**Curso "Ciudadanía y Derechos Humanos en la era digital"**

**Módulo 3: Ciberdelitos y estrategias de ciberseguridad**

**Documento de contenido**

Docente: Cristian León

## 1. Objetivo de aprendizaje

El objetivo de este módulo es reconocer las formas de ciberdelitos, el marco normativo existente y posibles estrategias de prevención de ciberseguridad a través del análisis e indagación de un caso.

## 2. Justificación

La ciberdelincuencia creció exponencialmente durante la pandemia debido a un mayor uso y dependencia de las tecnologías digitales, pues más personas tuvieron que empezar a conectarse a internet para el trabajo, la educación, la oferta de bienes y servicios, la comunicación con los seres queridos y el entretenimiento.

Entre las múltiples razones que facilitaron el incremento de la ciberdelincuencia están, por ejemplo, el mayor intercambio de datos personales que las personas ceden para acceder a bienes y servicios. Esta información circula y en algunos casos llega a manos de ciberdelincuentes, quienes la utilizan para cometer delitos. También el incremento de transacciones de dinero de manera electrónica a través del uso de QRs, los encuentros presenciales para concretar compras realizadas por espacios como Facebook Market o Whatsapp, la descarga de aplicaciones, juegos, películas, entre otras. Todos son factores que de alguna manera amplían las vulnerabilidades y la posibilidad de ser víctima del cibercrimen.

En ese contexto, la Policía Internacional (Interpol) reportó que sólo en el primer cuatrimestre de 2020, los reportes de ciberestafas y la ciberdelincuencia aumentaron dramáticamente. Así, detectaron un incremento de páginas web y enlaces maliciosos usados para hacer estafas de 788%. A dos años de la pandemia, esa situación no se ha revertido, incluso se ha agudizado. Distintas empresas globales de ciberseguridad, reportaron que el año 2021 hubo un incremento del 40% de casos detectados y atendidos con relación al año anterior.

La poca información que se brinda a la ciudadanía sobre la prevención de la ciberdelincuencia, las barreras técnicas que existen con respecto a la seguridad de la información y las múltiples falencias y vacíos de seguridad de las aplicaciones, programas y páginas web que usamos diariamente, aumentan los niveles de exposición. Los ciberdelincuentes han mostrado gran habilidad para encontrar errores y explotarlos, o ejecutar técnicas de manipulación para que ciudadanos y ciudadanas con menos habilidades digitales, caigan en estafas más fácilmente.

En Bolivia, los casos son cada vez más comunes. A fines del 2021, se suscitaron dos casos que tuvieron una amplia repercusión en los medios debido a sus múltiples víctimas. El primero tuvo relación con la aplicación "IShop". Esta aplicación básicamente ejecutaba una estafa piramidal de forma virtual. Se pedía a las personas que se registren, paguen una cuota y reciban intereses a cambio o recompensas por atraer más personas. Cientos de personas

se registraron y depositaron en conjunto una gran cantidad de dinero. En algún momento la aplicación desapareció y con ella, el dinero que habían depositado. Si bien se abrió una investigación e incluso la Policía Nacional capturó a algunos involucrados, se alegó la dificultad con dar con los creadores de la aplicación debido a que los servidores y registros no se encontraban en Bolivia.

El segundo caso de gran repercusión fueron las transferencias no autorizadas de cuentas del Banco Unión. Estas estafas fueron aún más sofisticadas, pues los ciberdelincuentes requirieron acceder a datos personales de las víctimas e identificar vulnerabilidades en el sistema del banco y la validación vía celular. Lo primero se debió a que los ciberdelincuentes pudieron asociar números de cuentas, con nombres, identificaciones, números de celular e incluso saldos en cuentas. Lo siguiente fue, para ingresar a las cuentas de las víctimas y realizar transacciones, acceder al sistema del banco, presuntamente a través de suplantar números telefónicos, hacer la solicitud de las claves y con ellas ingresar a las cuentas.

Si bien estos casos fueron conocidos debido a su magnitud, todos los días se dan todo tipo de incidentes que en varias ocasiones no son reportados por las dificultades de comprensión de cómo funcionan los ciberdelitos. Por ejemplo, a veces se piensa que, porque un delito se suscitó en la presencialidad, no tiene relación alguna con las tecnologías, cuando éste podría haber sido facilitado por éstas. Aún más, incluso si éstos son reportados, las autoridades encargadas muestran serias dificultades para poder actuar debido a la falta de legislación, protocolos y/o capacidades técnicas.

Tomando en cuenta ese contexto se hace necesario abordar esta problemática desde la propia ciudadanía, a partir de un uso más consciente de las tecnologías, la mayor cautela con respecto a compartir o no datos personales y un conocimiento de la normativa.

## 3. Marco teórico.

### 3.1. ¿Qué es la ciberdelicuencia?

La ciberdelincuencia es un acto que -como cualquier otra acción delincuencial- infringe la ley o alguna convención social que deriva en una sanción o pena. La diferencia es que, al hablar de ciberdelincuencia, nos referimos específicamente al involucramiento de tecnologías de la información y la comunicación (TIC) en el hecho delincuencial.

El involucramiento de las TIC en los delitos puede darse de dos maneras, este nivel de involucramiento nos ayuda a clasificar o diferenciar el tipo de ciberdelito en dos: delitos dependientes de medios informáticos y delitos propiciados por medios informáticos.

Los **delitos dependientes de medios informáticos** se refieren a que las tecnologías son el blanco del delito. Es decir, el ciberdelito busca afectar a los sistemas de información, los programas, el funcionamiento de un dispositivo, de una red de telecomunicaciones, etc. Estos ciberdelitos están normalmente asociados a lo que se denomina, seguridad de la información.

Cuando las TIC forman parte del *modus operandi* del delito pero no son su objetivo final sino la realización de cualquier otro tipo de delito común (fraude, robo, estafa, amenaza, pornografía infantil u otro) hablamos entonces de **delitos propiciados por medios informáticos**. Es decir, las tecnologías se convierten en medios y no fines de los delincuentes.

Estadísticamente, los delitos propiciados por medios informáticos son más comunes y hoy en día, muchos delitos tienen componentes tecnológicos debido a la dependencia a los celulares,

a las redes sociales y a la informatización que ha desarrollado la sociedad. En un futuro, la categoría de delitos habilitados por medios informáticos no tendrá mucho sentido como algo aparte, sino que será lo más común.

### 3.2. Desafíos de la ciberdelincuencia.

La ciberdelincuencia implica una serie de desafíos y complejidades que no han sido resueltos aún. Estos desafíos son: la falta de límites físicos y jurisdicciones, la atribución, las barreras técnicas, la falta de conocimientos, los vacíos legales y regulatorios. Vamos a desarrollar cada uno a continuación:

a) **Falta de límites físicos**. La ciberdelincuencia, a diferencia de un acto de delincuencia, no tiene barreras físicas o geográficas, pues a partir de las interconexiones que permite internet se puede dar en múltiples países con delincuentes que pueden estar ubicados en diferentes ubicaciones geográficas de donde sucede el delito. Imaginemos que un grupo de ciberdelincuentes ubicados en un país en Asia, puede llevar a cabo acciones de intrusión de sistemas en Bolivia. ¿Bajo qué normativa se juzgaría a esos ciberdelincuentes, la de Asia o la de Bolivia? La policía o las fuerzas del orden de Bolivia ¿pueden actuar en relación a personas o ciudadanos que no se encuentren en la jurisdicción de su Estado?

b) **Atribución**. Otro problema referido a la ciberdelincuencia es la dificultad de identificar a los ciberdelincuentes. Si bien todo dispositivo conectado a internet es identificable y rastreable a través de su dirección de internet (IP[1]), a través de sus cuentas en redes sociales o en otros servicios, y a través de la información que van dejando en Internet (sus huellas), también se han generado varios mecanismos para esconder la identidad o disfrazarla. Por un lado, los delincuentes pueden crear cuentas falsas para realizar sus acciones, y por el otro, también pueden usar herramientas como las VPN, las redes TOR, las redes Proxy[2], para evitar ser rastreados. Ello genera grandes dificultades para identificar a las y los ciberdelincuentes pero, de cualquier manera, no es imposible dar con los ciberdelincuentes pues siempre dejan huellas.

c) **Barreras técnicas**. En tanto existen dificultades de atribución e identificación de los ciberdelincuentes, se generan otras barreras referidas a la capacidad técnica de los y las investigadores en cibercrimen. Estas personas requieren altas habilidades en seguridad de la información para hacer análisis forense de dispositivos, monitoreo de redes de telecomunicaciones, análisis de fuentes abiertas, entre otras, para poder dar con los ciberdelincuentes. No obstante, hay déficit de especialistas pues estos son temas nuevos sobre los cuales, aún hay pocos programas de formación. A su vez, en las fuerzas del orden existe rotación de cargos que evita que el personal pueda especializarse.

   Además, los programas informáticos, aplicaciones, sitios web, entre otros, a menudo tienen errores o vulnerabilidades que se desconocen y que son aprovechados por ciberdelincuentes para llevar a cabo sus acciones. Empresas y gobiernos no hacen

[1] La Dirección IP es un número único que es asignado a cada conexión a Internet, este IP ayuda a identificar la conexión y así poder conectarse en red con otras IP. Normalmente es una etiqueta numérica similar a "192.0.10.1".

[2] VPN, redes TOR y redes Proxy son diferentes métodos o formas de anonimizar la dirección IP de nuestra conexión a internet. Es decir, estos métodos ocultan nuestras conexiones o las disfrazan para que no se puedan rastrear o identificar. En el punto 4.3. de Definiciones básicas, puedes encontrar una mayor explicación de cada una.

públicas la identificación de estos problemas de seguridad, esto evita que las fuerzas del orden y las/os investigadores de seguridad puedan resolverlos a tiempo.

d) **Falta de conocimientos**. Aunque el personal encargado de ciberdelincuencia pueda estar bien entrenado, también se requiere conocimiento en el resto del sistema de justicia. La falta de experiencia en estos temas puede derivar en que jueces y fiscales pasen por alto aspectos técnicos que debilitan la denuncia de casos y no puedan tomar decisiones en la materia.

e) **Vacíos legales y regulatorios**. La ciberdelincuencia ha generado desafíos con respecto a cómo entender los casos, adaptarlos a tipos penales existentes, investigarlos, entre otros. Actualmente, la legislación boliviana, no reconoce varios tipos de cibercrímenes que sí están reconocidos internacionalmente y se carece de protocolos, lo que dificulta que la Policía y las autoridades puedan actuar.

### 3.3. Definiciones básicas

| Término | Definición |
|---|---|
| **Sistema informático** | Cualquier sistema, programa, aplicación que puede ser accedido por un dispositivo electrónico para almacenar y procesar información. |
| **Dispositivo electrónico** | Es cualquier aparato que permita utilizar sistemas informáticos y conectarse a una red. Puede ser una computadora, un celular, tablet, consola de videojuegos, entre otros. |
| **Proveedor de servicio/Internet** | Es cualquier empresa que ofrezca servicio de telecomunicaciones (telefonía, internet, cable). En Bolivia las más grandes son Entel, Tigo, Viva y AXS, aunque existen varias otras empresas y cooperativas que brindan servicios de telecomunicaciones en ciudades específicas. |
| **Datos personales** | Son datos que permiten identificar a una persona (nombre, CI, edad, domicilio, identidad sexual, etc.). |
| **VPN** | Es una red privada que se sobrepone a la conexión a internet y que en lugar de conectarse directamente con el sitio o persona, genera un punto intermedio. De ese modo logra disfrazar las direcciones IP. Es decir, es como si iniciamos un viaje usando ropa de un color y en el medio nos cambiamos de ropa de otro color para que no nos reconozcan. |
| **Red TOR** | Es una red distribuida y superpuesta sobre nuestra conexión de internet que permite reencaminar los mensajes y conexiones entre varios puntos. Al generar muchas conexiones en el medio, nuestra dirección de IP se vuelve difícil de rastrear o identificar porque pasamos por varios puntos intermedios antes de llegar al destino final. |
| **Ciberdelincuente** | Persona que infringe la ley y comete crímenes usando las TIC. |
| **Ciberpatrullaje** | Acciones de investigación en internet usadas por las fuerzas del orden las cuales normalmente usan fuentes abiertas y de libre |

| | |
|---|---|
| | acceso como plataformas de redes sociales, blogs, páginas de internet, entre otras. |
| **Plataforma de red social** | Son aquellas plataformas, aplicaciones, sistemas que nos permiten conectar con otras personas, conversar con ellas y compartir información, fotografías, videos, estados, visitas a lugares, entre otras. |

### 3.4. Marco normativo

Para que un acto sea ilegal o considerado criminal debe estar descrito y establecido como tal en una ley. A esto se le denomina el principio *nullim crimen sine lege* (no hay crimen sin ley).

Una ley de ciberdelitos o política similar, de acuerdo a la Oficina de Naciones Unidas acerca de Drogas y Delitos (ONUDC), debería identificar los estándares de comportamiento aceptables con respecto a las tecnologías, establecer sanciones socio-jurídicas, demarcar los protocolos y límites de la investigación cibercriminal, facilitar formas de cooperación internacional, crear mecanismos de protección y prevención, así como estrategias de mitigación.

Las leyes de ciberdelitos incluyen delitos tradicionales como fraude, falsificación, crimen organizado, robo, u otros, que pueden ya estar tipificados previamente a su identificación. También incluyen delitos nuevos o delitos "ciberdependientes" que sólo existen en el marco del ciberespacio y las tecnologías. En ambos casos, se requieren tanto normativas específicas como potenciales modificaciones al código penal.

#### a) Internacional

A nivel internacional aún se debate un marco regulatorio que defina qué es y qué no es el cibercrimen o ciberdelincuencia, cuáles son los mecanismos de cooperación, cuáles son los límites de investigación, entre otros.

Entre los mecanismos internacionales que se han creado para luchar contra la ciberdelincuencia, uno de los más importantes es el Convenio de Budapest sobre la Ciberdelincuencia, creado el año 2001 e impulsado primordialmente por la Unión Europea.

Este Convenio busca armonizar la normativa a nivel de los países, estandarizar técnicas de investigación, promover acciones de articulación internacional en esta área y facilitar orientación y asistencia legal mutua entre países. Bolivia no se ha adherido a este Convenio, pese a que varios países en América Latina sí lo hicieron (Chile, Perú, Brasil, Paraguay, Costa Rica, República Dominicana y Argentina).

Actualmente se discute un nuevo instrumento de lucha contra el ciberdelito en el marco de la Organización de Naciones Unidas (ONU).

Es importante entender que la Policía podrá llevar a cabo una investigación de ciberdelitos y el sistema judicial procesar denuncias sólo si se pueden adjudicar los casos a delitos tipificados y cuando tiene jurisdicción. Si no están tipificados, difícilmente se podrá proceder con la denuncias. Por eso, es importante que haya un reconocimiento explícito de los ciberdelitos en las leyes de los países.

Por otro lado, si el delito está tipificado pero la jurisdicción es otra - el delito se lleva a cabo en otro país- las autoridades tampoco podrán actuar. En el caso de los ciberdelitos, muchos casos no se dan necesariamente en territorio del mismo país, lo cual perjudica que puedan ser debidamente procesados. En el ciberespacio se requieren varios factores para determinar la jurisdicción:

- Nacionalidad del ciberdelincuente bajo el principio de que los Estados tienen la autoridad para enjuiciar a sus nacionales.
- La nacionalidad de la víctima también puede utilizarse pero ese criterio no es tan frecuente.
- Afectación de interés y seguridad propia, cuando si bien el Estado no tiene jurisdicción pero sí se vio afectado por el incidente.
- Atrocidades masivas, cuando se considere que el delito afectó a todos los seres humanos independientemente de su ubicación geográfica bajo el principio de universalidad.

**b) Nacional**

Bolivia no cuenta con un marco normativo específico para el cibercrimen aunque sí incluye dos artículos referidos a ciberdelitos dependientes en el Código Penal en el año 1997 (veremos estos más adelante). Por tanto, existen serias dificultades para que las fuerzas del orden puedan actuar, sobre todo en lo que respecta a delitos dependientes de medios informáticos, en tanto al no estar tipificadas varias acciones, no son punibles ni identificadas como delitos.

En el caso de delitos habilitados por medios informáticos, la segunda categoría que vimos, se pueda adaptar a la normativa ya existente. Es decir, las autoridades y fuerzas del orden, pueden actuar y procesar los mismos, aunque deben ampararse en jurisprudencia y/o antecedentes que lo faciliten.

La Policía boliviana tiene ya varios años de experiencia en delitos informáticos. El año 2018 creó la División de Cibercrimen en La Paz, bajo la dependencia de la División de Trata y Tráfico de Personas, dependiente de la Fuerza Especial de Lucha Contra el Crimen. Esta División también fue replicada en Santa Cruz. Aunque existen varios vacíos aún en cuanto a sus protocolos y normativa, su equipo de investigación puede desarrollar una serie de investigaciones cuando las tecnologías tienen implicaciones en delitos ya conocidos.

Otro de los problemas de no tener marco normativo específico para cibercrimen es que los países que carecen de él pueden fácilmente convertirse en refugios seguros para cometer cibercrímenes con impunidad, pues hay menos maneras de poder investigarlos y procesarlos. Es por ello que la ONU recomienda que los países generen estos marcos normativos.

### 3.5. Ciberseguridad y derechos humanos.

Existe un debate en torno a la priorización de la seguridad y protección contra los ciberdelitos y el cumplimiento de los derechos humanos. Este debate surge a partir de que muchas investigaciones de ciberdelitos pueden vulnerar la privacidad de las personas y de su información. En realidad, ninguna normativa referida a ciberdelitos debería ser justificativo para vulnerar derechos humanos aunque existen instrumentos internacionales que permiten ciertas restricciones.

Las restricciones pueden darse en casos excepcionales y que persigan fines justificables, sean necesarias y proporcionales a la amenaza que enfrentan, como lo son por ejemplo, los casos de terrorismo o narcotráfico. Debe tomarse en cuenta los objetivos que pueden

perseguir los fines de investigación y cómo estos afectan a los derechos humanos directa o indirectamente. Siempre se necesitará una orden judicial para acceder a información privada.

### 3.6. ¿Cómo se investigan los ciberdelitos?

Las autoridades judiciales normalmente tienen poderes especiales para realizar investigaciones especializadas en casos de delitos. Estos poderes están autorizados por ley y pueden cubrir tanto el acceso a información como aspectos referidos a condiciones que tienen que cumplir las pruebas para que sean procesadas.

En el caso de los ciberdelitos, estos poderes requieren ser establecidos por normativa pues posiblemente pueden implicar, además de la revisión de los dispositivos de las personas implicadas, el análisis de servicios de telecomunicaciones de empresas, uso de aplicaciones, navegación en páginas web, términos buscados en motores de búsqueda, entre otras varias opciones.

En tanto esta investigación puede afectar directamente derechos consagrados como la privacidad e intimidad, incluso los derechos de personas no directamente involucradas sino de conjuntos poblacionales completos en una determinada zona, estas acciones de investigación requieren normativa que establezca alcances y límites. Así por ejemplo, se requiere leyes de protección de datos personales, protocolos de uso de fuentes abiertas para ciberpatrullaje, entre otros.

Toda facultad o poder específico para realizar esta investigación debe estar basada en el Estado de derecho y los derechos humanos para evitar potenciales abusos y afectaciones innecesarias a la población. Las investigaciones deben seguir tres principios: proporcionalidad (que la investigación sea lo más acotada posible en tiempo y extensión), necesidad (que sólo se investigue lo necesario para el delito) y legalidad (que se sustente en los marcos legales existentes).

A diferencia de la ciencia forense con respecto a los delitos tradicionales, la evidencia digital para probar ciberdelitos es de difícil obtención, así como su manejo y su uso por parte de las autoridades.

A continuación vemos dos formas esenciales de investigar ciberdelitos, tanto los dependientes como aquellos que usan las tecnologías solamente como medios.

- Análisis forense

Para investigar casos de ciberdelitos, se requiere la recopilación, almacenamiento y análisis de dispositivos que pudieron estar implicados en el hecho. La evidencia que se encuentra en éstos puede ser determinante para respaldar o refutar un hecho.

¿Qué tipo de evidencia se busca? La evidencia que se tome en cuenta depende de los protocolos y/o manuales que utilicen los tribunales de justicia pero normalmente serán archivos, documentos, ubicaciones o geolocalizaciones, mensajes, registros de llamadas, fotografías y/o hasta, búsquedas realizadas, patrones de comportamiento u otras. El mayor problema es que para que esta sea admitida y usada como prueba, la evidencia digital tiene que demostrar que sea auténtica, es decir que corresponda a la fuente y/o autor a quien se adjudica, y que no haya sido modificada, manipulada ni dañada.

Demostrar la autenticidad e integridad de una prueba digital es complejo, pues los archivos digitales pueden ser manipulados y modificados. La autenticidad puede ser demostrable a través de los metadatos -información que describe un determinado archivo y que se guarda en éste-, pero la integridad en cambio, es más difícil de comprobar. Para ello se deben establecer cadenas de custodia que lleven registros detallados sobre la condición en la que está la prueba. Hay mecanismos como la tecnología de cadena de bloques -*blockchain*- que evita posibles modificaciones y robustece la verificación de éstas.

La Policía Boliviana creó el Instituto de Investigaciones Técnico Científico de la Universidad Policial (IITCUP) el 28 de diciembre de 2010, para brindar más de 15 servicios en indagaciones criminales y forenses. Uno de esos servicios era el análisis informático en discos duros, *flash drives*, disquetes, CD, DVD, teléfonos móviles, organizadores de mano PDA, Pocket PC, cámaras de fotos y videos digitales. Actualmente la División de Cibercrimen de la Policía Nacional cuenta con estas capacidades que permiten analizar la información guardada en los dispositivos, tanto la generada por las personas a quienes pertenecen como aquella de sus contactos.

Para realizar este tipo de investigación de casos, lo primero que hará la Policía es obtener una copia de seguridad del dispositivo y su información, para no afectar la información original. Sobre esta copia, hará un análisis que puede implicar: analizar cambios recientes en el dispositivo (instalación o eliminación de aplicaciones, información, descargas) y funcionamiento general; analizar geolocalizaciones, fotografías, videos y otra información accesible; analizar conversaciones recientes, salidas y entradas de llamadas, mensajes u otros; metadatos que pueda brindar el dispositivo y que sean pertinentes a la investigación.

- OSINT y ciberpatrullaje.

Es importante que las investigaciones policiales o de las autoridades pertinentes, utilicen a su favor la tecnología, para poder recabar elementos que sirvan para prevenir la comisión de delitos o para la recolección de pruebas que sirvan en un proceso judicial. Una de ellas es el ciberpatrullaje. El ciberpatrullaje se puede definir como la acción de vigilancia para la prevención de delitos en la red a partir de fuentes abiertas o canales no cerrados de comunicación.

Un aspecto que se relaciona con el ciberpatrullaje es la denominada OSINT, que es la sigla en inglés para *Open Source Intelligence* (Inteligencia de Fuentes Abiertas) que es básicamente el conjunto de técnicas y herramientas para recopilar información pública de los y las usuarias.

La Inteligencia de Fuentes Abiertas utiliza datos públicos para la realización de análisis como las fotos, videos, estados, reacciones, ubicación que las personas publican en Facebook y otras redes sociales. Por lo que los datos que se generan en espacios digitales públicos pueden servir para recabar elementos que permitan prevenir, investigar y sancionar la comisión de delitos.

El uso de herramientas tecnológicas requiere la capacitación del personal que vaya a aplicarlas, tanto a nivel de manejo como a nivel de visión estratégica de la utilización de la tecnología. Por ello es importante establecer procesos de formación que incluyan aspectos relacionados con la garantía de los derechos humanos y los conflictos que pueden generarse.

El uso de Inteligencia de Fuentes Abiertas, debería estar normado, determinando los límites, prohibiciones, mecanismos de transparencia y rendición de cuentas de las actividades

realizadas. A partir del desarrollo legislativo, deben establecerse protocolos de actuación por parte de las entidades que realicen la Inteligencia de Fuentes Abiertas, los que tendrían que ser de conocimiento público.

Se debe considerar ese contexto y definiciones para entender la forma en la que se concibe el ciberpatrullaje, y cómo dichos aspectos son desarrollados en Bolivia, considerando la orgánica estatal y el ámbito normativo.

El ordenamiento jurídico boliviano establece que las entidades encargadas de la investigación de delitos son la Policía Boliviana y el Ministerio Público. Así la Ley Orgánica de la Policía Nacional- Ley No. 734[3] de 8 de abril de 1985 establece en el artículo 7 las atribuciones de la Policía Boliviana, entre las cuales se encuentran: "c) Prevenir los delitos, faltas, contravenciones y otras manifestaciones antisociales. (…) h) Investigar los delitos (...)".

Por otro lado, la Ley Orgánica del Ministerio Público- Ley 260 de 11 de julio de 2012, establece que el Ministerio Público tiene entre sus funciones: "Ejercer la acción penal pública, la dirección funcional de la investigación y de la actuación policial"[4]. No obstante, no se cuenta con una norma concreta que regule la investigación que se realice a través de ciberpatrullaje[5].

En diciembre de 2017 se crea en la FELCC de La Paz la "Sección de Ciberpatrullaje", posteriormente se replica esta unidad en Cochabamba, conformada por cinco policías que tenían preparación informática, haciendo rastrillaje en Facebook, WhatsApp, Instagram y Twitter buscaban siete tipos de delitos identificados: venta ilegal de pornografía, venta de píldoras abortivas, compra y venta de armas de fuego, estafa en venta de casas o anticréticos, tráfico de animales silvestres, trata de personas y tráfico de personas.

El Ciberpatrullaje comprende, en ese sentido, la identificación de personas de interés -ya sean víctimas o posibles ciberdelincuentes-, sus cuentas en redes sociales, su información pública que haya sido subida y/o compartida en estas plataformas (fotografías, videos, localizaciones, texto), registros y publicaciones en páginas web, blogs u otros espacios de acceso público, asociaciones y contactos con otras personas, entre otras.

Hoy en día existen una serie de herramientas que permiten analizar el comportamiento de las personas en diferentes plataformas y que son de gran utilidad para la investigación judicial. Así se puede identificar, por ejemplo, horas de mayor uso de redes, grados de vinculación con otras cuentas, coincidencias entre nombres y diferentes servicios, incluso localizaciones de celulares y dispositivos.

### 3.7. Tipos de cibercrimen y técnicas.

Existen muchos tipos de cibercrimen o ciberdelitos. Conviene, antes, diferenciar estos de las técnicas cómo se ejecutan, es decir, los *modus operandi* de los ciberdelitos en sí mismos. Estos ciberdelitos, como se vio anteriormente, se dividen en dos: ciberdelitos dependientes, que son aquellos cometidos contra las tecnologías y los sistemas en sí mismas, y los ciberdelitos habilitados por las tecnologías, es decir que pueden ocurrir fuera de los sistemas y tecnologías pero que son facilitados por estos.

[3] La Ley es antigua pero actualmente se encuentra en vigencia; sin embargo, el Ministerio de Gobierno ha preparado un anteproyecto de ley que procedería a modificar disposiciones de la referida Ley.

[4] Artículo 12, numeral 2.

[5] Tampoco se cuenta con información pública sobre la existencia de protocolos o reglamentos que se manejen a nivel interno por parte de la Policía boliviana.

- Ciberdelitos dependientes contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

Son acciones que tienen como objetivos los sistemas, redes, bases de datos, interfaces, información en lo que respecta a que sean accesibles, sean precisos y confiables, y estén protegidos con respecto a accesos no autorizados. El Código Penal boliviano introdujo en 1997 dos delitos informáticos de esta índole:

> Art. 363. bis. Manipulación informática, se refiere a la obtención un beneficio indebido a la manipulación de procesamiento o transferencia de datos informáticos que conduzcan a resultados incorrectos o evite un proceso cuyo resultado habría sido correcto
>
> Art. 363. ter. ter.- Alteración, acceso y uso indebido de datos informáticos, se refiere a que sin estar autorizados, una persona se apodere, acceda, utilice, modifique, suprima o inutilice datos almacenados en una computadora o en cualquier soporte informático.

No obstante, el Código Penal quedó desactualizado, existiendo otras tantas acciones que están catalogadas como delitos informáticos en instrumentos internacionales, como:

- **Intrusión a sistemas y/o acceso no autorizado**. Se refiere a ingresar a cualquier sistema, cuenta, aplicación u otro, sin autorización ya sea para eliminar, aumentar, transmitir, editar, borrar, dañar, o incluso sólo observar, información contenida en esté. Este ciberdelito se encuentra normado en los Art. 4 y 5 del Convenio Internacional contra el Cibercrimen de Budapest.
- **Creación y distribución de programas maliciosos**. Es la producción, venta, compra, distribución de herramientas y/o programas informáticos diseñados o adaptados con el propósito de cometer modificaciones, falsificaciones, daños, eliminación de sistemas o información. Este se encuentra normado en el Art. 6 del Convenio de Budapest. Algunos programas maliciosos identificados y que se encuentran prohibidos, son:
  - Gusanos informáticos. Programas maliciosos independientes que se copian sin intervención del usuario.
  - Virus. Programa que requiere de la actividad del usuario para copiarse o ejecutarse.
  - Troyano. Programa diseñado para parecerse a otro programa con el fin de engañar al usuario
  - Programa espía. Programa diseñado para monitorear la actividad del usuario.
  - Programa secuestrador (Ransomware). Programa que secuestra y/o cifra sistemas o información para que el usuario no pueda usarla.

- **Ataques de denegación de servicios (DoS) o de distribución de servicios (DDoS)**. Son ataques que usan múltiples computadoras o dispositivos coordinados para tratar de ingresar o usar un servicio al mismo tiempo, con el fin de saturarlo y desactivarlo, evitando que otras personas lo usen. Normalmente se usan contra infraestructuras y/o servicios estratégicos. Este delito se encuentra normado a través del Art. 5 del Convenio de Budapest.
- **Desfiguración de sitios web**. Se refieren a acciones por la cual el atacante ingresa a la página web de una empresa, gobierno o servicio, y la modifica dejándola inutilizable.

- Ciberdelitos habilitados por las tecnologías.

Esos son delitos, normalmente ya tipificados y conocidos, que aprovechan las tecnologías como medio para ser ejecutados. Estos pueden ser:

○ **Fraude**. Es el delito de estafa, falsificación de información u otro que conlleve la manipulación o el engaño deliberado a una persona. En el Código Penal boliviano se encuentra reconocido en el Art. 335: “El que induciendo en error por medio de artificios o engaños, sonsacare a otro dinero u otro beneficio o ventaja económica”.

En cuanto a delitos informáticos, el Art. 7 del Convenio de Budapest lo define como la forma deliberada e ilegítima, alteración, borrado o supresión de datos informáticos con la intención de que sean tenidos en cuenta o utilizados como si se tratará de datos auténticos.

También éste se encuentra reconocido en el Art. 8 del mismo instrumento internacional, lo reconoce también como los actos deliberados e ilegítimos que causen perjuicio a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos.

Este también puede tomar la forma de fraudes que involucran promesas falsas o engañosas, como mensajes que se hacen pasar por familiares, amistades, parejas, u otras personas cercanas para generar perjuicios de algún tipo.

○ **Delitos informáticos relacionados con la identidad**. Este delito implica la suplantación de la identidad de una persona o de entidades jurídicas y comerciales con la intención de hacerse pasar por estas, con diferentes fines como engaño, manipulación, etc.

Este delito es bastante común y es utilizado por ciberdelincuentes para engañar personas y pedir dinero, información o aprovechar relaciones de confianza y llevar adelante acciones de phishing u otras.

En el Código Penal boliviano no está directamente tipificado, no obstante, los Art. 198 (Falsedad material) y Art. 199 (Falsedad ideológica), podrían aplicarse en algunos casos cuando se tratan de documentos y/o instrumentos públicos.

○ **Delitos informáticos de derechos de autor y marcas comerciales**. El Convenio de Budapest, en su Art. 10, alega como delito el uso, copia, comercialización de propiedad intelectual sin autorización.

○ **Actos relacionados con la informática que causen daño personal**. Estos son acciones referidas a hostigamiento, abuso, amenaza, acoso, intimidación u otra dirigida directamente a una persona con la intención de causarle daño psicológico, de prestigio u otro. Este tipo de acto no se encuentra tipificado en la mayoría de los instrumentos internacionales, pero ya está siendo tomado en cuenta por diversos informes referidos a ciberseguridad y violencias digitales.

En el Código Penal, el acoso solo es reconocido como delito cuando éste implica actos sexuales y acoso político: Art. 312 quater: “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"

Artículo 148 Bis: "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"

También está reconocida en el Código Penal la amenaza: Art. 293. "El que mediante amenazas graves alarmare o amedrentare a una persona, será sancionado".

- **Instigación o «captación de niños con fines sexuales» por medios informáticos**. Este delito se refiere al uso de tecnologías para captar niños y niñas con la intención de abusar sexualmente de ellos. El delincuente manipula a la víctima mediante el uso de una variedad de tácticas para generar confianza, como compartir intereses, otorgar regalos, generar curiosidad, u otro.
- **Grooming**. Es un delito referido al engatusamiento de un adulto hacia un menor por medio de medios telemáticos con un fin sexual.
- **Delitos relacionados con obtención y guardado de contenidos ilícitos**. Se refieren por ejemplo a obtener, comercializar, guardar o compartir material de abuso sexual infantil, violaciones, autolesiones, tortura, imagenes sexualmente explícitas que estén prohibidas en algunos países, entre otras.

En el Código Penal boliviano este delito está reconocido en el Art. 323 bis relacionado a la pornografía:

I. Quien procure, obligue, facilite o induzca, por cualquier medio, por sí o por tercera persona a otra que no de 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 condena privativa de libertad.

- **Trata de personas y el tráfico de migrantes**. Estos delitos están estrechamente ligados con las tecnologías debido a que éstas han facilitado los *modus operandi* de los delincuentes. Actualmente existen diversos protocolos y normativas internacionales que prohíben y sancionan severamente este delito debido a su severidad, por lo que en éstos se sugiere penarlos con condenas mayores a cuatro años. Las tecnologías digitales han influido en este tipo de delito a partir de facilitar los medios y tácticas de captación de víctimas, la comunicación del crimen organizado, y las maneras como se comercializan y se realizan las transacciones.

En el Código Penal boliviano este delito se encuentra tipificado en el Art. 281 (Trata de personas) Bis. I. Será sancionado con privación de libertad de diez (10) a quince (15) años, quien por cualquier medio de engaño, intimidación, abuso de poder, uso de la fuerza o cualquier forma de coacción, amenazas, abuso de la situación de dependencia o vulnerabilidad de la víctima, la concesión o recepción de pagos por sí o por tercera persona realizare, indujere o favoreciere la captación, traslado, transporte, privación de libertad, acogida o recepción de personas dentro o fuera del territorio nacional, aunque mediare el consentimiento de la víctima, con cualquiera de los siguientes fines: 1. Venta u otros actos de disposición del ser humano con o sin fines de lucro. 2. Extracción, venta o disposición ilícita de fluidos o líquidos corporales, células, órganos o tejidos humanos. 3. Reducción a esclavitud o estado análogo. 4. Explotación laboral, trabajo forzoso o cualquier forma de servidumbre. 5.

Servidumbre costumbrista. 6. Explotación sexual comercial. 7. Embarazo forzado. 8. Turismo sexual. 9. Guarda o adopción. 10. Mendicidad forzada. 11. Matrimonio servil, unión libre o de hecho servil. 12. Reclutamiento de personas para su participación en conflictos armados o sectas religiosas. 13. Empleo en actividades delictivas. 14. Realización ilícita de investigaciones biomédicas.

También en el Art. 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 (5) a diez (10) años.

La sanción se agravará en la mitad, cuando: 1. Las condiciones de transporte pongan en peligro su integridad física y/o psicológica. 2. La autora o el autor sea servidor o servidora pública. 3. La autora o el autor sea la persona encargada de proteger los derechos e integridad de las personas en situación vulnerable. 4. La autora o el autor hubiera sido parte o integrante de una delegación o misión diplomática, en el momento de haberse cometido el delito. 5. El delito se cometa contra más de una persona. 6. La actividad sea habitual y con fines de lucro. 7. La autora o el autor sea parte de una organización criminal

### 3.8. Medidas de prevención.

En el contexto del ciberdelito las medidas preventivas buscan justamente evitar que los delitos se lleguen a cometer o al menos mitigar el daño o los impactos que puedan causar.

Hay muchas maneras de prevenir los ciberdelitos, varias de las cuales ya fueron mencionadas en el módulo referido a violencias digitales. En ese sentido, resumiremos diciendo que se puedan abordar las siguientes medidas:

- Medidas legislativas de derecho preventivo. Leyes o marcos normativos orientados a fortalecer la información y mayor cuidado con respecto al bienestar e integridad de los usuarios, como protección de datos personales, ciberseguridad, prevención de violencias, telecomunicaciones.

- Campañas de información. Difusión amplia sobre los posibles modus operandi de ciberdelincuentes para que las personas los conozcan y tomen recaudos.

- Investigación preventiva. Investigación activa de fuerzas de orden a acciones sospechosas o personas de interés que pueden tener antecedentes. Esta investigación puede llevarse a cabo a través del ciberpatrullaje, OSINT u otras técnicas aún más intrusivas. No obstante, este tipo de acción puede ser lesiva a varios derechos, como la privacidad, la libertad de expresión, de asociación, entre otros, sobre todo si no se tienen adecuados protocolos que establezcan sus alcances y generen garantías suficientes para la población.

- Medidas de seguridad propias. Son los cuidados que las propias personas pueden adoptar para proteger su información y dispositivos, y así reducir el margen de ser víctimas de cibercrimen.