A Coruña, junio 2026

PRUEBA DIGITAL. VALOR PROBATORIO

JOAQUÍN DELGADO MARTÍN

Magistrado Sala Penal Audiencia Nacional

Miembro Red Especialistas Derecho Europeo (REDUE)

Doctor en Derecho

MENÚ

1. **Investigación de la violencia digital en RRSS**
2. **Prueba de mensajería instantánea**

PROBLEMA 1: Investigación de la violencia digital en RRSS

solunion.es

RRSS: Acreditación del contenido ilícito de violencia digital y su autor

1. Conocimiento del acto de violencia digital
2. Averiguación de la fuente del contenido de violencia digital (IP)
3. Actuaciones para concretar la persona autora

Fase 1.- Notitia criminis de la violencia digital

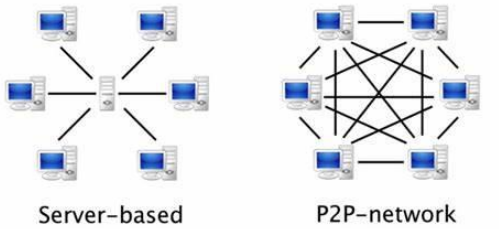
Fase 1.- Notitia criminis de la violencia digital

- Ciberpatrullaje
- Denuncia de la víctima
- Denuncia de la plataforma o prestador de servicios

Fase 1.- Conocimiento de la acción de violencia digital

1.1.- Ciberpatrullaje

- Seguimiento de RRSS
- Análisis de la huella dejada por los hashs en redes P2P (especialmente para contenidos pedófilos).
  - Posible por medios policiales, sin necesidad de autorización judicial (SSTS 238/2008, de 9 de mayo; 247/2010, de 18 de marzo, entre otras)
- Pero los investigados modificaron su forma de actuar:
  - pasan a compartir archivos en la nube y/o en redes privadas; pérdida de eficacia del mencionado Ciberpatrullaje
- Investigación en redes privadas (canal cerrado de comunicación):
  - autorización judicial ex artículo 282 bis .6 LECRIM)



Fase 1.- Conocimiento de la acción de violencia digital

1.2.- Denuncia por la víctima

¿Cómo puede acreditarse en la denuncia el contenido ilícito?

- Soporte papel
- Documento electrónico con la captura de pantalla (DVD, pendrive…)
- Documento electrónico con intervención de servicio de certificación cualificado (tercero de confianza), art. 326.4 LEC
- Acta notarial

Fase 1.- Conocimiento de la acción de violencia digital

1.3.- Colaboración público-privada

- **Organizaciones de la sociedad civil** que realizan labores de investigación de material de abuso sexual infantil —CSAM/MASI— que circula a través de las redes de telecomunicaciones;
  - Rastrear chats o ubicaciones de intercambio de archivos
  - Por ejemplo, National Center for Missing & Exploited Children — NCMEC
- Política corporativa de ciertos **prestadores de servicios** de comunicaciones y/o de servicios de redes sociales (Microsoft, Facebook, Twitter-X, Adobe….)
  - Instrumentos automatizados para filtrar contenidos + metadatos + datos de tráfico de comunicaciones = detectar contenidos sospechosos de ser ilícitos.
- Una vez detectado el material ilícito, se pone en conocimiento de **autoridades policiales o judiciales** del Estado competente.

Fase 1.- Conocimiento de la acción de violencia digital

1.3.- Colaboración público-privada: prestadores de servicios

- **Actuaciones sobre motores de búsqueda** (Google,Yahoo o Bing):
  - sistemas de bloqueo de información mediante el control de términos empleados en motores de búsqueda, mediante la detección de hasta 100.000 vocablos
- **Actuación sobre repositorios virtuales**.
  - Tecnología de funciones de resumen (hashing) para imágenes y vídeos: se compara el hash de los archivos (base de datos con material verificado de abuso sexual de menores) con los hashes de otros archivos de los repositorios virtuales
  - Tecnología de comparación de imágenes en Apple: se analizan todas las imágenes que son almacenadas por dispositivos de Apple, son automáticamente guardadas en la iCloud
  - Clasificadores e inteligencia artificial para el análisis de textos o datos de tráfico. Clasificación por procedimientos de inteligencia artificial (aprendizaje automático) para evaluar y predecir si un determinado archivo contiene elementos de pornografía infantil o abuso de menores.

Fase 1.- Conocimiento de la acción de violencia digital

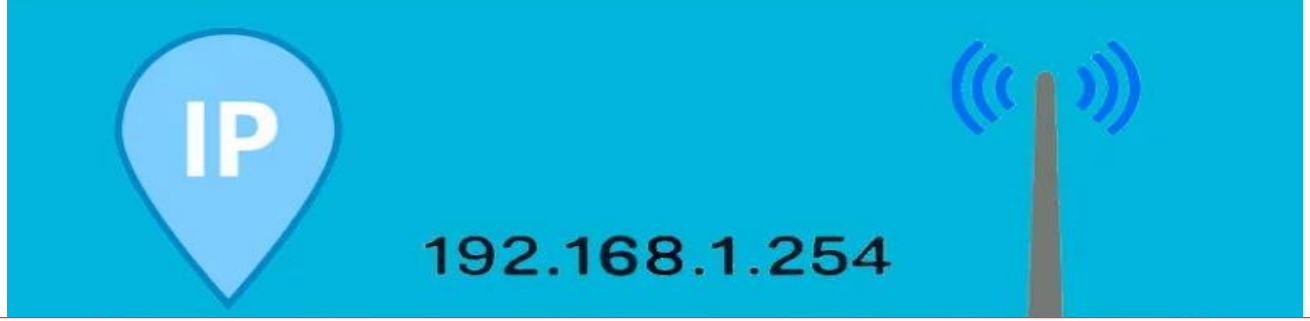
1.3.- Colaboración público-privada: prestadores de servicios

- Estas actividades de colaboración son voluntarias por parte de los prestadores de servicios
- Representan una injerencia en los derechos fundamentales al respeto de la vida privada y familiar y a la protección de los datos personales de todos los usuarios de servicios de comunicaciones interpersonales
- Reglamento (UE) 2021/1232, de 14 de julio (prórrogas):
  - Permite a determinados proveedores de servicios de comunicaciones interpersonales tecnologías específicas para el tratamiento de datos personales y de otro tipo en la medida estrictamente necesaria para detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos y para retirar el material de abuso sexual de menores en línea de sus servicios (excepción temporal)
  - Los tipos de tecnologías utilizadas a efectos del presente Reglamento deben ser los menos intrusivos para la intimidad a la vista del estado de la técnica en el sector. Dichas tecnologías no deben emplearse para filtrar y escanear sistemáticamente el texto de las comunicaciones, salvo con el fin de detectar pautas que apunten a posibles razones concretas para sospechar de abuso sexual de menores en línea, y no deben poder deducir la sustancia del contenido de las comunicaciones. En el caso de la tecnología utilizada para identificar el embaucamiento de menores, tales razones concretas de sospecha deben basarse en factores de riesgo identificados objetivamente, como la diferencia de edad y la probable participación de un menor en la comunicación escaneada.
- Han sido admitidas por jurisprudencia (SSTS 694/2020 y 807/2022)

Fase 2.- Averiguación de la dirección IP

Fase 2.- Averiguación de la fuente del contenido de violencia digital: <u>localización de la IP utilizada</u>

- Uso de rastreos, artificios técnicos u otros medios para averiguarlo; cooperación internacional; o solicitud de información a la operadora (posible internacional)
- Dificultades de IP dinámica; y de tecnología NAT
- Si se trata de una wifi abierta, la labor de esta investigación es más compleja



FASE 2: averiguación de IP

1. **Acceso al dato mediante solicitud a la operadora de comunicaciones obligada por la Ley 25/2007**: la petición del dato deberá acomodarse a las previsiones del art. 588 ter j LECRIM, al tratarse de un dato vinculado a un proceso de comunicación; por lo que es necesaria autorización judicial
2. Sin embargo, **la Policía puede obtener la IP por sus propios medios** (art. 588 ter k LECRIM). El fundamento de esta previsión se encuentra en que la dirección IP, por sí sola, no identifica a persona alguna.
    1. Según jurisprudencia consolidada (SSTS n.º 292/2008, de 28 de mayo; y 776/2008, de 18 de noviembre), la dirección IP **no se encuentran protegida ni por el art. 18.1 CE (intimidad), ni por el art. 18.3 CE (secreto comunicaciones)**
    2. La dirección IP no identifica, pero permite identificar, por lo que tiene la consideración de **dato personal** (Informe 327/2003 AEPD); pero entra dentro de la categoría de datos a los que **puede acceder la policía** de conformidad con el artículo 11.1 LO 7/21: tratamiento realizado por la Policía que resulta necesario para la detección e investigación de infracciones penales; no es dato personal ligado a proceso de comunicación
3. Obtención de la IP mediante **cooperación internacional**

Fase 3.- Ligar IP con la persona responsable

Ligar la IP con el autor (identificación del responsable)

- Acceso a datos de las operadoras: cesión de datos de identificación y localización del dispositivo y la identificación personal del usuario necesita autorización judicial (588 ter k LECRIM)
- Actuaciones para **excluir que se trate de una suplantación de identidad** (denuncias previas por sustracción documentos, indicios de uso de identidad supuesta)
- **Posteriores investigaciones para concretar la imputación**:
  - Medios de investigación tradicional (entrada en domicilio…)
  - Medios de investigación tecnológica (registro de dispositivos, análisis de fuentes abiertas en la web…)
  - Incluso medios de investigación patrimonial

¿Cómo acceder a los datos de Redes Sociales?

- **Acceso a la Red Social por una persona desde su dispositivo**
  - Fuentes abiertas
  - Salvo proceso de comunicación: autorización judicial (agente encubierto virtual)
  - Problema: acreditar la integridad y autenticidad del contenido descargado o del pantallazo
- **Datos en poder de PSSI (remisión de solicitud)**
  - Datos de abonado
  - Datos de tráfico
  - Datos de contenido
- **Datos en el dispositivo (ordenador, móvil…) desde el que se realizó el acceso (registro de dispositivos)**
  - Datos de tráfico (fechas y horas de acceso, registros de inicio de sesión, historial del navegador…) o y datos de contenido (imágenes o vídeos descargados…)
  - Acceso mediante navegador o mediante app

Registros técnicos en infraestructuras intermedias (Firewalls, Sistemas antiDDos, CDN..)

Usuario → Proveedor Acceso a Internet (ISP) → Servidor Red Social (Instagram, X, TikTok…) → Otros usuarios

Datos de tráfico

- Desde ordenador
  - Asigna dirección IP de conexión en un concreto momento
- Desde dispositivo móvil
  - Asigna dirección IP de conexión en un concreto momento
  - Y guarda registro con IMSI (SIM del usuario) y con IMEI (terminal) usados para conexión

Datos de abonado

- Información identificativa del usuario a quien se ha asignado la dirección IP en cada momento

Datos de tráfico

En los servidores del PSSI (Meta para Instagram, BetyDance para TikTok…) se almacenan registros (logs) de un determinado acceso:

- Cuenta del usuario
- Dirección IP de acceso
- Hora de acceso
- Acción realizada (publicación, login…)

Datos de contenido

- Tras eliminación de contenido por usuario o tras cierre de la cuenta: pueden ser conservados durante un tiempo (políticas internas…)
- Orden de conservación

Volatilidad de los datos en Redes Sociales

- **Causas**
  - Enorme velocidad con que se trasmiten, se difunden y/o desaparecen los datos (transitoriedad); mensajes temporales
  - Los contenidos insertados por los usuarios quedan almacenados en los servidores gestionados por los administradores, donde permanecen hasta que el usuario toma la decisión de borrarlos o es baja en la comunidad, aunque los proveedores pueden conservar los datos durante determinados periodos de tiempo
  - La información debe ser recogida con rapidez y almacenada para su posterior análisis
- **Posibilidades de actuación**
  - Policía: acta de captura de pantalla realizada por la propia Policía
  - Acta notarial
  - Acta con la fe pública del Letrado de la Administración de Justicia
  - Denuncia: DVD, pendrive.... con la captura de pantalla (documento electrónico); o acta por empresa certificadora (tercero de confianza);
  - Orden de conservación de datos a la empresa-MF-Policía (588 octies LECRIM)

VALORACIÓN DOCUMENTOS PRIVADOS ELECTRÓNICOS

Documento electrónico acreditado por un servicio electrónico de confianza (art. 3.2 Ley 6/2020)

1. Por servicio de confianza no cualificado (no cumple los requisitos aplicables establecidos en el Reglamento UE 910/14): se rige por el art. 326.3 LEC
   a. Si se impugna por la otra parte (o lo solicita la parte proponente de la prueba): aplicación del régimen del 326.2 LEC
   b. En otro caso: harán prueba plena
2. **Por servicio de confianza cualificado** (se encuentra en la lista de confianza de prestadores y servicios cualificados por cumplir los requisitos del Reglamento UE 910/2014): se rige por el art. 326.4 LEC
   a. **Se presumirá que el documento reúne la característica cuestionada y que el servicio de confianza se ha prestado correctamente** si figuraba, en el momento relevante a los efectos de la discrepancia, en la lista de confianza de prestadores y servicios cualificados
   b. Si aun así se impugnare el documento electrónico, la carga de realizar la comprobación corresponderá a quien haya presentado la impugnación.
      - Si dichas comprobaciones obtienen un resultado negativo, serán las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 300 a 1200 euros

PROBLEMA 2: prueba de la mensajería instantánea

PRESUPUESTOS DE PARTIDA: WHATSAPP

1. Criterios de valoración
   a. Libre valoración del juez
   b. Valoración conjunta
   c. Postura procesal de las partes (seriedad de la impugnación)
2. El PSSI no conserva contenidos (WhatsApp utiliza cifrado de extremo a extremo basado en el Signal Protocol): sí otros metadatos
   a. Para acreditar contenidos: sobre los dispositivos utilizados en la conversación
   b. Posibles copias de seguridad (backups): si el usuario activa las copias de seguridad en Google Drive (Android) o en iCloud (iPhone), el contenido de los mensajes sí se almacena en esos servicios y puede ser accesible legalmente bajo orden judicial. Pero depende de si el backup está cifrado o no.
3. Un mensaje whatsapp ha de tener acceso al proceso a través de alguno o algunos de los medios probatorios regulados por las normas procesales (pueden ser cumulativos)
4. En la práctica la prueba se fundamentará en lo que aporten dos fuentes probatorias:
   a. Por un lado, las manifestaciones de las personas que han participado de alguna forma en la misma: Testifical, Interrogatorio parte…
   b. Por otra parte, los datos contenidos en los dispositivos electrónicos usados durante la conversación: documental, pericial

	WhatsApp
Información básica	WhatsApp es la aplicación de mensajería instantánea gratuita, multiplataforma y con cifrado de extremo a extremo más utilizada en el mundo. WhatsApp está disponible para Android, iPhone, Mac y PC con Windows. Sus principales funcionalidades incluyen mensajería/chat en línea entre dos o más usuarios (chats grupales), llamadas telefónicas gratuitas por Internet, videollamadas, intercambio de archivos multimedia (imágenes, videos, audios, documentos), listas de distribución y compartición de ubicaciones. WhatsApp forma parte de la empresa Meta Platforms.

¿Cómo contactar?	• Europa:
	  ○ WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour Dublin 2, IrelandPortal
	• Solicitudes via the Law Enforcement Online Request System (LEORS):
	  ○ https://www.whatsapp.com/records/login
	• Dirección de correo electrónico para autoridades:
	  ○ records@records.whatsapp.com

Recursos de interés	• Directrices para autoridades: ○ https://faq.whatsapp.com/en/android/26000050/?category=5245250

PRESUPUESTOS DE PARTIDA: TELEGRAM

1. **Datos básicos de la cuenta**
   - Se almacenan por Telegram
   - Nombre de usuario elegido, número de móvil y foto de perfil
   - También dirección mail sólo cuando es necesaria para la verificación en dos pasos
2. **Cloud chats**
   - Almacena en sus servidores (nube) el contenido de los mensajes (contenido, fotos, vídeos y documentos) para que el usuario pueda acceder a los datos desde cualquiera de tus dispositivos en cualquier momento sin tener que depender de copias de seguridad de terceros.
   - "*Todos los datos se almacenan fuertemente cifrados y las claves de cifrado en cada caso se almacenan en varios otros centros de datos en diferentes jurisdicciones*" (política de privacidad)
3. **Secret chats** (usan cifrado extremo a extremo)
   - Todos los datos están cifrados con una clave que sólo el remitente y el destinatario conocen.
   - En sus servidores no se almacena el contenido, y tampoco ningún registro de los mensajes en chats secretos (salvo un corto periodo de tiempo).
   - Solamente se puede conocer su contenido accediendo a los dispositivos usados en la comunicación
4. **Chats públicos**
   - Telegram también admite canales públicos y grupos públicos
   - Todo lo que se publique en público será accesible para todos.
5. **Plataforma de pago**
   - "*Telegram no almacena ningún detalle de tarjeta de crédito ni información de transacciones*" (política de privacidad)

	TELEGRAM
Información básica	Telegram es una aplicación de mensajería en la nube para móviles, tabletas y ordenadores de escritorio que permite intercambiar textos, fotos, videos y archivos de cualquier tipo y tamaño. La aplicación también permite realizar llamadas de voz y video. Asimismo, ofrece a los usuarios la posibilidad de crear "chats secretos" con cifrado de extremo a extremo, el cual no está habilitado por defecto

¿Cómo contactar?	• Solicitudes de emergencia relacionadas con terrorismo:
	  ○ Telegram Messenger Inc Vistra Corporate. Services Centre, Wickhams Cay II VG1110 Road. Town, Tortola.British Virgin Islands
	• Europa (para solicitudes artículo 10 DSA):
	  ○ Telegram Messenger Inc. Avenue Huart Hamoir 71, 1031, Brussels. Belgium
	• Dirección de correo electrónico para autoridades:
	  ○ abuse@telegram.org

Recursos de interés	Consulta de la política de privacidad de Telegram: • https://telegram.org/privacy

Nivel primario: papel

Nivel intermedio: digital

Nivel intermedio superior: fe pública

Nivel avanzado: pericial

- **NIVEL PRIMARIO-DOCUMENTO EN FORMATO PAPEL**
  - imprimir los mensajes (capturas de pantalla) en formato papel
  - Se escanea el formato papel y se presenta por lexnet
- **NIVEL INTERMEDIO-DOCUMENTO EN FORMATO DIGITAL**
  - Resultado: presentación de la conversación en formato electrónico
  - Medio: Utilizar la función "exportar chat" de la aplicación whatspp + remisión por mail (archivo de texto .txt + posible inclusión de archivos multimedia)
  - También se pueden obtener capturas de pantallas de las partes relevantes de la conversación (formato .jpg) y remitirlas por mail
  - Este medio aporta una mayor eficacia porque contiene los **metadatos**
- **NIVEL INTERMEDIO SUPERIOR- DOCUMENTAL-ACTA CON FE PUBLICA (JUDICIAL O NOTARIAL)**
  - Lo que el LAJ o el Notario observa
- **NIVEL AVANZADO: PERICIAL**
  - Resultado: presentación de la conversación en el seno de una pericial
  - Medio: obtención de la conversación desde la base de datos interna del dispositivo usado en la conversación, mediante una pericial
  - Acreditación de la no manipulación

Problema de la manipulación del whatsapp

- Lo que se descarga es el estado actual de la conversación, según está almacenada en la base de datos del dispositivo
- La conversación "original" (la que se produjo realmente) puede ser manipulada mediante la modificación de la base de datos del dispositivo
  - Manipulación por usuario utilizando la propia aplicación whatsapp
  - Manipulación mediante otra aplicación (app) instalada en el dispositivo
  - Manipulación por especialista actuando sobre el dispositivo mediante ordenador conectado, actuando sobre la base de datos: no se borra el mensaje, sino que se modifica el contenido de texto de los propios registros
  - Simuladores de mensajería
- Relevancia del resto de dispositivos que intervienen en la conversación

MUCHAS GRACIAS

Linkedin:

www.linkedin.com/in/joaquín-delgado-martín