
OBSTÁCULOS EN ÓRGANOS JUDICIALES Y COMISARIAS

Transformación digital

- No es algo nuevo o aislado: Ha producido un cambio estructural en el proceso penal
- Prácticamente cualquier delito puede se cometido en el ámbito digital o guarda relación con ese mundo, lo que produce un rastro muy importante para la investigación.
- La violencia de género NO ES AJENA:
  - Han surgido nuevas formas de violencia: comportamientos abusivos, posesivos y controladores por parte de los agresores hacia sus víctimas, que se plasman en todos los espacios de su vida entre ellos las interacciones online,
  - El uso de redes sociales, aplicaciones de mensajería, videollamadas, compartición de archivos documentos es algo consustancial en nuestras vidas y ha generado que con un solo clic se pueda ejercer el control sobre la mujer,
  - La **Recomendación General núm. 1 de GREVIO, de 20 de octubre de 2021,** reconocía EL PROBLEMA GLOBAL DE LA DIMENSIÓN DIGITAL DE LA VIOLENCIA SOBRE LA MUJER, COMO ALGO CADA VEZ MÁS PREVALENTE Y DESPROPORCIONADO.

El concepto de violencia digital

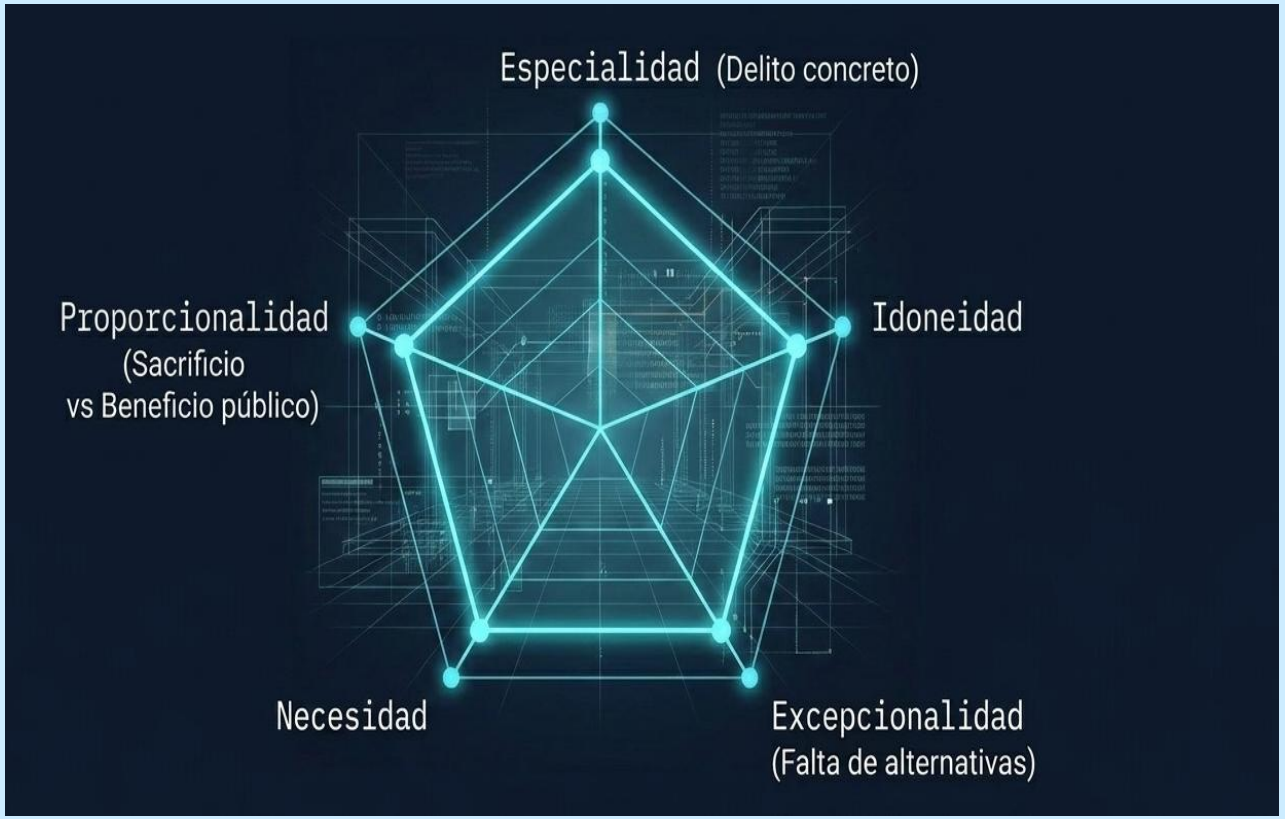
- La Ley 15/2021, de 3 de diciembre, que modifica la **Ley 11/2007, de 27 de julio, gallega para la prevención y el tratamiento integral de la violencia de género** define la violencia de género digital como una modalidad específica de violencia ejercida contra las mujeres. En la Letra h del art. 3 INCLUYE CON FORMA DE VIOLENCIA DE GÉNERO:

"Violencia de género digital o violencia en línea contra la mujer, que incluye ***todo acto o conducta de violencia de género cometido, instigado o agravado, en parte o en su totalidad, por el uso de las nuevas tecnologías de la información y la comunicación (TIC),*** *como Internet, plataformas de redes sociales, sistemas de mensajería y correo electrónico o servicios de geolocalización,* ***con la finalidad de*** *discriminar, humillar, chantajear, acosar o ejercer dominio, control o intromisión sin consentimiento en la privacidad de la víctima; con independencia de que el agresor guarde o no relación conyugal, de pareja o análoga de afectividad en el presente o en el pasado, o de parentesco con la víctima.*

Igualmente, tendrán la consideración de actos de violencia digital contra la mujer los ejercidos por hombres de su entorno familiar, social, profesional o académico".

Hitos normativos esenciales

- Las medidas de investigación tecnológicas introducidas por la **LO 13/2015, de 5 de octubre**, que marcan un antes y un después.
- Permiten que la EVIDENCIA DIGITAL se transforme en PRUEBA DIGITAL
- La normativa sienta unos principios rectores y enumera toda una serie de diligencias o medidas a las que da una regulación específica, sin que la enumeración se considere un numerus clausus.
- Artículo 588 bis a permite acordar alguna de las medidas del Capítulo IV (artículo 588 bis a) a 588 octies) SIEMPRE QUE MEDIE AUTORIZACIÓN JUDICIAL con sujeción a los **CINCO PRINCIPIOS RECTORES**:



Marco Normativo y Canon de validez

- Especialidad – idoneidad- excepcionalidad- necesidad y proporcionalidad.
- No basta una sospecha anímica SE REQUIEREN indicios objetivables, NO SE INVESTIGA PARA VER QUE SE ENCUENTRA
- PROHIBICIÓN DE INVESTIGACIÓN PROSPECTIVA

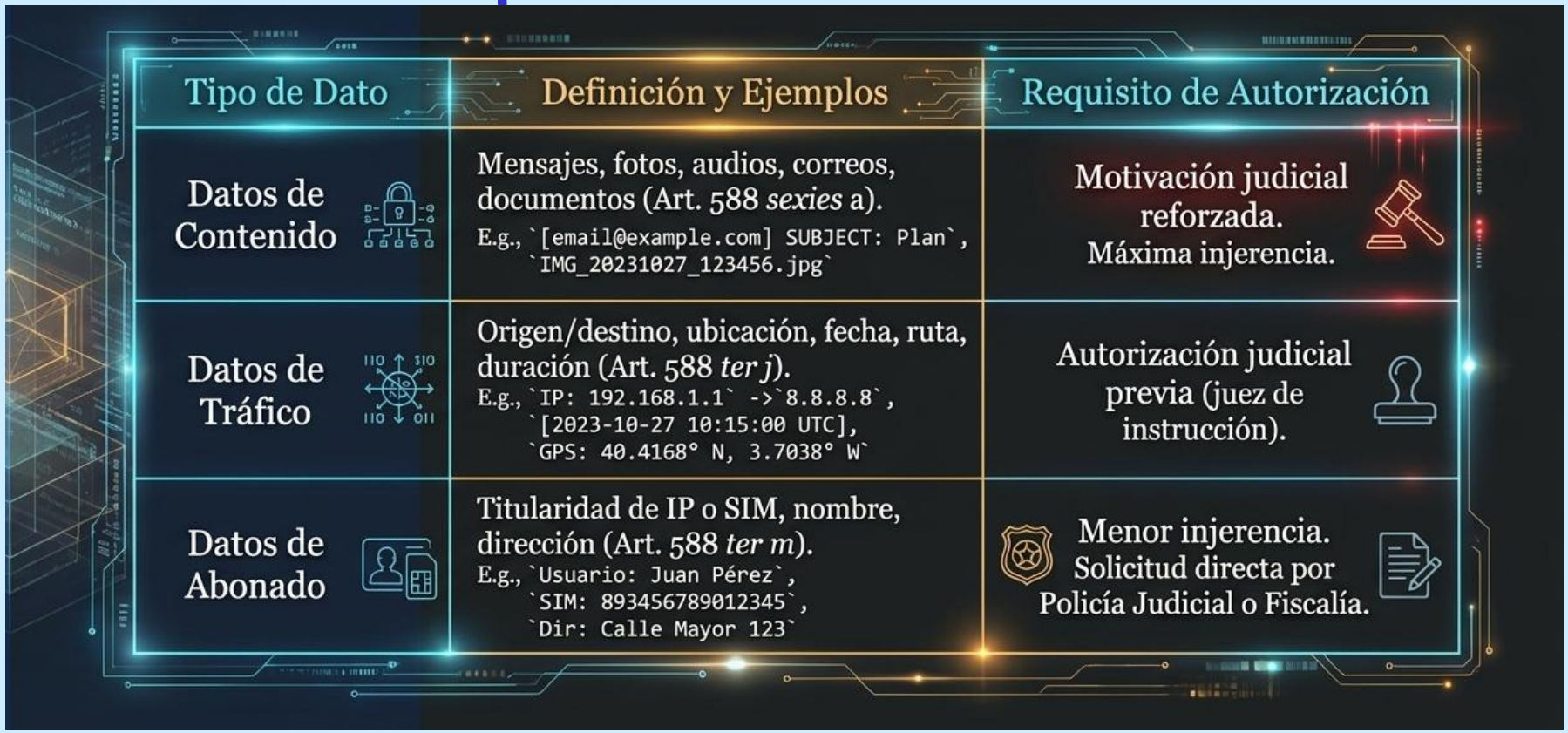
STC 167/2002

No se puede desvelar el secreto de las comunicaciones para "ver qué se encuentra". Se exigen indicios objetivables accesibles a terceros, no meras suposiciones o conjeturas de la existencia del delito o de su posible comisión.

Debe existir una **vinculación real** de la persona sobre la que se adopta la medida con el hecho investigado.

Marco normativo y canon de validez

- JUICIO DE PROPORCIONALIDAD.- El nivel de autorización depende directamente de la profundidad de la injerencia en los derechos fundamentales.



STS 753/2024, 22 de julio.- La simple obtención de un numero asociado a una tarjeta prepago no interfiere en la comunicación, porque ésta no se ha entablado. No afecta al art.18.3 CE. Se trata de un dato desvinculado de los procesos de comunicación. Se admite su sacrificio sin necesidad de autorización judicial.

Recogida de evidencias

- La recogida de las evidencias NO puede ser aleatoria, nos puede proporcionar información relevante que vincule al investigado con los delitos cometidos y proporcionar pruebas para el enjuiciamiento.
- La evidencia digital tiene una naturaleza volátil o deleble, intangible, alterable, duplicable, heterogénea y, a menudo, intrusiva y anónima. Esta fragilidad exige un rigor técnico-legal en su obtención que, si falla, puede viciar años de investigación.
- En los protocolos internacionales destaca como norma básica **ISO/IEC 27037:2012 Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital**, nos permite manejar la evidencia digital de forma correcta, segura y legal.
  - **Principios:** Relevancia (para la vinculación sospechoso con delito y victima, capacidad de esclarecimiento) – Confiabilidad (las técnicas utilizadas han debido ser probadas, requieren unos test de eficiencia y eficacia) – Suficiencia (la recolección de evidencias debe estar enfocada a la investigación y debe ser rigurosa, analizar la totalidad de los dispositivos y confirmar su no alteración)
  - **Fases:** Identificación – Recogida – Adquisición- Preservación

Fases críticas de la adquisición de evidencias

1. IDENTIFICACIÓN
Localizar fuentes físicas (móviles, ordenadores…) y lógicas (nube).

2. RECOGIDA Y ASEGURAMIENTO.
Aislar el dispositivo. Evitar accesos de personal no autorizado e impedir accesos remotos (uso de bolsas de Faraday y modo avión).

3. ADQUISICIÓN.
Fase más crítica. Extracción de información para su reproducción o verificación.

4. PRESERVACIÓN.
Mantenimiento absoluto de la inalterabilidad de los datos hasta el plenario.

Clonado	Imagen Lógica (Estándar)	Volcado Selectivo
Réplica bit a bit. Genera soporte arrancable (disco idéntico). No requiere intervención del LAJ in situ, pero exige estricta cadena de custodia.	El estándar forense preferido (formatos .dd o .E01). Comprime, cifra y permite recuperar archivos borrados manteniendo la geometría exacta del disco original.	Extracción específica. Estrictamente necesario en grandes servidores donde la copia total es inabarcable técnica y legalmente.

Cadena de custodia

- Es la garantía de que lo que se presenta en el plenario es lo que se intervino en la escena, sin alteraciones ni contaminaciones.
  - **El ADN Digital o Función Hash:** El uso de algoritmos matemáticos como SHA256 es el instrumento técnico básico para acreditar la mismidad e integridad del dato. Debe calcularse antes y después de cualquier volcado o clonado, reflejándose obligatoriamente en el acta judicial o policial para detectar cualquier alteración. Propiedades clave: La unidireccionalidad y el efecto avalancha
  - **Cometido del LAJ:** Doctrina consolidada (SS TS 957/2013, 17 diciembre y 342/2013, de 17 de abril) establece que la presencia del LAJ en volcados técnicos no es un requisito de validez. Se consideran una prueba pericial especializada, no una inspección ocular tradicional.
  - **Manipulación Abstracta:** STS 1077/2025, de 16 de enero de 2026, la mera posibilidad teórica o "en abstracto" de que una prueba digital sea manipulable no es motivo suficiente para descalificarla. Los déficits en la cadena de custodia no suelen generar nulidad (utilizabilidad), sino que afectan a su valoración (fiabilidad).
  - **Importancia del Informe Pericial Informático:** Para garantizar la eficacia legal de la prueba ante impugnaciones, es fundamental la emisión de informes por expertos informáticos (públicos o privados).

Valor probatorio de pantallazos, metadatos y registros.- TS

- **PRONUNCIAMIENTOS MÁS DESTACADOS:**

- **1.-Prueba Personal Documentada:** STS 300/2015, 12 diciembre, los pantallazos de WhatsApp o redes sociales NO son documentos a efectos de casación, SON PRUEBAS PERSONALES DOCUMENTADAS que requieren la ratificación de los intervinientes.

- **2.- Impugnación de autenticidad:** La impugnación genérica no es suficiente para invalidar la prueba, no existe una presunción de falsedad de la mensajería digital. Si la defensa aporta sospechas concretas se invierte la carga de la prueba y la acusación esta obligada a proponer pericial informática. STS 116/2025, de 13 de febrero *"haberse impugnado por la existencia de sospechas o indicios de manipulación, pero no de forma genérica y retóricamente"*, insisten STS 603/2025, de 1 de julio y 629/2015, de 3 de julio.

- **3.- Importancia de los metadatos:** A menudo son más valiosos que el texto. Permiten trazar la creación de archivos Word, la geolocalización de fotos o el terminal de origen de un mensaje. Historia real del archivo.

Valor probatorio de pantallazos, metadatos y registros.- TS

- **PRONUNCIAMIENTOS MÁS DESTACADOS:**

- **4.- Registros de dispositivos:** Exige motivación individualizada. STS 254/2026, de 26 de enero, si hay auto previo de entrada y registro y ocupación ADMITE PROVIDENCIA sin repetir motivación. Acceso a SIM o IP puede pedirse directamente por Policía o Fiscalía -588 ter m) y STJUE 2 octubre 2018-. Dispositivos incautados fuera de registro precisas consentimiento o autorización.

- **5.- Consentimiento al registro dispositivo:** Sobre consentimiento STS 864/2015, de 10 de diciembre (padres de menor a perfil Facebook) y 462/2019, de 14 de octubre (titular dispositivo). Garantías del consentimiento: libre, documentado y asistencia letrada. En caso de dispositivo de tercero: si es mero depositario consentimiento también de interviniente.

- **6.- Datos de GPS en vehículos:** STS 835/2022, de 21 de noviembre obtención de datos GPS de vehículos de alquiler se considera una injerencia de menor intensidad que no siempre requiere autorización judicial previa, según modelos avalados por el. TEDH

Valor probatorio de pantallazos, metadatos y registros.- TS

- **PRONUNCIAMIENTOS MÁS DESTACADOS:**

- **7.- Registros remotos:** Autorización previa -588 septies a) solo para delitos del precepto entre los que se incluyen delitos cometidos a través de instrumentos informáticos. Medida muy invasiva motivación reforzada y proporcionalidad medida. Puede llevarse a cabo utilizando contraseñas de investigado obtenidas en el curso de la investigación o mediante instalación de herramientas que permitan acceso remoto (sin que propietario lo conozca).

- **7.- Acceso al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI:** Art. 588 ter l) permite a Policía Judicial códigos de identificación o etiquetas técnicas del aparato de telecomunicación sin necesidad de una previa resolución judicial directamente o utilizando artificios técnicos. STS 184/2022, 24 de febrero *"otra, muy distinta, que su conocimiento pueda obtenerse de forma coactiva de los titulares del aparato de telecomunicación".* Identificados códigos puede solicitar del juez datos de trafico y datos de contenido.

OBSTÁCULOS, PROBLEMAS Y ERRORES

- **1.- Mandamientos a operadores erróneos:** Es frecuente enviar oficios con solo el "nickname" (nombre de usuario), que es un dato variable. Es imperativo incluir la URL del perfil y el ID numérico único e invariable, además de la fecha y hora en formato UTC de la conversación o envío. LAS OPERADORAS/PRESTADORAS requieren exactitud.

- **2.- Cooperación internacional:** El 80% de los datos digitales residen en servidores de EEUU, las comisiones rogatorias tardan una media de 10 meses lo que colisiona con el LÍMITE DE LA INSTRUCCIÓN (324 LECR). ACCIONES CONVENIENTES: a) Petición de conservación de datos, es además un trámite obligatorio en EEUU, b) Declarar compleja la causa (protegemos necesidad otras diligencias) o sobreseimiento provisional o archivo hasta respuesta, manteniendo medidas cautelares si existen

OBSTÁCULOS, PROBLEMAS Y ERRORES

- **3.- Drones y vigilancias:** La captura de imágenes con drones en domicilios o lugares privados sin orden judicial es nula por vulnerar la expectativa razonable de privacidad (STS 329/2016, de 20 de abril (prismáticos), STC 92/2023, de 11 de septiembre (garaje) y STS 797/2025, 2 de octubre). La expectativa no desaparece aunque el titular no haya reforzado los elementos de exclusión de su propiedad.

- **4.- Retirada de contenidos. Modificación del 13 LEC** por LO 10/2022 *"podrá acordar, como primeras diligencias, de oficio o a instancia de parte, las medidas cautelares consistentes en la retirada provisional de contenidos ilícitos, en la interrupción provisional de los servicios que ofrezcan dichos contenidos o en el bloqueo provisional de unos y otros cuando radiquen en el extranjero".* También 189.8 CP en pornografía infantil.

  - **El mandamiento de ejecución de la retirada al PSSI debe ser MUY PRECISO:** identificación URL, ID numérico, precisión temporal (fecha y hora exacta (en formato UTC preferiblemente sino indicarlo) y descripción clara del hecho investigado.

  - **Reglamento de Servicios Digitales (DSA) o Reglamento (UE) 2022/2065**, aplicable desde el 17 de febrero de 2024, es fundamental para el bloqueo y retirada de contenidos, ya que establece un marco de responsabilidad y cooperación obligatoria para los prestadores de servicios de intermediación

  - Canal Prioritario de la Agencia Española de Protección de Datos (AEPD)

OBSTÁCULOS, PROBLEMAS Y ERRORES

- **5.- Conversaciones víctima e investigado (pantallazos):** Conveniencia de aportar, además del pantallazo, la transcripción y la comprobación de los números de teléfono entre los que se realiza (identificar usuario-número teléfono), cotejo LAJ o acta notarial.

- **6.- Grabaciones de conversaciones o notas de voz intercambiadas entre las partes:** Aportar en formato electrónico audible (que se pueda reproducir a posteriori en juicio en unas mínimas condiciones) y si es posible transcribir para cotejo.

- **7.- Conversaciones o transmisiones de información por teléfono:** Lo optimo es que se deje el teléfono desde un momento inicial a disposición del órgano.

  - Motivo: hacer constar datos terminal, vía de la comunicación, nombres titular y usuario, perfiles, números asociados, datos de terceros intervinientes en caso de conversaciones múltiples, fecha y hora de la conversación, archivos adjuntados.

  - Cotejo por LAJ o acta notarial si la aporta la parte.

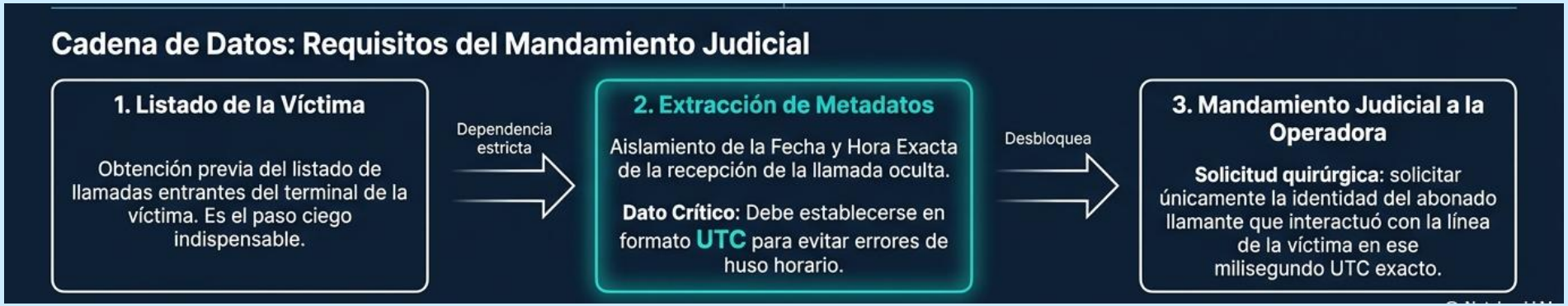
  - No importa que conversación sea subrepticia si es grabada por uno de los interlocutores STS 753/2024, 22 junio, **214/2018, de 8 de mayo.**

OBSTÁCULOS, PROBLEMAS Y ERRORES

- **8.- Datos asociados al proceso de comunicación:** Es habitual su petición en delitos de acoso o quebrantamiento.
  - **Datos de comunicación y tráfico:** Incluyen la determinación de números de origen y destino, fecha, hora, duración de llamadas o mensajes (SMS/MMS), direcciones IP y códigos como el IMSI. Salvo datos de abonado exigen autorización judicial. Son los clásicos listados de llamadas entrantes y salientes.
  - **Flexibilidad en el ámbito delictivo:** Tras la reforma 2015, la interceptación de estos datos no se reserva únicamente a delitos "graves" (penas superiores a tres años conforme al artículo 579.1); es suficiente que el ilícito se cometa mediante instrumentos informáticos o cualquier tecnología de la información y comunicación (Art. 588 ter a)
  - **Juicio de proporcionalidad:** A pesar de la apertura a delitos de menor gravedad penal, toda medida de este tipo debe estar estrictamente motivada y superar el juicio de proporcionalidad, especialidad, idoneidad y necesidad
  - **Identificación IP (Art. 588 ter k):** Cuando la Policía Judicial detecta una dirección IP vinculada a un delito pero carece de los datos del usuario o la localización del equipo, debe solicitar al juez de instrucción que requiera a los prestadores de servicios la cesión de la información identificativa
  - **Deber de colaboración:** Los prestadores de servicios (PSSI) tienen la obligación legal de colaborar con las autoridades judiciales y policiales para facilitar los datos técnicos y de suscripción que permitan identificar al sospechoso

OBSTÁCULOS, PROBLEMAS Y ERRORES

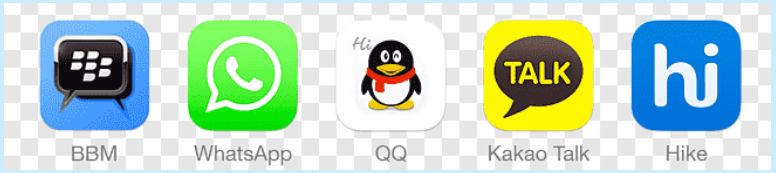
- **9.- Llamadas con números ocultos o privados:**
  - **Necesaria autorización judicial.-** El 588 ter m) permite que la Policía Judicial y el Ministerio Fiscal soliciten la titularidad de un número conocido sin autorización judicial (Art. 588 ter m), la situación cambia cuando el número es oculto o privado. NO ES EL MISMO CASO. Si la victima consiente acceso a sus registros la motivación del auto es más sencilla.
  - **Juicio de proporcionalidad,** existencia de indicios de que con la llamada se comete un delito, sopesar injerencia.
  - **Mandamiento judicial:**

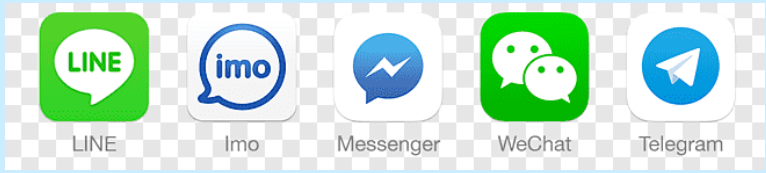


  - **Llamadas de número desconocido de WhatsApp:** El proceso de identificación es más complejo, aportación móvil y cotejo por LAJ, transcripción de mensajes o llamadas y pantallazos del terminal, horario y duración. En caso de impugnación por defensa pericial informática que identifique origen e identidad

OBSTÁCULOS, PROBLEMAS Y ERRORES

- **10.- Mensajería instantánea (WhatsApp, Telegram, Line, etc.):**





- **TIPO DE COMUNICACIÓN:** Comunicación entre usuarios, pero también el intercambio de fotos, documentos, videos e incluso mensajes de voz; comunicación bilateral y multilateral. Operan sobre red de datos (protocolo TCP/IP)

- **IDENTIFICACIÓN DEL USUARIO:** a través del número teléfono móvil. Opera tanto por red móvil como por wifi, algunas se pueden sincronizar en PC

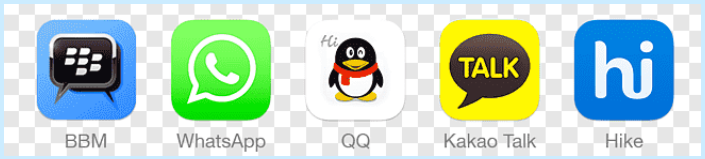
- **DÓNDE SE ALOJA LA INFORMACIÓN:** No existe un servidor externo que conserve la información sobre los contenidos de los mensajes, sino que la misma se encuentra alojada - generalmente una vez ha sido encriptada- en las bases de datos alojadas en los propios dispositivos utilizados para llevar a efecto la transmisión o, en su caso, accesibles desde los mismos cuando se haya configurado la aplicación para hacer copias en la nube.

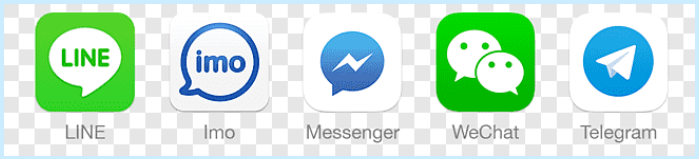
- **QUÉ INFORMACIÓN PODEMOS SOLICITAR DEL PROVEEDOR DEL SERVICIO:** datos de tráfico 588 ter j LECR, los administradores de las aplicaciones sólo conservan datos de tráfico y abonado.

- **ACREDITACIÓN CONVERSACIÓN** x comprobación dispositivo de la transmisión. Indagar si estamos ante comunicaciones bidireccionales o de grupo. Copias de seguridad.

OBSTÁCULOS, PROBLEMAS Y ERRORES

- **10.- Mensajería instantánea (WhatsApp, Telegram, Line, etc.):**





  - **FORMA DE APORTACIÓN:** STS 332/2019, 27 junio (pantallazos, acta notarial, cotejo= 46/2019, 1 febrero (consecuencia de q no son documentales).

  - **JOAQUIN DELGADO nos da una escalera de valores:**

OBSTÁCULOS, PROBLEMAS Y ERRORES

- **11.- Mensajes SMS (Short Message Service) o mensajería multimedia MMS (Multimedia Messaging Service):**
  - **TIPO DE COMUNICACIÓN:** servicios prestados por los operadores de telefonía móvil a través de una red privada para el envío de textos cortos o contenidos multimedia. Están diseñados principalmente para comunicaciones bidireccionales.
  - **IDENTIFICACIÓN DEL USUARIO:** a través del número teléfono móvil.
  - **DÓNDE SE ALOJA LA INFORMACIÓN:** A diferencia de la mensajería instantánea, aquí interviene directamente el operador en el proceso de transmisión, el centro de servicio se encarga de comprobar si el receptor destinatario está operativo, almacenando temporalmente, por el tiempo mínimo imprescindible, el envío hasta que esta circunstancia se produce..
  - **QUÉ INFORMACIÓN PODEMOS SOLICITAR DEL PROVEEDOR DEL SERVICIO:** datos de tráfico 588 ter j LECR y 6 y 7 de la Ley 25/2007, de 18 de octubre. Solo conservan datos de tráfico (por un año) y abonado.
  - **ACREDITACIÓN CONVERSACIÓN** x comprobación dispositivo de la transmisión. Si el mensaje se ha borrado puede estar en la memoria del terminal pero se precisan utilizar técnicas forenses adecuadas.

OBSTÁCULOS, PROBLEMAS Y ERRORES

12.- Correo electrónico:

- **TIPO DE COMUNICACIÓN: :** Permite el intercambio de mensajes de texto y también de la documentación digital por adjuntos (imágenes, videos, documentos); puede dirigirse a una sola persona o a una pluralidad de personas simultáneamente que se hacen figurar como destinatarios de un mismo correo o que figuran en copia o en copia oculta.

- **DÓNDE SE ALOJA LA INFORMACIÓN:** El correo remitido se recoge por el servidor MTA (Mail Transfer Agent) del usuario emisor, que se encarga de trasladarlo al servidor de correo entrante MDA (Mail Delivery Agent) del usuario destinatario. Este último almacena el correo electrónico en tanto el usuario lo acepta. Por ello, cuando se utilice este medio de trasmisión, es posible localizar copia del mensaje enviado no solo en poder del usuario remitente y del usuario receptor, sino también en los respectivos servidores de envío y de recepción, dependiendo de los criterios establecidos sobre almacenaje de cada proveedor (si lo conservan los que utilizan protocolos IMAP)

- **QUÉ INFORMACIÓN PODEMOS SOLICITAR DEL PROVEEDOR DEL SERVICIO:** datos de abonado tráfico y de contenido, 588 ter j) y Comisión Rogatoria.

- Se pueden solicitar los datos de apertura de la cuenta (fecha, hora, titular, cuenta asociada), IP de creación, IP de las conexiones que han accedido a esa cuenta de correo electrónico. Averiguada la IP, ex 588 ter k) se solicita a la proveedora de acceso (Compañías telefónicas: Movistar, Orange, Vodafone) la titularidad de la línea telefónica a la que está asociada la IP.

OBSTÁCULOS, PROBLEMAS Y ERRORES

13.- Comunicación por redes sociales (Facebook, Tuenti, Google+, Twitter X, Instagram, Tik tok,...):

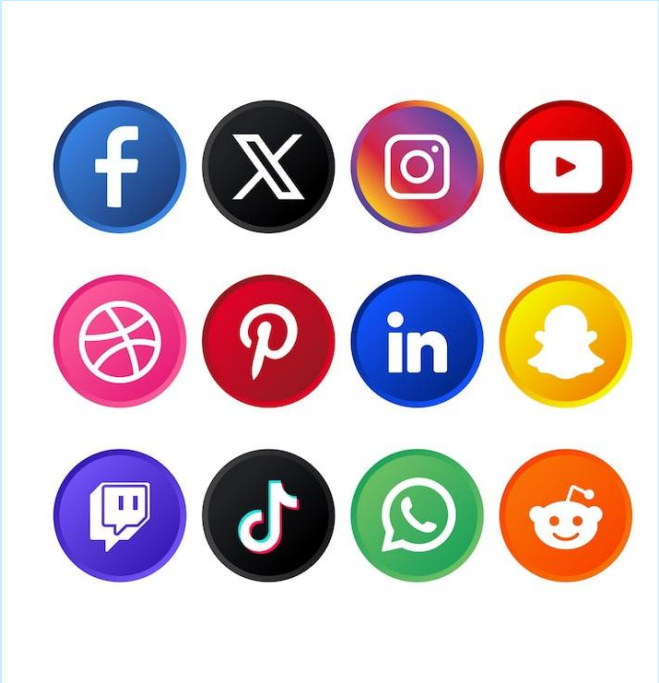
- **TIPO DE COMUNICACIÓN:** : Los usuarios aportan y publican ideas, imágenes, datos o contenidos multimedia, que quedan almacenados en inmensas bases de datos gestionadas por los correspondientes administradores, y son accesibles a determinadas comunidades de usuarios, respecto de las que se pueden establecer determinados niveles de aceptación o accesibilidad (amigos/amigos de amigos/ público). TODO LO QUE EL USUARIO VUELCA O SUBE QUEDA ALMACENADO

- **IDENTIFICACIÓN DEL USUARIO:** cuenta de usuario, información de registro que incluye: nombre, dirección de correo electrónico, fecha de nacimiento y sexo, y en algunos casos un número de teléfono. En casos, se puede recuperar aunque el contenido se retire o el usuario se de baja (depende política conservación)

- **DÓNDE SE ALOJA LA INFORMACIÓN:** Permanece en las bases de datos del servidor en tanto en cuanto el usuario no decida borrarlas, bien por una acción voluntaria , bien por causar baja en la comunidad

- **QUÉ INFORMACIÓN PODEMOS SOLICITAR DEL PROVEEDOR DEL SERVICIO:** Datos de tráfico y de contenido- 588 ter j) LCR + Comisión Rogatoria. Conveniente solicitar preservación de la información (OCD 588 octies 90 días prorrogable a 180)

- **INDAGACIÓN ESENCIAL:** Nick, URL, ID, horas de publicación, nivel de privacidad del usuario (tanto por nivel de difusión como por acceso a la evidencia si la víctima no la tiene)



OBSTÁCULOS, PROBLEMAS Y ERRORES

- **14.- Anuncios en páginas web:**
  - **INDAGACIÓN:** Obtener del denunciante los datos concretos del anuncio, fecha y hora de la publicación y averiguar IP del autor de la inserción; averiguada IP, solicitar ex art 588 ter k) la titularidad de la línea telefónica a la que estaba asignada la dirección IP.
- **15.- Aplicaciones para citas como Tinder, Grinder, Hinge, Match.com:**
  - **INDAGACIÓN:** Obtener del denunciante los datos concretos del anuncio, fecha y hora de la publicación y averiguar IP del autor de la inserción; averiguada IP, solicitar ex art 588 ter k) la titularidad de la línea telefónica a la que estaba asignada la dirección IP.
- **16.- Que pasa si no cumplimos plazos del 588 bis c):**
  - **PLAZO DE 24 HORAS:** Dificultad de cumplimiento en SVM de TI. Cuenta desde que se presente solicitud.
  - **STS 463/2020, de 21 de septiembre** "el citado plazo no tiene naturaleza esencial, como lo demuestra el hecho de que el mismo es susceptible de interrupción" (ni se especifica en el precepto el plazo de la interrupción) "no toda infracción o irregularidad procesal implica indefensión con relevancia constitucional" y mantiene la misma argumentación para el preceptivo informe del Ministerio Fiscal emitido fuera del plazo de veinticuatro horas.

OBSTÁCULOS, PROBLEMAS Y ERRORES

- **17.- Problemática en la identificación IP y si el investigado alega que le han suplantado la identidad:**
- **La IP NO ES IGUAL A USUARIO**

OBSTÁCULOS, PROBLEMAS Y ERRORES

- **17.- Problemática en la identificación IP y si el investigado alega que le han suplantado la identidad: COMPLEJIDAD MAYOR SI UTILIZA VPN**
- **Enmascaramiento:** Cifra la comunicación y sustituye la dirección IP real por la del servidor, rompiendo el vínculo directo entre la actividad delictiva y la ubicación física del investigado. Genera un rastro "zigzagueante" difícil de seguir. Los delincuentes aprovechan proveedores que no conservan registros (logs) o se ubican en jurisdicciones que no colaboran con las autoridades españolas, creando "paraísos de impunidad tecnológica". COOPERACIÓN INTERNACIONAL LENTA.
- **Estrategia de Defensa y Suplantación:** "Robo de Cuenta": El investigado suele alegar que un tercero obtuvo sus claves (mediante phishing o robo de credenciales) y utilizó una VPN para cometer el delito desde una ubicación distinta, simulando su identidad
- **Necesidad de la Prueba Pericial Avanzada:** Más allá de la IP, para desmontar la defensa del robo de cuenta, es obligatorio realizar un análisis forense especializado del hardware del sospechoso. Búsqueda de Evidencias: Se deben localizar restos de la sesión, metadatos o registros de sistema que confirmen que el acceso se realizó efectivamente desde el dispositivo controlado por el investigado.

OBSTÁCULOS, PROBLEMAS Y ERRORES

- **18.- Problemática de manipulación de conversaciones WhatsApp y otras mensajerías:**
  - Al exportar un chat de WhatsApp lo que se obtiene es el estado actual de la conversación, tal y como está guardada en la base de datos del dispositivo en ese momento. Esto implica que no necesariamente refleja de forma fiel la conversación original tal y como se produjo, sino la versión existente tras posibles alteraciones. La conversación "original" puede o pudo ser objeto de manipulación mediante la modificación de dicha base de datos.

- **Posibles alteraciones:**

Manipulación del usuario: El uso de las funciones nativas de WhatsApp para editar o eliminar mensajes, cambiando lo que es visible en la pantalla

Aplicaciones de intervención: Empleo de software externo diseñado para modificar datos almacenados localmente en el dispositivo.
Modificación técnica de bases de datos: Acceso avanzado mediante un ordenador para alterar directamente los registros internos del terminal, permite cambiar el contenido de un mensaje.

Simuladores de conversaciones: El uso de herramientas como WhatFake o Yazzy para crear chats completamente ficticios que aparentan ser reales.

- **SOLUCIONES:** Contenido demás dispositivos, copias guardadas en cada terminal, contexto de la totalidad conversación, pericial.

MUCHAS GRACIAS A TODOS Y TODAS

TERESA CORTIZAS

PRESIDENTA AUDIENCIA PROVINCIAL A CORUÑA