Humanity In War

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

DOCUMENTO DE ANTECEDENTES*

* Este documento de antecedentes se redactó para la primera consulta con los Estados; en septiembre de 2025, se incorporaron correcciones y cambios.

INTRODUCCIÓN

El creciente uso de las tecnologías de la información y las comunicaciones (TIC) durante los conflictos armados plantea importantes cuestiones humanitarias y jurídicas. Si bien está ampliamente aceptado que el derecho internacional humanitario (DIH) impone límites al uso de las TIC en los conflictos armados, las especificidades del entorno de estas tecnologías dan lugar a interrogantes complejos en cuanto a su aplicación. Los Estados han reconocido la necesidad de seguir debatiendo estas cuestiones. La línea de trabajo sobre las TIC forma parte de un esfuerzo continuo por fomentar un entendimiento común.

I. EL USO DE LAS TIC EN LOS CONFLICTOS ARMADOS Y EL DIH: DEBATES MUNDIALES Y NUEVOS CONSENSOS

La aplicación del derecho internacional, incluido el DIH, a las actividades relacionadas con las tecnologías de la información y las comunicaciones ha sido objeto de debates multilaterales durante casi veinte años. En 2021, el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional señaló por consenso que "el derecho internacional humanitario solo se aplica en situaciones de conflicto armado. En este sentido, recuerda los principios jurídicos internacionales establecidos, incluidos, en su caso, los principios de humanidad, necesidad, proporcionalidad y distinción que se señalaron en el informe de 2015. El Grupo reconoce la necesidad de seguir estudiando cómo y cuándo se aplican estos principios al uso de las TIC por parte de los Estados y subraya que recordar estos principios no legitima ni fomenta en absoluto los conflictos"[1]. El Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) se hizo eco de esta conclusión en sus informes[2].

Hasta la fecha, y que nosotros sepamos, 35 Estados han publicado posiciones nacionales individuales sobre cómo se aplica el derecho internacional a las operaciones cibernéticas[3]. Además, dos organizaciones regionales, la Unión Africana y la Unión Europea, publicaron posiciones o interpretaciones comunes sobre la aplicación del derecho internacional al uso de las TIC, lo que supone un avance en la creación de un consenso regional y eleva a más de 100 el número de Estados que se pronuncian sobre este tema. Entre los nuevos entendimientos comunes figura la reafirmación de la aplicación de los principios y normas del DIH, entre ellos los de humanidad, necesidad, proporcionalidad y distinción, al uso de

[1] Informe del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, A/76/135, 2021, párr. 71(f). V. también la Resolución 76/19 de la Asamblea General de las Naciones Unidas, 2021, párrs. 2 y 3, aprobada por consenso, que acoge con satisfacción el informe final consensuado del Grupo de Expertos Gubernamentales y pide a los Estados miembros que se guíen por el informe en su uso de las TIC.

[2] V. el primer informe anual sobre los progresos realizados del Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, A/77/275, 2022, párr. 15(b)(ii); segundo informe anual sobre los progresos realizados, A/78/265, 2023, párr. 29(b)(ii); tercer informe anual sobre los progresos realizados, A/79/214, 2024, párr. 36(b)(ii); informe final preliminar, A/AC.292/2025/CRP.1, 2025, párr. 40(b)(ii).

[3] Todas las posiciones nacionales individuales y las posiciones comunes pueden consultarse en Cyber Law Toolkit, "Common and National Positions", en https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Common_and_national_positions.

las tecnologías de la información y las comunicaciones durante los conflictos armados. Un número cada vez mayor de Estados ha expresado también su opinión sobre la protección que otorga el DIH a las personas civiles, la infraestructura civil, los datos de carácter civil, el personal y las instalaciones médicas, y las actividades y el personal humanitarios contra las actividades maliciosas relacionadas con las TIC, entre otros.

Aprovechando este impulso, en octubre de 2024, la XXXIV Conferencia Internacional de la Cruz Roja y de la Media Luna Roja —que reunió a todos los Estados y a todos los componentes del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja (Movimiento)— aprobó la resolución "Protección de la población civil y de otras personas y bienes protegidos ante el posible costo humano de las actividades relacionadas con las tecnologías de la información y las comunicaciones durante conflictos armados" (resolución sobre las TIC). La resolución insta a los Estados y a las partes en conflictos armados a salvaguardar a la población civil y a otras personas y bienes protegidos en situaciones de conflicto armado, en particular contra los riesgos causados por las actividades maliciosas relacionadas con las TIC. También pide a los Estados y a las partes en conflictos armados que respeten las protecciones del DIH para la población civil, las infraestructuras civiles esenciales (incluidas las infraestructuras digitales críticas, como los cables submarinos y las redes de comunicaciones orbitales), el personal y las actividades médicas y humanitarias, y los bienes culturales, entre otras cosas, contra los riesgos derivados de las actividades de las TIC. Reitera la prohibición de alentar la comisión de actos violatorios del DIH y aborda cuestiones relativas a las personas civiles que realizan actividades relacionadas con las tecnologías de la información y las comunicaciones y a las empresas tecnológicas privadas que prestan servicios de TIC en el contexto de conflictos armados.

A pesar de los avances señalados, se ha reconocido que las especificidades del entorno de estas tecnologías plantean interrogantes sobre el modo en que los principios y las normas del DIH se aplican a las actividades relacionadas con las TIC, y que es necesario proseguir los debates[4].

Esta línea de trabajo responde a dicha necesidad y ofrece un espacio exclusivo para realizar intercambios específicos y en profundidad. A la luz del costo humano del uso de las TIC en los conflictos armados, el objetivo de la línea de trabajo es fomentar un entendimiento común de los límites que el DIH impone a las actividades relacionadas con estas tecnologías en los conflictos armados a fin de proteger de los daños a la población civil.

II. EL USO DE LAS TIC EN LOS CONFLICTOS ARMADOS DE HOY EN DÍA Y SU COSTO HUMANO

La rápida digitalización de las sociedades ha aportado importantes beneficios, lo que ha permitido mejorar las oportunidades sociales, económicas y de comunicación. En las zonas afectadas por conflictos, es esencial contar con TIC fiables para que la población civil pueda acceder a bienes y servicios esenciales, para que los Gobiernos presten servicios y para apoyar las actividades médicas y humanitarias, como las del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja.

[4] Informe del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, A/76/135, 2021, párr. 71(f), y XXXIV Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, Ginebra, 2024, Resolución 2, "Protección de la población civil y de otras personas y bienes protegidos ante el posible costo humano de las actividades relacionadas con las tecnologías de la información y las comunicaciones durante conflictos armados", párr. 19 del preámbulo.

Sin embargo, estas ventajas también conllevan riesgos, entre ellos los que supone el aumento del uso de las TIC por parte de Estados y actores no estatales en los conflictos armados. Varios Estados vienen desarrollando capacidades en materia de TIC con fines militares, con un despliegue y uso crecientes de estas tecnologías como medios o métodos de guerra. Si bien el desarrollo y el uso de las capacidades militares de las TIC pueden ofrecer a los beligerantes la posibilidad de alcanzar sus objetivos sin causar necesariamente daños directos a la población civil o daños físicos a las infraestructuras civiles, el riesgo que estas actividades suponen para las poblaciones e infraestructuras civiles sigue siendo motivo de gran preocupación. Mediante el uso de las capacidades militares de las TIC, los procesos controlados por sistemas informáticos pueden activarse, modificarse o manipularse de otro modo con el potencial de causar importantes efectos perjudiciales en la población civil.

El uso de las TIC dirigidas contra infraestructuras civiles esenciales —como instalaciones nucleares, redes eléctricas, sistemas de abastecimiento de agua y redes de telecomunicaciones— podrían tener "consecuencias humanitarias devastadoras" [5]. Las actividades relacionadas con las tecnologías de la información y las comunicaciones también pueden interrumpir los servicios de gobierno electrónico y las operaciones del sector privado, con costos sociales y económicos. Estos riesgos se ven agravados por la interconectividad que caracteriza al ciberespacio. Las actividades relacionadas con las TIC dirigidas a un sistema pueden repercutir en otros, independientemente de su ubicación.

El sector de la salud, junto con las organizaciones humanitarias, es especialmente vulnerable a las actividades relacionadas con las TIC en conflictos armados, que pueden afectar las operaciones médicas vitales, perjudicar el funcionamiento de las organizaciones humanitarias imparciales y su personal, y poner en peligro la prestación de asistencia esencial a quienes la necesitan. Por ejemplo, el Comité Internacional de la Cruz Roja (CICR) y otros componentes del Movimiento han sido objeto de ataques mediante actividades relacionadas con las TIC[6].

Además, la participación de la población civil en actividades militares por medio del uso de las TIC durante los conflictos armados se ha intensificado. Los Estados han tolerado, facilitado o alentado la participación de hackers y grupos de hackers civiles en actividades relacionadas con estas tecnologías, con lo que han atacado o afectado a la población civil y los bienes de carácter civil asociados con el adversario. También se ha alentado a personas civiles a informar sobre los movimientos de tropas enemigas, por ejemplo, a través de aplicaciones para teléfonos inteligentes. Las empresas privadas brindan cada vez más servicios de ciberseguridad u otros servicios digitales a las partes en conflictos armados. Si las personas civiles se acercan a las hostilidades, corren el riesgo de sufrir daños. Además, a menudo desconocen los riesgos que asumen, las consecuencias jurídicas de sus actividades o las normas del DIH que deben respetar.

Otra dimensión es el uso de las TIC para difundir información perjudicial durante los conflictos armados. Si bien las operaciones de información han formado parte de la guerra desde hace mucho tiempo y no son ilícitas en sí mismas, el uso de las TIC —especialmente en las redes sociales o cuando se combina con la inteligencia artificial y otras tecnologías emergentes— amplifica la velocidad y la magnitud de la difusión de información dañina, lo

[5] Grupo de trabajo de composición abierta sobre los Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, informe sustantivo final, A/AC.290/2021/CRP.2, 2021, párr. 18.

[6] La violación de datos de 2022 y los repetidos ataques de denegación de servicios distribuidos contra el sitio web del CICR ponen de relieve la necesidad de una protección de datos sólida para salvaguardar la información confidencial, garantizar la continuidad operacional y proteger el diálogo humanitario confidencial con las partes en conflicto. V. CICR, "Ciberataque contra el CICR: qué sabemos", en https://www.icrc.org/es/document/ciberataque-cicr-que-sabemos-hasta-ahora.

que incluye esfuerzos para incitar a la violencia, exponer a los detenidos a la curiosidad pública o socavar la confianza en las organizaciones humanitarias.

Los Estados han reconocido estos cambios y riesgos. El Grupo de trabajo de composición abierta 2021-2025 ha señalado que los Estados están desarrollando capacidades de TIC con fines militares, que cada vez es más probable que estas tecnologías se utilicen en conflictos, y que las TIC ya se han utilizado en conflictos armados en distintas regiones, lo que podría tener consecuencias humanitarias devastadoras para personas civiles y bienes de carácter civil, así como para las organizaciones internacionales y humanitarias[7]. La XXXIV Conferencia Internacional de la Cruz Roja y de la Media Luna Roja también ha destacado el daño que puede causar a la población civil el uso de las TIC por las partes en conflictos armados, en particular, si ese uso se dirige contra infraestructura y servicios civiles esenciales, o los afecta incidentalmente, y los posibles daños a organizaciones humanitarias imparciales, lo que dificulta el acceso de estas a las poblaciones perjudicadas[8].

III. EL USO DE LAS TIC EN LOS CONFLICTOS ARMADOS: ENCUADRAR LAS CUESTIONES JURÍDICAS Y HUMANITARIAS EN EL MARCO DEL DIH

Los tratados de DIH y el derecho consuetudinario vigentes protegen a la población civil y a los bienes de carácter civil contra los peligros derivados de las actividades relacionadas con las TIC durante conflictos armados. Como se reitera en la resolución sobre las TIC, "en situaciones de conflicto armado, las normas y los principios del DIH —incluidos el principio de distinción, la prohibición de ataques indiscriminados y desproporcionados, las obligaciones de preservar a la población civil, así como los bienes de carácter civil, en la conducción de las operaciones militares, y de adoptar todas las medidas de precaución posibles para evitar o, al menos, reducir a un mínimo los daños civiles incidentales, la prohibición de alentar o incitar la comisión de actos violatorios del DIH y la prohibición de cometer actos o formular amenazas de violencia cuya finalidad principal sea sembrar terror en la población civil— sirven para proteger las poblaciones civiles y a otras personas y bienes protegidos, incluso contra los riesgos que entrañan las actividades relacionadas con las TIC"[9].

Con base en lo anterior, se propone un debate más profundo sobre las siguientes cuestiones jurídicas fundamentales en relación con las preocupaciones humanitarias más acuciantes.

[7] Grupo de Trabajo de composición abierta sobre seguridad y utilización de las tecnologías de la información y las comunicaciones, informe final preliminar, A/AC.292/2025/CRP.1, 2025, párrs. 15, 16 y 21.
[8] Resolución sobre las TIC, párrs. 7 y 14 del preámbulo.
[9] Resolución sobre las TIC, párr. 4.

I. PROTECCIÓN DE LAS POBLACIONES CIVIL Y DE OTRAS PERSONAS Y BIENES PROTEGIDOS ANTE LOS PELIGROS DERIVADOS DE LAS ACTIVIDADES RELACIONADAS CON LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DURANTE CONFLICTOS ARMADOS

Protección de la población civil de los efectos de las operaciones relacionadas con las TIC durante conflictos armados y el concepto de ataque en el DIH

Las operaciones relacionadas con las TIC pueden inutilizar o dañar físicamente instalaciones industriales, redes de comunicación y otros elementos de la infraestructura esencial de un Estado. Dichas operaciones también pueden causar daños directa o indirectamente, y provocar lesiones o la muerte de personas civiles, incluso por interrumpir el funcionamiento de los servicios esenciales. Estos riesgos se ven agravados por la interconectividad del ciberespacio. Si bien se ha prestado especial atención a las operaciones relacionadas con las TIC que provocan daños físicos, los usos recientes de estas tecnologías, por ejemplo, en conflictos armados, han demostrado que, incluso en ausencia de daños físicos, pueden alterar gravemente la infraestructura civil e interrumpir la prestación de servicios esenciales. De hecho, esto constituye uno de los riesgos más importantes de las TIC para la población civil durante conflictos armados.

El objetivo de las normas del DIH que rigen la conducción de las hostilidades es garantizar el respeto y la protección de la población civil y de los bienes de carácter civil[10]. La mayoría de las reglas derivadas de los principios y normas que rigen la conducción de las hostilidades, en particular la distinción, la proporcionalidad y las precauciones —que brindan protección general a la población civil y a los bienes de carácter civil—, se aplican únicamente a las operaciones o actividades que se califican como "ataques", según la definición del DIH, es decir, "actos de violencia contra el adversario, sean ofensivos o defensivos"[11]. Por lo tanto, la interpretación del concepto de "ataque" en relación con el uso de las tecnologías de la información y las comunicaciones durante conflictos armados, en particular en el caso de las operaciones relacionadas con las TIC que inhabilitan bienes de carácter civil sin causar daños físicos, es esencial, ya que esto determina si estas normas se aplican y, por consiguiente, si la población civil y otras personas y bienes protegidos están protegidos contra los peligros derivados de dichas operaciones.

Se sabe que el concepto de violencia en la definición de "ataque" del DIH puede referirse tanto a los medios empleados como a las consecuencias o efectos producidos. Una operación que causa efectos violentos se considera un ataque, incluso si los medios utilizados no son violentos en sí mismos[12].

También se acepta ampliamente que una operación de TIC que se prevé que cause la muerte o lesiones a una persona, o daños o destrucción a un bien, constituye un ataque según el DIH[13]. Se entiende comúnmente que esto incluye el daño debido a los efectos directos e

---

[10] Protocolo adicional I del 8 de junio de 1977, artículo 48 y títulos de la parte IV y la sección I.

[11] Protocolo adicional I, artículo 49(1). Existen algunas normas del DIH que se aplican a todas las operaciones militares, entre ellas, las realizadas mediante actividades relacionadas con las TIC. V., por ejemplo, el Protocolo adicional I, artículos 48, 51(1) y 57(1).

[12] Y. Sandoz, C. Swinarski y B. Zimmermann (eds.), Commentary *on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, CICR, Geneva/Martinus Nijhoff, Leiden, 1987. Versión española: Comentario del Protocolo del 8 de junio de 1977 adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I), CICR, Plaza y Janés Editores, Bogotá, 1998, tomo I (en adelante, CICR, Comentario del Protocolo adicional), párr. 1881, relativo al artículo 49(1) del Protocolo adicional I, establece que "existe un ataque cada vez que una persona está directamente puesta en peligro por una mina colocada", lo que es una interpretación coherente con el enfoque basado en las consecuencias. Otro ejemplo generalmente aceptado es que el uso de un agente químico o biológico constituiría un ataque debido a sus efectos violentos, incluso si los medios para distribuir dichos agentes no son violentos.

[13] CICR, "El derecho internacional humanitario y los retos de los conflictos armados contemporáneos", 2015, pp. 41-42.

indirectos (o residuales) previsibles de una operación; por ejemplo, la muerte de pacientes en unidades de cuidados intensivos causada por una operación de TIC contra una red eléctrica que provoca el corte del suministro eléctrico de un hospital[14].

Más allá de eso, es necesario que los Estados sigan debatiendo qué normas del DIH limitan las operaciones relacionadas con las TIC que afectan la funcionalidad de los sistemas de TIC sin necesariamente provocar daños físicos o la destrucción de un objeto, ni lesiones o la muerte a una persona, y si se califican como "ataques" según el DIH.

Desde una perspectiva de la guerra contemporánea, reconocer como ataque en el DIH una operación de TIC que inhabilita un bien sin causar daño físico es fundamental para la protección de la población civil y los bienes de carácter civil contra las actividades relacionadas con las TIC durante conflictos armados. Una interpretación restrictiva del concepto de ataque que excluya ciertas actividades relacionadas con las TIC de la protección que ofrecen las normas clave del DIH sobre la conducción de las hostilidades sería difícil de conciliar con el objeto y fin de esta rama del derecho y con la necesidad de garantizar que su marco de protección siga siendo eficaz, a la luz de la evolución de los medios y métodos de guerra. En este sentido, es esencial que los Estados lleguen a un entendimiento común a fin de proteger a la población civil y los bienes de carácter civil contra los efectos del uso nocivo de las TIC durante conflictos armados.

Datos civiles y la noción de bienes de carácter civil según el DIH

Los datos civiles —datos médicos, biométricos, de seguridad social, registros impositivos, cuentas bancarias, datos humanitarios, expedientes de clientes de empresas o listas y registros de elecciones— son un componente esencial de las sociedades digitalizadas. Esos datos son imprescindibles para el funcionamiento de la mayoría de los aspectos de la vida civil, a nivel individual o social. Preocupa cada vez más la protección de esos datos. La eliminación o la alteración de los datos de personas civiles rápidamente pueden dejar a los servicios gubernamentales y a las empresas privadas en un estado de paralización, y pueden causar más daño a la población civil que la destrucción de determinados bienes físicos. Asimismo, el robo o la filtración de los datos de personas civiles puede exponer a las personas y comunidades a graves riesgos de daño.

Con respecto a los datos pertenecientes a ciertas categorías de personas y bienes que gozan de protección específica en el DIH, las normas de protección son extensivas. Por ejemplo, la obligación de respetar y proteger al personal, las unidades y los transportes sanitarios, el personal y los bienes humanitarios, y los bienes indispensables para la supervivencia de la población civil[15].

Sin embargo, más allá de eso, es importante entender mejor en qué medida los datos de personas civiles están protegidos por las normas actuales del DIH[16], en particular si los datos constituyen bienes según los define el DIH, en cuyo caso las operaciones relacionadas con las TIC contra los datos (como causar daños o eliminarlos) se regirían, en gran medida, por los principios de distinción, proporcionalidad y precaución.

---

[14] CICR, Documento de posición sobre el derecho internacional humanitario y ciberoperaciones durante conflictos armados, , 2019, p. 7. V. un resumen de las posiciones de los Estados en Cyber Law Toolkit, "Attack (International Humanitarian Law)", en https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law).

[15] V. la próxima sección de este documento, "Personas y bienes que gozan de protección específica en virtud del derecho internacional humanitario".

[16] Entre ellas se incluyen los principios y normas del DIH sobre la conducción de hostilidades. Otras normas pertinentes pueden ser la protección de los bienes culturales, la protección de bienes contra confiscación y destrucción, y la prohibición del pillaje.

A este respecto, algunos Estados han adoptado la postura de que la protección de los bienes de carácter civil se extiende a todo tipo de datos de carácter civil; algunos parecen diferenciar entre "datos de contenido" y otros datos; mientras que otros han considerado que, en general, los datos digitales no pueden considerarse bienes en el marco del DIH[17].

Es necesario seguir debatiendo entre los Estados para fomentar un entendimiento común sobre este tema crucial. Desde el punto de vista humanitario, la afirmación de que una operación concebida para eliminar o adulterar esos datos de carácter civil, o de la que quepa prever que lo haga, no estaría prohibido por el DIH en un mundo que depende de los datos como el de hoy en día parece difícil de conciliar con el objeto y fin de esta rama del derecho. Lógicamente, el reemplazo de archivos y documentos en papel por datos digitales no debe disminuir la protección que el DIH confiere a la información almacenada en los datos.

Protección específica de personas, bienes y actividades en virtud del DIH

Algunas normas del DIH otorgan protecciones específicas a ciertas categorías de personas, bienes y actividades, más allá de la prohibición de ataques, incluso en lo que respecta a las actividades relacionadas con las TIC.

Por ejemplo, los beligerantes deben respetar y proteger al personal y las instalaciones sanitarias en todo momento[18], lo que incluye el requisito de no interferir indebidamente en el funcionamiento de los servicios médicos y adoptar las medidas viables para protegerlos de daños o interferencias de particulares no atribuibles a las partes en un conflicto armado[19]. Asimismo, se debe respetar y proteger al personal de humanitario y los bienes que se utilizan en las operaciones humanitarias[20], y las partes en conflictos armados deben permitir y facilitar las actividades humanitarias imparciales durante conflictos armados, a reserva de su derecho de control[21]. Tanto en el caso de los servicios médicos como del personal y los bienes humanitarios, la protección específica se extiende a las comunicaciones y los datos[22].

Para reforzar la protección de los servicios médicos y las actividades humanitarias contra los riesgos relacionados con las TIC, los futuros debates podrían centrarse en cómo hacer efectiva dicha protección. Una forma es la iniciativa emprendida por el CICR para desarrollar un emblema digital, esto es, un medio digital de identificación de la infraestructura y los datos de las organizaciones y las entidades que tienen derecho a desplegar los emblemas distintivos reconocidos en el DIH[23]. La resolución sobre las TIC, tomando nota de la labor en curso del CICR en consulta con los Estados y los componentes del Movimiento, alienta a que

---

[17] V. un resumen de las posiciones de los Estados en Cyber Law Toolkit, "Data as a military objective", en https://cyberlaw.ccdcoe.org/wiki/Military_objectives#Qualification_of_data_as_a_military_objective_under_IHL.

[18] V., por ejemplo, Primer Convenio de Ginebra del 12 de agosto de 1949, artículo 19; Segundo Convenio de Ginebra del 12 de agosto de 1949, artículo 12; Cuarto Convenio de Ginebra del 12 de agosto de 1949, artículo 18; Protocolo adicional I, artículo 12; Protocolo adicional II del 8 de junio de 1977, artículo 11; CICR, Estudio sobre el derecho internacional humanitario consuetudinario, en https://ihl-databases.icrc.org/en/customary-ihl/rules (en adelante, Estudio del CICR sobre DIH consuetudinario), normas 25, 28 y 29.

[19] CICR, Comentario del Protocolo adicional, párr. 517, relativo al artículo 12 del Protocolo adicional I, y CICR, Comentario del Primer Convenio de Ginebra: Convenio de Ginebra (I) para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña, primera edición en español, CICR, Ginebra/Cambridge University Press, Cambridge, 2021 (en adelante, CICR, Comentario del Primer Convenio de Ginebra, 2021), párr. 1799, relativo al artículo 19.

[20] Protocolo adicional I, artículos 70(4) y 71(2); Estudio del CICR sobre DIH consuetudinario, normas 31 y 32.

[21] V. Cuarto Convenio de Ginebra, artículo 23; Protocolo adicional I, artículo 70(2); Protocolo adicional II, artículo 18(2); Estudio del CICR sobre DIH consuetudinario, norma 55.

[22] CICR, Comentario del Primer Convenio de Ginebra, 2021, párr. 1804, relativo al artículo 19.

[23] El proyecto de emblema digital es una iniciativa independiente encabezado por el CICR en consulta y colaboración con los Estados y los componentes del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja. El debate de esta línea de trabajo no se centrará en dicho proyecto.

se sigan realizando trabajos y consultas, entre otras cosas, para estudiar posibles vías jurídicas y diplomáticas para el posible uso de un emblema digital[24].

Además, las actividades de TIC que destruyen, sustraen o inutilizan bienes indispensables para la supervivencia de la población civil, como las instalaciones de agua potable y las obras de riego, se incluyen en el ámbito de la protección especial conferida en virtud del DIH, independientemente de si se califican como "ataques"[25]. Esta protección especial se extiende a la infraestructura de TIC que es, en sí misma, "indispensable" para el funcionamiento de dichos bienes. Es necesario seguir debatiendo las medidas para hacer efectiva dichas protecciones.

Por último, las normas del DIH prohíben la violencia sexual y otorgan protecciones específicas a ciertas categorías de personas, entre ellas, las mujeres, las personas mayores, las personas con discapacidad y los niños (por ejemplo, contra su reclutamiento ilícito o su uso en las hostilidades)[26]. Es necesario seguir debatiendo, entre otras cuestiones, las medidas prácticas para garantizar el cumplimiento de estas normas, también cuando intervienen las TIC.

II. PROTECCIÓN DE LAS POBLACIONES CIVILES Y OTRAS PERSONAS PROTEGIDAS ANTE LA DIFUSIÓN DE INFORMACIÓN QUE INFRINGE LAS NORMAS DEL DIH DURANTE CONFLICTOS ARMADOS

Los Estados y los grupos armados no estatales están difundiendo información digital con diversos fines, por ejemplo, al llevar a cabo operaciones psicológicas o de información. Algunas operaciones tienen por objeto reducir el riesgo de daños a las personas durante conflictos armados, por ejemplo, dando a la población civil aviso de un ataque con la debida antelación o ayudándolos a ponerse a salvo. Otras tienen por objeto causar confusión o daño, engañar al adversario o apoyar los objetivos militares o políticos de una de las partes en el conflicto. En los conflictos armados actuales, las actividades relacionadas con las TIC se utilizan para difundir información en violación del DIH. La información difundida mediante actividades relacionadas con estas tecnologías puede contribuir a la violencia o fomentarla, provocar daños psicológicos duraderos, dificultar el acceso a servicios esenciales e impedir las actividades de las organizaciones humanitarias, lo que puede debilitar la confianza en estas instituciones.

El DIH contiene varias normas específicas que imponen límites a la difusión de información, por ejemplo, a través de medios digitales, en particular las siguientes:

- Los funcionarios civiles y militares de una parte en un conflicto armado no deben alentar las violaciones del DIH, norma que contempla la actividad en plataformas digitales[27]. La resolución sobre las TIC reafirma también la prohibición de alentar la comisión de actos violatorios del DIH a través de medios digitales[28].

[24] Resolución sobre las TIC, párr. 15 del preámbulo y párr. dispositivo 12.
[25] Entre los ejemplos de estos bienes se incluyen "los artículos alimenticios y las zonas agrícolas que los producen, las cosechas, el ganado, las instalaciones y reservas de agua potable y las obras de riego". Protocolo adicional I, artículo 54(2); Protocolo adicional II, artículo 14; Estudio del CICR sobre DIH consuetudinario, norma 54. V. también CICR, *El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos*, 2024, pp. 46-47.
[26] Cuarto Convenio de Ginebra, artículo 27(2); Protocolo adicional I, artículos 76(1) y 77(1) y (2): Protocolo adicional II, artículo 4(3)(c); Estudio del CICR sobre DIH consuetudinario, normas 134 a 138.
[27] Cuarto Convenio de Ginebra, artículo 1 común; Estudio del CICR sobre DIH consuetudinario, norma 139.
[28] Resolución sobre las TIC, párr. 4.

- Los prisioneros de guerra y otras personas protegidas en virtud del DIH deben ser protegidos contra la curiosidad pública[29]. El hecho de que las autoridades compartan públicamente datos, imágenes y videos de prisioneros de guerra y otras personas privadas de libertad, salvo excepciones limitadas, constituiría una infracción de esta norma, y los Estados también deben protegerlos contra la publicación por parte de entidades privadas[30].
- El DIH prohíbe las amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil[31].
- La divulgación de información falsa por las partes en un conflicto armado con el fin de obstaculizar la labor médica o humanitaria es incompatible con las obligaciones de respetar y proteger al personal médico y humanitario y sus actividades[32].
- La difusión de información con el fin de reclutar niños, o propaganda dirigida a que se alisten personas protegidas en territorios ocupados, en las fuerzas armadas es ilícita[33].

Habida cuenta de los riesgos de daños para la población civil y otras personas protegidas en virtud del DIH mencionados anteriormente, es necesario seguir debatiendo para establecer un entendimiento común sobre cómo se aplica esta rama del derecho a la divulgación de información, a fin de garantizar la protección efectiva de todas las personas y objetos protegidos en virtud del DIH.

III. EL RIESGO QUE SUPONE EL USO DE INFRAESTRUCTURA DE TIC DE CARÁCTER CIVIL CON FINES MILITARES Y LA PARTICIPACIÓN DE PERSONAS CIVILES EN ACTIVIDADES RELACIONADAS CON LAS TIC DURANTE CONFLICTOS ARMADOS

El uso de infraestructura de TIC de carácter civil con fines militares y su repercusión en la protección que otorga el DIH

Salvo por determinadas redes militares específicas, el ciberespacio tiene carácter predominantemente civil. Sin embargo, la interconexión de las redes civiles y militares y el uso de infraestructuras civiles de TIC por parte de los ejércitos plantean dificultades concretas para su protección.

Si cierta infraestructura civil de TIC —por ejemplo, infraestructura provista por empresas tecnológicas— se usa con fines militares (en cuyo caso dicha infraestructura se denomina en ocasiones de "doble uso"), existe el riesgo de que pase a constituir un objetivo militar en el marco del DIH y pierda su protección frente a ataques[34]. En estos casos, las personas y bienes de carácter civil que están físicamente cerca de dicha infraestructura, que mantienen

[29] V, por ejemplo, Tercer Convenio de Ginebra del 12 de agosto de 1949, artículo 13, y Cuarto Convenio de Ginebra, artículo 27.
[30] Para un análisis más exhaustivo de esta cuestión, v., por ejemplo, CICR, *Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War, 2nd ed.*, CICR, Ginebra, 2020 (en adelante, CICR, Commentary on the Third Geneva Convention, 2020), párrs. 1623-1632.
[31] Protocolo adicional I, artículo 51(2); Protocolo adicional II, artículo 13(2); Estudio del CICR sobre DIH consuetudinario, norma 2.
[32] Esto, por supuesto, es diferente de la crítica o la expresión de ira por parte de las autoridades o los beneficiarios dirigida a los servicios médicos o las organizaciones humanitarias, que, a primera vista, no constituye un acto ilícito.
[33] En relación con el reclutamiento de niños, v. el Estudio del CICR sobre DIH consuetudinario, norma 136, y las obligaciones en virtud del Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la participación de los niños en los conflictos armados, del 25 de mayo de 2000. Por lo que respecta a las personas protegidas en situaciones de ocupación, v. el Cuarto Convenio de Ginebra, artículo 51.
[34] Los objetos de doble uso pueden convertirse en objetivos militares si, en las circunstancias del momento, se ajustan a la definición que figura en el artículo 52(2) del Protocolo adicional I: "En lo que respecta a los bienes, los objetivos militares se limitan a aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida".

con ella una conexión digital o que dependen de ella corren el riesgo de sufrir daños incidentales.

Sin embargo, no todo uso militar convierte un bien de carácter civil en un objetivo militar en el marco del DIH; esto solamente ocurre cuando el uso cumple los criterios de un objetivo militar según la definición del DIH. Además, incluso si un beligerante considera que una persona civil o un bien de carácter civil ha perdido protección debido a su participación en operaciones relacionadas con las TIC, cualquier ataque sigue estando sujeto a las prohibiciones de ataques indiscriminados y desproporcionados y a la obligación de tomar todas las precauciones que sean factibles. Además, ciertos bienes que gozan de protección específica no deben ser objeto de ataques o pueden estar sujetos a limitaciones más estrictas, incluso si cumplen la definición de objetivo militar.

Para proteger a la población civil y los servicios civiles esenciales que dependen de la infraestructura de TIC, es necesario proseguir los debates para determinar cuándo el uso militar de una infraestructura de TIC predominantemente civil la convierte en un objetivo militar, e identificar e implementar otras medidas de protección viables. Por ejemplo, el CICR ha pedido a los Estados que, siempre que sea posible, procuren separar físicamente o distinguir por medios técnicos la infraestructura de TIC o sus partes que se usen con fines militares de la que se usen con fines civiles[35]. También es esencial garantizar que se respete cualquier protección específica otorgada en virtud del DIH.

La participación de personas civiles en actividades relacionadas con las TIC durante conflictos armados

En los conflictos armados actuales, varias tendencias plantean riesgos para la población civil: los hackers civiles atacan cada vez más bienes de carácter civil en operaciones relacionadas con las TIC; las partes en conflictos armados alientan a las personas civiles a recopilar información de importancia militar por medios digitales, exponiéndolas a ataques; y las empresas tecnológicas civiles que prestan servicios e infraestructuras de TIC a las fuerzas armadas corren el riesgo de perder su protección jurídica.

El DIH se erige sobre el principio cardinal de distinción. La creciente participación civil en las operaciones relacionadas con las TIC y el uso militar de infraestructura civil de TIC están erosionando la protección que este principio fundacional debería significar para las personas civiles, incluida la protección contra su identificación errónea como objetivos legítimos.

Las personas y los grupos, por ejemplo, los hackers y los empleados de empresas tecnológicas, que llevan a cabo actividades relacionadas con las TIC en el contexto de conflictos armados deben respetar los límites que el DIH establece para dichas actividades[36] y ser conscientes de los riesgos que entrañan. En casos excepcionales, la participación civil en actividades relacionadas con las TIC puede constituir una "participación directa en las hostilidades", de modo que una persona civil pierda su protección contra ataques durante el

[35] Un ejemplo sería, al decidir si se almacenan datos militares en una nube comercial sin distinción, un segmento de una nube comercial o infraestructura digital militar, los encargados de la planificación y las operaciones militares no deben utilizar la nube comercial sin distinción. V. CICR, *El derecho internacional humanitario y los retos de los conflictos armados contemporáneos*, 2024, pp. 53-54.

[36] En lo que respecta a los hackers civiles que realizan actividades relacionadas con conflictos armados, esos límites se resumen en un artículo del CICR ("Eight rules for 'civilian hackers' during war, and four obligations for states to restrain them"), en el que se señalan ocho normas para estos hackers y cuatro obligaciones de los Estados para refrenarlos, en https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them. En relación con la pertinencia del DIH para las empresas privadas, v., más en general, CICR, *Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law*, 2024.

período en que así sea. Sin embargo, en caso de duda, el DIH exige que las personas se consideren civiles y, por lo tanto, protegidas[37].

La responsabilidad de los Estados en la difusión del DIH y en la prevención y cese de violaciones de este marco jurídico

Por lo que respecta a la participación de personas civiles en actividades relacionadas con las TIC durante un conflicto armado, cabe señalar que los Estados se han comprometido a respetar y hacer respetar el DIH. En el caso de que hackers civiles, empresas privadas u otras personas o entidades privadas actúen bajo la instrucción, dirección o control de un Estado, dicho Estado es jurídicamente responsable a nivel internacional de cualquier conducta de esas personas que sea incompatible con las obligaciones jurídicas internacionales del Estado, incluido el DIH[38].

Aunque la conducta de las personas civiles no sea atribuible a una parte en un conflicto armado, los Estados tienen la obligación de hacer respetar el DIH. Como mínimo, las partes en un conflicto armado no deben alentar a las personas civiles que participan en actividades relacionadas con las TIC ni prestarles ayuda o asistencia en la comisión de actos violatorios del DIH[39], por ejemplo, alentándolas a dirigir operaciones relacionadas con las TIC contra bienes civiles. Además, los Estados deben difundir el conocimiento del derecho internacional humanitario, así como prevenir y eliminar las violaciones del DIH, e investigar y procesar los crímenes de guerra, incluidos los cometidos por la población civil[40].

[37] Protocolo adicional I, artículo 50(1). Si existe el riesgo de que los niños se vean arrastrados a las hostilidades por medio de las actividades de las TIC y se considere que participan directamente en las hostilidades, los beligerantes tienen la obligación adicional de impedir la participación de niños menores de 15 o 18 años, en función del marco jurídico aplicable.
[38] Según el derecho internacional público, un Estado es responsable de la conducta de personas, grupos o entidades privadas, como los hackers o grupos de hackers civiles, si están "facultados por el derecho de ese Estado para ejercer elementos de la autoridad gubernamental" o "actúan de hecho siguiendo las instrucciones de dicho Estado o bajo su dirección o control". V. Comisión de Derecho Internacional, *Responsibility of States for Internationally Wrongful Acts*, 2001, artículos 5 y 8.
[39] CICR, Commentary on the Third Geneva Convention, 2020, párr. 191, relativo al artículo 1.
[40] CICR, Commentary on the Third Geneva Convention, 2020, párr. 183, relativo al artículo 1.