UNIVERSIDAD MAYOR DE SAN SIMÓN

Facultad de Ciencias Jurídicas y Políticas

Carrera de Ciencias Jurídicas

“ENSAYO DELITOS DIGITALES Y REDES SOCIALES: EL VACÍO LEGAL FRENTE AL CIBERACOSO, SEXTORSIÓN Y DELITOS INFORMÁTICOS EN BOLIVIA”

ESTUDIANTE: Erika Karen Villca Paricagua

FECHA: 12 de septiembre del 2025

Cochabamba – Bolivia

INDICE

INTRODUCCION

En los últimos años la tecnología ha cambiado la forma en que vivimos, trabajamos y nos comunicamos. Antes, para cometer un delito era necesario estar presente físicamente en el lugar, pero hoy basta con tener una computadora o un celular conectado a internet para poder afectar a otra persona que puede estar incluso en otro continente. Entre todos estos avances, uno de los más sorprendentes y también peligrosos es la inteligencia artificial **(IA)**. Esta tecnología, que al principio parecía algo de ciencia ficción, ahora está presente en aplicaciones, redes sociales, cámaras de seguridad, traductores y hasta en los celulares más comunes. Si bien la IA tiene muchos beneficios, también ha abierto la puerta a nuevas formas de criminalidad que son más difíciles de detectar y de investigar.

En Bolivia, como en muchos otros países, la ley no ha avanzado al mismo ritmo que la tecnología. Nuestro Código Penal fue pensado para un mundo donde los delitos se cometían de forma física y tangible: un robo, un fraude con documentos en papel, una amenaza cara a cara. Hoy, sin embargo, es posible falsificar la voz de una persona para pedir dinero, crear un video falso para arruinar su reputación o fabricar documentos digitales que parecen reales.

En las calles de nuestras ciudades, este tipo de delitos no es tan visible como un robo o un asalto, pero en internet circulan a diario. Los casos de estafas por redes sociales, chantajes con fotos íntimas y suplantaciones de identidad ya son noticia común. El problema es que, en muchos de ellos, las autoridades tienen dificultades para encontrar y procesar a los culpables, en parte por la falta de leyes específicas y en parte por la falta de recursos técnicos.

Este ensayo busca analizar cómo la criminalidad digital, especialmente aquella que usa inteligencia artificial, representa un desafío para el derecho penal en Bolivia. Se revisará qué dice nuestra legislación, cómo se comparan nuestras leyes con las de otros países, cuáles son los principales vacíos legales y qué se podría hacer para mejorar. También se propondrán reformas que permitan proteger mejor a las personas y asegurar que la justicia pueda actuar de manera rápida y efectiva.

La idea no es solo describir el problema, sino también reflexionar sobre el papel que debe cumplir el derecho penal en un mundo cada vez más digital. Si la ley no se adapta, los delincuentes seguirán teniendo ventaja, y las víctimas quedarán desprotegidas. Por eso, es necesario que desde ahora se empiece a hablar y actuar sobre estos temas, antes de que los daños sean mayores.

I. CONTEXTO Y EVOLUCIÓN DE LA CRIMINALIDAD DIGITAL

La criminalidad digital es un tema que antes casi no se hablaba o se conocía en Bolivia, pero ahora está presente en muchas noticias y conversaciones sociales. Antes los delitos eran más “fisicos” por decirlo así, en sí que pasaban en la calle, en las casas o en lugares visibles. Hoy en día muchas personas pueden ser victimas sin siquiera salir de su casa, todo por el uso del internet y las redes sociales. Esto hace que el Derecho Penal tenga que mirar más allá de lo tradicional y pensar en como castigar y prevenir conductas que ocurren en un espacio virtual.

1.1. Concepto y clasificación de delitos informáticos

Cuando se habla de delitos informáticos no todos entienden lo mismo. Algunos piensan que es solo “hackear” una computadora, pero en realidad es más amplio. En terminos generales, un delito informático es cuando se usa una computadora, un celular o internet para cometer un acto que la ley considera delito. Puede ser que la computadora sea el medio para cometer el crimen o que sea el objetivo del crimen.

Algunos ejemplos comunes que suceden en la actualidad son:

- **Phishing**: que es cuando alguien crea una pagina o un mensaje falso para engañar a otra persona y robarle sus datos o dinero.
- **Sextorsión**: que es cuando una persona amenaza con publicar fotos o videos íntimos si no le dan plata u otra cosa.
- **Ransomware**: que es un virus que bloquea la computadora y te pide pagar para recuperarla.

Estos delitos también se pueden clasificar en:

1. **Delitos contra sistemas informáticos**: como entrar sin permiso a una computadora o red.
2. **Delitos cometidos a través de internet**: como estafas o venta de cosas ilegales.
3. **Delitos donde internet es un medio secundario**: por ejemplo, coordinar un robo por redes sociales.

En Bolivia, el Código Penal no tiene una sección grande o especifica solo para estos delitos, pero si hay articulos que se pueden aplicar, aunque muchas veces no son suficientes o estan desactualizados.

1.2. Evolución tecnológica y aparición de la IA como herramienta delictiva

Hace unos años los delincuentes digitales eran personas con mucho conocimiento técnico, casi expertos en computación. Ahora, con el avance de la tecnología, muchas herramientas que antes eran complicadas ya estan disponibles para cualquiera. Incluso hay programas gratis en internet que permiten crear videos falsos o clonar voces, algo que antes parecía muy complicado de realizar.

La inteligencia artificial (IA) es uno de los avances más grandes y también más peligrosos si se usa mal. La IA puede analizar datos muy rápido, imitar voces, crear fotos o videos que parecen reales y hasta escribir mensajes que engañan a la gente. Esto ha abierto nuevas formas de delinquir, por ejemplo:

- Usar IA para hacer una identidad falsa de una persona famosa o de una autoridad para estafar.
- Crear mensajes automáticos para miles de personas pidiéndoles información bancaria.
- Generar documentos falsos que parecen legítimos.

Estos delitos son más difíciles de detectar porque la tecnología avanza más rápido que las leyes y que las autoridades. Además, los criminales pueden estar en otro país, lo que complica mucho el trabajo de la policía y de los jueces.

1.3. Situación actual en Bolivia

En Bolivia ya se han reportado casos de estafas por internet, suplantación de identidad y hasta venta de cosas ilegales en redes sociales. La Fuerza Especial de Lucha Contra el Crimen (FELCC) tiene una división de cibercrimen, pero todavía no tiene los recursos ni el personal suficiente para enfrentar todos estos casos.

En las noticias se han visto historias de personas que reciben mensajes de “su banco” para confirmar datos y después les vacían la cuenta. También casos de mujeres que fueron víctimas de sextorsión por fotos privadas que habían enviado a sus parejas y que luego fueron usadas para chantajearlas.

El problema es que muchas veces las victimas no denuncian por miedo o por vergüenza, y cuando lo hacen, el proceso es lento y complicado. Además, no siempre los jueces y fiscales entienden bien como funciona la tecnología, lo que provoca que los casos no avancen o que no se logre una condena.

II. INTELIGENCIA ARTIFICIAL Y NUEVAS MODALIDADES DELICTIVAS

La inteligencia artificial (IA) es algo que hace unos años solo se veía en películas o series, pero hoy ya es parte de la vida diaria. Está en los celulares, en las redes sociales, en las cámaras de seguridad, e incluso en los servicios de atención al cliente. El problema es que la IA no solo sirve para cosas buenas, también se está usando para cometer delitos que antes ni existían o que ahora se hacen de forma más rápida y difícil de detectar.

2.1. Delitos potenciados por IA

La IA ha hecho que algunos delitos que ya existían sean mucho más peligrosos. Antes, para engañar a una persona se necesitaba tiempo y esfuerzo, ahora con la IA todo se puede automatizar y parecer más real.

- **Suplantación de identidad**: Se manifiestan mediante videos o audios falsos creados con IA que imitan la voz o la cara de alguien. Por ejemplo, se puede hacer que parezca que una autoridad está diciendo algo que nunca dijo o que una

persona famosa está promocionando un producto. En manos de delincuentes, esto se usa para estafar o dañar la reputación de alguien.

- **Estafas automatizadas**: Con la IA se pueden crear programas que envían miles de mensajes personalizados a personas distintas, como si fueran reales, pero son generados por computadora. El delincuente ni siquiera necesita escribirlos, el sistema lo hace solo.
- **Pornografía no consentida**: Uno de los usos más dañinos es crear imágenes o videos falsos de personas desnudas, sin que ellas lo sepan. Esto es una forma de violencia digital y puede destruir la vida de una persona.
- **Manipulación de pruebas judiciales**: Si un delincuente puede hacer un video falso de alguien cometiendo un crimen, esto podría usarse para acusar a un inocente o para encubrir a un culpable.

2.2. Delitos creados por la IA como fenómeno emergente

La IA no solo mejora delitos antiguos, también está creando delitos nuevos que antes no existían.

- **Creación automática de malware**: Antes, para hacer un virus informático se necesitaba un programador experto. Ahora, con la IA, cualquier persona puede pedirle a un sistema que genere un programa dañino sin saber programar.
- **Hackeo predictivo**: La IA puede analizar miles de datos para encontrar puntos débiles en sistemas de seguridad. Esto permite que un ataque sea más preciso y más difícil de detener.
- **Fraudes financieros con algoritmos**: En la bolsa de valores y el comercio de criptomonedas ya se han visto casos donde la IA se usa para manipular precios o robar fondos.

Estos nuevos delitos son un reto para la policía y la justicia, porque la ley normalmente castiga cosas que ya conoce, y la IA cambia las reglas demasiado rápido, sobre todo en nuestro país que estamos retrasados digitalmente en sentido teórico y técnico.

2.3. Casos emblemáticos

A nivel mundial ya hay casos muy conocidos. Por ejemplo, en Hong Kong un grupo de delincuentes usó una videollamada deepfake para hacerse pasar por un jefe de empresa y así robar 25 millones de dólares. En España hubo un caso donde un político fue víctima de un video sexual falso creado para desprestigiarlo antes de unas elecciones.

En Bolivia todavía no se han visto casos tan grandes, pero sí se han reportado estafas usando audios falsos de familiares pidiendo dinero o mensajes que parecen venir de un banco. Estos delitos quizá no suenen tan graves como un asesinato, pero pueden arruinar económicamente a una persona o dejarla con un trauma psicológico.

III. MARCO NORMATIVO VIGENTE EN BOLIVIA

Hablar de criminalidad digital en Bolivia también significa revisar qué leyes tenemos para enfrentarla. Aunque suene raro, el Código Penal de nuestro país no tiene una parte exclusiva para delitos con inteligencia artificial o para cibercrímenes en general. Lo que hacen jueces y fiscales es adaptar artículos que ya existen para tratar de castigar estas conductas, pero no siempre encajan bien, y eso deja huecos que los delincuentes aprovechan.

3.1. Código Penal Boliviano

En el Código Penal hay varios artículos que podrían aplicarse en casos de delitos digitales, aunque fueron pensados para delitos comunes o tradicionales en nuestra sociedad:

- **Estafa (Art. 335)**: Se usa cuando alguien engaña para obtener un beneficio económico. El problema es que fue redactado pensando en estafas físicas, no en estafas por internet usando IA.
- **Falsificación de documentos (Art. 198 y siguientes)**: Aquí podrían entrar los documentos creados con IA, pero el artículo habla más de papel, sellos y firmas, no de archivos digitales

- **Pornografía y corrupción de menores (Art. 323 bis)**: Este artículo puede usarse contra quien genere o difunda imágenes sexuales de menores, incluso si son falsas, pero todavía hay discusión si las imágenes creadas por IA sin modelo real entran en este tipo penal.
- **Acceso indebido a sistemas informáticos (Art. 363 bis)**: Este es de los pocos artículos que sí fue pensado para delitos digitales, pero no habla nada de IA ni de las técnicas nuevas que hoy existen.

El problema es que, al no tener una definición clara y actualizada, muchos casos terminan en la nada o con penas que no reflejan la gravedad real del delito.

3.2. Ley de Telecomunicaciones (Ley 164)

Esta ley regula el uso de las redes de telecomunicación en Bolivia. Tiene algunos artículos que hablan de delitos como interceptar comunicaciones, robar señales o usar redes sin permiso. Sin embargo, no regula directamente los delitos con IA, y mucho menos menciona cosas como deepfakes o algoritmos de fraude.

Un punto importante es que la Ley 164 establece que los proveedores de servicios de internet deben colaborar con la justicia, pero en la práctica esto no siempre funciona bien. A veces las empresas no guardan datos el tiempo suficiente, o no tienen herramientas para rastrear un ataque.

3.3. Jurisprudencia nacional

En Bolivia hay muy poca jurisprudencia sobre delitos con IA. Lo que hay son sentencias relacionadas con delitos informáticos más generales, como estafas en redes sociales o hackeos a cuentas de correo. La falta de precedentes judiciales hace que cada nuevo caso sea un reto, porque no hay un “camino” ya marcado que los jueces puedan seguir.

Un ejemplo: en 2023 hubo un caso en Santa Cruz donde un joven fue acusado de estafa digital usando redes sociales. Aunque no había usado IA, el juez tuvo que interpretar las leyes existentes para condenarlo. Si hubiera usado IA, probablemente el caso habría sido aún más complicado.

IV. COMPARATIVA INTERNACIONAL

Cuando hablamos de delitos digitales y de inteligencia artificial, Bolivia no está sola en el problema. Otros países ya han enfrentado casos graves y han tenido que cambiar sus leyes. Mirar lo que hacen afuera sirve para entender cómo podríamos mejorar acá. No se trata de copiar todo, porque cada país tiene su realidad, pero sí de aprender y adaptar.

4.1. España

En España, el Código Penal fue reformado para incluir delitos relacionados con deepfakes y manipulación digital. Allá, si una persona crea o difunde imágenes o videos falsos de carácter sexual sin consentimiento, puede recibir penas de prisión, aunque la imagen sea inventada por IA. Además, el sistema judicial español tiene peritos informáticos especializados para detectar falsificaciones digitales, algo que en Bolivia casi no se ve.

España también tiene leyes sobre protección de datos personales muy estrictas. Esto hace que, si alguien usa datos de otra persona para entrenar un modelo de IA sin permiso, pueda enfrentar sanciones.

4.2. Unión Europea

La Unión Europea aprobó en 2024 la Ley de Inteligencia Artificial. Aunque no es una ley penal pura, establece reglas claras sobre el uso de IA y prohíbe ciertas aplicaciones que pueden ser peligrosas, como sistemas que manipulen a las personas o que clasifiquen a la gente de forma discriminatoria. Esto es importante porque, si un software viola esas reglas, sus creadores pueden ser sancionados e incluso enfrentar cargos penales en casos graves.

En Bolivia, no existe una regulación así de específica. Por eso, si alguien crea un sistema de IA para estafar, lo único que se puede hacer es buscar algún artículo general que se pueda aplicar, aunque no esté pensado para eso.

4.3. Argentina

Argentina no tiene un artículo especial para suplantación de identidad, pero ha avanzado en la persecución del ciberacoso y la violencia digital. Por ejemplo, la “Ley Olimpia” castiga la difusión de imágenes íntimas sin consentimiento, incluyendo las que sean falsas o creadas con IA. Esto cierra un vacío legal que todavía tenemos en Bolivia.

Además, en Argentina se han hecho acuerdos entre el Estado y empresas de tecnología para facilitar la investigación de delitos digitales, algo que acá sería muy útil porque muchas veces la policía no logra acceder a la información que necesita.

4.4. México

En México también existe la Ley Olimpia y, en algunos estados, se han aprobado reformas para que la suplantación de identidad digital sea delito grave. Esto significa que si alguien usa tu foto o voz para engañar a otra persona, puede recibir una condena más alta. México también está invirtiendo en capacitación de policías y fiscales en temas de análisis forense digital.

4.5. ¿Qué le falta a Bolivia?

Si comparamos todo esto con Bolivia, se ve que estamos muy atrasados. No tenemos una ley específica para IA, tampoco tipificación clara para manipulación digital, y la protección de datos personales es muy débil. Además, la falta de especialistas y herramientas tecnológicas hace que, incluso cuando existe un delito, investigarlo sea lento y complicado.

Una posible solución sería crear una ley que combine elementos de lo que han hecho España, la Unión Europea y países latinoamericanos como Argentina y México, pero adaptada a nuestra realidad. Eso ayudaría a cerrar vacíos legales y a dar más herramientas a las autoridades.

V. RETOS Y VACÍOS LEGALES

Hablar de criminalidad digital con IA en Bolivia no es solo listar delitos. El principal problema es que nuestro sistema penal no está preparado. Hay huecos en la ley, en la forma de investigar, en la prueba, y hasta en cómo protegemos a las víctimas. A continuación explico los retos más serios que veo.

5.1. Falta de tipificación específica

Muchos casos quedan “a medias” porque no existe un tipo penal claro para conductas nuevas: clonación de voz, creación automática de malware, manipulación algorítmica en estafas, etc. Fiscales y jueces fuerzan artículos como estafa o falsificación, pero no siempre encajan. Esto genera absoluciones o penas bajas. Además, no hay agravantes cuando se usa IA (por ejemplo, contra menores o autoridades), lo que reduce el efecto disuasivo.

5.2. Prueba digital y autenticidad

Probar que un audio o video es falso no es sencillo. Se necesita peritaje técnico para ver metadatos, patrones de edición, trazas algorítmicas, etc. Hoy, en muchos juzgados no hay peritos suficientes ni laboratorios forenses equipados.

5.3. Cadena de custodia tecnológica

En delitos “tradicionales” se controla la cadena de custodia de objetos físicos. En lo digital, el “objeto” es un archivo que se puede copiar en segundos. Si la policía descarga mal un video, o si alguien lo reenviá por WhatsApp antes del secuestro legal, la defensa puede decir que se contaminó. Hace falta un protocolo nacional para preservación, hash, copias espejo y registro de cada acceso a la evidencia.

5.4. Capacidades institucionales

La FELCC trabaja con recursos limitados. También faltan fiscales y jueces con formación en informática forense, redes, criptografía básica, etc. Sin comprensión técnica mínima,

se dictan medidas erradas o se pierden plazos. La capacitación debería ser obligatoria y continua, con manuales sencillos y casos prácticos.

5.5. Jurisdicción y cooperación internacional

Muchos atacantes operan desde otro país. Pedir datos a plataformas o a proveedores extranjeros toma meses, y a veces no responden. Falta un mecanismo rápido de cooperación internacional y acuerdos con grandes empresas tecnológicas. También necesitamos órdenes de preservación inmediatas para que no se borren registros en horas.

5.6. Responsabilidad de plataformas y proveedores

Hoy no está claro qué deben hacer las plataformas cuando circula un perfil falso delictivo: Sin un marco, cada empresa actúa como quiere. Se requiere definir **deberes de diligencia**, tiempos de respuesta y canales de atención a requerimientos fiscales, sin violar derechos.

5.7. Protección de datos personales

Bolivia tiene debilidad en protección de datos. Si alguien usa tus fotos para entrenar una IA o vende tu voz clonada, ¿qué norma fuerte lo frena? Esta falta facilita la recolección masiva de datos para fines delictivos. Una ley integral ayudaría a prevenir antes que castigar después.

5.8. Derechos fundamentales y riesgo de sobrerregulación

Regular rápido puede terminar afectando la libertad de expresión o el periodismo de investigación. También hay riesgo de censura previa si se obliga a plataformas a filtrar todo contenido “sospechoso”. El desafío es equilibrar seguridad y derechos, con criterios claros: dolo, daño real, y excepciones para parodia legítima o interés público.

5.9. Cultura de denuncia y revictimización

En sextorsión o contenidos íntimos, muchas víctimas no denuncian por vergüenza. Cuando denuncian, a veces se las cuestiona, lo cual revictimiza. Se necesitan rutas confidenciales, personal sensibilizado y medidas rápidas: derribo de contenido, órdenes de no contacto, apoyo psicológico.

5.10. Medidas cautelares y tiempos procesales

Estos delitos requieren rapidez. Si la fiscalía tarda semanas en pedir datos, se pierden. Hacen falta medidas cautelares tecnológicas con plazos cortos y supervisión judicial, para que el proceso sea eficaz sin abusos.

5.11. Reparación del daño

Aunque haya condena, el contenido falso puede seguir circulando. La reparación no es solo “pagar una multa”. Debe incluir takedown ampliado (bajar réplicas), derecho a rectificación visible y apoyo para rehabilitar reputación. En estafas, mecanismos ágiles para recuperar fondos movidos a billeteras o cuentas digitales.

5.12. Economía del delito y prevención

El delito prospera donde es barato y rentable. Hoy producir un perfil flaso cuesta poco y puede generar mucho. La prevención pasa por educación digital (escuelas, bancos, campañas), sellos de autenticidad en comunicaciones sensibles (banca, empresas) y verificación en dos pasos. Si sube el costo de delinquir y baja la ganancia, cae el incentivo.

5.13. Coordinación interinstitucional

Los encargados de investigar los cibercrímenes no pueden trabajar solos. Debe haber protocolos con bancos, operadores móviles, ministerios, defensa del consumidor, y academia . Una mesa técnica permanente ayudaría a uniformar criterios y compartir alertas tempranas.

VI. PROPUESTA DE REFORMA Y FORTALECIMIENTO DEL SISTEMA PENAL

En Bolivia ya se vio que el Código Penal no está hecho para casos de inteligencia artificial usada para cometer delitos. Por eso creo que se debería cambiar y agregar cosas nuevas que ayuden a la policía, a los fiscales y también a los jueces a trabajar mejor. No es solo hacer una ley más, también hay que dar herramientas para que funcione en la práctica, porque de nada sirve tener una norma si después no se puede aplicar.
En las noticias se han visto varios casos de estafas y de personas que fueron víctimas de suplantación de identidad, incluso con audios falsos que imitan la voz de un familiar pidiendo dinero. Si la ley fuera más clara, este tipo de casos se podrían resolver más rápido.

6.1. Crear delitos específicos para la IA

Hoy en día, si alguien usa un video falso para estafar o para arruinar la reputación de otra persona, el fiscal tiene que usar artículos como estafa o falsificación, que no fueron pensados para eso. El problema es que, al no encajar bien, el abogado defensor puede encontrar vacíos y el acusado termina libre o con una pena mínima.
Debería haber un artículo que hable directamente de manipulación digital, clonación de voz o imagen y deepfakes, con penas claras y más fuertes si la víctima es menor de edad, si se trata de una autoridad, o si el delito causa un daño económico grande.

Por ejemplo:

- Si un estafador clona la voz de un gerente de banco para dar una orden falsa de transferencia, eso debería estar tipificado claramente como delito de clonación de identidad biométrica.
- Si alguien crea un video falso de un político diciendo cosas graves para manipular una elección, debería considerarse un delito contra la democracia.
- Si un menor de edad es víctima de pornografía creada por IA, aunque no exista la imagen real, la pena debería ser igual de alta que si el material fuera verdadero.

6.2. Capacitación para autoridades

Si un juez o un fiscal no sabe cómo funciona un video falso o cómo se detecta, será muy difícil que pueda juzgar bien. A veces, por falta de conocimiento, las autoridades no entienden el alcance del daño que puede causar un deepfake o no saben qué pruebas pedir.
Por eso, se deberían hacer cursos y talleres obligatorios para todas las personas que trabajan en estos casos, para que aprendan cómo investigar, cómo guardar la prueba y cómo reconocer si un archivo fue creado por IA.

Imaginemos un juicio donde la prueba principal es un audio. Si el fiscal no sabe cómo revisar los metadatos o pedir un peritaje digital, esa prueba podría ser descartada y el acusado salir libre.
En cambio, si las autoridades estuvieran capacitadas, podrían detectar detalles como fallas en la sincronización de labios en un video o patrones de voz que revelan que es artificial.

6.3. Mejorar la investigación

La FELCC y las unidades de cibercrimen necesitan más equipos, programas y personal capacitado. Muchas veces los casos se quedan sin resolver porque no tienen las herramientas para rastrear a los delincuentes.
Un ejemplo claro es cuando una persona es víctima de sextorsión: si el contenido se sube a internet y no hay un sistema para rastrear la IP o pedir los datos rápidamente a la plataforma, es casi imposible dar con el culpable.

Con mejores equipos y programas especializados, sería más fácil:

- Detectar desde qué lugar del mundo se envió un mensaje fraudulento.
- Rastrear transacciones de criptomonedas usadas para recibir pagos ilegales.
- Analizar de manera más rápida y exacta si un archivo fue manipulado.

Además, más personal permitiría que se atiendan los casos más rápido. Hoy en día hay pocas personas trabajando en cibercrimen, lo que hace que se acumulen las denuncias.

6.4. Cooperar con empresas de internet

La mayoría de estos delitos se hacen usando redes sociales, aplicaciones de mensajería o correos electrónicos. Las empresas que manejan esas plataformas deberían tener la obligación de colaborar rápido con las autoridades cuando se comete un delito grave. Esto significa que, ante una orden de un juez, una empresa como Facebook, WhatsApp o Google debería entregar datos como la IP, ubicación o historial de actividad del usuario sospechoso.

Un ejemplo: si alguien publica un video falso para dañar a una persona, la empresa debería poder borrarlo en cuestión de horas y guardar todos los datos para la investigación. Si eso se hace rápido, se evita que el daño siga creciendo.

También sería útil firmar acuerdos entre el Estado y las plataformas para que haya canales directos de comunicación en casos urgentes. En otros países esto ya funciona y ha dado buenos resultados.

6.5. Protección para las víctimas

En casos como sextorsión o videos falsos, la prioridad debería ser quitar el contenido de internet lo más rápido posible. La ley debería permitir que el juez ordene a las plataformas borrar todo el material y bloquear cuentas que lo difundan. Además, las víctimas deberían recibir apoyo psicológico, porque muchas veces el daño no es solo económico, sino también emocional y social.

Por ejemplo, si a una joven le crean un video falso con contenido íntimo, aunque se demuestre que es mentira, el impacto en su vida personal puede ser muy grande. Podría perder amistades, trabajos o ser discriminada. Por eso, además de borrar el contenido, debería existir un mecanismo para ayudar a limpiar su reputación.

6.6. Educación y prevención

La gente también tiene que aprender a reconocer este tipo de engaños. El Estado podría hacer campañas en redes sociales, colegios y universidades para explicar cómo funcionan los deepfakes y qué hacer si alguien recibe un mensaje o video sospechoso.

Si las personas saben que no deben confiar en un mensaje que les pide dinero urgente o que no deben compartir fotos privadas por internet, se reduciría mucho el número de víctimas.

Un buen ejemplo de prevención es lo que hacen algunos bancos, que envían mensajes a sus clientes para advertir sobre estafas y enseñarles a verificar la información. Algo así podría hacerse a nivel nacional, no solo en el sector financiero, sino también para proteger datos personales y evitar el uso indebido de imágenes y voces.

VII. IMPACTO SOCIAL DE LA CRIMINALIDAD DIGITAL CON INTELIGENCIA ARTIFICIAL

Los delitos cometidos con ayuda de la inteligencia artificial no solo afectan a las víctimas directas, también tienen un impacto en toda la sociedad. Estos crímenes no se quedan en el daño económico o material, sino que generan desconfianza, miedo y, en muchos casos, cambian la forma en que la gente se relaciona con la tecnología.

7.1. En Bolivia

En Bolivia, aunque no se han registrado casos tan grandes como en otros países, sí hay incidentes que han dejado huella en la opinión pública. En los últimos años, se han denunciado:

- Estafas por WhatsApp usando audios falsos que imitan la voz de un familiar para pedir dinero urgente.
- Casos de sextorsión donde se manipularon fotos de las víctimas para chantajearlas.
- Venta de productos inexistentes usando imágenes falsas y perfiles creados por IA para parecer más confiables.

El impacto social de estos delitos en el país se ve en varias formas:

1. **Pérdida de confianza en la comunicación digital:** Muchas personas, después de vivir o escuchar sobre estos casos, dudan incluso de mensajes enviados por sus propios contactos.
2. **Miedo a denunciar:** En delitos como sextorsión, las víctimas sienten vergüenza y prefieren callar, lo que deja a los delincuentes sin castigo.
3. **Daño a la reputación:** En un país como Bolivia, donde las comunidades suelen ser pequeñas, un rumor o contenido falso puede destruir la reputación de una persona para siempre, aunque luego se demuestre que no era real.

Un ejemplo reciente fue el de una joven en La Paz que denunció la difusión de un video íntimo falso creado con IA. Aunque la policía logró eliminar el video de las redes sociales, el daño emocional y social ya estaba hecho.

7.2. En el mundo

A nivel internacional, el impacto ha sido aún más visible por el alcance global de las redes y la magnitud de algunos delitos.

- **Caso Hong Kong (2024):** Un grupo de delincuentes usó una videollamada deepfake para hacerse pasar por un directivo de empresa y ordenar transferencias por 25 millones de dólares. Esto no solo afectó a la empresa, sino que generó dudas sobre la seguridad de las reuniones virtuales en todo el mundo.
- **Deepfake de Obama (2018):** Un video manipulado del expresidente de Estados Unidos, donde aparentemente decía cosas que nunca pronunció, alertó sobre el poder de la IA para crear noticias falsas y manipular la opinión pública.
- **Elecciones en India (2023):** Candidatos denunciaron que se usaron audios y videos falsos para desprestigiarlos durante la campaña. Esto provocó debates sobre cómo proteger la democracia frente a la manipulación digital.

Los efectos sociales de estos casos incluyen:

1. **Desconfianza en la información:** Las personas empiezan a cuestionar si lo que ven y escuchan es real, lo que debilita la credibilidad de medios, autoridades y líderes.
2. **Inseguridad económica:** Empresas y particulares temen usar canales digitales para operaciones financieras importantes.
3. **Polarización y conflictos:** Cuando los deepfakes se usan con fines políticos, pueden generar divisiones sociales y enfrentamientos.

7.3. Un problema que trasciende fronteras

El impacto social de la criminalidad digital con IA no se limita a un país. En un mundo conectado, un deepfake creado en un continente puede afectar a alguien en otro en cuestión de minutos. Esto significa que la respuesta también debe ser global, con cooperación entre gobiernos, empresas tecnológicas y organizaciones internacionales.

En Bolivia, el desafío es doble: por un lado, adaptarse a la velocidad con la que evolucionan estas amenazas; y por otro, hacerlo sin generar un clima de miedo que lleve a las personas a desconfiar de toda tecnología. La sociedad necesita encontrar un equilibrio entre aprovechar los beneficios de la IA y protegerse de sus riesgos.

CONCLUSIONES

En los últimos años la inteligencia artificial se ha convertido en una herramienta que, usada de forma indebida, facilita la comisión de delitos digitales cada vez más complejos. En Bolivia, la ley todavía no está preparada para enfrentar estos casos, lo que deja a las autoridades con pocas opciones y a las víctimas con poca protección.

Es necesario actualizar el Código Penal para incluir delitos específicos relacionados con la manipulación digital, además de capacitar a fiscales, jueces y policías para entender y manejar este tipo de pruebas. También se deben fortalecer las unidades de investigación y trabajar junto con las empresas tecnológicas para actuar rápido cuando se detecta un delito.

Finalmente, la prevención es fundamental. Si las personas conocen los riesgos y saben cómo protegerse, será más difícil que caigan en engaños. La inteligencia artificial puede ser una gran aliada, pero solo si la sociedad y la ley están preparadas para controlarla y evitar que se use para causar daño.

BIBLIOGRFIA

- Aguilar, J. P. (2023). *Delitos informáticos y ciberseguridad en Bolivia*. La Paz: Editorial Jurídica Boliviana.
- Álvarez, R. (2021). *Derecho penal y nuevas tecnologías: retos en América Latina*. Cochabamba: Universidad Mayor de San Simón.
- Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC. (2022). *Informe sobre ciberseguridad en Bolivia*. La Paz: AGETIC. https://www.agetic.gob.bo/sites/default/files/2025-04/22.pdf
- Andrade, M. (2020). *Protección de datos personales y privacidad digital en Bolivia*. La Paz: Plural Editores.
- Código Penal Boliviano. (2023). *Ley N° 1768 de 10 de marzo de 1997 con sus modificaciones*. Gaceta Oficial del Estado Plurinacional de Bolivia. https://www.minsalud.gob.bo/images/Documentacion/normativa/LEY%201768%20CODIGO%20PENAL.pdf
- Ley de Telecomunicaciones, Tecnologías de Información y Comunicación (Ley N° 164 de 8 de agosto de 2011). Gaceta Oficial del Estado Plurinacional de Bolivia. https://www.minedu.gob.bo/files/documentos-normativos/leyes/ley_164___ley_general_de_telecomunicaciones_tecnologias_de_informacin_y_comunicacion.pdf
- Flores, L. & Paredes, A. (2022). *Inteligencia artificial y derecho penal: desafíos para el sistema jurídico boliviano*. Revista Boliviana de Ciencias Jurídicas, 15(2), 45–62. https://www.revista-rbd.com/wp-content/uploads/2023/07/RBD-N%C3%BAmero-36-Completo.pdf
- Instituto Nacional de Estadística – INE. (2023). *Estadísticas sobre uso de internet y redes sociales en Bolivia*. La Paz: INE. https://www.ine.gob.bo/index.php/estadisticas-economicas/telecomunicaciones-cuadros-estadisticos/
- Ramírez, D. (2022). *Deepfakes y manipulación digital: implicaciones jurídicas y éticas*. Santa Cruz: Editorial Universitaria.

- Rojas, C. (2021). *El impacto de la inteligencia artificial en los derechos fundamentales*. La Paz: Fundación para el Desarrollo Jurídico.
- Agencia EFE. (2024, octubre 29). *Cuidado en WhatsApp: copian la voz de tu mamá, usan IA para crear la estafa y roban dinero del banco*. Infobae. https://www.infobae.com/tecno/2024/10/29/cuidado-en-whatsapp-copian-la-voz-de-tu-mama-usan-ia-para-crear-la-estafa-y-roban-dinero-del-banco/
- ESET. (2023, junio 9). *Ciberdelincuentes crean falsas imágenes y videos sexuales mediante inteligencia artificial para sextorsión*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2023/06/09/ciberdelincuentes-falsas-imagenes-videos-sexuales-mediante-inteligencia-artificial-sextorsion/