas redes podrían encajar en otra.

1. **Mensajería instantánea:** Popularmente, menos ligada al concepto de red social, pero objeto clave de esta investigación. Pertenecen a esta categoría aplicaciones cuyo eje de funcionamiento sean los mensajes que se intercambian los usuarios en privado o en grupo, que pueden tener funcionalidades adicionales de compartición de archivos. Entre otras: WhatsApp, Telegram, Facebook Messenger, iMessage, Signal o Line.
2. **Redes de contactos:** Cualquier red social cuyo propósito sea poner en contacto a desconocidos con el fin de posibilitar el establecimiento de una relación amistosa o amorosa entre varios individuos. Algunos ejemplos son: Tinder, Badoo o Grindr.
3. **Redes sociales generalistas:** No se dirigen a un público con un objetivo concreto como otras que se exponen aquí. En su lugar, abarcan el concepto más clásico de red social entre conocidos y otras redes de *microblogging* como Instagram, TikTok, Twitter, Facebook, Snapchat o Tumblr.
4. **Redes sociales profesionales:** Su propósito es poner en contacto a trabajadores y empleadores para que finalmente puedan llegar a algún acuerdo que suponga beneficios para ambos. Algunas de las redes más comunes son Linkedin, Infojobs o Xing.
5. **Redes de geolocalización:** Las publicaciones están orientadas a la ubicación geográfica de los usuarios. Algunos ejemplos de este tipo son Foursquare, Google Places o incluso Strava en el ámbito deportista.

6. **Foros:** La evolución del concepto más clásico y disperso de un foro en cada sitio a aglomerantes de diversos temas. Algunos de los ejemplos más famosos son Reddit, Quora, ForoCoches o Hispachán.
7. **Tablón de imágenes:** Redes sociales que giran en torno a la publicación de una imagen junto a un texto y su discusión. Ejemplos: 4chan, Pinterest.
8. **Servicios de voz:** Aunque puedan concurrir otras funcionalidades, destacan por el uso de *streaming* de voz para poner en contacto a individuos y grupos de personas. Algunos ejemplos más famosos son Discord, TeamSpeak o Skype.
9. **Juegos online:** Más que redes sociales en sí mismas, juegos con funcionalidades de redes sociales, que pueden ir más orientados a ser un complemento al juego (como un chat o un foro) o tener por objetivo emular la interacción social (SecondLife, VRChat).
10. **Plataformas de vídeo y *streaming*:** Redes cuyo principal objetivo es compartir vídeos y emisiones en directo. Las más extendidas son Twitch y YouTube.
11. **Otros:** Existen otros tipos de redes sociales, programas o aplicaciones que pueden no estar tan estrictamente ligadas al concepto intuitivo de red social, pero que incluyen características de interacción entre usuarios que dan lugar a que se puedan producir casos de abuso. Algunos ejemplos de esta categoría podrían ser aplicaciones de estilo de vida y deporte o pulseras de actividad que permitan algún grado de interacción entre usuarios. También caerían en esta categoría nuevos modelos de redes sociales basados en paradigmas de interacción distintos a los aquí expuestos.

Si se ha seguido paso por paso la metodología, en estos momentos el investigador tendrá identificado el delito que es objeto de la pesquisa, un conjunto de potenciales pruebas, indicadores, patrones y elementos que puedan ayudar en el esclarecimiento de los hechos, y una lista de redes sociales implicadas en las que buscar.

5.7. Sexto paso: Recolectar las pruebas de las redes sociales según el tipo de delito y la red social

Con toda la información recopilada hasta el momento solo queda recabar todo rastro, indicio y evidencia que sirva para demostrar que el delito que se investiga ha sido realmente cometido, cómo se ha cometido y quién es el verdadero autor.

En esta fase se ofrecerá para cada tipo de red social identificada en el paso anterior, un conjunto de guía, consejos y orientación para la extracción de evidencias generales y se ofrecerá esta misma información de manera más específica (incluyendo procedimientos concretos cuando fuere posible) en las redes sociales *insignia*, más populares, de cada categoría.

Para determinar el conjunto de redes sociales más populares en cada categoría se ha utilizado el estudio de We Are Social de 2022 en el cual se presentaba un informe de uso de redes sociales en España por parte de habitantes de entre 16 y 64 años (Moreno, 2022).

Esta guía para la recolección de pruebas tiene por objetivo ser la principal aportación en términos de utilitarismo para los usuarios de esta metodología, pues busca acelerar el proceso asociado a la recolección y adquisición de evidencias particular para cada red social, que puede verse ralentizado por la falta de experiencia o desconocimiento del funcionamiento de esta red, así como también busca garantizar la calidad de las evidencias recopiladas.

Así pues, se presenta la siguiente lista de recomendaciones y procesos ordenadas por tipo de red social:

- **Mensajería instantánea:**

  Por lo general, este tipo de aplicaciones almacenan en los dispositivos físicos de las víctimas las conversaciones con otros usuarios. Por ello, es conveniente obtener los *hashes* de los archivos de las bases de datos encriptadas junto a los mismos archivos para sustentar la veracidad de cualquier otra prueba en formato de captura de pantalla que se pueda presentar e indicando cómo comprobarlo en la propia base de datos.

  Los mensajes que se quieran utilizar como prueba deberán ser acompañados con la mayor cantidad de metainformación posible que lo identifiquen verazmente.

  WhatsApp:

  - Es posible encontrar las bases de datos encriptadas en Android en los archivos de la aplicación, generalmente en la ruta */storage/emulated/0/Android/media/com.whatsapp/WhatsApp/Databases/*

(puede cambiar entre dispositivos la ubicación del directorio *com.whatsapp* con las bases de datos).

- En iOS, se buscará la base de datos ChatStorage.sqlite, generalmente bajo la ruta */private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/*
- Las tablas más interesantes en la base de datos son *wa_contacts,* que contiene información sobre contactos (ID, estado, nombre, marcas de tiempo, etc.), *sqlite_sequence* (número de contactos), a*ndroid_metadata* (localización e idioma) y *messages* (que contiene los mensajes e información) (Mikhailov, 2019).
- No almacena conversaciones en sus servidores, solo mensajes pendientes de ser entregados (Katalov, 2020a)

Telegram:

- Más extendido en Android, tiene numerosos clientes además del oficial, por lo que el proceso podría sufrir variaciones dependiendo de este cliente.
- En Android, bajo el directorio de */data* y */media* se encuentran los artefactos de mayor interés forense. Estos son la carpeta *database*, que contiene la base de datos principal del servicio (llamada *cache4.db)*, *preferences*, con opciones de configuración, *cache*, que almacena imágenes de usuarios y contactos, y la carpeta de contenido multimedia (archivos enviados y recibidos)(Anglano et al., 2017).
- Los servidores guardan copia de los chats no secretos, según la jurisdicción se pueden solicitar con una orden judicial.

Facebook Messenger:

El servicio de mensajería separado de la aplicación principal de Facebook, con capacidad de intercambio de mensajes y contenido multimedia, así como interacción con bots.

- Se puede realizar una adquisición convencional en el teléfono en el que se encuentren las evidencias y proceder con software de análisis de evidencias

para buscar entre los mensajes, gifs y archivos cualquier contenido de interés (Samara, 2022).

iMessage:

El servicio de mensajería nativo de los dispositivos iOS.

- Se pueden llegar a obtener los contenidos de las conversaciones (mensajes y adjuntos) en la copia de seguridad que realiza en iTunes o iCloud.
- Se realizar una adquisición del sistema de archivos al completo, lo cual puede incluso arrojar más información acerca de mensajes borrados (Katalov, 2020b).

Signal:

- No guarda historial de conversación en los servidores, por lo que se descarta cualquier posible petición legal.
- No realiza copias de seguridad de conversaciones localmente ni en ningún servicio en la nube.
- La base de datos está cifrada con contraseña, en el caso de iOS, en el KeyChain con la máxima clase de protección.
- Para la extracción es necesario obtener el sistema de archivos y descifrar la base de datos con la contraseña (Katalov, 2020a).

- **Redes de contactos:**

Badoo:

- El contenido de mayor interés son los mensajes intercambiados entre los usuarios.
- El acceso a los mensajes se consigue mediante el sistema de archivos.
- En algunas versiones el acceso a los archivos de Badoo puede estar protegido bajo derechos de root, aunque existen algunas herramientas para bajar la aplicación a una versión anterior y solventar este inconveniente (Avilla, 2022).

Tinder:

- Se aplican los mismos consejos que con Badoo, destacando la importancia del intercambio de mensajes y el consejo sobre la versión en algunos dispositivos.

- Adicionalmente, el uso de la localización que hace la app puede favorecer los procesos de investigación, especialmente ligado a delitos sexuales (Saliba & McQuaid, s. f.).

- **Redes sociales generalistas:**

  Facebook:

  - Presenta la complejidad de que chats de mensajería, publicaciones en el muro e interacciones en grupos pueden dejar una huella distribuida a lo largo de distintas ubicaciones
  - Se pueden buscar datos en memoria volátil (RAM), caché del navegador, máquinas virtuales y *snapshots*, y volcado de sistema de archivos en iOS y Android (Wong, s. f.).

  Instagram:

  - Los datos de mayor interés son: Contenido multimedia publicado, contenido de los chats, números de teléfono asociados, geolocalización o incluso interacciones.
  - Dispone de funcionalidad en diversas plataformas y la información acerca de una cuenta se sincronizará en dichos dispositivos (Duc, 2019).

  Twitter:

  - Muy similar a Instagram en cuanto a contenido de interés.
  - En dispositivos móviles, será conveniente focalizar la atención en las bases de datos del sistema de archivos y memoria volátil (Peachyessay, 2021).

  TikTok:

  - La política de la empresa, en conjunción con la gestión de datos en servidores fuera de la unión europea puede llegar a complicar las tareas forenses, retirada de contenido y solicitudes judiciales.
  - El proceso de análisis en TikTok se ajusta al proceso de análisis forense estándar, enfocado a la recolección, adquisición y análisis, si bien es cierto que puede llegar a presentar problemas en la obtención de vídeo (Pandela & Riadi, 2020).

- **Redes sociales profesionales:**

  LinkedIn:

  - Resulta especialmente de utilidad en proceso de elaboración de informes de OSINT.
  - Uno de los delitos más frecuentes está relacionado con la suplantación. Generalmente con el uso de herramientas de webscrapping para reconstruir clones de algunas cuentas concretas (Skulkin, 2021).
  - Estas mismas herramientas de webscrapping pueden ayudar a un investigador a obtener información acerca de los individuos.

- **Redes de geolocalización:**

  Foursquare:

  - La información más relevante que se puede obtener de esta red social es la geolocalización.

  Strava:

  - Especialmente interesante para geolocalizar a un individuo y determinar algunos de sus hábitos, ya que esta red social está orientada al deporte.

- **Foros:**

  Reddit:

  - Al estar centrado en publicaciones, dichas publicaciones y los comentarios en estas serán el principal foco de interés.
  - La mayor parte de la información es de carácter público.
  - Tiene un carácter marcadamente internacional. El rastreo de usuarios puede acarrear problemas.

  ForoCoches:

  - Su funcionamiento y su análisis se puede llevar a cabo de manera análoga a Reddit.
  - Es un foro mayormente usado a nivel nacional, pudiendo llegar a reducir la complejidad del rastreo y el emprendimiento de acciones legales.

- **Tablón de imágenes:**

  Pinterest:

  - Puesto que su uso está enfocado a la publicación de imágenes y comentarios se aplican las recomendaciones explicadas para este tipo de publicaciones.
  - Las técnicas de análisis forense de imágenes (como metadatos o búsqueda inversa) pueden aportar información relevante a la investigación.

4chan:

- Menos popular en España, con menos referencias en el sistema judicial español.
- En EEUU, se han aceptado como pruebas el resultado de un análisis forense centrado en publicaciones, enlaces, dispositivos involucrados, redes y direcciones IP (Palli, 2017). De lo cual se puede inferir que se pueden aplicar procedimientos de análisis forense estándar.

- **Servicios de voz:**

  Discord:

  - Se centra en el intercambio de mensajes, archivos y actividad.
  - Se aplican técnicas estándar de análisis para recabar metadatos, contenido y direcciones IP.
  - Presente en diversas plataformas (PC y móvil), podemos acceder a esta información desde el sistema de archivos (Iqbal et al., 2021).
  - En algunos casos, como en la app de Windows 10, que ostenta la mayor base de usuarios, es posible encontrar conversaciones en texto plano entre los logs de la aplicación (Moffitt et al., 2021).

- **Juegos online:** Más que redes sociales en sí mismas, juegos con funcionalidades de redes sociales, que pueden ir más orientados a ser un complemento al juego (como un chat o un foro) o tener por objetivo emular la interacción social (SecondLife, VRChat).
  - Siendo dependientes del juego en particular, se pueden aplicar técnicas de identificación de usuarios estándar (redes, memoria volátil y *post mortem*).
  - Los perfiles delictivos más comunes son los asociados al ciberacoso, la estafa y, en ocasiones la explotación de vulnerabilidades para robar información o bienes digitales (Tabuyo-Benito et al., 2019).

- **Plataformas de vídeo y *streaming*:**

  YouTube:

  - Se centra en el análisis forense aplicado a la publicación de vídeos y las interacciones con este tipo de publicaciones.

- **Otros:**
  - A lo largo de esta exposición de consejos, recomendaciones y guías, se puede apreciar la repetición del patrón de investigación: Recolectar del sistema de

archivos siempre que fuera posible y solicitar del servidor cualquier información que restara para el proceso de investigación. Una vez concluida esa fase, se procedería al propio análisis de las evidencias recolectadas. Este proceso deriva directamente del concepto clásico de análisis forense, y como norma general será el proceso a seguir en las redes sociales que se popularicen en los próximos años.

5.8. Séptimo paso: Presentación de conclusiones

Con todas las evidencias encontradas se ha de presentar en un documento las conclusiones para determinar qué se ha cometido, cómo, cuándo y quién lo ha hecho. El formato por excelencia para la presentación de este informe en el contexto judicial es el informe pericial.

Como se destacó en el estado del arte, la principal referencia para la elaboración de informes y dictámenes periciales en el ámbito de las Tecnologías de la Información y las Comunicaciones es la norma UNE 197010 (AENOR, 2015). Este paso se centrará en proporcionar una guía basada en esta norma.

El informe pericial a elaborar tendrá los siguientes requisitos:

1. **Título**: Ha de tener un título que identifique el caso unívocamente. Como sugerencia, se puede incluir el hecho denunciado, los actores o redes implicadas y la fecha.
2. **Estructura**: El documento ha de contener:
    a. **Identificación del caso y del perito**: Un código alfanumérico que lo identifique de manera inequívoca y única, y que además contenga el organismo al que se dirige el informe, identificación del perito, del solicitante, emplazamiento geográfico (si corresponde), letrado y procurador del solicitante (si procede) y la fecha de emisión del informe. También se deberá indicar la formación y experiencia del perito o peritos que lo han elaborado junto con su firma.
    b. **Declaración de imparcialidad:** Si procede, el perito podrá aplicar el sistema de tachas o hacer constar su imparcialidad.
    c. **Juramento o promesa:** Donde el perito manifiesta bajo juramento que dirá la verdad, que actuará verazmente y que evitará favorecer o causar un perjuicio a cualquiera de las partes.
    d. **Índice:** Que tiene por objetivo facilitar la localización de los capítulos y apartados. Deberá indicar el número de página en el que comienza cada uno de los capítulos y apartados del documento.
    e. **Cuerpo del informe:** Componente principal del informe. Incluirá el objeto, alcance, antecedentes, consideraciones preliminares, documentos de

referencia, terminología y abreviaturas y, sus partes más relevantes, análisis y conclusiones, donde se indican los datos de partida, las operaciones realizadas sobre ellas hasta la finalización del proceso y llegar a las conclusiones que permitan a personas no expertas en la materia entender lo sucedido.

f. **Anexos:** Cuando procedan, que pueden incluir referencias, documentos, muestras y procedimientos para fundamentar las conclusiones del informe.

3. **Paginación**: En toda página del informe se incluirá el código de identificación, el número de página y el total de páginas. No pueden tener páginas en blanco.

Con el informe debidamente elaborado solo queda que este sea presentado ante la entidad solicitante y esperar a la resolución judicial si la investigación forma parte de este tipo de procesos.

6. Evaluación

En este capítulo se realiza una evaluación de esta metodología, estudiando su desempeño en comparación con casos conocidos y analizando cuáles han sido los beneficios obtenidos de la aplicación de esta metodología. Se ha contactado, sin éxito, con peritos especializados en redes sociales con el fin de obtener conocimiento experto que sirviera para validar esta metodología mediante una entrevista estructurada.

Con la metodología debidamente definida es necesario hacer una evaluación para corroborar que responde al fin último por el cual fue propuesta y cuantificar cualitativamente en qué medida cumple los objetivos propuestos.

Para el fin de evaluar la metodología, se ha realizado la siguiente propuesta: Por un lado, contrastar con casos disponibles públicamente, analizando las fallas que han tenido en esos procesos y explicando cómo la metodología propuesta en este proyecto habría solventado este tipo de inconvenientes, reflejando cómo hubiera diferido el resultado y cuáles son las aportaciones que esta metodología está haciendo sobre el campo. Por otro lado, se ha elaborado una entrevista estructurada para debatir con expertos acerca de los principales problemas del proceso de recolección y admisión de evidencias en redes sociales y las fortalezas y debilidades que se pueden encontrar a grandes rasgos en la metodología que se presenta.

6.1. Comparativa con casos reales

6.1.1. Comparativa con casos a nivel internacional

Empezando con la evaluación en tanto a casos públicos, partiremos de los casos que sirvieron de motivación para este proyecto.

Recordando el caso de Ramel Brown, acusado de asesinato que fue absuelto de los cargos de pertenencia a bandas criminales por ausencia de pruebas concluyentes (*Brown v. State*, 2017), si bien es cierto que los testimonios que lo situaban en la escena del crimen fueron irrefutables, las pruebas que se presentaron para demostrar su pertenencia a bandas criminales fueron capturas de pantalla de vídeos de YouTube, páginas de Facebook, descargas de Twitter y similares. Si bien es cierto que se apoyaron en un experto en bandas criminales para certificar que el contenido de las imágenes eran pruebas suficientes para demostrar la

pertenencia a este tipo de bandas, no se procedió con un método forense que garantizara la autenticidad de dichas pruebas.

Con la metodología propuesta en este trabajo, se pone el foco en la aplicación de las técnicas y normas de análisis forense reconocidas internacionalmente, como la ISO 27037, aplicadas a los casos particulares de cada red social, indicando en qué lugar se encuentran cada tipo de evidencias para cada red social implicada y qué información puede ser más relevante en cada una de esas redes.

En su totalidad, mediante la aplicación de la metodología, se habría logrado demostrar la autenticidad de las pruebas si es que realmente eran auténticas, habría reducido los tiempos de investigación y, posiblemente, se habrían localizado adicionalmente evidencias de interés en las redes involucradas que reforzaran este argumento. De este modo, se podría haber condenado al acusado por su pertenencia a bandas criminales y haber clarificado los hechos. En definitiva, haber hecho justicia.

Este mismo razonamiento es aplicable en líneas generales al estudio de las fallas encontradas en el estudio de procesos judiciales en Estados Unidos (Patzakis & Carpenter, 2017), las carencias que se percibían eran la mala adquisición de las evidencias, como pasaba en el caso de Ramel Brown, la falta de celo en el cumplimiento de los plazos, que excedían los límites legales de reclamación entre otros problemas como la subjetividad de las declaraciones en los casos de calumnia.

La metodología que se propone ataca directamente a estas amenazas. Mejorar las prácticas aplicando los procedimientos de estándares con mayor recorrido, una rápida identificación de los objetivos de la investigación y localización de evidencias, que solventaría el problema de los plazos de reclamación, e incluso el segundo paso de la metodología, la toma de decisiones para categorizar el caso bajo alguna tipología delictiva en base a la información que se tiene, podría contribuir en reducir este tipo de problemas de subjetividad, pues el propio perito, haciendo uso de su experiencia y cualificaciones como herramientas, sería capaz de determinar si una evidencia es lo suficientemente objetiva para demostrar un delito de calumnias o indicar con qué grado de probabilidad una declaración de ese tipo suele ser admitido en tanto a la jurisprudencia.

6.1.2. Comparativa con el caso de la justicia en España

Si nos centramos en la situación de la justicia española en este ámbito, el último caso de estudio que será usado para la evaluación de la metodología es una sentencia del Tribunal Supremo que ha dictaminado jurisprudencia en el ámbito de las evidencias adquiridas en las redes sociales y aplicaciones de mensajería instantánea.

La sentencia del Tribunal Supremo STS 2047/2015 (Marchena Gómez, 2015) presenta un recurso de casación solicitado por el acusado, condenado en instancias inferiores por un delito de abusos sexuales a una menor de edad. Amparándose en la Ley de Enjuiciamiento Criminal, artículos 849.2 y 850, presentó dicho recurso.

Una de las pruebas que se quieren atacar con el recurso es la presentación de unas capturas de pantalla de conversaciones de la red social ya clausurada *Tuenti*. El Tribunal, en este caso afirma claramente que, efectivamente, no adquieren un carácter de documento que respalde la impugnación casacional. Sin embargo, se adjuntó a la causa, con el fin de documentar el caso de manera que se ayude a explicarse a sí mismo o a su móvil.

La defensa acusó la falta de autenticidad en otras pruebas que le incriminaban, también relativas a conversaciones en la red social *Tuenti*. El Tribunal manifiesta que la prueba se sostenía por dos motivos: El primero, más técnico, la víctima proporcionó las credenciales de esta red social para facilitar cualquier tarea en el informe pericial posterior que, de hecho, fueron usadas para hacer una adquisición de las pruebas. Estas pruebas, por la naturaleza de la aplicación en uso, tuvieron que ser tomadas por los peritos mediante la fotografía de la pantalla del móvil de la víctima. El segundo motivo, más acorde al razonamiento judicial, el testimonio de la otra parte de la conversación concordaba con lo presentado, además, en ningún caso podría la víctima haber obtenido un beneficio del proceso judicial ni ofreció testimonios y acusaciones graves. Lo cual aportaba credibilidad al valor de las pruebas.

Este caso aporta una visión más realista de los múltiples factores que intervienen en este tipo de procesos judiciales en España. El análisis y evaluación con respecto a la metodología desarrollada en este trabajo se estructurará en dos partes: Una comparativa del desarrollo del caso con las mejoras que podría haber aportado la metodología propuesta y un análisis de los factores adicionales que se pueden apreciar de este análisis concreto.

En cuanto a la comparativa, partimos de un caso en el cual se realizó un adecuado examen pericial para demostrar la autenticidad de las pruebas. Sin embargo, está el pequeño detalle de que algunas de estas pruebas fueron fotografías tomadas por forenses a dispositivos que mostraban el contenido de alguna aplicación. En la actualidad existen medios más sofisticados de falsificación y el proceso técnico para extraer ese tipo de pruebas, como se propone en esta metodología, pasaría por una adquisición del contenido del dispositivo y la certificación de esta conversación, además de solicitar la información a la plataforma (si fuera necesario, mediante orden judicial), que aportaría más credibilidad al informe pericial. Contextualmente, se siguió un proceso exitoso el cual la metodología defendida podría haber optimizado en términos cualitativos y temporales.

El otro foco de la evaluación es lo que transmite este caso que es muy frecuente en un proceso judicial, pero que no se ha hecho mucho hincapié en la metodología, pues no es tarea del perito, aunque puede ser una competencia transversal muy útil. Este factor es la coherencia de los hechos, el móvil, y la lógica judicial. Es cierto que las pruebas estaban respaldadas por un análisis pericial, pero uno de los motivos que expone el Tribunal para desestimar el recurso, la invalidación de las pruebas, es la coherencia del discurso, la ausencia de un móvil para que ese testimonio fuera falso.

En esta metodología no se contempla el contexto de interés judicial que pueda haber motivado las acciones. La tarea de un perito es esclarecer los hechos, responder al qué, quién, cuándo y cómo, pero nunca el por qué. Por tanto, este factor simultáneamente se escapa del ámbito de la metodología, pero también es una competencia que puede ayudar a un perito a predecir el recorrido judicial de un caso o una investigación antes de comenzar la propia metodología.

6.2. Entrevista estructurada

Con el fin de evaluar la metodología mediante conocimiento experto, se ha elaborado una entrevista estructurada. A continuación, se exponen las preguntas de la entrevista junto a una justificación de por qué se ha elegido dicha pregunta y qué información se pretende extraer a partir de la misma.

Preguntas:

En el contexto del desarrollo de una metodología de recolección y análisis de evidencias en redes sociales con el fin de que sean admitidas como pruebas en un proceso judicial, como trabajo de fin de máster de Seguridad Informática.

1. *¿Hace uso de alguna metodología específica para la recolección y análisis de evidencias en redes sociales?*

   En primer lugar, averiguar si el entrevistado actualmente usa alguna metodología para este caso concreto o si utiliza alguna más específica con el fin de evaluar dicha metodología en contraposición de la que se propone en este proyecto.
2. *¿Cuáles son los factores que más amenazan a un proceso de investigación? (Por ejemplo: manipulación accidental de evidencias, retrasos y volatilidad, trabas en las solicitudes a las redes sociales…)*

   Con el objetivo de descubrir cuales son los problemas a los que se enfrenta un experto en los casos reales y si nuestra metodología aborda esos problemas.
3. *¿Cómo se procuran abordar estas amenazas, en su experiencia?*

   El propósito de esta pregunta es analizar la estrategia del experto frente a las amenazas que considera en sus investigaciones y contrastarla con la estrategia usada en la metodología que se desarrolla en este proyecto.
4. *¿Cómo se valoraría la eficacia y la eficiencia de una metodología con este objetivo? ¿Cómo podría ponerse a prueba, evaluarse, antes de ponerse en práctica en un proceso judicial?*

   Con el fin de validar los métodos de evaluación que se han seguido en este trabajo.
5. *¿Considera que una nueva metodología para la adquisición de evidencias en redes sociales (como la que se presenta) puede beneficiar al colectivo de peritos y otros interesados en la materia? ¿O se considera que no se puede aglomerar bajo una metodología ya que cada experto utiliza las técnicas que mejor le convienen adaptándose a la particularidad de cada caso? (Aclaración: No se pregunta por la utilidad de esta metodología en particular, sino acerca de la sensación general de que se carezca de una metodología más extendida o estandarizada para este tipo concreto de casos)*

Esta pregunta está orientada al estado del arte, a confirmar existe o no alguna metodología que ya responda a este problema o si no tiene sentido plantear una única metodología puesto que la investigación diverge en cada caso particular.

6. *Opcional: La metodología desarrollada se basa en siete pasos: Recopilación de información del caso, determinar si con la información proporcionada se puede aplicar la metodología, identificación del delito que se está cometiendo, determinar qué tipo de pruebas sirven para demostrar este delito, identificar las redes sociales involucradas, recolectar las pruebas según la red social y el tipo de delito que se esté investigando y, séptimo paso, presentación de conclusiones. ¿Qué fortalezas o debilidades se podrían reconocer en esta estructura? En el caso de que se desee indagar más sobre el contenido de la metodología, tras ser proporcionada una documentación más extensa: ¿qué recomendaciones se podrían hacer sobre esta metodología?*

   Pregunta opcional para pedir opinión explícita sobre la metodología que se desarrolla en este trabajo en lugar de abordar indirectamente los objetivos. Es opcional porque requiere un mayor grado de implicación directa con este trabajo y puede exceder los límites de una entrevista liviana.

Esta entrevista, lejos de ser una prueba directa de la validez de la metodología (salvo la sexta pregunta que es una revisión explícita de la misma), busca extraer del conocimiento de expertos cuales son los objetivos, problemas y fines que se proponen los peritos en este tipo de casos para verificar que estén alineados estos objetivos con los de la metodología y así reforzar la validez de la misma.

7. Conclusiones y trabajos futuros

Las redes sociales han visto incrementado el índice de actividad delictiva a la par que su popularidad se ha disparado. Un factor clave en esto ha sido la facilidad que ofrecen las redes sociales para interactuar con otros seres humanos. En particular, el uso que pueden hacer los delincuentes con la simplificación de la interacción.

Con este incremento de la delincuencia se ha multiplicado el número de víctimas y, consecuentemente, el número de denuncias y procesos judiciales asociados. Desafortunadamente, el crecimiento de esta necesidad no ha ido acompañado de una concienciación acorde. Resultando en un trato inadecuado de las evidencias, una adquisición indebida y, consecuentemente, la incapacidad de demostrar la veracidad o falsedad de hechos, encontrándose multitud de pruebas desestimadas por no haber sido presentadas de manera apropiada.

Esta metodología se presenta como solución a este problema. Optimizando el proceso de recolección de evidencias para investigación de delitos en redes sociales para reducir el tiempo empleado y asegurándose la mayor completitud en el recabado de pruebas. En definitiva, mejorar la calidad y reducir el tiempo.

Si bien es cierto que una de las principales debilidades de este proyecto es la incapacidad para poner en práctica la metodología en casos reales, pues no se dispone de una capacitación suficiente para poder conducir una investigación pericial y presentar los resultados en un proceso judicial, se ha podido contrastar con algunos casos reales la metodología usada. Haciendo énfasis en las carencias de los procesos que se siguieron en dichos casos y destacando cómo la aplicación de la metodología que se desarrolla en este trabajo podría haber prevenido muchos de los problemas que se encontraron en esos procedimientos judiciales y haber ayudado en el esclarecimiento de los hechos y la búsqueda de la verdad y la justicia.

Esta causa sirve como motivación para un trabajo futuro: La puesta en práctica de la metodología aquí descrita en casos reales. Bien si se adquirieren los requisitos legales para poder asumir la responsabilidad de una investigación pericial o si cualquier perito en esta

situación estuviere interesado en aplicar la metodología en este tipo de situaciones podría hacer un trabajo centrado en la evaluación de esta.

Adicionalmente, esta metodología busca ser una propuesta generalista que simultáneamente proporcione las instrucciones más específicas posibles para el mayor rango de casos posibles sin entrar en un nivel de detalle que pudiera implicar que a corto-medio plazo se quedara obsoleto. De este modo, se contempla una propuesta centrada en una metodología ya no generalista, sino que fuera una guía con un alto nivel de detalle que indicara medios concretos para la extracción de evidencias y lo que se espera sacar de dichos archivos. Esta investigación tendría por contrapunto que, dado el dinamismo de las redes sociales y su implementación en diversas plataformas, sería muy propensa a quedarse obsoleta rápidamente.

En definitiva, este trabajo ha permitido que se realice un estudio de la situación criminal en las redes sociales y ha proporcionado una guía orientada a personal especializado de modo que ayude en los procesos de investigación, pero también, el contexto que introduce a la metodología, procura ser una recomendación para el público en general, para divulgar acerca de la situación de uso de las redes sociales, los delitos que se pueden encontrar más frecuentemente para estar alerta sin entrar en detalles de prevención y, sobre todo, concienciar sobre la importancia de la gestión apropiada de las potenciales evidencias y la manera en la que se han de recoger y presentar en un juicio para que tenga validez legal y se pueda hacer realmente justicia.

Referencias bibliográficas

AENOR. (2015). UNE 197010—Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC).

Aji, M. P., Hariyadi, D., & Rochmadi, T. (2020). Logical Acquisition in the Forensic Investigation Process of Android Smartphones based on Agent using Open Source Software. IOP Conference Series. Materials Science and Engineering, 771(1). http://dx.doi.org/10.1088/1757-899X/771/1/012024

Almulla, S., Iraqi, Y., & Jones, A. (2014). A State-of-the-Art Review of Cloud Forensics. The Journal of Digital Forensics, Security and Law : JDFSL, 9(4), 7-28.

Anglano, C., Canonico, M., & Guazzone, M. (2017). Forensic analysis of Telegram Messenger on Android smartphones. Digital Investigation, 23, 31-49. https://doi.org/10.1016/j.diin.2017.09.002

Arshad, H., Abdullah, S., Alawida, M., Alabdulatif, A., Abiodun, O. I., & Riaz, O. (2022). A Multi-Layer Semantic Approach for Digital Forensics Automation for Online Social Networks. Sensors, 22(3), 1115. http://dx.doi.org/10.3390/s22031115

Avilla, D. (2022). Avilla Forensics 3.0. https://github.com/AvillaDaniel/AvillaForensics (Original work published 2022)

Carroll, O. L., Brannon, S. K., & Song, T. (2008). Computer Forensics: Digital Forensic Analysis Methodology. 9.

Duc, H. N. (2019, abril 9). Instagram Forensics -Windows App Store | By Justin Boncaldo— EForensics. https://eforensicsmag.com/instagram-forensics-windows-app-store-by-justin-boncaldo/

El Orden Mundial. (2021, mayo). El mapa del acceso a internet en el mundo. El Orden Mundial - EOM. https://elordenmundial.com/mapas-y-graficos/mapa-acceso-internet-mundo/

Hubert, K. (2014, diciembre 1). Evidence Collection From Social Media Sites. Egnyte. https://sansorg.egnyte.com/dl/aWVzuBxVtK

Iqbal, F., Motylinski, M., & MacDermott, A. (2021). Discord Server Forensics: Analysis and Extraction of Digital Evidence. 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 1-8. https://doi.org/10.1109/NTMS49979.2021.9432654

ISO. (2012). Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence. https://www.iso.org/standard/44381.html

Jaishankar, K. (Ed.). (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior (0 ed.). Routledge. https://doi.org/10.1201/b10718

Katalov, V. (2020a, abril 29). Forensic guide to iMessage, WhatsApp, Telegram, Signal and Skype data acquisition. ElcomSoft Blog. https://blog.elcomsoft.com/2020/04/forensic-guide-to-imessage-whatsapp-telegram-signal-and-skype-data-acquisition/

Katalov, V. (2020b, octubre 29). The Forensic View of iMessage Security. ElcomSoft Blog. https://blog.elcomsoft.com/2020/10/the-forensic-view-of-imessage-security/

Marabel Matos, J. J. (2021). Delitos de odio y redes sociales: El derecho frente al reto de las nuevas tecnologías. Revista de Derecho de la UNED (RDUNED), 27, 137-172. https://doi.org/10.5944/rduned.27.2021.31076

Marchena Gómez, M. (2015). STS 2047/2015. 8.

Mikhailov, I. (2019, julio 11). WhatsApp in Plain Sight: Where and How You Can Collect Forensic Artifacts. Group-IB. https://blog.group-ib.com/whatsapp_forensic_artifacts

Moffitt, K., Karabiyik, U., Hutchinson, S., & Yoon, Y. H. (2021). Discord Forensics: The Logs Keep Growing. 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 0993-0999. https://doi.org/10.1109/CCWC51732.2021.9376133

Moreno, M. (2022, marzo 4). Informe Digital 2022 de Hootsuite y We Are Social. TreceBits - Redes Sociales y Tecnología. https://www.trecebits.com/2022/03/04/informe-digital-2022-de-hootsuite-y-we-are-social/

Moro Díaz, C. (2017, noviembre 12). El delito de enaltecimiento y humillación de las víctimas del terrorismo en las redes sociales. https://reunir.unir.net/bitstream/handle/123456789/6463/MORO%20DIAZ%2c%20CLARA.pdf?sequence=1&isAllowed=y

OEDI. (2016, octubre). CIBERDELITOS. OEDI | Observatorio Español Delitos Informaticos. https://oedi.es/ciberdelitos/

Palli, K. (2017). AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANT. 13.

Pandela, T., & Riadi, I. (2020). Browser Forensics on Web-based Tiktok Applications. International Journal of Computer Applications, 175, 47-52. https://doi.org/10.5120/ijca2020920897

Patzakis, J., & Carpenter, C. (2017, febrero 8). Criminal Conviction Overturned Due to Failure to Authenticate Social Media Evidence. Next Gen EDiscovery Law & Tech Blog. https://blog.x1discovery.com/2017/02/08/criminal-conviction-overturned-due-to-failure-to-authenticate-social-media-evidence/

Peachyessay. (2021, julio 26). Forensic analysis of Instagram and Twitter on Mobile Devices. Peachy Essay. https://peachyessay.com/sample-essay/forensic-analysis-of-instagram-and-twitter-on-mobile-devices/

Saliba, J., & McQuaid, J. (s. f.). Investigating Sexual Crimes in the Tinder Age. Magnet Forensics. Recuperado 27 de junio de 2022, de https://www.magnetforensics.com/resources/webinar-investigating-sexual-crimes-in-the-tinder-age/

Samara, R. (2022, mayo 10). Facebook Messenger Forensic Investigation. https://doi.org/10.13140/RG.2.2.28083.91681

Skulkin, O. (2021, abril 23). How to acquire a LinkedIn account for forensics | Digital Forensics | Computer Forensics | Blog. https://web.archive.org/web/20210423112401/https://www.digitalforensics.com/blog/how-to-acquire-a-linkedin-account/

Statista. (2022, enero). Most used social media 2021. Statista. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Brown v. State, S16A1530 (Supreme Court 23 de enero de 2017). https://scholar.google.com/scholar_case?case=58777068442197356 6&q=facebook+OR+twitter+OR+linkedin+OR+youtube+OR+tumblr+OR+instagram+OR+myspace&hl=en&as_sdt=2006&as_ylo=2017

Tabuyo-Benito, R., Bahsi, H., & Peris-Lopez, P. (2019). Forensics Analysis of an On-line Game over Steam Platform. En F. Breitinger & I. Baggili (Eds.), Digital Forensics and Cyber Crime (Vol. 259, pp. 106-127). Springer International Publishing. https://doi.org/10.1007/978-3-030-05487-8_6

UNODC. (2013). COMPREHENSIVE STUDY ON CYBERCRIME - Draft February 2013. 320.

Wong, K. (s. f.). Facebook forensics. Recuperado 27 de junio de 2022, de https://www.fbiic.gov/public/2011/jul/facebook_forensics-finalized.pdf

Anexo A. Glosario

En orden alfabético:

- Cloud: O nube, en español. Abstracción de una solución, programa o aplicación de software que se ejecuta en un proveedor de servicios virtualizados en servidores.
- Hash: Transformación matemática que se realiza sobre los bits que conforman un archivo para obtener una especie de resumen que permite garantizar la integridad del mismo. Plural: *Hashes.*
- Peer-to-peer: Sistema de comunicación «puerto a puerto», directa entre dos ordenadores conectados directamente entre sí para intercambio de información.
- Phishing: Técnica de ingeniería social, engaño, que busca obtener información confidencial de algún individuo mediante el embauco, falsificación o suplantación.
- Snapshot: Copia de seguridad, generalmente incremental, que utilizan muchos sistemas para almacenar los cambios en su base de datos.
- Streaming: Medio de retransmisión de información audiovisual en directo a través de internet.