Cuestionario - Grupo de Trabajo sobre la Detención Arbitraria

Datos de contacto

David Ricardo Urquilla Bonilla, abogado y experto en tecnología en el Instituto Internacional de Responsabilidad Social y Derechos Humanos - IIRESODH.

E-mail: durquilla@iiresodh.org

Confidencialidad
Tenga en cuenta que todos los aportes recibidos se publicarán en el sitio web del Grupo de Trabajo sobre Desapariciones Forzadas o Involuntarias, a menos que se indique expresamente que la presentación debe mantenerse confidencial.

Preguntas
Puede responder todas o sólo las preguntas que considere relevantes para usted.

1. *1.1*) ¿Podría ilustrar cuáles son los principales riesgos que presenta el uso de las nuevas tecnologías en relación con el trabajo de las personas defensoras de derechos humanos y, en particular, de las y los familiares de las personas desaparecidas?

El uso de nuevas tecnologías en relación con el trabajo de las personas defensoras de derechos humanos y, en particular, de las y los familiares de las personas desaparecidas, presenta una serie de riesgos. Estos incluyen el riesgo de ser expuestos a la vigilancia y seguimiento por parte de gobiernos, a la intercepción de datos y comunicaciones, así como al uso indiscriminado de la fuerza por parte de las autoridades. También existe el riesgo de que los datos personales de las personas defensoras de derechos humanos y las familias de las personas desaparecidas sean vulnerables a ataques informáticos y a la explotación de información confidencial. Por último, el uso de nuevas tecnologías también puede dar lugar a nuevas formas de acoso y violencia en línea. Por lo que es importante que las personas defensoras de derechos humanos y las familias de las personas desaparecidas sean conscientes de los riesgos que conlleva su utilización, y tomen las precauciones necesarias para protegerse.

1.2) ¿Cómo se pueden mitigar estos riesgos?

Existen varias medidas que se pueden tomar para mitigar los riesgos mencionados anteriormente:

- Educación y capacitación en seguridad cibernética: Es importante que las personas defensoras de derechos humanos y las familias de las personas desaparecidas reciban educación y capacitación en cómo protegerse de los riesgos cibernéticos, como el acoso cibernético y la vigilancia masiva.
- Implementación de medidas técnicas de seguridad: Implementar medidas de seguridad en dispositivos y plataformas en línea para proteger la información personal y prevenir ataques cibernéticos.
- Aplicación de leyes y regulaciones existentes: Aplicar las leyes y regulaciones existentes para perseguir y sancionar a los perpetradores de acoso cibernético, vigilancia masiva y desinformación.
- Mecanismos específicos de investigación y persecución: Pueden ser necesarios mecanismos específicos para investigar y perseguir los delitos

cibernéticos cometidos contra personas defensoras de derechos humanos y familiares de personas desaparecidas.
- Cooperación interinstitucional: Es muy importante fomentar la cooperación interinstitucional para combatir los riesgos cibernéticos y proteger a las personas defensoras de derechos humanos y familiares de personas desaparecidas.
- Monitoreo y supervisión independiente: Contar con mecanismos de supervisión independiente encargados de monitorear el sector de seguridad ofensiva (cyber-security) para detectar y sancionar las violaciones a las regulaciones y leyes.

1.3) ¿Puede proporcionar ejemplos concretos sobre cómo se han utilizado las nuevas tecnologías como una herramienta para obstaculizar la lucha de las familias de las personas desaparecidas y las personas defensoras de los derechos humanos por la verdad y la justicia (incluso a través del acoso cibernético, el acoso sexual, etc.)?

Sí, hay varios ejemplos concretos de ello:

- Acoso cibernético: Han sufrido acoso cibernético a través de las redes sociales y los medios digitales. Han recibido amenazas, insultos, y han sido víctimas de campañas de difamación.
- Espionaje: Han sido espiados mediante el uso de malware y otros programas de vigilancia electrónica.
- Censura: Sus cuentas de redes sociales han sido objeto de suspensión o bloqueo como parte de campañas de censura.
- Ataques a la privacidad: Robo de identidad y difusión de información personal.
- Acoso sexual: Son objeto de acoso sexual por medio de redes sociales y medios de comunicación electrónicos, así como objeto de envío de material de naturaleza sexual no deseados.
- Dispersión de información falsa: Han sido objeto de campañas de difamación y difusión de información falsa para desacreditarlos.
- Ataques a la infraestructura tecnológica: También han visto sus sitios web o redes sociales hackeados o sufrir un ataque DDoS.

En algunos casos, estas herramientas han sido utilizadas para sofocar la voz de las personas y generar un ambiente de temor y represión. Por ejemplo, en México, el [redacted] fue asesinado y previamente había sido objeto de amenazas y otros abusos por parte de las autoridades mexicanas por su trabajo en defensa de los derechos humanos. En Venezuela, los activistas y defensores de los derechos humanos han sido víctimas de ciberataques y vigilancia electrónica por parte de las autoridades venezolanas. Y en El Salvador recientemente se ha denunciado públicamente el uso del programa de espionaje “Pegasus” por parte del gobierno para espiar a sus contrapartes políticos, incluyendo defensores de derechos humanos.

1.4) ¿Cómo puede el sistema judicial ofrecer una protección efectiva frente a este tipo de acoso?

El sistema judicial puede ofrecer una protección efectiva frente al acoso cibernético y otras formas de abuso en línea de varias maneras:

- Proposición de leyes: El sistema judicial puede proponer la creación de leyes específicas para abordar el acoso cibernético y otros delitos en línea. Estas leyes deben ser actualizadas periódicamente para cubrir las nuevas formas de abuso.
- Proporcionando un mecanismo de denuncia: Puede y debe proporcionar un mecanismo fácil y seguro para que las personas denuncien el acoso cibernético y otros delitos en línea y brindarles la asesoría correspondiente.
- Proporcionando recursos para la investigación: Puede proporcionar recursos para la investigación de delitos en línea, incluyendo la capacitación para los investigadores y la tecnología necesaria para rastrear a los perpetradores.
- Asegurando la protección de las víctimas: Debe asegurar que las víctimas de acoso cibernético y otros delitos en línea sean protegidas de la represalia y el acoso adicional.
- Asegurando la responsabilidad de los perpetradores: Debe asegurar que los perpetradores de acoso cibernético y otros delitos al ser llevados ante la justicia sean procesados de manera contundente y adecuada.
- Promoviendo la educación y concientización: Puede promover la educación y concientización sobre el acoso cibernético y otros delitos en línea, para ayudar a las personas a reconocer y prevenirlos.
- Cooperación: Puede cooperar con otros actores relevantes, como la industria tecnológica, los grupos de defensa de derechos humanos y otros expertos en seguridad digital, para mejorar la protección contra el acoso cibernético y otros delitos en línea.

2. *2.1*) ¿Cómo cree que las nuevas tecnologías se están utilizando/pueden utilizarse para facilitar la comisión de una desaparición forzada (por ejemplo, rastreando a posibles víctimas o ejerciendo vigilancia sobre sus familiares) y para encubrir la comisión de una desaparición forzada (si es posible, proporcione ejemplos concretos)?

Las nuevas tecnologías pueden utilizarse para facilitar y encubrir la comisión de desapariciones forzadas de diversas maneras. Por ejemplo, las redes sociales se pueden usar para rastrear a las posibles víctimas, especialmente si tienen un perfil público y comparten información sobre sus ubicaciones y planes. También se pueden usar para monitorizar a los familiares de la víctima, para ver si hay alguna actividad sospechosa o si se están realizando búsquedas. También existen casos donde tanto autoridades como grupos paramilitares han utilizado malware y spyware para obtener información personal y monitorear las actividades de las víctimas y sus familiares

Las nuevas tecnologías también se pueden usar para encubrir la comisión de una desaparición forzada. Los agresores pueden usar aplicaciones de mensajería para comunicarse entre ellos, potencialmente sin que sus víctimas se enteren. También pueden usar el cifrado para mantener sus conversaciones privadas. Además, los agresores pueden usar la geolocalización para evitar zonas de riesgo o lugares donde se realicen búsquedas.

Existen dispositivos de seguimiento en tiempo real por medio del sistema de posicionamiento global (GPS) que una vez instalados permiten ubicar a posibles víctimas. Lo mismo sucede con los llamados “AirTag” que han sido utilizados para seguimiento en tiempo real de víctimas.

2.2) ¿Cuáles son las medidas preventivas que se han implementado (o se pueden implementar)?

Existen varias medidas preventivas que se pueden tomar para evitar la comisión de desapariciones forzadas. Estas incluyen el fortalecimiento de la seguridad ciudadana, el desarrollo de una cultura de respeto a los derechos humanos, el monitoreo de zonas de alto riesgo y la adopción de normas internacionales sobre desapariciones forzadas.

Además, los gobiernos y organizaciones podrían fomentar el acceso a la información, la transparencia y la rendición de cuentas para prevenir la violencia y las desapariciones forzadas. Esto implica el monitoreo y la difusión de información sobre el uso del poder estatal y el establecimiento de mecanismos para hacer cumplir la ley.

Los gobiernos también deberían apoyar y garantizar el derecho de la gente a reunirse y participar en actividades pacíficas. Esto incluye el respeto a la libertad de expresión y el derecho de los periodistas a informar sin temor a represalias. Asimismo, los gobiernos deben desarrollar y respetar los mecanismos de protección de los derechos humanos y garantizar el acceso a la justicia para los afectados por desapariciones forzadas.

3. *3.1*) ¿Puede ilustrar el marco legal aplicable (regulaciones y políticas), si lo hay, en su país (o países de interés) para tratar, en particular, (a) apagones o restricciones de acceso a Internet (*internet shutdowns or restrictions*); (b) cyber-vigilancia y ataques, (c) campañas de desinformación; y (d) el uso de spyware?

El marco legal para tratar el apagón o restricciones de acceso a Internet (internet shutdowns o restrictions) depende de cada país. Por ejemplo, en los Estados Unidos, el "Internet Freedom Preservation Act" ofrece alguna protección a los usuarios de Internet contra los apagones. En otros países, como el Reino Unido, la legislación reguladora es más laxa. En cuanto a la vigilancia cibernética y los ataques, hay una serie de regulaciones legales que se aplican. Estas regulaciones prohíben la intromisión en la privacidad de las personas, el robo de información y la interrupción ilegal del servicio de Internet. En cuanto a la desinformación, hay una serie de regulaciones establecidas por la FTC (Federal Trade Commission) de los Estados Unidos que prohíben la publicación de información engañosa o falsa con fines comerciales. Por último, el uso de spyware no está permitido en la mayoría de los países, incluidos los Estados Unidos, y hacerlo se considera una violación de la ley.

3.2) ¿Puede proporcionar ejemplos concretos sobre el uso de las herramientas/técnicas mencionadas en la práctica?

- Apagones o restricciones de acceso a Internet: En países como Egipto, Irán y Siria, se han registrado apagones masivos durante conflictos políticos y protestas civiles para evitar que los ciudadanos organizaran y compartieran información sobre los eventos.
- Cyber-vigilancia y ataques: En países como China, Rusia y Turquía, se han registrado casos de vigilancia cibernética masiva de ciudadanos y organizaciones críticas del gobierno, así como ataques cibernéticos contra sitios web y cuentas de redes sociales de estos grupos.
- Campañas de desinformación: En países como Rusia y China, se han registrado campañas sistemáticas de desinformación a través de medios de comunicación controlados por el estado y medios sociales para influir en la opinión pública y desacreditar a los oponentes políticos.

- Uso de spyware: En países como El Salvador, México, Turquía y Egipto, se han registrado casos de uso de spyware por parte de las autoridades para monitorear y recolectar información sobre defensores de derechos humanos, periodistas y oponentes políticos.

Es importante tener en cuenta que estos abusos pueden ser originados por distintos actores, no solo por parte de las autoridades gubernamentales, sino también por grupos paramilitares, criminales y otros actores no estatales. Aquí queda de manifiesto la importancia de la regulación adecuada y la protección de derechos humanos frente a estas prácticas y también la necesidad de una respuesta multisectorial e intergubernamental para hacer frente a estos desafíos.

4. ¿Cuáles son las normas aplicables en su país (o países de interés) para regular la importación/exportación y el uso de tecnologías de vigilancia?

En Costa Rica podemos encontrar leyes que pueden en alguna medida regular el uso de tecnologías de vigilancia, y entre ellas encontramos:

- Ley de Protección de la Persona frente al tratamiento de sus datos personales
- Reglamento Regulador de la Vigilancia de Calles, Avenidas, Carreteras y Caminos mediante Dispositivos Tecnológicos o Técnicos
- Código Penal en cuanto a la regulación de la difusión de información falsa, violación de comunicaciones electrónicas, estafa o fraude informático, alteración de datos y sabotaje informático.

Es de hacer notar que estas normativas pueden ser utilizadas para luchar contra el mal uso de las tecnologías frente a los ciudadanos.

5. ¿Existe en su país (o países de interés) algún mecanismo de supervisión independiente encargado de monitorear el sector de seguridad ofensiva (*cyber-security*)?

En Costa Rica, no existe un mecanismo de supervisión independiente específico encargado de monitorear el sector de seguridad ofensiva (cyber-security). Sin embargo, existen ciertos organismos encargados de supervisar y regular el sector de la seguridad cibernética en general.

El Instituto Costarricense de Electricidad (ICE) es el organismo encargado de regular el sector de las telecomunicaciones en Costa Rica, y por tanto tiene la responsabilidad de velar por la seguridad en las comunicaciones. También existe el "Sistema Nacional de Protección Civil y Seguridad en Tecnologías de la Información" (SISPROTEC) creado para la protección de las infraestructuras críticas y el fortalecimiento de la seguridad cibernética en Costa Rica.

Además, existe el "Sistema Nacional de Ciberseguridad" (SNC) creado para proteger los sistemas informáticos y las redes de comunicaciones de ataques cibernéticos, y garantizar la continuidad del funcionamiento de los sistemas críticos del país. El SNC es coordinado por el Ministerio de Seguridad Pública y cuenta con la participación de distintas entidades gubernamentales y del sector privado.

En general, existen instituciones encargadas de supervisar y regular la seguridad cibernética en Costa Rica, pero no hay un mecanismo específico para monitorear el sector de seguridad ofensiva.

6. ¿Existe algún ejemplo concreto en el que el uso indebido de las nuevas tecnologías para hostigar a personas defensoras de los derechos humanos, incluidos las y los familiares de personas desaparecidas, o para facilitar la comisión de una desaparición forzada o para encubrirla, haya sido objeto de investigación, enjuiciamiento y sanción de los responsables? Sírvase ilustrar los principales obstáculos encontrados en este ámbito, así como las lecciones aprendidas y las buenas prácticas.

En Costa Rica no se ha registrado un ejemplo concreto en el que el uso indebido de las nuevas tecnologías para hostigar a personas defensoras de los derechos humanos, incluidos las y los familiares de personas desaparecidas, o para facilitar la comisión de una desaparición forzada o para encubrirla, haya sido objeto de investigación, enjuiciamiento y sanción de los responsables. Sin embargo, en otros países, se han registrado casos de abuso de tecnología para perseguir a defensores de derechos humanos y sus familiares, así como para facilitar o encubrir desapariciones forzadas.

Uno de los principales obstáculos en este ámbito es la falta de regulación y supervisión adecuadas para garantizar el uso responsable de estas tecnologías. Además, los perpetradores de estos abusos a menudo utilizan técnicas sofisticadas para eludir la detección y el enjuiciamiento, lo que dificulta la investigación y el procesamiento de los responsables.

Para abordar estos desafíos, se han desarrollado algunas buenas prácticas, como la creación de mecanismos de denuncia y de investigación independientes para recibir y procesar quejas sobre abusos de tecnología, y la capacitación de funcionarios judiciales y otros profesionales para investigar y procesar casos de abuso de tecnología.

Otra buena práctica es la promoción de la educación y la conciencia sobre los riesgos y las implicaciones éticas y legales del uso de tecnologías de vigilancia, para que las personas puedan tomar medidas para protegerse a sí mismas y a sus comunidades de los abusos de tecnología.

En general, es importante seguir desarrollando mecanismos efectivos de prevención, investigación y sanciones para abordar los abusos de tecnología contra defensores de derechos humanos y sus familiares, así como la promoción de un marco legal y regulación adecuado para garantizar el uso responsable de estas tecnologías. Es importante también la colaboración interinstitucional y la cooperación internacional para abordar estos desafíos complejos y globalizados, teniendo en cuenta que estas violaciones no solo tienen consecuencias a nivel local sino también internacional.

7. ¿Cómo pueden las nuevas tecnologías (y qué nuevas tecnologías) facilitar la búsqueda de personas desaparecidas forzadamente (si es posible, proporcionando ejemplos concretos e ilustrando cómo funcionan dichas tecnologías)? ¿Cuáles deberían considerarse las herramientas "indispensables" en este ámbito? ¿Son estas herramientas fácilmente accesibles y asequibles o existen obstáculos específicos en su compra y uso?

Existen varias nuevas tecnologías que pueden facilitar la búsqueda de personas desaparecidas forzadamente. Algunos ejemplos incluyen:

- Inteligencia artificial (IA) y análisis de datos: La IA y el análisis de datos pueden ayudar a identificar patrones y conexiones en grandes cantidades de información, como datos de redes sociales, imágenes y videos, lo que puede ayudar a localizar a personas desaparecidas.
- Geolocalización: La geolocalización permite rastrear la ubicación de dispositivos móviles y otros dispositivos conectados a Internet, lo que puede ayudar a localizar a personas desaparecidas.
- Reconocimiento facial: El reconocimiento facial puede ayudar a identificar a personas desaparecidas a partir de imágenes y videos, incluso en casos en los que las personas han cambiado su apariencia física.
- Tecnologías de seguimiento: Las tecnologías de seguimiento, como los dispositivos GPS, pueden ayudar a rastrear la ubicación de personas desaparecidas y proporcionar información valiosa para las investigaciones.
- Drones: Los drones pueden utilizarse para buscar personas desaparecidas en áreas de difícil acceso o de riesgo.
- Tecnologías de escaneo: Los escáneres de huellas dactilares y de ADN pueden ayudar a identificar a personas desaparecidas, especialmente en casos en los que las personas no tienen documentación o no pueden ser reconocidas por su apariencia física.

En general, las herramientas "indispensables" en este ámbito incluyen aquellas que pueden ayudar a recopilar y analizar información, identificar a personas desaparecidas y rastrear su ubicación. Estas herramientas deben ser fácilmente accesibles y asequibles, y deben ser utilizadas de manera ética y respetando los derechos humanos.

Sin embargo, aunque existen estas tecnologías que pueden ayudar en la búsqueda de personas desaparecidas, existen obstáculos específicos en su compra y uso, como el alto costo de algunas de estas herramientas, la falta de capacitación para su uso, y la falta de regulación y supervisión adecuadas para garantizar su uso ético y respetando los derechos humanos.

8. ¿Cuáles son las nuevas tecnologías que han arrojado resultados más significativos en términos de búsqueda de personas desaparecidas forzadamente y cómo funcionan? ¿Existen diferencias prácticas significativas en cuanto a las tecnologías que se emplearán en la búsqueda de la persona viva o muerta?

Algunas de las nuevas tecnologías incluyen:

- Inteligencia artificial (IA) y análisis de datos.
- Geolocalización.
- Reconocimiento facial.
- Tecnologías de escaneo.

En cuanto a las diferencias prácticas entre buscar una persona viva o muerta, en general, la búsqueda de una persona viva requiere una mayor cantidad de recursos y un enfoque más amplio, ya que es necesario buscar en un área más amplia y considerar más posibilidades. En contraposición, en la búsqueda de una persona muerta, las acciones se concentran en localizar el cuerpo y en la identificación de la persona. La tecnología de geolocalización y reconocimiento facial pueden ser útiles en ambos casos, mientras que la tecnología de escaneo, como los escáneres de huellas dactilares y ADN, son más específicas para la identificación de una persona muerta.

Es importante tener en cuenta que la búsqueda de personas desaparecidas forzadamente es un proceso complejo que requiere un enfoque multidisciplinario, incluyendo la colaboración de organismos gubernamentales, organizaciones no gubernamentales y familiares, así como la utilización de una variedad de herramientas y tecnologías para maximizar las posibilidades de éxito.

9. ¿Se pueden superar los obstáculos generados por el paso del tiempo en la búsqueda de personas desaparecidas mediante el uso de las nuevas tecnologías? ¿Si es así, cómo?

Con el uso de las nuevas tecnologías se puede ayudar a superar algunos de los obstáculos generados por el paso del tiempo. Por ejemplo:

Análisis de datos: El análisis de datos puede ayudar a identificar patrones y conexiones en grandes cantidades de información, como datos de redes sociales, imágenes y videos, lo que puede ayudar a localizar a personas desaparecidas.

Inteligencia Artificial: A través de algoritmos de IA se puede analizar información a través de patrones, conexiones, y características similares para poder conectar información y personas desaparecidas.

Tecnologías de escaneo: Los escáneres de huellas dactilares y de ADN pueden ayudar a identificar a personas desaparecidas, incluso en casos en los que las personas no tienen documentación o no pueden ser reconocidas por su apariencia física.

Reconstrucciones 3D: A través de tecnologías de reconstrucciones 3D, es posible crear imágenes y modelos 3D de la persona desaparecida para poder dar una idea de cómo se veía en el momento de su desaparición y poder comparar con imágenes actuales.

Es importante señalar que en la búsqueda de personas desaparecidas, pueden existir desafíos muy grandes debido a la complejidad del proceso y la falta de información disponible.

10. ¿Puede indicar buenas prácticas, así como los principales obstáculos (prácticos y legales) encontrados por usted/su país (o países de interés)/institución/organización en el uso de nuevas tecnologías para investigar casos de desapariciones forzadas (de ser posible, brindando ejemplos concretos)? ¿Cuáles son las herramientas que consideraría más eficaces para tales fines? ¿Son estas herramientas fácilmente accesibles y asequibles o existen obstáculos específicos en su compra y uso?

La investigación de casos de desapariciones forzadas es un desafío complejo que requiere la combinación de esfuerzos de diferentes entidades y la utilización de diferentes herramientas y tecnologías. Algunas buenas prácticas incluyen:

- La colaboración interinstitucional: Es importante que diferentes entidades estatales, como la Policía, el Ministerio Público y el sistema de justicia, trabajen juntas para investigar y resolver los casos de desapariciones forzadas.
- La utilización de tecnologías avanzadas: La tecnología puede ser una herramienta valiosa para investigar casos de desapariciones forzadas, como el uso de sistemas de geolocalización, análisis de datos, inteligencia artificial y análisis de imágenes.

- La importancia de la comunicación: Es importante mantener una comunicación fluida entre las diferentes entidades involucradas en la investigación y con las familias de las personas desaparecidas.

Entre los principales obstáculos prácticos y legales se encuentran:

- Falta de capacitación y recursos: Muchas veces, las entidades estatales no cuentan con los recursos y la capacitación necesarios para utilizar las herramientas y tecnologías disponibles de manera eficaz.
- Protección de datos personales: La recolección y el manejo de datos personales pueden enfrentar obstáculos legales debido a las leyes de protección de datos personales.
- Acceso a tecnologías costosas: Muchas veces, el acceso a ciertas tecnologías y herramientas avanzadas puede ser limitado debido a su elevado costo.

En cuanto a las herramientas más eficaces se pueden incluir:

- Geolocalización: El uso de sistemas de geolocalización puede ayudar a rastrear la ubicación de una persona desaparecida.
- Análisis de datos: El uso de herramientas de análisis de datos puede ayudar a identificar patrones y relaciones relevantes en los casos de desapariciones forzadas.
- Inteligencia artificial: La inteligencia artificial puede ser utilizada para analizar grandes cantidades de información y ayudar en la identificación de sospechosos y víctimas de desapariciones forzadas.
- Análisis de imágenes: El uso de tecnologías de análisis de imágenes, como el reconocimiento facial y la detección de objetos, puede ayudar a identificar a personas desaparecidas a partir de imágenes y videos.

En cuanto a la accesibilidad y asequibilidad de estas herramientas, es importante mencionar que algunas de ellas son muy costosas y solo están disponibles para entidades estatales, mientras que otras son más accesibles y asequibles pero pueden no ser tan avanzadas tecnológicamente. Además, algunas de estas herramientas pueden requerir de una capacitación especializada para su uso y algunas herramientas pueden ser ilegales o no estar reguladas en algunos países.

11. ¿Cuáles son las "pruebas" que usted consideraría esenciales para acreditar el delito de desaparición forzada y que pueden ser recaudadas mediante el uso de nuevas tecnologías? ¿Ve algún problema específico en la preservación de la cadena de custodia aquí y en la admisibilidad de algunas pruebas específicas de este delito recopiladas mediante el uso de las nuevas tecnologías?

Existen diferentes tipos de pruebas que pueden ser recaudadas para acreditar el delito de desaparición forzada, algunas de las cuales pueden ser recopiladas mediante el uso de nuevas tecnologías. Algunas de estas incluyen:

- Pruebas de testigos: Los testimonios de testigos que presenciaron la desaparición de una persona pueden ser recaudados mediante entrevistas y declaraciones y las mismas ser documentadas en plataformas electrónicas mucho más seguras ante la pérdida, mutilación o alteración que la documentación tradicional en papel.
- Pruebas de geolocalización: El uso de sistemas de geolocalización puede ayudar a rastrear la ubicación de una persona desaparecida y proporcionar información sobre su movimiento antes de su desaparición.

- Pruebas de comunicaciones: Los registros de comunicaciones, como llamadas telefónicas y mensajes de texto, pueden proporcionar información sobre la persona desaparecida y sus contactos previos a su desaparición.
- Pruebas de análisis de imágenes: El uso de tecnologías de análisis de imágenes, como el reconocimiento facial y la detección de objetos, puede ayudar a identificar a personas desaparecidas a partir de imágenes y videos.

En cuanto a la preservación de la cadena de custodia y la admisibilidad de las pruebas recopiladas mediante el uso de nuevas tecnologías, es importante mencionar que estas pruebas deben cumplir con los estándares legales y procedimientos adecuados para garantizar su fiabilidad y legalidad. Esto puede incluir la documentación detallada del proceso de recolección de pruebas, la identificación de las personas responsables de la recolección y el almacenamiento de las pruebas, y la verificación de la integridad de las pruebas. También es importante que se cumplan las leyes y regulaciones relativas a la protección de datos personales y privacidad en el uso de las nuevas tecnologías.

12. ¿Se pueden superar los obstáculos generados por el paso del tiempo en la identificación de los autores de una desaparición forzada mediante el uso de las nuevas tecnologías? ¿Si es así, cómo?

Si, algunas de las tecnologías y técnicas que pueden ser útiles incluyen:

- Análisis de ADN: El uso de técnicas de análisis de ADN puede permitir la identificación de personas desaparecidas incluso después de muchos años, lo cual incluye casos donde no existen restos óseos.
- Reconstrucción facial: La tecnología de reconstrucción facial puede utilizarse para generar una imagen de una persona desaparecida a partir de restos óseos o cualquier otra parte del cuerpo, y también puede ayudar a identificar a los responsables.
- Análisis de datos: El uso de herramientas de análisis de datos puede ayudar a identificar patrones y relaciones relevantes en los casos de desapariciones forzadas, incluso después de muchos años, esto puede ayudar a establecer relaciones entre los posibles sospechosos y las víctimas.
- Inteligencia Artificial: La inteligencia artificial puede ser utilizada para analizar grandes cantidades de información y ayudar en la identificación de sospechosos y víctimas de desapariciones forzadas, incluso en casos antiguos.
- Técnicas de interrogatorio y peritaje psicológico: Estas técnicas pueden ayudar a obtener información valiosa de testigos y sospechosos, incluso después de muchos años.

13. ¿Cuáles son los principales asuntos relacionados con el tema de "nuevas tecnologías y desapariciones forzadas" que deberían ser abordados en los hallazgos y recomendaciones incluidos en el estudio temático del Grupo de Trabajo?

Los principales asuntos a abordar podrían incluir:

- La eficacia de las nuevas tecnologías en la investigación de casos de desapariciones forzadas: Se deberían evaluar las diferentes tecnologías

disponibles y su capacidad para mejorar la eficacia de la investigación y el rastreo de personas desaparecidas.
- La protección de datos personales y la privacidad: Es importante abordar las preocupaciones sobre la protección de datos personales y la privacidad al utilizar nuevas tecnologías en la investigación de casos de desapariciones forzadas.
- La capacitación y los recursos necesarios: Se deberían evaluar las necesidades de capacitación y los recursos necesarios para que las entidades estatales puedan utilizar eficazmente las nuevas tecnologías en la investigación de casos de desapariciones forzadas.
- La accesibilidad y asequibilidad de las tecnologías: Es importante abordar las preocupaciones sobre el acceso a tecnologías costosas y su impacto en la capacidad de investigar casos de desapariciones forzadas.
- La regulación y el marco legal: Es importante evaluar la regulación y el marco legal existente en relación con el uso de nuevas tecnologías en la investigación de casos de desapariciones forzadas y considerar la necesidad de cambios y adaptaciones.
- La preservación de la cadena de custodia y la admisibilidad de las pruebas: Se deben evaluar las medidas necesarias para garantizar la legalidad y confiabilidad de las pruebas obtenidas mediante el uso de nuevas tecnologías.
- El trabajo en colaboración y la comunicación: Debe abordarse la importancia de la colaboración interinstitucional y la comunicación en la investigación de casos de desapariciones forzadas, incluyendo la colaboración entre las diferentes entidades estatales, ONGs y organizaciones internacionales, así como la comunicación entre las diferentes partes interesadas, incluyendo a las familias de las personas desaparecidas.
- La inclusión de la perspectiva de las víctimas: Es importante considerar la perspectiva y las necesidades de las víctimas y sus familias en la investigación de casos de desapariciones forzadas, y asegurar que se les brinde apoyo y asistencia apropiados.
- La implementación de las recomendaciones: Un aspecto muy importante es la implementación práctica de las recomendaciones del estudio temático, incluyendo la capacitación necesaria para llevar a cabo las recomendaciones.

14. ¿Existe alguna otra información que considere relevante para los propósitos del estudio temático?

Sí, hay alguna otra información que podría ser relevante para los propósitos del estudio temático:

- El impacto de las nuevas tecnologías en la prevención de desapariciones forzadas: Se podría evaluar cómo las nuevas tecnologías pueden utilizarse para prevenir desapariciones forzadas mediante la monitorización y el análisis de información para detectar y prevenir patrones de violencia.
- La coordinación inter-agencias: Se podría evaluar cómo las diferentes entidades estatales y agencias pueden coordinar sus esfuerzos para mejorar la eficacia de la investigación de casos de desapariciones forzadas mediante el uso de nuevas tecnologías.
- El uso de nuevas tecnologías en casos de desapariciones forzadas en contextos de crisis humanitarias: Se podría evaluar cómo las nuevas tecnologías pueden

utilizarse para investigar casos de desapariciones forzadas en contextos de crisis humanitarias, como conflictos armados, desastres naturales, y desplazamientos masivos de población.

- La colaboración con familias de desaparecidos y organizaciones no gubernamentales: Es importante considerar la colaboración con las familias de las personas desaparecidas y las organizaciones no gubernamentales para mejorar la eficacia de la investigación de casos de desapariciones forzadas. Esto podría incluir la posibilidad de trabajar con las familias para recopilar información valiosa y brindarles apoyo y asistencia apropiados, así como la colaboración con organizaciones no gubernamentales para compartir información y recursos.
- La evaluación continua y el monitoreo: Es importante considerar la necesidad de evaluar continuamente el impacto de las nuevas tecnologías en la investigación de casos de desapariciones forzadas y monitorear su eficacia para garantizar que se estén utilizando las mejores prácticas y tecnologías disponibles.
- La importancia de la formación continua y la actualización en tecnologías: Es importante considerar la importancia de la formación continua y la actualización en tecnologías para asegurar que las entidades estatales estén utilizando las mejores prácticas y las tecnologías más actuales en la investigación de casos de desapariciones forzadas.