INTERNATIONAL REVIEW of the Red Cross

EDITORIAL. EL PAPEL DE LAS TECNOLOGÍAS DIGITALES EN EL DERECHO, LA ACCIÓN Y LAS POLÍTICAS HUMANITARIAS: TRAZAR UN CAMINO PARA EL FUTURO

Saman Rejali y Yannick Heiniger*

¿Por qué se ha seleccionado la cuestión de "Las tecnologías digitales y la guerra" como eje temático de un número entero de la *International Review of the Red Cross*? Quienes contribuyen a esta edición destacan dos motivos dominantes.

En primer lugar, la digitalización es un tema prioritario para las organizaciones humanitarias como el Comité Internacional de la Cruz Roja (CICR)[1], dado que este fenómeno está cambiando con rapidez la forma en que se llevan a cabo las operaciones y actividades de asistencia humanitarias e incide en el modo en que el sector humanitario presta servicios a las poblaciones afectadas.

En este sentido, algunas de las personas que contribuyeron a este número de la *International Review* (cuyos artículos aparecen bajo los títulos de "La acción humanitaria en la era digital" y "La industria y las tecnologías digitales en las crisis humanitarias") analizan cómo el uso de las tecnologías digitales para la provisión de ayuda humanitaria conlleva tanto oportunidades inéditas como riesgos sin precedentes. Destacan que algunas tecnologías digitales, en particular aquellas que facilitan la comunicación y la prestación de servicios, son herramientas vitales para el sector humanitario, dado que ayudan a garantizar que dicho sector aporte soluciones en contextos de crisis y continúe prestando servicios a las poblaciones afectadas. Por ejemplo, el aumento de la conectividad y del acceso digital puede empoderar a las personas afectadas por conflictos armados y otras situaciones de violencia y ayudarlas a conectarse con otros a través de aplicaciones de mensajería y de las plataformas de las redes sociales, encontrar información en línea y expresar sus necesidades mediante mecanismos de comunicación rápida, lo que les permite actuar como agentes activos y cooperar con las organizaciones humanitarias[2].

* Saman Rejali es asesor en Derecho y Políticas del CICR y se desempeñó como redactor temático para este número de la *International Review* sobre el tema "Las tecnologías digitales y la guerra". Yannick Heiniger es director general adjunto de Swissnex San Francisco y, con anterioridad, fue responsable de Asociaciones en la Oficina para la Oficina de Datos y Transformación Digital del CICR.

1 En el caso del CICR, "Sumarse a la transformación digital" es el quinto pilar de la *Estrategia Institucional para el período 2019-2022*, disponible en https://www.icrc.org/es/publication/estrategia-del-cicr-2019-2022 (todas las referencias de internet fueron consultadas en enero de 2021).

2 Una mirada a la tapa de este número ilustra esta realidad: en Siria, donde, tras años de violencia, la población sufre enormes necesidades urgentes y de largo plazo, un padre sostiene un teléfono inteligente con una foto de su hijo en la pantalla, rodeado de la destrucción creada por el conflicto armado. V. "In Eastern Ghouta Rubble, a Father Looks for His Son", *Reuters*, 4 de marzo de 2018, disponible en www.reuters.com/article/us-mideast-crisis-syria-ghouta-victims-idUSKBN1GG0EJ.

Asimismo, gracias a los análisis contextuales basados en la tecnología digital, el mapeo de crisis y los servicios digitalizados, las organizaciones humanitarias pueden asistir a las personas afectadas con mayor eficiencia, así como predecir y responder a crisis humanitarias.

Por otra parte, los autores también subrayan la existencia de ciertos riesgos y consideraciones que van de la mano con las oportunidades derivadas del uso de las tecnologías digitales en las actividades de ayuda humanitaria. Para las organizaciones humanitarias, tener presentes estos riesgos y mitigarlos es la mejor forma de estar bien preparadas para embarcarse en los procesos de transformación digital. Un factor de riesgo predominante es la protección y la privacidad de los datos: recopilar los datos de las poblaciones afectadas impone a las organizaciones humanitarias la carga ineludible de garantizar que los datos de las personas afectadas no sean utilizados en forma indebida y que ese uso no las ponga en peligro, contrariando la finalidad para la que fueron recopilados. Además, las distintas formas de diseminar los datos y la información influyen en el desarrollo de los conflictos y otras situaciones de violencia, como sucedió en Myanmar[3]. La información falsa, la desinformación o manipulación informativa y los discursos de odio, así como las "nuevas realidades" que se presentan a través de los "deepfakes" (materiales digitales "ultrafalsos" en cuya producción se utiliza el aprendizaje automático para generar contenidos sintéticos de video, audio y texto)[4], se cuentan entre los nuevos riesgos que han aparecido en paralelo con el uso generalizado de las redes sociales y otras herramientas de difusión en línea. Por este motivo, se ha dedicado una sección de este número de la *International Review* al papel de las empresas, concretamente las tecnológicas, que vienen apoyando en creciente medida la labor de las organizaciones humanitarias, a la vez que, debido al uso que se hace de sus tecnologías, participan indirectamente en la conducción de hostilidades.

Hay una segunda razón que hace que la digitalización sea importante para el sector humanitario. Las tecnologías digitales (o "nuevas tecnologías") se utilizan en los conflictos armados como medio y método de guerra, aspecto regido por el derecho internacional humanitario (DIH). Los usos de estas nuevas tecnologías acarrean consecuencias humanitarias, puesto que dan lugar a medios y métodos de guerra nunca antes vistos. Por ejemplo, como señalan Gisel, Rodenhäuser y Dörmann en su artículo para este número de la *International Review,* las ciberoperaciones contra las redes eléctricas, los sistemas de salud, las instalaciones nucleares y otros tipos de infraestructura crítica podrían causar "daños humanos significativos" y consecuencias humanitarias catastróficas[5]. Además de las amenazas

3 Alexandra Stevenson, "Facebook Admits It Was Used to Incite Violence in Myanmar", *New York Times*, 6 de noviembre de 2018, disponible en www.nytimes.com/2018/11/06/technology/myanmar-facebook.html.

4 Aengus Collins, *Forged Authenticity: Governing Deepfake Risks*, EPFL International Risk Governance Center, 2019, disponible en https://infoscience.epfl.ch/record/273296?ln=en.

5 V. Laurent Gisel, Tilman Rodenhäuser y Knut Dörmann, "Veinte años después: el derecho internacional humanitario y la protección de las personas civiles de los efectos de las ciberoperaciones durante los conflictos armados", en este número de la *International Review*.

cibernéticas, los sistemas de armas autónomas, incluidos los que se activan mediante la inteligencia artificial, también plantean preocupaciones humanitarias, jurídicas y éticas, puesto que seleccionan y aplican la fuerza contra los objetivos sin intervención humana. Esto significa que el usuario no conoce el objetivo específico que se ataca, ni sabe dónde ni cuándo será atacado[6]. En la tercera y cuarta partes de esta edición, respectivamente dedicadas a la inteligencia artificial y los sistemas de armas autónomas, y a las operaciones y la guerra cibernéticas, los autores adoptan posiciones diferentes y analizan el uso de las tecnologías digitales en la guerra desde distintos puntos de vista, evaluando la aplicación del DIH en aquellos casos en que las tecnologías digitales se utilizan con fines de destrucción.

Sin embargo, las "nuevas" tecnologías evolucionan al ritmo de los avances tecnológicos más recientes. Como sucedió con el telégrafo —hoy prácticamente extinto—, que dos siglos atrás "cambió el juego de la comunicación"[7], llegará el día en que algunas de estas tecnologías perderán su importancia y dejarán de ser "nuevas", y quizás entonces los riesgos y oportunidades relacionados con la protección de datos y la información falsa, la desinformación y los discursos de odio pasen a ser irrelevantes. No obstante, hay una serie de temas "atemporales" relacionados con las tecnologías digitales y con el derecho, la acción y las políticas humanitarias que resistirán el paso del tiempo y que se abordan en el análisis que se desarrolla a continuación.

Consideramos[8] que el común denominador clave de todos estos artículos es la confianza. La acción humanitaria basada en principios se funda en la confianza y los trabajadores humanitarios tienen la responsabilidad de granjearse la confianza de las poblaciones afectadas a las que desean prestar servicios[9]. Las tecnologías digitales ofrecen oportunidades incomparables para proporcionar ayuda humanitaria, pero, para reducir los riesgos que se describen en estas páginas, deben usarse con ética y responsabilidad. Solo así las organizaciones humanitarias podrán aspirar a ganarse la confianza de las poblaciones afectadas a las que deben rendir cuentas.

La confianza trae consigo la ética: debemos actuar de una forma que haga justicia a las personas que servimos, garantizar que los beneficios de las tecnologías digitales sean superiores a sus riesgos y asegurarnos de trabajar *con* las personas afectadas y no decidir por ellas respecto de las cuestiones que inciden en su vida.

6 V. Vincent Boulanin, Neil Davison, Netta Goussac y Moa Peldán Carlsson, *Establecer límites a la autonomía de los sistemas de armas: identificación de elementos prácticos del control humano*, SIPRI y CICR, junio de 2020, incluido en la sección "Informes y documentos" de este número de la *International Review*; Frank Sauer, "Dar un paso atrás: por qué la reglamentación multilateral de la autonomía en los sistemas de armas es difícil y, a la vez, necesaria y realizable", en este número de la *International Review*.

7 Jimmy Stamp, "How the Telegraph Went from Semaphore to Communication Game Changer", *Smithsonian Magazine*, 11 de octubre de 2013, disponible en www.smithsonianmag.com/arts-culture/how-the-telegraph-went-from-semaphore-to-communication-game-changer-1403433/.

8 En este editorial, el término "nosotros" se refiere exclusivamente a sus autores y no al CICR o al sector humanitario. Las opiniones aquí expresadas reflejan solamente las de los autores y no las del CICR ni las de Swissnex San Francisco.

9 Hugo Slim, "Trust Me - I'm a Humanitarian", *Humanitarian Law and Policy Blog*, 24 de octubre de 2019, disponible en https://blogs.icrc.org/law-and-policy/2019/10/24/trust-humanitarian/.

Los marcos éticos también se aplican a los medios y métodos de guerra. Por ejemplo, en el caso de la inteligencia artificial, Pizzi, Romanoff y Engelhardt[10], miembros de UN Global Pulse, la iniciativa del Secretario General de la ONU sobre *big data* e inteligencia artificial, señalan que para regular la inteligencia artificial es preciso aplicar marcos éticos, pero que estos no siempre son suficientes en las estructuras organizativas donde el enfoque de "la ética primero" no se complementa con mecanismos de rendición de cuentas sólidos.

Los autores incluidos en este número de la *International Review* también destacan las consideraciones éticas y las posibles barreras relacionadas con la inclusión que afronta la "innovación humanitaria". Esta permite abrir nuevas vías para prestar servicios a las personas afectadas, pero si los proyectos innovadores no toman en cuenta las medidas de protección de los datos y de la información personal, y si esos proyectos se crean sin estar realmente centrados en las personas afectadas y sin incluirlas, es posible que los riesgos que conllevan superen los beneficios[11]. En tales casos, el "producto" podría omitir la diligencia debida que se necesita para garantizar que las tecnologías digitales traigan a las poblaciones afectadas más beneficios que daños. En efecto, Sandvik y Lohne[12] mencionan este aspecto y señalan claramente que el problema reside en que "las poblaciones afectadas no suelen estar presentes en los procesos de innovación; no se las consulta apropiadamente ni se las invita a participar". Esta situación puede ocasionar "nuevos daños digitales, ya sea porque se (in)visibiliza el sufrimiento de determinados grupos o individuos, se generan consecuencias no deseadas o se introducen nuevos riesgos". En las páginas que siguen, reseñaremos el modo en que los artículos incluidos en este número de la *International Review* analizan los beneficios y los riesgos de las tecnologías digitales utilizadas para la acción humanitaria, identificando las oportunidades y las medidas de mitigación —que son las vías que se deben seguir si se desea acometer la digitalización de la acción humanitaria— y tomando en cuenta el creciente papel del sector privado. Más adelante, presentaremos un panorama del posible uso de las tecnologías digitales como medio y método de guerra en los conflictos armados, remitiéndonos a los artículos que abordan las ciberoperaciones y la aplicación del DIH, los sistemas de armas autónomas, el aprendizaje automático y la inteligencia artificial. Este análisis viene acompañado de la explicación de quiénes somos: dos *millennials* con experiencia sobre el tema en cuestión y autores conjuntos de este editorial. El análisis concluye con el examen de algunos elementos contextuales que influyeron en la publicación de este número de la *International Review* y con una reflexión sobre las conclusiones generales que se desprenden de esta edición.

10 V. Michael Pizzi, Mila Romanoff y Tim Engelhardt, "La inteligencia artificial y la acción humanitaria: derechos humanos y ética", en este número de la *International Review*.

11 V. CICR, Informe del simposio "Los riesgos digitales en los conflictos armados", Ginebra, octubre de 2019, incluido en la sección "Informes y documentos" de este número de la *International Review*.

12 V. Kristin Bergtora Sandvik y Kjersti Lohne, "Abordar la violencia sexual en el marco de los conflictos: indagación del giro digital", en este número de la *International Review*.

Los puntos de vista de los *millenials* acerca de las tecnologías digitales y la guerra

En este editorial, pretendemos echar un vistazo transversal a las diversas ideas que los lectores hallarán en este número de la *International Review.* Como dos *millennials* dedicados desde hace varios años al tema general de las tecnologías en la acción humanitaria, claramente pertenecemos a la primera generación de "nativos digitales"[13]. Se supone que estamos a nuestras anchas con el uso y la integración de las nuevas tecnologías digitales en nuestra vida cotidiana. Así sucede, sin duda alguna, con muchos aspectos de nuestra vida social: Facebook, Twitter, LinkedIn, TikTok y demás consumen buena parte de nuestro tiempo y muchos *millenials* perciben que las interacciones digitales son un complemento esencial de las físicas.

Como se destaca en el informe de 2020 *Los* millennials *y la guerra*[14], los *millennials* tienen una opinión muy positiva del potencial de las tecnologías digitales para ayudar a las personas afectadas por la guerra. Al analizar las repercusiones y consecuencias de las tecnologías digitales en los conflictos armados, aspiramos a que este número de la *International Review* brinde una "verificación de la realidad" en el mundo que nosotros, como *millennials,* contribuimos a crear, señalando cómo nuestras acciones en la esfera humanitaria tienen consecuencias para las personas afectadas a quienes deseamos prestar servicios. También reconocemos que, siendo *millenials,* tenemos nuestro propio sesgo. Los "nativos digitales" tienden a establecer una relación diferente con los principios que forman la base de la práctica humanitaria, es decir, la neutralidad, la imparcialidad y la independencia en la acción humanitaria[15]. Las tecnologías digitales y los algoritmos desempeñan un papel importante en nuestra visión del mundo.

Con respecto al principio de humanidad, no solo reconocemos que "el sufrimiento es universal y exige una respuesta"[16], sino que, además, adoptamos una postura "activista". Utilizamos los diferentes canales de los medios sociales a nuestra disposición para movilizar acciones, tanto en línea como fuera de línea[17].

13 Berkman Klein Center for Internet and Society, Harvard University (BKC), "Digital Natives", disponible en https://cyber.harvard.edu/research/youthandmedia/digitalnatives. BKC define a los nativos digitales como "una generación 'nacida digital', esto es, las personas que crecen inmersas en las tecnologías digitales, para quienes una vida plenamente integrada con los dispositivos digitales es la norma".

14 CICR, *Los* millennials *y la guerra*, Ginebra, 2020, disponible en https://www.icrc.org/es/millennials-y-guerra.

15 En comparación, los Principios Fundamentales del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja (el Movimiento) consisten en siete principios: humanidad, imparcialidad, neutralidad, independencia, voluntariado, unidad y universalidad. Jérémie Labbé y Pascal Daudin, "Aplicación de los principios humanitarios: una reflexión acerca de la experiencia del Comité Internacional de la Cruz Roja", *International Review of the Red Cross*, n.º 897/898, 2016; Oficina del Alto Comisionado de las Naciones Unidas para los Refugiados, "Humanitarian Principles", disponible en https://emergency.unhcr.org/ entry/44765/humanitarian-principles; CICR, *Principios Fundamentales de la Cruz Roja y de la Media Luna Roja*, agosto de 2015, disponible en https://www.icrc.org/es/publication/los-principios-fundamentales-de-la-cruz-roja-y-de-la-media-luna-roja.

16 CICR, nota 15 *supra*.

17 Emily Logan, "Millennial Activism: Tapping into a Network of Millennial Donors", disponible en https://csic.georgetown.edu/magazine/millennial-activism-tapping-network-millennial-donors/.

Escribimos como dos coautores que crecieron principalmente en el Norte global y reconocemos que nuestras experiencias no son comunes a todos los *millennials*, sino que corresponden a un subconjunto de "ciudadanos del mundo" de los centros neurálgicos de Ginebra, Londres, Nueva York, Toronto y París (entre otros)[18]. Honrando nuestro compromiso de hacer una diferencia y de no ser *indiferentes* al sufrimiento, soportamos una crisis financiera (y otra más, en el momento de escribir este texto), cumplimos una pasantía tras otra, un contrato de corto plazo tras otro, renunciamos a la estabilidad de la vida de nuestros padres[19] en favor de la vida global que llevamos[20], caímos parados y continuamos persiguiendo nuestra vocación en el sector humanitario. No nos desalentamos fácilmente, y esto es lo que el mundo necesita, dado que lidiamos con los riesgos que las tecnologías digitales acarrean para la acción humanitaria y con su posible uso indebido en la guerra. Nuestro mundo no es manejado solo por los Estados: es multipolar, con un "creciente número" de grupos armados no estatales[21] que utilizan las tecnologías digitales como medio para lograr sus objetivos en los conflictos armados[22]. Además, hemos crecido con los medios sociales, pero también los criticamos cada vez más[23]. Así sucede, en particular, cuando examinamos específicamente el accionar de las empresas tecnológicas mundiales y vemos cómo la reciente crisis del coronavirus ha fortalecido su dominio sobre aspectos claves de nuestra sociedad, empeorando la realidad cotidiana de miles de personas, incluso en contextos humanitarios.

Como *millennials*, abogamos por la aceptación del principio de imparcialidad como la fuerza que impulsa la inclusión y la diversidad verdaderas en el sector humanitario[24]. Por ello, comprendemos que, aunque las tecnologías digitales facilitan la conexión con las personas afectadas, también pueden causar una brecha digital, provocando desigualdades intersectoriales en el acceso a las tecnologías digitales y sus beneficios, y dejando en desventaja a ciertas poblaciones

18 April Rinne, "What Is Global Citizenship?", 9 de noviembre de 2017, disponible en www.weforum.org/agenda/ 2017/11/what-is-global-citizenship/.

19 Janet Adamy, "Millennials Slammed by Second Financial Crisis Fall Even Further Behind", *Wall Street Journal*, 9 de agosto de 2020, disponible en www.wsj.com/articles/millennials-covid-financial-crisis-fall-behind-jobless-11596811470.

20 BKC, nota 13 *supra*.

21 Jelena Nikolic, Tristan Ferraro y Thomas de Saint Maurice, "Aggregated Intensity: Classifying Coalitions of Non-State Armed Groups", *Humanitarian Law and Policy Blog*, 7 de octubre de 2020, disponible en https://blogs.icrc.org/law-and-policy/2020/10/07/aggregated-intensity-classifying-coalitions-non-state-armed-groups/.

22 Delphine van Solinge, "Digital Risks for Populations in Armed Conflict: Five Key Gaps the Humanitarian Sector should Address", *Humanitarian Law and Policy Blog*, 12 de junio de 2019, disponible en https://blogs.icrc.org/law-and-policy/2019/06/12/digital-risks-populations-armed-conflict-five-key-gaps-humanitarian-sector/.

23 Nick Statt, "Facebook's US User Base Declined by 15 Million since 2017, According to Survey", *The Verge*, 6 de marzo de 2019, disponible en www.theverge.com/2019/3/6/18253274/facebook-users-decline-15-million-people-united-states-privacy-scandals; Jack Nicas, Mike Isaac y Sheera Frenkel, "Millions Flock to Telegram and Signal as Fears Grow over Big Tech", *New York Times*, 13 de enero de 2021, disponible en www.nytimes.com/2021/01/13/technology/telegram-signal-apps-big-tech.html.

24 Saman Rejali, "Race, Equity, and Neo-Colonial Legacies: Identifying Paths Forward for Principled Humanitarian Action", *Humanitarian Law and Policy Blog*, 16 de julio de 2020, disponible en https://blogs.icrc. org/law-and-policy/2020/07/16/race-equity-neo-colonial-legacies-humanitarian/.

afectadas[25]. En su artículo para este número de la *International Review*, Jo Burton explica claramente la brecha digital a través del ejemplo de la digitalización del dinero en efectivo, señalando que

> el mayor uso de los pagos digitales puede profundizar la "brecha digital"... Todas las personas pueden usar efectivo, si lo consiguen y si los bienes y servicios que necesitan pagar están disponibles... Sin embargo, el uso del pago digital requiere que el receptor cuente con cierto nivel de alfabetización digital y financiera. Según las estimaciones, solamente uno de cada tres adultos en el mundo comprende los conceptos financieros básicos, y el conocimiento de las finanzas es menor aún entre las mujeres y los pobres[26].

Como se destaca en el análisis de Burton, la desigualdad intersectorial —incluida la inequidad financiera y basada en el género— profundiza la brecha digital. No obstante, creemos que la adopción de medidas que encarnen el principio de la imparcialidad permitiría encarar las desigualdades sistémicas que obstaculizan la respuesta humanitaria.

Con respecto al principio de neutralidad, como *millennials* y a través de nuestra experiencia de primera mano con muchas campañas de información falsa y desinformación operadas a través de los medios sociales, hemos tomado conciencia de que, debido a la forma en que algunas personas usan las tecnologías digitales, estas no son necesariamente neutrales. Así lo ilustra a las claras el uso de las tecnologías digitales como medios destructivos durante los conflictos armados y otras situaciones de violencia.

En suma, nuestra visión *millennial* de los principios de neutralidad, imparcialidad e independencia en la acción humanitaria modela la forma en que vemos, analizamos y trabajamos con las tecnologías digitales en las crisis humanitarias y en el contexto de la evaluación de la aplicación del DIH a los medios y métodos de guerra. La perspectiva de las tecnologías digitales expuesta en estas páginas nos brinda una oportunidad única para (re)pensar y ampliar nuestras reflexiones sobre las tecnologías digitales y la guerra y sobre el papel más amplio de esas tecnologías en la acción humanitaria. Esperamos que así sea también para todos los lectores, más allá de los límites generacionales.

Las tecnologías digitales y la acción humanitaria: los riesgos

Varios de los artículos presentados en este número de la *International Review* señalan cómo las tecnologías digitales pueden ser utilizadas sin plena conciencia de sus consecuencias. Por ello, esas tecnologías plantean, en el contexto

25 Barnaby Willitts-King, John Bryant y Kerrie Holloway, *The Humanitarian "Digital Divide"*, Documento de trabajo del Grupo de Políticas Humanitarias, Instituto de Desarrollo de Ultramar (ODI), Londres, noviembre de 2019, p. 15; Lina Gurung, "The Digital Divide: An Inquiry from Feminist Perspectives", *Dhaulagiri Journal of Sociology and Anthropology*, vol. 12, 2018.

26 V. Jo Burton, "'No causar daño' en la era digital: El significado de la digitalización del dinero en efectivo para la acción humanitaria", en este número de la *International Review*.

de los conflictos, ciertos riesgos —sociales, económicos, políticos y cognitivos— que las organizaciones humanitarias deben tener en cuenta en sus actividades operacionales y de asistencia. El aspecto más problemático es, quizás, que las evaluaciones de los beneficios y los riesgos suelen realizarlas únicamente las organizaciones humanitarias, y no lo hacen *con* las personas afectadas. Además, las personas más afectadas por esos riesgos son los individuos y las comunidades en contextos de crisis.

Se han identificado tres vectores de riesgo principales[27] en relación con la acción humanitaria: 1) la vigilancia, el seguimiento y la intrusión digitales; 2) la información falsa, la desinformación y los discursos de odio; y 3) el uso indebido y el manejo incorrecto de los datos y de la información personal.

Vigilancia, seguimiento e intrusión digitales

Los riesgos asociados con la vigilancia, el seguimiento y la intrusión digitales pueden tener distintos orígenes, como los análisis de *big data,* los modelos de aprendizaje automático o el uso indebido de datos por las autoridades, o pueden derivar de la presencia y de las actividades en línea de las personas. Como señalan Gazi y Gazis[28] en su contribución a este número de la *International Review,* los análisis de *big data* y de datos abiertos no solo acarrean riesgos para la privacidad, sino que también pueden producir resultados sesgados. Esto último se debe a que, muchas veces, los *big data* y los datos abiertos

> carecen de la información demográfica fundamental para la investigación epidemiológica, como la edad y el género. [Además], esos datos representan solo una parte limitada de la población —es decir, no incluyen a los grupos marginados y subrepresentados, como los niños pequeños, las personas analfabetas, las personas mayores, las comunidades indígenas y las personas con discapacidades—, a la vez que pueden subrepresentar a algunos países en desarrollo donde el acceso digital no se ha generalizado.

Esto resulta particularmente problemático para las actividades de asistencia y protección humanitarias, ya que los análisis de *big data* y de datos abiertos pueden llevar a las organizaciones humanitarias a omitir, inadvertidamente, a las personas marginadas situadas en diversas intersecciones de la desigualdad a las que desean

27 Según menciona el CICR en el Informe del simposio "Los riesgos digitales en los conflictos armados", los riesgos digitales "incluyen los efectos colaterales (a menudo no intencionales) de la experimentación con datos digitales, de violaciones de la privacidad y del manejo indebido de la información sensible que acompaña los esfuerzos del sector humanitario por desplegar tecnologías emergentes en contextos ya frágiles". CICR, nota 11 *supra*.

28 V. Theodora Gazi y Alexandros Gazis, "Asistencia humanitaria en tiempos de COVID-19: una evaluación del análisis de *big data* relativa a la crisis y el Reglamento general de protección de datos", en este número de la *International Review.*

ayudar. Así lo reafirma el análisis de Milaninia[29], que ilustra cómo los modelos de aprendizaje automático y los análisis de *biga data* son "altamente susceptible a los sesgos humanos comunes", por lo cual pueden "acentuar las desigualdades raciales, políticas y de género existentes" y potencialmente presentar "una imagen engañosa y distorsionada de la realidad en el terreno".

En la misma línea, Pizzi, Romanoff y Engelhardt[30] señalan que la falta de calidad de los datos aumenta los riesgos de que un sistema de inteligencia artificial produzca resultados inequitativos, dado que

> los sistemas de inteligencia artificial pueden revelar información sensible sobre la ubicación, las redes sociales, las afiliaciones políticas, las preferencias sexuales y otros datos de las personas, todo ello sobre la base de la información que estas publican en línea en forma voluntaria (como los textos y las fotografías que los usuarios publican en los medios sociales) o que producen fortuitamente a partir de sus dispositivos digitales (como el GPS o los datos de localización del teléfono móvil).

Una vez recopilados, esos datos son sumamente susceptibles de los usos indebidos, si no se adoptan las medidas de protección de datos necesarias. Lo que es más peligroso aún, a través de su comportamiento en línea, las poblaciones afectadas, sin saberlo, pueden tornarse vulnerables a posibles daños reales. Por ejemplo, en contextos de crisis, puede suceder que las personas sean vigiladas y su perfil investigado[31], o pueden ser víctimas de amenazas de violencia, crímenes de odio o discriminación[32]. El informe del CICR sobre el simposio "Los riesgos digitales en los conflictos armados", incluido en la sección "Informes y documentos" de este número de la *International Review*, presenta un caso real de vigilancia de ese tipo, en el cual un ataque de *software* malicioso afectó los dispositivos móviles de algunos refugiados sirios. En otros ejemplos, son los propios trabajadores humanitarios quienes ejercen esa vigilancia al utilizar las tecnologías para responder mejor a las necesidades, por ejemplo, mediante el uso de drones con fines de mapeo y evaluación de riesgos[33]. En este caso, los riesgos de vigilancia mencionados son particularmente pertinentes, ya que los drones pueden recopilar información de los contextos donde viven poblaciones afectadas sin el consentimiento ni el conocimiento de estas. El artículo de Siatitsa[34], por ejemplo, describe casos más

29 V. Nema Milaninia, "Sesgos en los modelos de aprendizaje automático y el análisis de *big data*: efectos jurídicos respecto del derecho penal internacional y del derecho internacional humanitario", en este número de la *International Review*.

30 M. Pizzi, M. Romanoff y T. Engelhardt, nota 10 *supra*.

31 J. Burton, nota 26 *supra*.

32 CICR, nota 11 *supra*.

33 Faine Greenwood, "Data Colonialism, Surveillance Capitalism and Drones", en Doug Specht (ed.), *Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping*, University of London Press, Londres, 2020.

34 V. Ilia Siatitsa, "Ataque a la libertad de reunión: vigilancia e interferencia general e indiscriminada en las comunicaciones virtuales", en este número de la *International Review.*

sofisticados de vigilancia, seguimiento e intrusión y examina esas cuestiones en relación con las técnicas de reconocimiento facial.

Información falsa, desinformación y discursos de odio

Hablando sobre este tema al responder a las preguntas y respuestas de este número de la *International Review*[35], Delphine van Solinge describe cómo, a través de la información falsa, la desinformación y los discursos de odio, se puede manipular y diseminar información mediante las tecnologías digitales, especialmente en medio de la pandemia causada por el coronavirus, cuando las poblaciones dependen en mayor medida de las tecnologías de comunicación digitales. Un ejemplo de táctica de desinformación es la creación de "deepfakes" usando el aprendizaje automático para generar contenidos de video y audio falsos[36]. En contextos de crisis como los de Myanmar, Sudán del Sur y Etiopía[37], la información falsa, la desinformación y los discursos de odio se diseminan a través de las plataformas de las redes sociales y la opinión pública se manipula mediante información falsa o incompleta, exacerbando así las crisis humanitarias del momento. El uso de las tecnologías por los públicos masivos dota de creciente poder a las empresas que operan las plataformas de los medios sociales, de mensajería y de búsqueda, incluso en conflictos armados y otras situaciones de violencia. Recientemente, hemos observado que el accionar de las grandes empresas tecnológicas ha repercutido a nivel mundial, por un lado, debido a su actuación como árbitros de la libertad de expresión y, por el otro, a través del uso de las cuentas de los medios sociales para difundir información dañina (por ejemplo, información falsa, desinformación y discursos de odio). Esta situación es más evidente ahora, en medio de la pandemia causada por el coronavirus, dado que las poblaciones afectadas dependen más que nunca de esas plataformas para recibir información y comunicarse entre sí.

Uso indebido y manejo incorrecto de datos y de información personal

En relación con el uso indebido y el manejo incorrecto de los datos, el concepto de "tecnocolonialismo", acuñado por Mirca Madianou[38], es una excelente guía que permite vislumbrar lo que puede salir mal, incluso con las mejores intenciones, si aplicamos la innovación digital y los datos biométricos agregados en las crisis humanitarias sin antes implementar las prácticas de protección de datos y los marcos de protección digitalmente adaptados que se necesitan. De hecho, las

35 V. "Preguntas y respuestas: Las actividades humanitarias, la difusión de información perjudicial y la protección de datos", en este número de la *International Review.*

36 Harvard Kennedy School, Belfer Centre for Science and Information Affairs, "Tech Factsheets for Policymakers: Deepfakes", 2020, disponible en www.belfercenter.org/sites/default/files/2020-10/tappfactsheets/Deepfakes.pdf.

37 "Preguntas y respuestas", nota 35 *supra*.

38 Mirca Madianou, "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises", *Social Media + Society*, vol. 5, n.° 3, 2019, disponible en https://journals.sagepub.com/doi/full/10.1177/2056305119863146.

tecnologías integran y refuerzan los sistemas de valores, las culturas y las visiones del mundo de sus creadores. La innovación digital y las prácticas de datos aplicadas sin inhibiciones pueden reforzar aún más las asimetrías de poder arraigadas en tiempos coloniales entre los trabajadores humanitarios y las poblaciones afectadas[39].

Ello se refleja en el "capitalismo de vigilancia", descrito por Zuboff como "datos de seres humanos utilizados para obtener una ganancia a expensas de las propias personas"[40]. En el contexto de las crisis humanitarias, esto significa que los datos de las poblaciones afectadas pueden no solo recopilarse, sino también usarse con fines de lucro. Como esta recopilación de datos a menudo se produce sin el conocimiento de la persona afectada, Zuboff traza un paralelo con las prácticas coloniales de extracción no autorizada. En este sentido, Sandvik y Lohne señalan cómo las ramificaciones de esa recopilación de datos irrestricta y el registro, en las nubes digitales, de la información sobre las poblaciones afectadas pueden crear "cuerpos digitales" con consecuencias de género respecto del modo en que se aborda la violencia sexual relacionada con los conflictos[41].

Las consecuencias de lo que sucede en el sector humanitario cuando no se implementan adecuadamente las medidas de protección de datos son descritas por Massimo Marelli en las "Preguntas y respuestas" de este número[42] y por Burton, quien aplica el principio de "no hacer daño (digital)" de la protección de datos a la digitalización del dinero en efectivo. Burton explica cómo los metadatos —los datos que proveen información sobre otros datos— pueden tener consecuencias graves para las crisis humanitarias y hasta pueden ser utilizados para obtener ventajas militares, en particular cuando personas influyentes como el general Hayden, exdirector de la Agencia Nacional de Seguridad y de la Agencia Central de Inteligencia (citado por Burton), dicen "Matamos gente basándonos en metadatos"[43].

Lo que sucede con los datos de las poblaciones afectadas una vez recopilados por las organizaciones humanitarias plantea problemas muy graves. En varias ocasiones, las grandes empresas tecnológicas han compartido los datos de los usuarios con los gobiernos, lo cual puede plantear riesgos de seguridad para los ciudadanos afectados por conflictos armados u otras situaciones de violencia[44]. Cabe destacar que, incluso cuando los datos de las personas afectadas no se comparten, la información almacenada puede ser pirateada o robada si las organizaciones humanitarias no la protegen apropiadamente[45]. Este riesgo relacionado con la protección de datos también se menciona en el informe del CICR sobre el simposio

39 Ibíd.

40 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future*, PublicAffairs, Nueva York, 2019.

41 K. B. Sandvik y K. Lohne, nota 12 *supra*.

42 "Preguntas y respuestas", nota 35 *supra*.

43 J. Burton, nota 26 *supra*.

44 Ibíd.; F. Greenwood, nota 33 *supra*.

45 Christopher Kuner y Massimo Marelli (ed.) señalan la importancia de las medidas relativas a la protección de datos en la acción humanitaria en el *Manual sobre protección de datos en la acción humanitaria*, 2.ª ed., CICR y Brussels Privacy Hub, Ginebra, junio de 2020, incluido en la sección "Informes y documentos" de este número de la *International Review*.

"Los riesgos digitales en los conflictos armados"[46]: "Las organizaciones humanitarias recopilan, almacenan, comparten y analizan datos que interesan a las partes en los conflictos armados... En consecuencia, las organizaciones humanitarias están expuestas a una creciente ola de ataques digitales y de ciberespionaje, porque se han transformado en objetivos sumamente apreciados".

Las tecnologías digitales y la acción humanitaria: medidas de mitigación y beneficios

Para hacer frente a los riesgos digitales, que tienen consecuencias sociales, económicas, políticas y cognitivas para las poblaciones afectadas y las crisis humanitarias, las organizaciones humanitarias pueden adoptar varias medidas activas, entre ellas las siguientes: 1) promover la alfabetización digital; 2) fortalecer las prácticas de protección de datos y crear las salvaguardias adecuadas para la adopción de tecnologías digitales; y 3) adoptar políticas humanitarias adecuadas, asegurando que las personas sigan ocupando el lugar central en su labor.

Promover la alfabetización digital

La alfabetización digital no es solo un componente que "es bueno tener" en las organizaciones humanitarias; es una necesidad fundamental de las poblaciones afectadas. Esta importante observación surge una y otra vez en este número de la *International Review*. Van Solinge, por ejemplo, aboga por fortalecer la resiliencia de las personas a la información falsa y la desinformación "promoviendo la alfabetización digital, el pensamiento crítico y... los valores humanitarios"[47]. Por su parte, Sandvik y Lohne subrayan que la alfabetización digital debe "ir más allá de la competencia técnica e incluir la concienciación y las percepciones relacionadas con la tecnología, la ley, los derechos y los riesgos"[48]. Estos elementos también son esenciales para las propias organizaciones humanitarias. Como ejemplo de las iniciativas en curso destinadas a proporcionar los elementos fundamentales de la alfabetización digital a los encargados de adoptar decisiones y a los abogados de las organizaciones humanitarias, el CICR se ha asociado con la Escuela Politécnica Federal de Lausanne (Ecole Polytechnique Fédérale de Lausanne, EPFL) en una serie de iniciativas colaborativas[49], una las cuales consiste en la creación de un curso introductorio de cinco días sobre los elementos básicos de la tecnología de la

46 CICR, nota 11 *supra*.
47 "Preguntas y respuestas", nota 35 *supra*.
48 K. B. Sandvik y K. Lohne, nota 12 *supra*.
49 La EPFL y ETH Zürich colaboran con el CICR para analizar soluciones innovadoras a las crisis humanitarias de hoy a través de la iniciativa HAC: v. EPFL, "Science and Technology for Humanitarian Action Challenges (HAC)", disponible en www.epfl.ch/research/services/fund-research/funding-opportunities/research-funding/science-and-technology-for-humanitarian-action-challenges-hac/. V. también EPFL, "EPFL, ETH Zurich and the ICRC Team Up to Bolster Humanitarian Aid", 10 de diciembre de 2020, disponible en https://actu.epfl.ch/news/epfl-eth-zurich-and-the-icrc-team-up-to-bolster-hu/.

información y la comunicación[50]. En la misma línea, la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (la Federación Internacional) ha desarrollado el proyecto Data Playbook, cuyo objetivo es "mejorar la alfabetización digital entre los equipos, los sectores y la Secretaría de la Federación Internacional y dentro de las Sociedades Nacionales"[51]. Si bien estos proyectos concretos se centran en los propios actores humanitarios, para muchas organizaciones humanitarias constituyen el primer paso hacia un territorio nuevo y esas iniciativas deberían complementarse con iniciativas similares a nivel del terreno, centradas en las poblaciones afectadas y en su alfabetización digital.

Fortalecer las prácticas de protección de datos

Sumadas a la alfabetización digital, las prácticas de protección de datos adecuadas pueden prevenir el acceso no deseado a los datos de las poblaciones afectadas a través de soluciones basadas en la vigilancia y el seguimiento o que impiden la violación del almacenamiento digital, lo cual constituye otra medida de mitigación de los riesgos digitales. Por ejemplo, en este sentido, Massimo Marelli describe cómo el CICR

> ha incorporado ahora una serie de salvaguardas específicas en [sus] Normas en materia de protección de datos personales, adoptadas en 2015, cuya finalidad es reducir los riesgos de uso o acceso no autorizados a los datos personales mediante la aplicación de normas y requisitos relativos al procesamiento de datos en toda la organización. Cuando el CICR considera la incorporación de tecnologías nuevas o de operaciones de procesamiento de datos más riesgosas, debe realizar una Evaluación de impacto relativa a la protección de datos, para identificar y mitigar los riesgos de daño. Las normas también obligan al CICR a aplicar un enfoque basado en la "protección de datos desde el diseño y por defecto", con el fin de reducir la recopilación de datos personales al mínimo necesario para la operación y garantizar que se respeten los derechos del titular de los datos[52].

La política humanitaria como factor que facilita el uso responsable de las tecnologías

Entre los recursos disponibles para las organizaciones humanitarias en este proceso de búsqueda del equilibrio entre las oportunidades y los riesgos, se destaca la política como un importante factor de facilitación. Al analizar las organizaciones que han emprendido procesos de transformación digital al tiempo que velan por la mitigación de los riesgos digitales, surgen algunos ejemplos interesantes que

50 EPFL, "Executive Training: Foundations of Information and Communication Technologies", disponible en www.c4dt.org/event/fict-executive-course/.

51 Federación Internacional, "Discover the Data Playbook Beta Project", 18 de octubre de 2018, disponible en https://media.ifrc.org/ifrc/ 2018/10/18/discover-data-playbook-beta-project/.

52 "Preguntas y respuestas", nota 35 *supra*.

complementan las observaciones recogidas en este número de la *International Review*. Una de las resoluciones clave de la XXXIII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja (Conferencia Internacional), celebrada en 2019, fue la Resolución 4 sobre "Restablecimiento del contacto entre familiares en un marco de respeto de la privacidad, incluso en materia de protección de los datos"[53]. En esta resolución, se exhorta a los Estados y al Movimiento Internacional de la Cruz Roja y de la Media Luna Roja (el Movimiento) a respetar numerosos requisitos relativos a la privacidad y a la protección de datos al procesar la información de las poblaciones afectadas. En particular, la resolución "insta a los Estados a cooperar para garantizar que no se soliciten ni se utilicen los datos personales con fines incompatibles con el carácter humanitario de la labor del Movimiento"[54]. Las disposiciones sobre protección de datos que subyacen a esta resolución se hallan establecidas en el "Código de Conducta sobre protección de datos personales para la Red de Vínculos Familiares del Movimiento"[55]. Este código estipula los principios, compromisos y procedimientos mínimos que debe cumplir el personal del CICR, de las Sociedades Nacionales y de la Federación Internacional al procesar datos en el marco de las actividades de restablecimiento del contacto entre familiares. Los documentos de este tipo pueden garantizar que las organizaciones humanitarias compartan un entendimiento común acerca de los riesgos inherentes y las medidas comunes necesarias para asegurar que las tecnologías funcionen de una forma que refuerce la protección de los datos sensibles de las personas que se hallan en zonas de conflicto.

De hecho, otro resultado de la Conferencia Internacional de 2019 fue la Promesa digital para todo el Movimiento denominada "Fortalecimiento de las capacidades digitales y de gestión de datos para la acción humanitaria a nivel nacional"[56], por la cual el Movimiento se comprometió a cumplir, para finales de 2023, un plan de acción cuyos objetivos son los siguientes: 1) fomentar asociaciones en este sentido; 2) favorecer deliberaciones sobre estos temas; y comprometerse con 3) la alfabetización digital, 4) la inclusión digital, 5) la protección de datos y 6) la responsabilidad digital. Este es otro ejemplo de la importancia de emprender el camino de la transformación digital basada en principios y de armonizar las percepciones en torno a las medidas necesarias para mitigar los efectos adversos de las tecnologías digitales. Asimismo, demuestra cómo el Movimiento puede

53 CICR, "Restablecimiento del contacto entre familiares en un marco de respeto de la privacidad, incluso en materia de protección de los datos", 33IC/19/R4, Resolución 4, adoptada en la XXXIII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, Ginebra, 9-12 de diciembre de 2019, disponible en https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL_es.pdf.

54 Ibíd., párr. 11.

55 CICR, "Código de Conducta sobre protección de datos personales para la Red de Vínculos Familiares del Movimiento", Ginebra, noviembre de 2015, disponible en https://www.icrc.org/es/document/codigo-conducta-proteccion-datos-personales-actividades-restablecimiento-contactos-familiares.

56 "Fortalecimiento de las capacidades digitales y de gestión de datos para la acción humanitaria a nivel nacional", Promesa digital, Conferencia Internacional de 2019, disponible en https://tinyurl.com/110x3pmp.

predicar con el ejemplo, aplicando los Principios Fundamentales del Movimiento[57] al uso de esas tecnologías.

También en la esfera de la política humanitaria, en 2019, el CICR adoptó una política sobre su utilización de las tecnologías biométricas[58], que se usan en el ámbito forense y para el restablecimiento del contacto entre familiares. Dado que la creación de un registro permanente para personas que quizás no quieran permanecer identificables para siempre es una cuestión sumamente sensible, esta política facilita el uso responsable de la tecnología por la organización y aborda los desafíos que ese uso plantea en materia de protección de datos. En suma, estas diferentes iniciativas ilustran claramente el papel que la política humanitaria puede desempeñar en la creación de un marco práctico que permita el uso basado en principios de las nuevas tecnologías digitales.

Los beneficios de las tecnologías digitales para la acción humanitaria

Aunque las tecnologías digitales plantean algunos riesgos como los ya mencionados, también traen consigo una serie de ventajas incomparables para las actividades operacionales y de asistencia de las organizaciones humanitarias. La sección "Testimonios y perspectivas" de este número de la *International Review*, en la que se presentan testimonios de las poblaciones afectadas, brinda varios ejemplos de esas ventajas.

En dicha sección, se presentan testimonios directos de personas cuyas vidas cambiaron para mejor gracias a las iniciativas digitales introducidas por el CICR. Uno de los testimonios se relaciona con la plataforma "Trace the Face" del CICR[59], que es "una galería de fotos en línea con las imágenes de miles de personas que buscan a sus familiares". A través de este sitio, Matty, que vive en Abiyán, pudo encontrar a su tío, de quien no tenía noticias desde el estallido de la crisis de 2010-2011 en Côte d'Ivoire[60].

Otro testimonio que destaca el potencial positivo de las tecnologías digitales en las crisis humanitarias es el de Zawadi, que cuenta cómo pudo contactar con la familia de su esposo a través de la iniciativa de mensajes electrónicos de Cruz Roja, un proyecto piloto colaborativo desarrollado entre el CICR, la Cruz Roja de la República Democrática del Congo y la Cruz Roja Ruandesa[61]. El proyecto piloto se inició en noviembre de 2018 y emplea mensajes electrónicos de Cruz Roja para restablecer el contacto entre familiares separados. Como parte del proyecto, los voluntarios de la Cruz Roja recorren las aldeas de la zona oriental de la República Democrática del Congo y de Ruanda con tabletas digitales conectadas a internet. El

57 CICR, nota 15 *supra*.

58 CICR, "La política de datos biométricos del CICR", 16 de octubre de 2019, disponible en https://www.icrc.org/es/document/la-politica-de-datos-biometricos-del-cicr.

59 CICR, "Trace the Face– Migrants in Europe", disponible en https://familylinks.icrc.org/europe/en/pages/publish-your-photo.aspx.

60 V. "El efecto de las tecnologías humanitarias en las poblaciones afectadas", en la sección "Testimonios y perspectivas" de este número de la *International Review*.

61 Ibíd.

proyecto es muy prometedor, ya que ha mejorado uno de los servicios más antiguos del CICR, el sistema de mensajes de Cruz Roja, logrando que el trabajo de restablecer el contacto entre familiares se haga con mayor rapidez y eficacia que antes. Esas iniciativas, vistas a través de los testimonios de las personas afectadas, son ejemplos de lo que es posible hacer cuando la innovación en el ámbito humanitario se suma a las tecnologías digitales con el propósito de aliviar los sufrimientos humanos en conflictos armados y otras situaciones de violencia. Aprovechando este impulso, el CICR está llevando a cabo la prueba piloto de "Red Safe"[62], una plataforma digital que permite a las poblaciones afectadas acceder a diversos servicios en forma digital.

En las "Preguntas y respuestas" de la *International Review*, Delphine van Solinge también destaca el modo en que las organizaciones humanitarias han "utilizado la mayor conciencia situacional y la información de aplicación práctica facilitadas por la era digital". Por ejemplo, señala que los defensores y profesionales de los derechos humanos

> han empleado herramientas de teledetección para fortalecer las capacidades de alerta temprana en relación con conflictos y para documentar las violaciones de derechos humanos. Han aprovechado las soluciones basadas en datos móviles para seguir de cerca las condiciones, los perfiles y las rutas de tránsito de las poblaciones de migrantes y refugiados; han empleado los metadatos de los registros de llamadas para comprender la propagación de enfermedades infecciosas; han escudriñado las redes sociales para realizar análisis de opiniones y seguir de cerca los rumores en contextos frágiles; y, claro está, han desplegado dispositivos de robótica aérea para examinar lugares dañados y vigilar la infraestructura crítica.
>
> En el caso de la pandemia de COVID-19, las herramientas digitales, la inteligencia artificial y el análisis de *big data* se utilizan en diversos contextos en apoyo de las respuestas sanitarias. Pueden ayudarnos a recopilar, analizar y transmitir información esencial que nos permite organizar los recursos y las capacidades en materia de salud, agilizar las cadenas médicas, logísticas y de adquisiciones, o gestionar los aspectos del confinamiento relacionados con la seguridad y la protección públicas.

Si bien Gazi y Gazis[63], en su artículo para este número de la *International Review*, analizan los riesgos del uso de *big data* ya mencionados, también hacen hincapié en los beneficios potenciales de esos datos para la acción humanitaria. Señalan cómo, en el contexto de la gestión de desastres, los *big data* pueden ayudar a responder a crisis migratorias, a epidemias y a catástrofes naturales. Pueden

62 V. CICR, "ICRC'S Activities in Favour of Migrants in Southern Africa", 2020, p. 5, disponible en www.icrc.org/en/download/file/147853/icrcs_activities_in_favour_of_migrants_in_southern_africa_newsletter.pdf.

63 T. Gazi y A. Gazis, nota 28 *supra*.

usarse también para la vigilancia de epidemias y la respuesta a estas. Un ejemplo interesante que presentan es el de Ushahidi, una aplicación de *software* utilizada para mejorar las actividades de ayuda humanitaria. A través de esta plataforma, entre junio de 2008 y junio de 2009, un grupo de investigadores en Kenia

> analizó los registros geográficos de los teléfonos móviles de casi 15 millones de personas para medir la movilidad humana en localidades de bajos ingresos en Kenia y así llegar a comprender la propagación de la malaria y de las enfermedades infecciosas. La empresa telefónica keniana Safaricom proporcionó información despersonalizada a los investigadores, quienes luego modelaron los patrones de desplazamiento de los usuarios. Los investigadores estimaron la probabilidad de contagio para los residentes y visitantes de cada zona cruzando los datos de sus desplazamientos con el mapa de prevalencia de la malaria provisto por el gobierno.

El uso de esos datos para el seguimiento de enfermedades infecciosas ofrece un gran potencial, sobre todo en medio de la actual pandemia de COVID-19. Es cierto que, como subrayan Gazi y Gazis, esa recopilación de datos plantea "el riesgo de que las personas sean nuevamente identificadas a través de sus patrones de actividad individuales. Por este motivo, cuando se utilizan datos despersonalizados con fines de análisis, los procedimientos para anonimizarlos suelen alterar ligeramente los datos originales (causando la pérdida de su utilidad) para proteger la identidad de las personas".

Milaninia[64], que también se refiere a algunas de las ventajas que brindan las tecnologías digitales en relación con la vigilancia del respeto del DIH y otros fines, describe cómo el aprendizaje automático se utiliza para fines positivos, "por ejemplo, para descubrir fosas comunes en México, hallar pruebas de la destrucción de viviendas y escuelas en Darfur, detectar videos falsos y pruebas manipuladas, predecir los resultados de los juicios ante el Tribunal Europeo de Derechos Humanos y reunir pruebas sobre los crímenes de guerra perpetrados en Siria".

Así pues, estos autores señalan los beneficios y los riesgos de las tecnologías digitales para la acción humanitaria y otras esferas y subrayan la necesidad de que el sector humanitario haga uso de las tecnologías digitales, pero adoptando las medidas de mitigación apropiadas.

La interacción entre los actores humanitarios y el sector tecnológico

Otra oportunidad interesante que se aborda en este número de la *International Review* dedicado a las tecnologías digitales se relaciona con las interacciones entre los actores humanitarios y los creadores de estas tecnologías. Hemos mencionado el uso de esas tecnologías en las operaciones cibernéticas y sus posibles consecuencias humanitarias, tema que se desarrolla más a fondo en la sección "Las ciberoperaciones y la guerra" y que se reseña en la siguiente parte

64 N. Milaninia, nota 29 *supra*.

de este editorial. Las tecnologías no se desarrollan en el vacío: son productos y soluciones elaborados por empresas particulares. En este contexto, ¿cómo pueden los actores humanitarios, cuya acción se basa en décadas de experiencia comprobada en el ejercicio de la "diplomacia humanitaria"[65], interactuar mejor con el sector tecnológico? Vienen a la mente algunos ejemplos que ilustran la sustancia de un posible diálogo y las formas que este puede adoptar.

En su artículo, Massimo Marelli explica que, para que la organización retenga el control absoluto sobre los datos sensibles que maneja, necesita contar con estructuras y soluciones digitales específicas que puede obtener, por ejemplo, a través de la creación de un espacio digital humanitario basado en el modelo de una "nube soberana" o de una "embajada digital"[66]. El desarrollo de tecnologías nuevas que garanticen que los datos recopilados por el CICR conforme a su cometido estén y permanezcan siempre bajo su control exclusivo es un ámbito productivo en el que deberían fortalecerse el diálogo y la colaboración concretos entre las organizaciones humanitarias, el sector de la tecnología, los gobiernos y los círculos académicos[67].

En este sentido, el CICR ha establecido una presencia en el Área de la Bahía de San Francisco, Estados Unidos (Bay Area), como un paso hacia la construcción de un diálogo sostenido con las empresas tecnológicas mundiales acerca de la forma en que las herramientas digitales pueden perjudicar a las personas afectadas por conflictos armados y otras situaciones de violencia[68]. El objetivo principal de esta interacción es aportar los conocimientos operacionales y jurídicos del CICR, así como su experiencia contextual, a un diálogo centrado en la aspiración de garantizar el uso responsable de las tecnologías —incluidos los principios básicos de la privacidad y la confianza— en contextos humanitarios. Esto requiere un aprendizaje mutuo acerca de cómo la tecnología, por un lado, puede ayudar a las poblaciones en zonas de conflicto y, por el otro, crear diversos riesgos y perjuicios para esas personas, comunidades y sociedades. Sobre esa base, se están haciendo esfuerzos para asegurar que la tecnología que usa el CICR, y que utilizan y a la que están expuestas las poblaciones afectadas, sea tan eficaz y segura como sea posible. Esta iniciativa puede conllevar la creación conjunta de nuevas herramientas y servicios (como los ya mencionados, que no son del tipo "listos para usar" y no se consiguen fácilmente en los comercios), así como el despliegue de actividades de diplomacia humanitaria destinadas a convencer a las distintas partes interesadas de que apoyen al CICR, su enfoque y sus recomendaciones (jurídicas, de política o éticas).

65 CICR, "Diplomacia humanitaria y comunicación", disponible en https://www.icrc.org/es/nuestras-actividades/diplomacia-humanitaria-y-comunicacion.

66 V. Massimo Marelli, "El sector humanitario y la piratería informática: perímetro cibernético y una estrategia de seguridad informática para la transformación digital de las organizaciones humanitarias internacionales", en este número de la *International Review*.

67 EPFL, "EPFL, ETH Zurich and the ICRC Leverage Science and Technology to Address Humanitarian Challenges", 10 de diciembre de 2020, disponible en https://essentialtech.center/engineering-humanitarian-aid-awards-six-epfl-ethz-icrc-projects/.

68 Sean Capitain, "The Red Cross Presses Silicon Valley to Fight Cyberwarfare", *Fast Company*, 10 de octubre de 2017, disponible en https://www.fastcompany.com/40476581/red-cross-could-silicon-valley-limit-cyberwar fare-if-governments-wont.

Al mismo tiempo, el diálogo privilegiado con el sector de la tecnología también es fundamental para comprender mejor su base intelectual. El creciente interés de las empresas tecnológicas en la colaboración con las organizaciones humanitarias deriva de la convicción de que las tecnologías digitales no solo hacen el bien, sino que también pueden ayudar a los actores humanitarios a satisfacer las necesidades de las poblaciones afectadas de manera eficiente y con efectos positivos duraderos. Sin embargo, la interacción puede deteriorarse fácilmente a causa del "determinismo tecnológico"[69] y de la "cultura del héroe emprendedor"[70]. Se ha observado que estos dos conceptos están estrechamente relacionados con el Área de la Bahía ya mencionada[71], donde existen dos creencias generalizadas: que la tecnología "produce buenos resultados para todos" y que "las nuevas tecnologías deberían desplegarse cuanto antes, aunque no se tenga una idea general de cómo funcionan ni de cuáles serán sus consecuencias para la sociedad"[72]. Esta es una de las dimensiones en juego cuando Jo Burton, citando a Nathaniel Raymond, recomienda al sector humanitario que evite "aceptar a ciegas las potenciales 'promesas de Silicon Valley'", ya que su tendencia a reducir los problemas complicados a soluciones tecnológicas es, sin duda, incompatible con las complejas situaciones que surgen en las zonas de conflicto. Estas suposiciones pueden tener repercusiones masivas al considerar la adopción de tecnologías en la acción humanitaria, y exigen una interacción crítica con el sector tecnológico, sus compañías y sus empleados, en todos los lugares dedicados al desarrollo de tecnología.

La naturaleza experimental de la interacción en el Área de la Bahía ilustra la posibilidad de entablar diálogos similares en otros centros de desarrollo de tecnologías digitales, que quizás influyan en las ciberoperaciones del futuro. Recientemente, el CICR ha fortalecido sus contactos tecnológicos en Japón[73], y seguramente hay margen para interacciones de este tipo en otros centros tecnológicos del mundo.

El multilateralismo y el desarrollo del derecho internacional

La creciente influencia del sector privado también trae consecuencias para el multilateralismo y el desarrollo del derecho, tema que se examina más a fondo en este número de la *International Review.* A la luz del rápido crecimiento del sector de la tecnología y del uso generalizado de las tecnologías digitales, el embajador Amandeep S. Gill, en su artículo "La variabilidad del papel de los

69 John Naughton, "Think the Giants of Silicon Valley Have Your Best Interests at Heart? Think Again", *The Guardian*, 21 de octubre de 2018, disponible en www.theguardian.com/commentisfree/2018/oct/21/think-the-giants-of-silicon-valley-have-your-best-interestsat-heart-think-again.

70 Daniela Papi-Thornton, "Tackling Heropreneurship", *Stanford Social Innovation Review*, 23 de febrero de 2016, disponible en https://ssir.org/articles/entry/tackling_heropreneurship.

71 Jasmine Sun, "Silicon Valley's Saviorism Problem", *The Stanford Daily*, 16 de febrero de 2018, disponible en www.stanforddaily.com/2018/02/16/silicon-valleys-saviorism-problem/.

72 J. Naughton, nota 69 *supra*.

73 NEC, "NEC and ICRC: A Blueprint for Ethical Technology Partnerships between the Private and Humanitarian Sectors", 11 de noviembre de 2020, disponible en www.nec.com/en/global/sdgs/innovators/project/article02.html.

foros multilaterales en la regulación de los conflictos armados en la era digital"[74], identifica los problemas estructurales que impiden a los foros multilaterales debatir cuestiones digitales de rápida evolución y producir oportunamente las medidas normativas y de política que se necesitan. Para Gill,

> [s]i bien las empresas privadas y la sociedad civil han desempeñado una función importante en lo que respecta al establecimiento de agendas y la formación de opiniones en algunos debates, frente a los actores estatales e interestatales más poderosos desempeñan un papel secundario. Esta asimetría de poder choca con la realidad de la tecnología digital. Por ejemplo, las plataformas digitales como Facebook, Alipay y WhatsApp posiblemente tengan más usuarios ("residentes virtuales") que las poblaciones de la mayoría de los países; operan infraestructuras casi mundiales; actúan como "policías de contenido" transfronterizos; y sus capitalizaciones en los mercados bursátiles superan ampliamente a las de otros sectores y a casi todos los productos internos brutos nacionales.

En su artículo, Gill subraya que "[s]i se desea que las normas relativas a las tecnologías digitales tengan algún efecto, la industria digital debe tomar parte en los debates sobre las respuestas de política y participar con los actores estatales en su implementación".

Esta afirmación también es aplicable al sector humanitario, sobre todo en lo que respecta al DIH y su desarrollo. En vista de las complejidades planteadas por el funcionamiento de las tecnologías y la rapidez de su evolución, y teniendo en cuenta que sus capacidades siguen siendo en gran parte desconocidas, la comunidad internacional y el sector humanitario deben encontrar nuevas formas de asegurar que las tecnologías innovadoras utilizadas como medios y métodos de guerra sean compatibles con el DIH.

Las tecnologías digitales y los medios y métodos de guerra

La segunda mitad de este número de la *International Review* se aparta del tema del uso de las tecnologías digitales para la asistencia humanitaria, previa evaluación de sus riesgos y beneficios, para centrarse en el uso de las nuevas tecnologías con fines destructivos en los conflictos armados.

A este respecto, el artículo de Frank Sauer[75] aborda las consecuencias de la falta de reglamentación de los sistemas de armas autónomas, en particular aquellos que dependen de la inteligencia artificial. Al describir las consecuencias de ese vacío jurídico, Sauer explica claramente tanto las dificultades para reglamentar los sistemas de armas autónomas como la imperiosa necesidad de hacerlo por razones éticas, jurídicas y de política. Según Sauer, es fundamental reglamentar la autonomía de los sistemas de armas mediante "la codificación de la obligación

74 V. Amandeep S. Gill, "La variabilidad del papel de los foros multilaterales en la regulación de los conflictos armados en la era digital", en este número de la *International Review*.

75 F. Sauer, nota 6 *supra*.

jurídicamente vinculante de conservar un control humano significativo sobre el uso de la fuerza".

Las nuevas aplicaciones de sensores y *software*, en especial la inteligencia artificial y los sistemas de aprendizaje automático, también conllevan consecuencias amplias para la adopción de decisiones en los conflictos armados. Pizzi, Romanoff y Engelhardt manifiestan que la inteligencia artificial y el aprendizaje automático "pueden ser extremadamente poderosos y generar información analítica y predictiva que supera cada vez más las capacidades humanas. Por lo tanto, pueden emplearse para reemplazar a los seres humanos en la toma de decisiones, sobre todo cuando los análisis deben realizarse con rapidez o en gran escala. En tales casos, los supervisores humanos a menudo pasan por alto los riesgos que plantean y la posibilidad de que causen daños graves a personas o grupos ya vulnerables"[76]. El documento de posición del CICR "La inteligencia artificial y el aprendizaje automático en los conflictos armados: un enfoque centrado en las personas", actualizado para este número de la *International Review* e incluido en la sección "Informes y documentos", es más cauteloso y destaca que "los sistemas de inteligencia artificial y aprendizaje automático siguen siendo herramientas que deben ponerse al servicio de agentes humanos y respaldar a los encargados de tomar decisiones, no reemplazarlos". Promueve un enfoque que sitúe las obligaciones jurídicas y éticas humanas en primer plano, a fin de "preservar el control y el criterio humanos al utilizar aplicaciones de inteligencia artificial y aprendizaje automático para aquellas tareas que pueden tener consecuencias graves para la vida de las personas, sobre todo cuando esas tareas y decisiones generan riesgos para la vida y son regidas por normas específicas del derecho internacional humanitario"[77]. Ambos documentos señalan las limitaciones técnicas de la inteligencia artificial que plantean cuestiones jurídicas. Pizzi, Romanoff y Engelhardt describen cómo la inteligencia artificial

> crea desafíos en materia de transparencia y de supervisión, dado que quienes diseñan e implementan esos sistemas a menudo no pueden "escudriñar su interior" para comprender cómo y por qué se tomó una decisión determinada. Este problema, descrito como una "caja negra", puede imposibilitar la rendición de cuentas efectiva en los casos en que estos sistemas causan daño, por ejemplo, cuando un sistema de inteligencia artificial adopta o apoya una decisión cuyos efectos son discriminatorios[78].

Las nuevas tecnologías digitales también pueden influir en las ciberoperaciones y en la guerra cibernética. La adopción de tecnologías digitales nuevas por las partes en un conflicto armado tiene efectos directos en los medios y métodos de la propia guerra y, por ende, en la aplicación e interpretación del DIH

76 M. Pizzi, M. Romanoff y T. Engelhardt, nota 10 *supra*.

77 V. CICR, "La inteligencia artificial y el aprendizaje automático en los conflictos armados: un enfoque centrado en las personas", en este número de la *International Review.*

78 M. Pizzi, M. Romanoff y T. Engelhardt, nota 10 *supra*.

en ese caso. En su artículo para este número de la *International Review,* Laurent Gisel, Tilman Rodenhäuser y Knut Dörmann[79] señalan que

> [e]l uso de ciberoperaciones durante los conflictos armados es hoy una realidad de esas situaciones y es probable que su importancia crezca en el futuro. Este fenómeno plantea una serie de preocupaciones en las sociedades de hoy, cada vez más dependientes de la cibernética, dado que las ciberoperaciones maliciosas pueden causar graves perturbaciones y daños a los seres humanos. [...] La comunidad internacional, las sociedades, y cada uno de nosotros a nivel individual, dependemos cada vez más de las herramientas digitales. Esta tendencia —que podría verse más acelerada aún por la pandemia de COVID-19 que se propaga al tiempo de escribir este artículo— aumenta nuestra dependencia del funcionamiento ininterrumpido de estas tecnologías, exacerbando nuestra vulnerabilidad a las ciberoperaciones.

Este último punto encuentra apoyo en los recientes hallazgos de Freedom House[80], que describe cómo los gobiernos del mundo han aprovechado la pandemia para expandir sus capacidades de vigilancia interna, utilizando, por ejemplo, aplicaciones de rastreo de contactos que recopilan información privada. Del mismo modo, el CyberPeace Institute[81] ha alzado la voz con respecto al creciente y alarmante número de ciberataques. Este fenómeno adopta una forma particular en el caso de las estructuras de salud porque, como señalan Gisel, Rodenhäuser y Dörmann, "el sector de la salud parece ser particularmente vulnerable a los ciberataques. Ese sector avanza hacia una mayor digitalización e interconectividad, lo cual aumenta su dependencia digital y su superficie de ataque"[82]. Estas tendencias también se destacan en el artículo escrito por Zhixiong Huang y Yaohui Ying[83]. Estos autores ofrecen una perspectiva convincente de la aplicación del principio de distinción al contexto cibernético, presentando las posiciones de los funcionarios chinos y las opiniones de los académicos chinos en este debate. Ponen de manifiesto que determinados elementos de la distinción, como los uniformes y las marcas distintivas, son impracticables o inviables en el mundo cibernético. Aunque el

79 L. Gisel, T. Rodenhäuser y K. Dörmann, nota 5 *supra*.

80 Adrian Shahbaz y Allie Funk, "The Pandemic's Digital Shadow", Freedom House, 2020, disponible en https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow.

81 CyberPeace Institute, "A Call to All Governments: Work Together Now to Stop Cyberattacks on the Healthcare Sector", 26 de mayo de 2020, disponible en https://cyberpeaceinstitute.org/call-for-government/.

82 A la luz de esta tendencia alarmante, el CICR se ha sumado a un llamamiento de los líderes mundiales en el que se exhorta a poner fin a los ataques contra la infraestructura de salud, sobre todo porque esos ataques pueden hacer peligrar la vida de personas civiles vulnerables. V. "Call by Global Leaders: Work Together Now to Stop Cyberattacks on the Healthcare Sector", *Humanitarian Law and Policy Blog*, 26 de mayo de 2020, disponible en https://blogs.icrc.org/law-and-policy/ 2020/05/26/call-global-leaders-stop-cyberattacks-healthcare/.

83 V. Zhixiong Huang y Yaohui Ying, "La aplicación del principio de distinción en el contexto cibernético: una perspectiva china", en este número de la *International Review*.

principio de distinción sigue siendo pertinente, los autores afirman que debería interpretarse de una manera apropiada para el ámbito cibernético.

Juntas, estas contribuciones a la *International Review* conjugan no solamente diversos perfiles de autores, sino también conjuntos de análisis diversos y multidisciplinarios que enriquecen la capacidad de este número de la revista de encarar el modo en que el DIH regula las tecnologías digitales en tiempo de conflicto armado.

Ámbito temático de esta edición de la *International Review* sobre "Las tecnologías digitales y la guerra"

Como ya se ha mencionado, los contenidos de esta edición de la *International Review* abordan los usos dobles de las tecnologías digitales: 1) para la acción y la asistencia humanitarias —previa evaluación de sus riesgos y beneficios— destinadas a asistir y proteger a poblaciones afectadas durante conflictos armados y otras situaciones de violencia, y 2) para la conducción de la guerra en los conflictos armados. Los artículos reunidos en este número también dan cuenta del creciente papel del sector privado —especialmente las empresas de alta tecnología— en la provisión de las plataformas que se usan para difundir información falsa, desinformación y discursos de odio y que influyen en el modo de compartir la información en contextos de crisis.

Al preparar esta edición, la *International Review* era consciente de que apenas estamos comenzando a elucidar los patrones y tendencias presentes en el modo en que las tecnologías digitales afectarán al mundo. Por esta razón, si bien este número temático dedicado a "Las tecnologías digitales y la guerra" abre la caja negra para mostrar cómo las tecnologías digitales determinan y son a su vez determinadas por los conflictos armados y otras situaciones de violencia, su contenido no es exhaustivo. Dicho de otro modo, nuestro entendimiento actual de las tecnologías existentes y emergentes sigue aumentando e identificando nuevos desafíos y oportunidades en torno a las tecnologías digitales que usamos, aceptamos y a las que, a veces, tememos.

Género, diversidad e inclusión en la *International Review*

Un parámetro esencial para la producción de esta edición fue la paridad de géneros y la inclusión de perfiles y pareceres diferentes. Las brechas de género en el sector de la tecnología son bien conocidas, dado que las mujeres representan menos del 35 % de la fuerza laboral del sector[84]. En lo que respecta a la diversidad, la mayoría de las grandes empresas tecnológicas[85] están pobladas por un grupo

84 Sam Daley, "Women In Tech Statistics for 2020 (and How We Can Do Better)", *Built In*, 13 de marzo de 2020, disponible en https://builtin.com/women-tech/women-in-tech-workplace-statistics.

85 Jonathan Ponciano, "The Largest Technology Companies in 2019: Apple Reigns as Smartphones Slip and Cloud Services Thrive", *Forbes*, 15 de mayo de 2019, disponible en www.forbes.com/sites/jonathanponciano/2019/ 05/15/worlds-largest-tech-companies-2019/.

casi homogéneo de hombres blancos jóvenes[86], procedentes de universidades estadounidenses prestigiosas[87] y con poca o ninguna formación en humanidades, ética o relaciones internacionales[88]. Asimismo, se ha afirmado que las propias tecnologías digitales muestran signos evidentes de discriminación racial y de género[89], al igual que los datos digitales, los cuales portan sesgos estructurales, puesto que representan y amplifican las discriminaciones sociales y las relaciones de poder existentes. El objetivo del equipo de la *International Review* era romper con esta tendencia al menos en cuanto a los perfiles de los autores presentados en este número. Sin embargo, en esta empresa tropezamos con ciertos obstáculos; mientras comenzábamos a producir este número temático a fines del invierno de 2019, el coronavirus nos golpeó como no lo hizo ningún otro virus en el último siglo[90].

Desde la *International Review*, constatamos los efectos de género de esta crisis en la composición de nuestro grupo de autores. Numerosas autoras cuya participación habíamos solicitado activamente no presentaron sus manuscritos a la revista. Esta tendencia se ha observado en todo el sector de la publicación académica: muchas académicas y autoras se han enfrentado con la doble carga de las tareas domésticas y el trabajo profesional, en una proporción mayor que la de sus homólogos masculinos. Como varias de nuestras autoras abandonaron el proyecto y nuestras invitaciones a presentar artículos recibieron un rechazo desproporcionado en este sentido, la *International Review* prorrogó el plazo de publicación con miras a lograr que el producto final no se viera dominado por un grupo demográfico. Como se ve en nuestra selección final, si bien lamentablemente no logramos alcanzar la paridad de género perfecta entre los autores, la brecha se sitúa en 0,82 (autoras a autores). La *International Review* asume el compromiso firme y activo de cerrar esta brecha en los números futuros[91]. Asimismo, seguimos trabajando en favor de una mayor diversidad en nuestras publicaciones. Recientemente, por ejemplo, la *International Review* ha dado la bienvenida a su nuevo Comité Editorial para el

86 Shelly Banjo y Dina Bass, "On Diversity, Silicon Valley Failed to Think Different", *Bloomberg Businessweek*, 3 de agosto de 2020, disponible en www.bloomberg.com/news/articles/2020-08-03/silicon-valley-didn-t-inherit-discrimination-but-replicated-it-anyway.

87 Avery Hartmans, "These 25 Universities Produce the Most Tech Employees", *Business Insider*, 2 de mayo de 2017, disponible en www.businessinsider.com/top-colleges-for-working-in-silicon-valley-2017-5.

88 Victor Lukerson, "The Ethical Dilemma Facing Silicon Valley's Next Generation", *The Ringer*, 6 de febrero de 2019, disponible en www.theringer.com/tech/2019/2/6/18212421/stanford-students-tech-backlash-silicon-valley-next-generation.

89 V., por ejemplo, Karen Hao, "An AI Saw a Cropped Photo of AOC. It Autocompleted Her Wearing a Bikini", *MIT Technology Review*, 29 de enero de 2021, disponible en www.technologyreview.com/2021/01/29/1017065/ai-image-generation-is-racist-sexist/; Ryan Steed y Aylin Caliskan, "Image Representations Learned with Unsupervised Pre-Training Contain Human-Like Biases", Carnegie Mellon University, 2021, disponible en https://arxiv.org/pdf/2010.15052.pdf.

90 Eskild Petersen *et al.*, "Comparing SARS-CoV-2 with SARS-CoV and Influenza Pandemics", *The Lancet Infectious Diseases*, 3 July 2020, disponible en www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30484-9/fulltext.

91 Como referencia, v. la nueva composición del Comité Editorial de la *International Review*, disponible en https://international-review.icrc.org/es/acerca-de/comite-editorial.

período 2021—2026, formado por un grupo diverso de 19 expertos de todas partes del mundo[92].

El elemento de la diversidad en la revista no solo se basa en los antecedentes de los autores, sino que además se enriquece con las perspectivas transversales y multidisciplinarias que estos aportan. Estos enfoques multidisciplinarios cobran una importancia cada vez mayor a la hora de comprender el modo en que los distintos profesionales, organizaciones y países dan cuenta de los efectos adversos de las tecnologías digitales en las crisis humanitarias, proponen medidas de mitigación y abordan los usos inéditos de las tecnologías digitales como medios y métodos de guerra.

El camino por seguir

Una de las conclusiones principales que surge en varios de los artículos presentados en este número de la *International Review* es la necesidad de evaluar y mitigar los riesgos presentes en la integración de las nuevas tecnologías digitales en la labor humanitaria a la hora de emprender procesos de transformación digital. Si bien es verdad que estas herramientas traen consigo ciertos beneficios, también plantean riesgos irreversibles; el uso de las tecnologías digitales en las crisis humanitarias tiene un "lado oscuro". Este tema también tiene otro aspecto: a medida que las tecnologías digitales evolucionan y se utilizan en conflictos armados y otras situaciones de violencia, existe la necesidad permanente de garantizar el respeto del DIH. Sin embargo, la pregunta sigue siendo: ¿qué camino deben seguir las organizaciones humanitarias para encarar la cuestión de las tecnologías digitales y la guerra?

Balthasar Staehelin, director de la Oficina de Datos y Transformación Digital de CICR, formula una reflexión perfecta sobre el futuro de las tecnologías digitales y la guerra, preguntándose: "¿Los datos son el 'nuevo petróleo' o el nuevo amianto? ¿Viviremos en un mundo de internet o de una internet balcanizada?"[93]. Sin embargo, como señala Staehelin, cualquiera sea la respuesta, en los próximos años y décadas "el CICR hará el máximo esfuerzo por adaptarse al impacto de la transformación y a su crecimiento exponencial con y para las poblaciones que pretende asistir en las zonas de guerra del mundo. La continuidad de su confianza en el CICR nos dirá si hemos conseguido aprovechar el enorme potencial de las nuevas tecnologías de manera responsable y para su bien".

En consonancia con este aspecto fundamental expuesto por Staehelin, la mayoría de las distintas cuestiones abarcadas en este número de la *International Review* se reducen a un requisito clave de la acción humanitaria: la confianza. En efecto, a lo largo de este número, la confianza emerge como la columna vertebral de la transformación digital en el sistema humanitario. Sin embargo, no existe un método rápido para crearla. Las organizaciones humanitarias obtienen su acceso humanitario sobre la base de la confianza que crean a través del trabajo cotidiano

92 Ibíd.

93 Reflexión de Balthasar Staehlin expresada a los autores de este editorial.

con las comunidades y las autoridades locales. Siguiendo la misma lógica, todas las partes interesadas en utilizar la "tecnología para el bien" deberían prestar especial cuidado y atención a la forma en que las tecnologías digitales afectan los lazos de confianza.

Con la mirada puesta en el futuro, el proceso de sumarse a la transformación digital no se debe limitar a la adopción de tecnologías nuevas; también es preciso asegurar que estas refuercen los lazos de confianza que el sector humanitario construye con las poblaciones afectadas, ofreciéndoles opciones nuevas para garantizar la respuesta a sus necesidades. Con tal fin, esperamos que este número de la *International Review* inspire el diseño de estrategias de transformación digital innovadoras, centradas en las personas a las que se desea prestar servicios y elaboradas en colaboración con estas.