INTERNATIONAL REVIEW of the Red Cross

Preguntas y respuestas: Operaciones humanitarias, difusión de información perjudicial y protección de datos

Entrevista a Delphine van Solinge, asesora de protección del CICR sobre riesgos digitales para las poblaciones durante los conflictos armados, y Massimo Marelli, jefe de la Oficina de Protección de Datos del CICR

En esta oportunidad, la International Review *entrevista a Delphine van Solinge y a Massimo Marelli, del Comité Internacional de la Cruz Roja (CICR). Van Solinge es la referencia del CICR para saber cómo afectan a las poblaciones que viven en contextos de conflicto las tecnologías digitales y la difusión de información perjudicial y qué significa esto para la acción humanitaria. Con este propósito, su departamento se dedica a explorar, en nombre del CICR y a través de asociaciones con otras organizaciones, cómo mitigar los riesgos que las tecnologías digitales llevan a los contextos humanitarios y cómo garantizar las respuestas de protección pertinentes en la era digital. Marelli es jefe de la Oficina de Protección de Datos del CICR. Desde que se unió al CICR, la Institución ha aprobado nuevos modos para realizar sus actividades operacionales,*

garantizando que los datos de las personas afectadas a las que asiste, así como los de sus empleados, estén perfectamente protegidos.
Durante la entrevista, Van Solinge y Marelli hablan de cómo sus departamentos se complementan y se refuerzan entre sí, formando dos caras de la misma moneda respecto de cómo la información y los datos digitales pueden emplearse para introducir cambios positivos y cómo pueden utilizarse indebidamente en entornos humanitarios. Marelli hace hincapié en cómo las organizaciones humanitarias procesan, protegen y usan los datos y la información digital. Van Solinge explica cómo a través de la información errónea, la desinformación y el discurso de odio puede manipularse la información y difundirse por medio de las tecnologías digitales, en especial, en la era de la COVID-19, cuando las poblaciones dependen más de las tecnologías digitales. Entre otras cuestiones, analizan cómo pueden usarse adecuadamente las tecnologías digitales, qué consideraciones éticas deben tener en cuenta las organizaciones humanitarias y cuáles son las formas posibles de colaboración futura entre los sectores público y privado en esta materia.

Palabras clave: difusión de información perjudicial, información inadecuada, desinformación, discurso de odio, redes sociales, COVID-19, protección de datos, no causar daño, metadatos humanitarios.

***

¿Qué significa para el CICR la "militarización de la información"? ¿En qué difiere del uso indebido de la información durante los conflictos armados y otras situaciones de violencia? ¿Cómo se relacionan el principio de "no causar daño" y la labor de la Oficina de Protección de Datos con la "militarización de la información"?

Delphine van Solinge: Antes que nada, es importante subrayar que la frase "militarización de la información" es inadecuada en varios sentidos, en particular, desde el punto de vista jurídico. Por ejemplo, está la cuestión de si, en términos jurídicos, la información puede convertirse en un arma, y de ser así, ¿cómo y cuándo? Por ese motivo, el CICR prefiere hablar de difusión de información perjudicial, término que abarca la información errónea, la desinformación y el discurso de odio (IDO), en sus distintas facetas.

Hace tiempo que el CICR observa con preocupación los casos en los que la información y los sistemas de comunicación digitales se usan de forma tal de generar nuevos o mayores riesgos humanitarios para las poblaciones afectadas: las personas internamente desplazadas, los migrantes, las personas detenidas y las minorías, así como el personal y los voluntarios humanitarios. A falta de un término más adecuado, el CICR emplea los términos información errónea, desinformación y discurso de odio (IDO) para referirse en general a ese fenómeno, si bien reconoce que la información puede utilizarse con otros fines o sin que implique un aumento del riesgo humanitario (como en las operaciones que tienen consecuencias negativas solo para las fuerzas adversarias). En este sentido, las consecuencias humanitarias

pueden tener que ver con el desplazamiento; la muerte; la desaparición; la pérdida o la destrucción de bienes; la pérdida de ingresos; el daño físico, mental/psicológico y social; la estigmatización; la separación de familiares; o la imposibilidad de acceso a servicios como la educación, la salud, el alojamiento o los alimentos. Las consecuencias humanitarias pueden abarcar también la creación o la agudización de necesidades humanitarias existentes, por ejemplo, alojamiento, alimentos y otros artículos, asistencia de salud, apoyo psicológico y psicosocial, apoyo económico, acceso a los servicios, acceso a información oportuna y relevante del ámbito local, servicios/asesoramiento jurídico o acceso a internet. El IDO puede adoptar la forma de información errónea, desinformación, rumores virales, discurso de odio digital, propaganda en línea, entre otras[1].

El modo en que se emplea la información no basta por sí solo para "causar" daño. En cambio, el "potencial" de causar daño puede intensificarse cuando se combina con la dinámica social, cultural e histórica subyacente; con las tensiones sociales o políticas existentes; con el desconocimiento de las nuevas tecnologías o con la falta de pensamiento crítico al buscar información en línea; o con la inexistencia de fuentes fiables y precisas con las que triangular información, entre otros factores.

Cabe preguntarse cuál es la diferencia con lo que ocurría antiguamente. La historia ofrece numerosos ejemplos de sistemas de información y comunicación que han demostrado su capacidad para hacer daño, como es el caso de Radio Mille Collines en Ruanda[2]. Lo que ha cambiado es el tipo de canal que se utiliza para difundir la información a escala mundial. Las tecnologías digitales, y las redes sociales en particular, han aumentado la velocidad, la escala y el impacto con los que la información puede difundirse y tener repercusiones en distintos públicos. La mayor penetración de internet, la disponibilidad de dispositivos inteligentes y las redes sociales son herramientas poderosas para que las personas compartan información y estén conectadas, pero también para agravar la violencia y el conflicto, como ilustra el aumento del discurso de odio en Facebook en Myanmar. Estas nuevas variables han afectado la forma en que la información puede considerarse un medio para producir daño civil.

1 Para leer más sobre estos términos, v. Peter Singer y Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, Houghton Mifflin Harcourt, Boston, Massachusetts, 2018, disponible en www.likewarbook.com; Mark Silverman, "Book Review: *LikeWar: The Weaponization of Social Media*", *International Review of the Red Cross*, vol. 101, n.º 910, 2019, disponible en https://international-review.icrc.org/sites/default/files/reviews-pdf/2019-12/irrc_101_910_21.pdf; John Mingers y Craig Standing, "What is information? Toward a theory of information as objective and veridical", *Journal of Information Technology*, vol. 33, n.º 3, 2018, disponible en https://link.springer.com/article/10.1057/s41265-017-0038-6.

2 Radio Mille Collines, también llamada Radio Télévision Libre des Mille Collines, era una radio de Ruanda que difundió información errónea y desinformación entre el 8 de julio de 1993 y el 31 de julio de 1994. La propaganda falsa emitida desempeñó un papel fundamental en la incitación del genocidio que tuvo lugar en Ruanda en 1994 contra el pueblo tutsi. Para más información, v. Elizabeth Baisley, "Genocide and constructions of Hutu and Tutsi in Radio Propaganda", *Race and Class*, vol. 55, n.º 3, 2014, disponible en https://journals.sagepub.com/doi/abs/10.1177/0306396813509194.

Massimo Marelli: Pienso que existe una relación entre lo que hacemos en la Oficina de Protección de Datos y lo que ha expresado Delphine. En nuestra labor con la protección de datos, adoptamos un enfoque similar: no se trata solo de los datos, sino también de cómo se los usa o, posiblemente, de cómo se los usa con fines indebidos. La Oficina de Protección de Datos se asegura de que los datos personales de los beneficiarios, los interlocutores y el personal del CICR estén protegidos y de que no se quiebre el vínculo fundamental de confianza con la organización y dentro de ella. En este contexto, "no causar daño" significa reconocer que una protección deficiente de los datos personales de los beneficiarios, los interlocutores y el personal del CICR podría ser sumamente perjudicial tanto para las personas afectadas como para la viabilidad de las operaciones de la Institución. La protección de datos como instrumento para "no causar daño en un entorno digital"[3] se vincula con su capacidad de proporcionar una lente a través de la cual se pueden analizar los flujos de datos generados por el uso de las tecnologías y saber qué nuevas partes interesadas pueden estar involucradas, los riesgos que pueden generarse y las formas posibles de mitigar o prevenir esos riesgos. Dicho esto, la protección de datos implica mucho más que "no causar daño": se trata de garantizar el respeto de los derechos y la dignidad de las poblaciones afectadas cuando procesamos sus datos, poniendo a las personas en primer lugar. También se trata de rendir cuentas ante las poblaciones afectadas sobre la base de normas claras.

¿Podrían explayarse acerca de por qué las organizaciones humanitarias deben ocuparse de la cuestión de la difusión de información perjudicial y de la protección de datos?

Massimo Marelli: Tanto la protección de datos como la lucha contra la difusión de información perjudicial forman parte del cometido más amplio de protección del CICR. Asimismo, ambas áreas de actividad son fundamentales para que el CICR mantenga la confianza de las poblaciones afectadas y de las partes con las que entabla diálogos confidenciales. En materia de protección de datos, además de las graves consecuencias para los titulares de los datos, una filtración en el CICR o en cualquier otra organización humanitaria podría socavar la confianza en el sector y debilitar su capacidad de acceder y asistir a quienes más necesitan de sus servicios.

El uso que hace el CICR de los datos biométricos en los ámbitos forense y de restablecimiento del contacto entre familiares es un ejemplo de cómo la protección de datos juega un papel en la labor operacional de una organización humanitaria y revela por qué las organizaciones humanitarias deben prestar atención a la protección de datos. El CICR adoptó su política de datos biométricos en agosto de 2019 con el objeto de abordar los problemas urgentes de protección de datos que plantea el uso de datos biométricos –huellas dactilares, reconocimiento

3 CICR, *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*, 2018, disponible en www.icrc.org/en/download/file/85089/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf.

facial y ADN, entre otros–, que son especialmente sensibles porque, una vez que se recogen, si se los conserva, se crea un registro permanente identificable de la persona a la que pertenecen[4]. Esto puede crear un problema en contextos humanitarios, donde las personas quizá no deseen que se las identifique de forma permanente, en especial, si existe el riesgo de que la información caiga en las manos equivocadas. La política de datos biométricos es una respuesta al creciente interés interno en el potencial que esos datos podrían tener para las operaciones del CICR y logra un equilibrio entre facilitar su uso responsable y abordar los riesgos inherentes a la protección de datos. La política de datos biométricos ayuda a planificar aspectos de la transformación digital de la Agencia Central de Búsquedas del CICR, que está desarrollando nuevas herramientas para aumentar nuestra capacidad de determinar la suerte y el paradero de las personas desaparecidas y, en colaboración con los asociados del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja [el Movimiento], restablecer el contacto entre familiares. Está incluido en esa política el posible uso de la tecnología de reconocimiento facial para hallar coincidencias entre fotografías de personas desaparecidas y personas buscadas, y el uso de inteligencia artificial para localizar personas en las bases de datos del CICR y de sus asociados humanitarios. El fuerte compromiso con los protocolos de protección de datos será fundamental para generar confianza en la integridad, la seguridad y el empleo de esas herramientas.

Delphine van Solinge: Lo mismo se aplica si pensamos en la difusión de información perjudicial, que se realiza por medio del IDO. La forma en que tienen lugar esas prácticas y dinámicas afecta nuestra labor humanitaria de protección. Si bien los fenómenos en sí no son nuevos y su potencial para causar daño está bastante consolidado, la rapidez de la digitalización –en los contextos operacionales del CICR y en otros contextos– ha incrementado la velocidad con la que se puede difundir la información perjudicial, y con la que se puede llegar a distintos públicos e influir en ellos. Los rumores ya no se limitan a una región en particular; las fotos y los videos pueden falsificarse rápidamente, a un bajo costo; y las personas y las comunidades pueden ser identificadas y convertirse en objetos de ataque.

Myanmar, Sudán del Sur y Etiopía[5] son ejemplos que muestran que los fenómenos relativos al IDO, en particular, en las redes sociales, desempeñan un papel cada vez más importante en contextos asolados por la violencia y la guerra. ¿Qué significa esto? Básicamente, significa que las organizaciones humanitarias se enfrentan, cada vez con mayor frecuencia, a prácticas y dinámicas que se valen de las tecnologías de la información y la comunicación, que pueden ser muy perjudiciales. Esas prácticas tienen la capacidad de desestabilizar entornos de por sí frágiles, aumentar la vulnerabilidad de las personas y contribuir a agravar las

4 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.

5 En esos contextos, se han utilizado las redes sociales como Facebook y Twitter para difundir noticias falsas, rumores y discursos de odio que han exacerbado las tensiones y generado actos de violencia en el terreno.

consecuencias humanitarias. Si no logramos comprender e identificar los factores de riesgo cuando elaboramos nuestra respuesta humanitaria, podríamos pasar por alto algunos daños o dar una respuesta parcial a las necesidades de las personas afectadas.

También tenemos que entender que el IDO puede afectar directamente las respuestas operacionales y la credibilidad de las organizaciones humanitarias. ¿Qué ocurriría si el CICR se convirtiera en el objetivo de una campaña de desinformación coordinada en un país azotado por la guerra? Nuestra credibilidad podría verse empañada, con lo que perderíamos la confianza de las personas afectadas; podrían denegarnos el acceso a las zonas de conflicto, con lo que se nos impediría prestar protección y asistencia a las poblaciones en el terreno; y hasta podríamos ser blanco de ataques.

Si estamos de acuerdo en que la difusión de información perjudicial puede ser un vector o un factor que contribuya a aumentar la vulnerabilidad de las personas, causar daño a la población civil o dañar la imagen o poner en riesgo la seguridad de las organizaciones humanitarias, tendremos que estar atentos a este fenómeno.

¿Qué problemas plantea la difusión de información perjudicial al sector humanitario? También se habla mucho de las dificultades que enfrentan las organizaciones humanitarias en términos de recopilación y protección de metadatos humanitarios. ¿Podrían comentarnos los riesgos que implica recopilar y proteger estos metadatos?

Delphine van Solinge: En lo que respecta a la primera pregunta, le diré que la difusión de información perjudicial trae aparejados muchos problemas, pero aquí me centraré en tres.

En primer lugar, las amenazas del IDO no se generan de forma localizada. No se originan en un grupo de personas sentadas en un búnker que tienen una capacidad extraordinaria de producir contenido perjudicial o de crear nuevas formas de difundir información falsa. En la era digital, cualquier persona con conexión a internet puede consumir, crear y compartir contenido y, de ese modo, convertirse en un actor que difunde información que causa daño, sin siquiera saberlo. En este sentido, en algunos casos, no se necesita hacer demasiado para conseguir resultados a la hora de desinformar o dar información falsa a un público potencialmente numeroso. Con un video de dos minutos de duración, filmado y editado con un dispositivo inteligente y publicado en las redes sociales, se puede alcanzar un efecto enorme. Todos hemos visto los videos de *flash mob*, cuyo concepto es similar: con un solo mensaje se consigue tener a muchísimas personas bailando en la Estación Central de Amberes[6]. Además, la disponibilidad de herramientas y *malware* a precios relativamente bajos facilita enormemente el trabajo de quienes buscan causar daño. Esto puede dar origen a un conjunto de

6 El video del baile *flash mob* al que se hace referencia está disponible en www.youtube.com/watch?v=7EYAUazLI9k.

interrogantes jurídicos respecto de la responsabilidad, la rendición de cuentas y la participación en las hostilidades.

En segundo lugar, también sabemos que el IDO no se detecta ni se verifica con facilidad por medios convencionales. En la marea de noticias e información que nos inunda, lleva tiempo y experiencia desarrollar un ojo experto. Además de la complejidad, está la dificultad de medir el impacto del IDO, que, a veces, puede ser difuso o intangible. Por ejemplo, ¿cómo habría de medirse la pérdida de confianza? ¿Cómo se determinaría la relación entre las actividades virtuales y sus consecuencias en el mundo real? Distintos académicos y organizaciones sin fines de lucro han estudiado en detalle los múltiples aspectos de la "militarización de la información", pero rara vez dirigen la atención a países afectados por la guerra y la violencia. La comunidad humanitaria está tomando conciencia poco a poco de los posibles riesgos que entrañan el IDO y la difusión de información perjudicial, pero aún tiene dificultades para determinar cómo integrar esa nueva dimensión en su labor.

Por último, la comunicación digital y el IDO van acompañados de un nuevo conjunto de actores con funciones y responsabilidades diversas, como los medios de comunicación y el sector privado. La cuestión de cómo entablar un diálogo valioso con esos actores, más allá de promover nuestras actividades humanitarias, es algo muy nuevo para nosotros.

Massimo Marelli: Creo que, al igual que en el caso de la difusión de información perjudicial, la protección y el almacenamiento de metadatos por las organizaciones humanitarias plantean una serie de dificultades. Pero antes quisiera hacer una aclaración terminológica. Los metadatos son datos referidos a otros datos. Eso incluye la información sobre comunicaciones, como quién se puso en contacto con quién y cuándo, y los rastros digitales que quedan cuando los dispositivos, las aplicaciones y las redes interactúan entre sí.

¿Por qué es importante reunir y proteger los metadatos? Porque los metadatos dicen mucho acerca de sus titulares. Los metadatos son utilizados por las empresas de publicidad virtual para identificar perfiles de usuarios en internet y por las agencias de seguridad para identificar personas y grupos de interés. En un contexto humanitario, los desafíos y los riesgos de reunir metadatos tienen que ver con cómo pueden usarse para conocer la ubicación, los movimientos y las interacciones de las organizaciones humanitarias y las poblaciones que reciben asistencia humanitaria, información que podría violar la confidencialidad y utilizarse con fines no humanitarios, por ejemplo, por las partes en un conflicto. No obstante, en algunos contextos, los metadatos pueden ser sumamente útiles para las organizaciones humanitarias, pues les permiten conocer mejor cómo se usan sus servicios y dónde se los necesita más. Los metadatos también pueden ayudar a determinar la suerte que han corrido las personas desaparecidas en entornos virtuales. La ubicuidad de este tipo de información es lo que hace que los riesgos vinculados con la protección de datos sean tan difíciles de gestionar. En este ámbito, el CICR se ha asociado con Privacy International para ayudar a crear

conciencia sobre el "problema de los metadatos humanitarios"[7] y ha colaborado con Brussels Privacy Hub en la elaboración de una guía para la protección de datos y la gestión de esos riesgos[8].

¿Cómo afecta una pandemia como la de COVID-19 a los casos y la prevalencia de la difusión de información perjudicial y a la necesidad de estar atentos a la protección de datos en el sector humanitario?

Delphine van Solinge: Durante los brotes de enfermedades contagiosas, a menudo se observa un incremento del IDO. Las ideas sobre la pandemia se nutren de nuestras emociones más intensas y profundas, induciendo el miedo y creando el pánico. Con una mayor incertidumbre y angustia, las personas buscan información para obtener respuestas. Las noticias que se publican en las redes sociales se difunden más rápido y llegan a un número mayor de personas con niveles muy bajos de selección y verificación. En este contexto, la información puede manipularse con fines económicos, ideológicos o políticos.

En el caso de la COVID-19, en numerosas plataformas digitales y sitios web, se han observado casos de información errónea, desinformación y rumores virales. La difusión de información ha alcanzado niveles tales que se la puede calificar de "infodemia"[9]. Algunos contenidos no verificados relativos a enfermedades contagiosas, amenazas inminentes y muerte pueden anular parte del costado racional de las personas y aumentar la polarización en las sociedades. En algunos casos, esas formas de pensar pueden manifestarse como comportamientos extremos, posiblemente violentos, incluidos los ataques físicos directos al personal o los establecimientos sanitarios, los disturbios reprimidos por la policía o el ejército mediante el uso de la fuerza, etc. La difusión de información engañosa o errónea a través de las redes sociales sobre centros de aislamiento, por ejemplo, ha fomentado la incertidumbre y el temor, incitando a los ciudadanos a atacar vehículos que trasladan pacientes y a bloquear evacuaciones.

La mayor difusión de desinformación o de información errónea en las redes sociales también puede deberse a que ya no hay administradores en las plataformas que ocupen de eliminar el contenido engañoso, tarea que se ha automatizado. Si bien la inteligencia artificial y otros sistemas automáticos tienen perspectivas prometedoras, su capacidad para eliminar contenido engañoso aún es insuficiente.

7 CICR, "Los rastros digitales podrían poner en peligro a las personas que reciben asistencia humanitaria: informe del CICR y Privacy International", 7 de octubre de 2018, disponible en https://www.icrc.org/es/document/los-rastros-digitales-podrian-poner-en-peligro-las-personas-que-reciben-asistencia.

8 CICR, *Manual sobre protección de datos en la acción humanitaria*, 23 de agosto de 2017, disponible en https://www.icrc.org/es/publication/manual-sobre-proteccion-de-datos-en-la-accion-humanitaria.

9 V., p. ej., Departamento de Comunicación Global de la ONU, "UN tackles 'Infodemic' of misinformation and cybercrime in COVID-19 crisis", 31 de marzo de 2020, disponible en www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19; Farah Lalani y Juraj Majcin, "Inside the battle to counteract the COVID-19 'infodemic'", Foro Económico Mundial, 9 de abril de 2020, disponible en www.weforum.org/agenda/2020/04/covid-19-inside-the-battle-to-counteract-the-coronavirus-infodemic/.

La información errónea y la desinformación pueden afectar a las organizaciones humanitarias, en particular, a aquellas que son cercanas, o que se percibe que son cercanas, a países con números elevados de contagios de COVID-19. La población local puede creer que los trabajadores humanitarios extranjeros son portadores del virus, lo que podría tener consecuencias de gran alcance para la seguridad y las capacidades operacionales.

¿Qué ha hecho el CICR hasta el momento con respecto al IDO en las operaciones humanitarias y a la aplicación del principio de "no causar daño" en las actividades relativas a la protección de datos?

Delphine van Solinge: Con respecto a las actividades operacionales y el IDO, en diciembre de 2018, el CICR organizó un simposio sobre riesgos digitales que se celebró Londres[10]. El objetivo de la conferencia era comprender cómo las tecnologías digitales y la forma en que se las usa afectan a las poblaciones civiles en los conflictos armados y conocer sus implicaciones para la protección y la respuesta humanitaria.

Basándose en algunas de las conclusiones clave del simposio, el CICR implementó un programa de trabajo sobre el IDO. La primera etapa de este programa, que se llevó a cabo en 2019, se centró en entender los obstáculos y los problemas principales que impiden que el personal del CICR incorpore las cuestiones relativas al IDO en su análisis y su labor. La investigación tuvo lugar en las delegaciones del CICR de Sri Lanka y de Etiopía. Teniendo en cuenta algunas de las necesidades iniciales identificadas durante el estudio, hemos elaborado una guía práctica sobre el IDO para ayudar al personal del CICR sobre el terreno a conocer y familiarizarse con el concepto.

Por último, estamos por crear una red de investigación sobre el IDO con académicos y organizaciones humanitarias interesadas. Nuestro objetivo es realizar una investigación empírica sobre el IDO y sus consecuencias humanitarias, con vistas a desarrollar los fundamentos conceptuales que necesitarán las organizaciones humanitarias para abordar la cuestión. Así, se podrán definir las implicaciones del IDO para la protección y la labor humanitaria. La investigación también contribuirá a determinar cuál es la mejor forma de incorporar el IDO al análisis del CICR y otras organizaciones humanitarias, y a sus respuestas frente a las personas afectadas.

Massimo Marelli: La labor que estamos realizando en protección de datos también está orientada a analizar los riesgos de que se cause daño durante el curso de una actividad operacional específica y luego adoptar medidas para mitigarlos, por ejemplo, no continuar con la operación o volver a idear una estrategia operacional. Con respecto a "no causar daño", en 2015 adoptamos numerosas salvaguardias específicas en las *Normas del CICR en materia de protección de datos personales* para

10 El informe del Simposio sobre riesgos digitales en los conflictos armados está disponible en www.icrc.org/fr/publication/4403-symposium-report-digital-risks-armed-conflicts.

reducir el riesgo del uso o el acceso no autorizados a los datos personales mediante normas y requisitos aplicables al procesamiento de datos en toda la organización[11]. Si el CICR considera el uso de nuevas tecnologías o de un procesamiento de datos más riesgoso, debe realizar evaluaciones de impacto relativas a la protección de datos a fin de identificar y mitigar los riesgos de daño[12]. Las *Normas del CICR en materia de protección de datos personales* también exigen que el CICR adopte un enfoque de "protección de datos desde el diseño"[13] para limitar la recopilación de datos personales a los que sean necesarios para la operación y garantizar el respeto de los derechos de los titulares de los datos.

Como comunidad humanitaria, ¿qué podemos hacer para comenzar a ocuparnos de los problemas que plantea la difusión de información perjudicial (IDO) y la protección de datos?

Delphine van Solinge: Para comenzar a ocuparnos de los problemas que plantea la difusión de información perjudicial, tenemos un conocimiento más profundo del IDO y sus consecuencias humanitarias, una orientación estratégica con fundamentos conceptuales sólidos y la voluntad de dialogar con nuevos actores en terrenos desconocidos.

Sin embargo, para eso, debemos tener en mente lo siguiente: si comenzamos a desarrollar soluciones aisladas y sin prioridades compartidas, el impacto será limitado y estaremos desperdiciando energía. A muchos de nosotros, nos preocupa el IDO; es un problema complejo en el que participan e interactúan numerosos sistemas, dinámicas y actores diferentes. Para abordar la cuestión, tenemos que adoptar un enfoque sistémico.

Por último, tenemos que desarrollar los fundamentos conceptuales de la difusión de información perjudicial; entre ellos, un conocimiento claro e integral de los riesgos y los daños que pueden representar las tecnologías digitales de la información y sus usos para las poblaciones afectadas y las organizaciones humanitarias, así como de la forma de responder a esos riesgos y mitigarlos. Es necesario, por lo tanto, desarrollar una teoría del daño digital y, para vincular la teoría con la práctica, necesitamos un marco conceptual. Dada la envergadura de esta tarea, es necesario asociarse y aunar fuerzas, por ejemplo, con otras organizaciones, estudiosos e instituciones académicas.

Massimo Marelli: Coincido con Delphine: tenemos que romper el aislamiento e identificar prioridades compartidas por todo el sector humanitario para ocuparnos efectivamente de la difusión de información perjudicial y de la protección de datos. En cuanto a la protección de datos, la utilización de las nuevas

11 CICR, *Normas del CICR en materia de protección de datos personales*, 2015, disponible en https://www.icrc.org/es/publication/normas-del-cicr-en-materia-de-proteccion-de-datos-personales.

12 Ibíd.; v. también CICR, "Policy on the processing of biometric data by the ICRC", 28 de agosto de 2019, disponible en www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf.

13 CICR, nota 11 *supra*.

tecnologías digitales por parte del sector humanitario y los riesgos específicos que estas entrañan han llevado al CICR a pensar seriamente qué quiere decir "no causar daño en entornos digitales". Para eso, nos hemos dedicado a formar asociaciones estratégicas con organizaciones y proveedores de servicios a los que les preocupa la protección de datos[14] y hemos implementado la "diplomacia digital" para abordar problemas específicos del sector humanitario. Entre otras cosas, realizamos esfuerzos para salvaguardar el "espacio digital humanitario"[15], garantizando que los datos recopilados con propósitos humanitarios solo puedan ser utilizados con ese fin, en consonancia con los principios de neutralidad e independencia.

Además de garantizar que se incorporen las normas sobre protección de datos a los acuerdos de asociación en el plano operacional, el CICR ha colaborado estrechamente, por ejemplo, con el Movimiento para elaborar normas de protección de datos para el restablecimiento del contacto entre familiares, que están representadas en un Código de Conducta del Movimiento[16]. Las cuestiones relativas a la protección de datos también fueron un tema destacado en la XXXIII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, celebrada en diciembre de 2019[17], donde se analizó en profundidad el principio de no causar daño en entornos digitales en el contexto de "Evolución de las vulnerabilidades" y "Confianza en la acción humanitaria". La Conferencia aprobó, además, una resolución innovadora sobre restablecimiento del contacto entre familiares y protección de datos que reconoce que la recopilación y uso de datos humanitarios con fines no humanitarios socava la confianza en las organizaciones humanitarias y pone en riesgo su capacidad operacional. La resolución "insta a los Estados a

14 P. ej., el CICR y Brussels Privacy Hub han trabajado juntos en el proyecto de protección de datos en la acción humanitaria, destinado al personal de las organizaciones humanitarias responsable del procesamiento de datos personales como parte de las operaciones humanitarias, en especial, a aquellas personas encargadas de asesorar en materia de normas de protección de datos y de aplicar dichas normas. Entre los resultados del proyecto, se encuentra el *Manual sobre protección de datos en la acción humanitaria*, disponible en https://www.icrc.org/es/publication/manual-sobre-proteccion-de-datos-en-la-accion-humanitaria. El CICR ha colaborado o hecho consultas con expertos de numerosas organizaciones para su trabajo de protección de datos, incluidos Brussels Privacy Hub, la Autoridad Suiza de Protección de Datos, el Supervisor Europeo de Protección de Datos, la Oficina del Alto Comisionado de las Naciones Unidas para los Refugiados, la Organización Internacional para las Migraciones, la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja, la Oficina de Coordinación de Asuntos Humanitarios de las Naciones Unidas, la Universidad de Yale, Privacy International, la Asociación Francófona de Autoridades de Protección de Datos Personales, el Instituto Federal Suizo de Tecnología de Lausana, Médicos sin Fronteras y la Autoridad de Protección de Datos de Senegal.

15 Para un análisis más minucioso del papel del CICR en la salvaguardia del "espacio digital humanitario", v. Massimo Marelli, "Hacking humanitarians: Moving towards a humanitarian cybersecurity strategy", *Humanitarian Law and Policy Blog*, 16 de enero de 2020, disponible en https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/.

16 Red de Vínculos Familiares del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja, *Código de Conducta sobre protección de datos*, noviembre de 2015, disponible en https://www.icrc.org/es/document/codigo-conducta-proteccion-datos-personales-actividades-restablecimiento-contactos-familiares.

17 Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, "XXXIII Conferencia Internacional: De un vistazo", disponible en https://rcrcconference.org/es/about/33rd-international-conference/.

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"[18].

¿Podrían proporcionar ejemplos de cómo la información digital y los sistemas de comunicación pueden utilizarse de manera beneficiosa?

Delphine van Solinge: Las tecnologías digitales de la información brindan oportunidades para mejorar las respuestas humanitarias a las poblaciones afectadas, entre otras cosas, facilitando la comunicación entre el personal humanitario y las personas afectadas por una crisis o usando formas innovadoras de obtener y utilizar información pertinente que sea útil para idear respuestas. Los defensores de los derechos humanos y los profesionales humanitarios utilizan el mayor conocimiento de las situaciones y la información de aplicación práctica que ofrece la era digital. De los muchos ejemplos existentes, daré solo algunos: se utilizan sensores remotos para amplificar la capacidad de alerta temprana de conflicto y para documentar abusos de los derechos humanos; se aprovechan las soluciones de datos móviles para hacer un seguimiento de las condiciones, los perfiles y las rutas de tránsito de las poblaciones de migrantes y refugiados; se extraen metadatos de los registros de llamadas para comprender cómo se propagan las enfermedades contagiosas; se estudian las redes sociales para analizar actitudes y rastrear rumores en contextos frágiles; y, desde luego, se despliegan robots aéreos para vigilar lugares destruidos y supervisar infraestructura crítica.

En el caso de la pandemia de COVID-19, las herramientas digitales, la inteligencia artificial[19] y el análisis de *big data* se usan en distintos contextos para dar apoyo a las respuestas de asistencia de salud. Pueden ayudarnos a recoger, analizar y transmitir información crítica a fin de organizar recursos y capacidades sanitarios, acelerar las cadenas de logística y adquisición de material sanitario o gestionar la seguridad pública durante el confinamiento.

Las tecnologías digitales de la información pueden ser valiosas para el intercambio de información clave y, por lo tanto, para ayudar a los investigadores médicos y epidemiológicos. En cuanto a la prevención y la sensibilización, durante la crisis causada por la COVID-19, también se han usado ampliamente aplicaciones para compartir información relevante y precisa con las poblaciones afectadas. Hay distintos modelos, interfaces, contenidos y niveles de seguridad y de cumplimiento de las normas de privacidad. En general, cuando provienen de organismos oficiales de salud pública y están validadas por ellos, esas aplicaciones ayudan a mejorar la

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

19 Shana Lynch, "Artificial intelligence and COVID-19: How technology can understand, track, and improve health outcomes", *Stanford Institute for Human-Centered Artificial Intelligence Blog*, 1 de abril de 2020, disponible en https://hai.stanford.edu/blog/artificial-intelligence-and-covid-19-how-technology-can-understand-track-and-improve-health.

sensibilización y el nivel de información de la población, que estará mejor preparada para adoptar las medidas adecuadas en materia de prevención y bienestar.

En total, existen muchas herramientas digitales que están siendo promovidas y analizadas en el contexto de la respuesta a la COVID. Pueden desempeñar funciones muy diferentes según su propósito y diseño, pero también del momento y los lugares en los que se despliegan y se utilizan. Así pues, si bien las nuevas tecnologías pueden resultar útiles en la respuesta a la COVID, es imprescindible avanzar en el análisis de su relevancia, su cumplimiento con las normas relativas a la protección de datos y su adecuación, para cada caso y según el contexto, pues su pertinencia y su valor añadido varía de un contexto a otro.

Massimo Marelli: Pienso que los sistemas de información y comunicación digitales pueden tener efectos positivos si los regulamos adecuadamente, Por ejemplo, la legislación sobre protección de datos garantiza que las tecnologías digitales puedan usarse de modo que aseguren la "dignidad digital" o la "dignidad de los datos", proporcionando a los titulares de los datos la información, el control y los derechos necesarios para ejercer control sobre cómo se usa la información sobre ellos. Las leyes también procuran imponer límites a qué pueden hacer con nuestra información los responsables de la administración de datos, a fin de garantizar un tratamiento de datos justo y sin discriminación y prevenir los abusos. Al incorporar esa legislación a nuestra labor, podemos garantizar que los efectos positivos de las tecnologías digitales tengan mayor peso que los negativos. De acuerdo con este concepto, los principios fundamentales para la protección de datos constituyen la base de las *Normas del CICR en materia de protección de datos personales*[20]. Desde luego, es fácil decir que puede ser difícil aplicar esos principios a la acción humanitaria, debido a las circunstancias en el terreno o porque a nuestros beneficiarios "no les importa", pero si queremos garantizar seriamente que las tecnologías digitales tengan un efecto neto positivo en general y respetar seriamente la dignidad de las personas afectadas, no causar daño, ser responsables y mantener la confianza, entonces con eso no basta. No tenemos más opción que tratar de superar esos desafíos y garantizar que nuestras acciones sigan los principios que definen la labor humanitaria en este ámbito.

¿Por qué el sector humanitario debería dialogar con el sector tecnológico privado?

Delphine van Solinge: Creo que soy yo quien tiene que responder esta pregunta. La rápida evolución de la tecnología, la conectividad y los datos es una fuerza de cambios multidimensionales en las sociedades y en la forma en que trabajamos y nos comunicamos. En los contextos humanitarios, esto repercute no solo en las expectativas y las necesidades de las poblaciones afectadas y otras partes interesadas, sino también en la forma en que pueden implementarse los programas y los servicios humanitarios.

20 CICR, nota 11 *supra*.

Si bien ofrece nuevas oportunidades para que el sector humanitario despliegue y amplíe su respuesta, la transformación digital también genera riesgos nuevos o amplificados para las poblaciones afectadas por conflictos. Aun así, la transformación digital de las sociedades y las empresas ya no es algo de lo que se pueda prescindir. Es una realidad, y tenemos que aprender a vivir y a trabajar con ella.

El sector humanitario tiene la doble obligación de estudiar la relevancia de las soluciones digitales y de encontrar el tipo adecuado de diálogo ético con el sector tecnológico. La primera razón para ello es que la tecnología y los datos tienen el potencial de mejorar las respuestas humanitarias y, por ende, de ayudar a aliviar el sufrimiento de las poblaciones afectadas. La segunda es que esas tecnologías pueden generar, según se usen adecuadamente o no, riesgos para las poblaciones o empañar la credibilidad de las organizaciones humanitarias. Es necesario estudiar, entender, explorar y desplegar responsablemente el potencial de las tecnologías digitales para mejorar la respuesta humanitaria conforme al principio de "no causar daño" y a las normas relevantes en materia de protección de datos.

Así como el sector humanitario puede aprender del sector tecnológico a elaborar una respuesta más eficaz, el sector tecnológico puede aprender del sector humanitario a pensar más allá de sus laboratorios, a conocer las consecuencias que puede tener el "tecnocolonialismo"[21] en la vida y la seguridad de las poblaciones afectadas en el mundo real y a encontrar en conjunto maneras de mitigar esas consecuencias.

Massimo Marelli: Creo que Delphine ha expresado todo lo que yo tengo para decir de esta cuestión. Retomo su afirmación de que los procesos de transformación digital son algo de lo que ya no podemos prescindir, y esto se ve en el predominio del sector tecnológico privado. Por nuestra parte, en el sector humanitario tenemos la obligación de dialogar con esos actores y de garantizar que nuestra labor se adapte para que podamos continuar dando prioridad a la seguridad y a la confianza de las personas afectadas en nuestras actividades operacionales.

¿Las redes sociales más populares tienen la responsabilidad de adoptar políticas que protejan a las poblaciones afectadas contra las campañas de información errónea o desinformación?

Massimo Marelli: Delphine es la experta en este tema.

Delphine van Solinge: Gracias, Massimo. Creo que se trata de una responsabilidad compartida. El IDO no se produce en el vacío; está arraigado en la

21 El "tecnocolonialismo", tal como lo define Mirca Madianou, hace referencia a "cómo la convergencia de los avances digitales con las estructuras humanitarias y las fuerzas de mercado revitaliza y reformula las relaciones coloniales de dependencia". V. Mirca Madianou, "Technocolonialism: Digital innovation and data practices in the humanitarian response to refugee crises", *Social Media and Society*, vol. 5, n.º 3, 26 de julio de 2019, disponible en https://journals.sagepub.com/doi/full/10.1177/2056305119863146.

historia, los comportamientos de las sociedades, las tensiones crónicas y la política, entre otros factores.

Las redes sociales no son en sí mismas la causa de la difusión de información perjudicial; sin duda, desempeñan un papel en la amplificación, la magnificación y la aceleración de cómo se comparte la información, pero no son las que redactan las publicaciones. Esto no debe entenderse como que las empresas responsables de las redes sociales tienen que "lavarse las manos" y no hacer nada con respecto al contenido que prolifera en sus plataformas. Como proporcionan un servicio lucrativo, en el que los algoritmos, la inteligencia artificial y la analítica de datos desempeñan un papel importante en el nivel de visibilidad y accesibilidad del contenido de acuerdo con el perfil, los intereses o el comportamiento social del usuario, esas empresas tienen la responsabilidad de implementar las políticas de mitigación y las medidas técnicas necesarias para restringir la difusión de información que pueda ser perjudicial para las personas.

Durante la crisis causada por la COVID-19, muchas redes sociales, como Facebook y Twitter, adoptaron medidas para restringir, por ejemplo, la cantidad de información falsa que circula sobre tratamientos que, claramente, podrían tener consecuencias letales, en concreto, consejos médicos incorrectos y potencialmente perjudiciales[22]. Si bien muchos podrían argumentar que es evidente que esa información es totalmente falsa, en medio de una crisis sanitaria, el miedo a la muerte puede hacer que las personas no piensen racionalmente. En situaciones de conflicto armado e incluso de violencia latente, es más fácil apelar a los temores básicos y al instinto de supervivencia. Publicar y hacer circular información alarmante o descontextualizada en esas circunstancias puede exacerbar la polarización, el estrés y el miedo, los comportamientos irracionales y, en última instancia, la violencia.

Por eso, es importante prestar atención a los distintos actores, funciones y responsabilidades más allá de las plataformas. Los políticos, las autoridades y la sociedad civil tienen una responsabilidad y un papel, con sus distintas capacidades y funciones, en la limitación de la creación y la difusión del IDO en las redes sociales. Sin embargo, también tenemos que ser realistas: la información errónea y la desinformación están muy arraigadas en la política, el poder y la conducta social y, por lo tanto, seguirán siendo utilizadas de múltiples formas y bajo distintas modalidades. Lo que puede hacerse, sin embargo, es fortalecer la resiliencia de las personas frente al IDO mediante la promoción de la alfabetización digital, el pensamiento crítico y –si me permiten una dosis de idealismo– los valores humanitarios.

22 Google, p. ej., está eliminando información falsa o engañosa sobre la COVID-19 de sus distintas plataformas y anuncios publicitarios; v. Sundar Pichai, "COVID-19: How we're continuing to help", *Inside Google*, 15 de marzo de 2020, disponible en https://blog.google/inside-google/company-announcements/covid-19-how-were-continuing-to-help/. Actualmente Twitter verifica la credibilidad de la información que proporcionan los tuits y las cuentas de Twitter y ha incluido el aviso #KnowTheFacts; v. "Coronavirus: Staying safe and informed on Twitter", *Twitter Blog*, 3 de abril de 2020, disponible en https://blog.twitter.com/en_us/topics/company/2020/covid-19.html.

¿Cuáles son las ventajas y las desventajas de que las poblaciones afectadas tengan mayor acceso a la conectividad digital?

Delphine van Solinge: Aquí, le cedo la palabra a Massimo.

Massimo Marelli: Gracias, Delphine. En primer lugar, tenemos que pensar en la conectividad como una realidad y no como un problema o una oportunidad. A medida que la vida social y material se traslada más y más al entorno digital, y el mundo está más y más conectado, las organizaciones humanitarias no tienen más opción que construir una presencia en los espacios virtuales donde se congregan las poblaciones afectadas, aprovechar los nuevos mecanismos de resiliencia que ofrece la conectividad e incorporar la conectividad en sus programas. Todo esto puede ser bastante sencillo, por ejemplo, proporcionando "conectividad como asistencia", pero también puede ser más complejo, por ejemplo, en lo relativo a los nuevos servicios digitales. Además del cumplimiento de las normas de protección de datos –y dando siempre las respuestas adecuadas a las necesidades de quienes no están conectados–, el principal problema es el de la innovación responsable. Debemos dedicarnos a construir espacios humanitarios digitales seguros y protegidos donde podamos estar seguros de que realmente no causamos daño y que nos movemos dentro de los límites de los entornos digitales actuales. Esto no es nada sencillo. Hay que educar a los asociados, los Estados y los proveedores de servicios tecnológicos en cuanto a las razones por las cuales esos espacios son necesarios y trabajar con ellos para desarrollar la infraestructura y las aplicaciones que requiere una acción humanitaria neutral, independiente y confiable.

¿Podrían mencionar algunas de las implicaciones éticas de, por ejemplo, usar las tecnologías digitales, como el reconocimiento facial, para identificar personas desaparecidas? ¿Cómo influyen esas consideraciones éticas en la labor del CICR?

Massimo Marelli: A menudo, la ética y la protección de datos se superponen. La legislación sobre protección de datos, como la mayor parte de las leyes, es, en última instancia, un reflejo de las respuestas que dan las sociedades a las cuestiones éticas y las normas que deciden imponerse para permanecer fieles a esas respuestas. Creo que, en el contexto de las tecnologías mencionadas, las preguntas clave son, por un lado, ¿esas tecnologías pueden tener beneficios reales para el CICR y las poblaciones afectadas? y, por el otro, ¿podemos utilizarlas con responsabilidad, poniendo a las poblaciones afectadas en primer lugar?