#LOVIRTUALESREAL

GUÍA DE **INVESTIGACIÓN DE CASOS DE VIOLENCIA DE GÉNERO** FACILITADA POR LA TECNOLOGÍA (VG FT)

PROYECTO:
CONECTADAS Y LIBRES DE VIOLENCIA

Por: Heidy Gil
Adriana Pérez Tudela

BICENTENARIO DE BOLIVIA · AGETIC Digitalizando Bolivia · ESTADO PLURINACIONAL DE BOLIVIA · INTERNET BOLIVIA.ORG · Asociación Aguayo · Cooperación Española BOLIVIA · ONU MUJERES

Créditos

- **PUBLICADO POR:**
  Fundación InternetBolivia.org/Asociación Aguayo
  ONU Mujeres
  AGETIC
- **FINANCIADO POR AECID**
- **ELABORADO POR:**
  Heidy Gil
  Adriana Pérez Tudela
- **EQUIPO CONSULTOR:**
  Lu An Méndez
  Narayani Rivera
  Tania Oroz
  Doris Quispe
- **EQUIPO DE COMUNICACIÓN:**
  Lisette Balbachán
  Juan Luis Gutiérrez
  Sabrina Lanza
- **DISEÑO Y DIAGRAMACIÓN:**
  Marcelo Lazarte
- **COORDINACIÓN DE PROYECTO:**
  Eliana Quiroz G.

La presente publicación ha sido elaborada en el marco del proyecto *Conectadas y Libres de Violencia,* financiado por AECID e implementado por Fundación InternetBolivia.org, Asociación Aguayo y ONU Mujeres en coordinación con AGETIC.

La Paz – Bolivia, enero 2025

Puedes acceder a material multimedia de este documento ingresando al código QR.
Te acompañamos al ingreso de un espacio digital seguro.

¿DÓNDE ESTÁ MI CELULAR?
CASOS REALES DE LA VIDA DIGITAL

Si deseas acceder a más recursos puedes ingresar al sitio web del proyecto:
www.internetbolivia.org/**donde-esta-mi-celular**

#LOVIRTUALESREAL

#LOVIRTUALESREAL

GUÍA DE **INVESTIGACIÓN DE CASOS DE VIOLENCIA DE GÉNERO** FACILITADA POR LA TECNOLOGÍA (VG FT)

PROYECTO:
CONECTADAS Y LIBRES DE VIOLENCIA

Por: Heidy Gil
Adriana Pérez Tudela

BICENTENARIO DE BOLIVIA · AGETIC Digitalizando Bolivia · ESTADO PLURINACIONAL DE BOLIVIA · INTERNET BOLIVIA.ORG · Asociación Aguayo · Cooperación Española Bolivia · ONU MUJERES

Índice

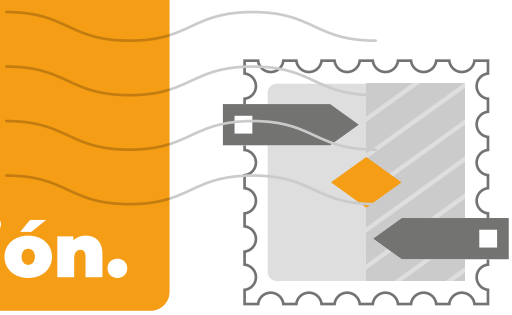
Acrónimos

CDH: Consejo de Derechos Humanos.
CIDH: Corte Interamericana de Derechos Humanos.
CEDAW: Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer.
CPP: Código de Procedimiento Penal.
CPE: Constitución Política del Estado.
DNA: Defensoría de la Niñez y la Adolescencia.
DS: Decreto Supremo.
IDH: Interamericano de Derechos Humanos.
IDIF: Instituto de Investigaciones Forenses.
IITCUP: Instituto de Investigaciones Técnico Científicas de la Universidad Policial.
FELCC: Fuerza Especial de Lucha Contra el Crimen.
FELCV: Fuerza Especial de Lucha Contra la Violencia.
NNA: Niño, Niña, Adolescente.
ONU: Organización de las Naciones Unidas.
PIDCP: Pacto Internacional de Derechos Civiles y Políticos.
SLIM: Servicios Legales Integrales Municipales.
TCP: Tribunal Constitucional Plurinacional.
TIC: Tecnologías de la Información y la Comunicación.
VG FT: Violencia de Género Facilitada por la Tecnología.

Glosario

- **Acoso Digital:** Conjunto de conductas reiteradas y no deseadas que incluyen insultos, amenazas, mensajes no solicitados y contenido ofensivo en plataformas digitales.
- **Ciberacoso:** Forma de violencia digital que utiliza plataformas tecnológicas para intimidar, humillar o amenazar a las víctimas de manera repetitiva.
- **Código Penal:** Normativa legal que define los delitos y sanciones en el marco jurídico de un país.
- **Convención Americana sobre Derechos Humanos (Pacto de San José):** Instrumento internacional que garantiza los Derechos Humanos fundamentales en los Estados miembros, incluyendo el derecho a la reparación.
- **Daño emergente:** El daño emergente se refiere a las pérdidas directas e inmediatas que sufre la víctima como resultado de un acto ilícito.
- **Daño moral:** Afectación emocional, psicológica o social reconocida como un perjuicio significativo para la víctima.
- **Doxing:** Divulgación no autorizada de información personal o confidencial de una persona, generalmente con la intención de acosarla, amenazarla o dañarla.
- **Grooming (engatusamiento pederasta):** Engaño y manipulación de menores a través de medios digitales con fines de abuso sexual o explotación.
- **Lucro cesante:** Ingresos que la víctima deja de percibir debido al acto ilícito.
- **Medidas de protección:** Acciones cautelares adoptadas para salvaguardar la integridad física de las víctimas de violencia, como la prohibición de comunicación, el retiro de contenido en línea y la restricción de acercamiento.
- **Reparación integral del daño:** Principio jurídico que busca restituir a la víctima a la situación previa a la violación de sus derechos, a través de medidas económicas, rehabilitación, satisfacción, y garantías de no repetición.
- **Reparación transformadora:** Enfoque que no sólo busca indemnizar a la víctima, sino también transformar las estructuras que perpetúan la violencia o la desigualdad, promoviendo cambios sociales y culturales duraderos.
- **SLIM (Servicio Legal Integral Municipal):** Instituciones locales encargadas de atender y proteger a mujeres en situaciones de violencia de género.
- **Violencia de Género Facilitada por la Tecnología (VG FT):** Cualquier acto cometido, asistido, agravado o amplificado por el uso de Tecnologías de Información y Comunicación (TIC) u otras herramientas digitales, que cause daño en diversos aspectos como físico, sexual, psicológico, social, político o económico a mujeres y niñas.

1. Introducción.



La investigación de casos de Violencia de Género facilitada por la Tecnología (VG FT) en Bolivia se enfrenta a una falta de normativa además de herramientas para la colección y custodia de las pruebas digitales que no tienen las mismas características de las pruebas físicas.

Los desafíos que presentan los procesos de investigación de casos de VG FT para abogados, fiscales y otros operadores de justicia derivan de la naturaleza de las pruebas involucradas que son altamente volátiles y susceptibles de ser destruidas o modificadas. Además, la identificación del agresor a menudo se complica debido al anonimato que es posible ejercer en espacios digitales, por lo que suele implicar la colaboración con empresas proveedoras de servicios digitales nacionales e internacionales y el uso de herramientas de rastreo tecnológico. Finalmente, otro de los retos es la rapidez con la que se difunden los contenidos en los entornos digitales.

La *Guía de investigación de casos de Violencia de Género Facilitada por la Tecnología (VG FT)* tiene como propósito proporcionar herramientas y directrices fundamentales para enfrentar la investigación de los delitos asociados con la violencia de género en el entorno digital, un fenómeno cada vez más presente en Bolivia. A lo largo de esta guía, se abordan aspectos esenciales para la comprensión y la investigación de estos delitos, tales como el marco jurídico nacional e internacional, las tipologías específicas de violencia digital, y las herramientas necesarias para la recolección y preservación de pruebas digitales. El enfoque está orientado a la prevención y a la atención efectiva de casos de VG FT, con un énfasis especial en la importancia de adaptar los procedimientos legales y técnicos a los retos que impone la digitalización.

Con ello, se busca ofrecer una herramienta que fortalezca la labor de los operadores de justicia y la sociedad en su conjunto para garantizar una vida libre de violencia a las mujeres y niñas, especialmente en el contexto digital.

La presente guía forma parte de una serie de tres guías y un manual acerca de VG FT en Bolivia que están dirigidas principalmente al sector público, aunque también a la sociedad civil, sector privado y academia, con la intención de aportar a la elaboración de una política pública que asegure justicia y reparación a las víctimas. Los cuatro documentos son resultado del Proyecto Conectadas y libres de violencia financiado por la Agencia de Cooperación Española AECID y ejecutado por ONU Mujeres, la Fundación InternetBolivia.org, la Asociación Aguayo en colaboración con la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) del Ministerio de la Presidencia de Bolivia.

Las otras dos guías están orientadas a la medidas de protección y reparación del daño de VG FT y al acompañamiento por parte de la sociedad civil a víctimas de VG FT, además el manual orienta las acciones de denuncia de casos de VG FT. Les invitamos a consultar este material en el sitio www.internetbolivia.org/donde-esta-mi-celular

2. ¿QUÉ ES LA VIOLENCIA DE GÉNERO FACILITADA POR LA TECNOLOGÍA (VG FT)?

La VG FT se refiere a conductas violentas que emplean tecnologías digitales como herramientas para acosar, controlar, humillar, amenazar o intimidar a las víctimas. Este tipo de violencia abarca un amplio rango de acciones que se realizan mediante dispositivos electrónicos, plataformas en línea, redes sociales, aplicaciones móviles, correos electrónicos, entre otros medios digitales, y que agravan o amplifican formas tradicionales de violencia de género.

Entre las manifestaciones comunes de la VG FT se incluyen el ciberacoso, la difusión no consentida de imágenes íntimas, la extorsión, el control y monitoreo digital, y la seducción y engaño pederasta a Niñas, Niños y Adolescentes (Grooming). Este tipo de violencia puede afectar diferentes aspectos de la vida de las víctimas, generando daños físicos, psicológicos, sociales, económicos y políticos.

La rápida digitalización y el acceso masivo a Internet han contribuido a la expansión de estas prácticas, permitiendo que los agresores utilicen el anonimato, la inmediatez y el alcance global de las plataformas digitales para perpetuar estas formas de violencia. Esta situación es especialmente preocupante ya que, a diferencia de la violencia física, la VG FT puede ocurrir de manera continua, sin limitaciones geográficas, y puede tener repercusiones graves y duraderas en la salud mental y la vida cotidiana de las víctimas.

En cuanto a la investigación de los delitos relacionados con la VG FT, se presentan desafíos significativos para abogados, fiscales y otros operadores de justicia. Estos retos derivan de la naturaleza de las pruebas involucradas, las cuales son altamente volátiles y susceptibles de ser destruidas o modificadas con facilidad. Además, la identificación del agresor a menudo se complica debido al anonimato y a la rapidez con la que se difunden contenidos en los entornos digitales.

Ante esta realidad, esta guía tiene como propósito proporcionar herramientas iniciales para identificar correctamente estos delitos y establecer estrategias efectivas para la recolección y preservación de pruebas digitales. Esto resulta fundamental en un contexto donde los delitos de esta naturaleza son cada vez más frecuentes en una sociedad que ha acelerado su digitalización a consecuencia de la pandemia.

2. 1. Marco Jurídico.

2.1.1. Normativa Nacional.

Tabla 1. Normativa Nacional

NORMA	FECHA DE PROMULGACIÓN	TIPO DE LEY
Constitución Política del Estado (CPE)	7 de febrero de 2009	Norma suprema
Código Penal y Código de Procedimiento Penal	Vigentes a partir de 1972, con modificaciones posteriores (hasta 2019)	Ley Penal y Procesal Penal
Ley Orgánica de la Policía Nacional	8 de abril de 1985	Ley referente a la Policía
Ley No. 004, Marcelo Quiroga Santa Cruz (Lucha Contra la Corrupción)	31 de marzo de 2010	Ley Integral Anticorrupción
Ley No. 045 Contra el Racismo y Toda Forma de Discriminación	8 de octubre de 2010	Ley Integral Antidiscriminación
Ley N° 164 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación	8 de agosto de 2011	Ley referente a las TIC
Ley No. 348, Integral para Garantizar a las Mujeres una Vida Libre de Violencia	9 de marzo de 2013	Ley Integral Contra la Violencia de Género
Ley N° 243, Ley Contra el Acoso y la Violencia Política hacia las Mujeres.	28 de mayo de 2012	Ley Contra la Violencia Política hacia las mujeres.
Ley N° 254, Código Procesal Constitucional,	5 de julio de 2012	Procesal Constitucional
Ley Orgánica del Ministerio Público	11 de julio de 2012	Ley Ministerio Público
Ley No. 263, Integral Contra la Trata y Tráfico de Personas	31 de julio de 2012	Ley Integral Contra la Trata y Tráfico de Personas
Ley No. 548, Código Niña, Niño y Adolescente	17 de julio de 2014	Ley de Protección a la Niñez y Adolescencia
Ley No. 1173, Abreviación Procesal Penal y Fortalecimiento Contra la Violencia a Mujeres y Niños	8 de mayo de 2019	Ley de Reforma Procesal Penal

Fuente: elaboración propia.

2.1.2. Normativa Internacional.

Tabla 2. Normativa Internacional

NORMA	FECHA DE PROMULGACIÓN	FECHA DE RATIFICACIÓN POR BOLIVIA	TIPO DE LEY
Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW)	18 de diciembre de 1979	8 de junio de 1990	Tratado Internacional de Derechos Humanos
Protocolo Facultativo de la CEDAW Declaración sobre la Eliminación de Violencia contra la Mujer Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra las mujeres	6 de octubre de 1999	20 de junio de 2000	Tratado Internacional de Derechos Humanos
Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belém do Pará)	9 de junio de 1994	4 de diciembre de 1994	Tratado Internacional de Derechos Humanos
Convenio sobre la Ciberdelincuencia (Convenio de Budapest)	No ratificado por Bolivia		

Fuente: elaboración propia.

2. 2. Tipicidad tradicional vs Tipicidad virtual.

La tipicidad es un concepto esencial en el derecho penal que establece la correspondencia entre una conducta específica y un tipo penal previsto en la ley. En el contexto de la VG FT, resulta crucial distinguir entre la tipicidad tradicional, vinculada a delitos cometidos en entornos físicos o analógicos, y la tipicidad virtual, que abarca conductas delictivas facilitadas por las Tecnologías de la Información y Comunicación (TIC).

Esta diferenciación permite comprender de manera más exacta el fenómeno de la violencia digital trasladado al ámbito penal. Mientras en la tipicidad tradicional, los actos suelen dejar rastros físicos tangibles que pueden ser evaluados a través de métodos de investigación tradicionales, en la tipicidad virtual, las pruebas son generalmente digitales, efímeras y altamente manipulables, como registros de chats, metadatos, capturas de pantalla o direcciones IP, lo que demanda enfoques técnicos especializados y herramientas adaptadas a este entorno.

La comprensión clara de esta diferencia permite a fiscales, investigadores y abogados enfocar correctamente la investigación, adaptando las estrategias para abordar los retos propios del ámbito digital. Por ejemplo, la preservación de evidencias electrónicas requiere procesos técnicos específicos para evitar su alteración o eliminación. Asimismo, la identificación del agresor en delitos virtuales suele implicar la colaboración con proveedores de servicios digitales y el uso de herramientas de rastreo tecnológico, algo que no es necesario en la mayoría de los delitos tradicionales.

Además, las conductas propias de la VG FT, como el ciberacoso, el doxing o la sextorsión, pueden no estar expresamente tipificadas en los códigos penales tradicionales, lo que obliga a interpretar los tipos penales existentes para adaptarlos al entorno virtual. Esta situación genera desafíos legales y jurisprudenciales, ya que se requiere analizar si las características del delito digital encajan dentro del marco normativo previsto para los delitos tradicionales.

En este sentido, la tabla presentado ofrece una introducción preliminar a la tipicidad virtual, facilitando la comprensión de las características distintivas que la digitalización imprime en el ámbito penal. Este enfoque inicial permite la familiarización con los elementos particulares que definen los delitos cometidos en entornos digitales.

Tabla 3. Tipicidad virtual

ELEMENTO	TIPICIDAD TRADICIONAL	TIPICIDAD VIRTUAL
Acción	Física, mensurable, observable	Inmaterial, digital, interactiva
Bien jurídico protegido	Tangibles (vida, patrimonio, integridad física)	Inmateriales (privacidad, honor, datos, seguridad informática)
Sujeto Activo	Fácilmente identificable	Posiblemente anónimo
Nexo de Causalidad	Directa, inmediata	Difusa, mediada por sistemas informáticos
Espacio y tiempo	Definido, localizable	Deslocalizado, en el ciberespacio[1]
Resultado	Tangible, físico (daños corporales, patrimoniales) visión analógica	Inmaterial (manipulación de datos, acceso no autorizado)
Intervención humana	Directa	Mediada por tecnología o automatizada
Normas	Estáticas, específicas	Flexibles, adaptables al cambio tecnológico
Ámbito	Físico, limitado a un espacio geográfico	Virtual, deslocalizado, global

Fuente: elaboración propia basada en "El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual" de Ricardo Posada Maya.

2.2.1. Acción

- **Descripción en contexto tradicional:** Física, medible, observable. En delitos tradicionales de violencia de género, la acción puede incluir agresiones físicas, insultos, amenazas verbales y otras conductas tangibles y observables, como golpear, empujar o gritar.

- **Contexto virtual:** Inmaterial, digital, interactivo. En el ámbito de la VG FT, las acciones se realizan a través de medios digitales, como redes sociales, aplicaciones de mensajería, correos electrónicos o cualquier otra plataforma tecnológica, sin embargo es importante mencionar que si bien las acciones pueden iniciar de manera digital, pueden posteriormente materializarse en un contexto físico.

- Clave para la investigación: Al momento de realizar la denuncia es crucial describir detalladamente las acciones del agresor, incluyendo capturas de pantalla, mensajes y otros registros que evidencien el comportamiento abusivo y violento.

1 "En los cibercrímenes, el ciberespacio y los medios informáticos no se pueden considerar como simples "medios ejecutivos", sino que son el ámbito digital en donde tiene lugar la realización lógica del delito."

2.2.2. Bien jurídico protegido

- **Tipicidad tradicional:** Tangibles (vida, integridad física, dignidad personal). En la violencia de género tradicional, los bienes jurídicos protegidos incluyen la vida, integridad física, libertad y dignidad de la persona, garantizando que no sufran daños corporales o ataques a su honor.

- **Contexto virtual:** Inmateriales (privacidad, seguridad digital, dignidad, integridad psicológica). En la violencia facilitada por la tecnología, los bienes jurídicos protegidos se expanden para incluir:

1. **Privacidad:** Protección contra el acceso no autorizado a información personal, imágenes o comunicaciones.
2. **Seguridad digital:** Prevención del monitoreo o rastreo sin consentimiento.
3. **Dignidad e integridad psicológica:** Evitar la humillación pública, el acoso y la manipulación emocional a través de medios digitales.
4. **Clave para la investigación:** Al momento de denunciar se debe enfatizar cómo las acciones del agresor violan estos bienes jurídicos, detallando la forma en que la tecnología ha sido utilizada para infringir la privacidad y seguridad de la víctima.

2.2.3. Sujeto activo

- **Tipicidad tradicional:** Fácilmente identificable En casos tradicionales, el agresor suele ser alguien conocido por la víctima y se puede identificar fácilmente a través de testigos o cámaras de seguridad.

- **Contexto virtual:** Posiblemente anónimo, utilizando perfiles falsos En los delitos facilitados por la tecnología, el agresor puede operar de manera anónima o utilizar perfiles falsos para acosar a la víctima. También puede emplear herramientas para ocultar su ubicación y evitar ser rastreado.

1. **Clave para la investigación:** Si bien es esencial aportar pruebas que vinculen al agresor con los perfiles o dispositivos utilizados en los actos de acoso. Esto puede incluir datos técnicos, como direcciones IP, mensajes guardados o registros de aplicaciones que demuestren la autoría de las acciones, es esencial copiar los links para facilitar la identificación del sujeto activo.

2.2.4. Nexo de causalidad

- **Tipicidad tradicional:** Directa, inmediata. En la violencia física, el nexo de causalidad es claro: el daño se produce como resultado directo de la acción del agresor (golpes, insultos, amenazas).

- **Contexto virtual:** Difusa, mediada por sistemas informáticos. En el contexto digital, el nexo de causalidad puede ser más complejo, ya que las acciones delictivas pueden implicar el uso de tecnología y plataformas que dificulten rastrear la fuente original del daño. Por ejemplo, el daño causado por la publicación de imágenes íntimas puede tener un impacto prolongado y difícil de medir de inmediato.

1. **Clave para la investigación:** Se debe explicar claramente cómo las acciones del agresor en línea han causado un daño directo a la víctima, en este punto un informe psicológico y una valoración social se pueden utilizar para demostrar el perjuicio sufrido.

2.2.5. Espacio y Tiempo

- **Tipicidad tradicional:** Definido, localizable. La violencia de género tradicional ocurre en lugares físicos específicos, como el hogar o el lugar de trabajo, y en momentos determinados.

- **Contexto virtual:** Deslocalizado, en el ciberespacio. Los delitos digitales carecen de un espacio físico claro, ya que las acciones pueden ser cometidas desde cualquier lugar del mundo, a cualquier hora y pueden afectar a la víctima en múltiples ubicaciones. Por ejemplo, un agresor puede acosar a la víctima desde una localidad o país diferente utilizando redes sociales.

Clave para la investigación: El tema de la ubicación es esencial, pues esto va a determinar la jurisdicción del proceso, una manera de manejar el tema de la competencia es a través del informe psicológico que, independientemente de la ubicación física del agresor demuestre la afectación a la vida de la víctima. En casos donde el resultado delictivo ocurre en un lugar diferente al de la comisión del delito, las leyes bolivianas permiten que el proceso se lleve a cabo en el lugar donde se produce el efecto delictivo. Esto de acuerdo a:

> **Artículo 28 del Código de Procedimiento Penal (CPP):** Competencia Territorial "son competentes para conocer y resolver las causas penales los jueces y tribunales del lugar donde se hubiere cometido el hecho punible o donde se hubiere producido el resultado."

Este artículo establece que, además del lugar donde se cometió el delito (lugar de la acción), también se puede considerar el lugar donde se produjo el **resultado** delictivo para determinar la competencia territorial. Esto es particularmente útil en casos donde el acto que origina el delito ocurre en una ubicación, pero las consecuencias o el daño se manifiestan en otro lugar.

> **Artículo 29 del Código de Procedimiento Penal (CPP):** Competencia Alternativa "Cuando el hecho punible se haya cometido en diferentes lugares, la competencia se radicará en el tribunal del lugar en el cual se inició el hecho o donde se produjeron sus efectos."

El artículo 29 amplía la posibilidad de elegir entre diferentes lugares para iniciar el proceso penal, siempre que exista una relación clara entre el hecho y sus efectos. Esto es particularmente relevante en casos donde el delito tiene una dimensión transregional o incluso internacional, permitiendo a las autoridades actuar en el lugar más adecuado para la investigación.

2.2.6. Resultado

- **Tipicidad tradicional:** tangible, físico (daños corporales, patrimoniales). En casos de violencia física, los resultados son daños visibles como lesiones, heridas o pérdidas materiales.

- **Contexto virtual:** inmaterial (manipulación de datos, daño psicológico, pérdida de privacidad). En la violencia facilitada por la tecnología, los resultados incluyen:

1. **Daño emocional y psicológico:** estrés, ansiedad, miedo constante y daño a la reputación.
2. **Pérdida de privacidad:** difusión de datos personales, imágenes íntimas o información sensible sin autorización.
3. **Manipulación y control:** uso de herramientas digitales para rastrear, intimidar o coaccionar a la víctima.

Clave para la investigación: es necesario describir los efectos emocionales y psicológicos que la víctima ha experimentado, así como cualquier evidencia que demuestre la difusión no autorizada de datos o la manipulación digital ejercida por el agresor.

2.2.7. Intervención humana

Tipicidad tradicional: directa en la violencia física, el agresor interactúa directamente con la víctima.

Contexto virtual: mediada por tecnología o automatizada. En el ámbito digital, el acoso y la violencia pueden ser facilitados por tecnología automatizada. Por ejemplo, el uso de bots para enviar mensajes ofensivos masivamente o aplicaciones para rastrear la ubicación de la víctima sin su conocimiento.

Clave para la investigación: se debe especificar cómo el agresor ha utilizado la tecnología para facilitar la violencia, aportando pruebas de los métodos empleados (aplicaciones, programas, cuentas falsas).

2.2.8. Normas

- **Tipicidad tradicional:** estática, específica. Las leyes que protegen contra la violencia física son claras y específicas, aplicables en territorios definidos.

- **Contexto virtual:** flexibles, adaptables al cambio tecnológico. Las normas contra la violencia digital deben ser flexibles para adaptarse a las nuevas formas de abuso que surgen con el avance tecnológico.

Clave para la investigación: en Bolivia no contamos con normativa específica de VG FT, sin embargo, esto no debe ser una limitante para abogados y personal jurisdiccional para atender estos casos, ya que muchos de estos se subsumen en delitos ya tipificados por nuestra normativa. En este sentido, se puede utilizar la SENTENCIA CONSTITUCIONAL PLURINACIONAL 0815/2019-S2.

2.2.9. Ámbito

- **Tipicidad tradicional:** físico, limitado a un espacio geográfico. La violencia física ocurre dentro de una jurisdicción específica.

- **Contexto virtual:** virtual, deslocalizado, global. La violencia digital puede ser global, permitiendo que el agresor afecte a la víctima desde cualquier lugar del mundo. Esto implica que las investigaciones pueden requerir el manejo de jurisdicciones múltiples.

Clave para la investigación: Es necesario que las medidas de protección se adapten a la violencia digital, el contexto de violencia digital multiplica los efectos de la violencia, por lo cual es esencial tomar medidas oportunas que frenen el daño contra las víctimas.

2. 3. ¿Qué tipos de delitos están relacionados con la violencia digital?

En el punto anterior se desarrollan los elementos de un delito, con sus características especiales en el ámbito virtual, sin embargo es importante conocer quien inicia la acción penal, es decir, quien es la persona autorizada para iniciar el proceso de investigación para llegar a una sanción. De acuerdo a la normativa boliviana, encontraremos delitos de acción pública, de acción pública a instancia de parte y de acción privada.

2.3.1. Delitos de acción pública

Son aquellos que pueden ser perseguidos de oficio, es decir, no requieren la intervención o denuncia de la víctima para que el Ministerio Público inicie la acción penal. Son delitos considerados de interés público debido a la gravedad de su naturaleza y al peligro social, por lo que la Fiscalía tiene la obligación de investigarlos y llevar el proceso judicial, aún cuando la víctima no lo solicite o participe activamente.

Artículo 16 del Código Penal. La acción penal pública será ejercida por la Fiscalía en todos los delitos perseguibles de oficio. Este tipo de acción no puede suspenderse ni cesar, salvo en los casos previstos por la ley.

Por ejemplo: Si la policía descubre que una persona está distribuyendo imágenes de pornografía infantil en una plataforma digital, las autoridades deben iniciar una investigación penal inmediatamente. No es necesario que los padres, las personas afectadas o la defensoría presenten una denuncia formal; el Estado tiene la obligación de intervenir de inmediato para detener la actividad, proteger a las víctimas y castigar a los responsables.

2.3.2. Delitos de acción pública a instancia de parte

Son delitos que, aunque se persiguen de manera pública, requieren que la víctima inicie el proceso penal mediante una denuncia formal. El Ministerio Público no puede actuar de oficio sin la intervención de la víctima, pero una vez presentada la denuncia, asume la investigación y persecución penal del caso.

> **Artículo 17 del Código Penal.** La acción penal pública requiere de la denuncia de la víctima para poder ejercerse en ciertos casos. El fiscal puede actuar incluso antes de recibir la denuncia si es necesario preservar pruebas.

De acuerdo al Artículo 19 del Código Penal, son delitos de acción pública a instancia de parte lo siguientes: violación, abuso deshonesto, estupro, corrupción de mayores, violencia y acoso político.

Por ejemplo: Un adulto tiene relaciones sexuales con una persona de 17 años que consintió, pero la Ley define que el consentimiento no es válido por la edad de la persona adolescente. si el delito es de acción pública a instancia de parte, el proceso sólo se iniciará si los padres del o de la adolescente deciden presentar una denuncia formal.

2.3.3. Delitos de acción privada

Son considerados delitos de acción privada en los que sólo la víctima puede iniciar el proceso penal mediante una querella y el Ministerio Público no participa en la investigación o el juicio. La persecución de estos delitos está completamente a cargo de la víctima, quien debe presentar la acusación ante el juez competente.

Artículo 18 del Código Penal La acción penal privada será ejercida exclusivamente por la víctima, quien puede iniciar el proceso penal mediante una querella.

Son delitos de acción privada todos aquellos relacionados al honor: difamación, injuria y calumnia.

Por ejemplo: Una persona acusa públicamente a otra de haber robado dinero de una empresa, pero sabe que esta afirmación es completamente falsa. La persona afectada, al verse perjudicada por esta falsa acusación, presenta una querella por calumnia para que se investigue el caso, ni la fiscalía o policía interviene, es la persona que se siente agredida la responsable de presentar las pruebas para que se sancione al responsable de la difamación.

2. 4. Contravenciones

Las contravenciones son faltas menores que no constituyen delitos graves, pero que infringen normas administrativas o de convivencia social. Aquellas violencias reconocidas por la Ley Nro. 348 que no son consideradas delitos, son contravenciones. Estas faltas son sancionadas con medidas leves como multas o trabajos comunitarios y no suelen implicar penas privativas de libertad y el proceso se lleva adelante por instancias diferentes al Ministerio Público. Por ejemplo, la violencia cibernética en el ámbito educativo.

Las contravenciones establecidas de la ley 348, se encuentran establecidas por el reglamento, Reglamento de la Ley N° 348 “Ley integral para garantizar a las mujeres una vida libre de violencia”, DS N° 2145, 14 de octubre de 2014, en su artículo 3. Siendo los siguientes:

Tabla 4. Contravenciones

TIPO DE VIOLENCIA	CONCEPTUALIZACIÓN LEGAL	EJEMPLO
Violencia mediática	La publicación y difusión de mensajes e imágenes estereotipadas que promuevan la sumisión de las mujeres o hagan uso sexista de su imagen como parte de la violencia mediática, simbólica y/o encubierta.	Corimexo ha presentado imágenes de mujeres en posiciones o vestimentas que resaltan estereotipos sexuales o de sumisión. En lugar de centrarse en las características del producto (muebles y mobiliario), la publicidad se enfoca en la figura femenina como un “accesorio” lo que contribuye a una representación de la mujer como un objeto decorativo.
Violencia contra los derechos reproductivos/ Violencia en servicios de salud	Las agresiones verbales, denegación de acceso al servicio o maltrato por motivos discriminatorios, maltrato e incumplimiento de deberes como parte de la violencia contra los derechos reproductivos, el derecho a la salud y la libertad sexual.	Una mujer acude a un ginecólogo para solicitar la realización de una ligadura de trompas como método de anticoncepción permanente. El ginecólogo, antes de proceder, le indica que es necesario obtener previamente la autorización de su pareja, limitando así su derecho a decidir sobre su propio cuerpo
Violencia laboral	El acoso laboral y la violencia laboral serán denunciados ante el Ministerio de Trabajo Empleo y Previsión Social; asimismo, la discriminación a través de agresiones verbales o maltrato e incumplimiento de deberes ante la misma institución donde se hubiere producido el hecho, todas estas contravenciones como parte de la violencia laboral.	En una oficina, una supervisora o supervisor asigna regularmente a una empleada tareas administrativas menores, como hacer fotocopias o preparar café, que no corresponden a su puesto ni a sus responsabilidades. Este tipo de asignación se da exclusivamente hacia ella, mientras que a sus colegas varones se les asignan tareas más relevantes y acordes al puesto que han sido contratados.
Violencia institucional	Las agresiones verbales, denegación injustificada de acceso al servicio o maltrato psicológico por motivos discriminatorios o cualquier otra forma de maltrato que no constituya delito, será denunciado ante las instancias donde se produjo el hecho como parte de la violencia institucional.	Cuando una mujer acude a una instancia de denuncia o de seguimiento de un caso y se le niega sin justificación válida la información sobre los requisitos necesarios, prolongando innecesariamente el proceso.
Violencia Simbólica y/o Encubierta	El maltrato o agresiones verbales por motivos discriminatorios, que no constituyan delito, serán denunciados ante la institución donde se produjo el hecho como parte de la violencia psicológica, contra la dignidad, la honra y el nombre.	Durante una audiencia en un proceso judicial, una mujer es objeto de comentarios despectivos por parte de un funcionario judicial, quien realiza observaciones peyorativas sobre su apariencia y cuestiona su capacidad para comprender el procedimiento, insinuando que su situación socioeconómica afecta su credibilidad.
Violencia en el sistema Educativo	Se presenta cuando una o un miembro de la comunidad educativa es hostigada u hostigado, amenazada o amenazado, acosada o acosado, difamada o difamado, humillada o humillado, de forma dolosa por otra u otras personas, causando angustia emocional y preocupación, a través de correos electrónicos, videojuegos conectados al internet, redes sociales, blogs, mensajería instantánea y mensajes de texto a través de internet, teléfono móvil o cualquier otra tecnología de información y comunicación.	Una estudiante es objeto de burlas por parte de otro compañero, el mismo realiza memes y reiterados ataques a través de redes sociales.

Fuente: elaboración propia.

2. 5. Manifestaciones de la violencia digital

La violencia digital, al igual que otros tipos de violencia, se manifiesta en distintos ámbitos, desde el abuso de datos personales, el acoso, las amenazas hasta la facilitacion de la violencia sexual y/o de trata y tráfico. Las mujeres en situación de violencia ven afectados sus derechos y sufren daños psicológicos, sociales y económicos, daños que son amplificados por la facilidad de anonimato y la amplia difusión que permiten las plataformas digitales. Debido a la diversidad de las tipologías de VG FT, se han identificado las siguientes categorías:

- Violencia sexual relacionadas a las TIC
- Acoso relacionado a las TIC
- Captación para la trata
- Delitos contra el honor
- Violencia institucional
- Discursos de odio a través de las TIC
- Afectaciones a mujeres en política
- Abuso de datos personales usando TIC

Es innegable que las acciones que emergen de la VG FT se subsumen en tipos penales ya establecidos en nuestra normativa nacional, por lo cual es necesario describir y explicar cada uno de estos delitos facilitados por la tecnología.

2.5.1. Violencia sexual relacionada a las TIC

La violencia sexual facilitada por tecnologías de la información y comunicación (TIC) consiste en el uso de herramientas digitales para ejercer control, explotación o abuso sexual contra una persona, violando su derecho a la privacidad, integridad y dignidad. Estas conductas son una extensión de las formas tradicionales de violencia sexual, agravadas por la capacidad de difusión masiva y anonimato que ofrecen las plataformas digitales.

De acuerdo con el marco normativo boliviano, se han identificado conductas específicas que se subsumen en diversos tipos penales establecidos en el Código Penal.

Difusión de Imágenes Íntimas sin Consentimiento

- **Tipo Penal:** Pornografía (Artículo 323° bis del Código Penal).

- **Acción Penal:** Pública de oficio

Tabla 5.

PORNOGRAFÍA	
Tipo penal	**ARTÍCULO 323° bis.- (PORNOGRAFÍA). I.** Quien procure, obligue, facilite o induzca, por cualquier medio, por sí o por tercera persona a otra que no dé su consentimiento a realizar actos sexuales o de exhibicionismo corporal con fines lascivos con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o de comunicaciones, sistemas informáticos, eléctricos o similares, será sancionado con pena privativa de libertad de diez a quince años. **Igual sanción será impuesta cuando el autor o participe reproduzca o almacene, distribuya o venda material pornográfico.** **II.** La pena privativa de libertad será agravada en un tercio cuando: La víctima sea niña, niño o adolescente o persona con discapacidad. La autora o el autor sea conyugue, conviviente, padre, madre o persona que ejerza algún tipo de autoridad o responsabilidad legal sobre la víctima. La autora o autor mantenga una relación laboral de parentesco consanguíneo o de afinidad con la víctima. La víctima sea una mujer embarazada. La autora o autor sea una servidora o servidor público. La autora o autor sea la persona encargada de proteger los derechos e integridad de las personas en situación vulnerable. La autora o autor hubiera sido parte integrante de una delegación o misión diplomática, en el momento de haberse cometido el delito. El delito se cometa contra más de una persona. La actividad sea habitual y con fines de lucro. La autora o autor sea parte de una organización criminal. **III.** Quien compre, venda o arriende material pornográfico, donde se exhiban imágenes de niñas, niños o adolescentes, será sancionado con pena privativa de libertad de cinco a ocho años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Libertad sexual
Sanción	10 a 15 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en trata y tráfico

Fuente: elaboración propia.

Sextorsión

- **Tipo Penal:** Extorsión (Artículo 333° del Código Penal).

- **Acción Penal:** Pública de oficio.

Tabla 6.

EXTORSIÓN	
Tipo penal	ARTÍCULO 333°.- (EXTORSIÓN). El que mediante intimidación o amenaza grave constriñere a una persona a hacer, tolerar que se haga o deje de hacer alguna cosa, con el fin de obtener para sí o un tercero indebida ventaja o beneficio económico, incurrirá en reclusión de uno a tres años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Propiedad Privada
Sanción	1 a 3 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos patrimoniales

Fuente: elaboración propia.

Seducción y Engaño pederasta a Niñas, Niños y Adolescentes (Grooming)

- Tipo Penal:

1. Corrupción de niño, niña y adolescente (Artículo 318° del Código Penal).
2. Estupro (Artículo 309° del Código Penal).

- Acción Penal:

3. Pública de oficio para corrupción de niña, niña y adolescente
4. Pública a instancia de parte para estupro.

Tabla 7.

CORRUPCIÓN DE NIÑA, NIÑO O ADOLESCENTE	
Tipo penal	ARTÍCULO 318°.- (CORRUPCIÓN NIÑA, NIÑO O ADOLESCENTE). El que mediante actos libidinosos o por cualquier otro medio corrompiere o contribuyere a corromper una persona menor de diez y ocho años, será sancionado con pena privativa de libertad de tres a ocho años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Menor de 18 años
Bien Jurídico Protegido	Libertad sexual
Sanción	3 a 8 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos en razón de género

Fuente: elaboración propia.

Tabla 8.

ESTUPRO	
Tipo penal	ARTÍCULO 309°.- (ESTUPRO). Quien mediante seducción o engaño, tuviera acceso carnal con persona de uno u otro sexo mayor de catorce y menor de dieciocho años, será sancionado con privación de libertad de tres a seis años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Persona mayor de 14 años y menor de 18
Bien Jurídico Protegido	Libertad sexual
Sanción	3 a 6 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos en razón de género

Fuente: elaboración propia.

Afectaciones a la Indemnidad Sexual

Tipo Penal:

1. Corrupción de mayores (Artículo 320° del Código Penal).
2. Engaño a personas incapaces (Artículo 342° del Código Penal).

Acción Penal:

1. Pública a instancia de parte en el caso de corrupción de mayores.
2. Pública de oficio para el engaño a personas incapaces..

Tabla 9.

CORRUPCIÓN DE MAYORES	
Tipo penal	ARTÍCULO 320°.- (CORRUPCIÓN DE MAYORES). Quien por cualquier medio corrompiere o contribuyere a la corrupción de mayores de diez y ocho años, será sancionado con reclusión de tres meses a dos años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Persona Mayor de 18 años
Bien Jurídico Protegido	Libertad sexual
Sanción	3 meses a 2 años años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos en razón de género

Fuente: elaboración propia.

ENGAÑO A PERSONAS INCAPACES	
Tipo penal	ARTÍCULO 342°.- (ENGAÑO A PERSONAS INCAPACES). El que para obtener para sí o para otros algún provecho, abusando de las necesidades, de las pasiones o de la inexperiencia de una persona menor de dieciocho años o abusando del estado de enfermedad o deficiencia psíquica de una persona, aunque no esté en interdicción o inhabilitada, la indujere a **realizar un acto que implique algún efecto jurídico perjudicial** para ella o para otros, incurrirá en privación de libertad de tres a ocho años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Persona menor de 18 años o estado de enfermedad
Bien Jurídico Protegido	Patrimonio del incapaz
Sanción	3 a 8 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos patrimoniales
Consideración	Este delito tiene carácter patrimonial, sin embargo, se podría analizar el efecto jurídico perjudicial.

Fuente: elaboración propia.

2.5.2. Acoso relacionado a las TIC

El acoso en el ámbito digital comprende un conjunto de conductas reiteradas, públicas o privadas, que generan un ambiente hostil e intimidante para la víctima. Estas conductas suelen incluir mensajes no solicitados, insultos, amenazas, expresiones discriminatorias o contenido sexualizado. Las TIC amplifican el alcance de este tipo de violencia, permitiendo a los agresores actuar con mayor anonimato y facilidad para hostigar a sus víctimas, sin embargo en muchos de estos casos los agresores son personas conocidas.

Ciberacoso

- **Tipo Penal:**

1. Acoso Sexual (Artículo 312 quater del Código Penal).
2. Violencia Familiar o Doméstica en su vertiente psicológica (Artículo 272 bis del Código Penal).

- **Acción Penal:** Pública de oficio.

Tabla 10.

ACOSO SEXUAL	
Tipo penal	ARTÍCULO 312 quater. (ACOSO SEXUAL). I. La persona que valiéndose de una posición jerárquica o poder de cualquier índole hostigue, persiga, exija, apremie, amenace con producirle un daño o perjuicio cualquiera, condicione la obtención de un beneficio u obligue por cualquier medio a otra persona a mantener una relación o realizar actos o tener comportamientos de contenido sexual que de otra forma no serían consentidos, para su beneficio o de una tercera persona, será sancionada con privación de libertad de cuatro (4) a ocho (8) años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Libertad sexual
Sanción	4 a 8 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos en razón de género

Fuente: elaboración propia.

Tabla 11.

ACOSO SEXUAL	
Tipo penal	ARTÍCULO 312 quater. (ACOSO SEXUAL). I. La persona que valiéndose de una posición jerárquica o poder de cualquier índole hostigue, persiga, exija, apremie, amenace con producirle un daño o perjuicio cualquiera, condicione la obtención de un beneficio u obligue por cualquier medio a otra persona a mantener una relación o realizar actos o tener comportamientos de contenido sexual que de otra forma no serían consentidos, para su beneficio o de una tercera persona, será sancionada con privación de libertad de cuatro (4) a ocho (8) años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Libertad sexual
Sanción	4 a 8 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos en razón de género

Fuente: elaboración propia.

Monitoreo y Acecho

- **Tipo Penal:** Lesiones Graves y Leves en su vertiente de daño psicológico (Artículo 271° del Código Penal).

- **Acción Penal:** Pública de oficio.

Tabla 12.

ACOSO SEXUAL	
Tipo penal	ARTÍCULO 312 quater. (ACOSO SEXUAL). I. La persona que valiéndose de una posición jerárquica o poder de cualquier índole hostigue, persiga, exija, apremie, amenace con producirle un daño o perjuicio cualquiera, condicione la obtención de un beneficio u obligue por cualquier medio a otra persona a mantener una relación o realizar actos o tener comportamientos de contenido sexual que de otra forma no serían consentidos, para su beneficio o de una tercera persona, será sancionada con privación de libertad de cuatro (4) a ocho (8) años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Libertad sexual
Sanción	4 a 8 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos en razón de género

Fuente: elaboración propia.

Coacción Digital

- Tipo Penal:

Extorsión (Artículo 333° del Código Penal)

Amenazas (Artículo 293° del Código Penal).

- **Acción Penal:** Pública de oficio.

Tabla 13.

AMENAZAS	
Tipo penal	ARTÍCULO 293°.- (AMENAZAS). El que mediante amenazas graves alarmare o amedrentare a una persona, será sancionado con prestación de trabajo de un mes a un año y multa hasta de sesenta días. La pena será de reclusión de tres a diez y ocho meses, si la amenaza hubiere sido hecha con arma o por tres o más personas reunidas.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Libertad individual
Sanción	3 a 18 meses de privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos en razón de género

Fuente: elaboración propia.

Ciberbullying

- **Infracción:** Violencia Cibernética en el Sistema Educativo (Artículo 151 del Código de la Niñez y Adolescencia, inciso g).

- **Clasificación:** Contravención.

La violencia cibernética es reconocida como una infracción en el ámbito educativo y se encuentra reconocida por la Ley No. 548, Código Niña, Niño y Adolescente, entre los tipos de violencia en el ámbito educativo. El código define la violencia cibernética como aquella que:

"Se presenta cuando una o un miembro de la comunidad educativa es hostigada u hostigado, amenazada o amenazado, acosada o acosado, difamada o difamado, humillada o humillado, de forma dolosa por otra u otras personas, causando angustia emocional y preocupación, a través de correos electrónicos, videojuegos conectados al internet, redes sociales, blogs, mensajería instantánea y mensajes de texto a través de internet, teléfono móvil o cualquier otra tecnología de información y comunicación."

Afectaciones a Canales de Expresión (Censura)

Se refiere a la interrupción o censura de la libertad de expresión de una persona en plataformas digitales, usualmente mediante ataques coordinados o reportes maliciosos para bloquear sus cuentas o publicaciones.

- **Tipo Penal:** No existe un delito penal específico relacionado con la censura.

- **Acción Jurídica:** Acción Constitucional (Recurso de Habeas Data o Amparo Constitucional)..

La censura en plataformas digitales consiste en la interrupción o restricción de la libertad de expresión de una persona o grupo mediante mecanismos como ataques coordinados o reportes maliciosos que resultan en el bloqueo de cuentas o la eliminación de publicaciones. Este tipo de actos puede generar graves afectaciones al derecho fundamental a la libertad de expresión, especialmente en un entorno digital que se ha convertido en un espacio clave para la comunicación, la participación pública y la defensa de derechos.

Aunque en Bolivia no existe un delito penal específico que regule la censura en plataformas digitales, las personas o grupos afectados por este tipo de conductas tienen la posibilidad de recurrir a mecanismos de defensa constitucional. Los dos recursos más relevantes en este contexto son el Recurso de Habeas Data y el Amparo Constitucional, ambos diseñados para proteger derechos fundamentales como la libertad de expresión.

2.5.3. Captación para la trata de personas

- Trata de personas

Tipo Penal: Trata de personas (Artículo 281 bis).

- **Acción Penal:** Pública de oficio.

Tabla 14.

TRÁFICO DE PERSONAS	
Tipo penal	ARTÍCULO 321° Bis. (TRÁFICO DE PERSONAS).- I. Quien promueva, induzca, favorezca y/o facilite por cualquier medio la entrada o salida ilegal de una persona del Estado plurinacional de Bolivia, a otro Estado del cual dicha persona no sea nacional o residente permanente, con el fin de obtener directa o indirectamente beneficio económico para sí o para un tercero, será sancionado con privación de libertad de cinco a diez años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Libertad
Sanción	5 a 10 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en trata y tráfico de personas

Fuente: elaboración propia.

Proxenetismo

- **Tipo Penal:** Proxenetismo (Artículo 321°).
- **Acción Penal:** Pública de oficio.

Tabla 15.

PROXENETISMO	
Tipo penal	Quien mediante engaño, abuso de una situación de necesidad o vulnerabilidad de una relación de dependencia o de poder, violencia amenaza o de cualquier otro medio de intimidación o coerción, para satisfacer deseos ajenos o con ánimo de lucro o beneficio promoviere, facilitare o contribuyere a la prostitución de persona de uno u otro sexo, o la que obligare a permanecer en ella, será sancionado con privación de libertad de diez a quince años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Libertad sexual
Sanción	10 a 15 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en trata y tráfico de personas

Fuente: elaboración propia.

Violencia Sexual Comercial

- **Tipo Penal:** Violencia sexual comercial (Artículo 322°).
- **Acción Penal:** Pública de oficio.

Tabla 16.

VIOLENCIA SEXUAL COMERCIAL	
Tipo penal	ARTÍCULO 322°.- (VIOLENCIA SEXUAL COMERCIAL). Quien pagaré, en dinero o especie, directamente a un niño, niña o adolescente o a tercera persona para mantener cualquier tipo de actividad sexual, erótica o pornográfica con un niño, niña o adolescente, para la satisfacción de sus intereses o deseos sexuales, será sancionado con privación de libertad de ocho a doce años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Niño, niña o adolescente
Bien Jurídico Protegido	Libertad sexual
Sanción	8 a 12 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en trata y tráfico de personas
Consideración	En este caso la persona en situación de violencia solo puede ser un niño, niña o adolescente, no se considera en este tipo penal a sujetos pasivos a mujeres que hayan superado la adolescencia[2].

Fuente: elaboración propia.

2 Ley 548, Código Niña, Niño y Adolescente, en el Artículo 5. Sujetos de Derechos. Establece que son sujetos de derechos los seres humanos hasta los dieciocho (18) años cumplidos, dividiendo las etapas de desarrollo en: niñez, desde la concepción hasta los doce (12) años cumplidos,y adolescencia, desde los doce (12) años hasta los dieciocho (18) años cumplidos.

2.5.4. Delitos contra el honor

La tipificación de los delitos contra el honor en el Código penal boliviano protege la reputación, credibilidad y dignidad de las personas frente a actos que busquen descalificarlas o dañarlas mediante la difusión de información falsa, manipulada o fuera de contexto. Esta tipificación busca salvaguardar el derecho al honor de las personas frente a ataques verbales o escritos, especialmente en un entorno digital donde la difusión de información es rápida y de amplio alcance, si bien la legislación boliviana clasifica estos delitos como de acción privada, es fundamental que las víctimas utilicen los mecanismos legales disponibles para garantizar la reparación de los daños y la sanción de los responsables.

Difamación

- **Tipo Penal:** Difamación (Artículo 282° del Código Penal).

- **Acción Penal:** Privada.

Tabla 17.

DIFAMACIÓN	
Tipo penal	ARTÍCULO 282°.- (DIFAMACIÓN). El que de manera pública, tendenciosa y repetida, revelare o divulgare un hecho, una calidad, o una conducta capaces de afectar la reputación de una persona individual o colectiva, incurrirá en prestación de trabajo de un mes a un año o multa de veinte a doscientos cuarenta días.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Honor
Sanción	1 mes a 1 año de prestación de trabajo o multa de 20 a 240 días.
Fiscalía Especializada	NO INTERVIENE LA FISCALÍA
Consideración	Delito de acción privada

Fuente: elaboración propia.

Calumnia

- **Tipo Penal:** Calumnia (Artículo 283° del Código Penal).

- **Acción Penal:** Privada.

Tabla 18.

CALUMNIA	
Tipo penal	ARTÍCULO 283°.- (CALUMNIA). El que por cualquier medio imputare a otro falsamente la comisión de un delito, será sancionado con privación de libertad de seis meses a dos años, y multa de cien a trescientos días.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Honor
Sanción	6 meses a 2 años privación de libertad y multa de 100 a 300 días.
Fiscalía Especializada	NO INTERVIENE LA FISCALÍA
Consideración	Delito de acción privada

Fuente: elaboración propia.

Injuria

- **Tipo Penal: I**njuria (Artículo 287° del Código Penal).

- **Acción Penal:** Privada.

Tabla 19

INJURIA	
Tipo penal	ARTÍCULO 287°.- (INJURIA). El que por cualquier medio y de un modo directo ofendiere a otro en su dignidad o decoro, incurrirá en prestación de trabajo de un mes a un año y multa de treinta a cíen días.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Honor
Sanción	1 mes a 1 año de prestación de trabajo y multa de 30 a 100 días
Fiscalía Especializada	NO INTERVIENE LA FISCALÍA
Consideración	Delito de acción privada

Fuente: elaboración propia.

OFENSA A LA MEMORIA DE DIFUNTOS	
Tipo penal	ARTÍCULO 284°.- (OFENSA A LA MEMORIA DE DIFUNTOS). El que ofendiere la memoria de un difunto con expresiones difamatorias o con imputaciones calumniosas, incurrirá en las mismas penas de los dos artículos anteriores.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Difunto
Bien Jurídico Protegido	Honor
Sanción	Dependiendo a qué delito subsume su conducta
Fiscalía Especializada	NO INTERVIENE LA FISCALÍA
Consideración	Delito de acción privada

Fuente: elaboración propia.

Tabla 20.

PROPALACIÓN DE OFENSAS	
Tipo penal	ARTÍCULO 285°.- (PROPALACIÓN DE OFENSAS). El que propalare o reprodujere por cualquier medio los hechos a que se refieren los artículos 282, 283 y 284, será sancionado como autor de los mismos.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Honor
Sanción	Dependiendo a qué delito subsume su conducta
Fiscalía Especializada	NO INTERVIENE LA FISCALÍA
Consideración	Delito de acción privada

Fuente: elaboración propia.

2.5.5. Violencia institucional

La violencia institucional se manifiesta en la negativa de atención de casos, la negligencia en la ejecución de sus funciones y la revictimización por parte de instituciones públicas, lo que resulta en la vulneración de los derechos fundamentales de las personas, particularmente de las mujeres que sufren VG FT. Uno de los aspectos más críticos de esta violencia es la negativa o dificultad para acceder a la justicia, ya que muchas víctimas enfrentan trabas institucionales como la falta de atención, revictimización o negligencia en el manejo de sus casos.

Cuando las instituciones públicas, encargadas de proteger los derechos de las víctimas, no actúan con la debida diligencia, se perpetúa la violencia de género. Esto incluye la imposibilidad de acceder a servicios legales, psicológicos o médicos esenciales, lo que agrava la situación de vulnerabilidad de las mujeres afectadas por la VG FT y refuerza la impunidad de los agresores. Garantizar el acceso efectivo a la justicia en estos casos no solo es una obligación legal, sino también un compromiso con los Derechos Humanos y la igualdad de género.

Violencia en Acceso a Servicios

La violencia en el acceso a servicios ocurre cuando una institución pública, de manera intencional o negligente, dificulta o niega a las víctimas el acceso a servicios esenciales, como asistencia legal, médica o psicológica. Esta negativa impide que las víctimas de VG FT obtengan el apoyo necesario para su bienestar y para buscar justicia. La negativa de atencion se traduce en la violación a los derechos fundamentales de las mujeres. El reconocimiento y la sanción de estas conductas son esenciales para garantizar que las instituciones públicas cumplan con su rol de proteger y asistir a las víctimas, erradicando así cualquier forma de violencia facilitada por la tecnología.

- **Tipo Penal:** Incumplimiento de deberes de protección a mujeres en situación de violencia (Artículo 154 bis del Código Penal).

- **Acción Penal:** Pública de oficio.

Uso de Recursos Públicos para Ejercer la Violencia

El uso de recursos públicos para ejercer la violencia se refiere a la utilización indebida de recursos o instancias estatales para perpetuar la violencia de género. Esto puede manifestarse mediante acciones que favorecen al agresor o la falta de protección hacia las víctimas, lo que refuerza un sistema de impunidad y perpetúa la violencia.

- **Tipo Penal:** Incumplimiento de deberes de protección a mujeres en situación de violencia (Artículo 154 bis del Código Penal).

- **Acción Penal:** Pública de oficio.

Tabla 21.

INCUMPLIMIENTO DE DEBERES DE PROTECCIÓN A MUJERES EN SITUACIÓN DE VIOLENCIA	
Tipo penal	ARTÍCULO 154 bis. (INCUMPLIMIENTO DE DEBERES DE PROTECCIÓN A MUJERES EN SITUACIÓN DE VIOLENCIA). La servidora o servidor público que mediante acción u omisión en ejercicio de una función pública propicie la impunidad u obstaculicen la investigación de delito de violencia contra las mujeres, recibirá sanción alternativa de trabajos comunitarios de noventa (90) días a ciento veinte (120) días e inhabilitación de uno (1) a cuatro (4) años para el ejercicio de la función pública.
Sujeto Activo	Servidora o servidor público
Sujeto Pasivo	Mujer, víctima de un delito de violencia.
Bien Jurídico Protegido	Función Pública
Sanción	Dependiendo a qué delito subsume su conducta
Fiscalía Especializada	Fiscalía Especializada en Delitos de Corrupción, Tributarios, Aduaneros y Legitimación de Ganancias Ilícitas.

Fuente: elaboración propia.

2.5.6. Discurso de odio a través de las TIC

Expresiones Discriminatorias y Estigmatizantes

- **Tipo Penal:**

Discriminación (Artículo 281° sexies del Código Penal).

Difusión e incitación al racismo o a la discriminación (Artículo 281° septies del Código Penal).

Insultos y otras agresiones verbales por motivos racistas o discriminatorios (Artículo 281° nonies del Código Penal).

- **Acción Penal:** Pública de oficio.

Tabla 22.

DISCRIMINACIÓN	
Tipo penal	ARTÍCULO 281° sexies.- (DISCRIMINACIÓN). I. La persona que arbitrariamente e ilegalmente obstruya, restrinja, menoscabe, impida o anule el ejercicio de los derechos individuales y colectivos, por motivos de sexo, edad, género, orientación sexual e identidad de género, identidad cultural, filiación familiar, nacionalidad, ciudadanía, idioma, credo religioso, ideología, opinión política o filosófica, estado civil, condición económica o social, enfermedad, tipo de ocupación, grado de instrucción, capacidades diferentes o discapacidad física, intelectual o sensorial, estado de embarazo, procedencia regional, apariencia física y vestimenta, será sancionado con pena privativa de libertad de uno a cinco años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Dignidad del ser humano
Sanción	1 a 5 años de privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos contra la vida y la integridad personal

Fuente: elaboración propia.

Tabla 23.

DIFUSIÓN E INCITACIÓN AL RACISMO O LA DISCRIMINACION	
Tipo penal	ARTÍCULO 281° septies.- (DIFUSIÓN E INCITACIÓN AL RACISMO O A LA DISCRIMINACIÓN). La persona que por cualquier medio difunda ideas basadas en la superioridad o en el odio racial, o que promuevan y/o justifiquen el racismo o toda forma de discriminación, por los motivos descritos en los Artículos 281 bis y 281 ter, o incite a la violencia, o a la persecución, de personas o grupos de personas, fundados en motivos racistas o discriminatorios, será sancionado con la pena privativa de libertad de uno a cinco años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Dignidad del ser humano
Sanción	1 a 5 años de privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos contra la vida y la integridad personal

Fuente: elaboración propia.

Tabla 24.

INSULTOS Y OTRAS AGRESIONES VERBALES POR MOTIVOS RACISTAS O DISCRIMINATORIOS	
Tipo penal	ARTÍCULO 281 nonies.- (INSULTOS Y OTRAS AGRESIONES VERBALES POR MOTIVOS RACISTAS O DISCRIMINATORIOS). El que por cualquier medio realizare insultos u otras agresiones verbales, por motivos racistas o discriminatorios descritos en los Artículos 281 bis y 281 ter, incurrirá en prestación de trabajo de cuarenta días a dieciocho meses y multa de cuarenta a ciento cincuenta días.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Dignidad del ser humano
Sanción	40 días a 18 meses de trabajo y multa de 40 a 150 días
Fiscalía Especializada	Fiscalía especializada en delitos contra la vida y la integridad personal

Fuente: elaboración propia.

Linchamiento Digital

- **Tipo Penal:** Instigación pública a delinquir (Artículo 130 del Código Penal).

- **Acción Penal:** Pública de oficio.

Tabla 25.

INSTIGACIÓN PÚBLICA A DELINQUIR	
Tipo penal	ARTÍCULO 130 o.- (INSTIGACIÓN PÚBLICA A DELINQUIR). El que instigare públicamente a la comisión de un delito determinado, será sancionado con reclusión de un mes a un año. Si la instigación se refiere a un delito contra la seguridad del Estado, la función pública o la economía nacional, la pena aplicable será de reclusión de tres meses a dos años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Cualquier persona
Bien Jurídico Protegido	Tranquilidad pública
Sanción	3 meses a 2 años privación de libertad
Fiscalía Especializada	Fiscalía Especializada en Delitos de Corrupción, Tributarios, Aduaneros y Legitimación de Ganancias Ilícitas.

Fuente: elaboración propia.

2.5.7. Afectaciones a mujeres en política

La participación política de las mujeres es un derecho fundamental consagrado en la Constitución Política del Estado Plurinacional de Bolivia y desarrollado en la Ley No. 243 Contra el Acoso y la Violencia Política hacia las Mujeres. Esta ley tiene como objetivo prevenir, sancionar y erradicar las diversas formas de violencia que enfrentan las mujeres en el ámbito político, garantizando su acceso, permanencia y desarrollo en espacios de toma de decisiones sin discriminación ni intimidación.

El acoso político y la violencia política contra las mujeres representan barreras significativas para el ejercicio pleno de sus derechos políticos y económicos. Estas conductas no sólo vulneran la dignidad de las mujeres, sino que también perpetúan la exclusión de género en la política, limitando la consolidación de la democracia paritaria.

Acoso político contra mujeres

- **Tipo Penal:** Acoso Político contra Mujeres (Artículo 148 Bis del Código Penal).

- **Acción Penal:** Pública a instancia de parte.

Tabla No 26

ACOSO POLÍTICO CONTRA MUJERES	
Tipo penal	ARTÍCULO 148 Bis (ACOSO POLÍTICO CONTRA MUJERES).- Quien o quienes realicen actos de presión, persecución, hostigamiento y/o amenazas en contra de una mujer electa, designada o en el ejercido de la función político - pública y/o de sus familiares, durante o después del proceso electoral, que impida el ejercicio de su derecho político, será sancionado con pena privativa de libertad de dos (2) a cinco (5) años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Mujer electa, designada o en el ejercido de la función político - pública
Bien Jurídico Protegido	Libertad política
Sanción	2 a 5 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos en violencia en razón de género

Fuente: elaboración propia.

Violencia política contra mujeres

- **Tipo Penal:** Violencia Política contra Mujeres (Artículo 148 Ter del Código Penal).

- **Acción Penal:** Pública a instancia de parte.

Tabla 27.

VIOLENCIA POLÍTICA CONTRA MUJERES	
Tipo penal	ARTÍCULO 148 Ter. (VIOLENCIA POLÍTICA CONTRA MUJERES).- Quien o quienes realicen, actos y/o agresiones físicas y psicológicas **contra mujeres candidatos, electas, designadas o en ejercicio de la función político - pública y/o en contra de sus familiares, para acortar**, suspender e impedir el ejercicio de su mandato o su función, será sancionado con pena privativa de libertad de tres (3) a ocho (8) años. En casos de actos o agresiones sexuales contra las mujeres candidatos, electas, designadas o en ejercicio de la función político – pública, se sancionará conforme dispone este Código Penal.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Mujeres candidatas, electas, designadas o en ejercicio de la función político - pública
Bien Jurídico Protegido	Libertad política
Sanción	3 a 8 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos en violencia en razón de género

Fuente: elaboración propia.

2.5.8. Abuso de datos personales usando TIC

Según la Guía de prevención y atención de violencia de género facilitada por la tecnología[3], el abuso de datos personales usando Tecnologías de Información y Comunicación (TIC) se refiere a la obtención, uso o divulgación no autorizada de información personal a través de tecnologías de la información y comunicación. Este abuso puede implicar suplantación de identidad, acceso no consentido a cuentas, o divulgación de datos sin permiso, y es una forma de violencia digital que vulnera el derecho a la privacidad y la protección de datos. Los delitos relacionados al abuso de datos personales usando TIC son:

Suplantación y Robo de Identidad

- **Tipo Penal:**

1. **Falsedad Material** (Artículo 198° del Código Penal).
2. **Falsedad Ideológica** (Artículo 199° del Código Penal).
3. **Falsificación de Documento Privado** (Artículo 200° del Código Penal).

- **Acción Penal:** Pública de oficio.

3 ONU Mujeres & AGETIC. (2024). Guía de prevención y atención: Violencia de género facilitada por la tecnología

Tabla 28.

FALSEDAD MATERIAL	
Tipo penal	ARTÍCULO 198°.- (FALSEDAD MATERIAL). El que forjare en todo o en parte un **documento público** falso o alterare uno verdadero, de modo que pueda resultar perjuicio, incurrirá en privación de libertad de uno a seis años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Colectividad
Bien Jurídico Protegido	Fé Pública
Sanción	1 a 6 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos patrimoniales
Consideración	El artículo 1287 del Código Civil establece que un documento público o auténtico es el extendido con las solemnidades legales por un funcionario autorizado para darle fe pública. Es decir que son documentos públicos 1) El otorgado por funcionario autorizado en ejercicio de su cargo 2) La escritura pública y demás documentos otorgados por o ante notario de fe pública.

Fuente: elaboración propia.

FALSEDAD IDEOLÓGICA	
Tipo penal	ARTÍCULO 199°.- (FALSEDAD IDEOLÓGICA). El que insertare o hiciere insertar en un **instrumento público verdadero** declaraciones falsas concernientes a un hecho que el documento deba probar, de modo que pueda resultar perjuicio, será sancionado con privación de libertad de uno a seis años. En ambas falsedades, si el autor fuere un funcionario público y las cometiere en el ejercicio de sus funciones, la sanción será de privación de libertad de dos a ocho años.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Colectividad
Bien Jurídico Protegido	Fé Pública
Sanción	2 a 8 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos patrimoniales
Consideración	Como se ha señalado anteriormente, el documento público está establecido por el artículo 1287 del Código Civil.

Fuente: elaboración propia.

Tabla 29.

FALSIFICACIÓN DE DOCUMENTO PRIVADO	
Tipo penal	ARTÍCULO 200°.- (FALSIFICACIÓN DE DOCUMENTO PRIVADO). El que falsificare material o ideológicamente un documento privado, incurrirá en privación de libertad de seis meses a dos años, siempre que su uso pueda ocasionar algún perjuicio.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Colectividad
Bien Jurídico Protegido	Fé Pública
Sanción	6 meses a 2 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos patrimoniales
Consideración	El tipo penal no se adapta a temas de género

Fuente: elaboración propia.

Obtención de Información personal no consentida

En la normativa nacional no existe un delito o contravención relacionado a la obtención de información personal no consentida, sin embargo, la Constitución Política del Estado protege el derecho a la privacidad, intimidad, honra, honor, propia imagen y dignidad. Este derecho asegura la protección contra interferencias indebidas en la vida privada de las personas, su imagen y su reputación en su artículo 21. Por su parte, el artículo 25 establece el derecho a la inviolabilidad de las comunicaciones y la privacidad del domicilio. Toda persona tiene derecho al secreto de sus comunicaciones privadas en cualquier forma, y estas no pueden ser interceptadas o divulgadas sin autorización judicial.

- **Acción Jurídica:** Acción Constitucional (como el Recurso de Amparo o Habeas Data).

Publicación no autorizada de datos personales (doxing)

Publicación No Autorizada de Datos Personales (Doxing) dependiendo del contexto, puede configurarse como una forma de acoso, que afecta la integridad y seguridad de la víctima.

- **Acción Jurídica:** Acción Constitucional o penal según el impacto del daño causado.

Aunque no hay un tipo penal específico para el doxing, esta práctica puede vincularse con delitos como el acoso digital o el daño a la privacidad, siendo necesario fortalecer la legislación para abordar esta problemática emergente. Sin perjuicio de lo anteriormente señalado, es importante destacar que el Código Civil Boliviano es la norma donde se desarrollan los derechos fundamentales relacionados a la imagen, privacidad e intimidad.

Derecho a la Privacidad

Artículo 21 del Código Civil Boliviano "Toda persona tiene derecho a la privacidad. Se prohíbe la intromisión en la vida privada sin el consentimiento del afectado, salvo en casos previstos por ley."

El derecho a la privacidad protege a las personas de intromisiones no deseadas en su vida personal. En el contexto digital, esto significa que nadie puede acceder, recopilar, almacenar o divulgar información personal sin el consentimiento explícito del titular de los datos. Las violaciones de privacidad en el ámbito digital incluyen el acceso no autorizado a correos electrónicos, la vigilancia sin consentimiento mediante software espía y la recopilación de datos personales por redes sociales o aplicaciones sin informar adecuadamente al usuario.

Derecho a la Intimidad

Artículo 22 del Código Civil Boliviano "Toda persona tiene derecho a la intimidad en los aspectos que afectan su vida personal y familiar. La vulneración de este derecho podrá dar lugar a acciones de defensa."

El derecho a la intimidad se refiere a la protección de aspectos personales y familiares que una persona desea mantener reservados. En el entorno digital, este derecho puede verse comprometido a través de la difusión no autorizada de imágenes íntimas, el monitoreo no consensuado de actividades en línea, y el acceso a mensajes privados. Las violaciones de la intimidad digital incluyen prácticas como el doxing (publicación de información privada para dañar a la persona). Para investigar estos delitos, es crucial que los investigadores forenses digitales sean capaces de rastrear las fuentes y documentar las violaciones sin comprometer aún más la intimidad de la víctima.

Derecho a la Honra

Artículo 23 del Código Civil Boliviano "La honra y el buen nombre son derechos inviolables que toda persona tiene. Cualquier acción que atente contra estos derechos podrá ser objeto de acciones legales para su protección."

El derecho a la honra protege la reputación de una persona frente a declaraciones o acciones que la deshonren o la difamen. En el ámbito digital, este derecho se ve frecuentemente afectado a través de difamaciones en redes sociales, publicaciones falsas y campañas de desprestigio. Por ejemplo, un comentario calumnioso en Facebook que busca dañar la reputación de una persona constituye una violación de su honra. Los delitos de cyberbullying, acoso en línea y la creación de contenido difamatorio son algunas de las acciones que deben ser investigadas cuidadosamente para proteger este derecho. Las pruebas digitales, como capturas de pantalla y registros de publicaciones, son esenciales para establecer la intencionalidad y el daño causado.

Derecho al Honor

Artículo 24 del Código Civil Boliviano "El derecho al honor protege la dignidad moral de las personas. Toda ofensa o menosprecio que atente contra esta dignidad podrá ser sujeto a reparaciones y sanciones."

El derecho al honor está vinculado con la dignidad moral de la persona, protegiendo a los individuos contra ataques que intenten menoscabar su integridad moral. En el entorno digital, esto se traduce en la protección contra insultos, humillaciones y comentarios degradantes publicados en plataformas sociales, foros en línea y sitios web.

Derecho a la Propia Imagen

Artículo 25 del Código Civil Boliviano "El uso y difusión de la imagen de una persona, sin su consentimiento, constituye una violación del derecho a la propia imagen. Toda persona puede demandar la protección de este derecho."

El derecho a la propia imagen protege a las personas de la difusión no autorizada de sus fotos o videos. En el ámbito digital, esto cubre situaciones donde se suben imágenes personales sin consentimiento en redes sociales, se crean *deepfakes* (imágenes o videos manipulados para alterar la identidad de alguien) o se distribuyen videos íntimos. La protección de la imagen en el entorno digital es crucial, y las acciones legales buscan garantizar que se respete la identidad visual de cada individuo. Las investigaciones deben incluir la identificación del origen de las imágenes compartidas, rastrear cómo se han distribuido y establecer la conexión entre la acción delictiva y el daño a la víctima.

Dignidad

Artículo 6 del Código Civil Boliviano "Toda persona tiene derecho a ser tratada con dignidad. Cualquier acto que atente contra este principio fundamental podrá ser objeto de acciones de protección y sanciones correspondientes."

El derecho a la dignidad es el fundamento que asegura que toda persona debe ser tratada con respeto, sin ser objeto de menosprecio o discriminación. En el entorno digital, la dignidad se ve vulnerada por prácticas como el ciberacoso, la humillación pública y la discriminación por motivos de género, raza o religión a través de plataformas en línea. Los discursos de odio y las acciones que degradan la dignidad de una persona en el ciberespacio son tan graves como los ataques en el mundo físico y merecen la misma atención legal. La documentación de las pruebas de estos ataques en línea es esencial para la presentación de denuncias efectivas.

Fraude Cibernético

El fraude cibernético implica el engaño económico a través de medios electrónicos, utilizando datos personales de la víctima con la intención de obtener un beneficio financiero, lo que genera un perjuicio patrimonial.

- **Tipo Penal:** Estafa (Artículo 335° del Código Penal).

- **Acción Penal:** Pública de oficio.

Tabla 30.

ESTAFA	
Tipo penal	ARTÍCULO 335°.- (ESTAFA). El que con la intención de obtener para sí o un tercero, un beneficio económico indebido, mediante engaños o artificios provoque fortalezca error en otro que motive la realización de un acto de disposición patrimonial en perjuicio del sujeto en error o de un tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Quien sufre perjuicio patrimonial
Bien Jurídico Protegido	Patrimonio
Sanción	1 a 5 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos patrimoniales
Consideración	El tipo penal no se adapta a temas de género, en el tipo penal es un requisito que exista un beneficio económico indebido.

Fuente: elaboración propia.

Crackeo (Acceso no autorizado a cuentas)

- **Tipo Penal:**

1. **Manipulación Informática** (Artículo 363 bis del Código Penal).
2. **Alteración, Acceso y Uso Indebido de Datos Informáticos** (Artículo 363 ter del Código Penal).

- **Acción Penal:** Pública de oficio.

Tabla 31.

MANIPULACIÓN INFORMÁTICA	
Tipo penal	ARTÍCULO 363 bis.- (MANIPULACIÓN INFORMÁTICA).- El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una **transferencia patrimonial** en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Quien sufre perjuicio patrimonial
Bien Jurídico Protegido	Integridad de sistemas informáticos
Sanción	1 a 5 años privación de libertad
Fiscalía Especializada	Fiscalía especializada en delitos patrimoniales
Consideración	El tipo penal no se adapta a temas de género, en el tipo penal es un requisito que exista la transferencia patrimonial

Fuente: elaboración propia.

ALTERACIÓN, ACCESO Y USO DE DATOS INFORMÁTICOS	
Tipo penal	ARTÍCULO 363 ter.- (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS).- El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.
Sujeto Activo	Cualquier persona
Sujeto Pasivo	Quien sufre perjuicio patrimonial
Bien Jurídico Protegido	Integridad de datos informáticos
Sanción	1 año prestación de trabajo o multa de 200 días
Fiscalía Especializada	Fiscalía especializada en delitos patrimoniales
Consideración	El tipo penal no se adapta a temas de género

Fuente: elaboración propia.

3. Elementos preliminares a la investigación

3.1. Recopilación de indicios

Un indicio es un hecho o conjunto de circunstancias que, sin ser concluyentes por sí mismos, permiten inferir la existencia de otro hecho que se busca probar en un proceso judicial. A diferencia de una prueba directa, los indicios no ofrecen una certeza inmediata, pero, mediante la lógica o el razonamiento, pueden llevar a la conclusión de un hecho relevante, los indicios son los elementos entregados por la parte denunciante al momento de la presentación de la denuncia.

Estos indicios se utilizan para construir una cadena de razonamientos que, de manera coherente, conducen a la conclusión sobre la existencia de un hecho. Es importante que los indicios sean concordantes, es decir, que no se contradigan entre sí y que apunten hacia la misma conclusión.

Los indicios con los que abre los delitos de VG FT y los demás descritos pueden ser:

- Valoraciones psicológicas y/o sociales
- Fotografías
- Enlaces (acompañado de capturas de pantalla del delito: foto de perfiles falsos)
- Correos electrónicos
- Captura de pantalla (de conversaciones, perfiles y otros, llamadas, mensajes de texto)
- Llamadas
- Mensajes de textos

¿Cómo obtener los indicios?

A efecto de obtener estos indicios existen herramientas gratuitas, una de ellas se denomina MOBILedit que es una herramienta forense utilizada para extraer datos de dispositivos móviles, como teléfonos y relojes inteligentes. Permite recuperar información eliminada, extraer contraseñas, analizar aplicaciones y generar informes forenses detallados. Es ampliamente utilizada en investigaciones policiales y forenses digitales para examinar dispositivos electrónicos como parte de una investigación criminal que demuestren los medios a través de los cuales se ha ejercido este tipo de violencia, posteriormente será la etapa investigativa la que reúna todas las pruebas necesarias para comprobar la existencia del ilícito y la participación del sindicado.

En todo proceso ya sea penal, civil, laboral o de cualquier otra materia, el elemento más importante es la recolección de pruebas, porque sólo así se puede demostrar el hecho; pero hoy en materia de procedimiento a las pruebas se las denomina de diferente forma dependiendo de la etapa procesal de una denuncia.

Algunas veces se ha confundido el término indicios con pruebas pero en un procedimiento judicial las pruebas son denominadas de esta forma en la última etapa de un proceso ya que demuestran la existencia del delito en cambio los indicios son elementos qué van a demostrar el posible hecho a ser investigado. Si una víctima tiene en su poder estos primeros elementos recién puede abrir una denuncia que dará paso a una investigación, esta denuncia es recibida o admitida en el departamento de análisis de la Fiscalía donde los fiscales analistas una vez leída la denuncia escrita o escuchada la denuncia verbal, pueden subsumir esta conducta a algún tipo en específico y remitir a la Fiscalía especializada de acuerdo al caso concreto para que un fiscal de materia sea quien comience la investigación.

Una vez ha tenido conocimiento el fiscal de materia del hecho delictivo requiere a la FELCC o a la FELCV se asigne un investigador para que como brazo operativo comience a recolectar los primeros elementos a partir de esos indicios y ya iniciada una investigación se denominan evidencias.

4. La investigación

Una vez admitida la denuncia, se dan dos hitos importantes, las directrices de investigación y las medidas de protección, sin embargo en esta guía, desarrollaremos las directrices de investigación

4. 1. Directrices de investigación

Las directrices de investigación son un conjunto de pautas, lineamientos o procedimientos establecidos para guiar y estructurar el proceso de investigación en diferentes ámbitos, incluyendo los campos jurídico, policial, académico y científico. Estas directrices sirven como un marco de referencia para asegurar que la investigación se realice de manera coherente, ordenada, eficiente y conforme a normas establecidas.

Características y objetivos de las directrices de investigación:

- **Organización:** Establecen un plan o cronograma que permite organizar las etapas y recursos de la investigación de manera sistemática.
- **Metodología:** Definen los métodos o técnicas que deben emplearse para obtener, analizar y verificar la información o pruebas.
- **Cumplimiento legal:** Aseguran que la investigación siga los marcos legales y éticos correspondientes, especialmente en el ámbito penal o judicial.
- **Claridad de objetivos:** Las directrices ayudan a precisar los objetivos de la investigación, identificando las preguntas que se quieren responder y los resultados esperados.
- **Eficiencia:** Permiten maximizar los recursos (tiempo, personal, tecnología) y minimizar los errores o la duplicación de esfuerzos.
- **Transparencia y rendición de cuentas:** Las directrices proporcionan un marco para documentar cada paso de la investigación, facilitando la revisión o auditoría en caso de que sea necesario.

En el ámbito judicial o penal, las directrices de investigación incluyen:

- **Métodos de recolección de pruebas:** Cómo deben ser obtenidas las evidencias físicas, digitales o testimoniales.

- **Custodia de pruebas:** Cómo preservar y manejar la cadena de custodia para que las evidencias no sean contaminadas o manipuladas.

- **Técnicas de interrogatorio:** Cómo y cuándo realizar interrogatorios o entrevistas, respetando los derechos de las personas involucradas.

- **Coordinación interinstitucional:** Cuando varias entidades están involucradas, las directrices aseguran una adecuada comunicación y cooperación.

Las directrices de investigación son esenciales para garantizar que el proceso investigativo sea riguroso, organizado y conforme a los estándares legales o científicos aplicables. Cabe señalar que estas directrices emitidas por el fiscal desde el primer momento en que tiene conocimiento de un hecho delictivo son estandarizadas en cada unidad especializada del Ministerio Público, pero casi siempre contienen:

- Declaración de la víctima
- Declaración de posibles testigos
- Registro del lugar del hecho
- Declaración del sindicado
- Valoraciones psicológicas y sociales

4. 2. ¿Qué pruebas y pericias recabar en casos de violencia digital?

Las pruebas se recabarán a través de los requerimientos fiscales, que son solicitudes emitidas por el Ministerio Público (fiscal) en el marco de una investigación penal, a fin de que se realicen determinadas actuaciones o diligencias relacionadas con el caso. Estos actos procesales permiten al fiscal dirigir la investigación, recolectar pruebas, y tomar decisiones en función de los hallazgos de la investigación.

Mediante los requerimientos fiscales, el fiscal puede solicitar a la policía o a otras autoridades la realización de actos investigativos como entrevistas, peritajes, recolección de evidencias, o inspecciones en lugares específicos, así mismo permiten al fiscal solicitar las actuaciones necesarias para esclarecer los hechos investigados, recolectar pruebas, y avanzar en el proceso penal.

En casos de Violencia de Género las valoraciones social y psicológica son las primeras en realizarse debido a su importancia para entender el contexto integral de la víctima y el impacto de la violencia. Ambas valoraciones son esenciales no sólo para orientar las intervenciones legales y de protección, sino también para definir medidas inmediatas de apoyo integral, asegurando que las respuestas sean oportunas y basadas en las necesidades específicas de la víctima.

Por otra parte tenemos las pericias, en los casos de VG FT, son tres las pericias que toman vital relevancia en la investigación, la pericia psicológica, la valoración social y la pericia informática. La pericia psicológica y la valoración social permitirán demostrar el daño ocasionado por este tipo de violencia, en el ámbito mental de la víctima y aspecto social; por otro lado la pericia informática forense permitirá respaldar el testimonio de la víctima en situación de violencia, así como identificar al agresor y su comportamiento.

4. 3. Valoración Social

La valoración social es un proceso integral de evaluación, realizado por un profesional en Trabajo Social, que analiza las condiciones sociales, económicas, familiares y ambientales de una persona o familia involucrada en un proceso legal. La valoración social es la herramienta que en delitos de violencia de género facilitados por la tecnología demostrarán cómo lo virtual afecta en el espacio físico.

Aspectos fundamentales de la valoración social

El fin de la valoración social es identificar los efectos sociales de la violencia en la vida de la víctima, por esta razón las dos ideas centrales son: evaluar el entorno social e identificar la necesidad de recursos, con estos dos aspectos se podrá realizar un análisis de cómo la violencia ha afectado la vida diaria de la mujer en situación de violencia.

- **Evaluar el Entorno Social:** Comprender el contexto en el que vive la persona o familia, incluyendo aspectos como la vivienda, el entorno comunitario, las relaciones familiares y sociales.

- **Identificar Necesidades y Recursos:** Determinar las necesidades específicas de la persona o familia y los recursos disponibles para satisfacerlas, tanto a nivel individual como comunitario.

Tratándose de VG FT las valoraciones sociales serán utilizadas para:

1. Evaluar el impacto del delito en la vida y entorno de la víctima.
2. Sirven de apoyo a momento de tomar decisiones en cuanto a las medidas de protección y sus alcances
3. Deberían ser utilizadas al momento de tomar decisiones relacionadas con la reparación integral del daño.

Métodos de recopilación de Información

- **Entrevistas:** Con la persona evaluada, miembros de la familia, amigos, maestros, empleadores, etc.

- **Observación Directa:** Visitas al hogar y al entorno comunitario.

- **Revisión de Documentos:** Historial médico, escolar, laboral, informes previos, entre otros.

- **Aplicación de Instrumentos de Evaluación:** Cuestionarios estandarizados y pruebas específicas para medir aspectos psicológicos y sociales.

El trabajador social analiza la información recopilada para identificar patrones, necesidades y recursos. Este análisis se basa en criterios objetivos y en estándares profesionales reconocidos.

El informe de valoración social se presenta ante el tribunal, que lo considera junto con las demás pruebas para tomar decisiones informadas y justas.

4. 4. Valoración Psicológica

La valoración psicológica es un procedimiento técnico realizado por profesionales en psicología con el objetivo de identificar y evaluar el impacto psicológico sufrido por la víctima debido a los actos de violencia. Este análisis se convierte en un elemento fundamental en el proceso penal, ya que permite proporcionar pruebas que acrediten no sólo la existencia de la agresión, sino también sus efectos emocionales, cognitivos y conductuales.

Aspectos fundamentales de la valoración psicológica

- **Obtener datos personales y familiares:** Un aspecto inicial y esencial de la valoración psicológica es recopilar información personal y familiar de la víctima. Este paso no sólo permite identificar plenamente a la persona evaluada, sino que también contribuye a contextualizar el entorno familiar y social en el que se desenvuelve. Conocer estos detalles es clave para comprender las dinámicas que pueden haber favorecido o agravado la situación de violencia, así como para identificar posibles factores de protección o vulnerabilidad. Entre los datos a considerar se incluyen la edad, el nivel educativo, la situación laboral, las relaciones familiares y los antecedentes de violencia en el entorno cercano.

- **Señalar el motivo de la evaluación:** La razón por la cual se lleva a cabo la valoración psicológica debe estar claramente definida. Esto implica detallar si la evaluación se realiza para determinar el impacto emocional de una situación de violencia, identificar indicadores de riesgo o proporcionar evidencia en un proceso judicial. Establecer el motivo es crucial para orientar la metodología de la evaluación, seleccionar las herramientas apropiadas y garantizar que los hallazgos respondan directamente a las necesidades específicas del caso. Además, comunicar el propósito de la valoración a la víctima ayuda a generar confianza y colaboración en el proceso.

- **Valoración Mental:** La valoración mental es un componente central del proceso, ya que permite evaluar el estado psicológico y emocional de la víctima en el momento de la evaluación. En esta etapa, el psicólogo analiza aspectos como el estado de ánimo, el nivel de ansiedad, la presencia de síntomas de estrés postraumático, alteraciones en la percepción o el pensamiento, y cualquier otro indicador relevante. Este análisis ofrece una visión integral del impacto de la violencia en la salud mental de la persona, proporcionando información crítica para el diagnóstico y la intervención.

- **Impresión diagnóstica:** La impresión diagnóstica es el resultado de la evaluación psicológica y sintetiza los hallazgos obtenidos durante el proceso. Esta incluye un diagnóstico preliminar sobre los efectos psicológicos de la violencia, como estrés, depresión, ansiedad o trastornos de estrés postraumático, entre otros. Además, la impresión diagnóstica relaciona estos hallazgos con los hechos de violencia denunciados, estableciendo un vínculo causal que puede ser de gran utilidad en el contexto judicial. Es importante que esta impresión sea clara, precisa y sustentada en los datos recopilados durante la evaluación.

4. 5. Métodos de recopilación de Información

La recopilación de información en una valoración psicológica se realiza utilizando diversas herramientas diseñadas para obtener datos relevantes de manera estructurada y confiable. Uno de los métodos más comunes es la entrevista semiestructurada, que permite explorar de manera flexible y profunda los antecedentes de la víctima, su percepción de los hechos y el impacto emocional experimentado. También se utilizan pruebas proyectivas como el test del "Hombre bajo la lluvia", que ayuda a identificar estados emocionales, miedos y recursos psicológicos de la persona evaluada.

Sin embargo, cada SLIM, DNA, o psicólogo tendrá sus métodos para realizar la valoración psicológica.

4. 6. Pericias relevantes para la violencia digital

En Bolivia, la **Resolución FGE/JLP/DAJ N° 186/2019**, emitida el 7 de agosto de 2019 por la **Fiscalía General del Estado**, establece los **puntos de pericia** para diversas áreas de las ciencias forenses. Esta resolución define lineamientos específicos para la realización de peritajes, incluyendo los procedimientos y criterios técnicos a seguir en cada especialidad.

En el contexto de VG FT, estas pericias forenses resultan especialmente relevantes, ya que proporcionan datos específicos y efectos relacionados a la VG FT Es importante destacar que estos puntos de pericia actúan como una guía técnica, sin embargo, es el abogado o fiscal quien deberá adaptar estos puntos de pericia según la necesidad del caso.

4.6.1. Perícias Psicológicas

Las pericias psicológicas son evaluaciones realizadas por profesionales de la psicología con el propósito de aportar información especializada al proceso judicial. Es importante señalar que la pericia psicológica o psiquiátrica se realizan posterior a la valoración psicológica. Estas pericias son fundamentales para demostrar el daño ocasionado por los agresores, estas pericias son cruciales al momento de que el juez o tribunal tome una decisión.

La pericia psicológica se puede realizar tanto a la víctima como al imputado o acusado, sin embargo, es importante enfatizar que, según los estándares internacionales de Derechos Humanos, la pericia psicológica no debe utilizarse para desacreditar o revictimizar a la víctima, sino como un medio para garantizar una investigación imparcial y efectiva.

4.6.2. Puntos de Pericia

Tabla 32.

VÍCTIMAS Y/O TESTIGOS	IMPUTADOS/ACUSADOS
• Establecer la presencia de daño psicológico o secuelas como consecuencia del hecho denunciado. • Determinar la credibilidad del testimonio respecto al hecho denunciado. • Determinar rasgos y características de personalidad de la víctima (este punto de pericia no es necesario solicitarlo en niñas y niños, por la etapa de desarrollo; además que debe solicitarse de acuerdo a cada caso particular). • Autopsia psicológica (sólo víctima fallecida en casos de muertes dudosas).	• Determinar la presencia de algún Trastorno mental. • Valorar el riesgo de violencia sexual. • Valorar el riesgo de violencia contra la mujer (pareja, madre, hija, otra). • Valorar el riesgo de violencia. • Establecer la presencia de trastorno por consumo de sustancias. • Determinar rasgos y/o características de personalidad del imputado/acusado.

Procedimiento para la solicitud de pericias

- **Solicitud de la Pericia:** Este tipo de pericias son solicitadas por la fiscalía o por las partes en el proceso de investigación, tanto el Instituto de Investigaciones Forenses (IDIF) como el Instituto de Investigaciones Técnico Científicas de la Universidad Policial (IITCUP) cuentan con profesionales con la experticia para este tipo de estudios científicos y especializados, la pericia sólo se lleva a cabo previo requerimiento fiscal; en la etapa de juicio también se pueden llevar a cabo si el juez o tribunal lo admite y sólo para llegar a conocer la verdad de los hechos y bajo el principio de verdad material consagrado en la Constitución Política del Estado.
- **Nombramiento del Psicólogo Perito:** Una vez emitido el requerimiento u orden judicial la designación se la hace internamente ya sea en el IDIF o IITCUP. Esta designación ya no requiere del juramento dispuesto en la normativa; ahora todo profesional a momento de formar parte del señalado instituto científico presta el juramento para ejercer su labor de manera imparcial y con la experiencia necesaria, toda vez que se requiera profesionales capacitados para llevar a cabo la evaluación.
- **Recopilación de Información:** El psicólogo realiza entrevistas, aplica pruebas psicológicas estandarizadas y recopila antecedentes relevantes (historial médico, escolar, laboral, etc.).
- **Elaboración del Informe:** El perito redacta un informe detallado que incluye metodología, hallazgos, conclusiones y recomendaciones basadas en la evaluación realizada.
- **Presentación del Informe al Tribunal:** El informe se presenta ante el fiscal, juez o tribunal, quien lo considerará como parte de las pruebas para la toma de decisiones.
- **Declaración del Perito en Juicio:** El psicólogo perito puede ser citado a declarar en el juicio para explicar sus hallazgos y responder a preguntas de las partes y del tribunal.

  Las pericias psicológicas también se llevan a cabo tratándose de los imputados, tratándose de VG FT además de obtener un perfil de personalidad y propensión a la agresividad sería crucial poder identificar a través de este método de investigación la propensión o adicción a la utilización de los medios digitales.

4.6.3. Pericia Psiquiatra

La pericia psiquiátrica es una evaluación especializada realizada por un psiquiatra en el contexto legal o forense para determinar el estado mental de una persona y su relación con hechos específicos en un caso judicial. Se utiliza en diferentes áreas del derecho, como el penal, civil, familiar o laboral, para proporcionar elementos técnicos que puedan influir en la resolución de un caso. Las pericias psiquiátricas tienen como fin: Determinar si una persona presenta trastornos psiquiátricos que puedan haber influido en su conducta.

4.6.4. Puntos de pericia

Tabla 33.

VÍCTIMAS Y/O TESTIGOS	IMPUTADOS/ACUSADOS
• Analizar si existe relación causal entre los hechos denunciados y las afectaciones psicológicas observadas en la víctima. • Determinar capacidad cognitiva intelectiva, indemnidad o afectación de sus funciones ejecutivas o juicio de realidad y enfermedad. • Necesidad de hospitalización, guarda, custodia y tratamiento psicofarmacológico. • Identificación de estructuras patológicas de riesgo social criminal, mórbidas y disfuncionales de la personalidad. (Antisocial, narcisista, sádica, paranoide, limítrofe, esquizotípica, compulsiva u otros en nivel umbral patológico) asociadas a conductas de ilícito.	• Determinar si el evaluado presenta alteraciones psiquiátricas que afecten su capacidad de comprender el carácter ilícito de sus acciones • Determinar la comprensión/ incomprensión de la licitud de sus acciones. • Riesgo de reincidencia de ilícitos y conductas predatorias. • Determinar Afectación, lesión o secuela psíquica. • Determinar Presencia / Ausencia de conductas violentas recurrentes y su asociación con la enfermedad mental.

Fuente: elaboración propia.

Procedimiento para la solicitud de pericia

Respecto a la pericia psiquiátrica es importante señalar que no se cuenta con un médico psiquiatra en el IDIF, por lo cual se debe requerir una terna a la Sociedad Boliviana de Psiquiatría, según su filial, para que se designe a un profesional en esta área.

4. 7. Pericias informática forense

La pericia informática forense es un conjunto de técnicas de investigación que se utilizan para recopilar, analizar y presentar evidencia digital derivadas de dispositivos electrónicos respetando las normas legales. Esto puede incluir la recuperación y análisis de información almacenada en ordenadores, dispositivos móviles, servidores y redes. Se utiliza en contextos jurídicos para descubrir y examinar datos de dispositivos electrónicos para su uso en procedimientos judiciales.

En Bolivia, según los tipos de VG FT se puede pedir una pericia informática al momento de iniciar una denuncia. Para esto es necesario identificar el delito relacionado con VG FT y los puntos de pericia para realizar la solicitud. Existen dos tipos de métodos de recopilación de información: física al secuestro o colecta del dispositivo y digital de la información en el dispositivo.

Para poder identificar en qué delito se necesita pericia informática forense, se presenta el siguiente cuadro con los puntos específicos de solicitud de pericia.

4.7.1. Puntos de Pericia

Las pruebas digitales (o pruebas electrónicas) se refieren a “cualquier tipo de información que puede ser extraída de sistemas informáticos u otros dispositivos digitales y que puede usarse para probar o desmentir un delito”. El principal punto de pericia es el siguiente:

- Proceder a la extracción y listado de toda la evidencia digital contenida en el medio de almacenamiento cuestionado (descripción e individualización de la evidencia). Al mencionar “evidencia digital” se engloba archivos digitales generados en software:
  - **De ofimática:** Word, Excel, power point, etc.
  - Audio
  - Video.
  - Bases de datos.
  - Correo electrónico.

Pueden ser medios de almacenamiento los discos duros HDD, discos SSD, pendrives, flash memories, y otros. Al mismo tiempo la evidencia digital contenida en equipos de telefonía móvil. Dicha evidencia consistente en pero no limitada a:

- Contactos,
- Listado de llamadas, perdidas, recibidas, salientes,
- Correo electrónico.
- Aplicaciones de redes sociales (Whatsapp, Messenger, telegram, etc.)
- Video.
- Grabaciones de audio.

Otros requerimientos a realizar:

- Proceder a la identificación del titular del número telefónico (especificar número), verificando a través de los registros oficiales del operador de telecomunicaciones (ENTEL, VIVA O TIGO) a nombre de quién se encuentra registrado dicho número, incluyendo detalles sobre la fecha de activación e historial de titularidad.

- Proceder a la extracción y análisis de los registros de llamadas del número telefónico (especificar número), incluyendo llamadas entrantes, salientes y perdidas, con detalle de fechas, horas, duración y números de contacto involucrados, a fin de identificar patrones de frecuencia y recurrencia.

4.7.2. Procedimiento para la solicitud de pericia

Se puede hacer la solicitud de pericias en dos instancias a través de la Policía Bolivia por el ITCUP y la Fiscalía por el IDIF.

- **Fiscalía.** En el caso con la Fiscalía, según la Guía de Puntos de Pericia se recomienda remitir los equipos a IDIF ni bien sea el secuestro o colecta. Al mismo tiempo, no se permite la observación ajena que no sea dentro de las condiciones forenses, principalmente para evitar pérdida o daño a la información.

- **Policía Boliviana.** Por otro lado, la Policía Boliviana puede solicitar informes a través del Área de Cibercrimen.

4.7.3. Claves en la Pericia

Respecto a la informática forense es importante destacar los siguientes puntos:

- **Desarrollar una línea del tiempo:** Es fundamental desarrollar una línea del tiempo detallada que establezca las fechas específicas de las agresiones digitales. Esto permite contextualizar los hechos denunciados, identificar patrones de conducta del agresor y fortalecer la correlación entre los eventos narrados por la víctima y la evidencia digital obtenida. Una cronología bien estructurada es esencial para sustentar la denuncia y garantizar que los elementos probatorios sean claros, precisos y fácilmente comprensibles en el proceso judicial.

- **Periodos exactos:** Es indispensable solicitar en los requerimientos judiciales las fechas exactas en las que presuntamente ocurrieron las agresiones. De igual manera, se debe especificar la plataforma o aplicación de la cual se hará la extracción de información, como redes sociales, servicios de mensajería o correos electrónicos. Sin esta especificidad, los operadores técnicos no podrán garantizar que los datos recolectados correspondan directamente a los hechos denunciados, lo que podría debilitar el caso. Por ello, los requerimientos deben incluir detalles como el tipo de contenido (mensajes, imágenes, videos, audios) y los periodos de tiempo exactos a investigar.

- **Concordancia entre pruebas presentadas y relato:** Los metadatos asociados a las capturas de pantalla constituyen un elemento crucial en la investigación, ya que contienen información técnica que valida la autenticidad de la evidencia. Detalles como la fecha y hora de creación, la aplicación utilizada y el dispositivo desde el cual se generó deben coincidir con los hechos narrados por la víctima. Una discrepancia entre los metadatos y el testimonio puede generar dudas sobre la validez de la prueba, comprometiendo su aceptación en el proceso judicial. Por esta razón, es imprescindible que el análisis técnico incluya la verificación de los metadatos y que estos sean preservados en su estado original.

- **Conservar dispositivo de origen:** El dispositivo de origen donde se almacenan las pruebas (como teléfonos móviles, computadoras o tablets) debe ser resguardado adecuadamente para garantizar la integridad de la evidencia. Esto implica mantener el dispositivo en condiciones seguras, evitar su manipulación y documentar cualquier acceso o extracción de información. La preservación del dispositivo no sólo asegura la autenticidad de la evidencia, sino que también permite realizar análisis técnicos adicionales en caso de ser necesario. Este resguardo es fundamental para prevenir alegaciones de alteración o manipulación.

4.7.4. Peritos de Parte

El artículo 209, permite la designación de peritos de parte, un perito de parte es un profesional especializado que es contratado por una de las partes involucradas en un proceso judicial (ya sea la parte acusadora o la parte acusada) para realizar una evaluación, análisis o dictamen técnico en un área determinada. Su objetivo es ofrecer una opinión experta que respalde la posición de la parte que lo contrata.

Aunque es contratado por una de las partes, el perito de parte debe realizar su labor con imparcialidad técnica y basarse en criterios objetivos y científicos en su informe o dictamen, aunque su análisis esté dirigido a favorecer los intereses de la parte que lo presenta.

El perito de parte puede ser un experto en diversas áreas como medicina, psicología, ingeniería, contabilidad, informática, entre otras, dependiendo de la naturaleza del caso. Su función es emitir un dictamen sobre aspectos técnicos o especializados que requieren conocimientos más allá del ámbito legal, elabora un informe con sus conclusiones, que será presentado ante el juez o tribunal. Este informe puede servir para contrarrestar o complementar el dictamen del perito estatal.

Otro factor importante a momento de ejercer el derecho a la defensa y producción de pruebas de parte, es el económico, toda vez que el perito de parte al ser un especialista particular experto en un tema determinado o con una experticia específica tiene un elevado costo, más si se toma en cuenta que por la excesiva carga laboral de los peritos designados por el Estado, muchas veces su trabajo y defensa de informe en etapa de juicio no da mayor explicación que toda autoridad jurisdiccional requiere al momento de emitir una resolución.

4.7.5. Consultor técnico

Un consultor técnico en el ámbito judicial es un profesional especializado que asiste a una de las partes en un proceso legal, brindando asesoramiento técnico o científico. A diferencia de un perito de parte, el consultor técnico no necesariamente presenta un dictamen oficial ante el juez o el tribunal, sino que asesora de manera interna a los abogados o las partes sobre cuestiones complejas y especializadas que pueden surgir durante el proceso.

El consultor técnico ofrece su experiencia y conocimientos en áreas técnicas o científicas para ayudar a la parte que lo contrata, a diferencia del perito, el consultor técnico no tiene una función formal en el proceso judicial. Su rol es más discreto, trabajando junto al equipo legal para preparar estrategias y entender aspectos técnicos que puedan ser relevantes para el caso, puede ayudar a revisar pruebas periciales, informes o dictámenes, asegurándose de que estén correctamente fundamentados o identificando puntos débiles en los informes de los peritos de la otra parte o los peritos judiciales.

5. Comunicación directa con las plataformas

De acuerdo a la Guía de prevención y atención de género facilitada por la tecnología[4] para la investigación en determinados casos, es necesario obtener información que es manejada por las plataformas de redes sociales (Facebook, Tiktok, Instagram, etc).

El Código de Procedimiento Penal, determina que las y los fiscales, jueces y tribunales pueden requerir informes a entidades públicas y privadas, y que dichos informes pueden ser solicitados por cualquier medio. Entre las entidades privadas deben considerarse a las plataformas de Internet y redes sociales.

Considerando estos aspectos, dichas plataformas han puesto a disposición de las autoridades judiciales, fiscales o policiales de los distintos países, la posibilidad de solicitar información con requerimientos judiciales.

Estas solicitudes se encuentran en las plataformas digitales con la denominación de *Law Enforcement Online Requests* o Solicitudes en línea para el cumplimiento de la ley, y requieren que las solicitudes se realicen por funcionarias/os autorizados, mediante el uso de correos electrónicos oficiales, descripción del caso, descripción del tipo de información solicitada y los requerimientos judiciales correspondientes.

Cabe mencionar que a través de estas plataformas de solicitud, se brinda solo determinado tipo de información sobre cuentas, por ejemplo IP de conexión, correos vinculados a las cuentas, horas de conexión, etc.

Pero cuando la información que se requiera sea más compleja, como por ejemplo el contenido de una comunicación, debe realizarse mediante exhortos suplicatorios[5] con todas las formalidades requeridas para procesos de cooperación judicial internacional.

A continuación, se presentan algunos enlaces de las plataformas[6] para la solicitud de información o de folletos informativos sobre dichas solicitudes:

- **Facebook e Instagram** - *Law Enforcement Online Requests* o Solicitudes en línea para el cumplimiento de la ley: https://www.facebook.com/records/login/
- **Facebook e Instagram** - Información para las fuerzas del orden (Español): https://www.facebook.com/help/instagram/494561080557017
- **Whatsapp** - Law Enforcement Online Requests o Solicitudes en línea para el cumplimiento de la ley: https://www.whatsapp.com/records/login
- **Meta** - Información para las autoridades encargadas de hacer cumplir la ley: https://about.meta.com/actions/safety/audiences/law/guidelines
- **X/ anteriormente Twitter** - *Law Enforcement Online Requests* o Solicitudes en línea para el cumplimiento de la ley: https://help.twitter.com/en/forms/law-enforcement/request-for-account-info/le-rep
- **Google** - Preguntas frecuentes acerca de las solicitudes de información sobre los usuarios: https://support.google.com/transparencyreport/answer/9713961?hl=es-419&sjid=6191332934861888661-SA#zippy=
- **Snapchat** - Información para las fuerzas de seguridad: https://values.snap.com/es-MX/safety/safety-enforcement

4 Documento emanado por la autoridad judicial cuando se debe realizar alguna diligencia en el extranjero en relación a los actos de comunicación procesal o de recepción u obtención de pruebas e informes.

5 En algunos casos, las plataformas y solicitudes se encuentran o deben realizarse en inglés.

6 Cespedes, D., Larrea, E., Sanabria Tovar, B. F., Méndez, L. A., & Rivera, N. (2024). Guía de prevención y atención de Violencia de género facilitada por la tecnología. Disponible: https://internetbolivia.org/wp-content/uploads/2024/01/violencia-cartilla-una-hoja-firmado.pdf

La investigación de casos de Violencia de Género Facilitada por la Tecnología (VG FT) en Bolivia se enfrenta a una falta de normativa además de falta de herramientas para la colección y custodia de las pruebas digitales que no tienen las mismas características que las pruebas físicas.

Los desafíos que presentan los procesos de investigación de casos de VG FT para abogados, fiscales y otros operadores de justicia derivan de la naturaleza de las pruebas involucradas que son altamente volátiles y susceptibles de ser destruidas o modificadas. Además, la identificación del agresor a menudo se complica debido al anonimato que es posible ejercer en espacios digitales, por lo que suele implicar la colaboración con empresas proveedoras de servicios digitales nacionales e internacionales y el uso de herramientas de rastreo tecnológico. Finalmente, otro de los retos es la rapidez con la que se difunden los contenidos en los entornos digitales.

La *Guía de investigación de casos de Violencia de Género Facilitada por la Tecnología (VG FT)* tiene como propósito proporcionar herramientas y directrices fundamentales para enfrentar la investigación de los delitos de VG FT. A lo largo de esta guía, se abordan aspectos esenciales para la comprensión y la investigación de estos delitos, tales como el marco jurídico nacional e internacional, las tipologías específicas de violencia digital, y las herramientas necesarias para la recolección y preservación de pruebas digitales. El enfoque está orientado a la prevención y a la atención efectiva de casos de VG FT, con un énfasis especial en la importancia de adaptar los procedimientos legales y técnicos a los retos que impone la digitalización.