Humanity In War

1 de junio de 2026

VERSIÓN PRELIMINAR PARA LA QUINTA CONSULTA CON LOS ESTADOS

Línea de trabajo 6 – PROCURAR QUE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES SE UTILICEN DE CONFORMIDAD CON EL DERECHO INTERNACIONAL HUMANITARIO DURANTE LOS CONFLICTOS ARMADOS

COLIDERADO POR Ghana, Luxemburgo, México, Suiza y el Comité Internacional de la Cruz Roja

Resumen

Las tecnologías de la información y la comunicación (TIC) se han vuelto esenciales para la vida de las personas en todas partes. En este mundo digitalizado y conectado, los servicios esenciales para la población civil, al igual que la capacidad de las personas para conectarse con sus seres queridos y perseguir el progreso económico, dependen de la integridad y la disponibilidad de las TIC. En las zonas afectadas por conflictos armados, las TIC confiables permiten que las personas civiles accedan a bienes

y servicios esenciales, que los gobiernos mantengan sus prestaciones, y que se desarrollen los servicios médicos y actividades humanitarias de apoyo como los que brinda el Movimiento Internacional de la Cruz Roja y de la Media Luna Roja. Si bien las capacidades en materia de TIC pueden darles a los bandos beligerantes la capacidad de alcanzar objetivos militares sin necesariamente causar daño, o causando menos daño a las personas civiles y a los bienes de carácter civil que con operaciones cinéticas, su uso en los conflictos armados contemporáneos también incluye actividades dañinas que afectan a las poblaciones, sus datos y su infraestructura, a veces de un lado al otro de las fronteras internacionales. Las desigualdades en materia de capacidades tecnológicas y resiliencia de la ciberseguridad pueden exacerbar esos riesgos, en particular afectando la posibilidad de los Estados y otros actores pertinentes de prevenir, mitigar y atender los daños causados por actividades relacionadas con las TIC en conflictos armados.

Esta línea de trabajo subrayó el imperativo de proteger a la población civil y preservar la dignidad humana en los conflictos armados de hoy y mañana. Para ello, es esencial defender y fortalecer el respeto del derecho internacional humanitario (DIH) en el uso de las TIC en contextos de conflicto armado a fin de proteger la infraestructura, las redes, las comunicaciones y los datos civiles ante actividades dañinas relacionadas con las TIC en conflictos armados.

Al hacer uso de las TIC, los Estados deben atenerse al derecho internacional, incluida la Carta de las Naciones Unidas, en particular la obligación de arreglar por medios pacíficos sus controversias internacionales y la prohibición de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas. Ninguna disposición del DIH puede interpretarse en el sentido de que legitime o autorice cualquier acto de agresión u otro uso de la fuerza incompatible con la Carta de las Naciones Unidas. La aplicación del DIH no legitima ni incentiva los conflictos armados.

Además, la línea de trabajo identificó buenas formas de acción y formuló recomendaciones prácticas, que se exponen más abajo, con los siguientes objetivos principales:

- proteger a la población civil y los datos y la infraestructura civiles contra las actividades dañinas relacionadas con las TIC;
- salvaguardar los servicios médicos y las actividades humanitarias ante las amenazas digitales, y hacer respetar la prohibición de la violencia sexual y del reclutamiento y uso de niñas, niños y adolescentes en hostilidades, en particular por medios virtuales;
- responder a la propagación de información que viola el DIH;
- minimizar el riesgo de que la población civil sufra daños a causa del uso militar de infraestructura civil de TIC, y evitar que las personas civiles que participan en actividades de TIC —desde hackers hasta empleados de empresas de tecnología— violen el DIH o se pongan en riesgo sin darse cuenta.

La línea de trabajo también subrayó la importancia de los siguientes elementos generales en el fortalecimiento de la protección que otorga el DIH en lo que respecta a las actividades relacionadas con las TIC:

- reconocer que, en las zonas afectadas por conflictos armados, las TIC confiables son vitales para la población civil, el gobierno y los actores humanitarios, y que las actividades relacionadas con ellas pueden generar costos humanos incluso sin causar daños físicos, lo que pone de relieve la necesidad de preservar la humanidad y la dignidad humana en la guerra;

- asumir el compromiso de promover y esclarecer la aplicación del DIH en las actividades relacionadas con las TIC, así como de adoptar todas las medidas necesarias, tanto individuales como colectivas, para mitigar los riesgos que afectan a la población civil y para que las actividades relacionadas con las TIC cumplan con las protecciones que otorga el DIH;
- continuar estudiando y debatiendo cómo se aplica el DIH a las actividades relacionadas con las TIC, sobre la base de las conversaciones de la línea de trabajo y este documento final, con miras a seguir generando e impulsando un consenso que preserve a las personas civiles de sufrir daños;
- fomentar la transparencia por medio de la difusión pública de perspectivas nacionales sobre la aplicación del derecho internacional, en particular el DIH, a las actividades relacionadas con las TIC, así como del intercambio de aprendizajes y buenas prácticas para mitigar los daños civiles;
- fortalecer las capacidades en el ámbito bilateral, regional y mundial, a fin de que los Estados estén mejor equipados para implementar y aplicar el DIH en las actividades relacionadas con las TIC.

Resultados

1. Protección de la población civil y de los datos y la infraestructura civiles contra los daños que pudieran surgir de actividades relacionadas con las TIC en contextos de conflicto armado

Los conflictos armados contemporáneos demuestran que las actividades relacionadas con las TIC pueden acarrear riesgos para la población civil, así como para los datos y la infraestructura civiles. Dichas actividades pueden afectar seriamente a la población civil y otras personas y bienes protegidos; por ejemplo, causando trastornos, incluso sin que ocurran daños físicos, en servicios esenciales —es decir, aquellos que son vitales para la subsistencia de la población civil, así como los sistemas interconectados de los que dependen las personas para satisfacer sus necesidades básicas—, entre ellos el suministro de electricidad, agua y saneamiento, la producción y distribución de alimentos, las telecomunicaciones, la atención de salud, la educación, los servicios humanitarios y de emergencia o los servicios financieros.

Cuando se llevan a cabo actividades relacionadas con las TIC en el contexto de un conflicto armado o vinculadas con él, se debe cumplir en todo momento con las disposiciones del DIH: entre otras, los principios de humanidad, necesidad militar, distinción, proporcionalidad y precaución.

Las operaciones de TIC de las que cabe razonablemente prever que tendrán un saldo de personas fallecidas o heridas, o que provocarán daños o destrucción de bienes, constituyen ataques en virtud del DIH. Eso incluye las operaciones de las que sea razonable suponer que dejarán sistemas de TIC inhabilitados y obligarán a realizar acciones para restaurar su funcionamiento. Ese tipo de operaciones de TIC deben realizarse de conformidad con todos los principios y las normas del DIH que rigen la conducción de las hostilidades, en particular la prohibición de cometer ataques contra personas civiles y bienes de carácter civil, ataques indiscriminados y ataques desproporcionados, así como el principio de precaución.

En un mundo cada vez más digitalizado, los datos son un elemento central para el funcionamiento de los servicios civiles esenciales y las actividades humanitarias. La forma en que se manejen los datos

durante los conflictos armados puede afectar la vida y la dignidad de las personas. Los datos médicos, biométricos, financieros y humanitarios, entre otros, son fundamentales para prestar servicios públicos y sociales. Eliminarlos, manipularlos, impedir el acceso a ellos o publicarlos sin autorización puede impedir el funcionamiento de servicios esenciales y exponer a las personas y comunidades a daños graves. Las actividades de recopilación de información en sí mismas no están prohibidas por el DIH, ni siquiera cuando implican acceder a datos.

Varios principios y normas del DIH confieren protección a las personas, los datos y la infraestructura civiles contra los peligros que acarrean las actividades relacionadas con las TIC en contextos de conflicto armado, a saber:

- los principios de que el derecho de las partes a elegir los métodos o medios de guerra no es limitado, y de que una parte en un conflicto armado solo puede recurrir a los métodos y medios de guerra que sean necesarios para debilitar a las fuerzas militares del enemigo;
- los principios y normas que rigen la conducción de las hostilidades, en particular los principios de distinción, proporcionalidad y precaución, y las prohibiciones relacionadas de cometer ataques contra personas civiles y bienes de carácter civil, ataques indiscriminados y ataques desproporcionados;
- la obligación de tomar precauciones constantemente para preservar a la población civil, las personas civiles y los bienes de carácter civil en la conducción de las operaciones militares;
- las normas que protegen la propiedad contra el pillaje, la confiscación y la destrucción.

Las siguientes medidas, que constituyen una combinación de legislación vigente y buenas prácticas, son especialmente importantes para la protección de la población civil y de la infraestructura y los datos civiles ante los daños que puedan acarrear las actividades relacionadas con las TIC en contextos de conflicto armado:

a) Formular y poner en práctica procedimientos rigurosos para que las operaciones de TIC respeten el DIH —en particular, que se verifique que los objetivos de los ataques correspondan a la categoría de objetivos militares y no gocen de protección especial—, así como para evaluar el riesgo de daño incidental para la población civil y evitarlo o, al menos, minimizarlo.

b) Apoyar las operaciones de TIC —incluidos los procedimientos de selección de objetivos— en toda la información razonablemente disponible, como datos e inteligencia confiables, que pueda obtenerse mediante una búsqueda activa en fuentes pertinentes, respaldadas por asesoramiento jurídico, conforme lo exige el DIH; y, en la mayor medida posible, recurrir a especialistas en ciberseguridad y otras áreas técnicas pertinentes en lo relativo a la estructura, la interconectividad y la dependencia civil de la infraestructura de TIC.

c) En los casos en que la infraestructura de TIC se clasifique como objetivo militar en virtud del DIH pero siga cumpliendo funciones civiles, tomar en cuenta todos los daños incidentales directos e indirectos que sea razonable prever para la población, los datos y la infraestructura civiles por la pérdida total o parcial de su uso civil, así como el consecuente impacto en los servicios civiles que presta o permite prestar, de conformidad con los principios y normas de proporcionalidad y precaución en la planificación y conducción de las hostilidades.

d) Al implementar la obligación de tomar todas las precauciones factibles en la elección de los métodos y medios de guerra, seleccionar aquellos de los que quepa esperar que causarán menos daños civiles incidentales, por ejemplo, evaluando rigurosamente si los que utilizan TIC u otros

métodos y medios no cinéticos reducirían el riesgo de daño civil en comparación con las alternativas cinéticas disponibles.

e) Aplicar limitaciones apropiadas de carácter geográfico, temporal y sistémico ("delimitación") en la conducción de las operaciones de TIC, para evitar o, al menos, minimizar el riesgo de daños incidentales para la población civil.

f) Hacer un seguimiento constante de las operaciones de TIC y disponer que sea posible modificarlas o concluirlas para prevenir daños civiles involuntarios o excesivos; siempre que sea posible, incorporar salvaguardas técnicas, como mecanismos de cancelación de emergencia o *kill switches*, que permitan detener, limitar o aislar las operaciones de TIC si existe el riesgo de que se propaguen más allá del objetivo previsto, en particular si pueden alcanzar redes o infraestructura civiles o de terceros Estados.

g) Tomar todas las medidas del caso para realizar las actividades relacionadas con TIC en las que se utiliza inteligencia artificial u otras tecnologías emergentes de manera compatible con el DIH y con las medidas expuestas más arriba.

2. Minimización del riesgo de daño a la población civil a raíz del uso militar de infraestructura civil de TIC en conflictos armados

Excepto en ciertas redes militares, el entorno de las TIC es predominantemente civil. Sin embargo, la interconexión entre las redes civiles y militares, así como el uso militar de la infraestructura civil de TIC, plantean desafíos específicos para su protección.

Cuando se usa infraestructura civil de TIC —por ejemplo, infraestructura que proveen las empresas de tecnología— con fines militares, no cualquier uso de ese tipo la convierte total ni parcialmente en objetivo militar en virtud del DIH. Así y todo, el uso militar puede elevar el riesgo de que dicha infraestructura sufra ataques y, por lo tanto, expone a sufrir daños incidentales a las personas civiles y a los bienes de carácter que se encuentren en sus inmediaciones, que tengan una conexión digital con ella o que la necesiten.

El DIH prohíbe los ataques contra bienes de carácter civil, lo que incluye la infraestructura civil de TIC. Aun así, el uso militar puede convertir dicha infraestructura o algunas de sus partes en objetivos militares, solo durante el lapso en el que cumplan los criterios que establece el DIH. Estas determinaciones requieren especial cuidado y una evaluación caso por caso.

Cuando se atacan esos objetivos militares, los Estados y las partes en conflictos armados deben respetar la prohibición de los ataques indiscriminados y desproporcionados, al igual que el principio de precaución, en particular cuando la población civil depende de esa infraestructura de TIC para la prestación de servicios esenciales. Se deben tomar todas las precauciones factibles para conducir los ataques de manera que únicamente se vean afectados los componentes o funciones de la infraestructura que se usen con fines militares, y para evitar o, en última instancia, minimizar los daños en aquellos que desempeñan funciones civiles.

Los Estados y las partes en conflictos armados deben tomar todas las precauciones posibles para proteger a las personas civiles y los bienes de carácter civil que estén bajo su control ante los peligros que representan las operaciones militares.

Además de las medidas expuestas en el Resultado 1, las siguientes medidas, que combinan legislación vigente y buenas prácticas, revisten especial importancia para minimizar el riesgo de daños a los que

queda expuesta la población civil como consecuencia del uso militar de la infraestructura civil de TIC en conflictos armados:

a) Asignar recursos técnicos y financieros suficientes, y adoptar medidas de planificación, diseño y configuración con antelación al conflicto armado y durante su desarrollo, con el fin de minimizar la exposición de las personas civiles y la infraestructura civil de TIC a las repercusiones de las actividades relacionadas con las TIC en conflictos armados.

b) En el mayor grado posible, separar física o técnicamente los componentes de la infraestructura de TIC utilizados con fines militares de aquellos que desempeñan funciones civiles; por ejemplo, mediante la segmentación de redes u otras medidas de configuración pertinentes. Eso incluye, en la medida de lo factible, segregar los datos que se utilizan con fines militares de los que satisfacen necesidades civiles, separando su almacenamiento y su gestión, o mediante controles de acceso, por ejemplo.

c) Fortalecer la resiliencia de la infraestructura y los servicios esenciales de TIC, en particular por medio de medidas de redundancia, planificación de contingencia y demás, a fin de reducir el riesgo de daños incidentales para la población civil.

3. Minimización de los riesgos emanados de la participación civil en actividades relacionadas con las TIC en contextos de conflicto armado en el territorio de un Estado o bajo su jurisdicción o control

En los conflictos armados de hoy, se ha vuelto más habitual la participación de personas civiles en actividades relacionadas con las TIC. En algunas situaciones, los Estados han tolerado, facilitado o alentado que las personas civiles lleven adelante actividades relacionadas con las TIC en contra del adversario, entre ellas actividades que pueden afectar a personas civiles y bienes de carácter civil.

Ese acercamiento a las hostilidades expone a las personas civiles al riesgo de sufrir daños. Muchos pueden no tener noción del peligro que entraña esa participación, de las consecuencias jurídicas que puede tener su conducta ni de las normas del DIH que deben cumplir.

Las personas civiles —desde los hackers hasta los empleados de empresas de tecnología— deben respetar el DIH y demás legislación aplicable al realizar actividades relacionadas con las TIC en el contexto de un conflicto armado o vinculadas con él.

De conformidad con el derecho internacional, los Estados y las partes en conflictos armados son responsables por las violaciones del DIH que cometan personas civiles, incluidos los hackers y empleados de empresas de tecnología, cuyas actividades relacionadas con las TIC en contextos de conflicto armado se puedan atribuir a dichos Estados o partes. Los Estados deben adoptar todas las medidas pertinentes para prevenir que las personas civiles cometan violaciones del DIH a través o con ayuda de actividades relacionadas con TIC, y hacer cesar dichas violaciones en el caso de que se produzcan. También deben ocuparse de difundir el DIH tanto como sea posible a fin de darlo a conocer a la población civil de su país. No deben alentar, ayudar ni asistir a las personas civiles para que violen el DIH, en particular por medio de actividades relacionadas con TIC.

Las personas civiles gozan de protección contra los ataques salvo si participan directamente en las hostilidades y mientras dure tal participación. En ciertas circunstancias limitadas, la participación de personas civiles en actividades relacionadas con las TIC puede constituir una participación directa en las hostilidades. A fin de evitar tomar como objetivo de forma errónea o arbitraria a las personas civiles, las partes en conflictos armados deben tomar todas las precauciones factibles para determinar si una

persona es civil y, llegado el caso, si está participando directamente en las hostilidades, por ejemplo, por medio de actividades relacionadas con TIC. En caso de duda, el DIH exige suponer que las personas gozan de protección frente a ataques.

No se debe permitir que los niños, niñas o adolescentes participen en las hostilidades durante un conflicto armado, lo que incluye las actividades relacionadas con las TIC.

Las siguientes medidas, que combinan legislación vigente y buenas prácticas, son especialmente importantes para minimizar los riesgos que pueda acarrear la participación civil en actividades relacionadas con TIC durante un conflicto armado:

a) Tomar medidas adecuadas para informar a la población civil que pueda tener participación en actividades relacionadas con las TIC en un contexto de conflicto armado y vinculadas con él sobre los riesgos jurídicos y prácticos de dicha participación. Esas medidas pueden consistir en difundir información sobre las normas del DIH por redes sociales, aplicaciones específicas, radio u otros medios de comunicación de masas, o formular modelos de códigos de conducta que respeten el DIH y pedir que las personas civiles que realizan actividades relacionadas con las TIC se atengan a ellos.

b) Evitar tanto como sea factible la actuación de personas civiles en operaciones de TIC que constituyan una participación directa en las hostilidades, para protegerlas contra los peligros que emanan de las operaciones militares. Cuando, a pesar de todo, se da esa participación, incorporar a dichas personas civiles en las fuerzas armadas en la medida de lo posible.

c) Tomar todas las medidas factibles para evitar que los niños participen en las hostilidades por medio de actividades relacionadas con las TIC, por ejemplo, por medio de programas educativos y de sensibilización orientados a niños y a cuidadores; adaptando la legislación y las políticas nacionales que prohíben reclutar y usar a niños, niñas y adolescentes de manera que abarquen los medios electrónicos de hacerlo, y haciéndolas cumplir; y considerando las restricciones de edad para el acceso a herramientas digitales cuyo uso podría constituir una participación directa en las hostilidades, si procede.

4. Protección de los productos y servicios civiles de TIC que brindan las empresas de tecnología durante los conflictos armados

Los productos y servicios de TIC que brindan las empresas de tecnología son de uso muy extendido entre la población civil, los gobiernos y las organizaciones humanitarias imparciales, en particular durante los conflictos armados. Por lo tanto, su alteración, degradación o uso indebido puede tener consecuencias humanitarias considerables. Esos productos y servicios de TIC, al igual que el personal civil que los brinda, gozan de protección en virtud del DIH.

Al mismo tiempo, las empresas de tecnología brindan cada vez más servicios de ciberseguridad y otros productos y servicios de TIC a partes en conflictos armados, como consecuencia de lo cual pueden perder la protección que confiere el DIH. En esas situaciones, las personas civiles y los bienes de carácter civil que dependen de esos productos y servicios también pueden quedar expuestos a sufrir daños.

Qué deben hacer las empresas de tecnología para mejorar la protección de los productos y servicios civiles de TIC que brindan durante un conflicto armado:

a) No perder de vista que brindar productos y servicios relacionados con las TIC a partes en conflictos armados acarrea riesgos de orden jurídico y práctico.

b) Conocer, evaluar y minimizar los riesgos de daño a los que se exponen las personas civiles y los bienes de carácter civil, ya sea porque se trata de su personal o de su propiedad, o a causa de una proximidad física, una conexión digital o una dependencia de la infraestructura o los servicios en cuestión. Eso implica separar física o técnicamente, en la medida de lo posible, los productos y servicios que se utilizan para operaciones militares de los que se emplean con fines civiles.

c) Disponer lo necesario para evitar que su personal adopte o facilite conductas que constituyan violaciones del DIH, o participe en ellas de cualquier otro modo, en particular por medio de la prestación de productos o servicios relacionados con las TIC a partes en un conflicto armado, y, si eso ocurre, tomar las medidas del caso.

5. Preservación de los servicios de salud, las actividades humanitarias y otras personas, bienes y actividades que gozan de protección específica ante los peligros que emanan de las actividades relacionadas con las TIC en contextos de conflicto armado

El sector de la salud y las organizaciones humanitarias imparciales son especialmente vulnerables a las actividades relacionadas con las TIC durante los conflictos armados. Puesto que los servicios médicos y humanitarios dependen cada vez más de sistemas interconectados y datos digitales, los trastornos en la infraestructura o los servicios de TIC pueden afectar directamente las actividades sanitarias que salvan vidas, comprometer datos sensibles, impedir el trabajo de las organizaciones humanitarias imparciales y su personal, y poner en riesgo la prestación de asistencia.

El personal, las unidades y los transportes sanitarios, así como el personal y los bienes humanitarios, se deben respetar y proteger en todo momento, de conformidad con el DIH, en particular contra los daños que puedan surgir de actividades relacionadas con las TIC. Cuando estas actividades se desarrollan en contextos de conflicto armado, se debe evitar que generen trastornos indebidos en el funcionamiento de los servicios médicos y las actividades humanitarias, lo que incluye sus datos, las TIC que utilizan y sus sistemas de comunicación.

La confidencialidad de los datos médicos y humanitarios se debe respetar en virtud del DIH. Esa protección es crucial para preservar la confianza en los servicios de salud y en la labor de las organizaciones humanitarias imparciales.

Las partes en un conflicto armado deben hacer todo lo posible, en función de las circunstancias imperantes y los recursos de los que disponen, para evitar que los servicios médicos y las actividades humanitarias sufran daños, entre otras causas, a raíz de actividades relacionadas con las TIC que sean obra de terceros como ciberdelincuentes y otros actores no estatales, y que no puedan atribuirse a una de las partes en el conflicto, de conformidad con el DIH y otras normas vigentes del derecho internacional.

Otros bienes y actividades a las que el DIH confiere protección específica, como los bienes indispensables para la supervivencia de la población civil, las obras e instalaciones que contienen fuerzas peligrosas, la propiedad cultural y la defensa civil, también pueden verse expuestos a graves riesgos emanados de actividades relacionadas con las TIC. Hay que respetar la protección específica de la que gozan, en particular cuando dichas actividades se realizan en contextos de conflicto armado. La protección abarca los datos y la infraestructura de TIC indispensable para el funcionamiento de dichos servicios, actividades y bienes.

Es posible usar actividades relacionadas con las TIC para cometer o facilitar actos de violencia sexual, o para el reclutamiento o uso de niños en las hostilidades. El DIH prohíbe la violencia sexual, así como el reclutamiento y uso de niños en hostilidades, también cuando dichos actos se cometen con el apoyo o a través de actividades relacionadas con las TIC.

Las siguientes medidas, que constituyen una combinación de legislación vigente y buenas prácticas, son particularmente importantes para preservar los servicios de salud, las actividades humanitarias y otras personas, bienes y actividades que gozan de protección específica ante los peligros que emanan de las actividades relacionadas con las TIC en contextos de conflicto armado:

a) Apoyar conversaciones e iniciativas para dar a conocer y visibilizar en el entorno de las TIC la protección específica que confiere el DIH a los servicios médicos y las actividades humanitarias, por ejemplo, mediante la creación de un "emblema digital", y seguir dialogando con el CICR sobre las vías jurídicas, técnicas y diplomáticas para su implementación.

b) Reafirmar explícitamente su compromiso de respetar y preservar los servicios médicos y las actividades humanitarias —en particular sus datos, TIC y sistemas de comunicación—, facilitar sus operaciones en el entorno de las TIC, y respetar la protección específica de la que gozan los bienes indispensables para la supervivencia de la población civil, entre ellos sus datos y la infraestructura de TIC imprescindible para su funcionamiento. Esos compromisos deben verse reflejados en la legislación, las políticas, la doctrina y la práctica nacionales.

c) Siempre que sea posible, apoyar y facilitar el diseño de medidas adecuadas de ciberseguridad y protección de datos para los prestadores de servicios de salud y las organizaciones humanitarias imparciales, y contribuir a mejorar su resiliencia ante las amenazas relacionadas con las TIC para sus sistemas y actividades.

d) Fortalecer los marcos jurídicos y de políticas nacionales que se ocupan de las conductas en línea que pueden constituir o facilitar violaciones del DIH, entre otras, aquellas relacionadas con la violencia sexual y el reclutamiento o uso de menores en conflictos armados, y disponer lo necesario para su implementación y coordinación eficaces entre las autoridades pertinentes. En particular, para prevenir el reclutamiento y la utilización ilícitos de niños, se deben emprender esfuerzos gubernamentales más amplios orientados a educar a niños y cuidadores sobre los riesgos asociados con esa participación.

e) Incorporar salvaguardas específicas en la doctrina militar, los procedimientos operativos estándar y las reglas de enfrentamiento para prevenir y hacer cesar las violaciones cometidas o facilitadas por medio de actividades relacionadas con las TIC, en particular la violencia sexual y el reclutamiento y uso de niños en las hostilidades. Por ejemplo, cuando resulta factible, se puede regular el uso de dispositivos personales de TIC en entornos operacionales a fin de restringir el intercambio de imágenes o información sensibles y prohibir el uso de TIC para reclutar o involucrar ilícitamente a menores en las hostilidades.

6. Responder a la propagación de información que viola el DIH

En los conflictos armados contemporáneos, es cada vez más habitual el uso de actividades relacionadas con las TIC para difundir información que puede violar el DIH. Si bien las operaciones de información forman parte de la guerra desde hace mucho tiempo y no son en sí mismas ilícitas, el uso de las TIC, en particular por medio de redes sociales o aplicaciones de mensajería, o en combinación con inteligencia

artificial y otras tecnologías emergentes, puede amplificar considerablemente la velocidad, la escala y el alcance de la información dañina.

Los Estados y partes en conflictos armados deben abstenerse de propagar información que entrañe una violación del DIH, en particular por medio del uso de TIC, y hacer todo lo posible para evitar que otros actores lo hagan. Eso incluye difundir información que incite o aliente a violar el DIH, que exponga a personas privadas de libertad a insultos o a la curiosidad del público, o cuyo propósito principal sea sembrar el terror entre la población civil. En ciertas circunstancias específicas, la difusión de información constituye o facilita actos de perfidia.

Los servicios médicos y la acción humanitaria deben estar protegidos contra las operaciones de desinformación realizadas con ayuda de TIC que obstruyen su labor en contextos de conflicto armado. Esos actos interfieren indebidamente y son incompatibles con la obligación de respetar y proteger al personal humanitario y de salud, así como sus actividades.

Las siguientes medidas, que combinan legislación vigente y buenas prácticas, son especialmente importantes para responder a la propagación de información que viola el DIH:

a) Tomar todas las medidas factibles para evaluar, prevenir y mitigar el riesgo de operaciones de información, incluidas aquellas en las que se utiliza inteligencia artificial u otras tecnologías emergentes, que ocasionen perjuicios a la población civil y otras personas protegidas; por ejemplo, que pongan en riesgo su seguridad, su dignidad o su acceso a los servicios esenciales.

b) Abstenerse de propagar información que deshumanice al adversario o difunda el odio hacia la población civil, en particular por medio de TIC, y disponer lo necesario para que no se produzca esa conducta entre sus fuerzas armadas, otras autoridades públicas ni personas que actúen en su nombre.

c) Cuando sea posible, apoyar a los prestadores de servicios de salud y a las organizaciones humanitarias imparciales para que desarrollen su capacidad de fortalecer la resiliencia contra la desinformación y otras actividades relacionadas con la información dañina: por ejemplo, facilitando la posibilidad de que reúnan, verifiquen y diseminen información veraz de conformidad con sus actividades médicas o humanitarias; mejorando su preparación y su planificación de contingencia ante la exposición a información dañina, y alentando la formulación de respuestas adecuadas al contexto para la información dañina que afecta a las personas civiles en sus zonas de actuación.

d) Trabajar con los actores pertinentes, en particular el sector de la tecnología, a fin de reducir el riesgo de que las plataformas en línea u otros servicios relacionados con las TIC se utilicen para incitar, propiciar o facilitar violaciones del DIH, o para ocasionar daños a la población civil y los bienes de carácter civil por cualquier otra vía. Ese trabajo puede consistir en formular marcos jurídicos y de políticas adecuados, así como en promover entre las empresas de tecnología la adopción de salvaguardas y prácticas diseñadas para detectar, evaluar y combatir la información dañina en situaciones de conflicto armado.

e) Buscar maneras de fortalecer la resiliencia ante las actividades relacionadas con información dañina, por ejemplo, contribuyendo a la disponibilidad de información confiable, protegiendo a los periodistas y a los medios de comunicación cuando así lo requieren el DIH y otras normas jurídicas aplicables, y fomentando la adopción de medidas de preparación que dejen mejor posicionada a la población civil para acceder a información fiable en contextos de conflicto armado.

f) Abstenerse de impedir el acceso de las personas civiles a internet u otros servicios de TIC, a menos que lo justifique una necesidad militar imperiosa, puesto que ese tipo de medidas pondría en riesgo a la población. Cuando se impongan esas restricciones, tomar medidas de mitigación a fin de minimizar los efectos adversos para la población civil en la mayor medida posible.

7. Medidas transversales para mejorar la implementación del DIH en las actividades relacionadas con las TIC

Las siguientes medidas transversales, que combinan legislación vigente y buenas prácticas, son especialmente importantes para mejorar la implementación del DIH en las actividades relacionadas con las TIC, también en tiempo de paz:

a) Difundir el DIH entre las fuerzas armadas y la población general, sobre todo entre aquellos que puedan participar en actividades relacionadas con las TIC, e incorporar los principios y normas del DIH, así como su aplicación a las actividades relacionadas con las TIC, en la legislación nacional, la doctrina militar, los procedimientos operativos estándar, las reglas de enfrentamiento, los códigos de conducta y la formación, según corresponda.

b) Poner asesores jurídicos calificados a disposición de las unidades y mandos militares responsables de las actividades relacionadas con las TIC, en particular durante la planificación y conducción de dichas operaciones.

c) Realizar exámenes jurídicos de las capacidades de las TIC que funcionan como nuevas armas, métodos o medios de guerra al estudiarlas, desarrollarlas, adquirirlas o adoptarlas, a fin de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el derecho internacional. Dichos exámenes se deben llevar a cabo, por ejemplo, mediante procedimientos rigurosos de prueba, evaluación, verificación y validación de dichas capacidades, a fin de conocer mejor su funcionamiento, su forma de propagarse y los efectos que pueden tener en los sistemas civiles.

d) Adoptar todas las medidas necesarias de orden legislativo, normativo y demás —incluso, cuando corresponda, sanciones penales— a fin de prevenir y hacer cesar las violaciones del DIH cometidas a través o con ayuda de actividades relacionadas con las TIC por personas o en territorios que se encuentran bajo su jurisdicción o control.

e) Tomar medidas adecuadas durante el diseño, desarrollo y utilización de capacidades de TIC para reducir el riesgo de que se difundan, adapten, rediseñen o usen indebidamente de maneras que puedan constituir violaciones del DIH o contribuir a ellas, en particular por medio de resguardos de ciberseguridad pertinentes como el cifrado, así como de medidas técnicas como la incorporación de mecanismos de cancelación de emergencia o *kill switches*, a fin de limitar su propagación o reutilización no autorizada.

f) Promover medidas de intercambio voluntario de información y generación de confianza diseñadas para reducir los riesgos a los que se expone la infraestructura civil de TIC, como el intercambio de buenas prácticas entre los Estados, el establecimiento de canales de comunicación y otros arreglos prácticos de reducción de riesgos, y, cuando corresponda, la notificación voluntaria de incidentes importantes relacionados con TIC que hayan causado daños civiles involuntarios, a fin de mejorar la comprensión colectiva y la mitigación de riesgos.

g) Promover la transparencia y el entendimiento común por medio de la formulación y la difusión pública de perspectivas nacionales sobre la aplicación del derecho internacional, en particular el DIH, a las actividades relacionadas con las TIC, por ejemplo en forma de posturas nacionales o compartidas, así como del intercambio de aprendizajes y buenas prácticas para mitigar los daños civiles.

h) Fortalecer las capacidades en el ámbito bilateral, regional y mundial, a fin de que los Estados estén mejor equipados para implementar y aplicar el DIH en lo que respecta a las actividades relacionadas con las TIC.

i) Fomentar la cooperación entre Estados, empresas de tecnología, organizaciones humanitarias imparciales y miembros de sociedad civil con el objeto de que las TIC se utilicen de maneras que mejoren la protección de las personas civiles; por ejemplo, mediante la formulación de disposiciones prácticas u orientaciones específicas para el contexto.

j) Alentar la cooperación entre las empresas de tecnología y las organizaciones humanitarias imparciales para mejorar la preparación y respuesta ante amenazas relacionadas con las TIC que afecten a personas y bienes protegidos; por ejemplo, mediante el intercambio de información y el apoyo en materia de ciberseguridad, sin dejar de respetar los principios humanitarios de neutralidad, imparcialidad e independencia.

k) Incorporar enfoques con sensibilidad etaria y de género, e inclusivos de las personas con discapacidad, en los marcos nacionales y la práctica operacional, a fin de fortalecer la implementación del DIH, en particular a la hora de detectar y atender los riesgos relacionados con las TIC.