DERECHO Y POLITICAS HUMANITARIAS

Facilitar la innovación, velar por la protección: política del CICR sobre biometría

marzo 14, 2022, Acción humanitaria

17 mins read

 Ben Hayes

 Massimo Marelli

El uso de sistemas de identificación biométrica por parte de las organizaciones humanitarias ha sido tema de intensos debates en los últimos años y ocupa un lugar destacado en el discurso sobre la "experimentación humanitaria". Desde hace mucho tiempo, el CICR utiliza la biometría para la consecución de su cometido en casos limitados, por ejemplo, la labor forense y el restablecimiento del contacto entre familiares, así como en la impresión de huellas dactilares en los documentos de viaje que expide (pero no en bases de datos).

Al igual que muchas otras organizaciones, el CICR ha indagado en el uso de nuevas tecnologías en apoyo a sus operaciones y sus beneficiarios, incluidas las oportunidades que las nuevas aplicaciones biométricas ofrecen. Como parte de su programa de transformación digital, el CICR decidió elaborar una Política sobre biometría que facilitara el uso responsable de esta tecnología y permitiera responder a las dificultades que plantea en materia de protección de datos. ¿Cómo es, entonces, el uso responsable de la biometría desde la perspectiva estratégica de una institución como el CICR?

¿De qué se trata la biometría?

Los datos biométricos son datos personales que se obtienen de un procesamiento técnico específico, referidos a las características físicas, fisiológicas o conductuales de una persona, que permiten o confirman la identificación distintiva de esa persona. De la mano de la popularización del uso de la biometría, las aplicaciones y el equipamiento que esta utiliza resultan más económicos y fáciles de instalar, lo que aumenta su atractivo para las organizaciones que necesitan validar en forma periódica la identidad de las personas. Entre ellas, se incluyen las organizaciones humanitarias que han desarrollado e implementado un número creciente de sistemas de identificación biométrica, debido a la percepción de eficacia y rendición de cuentas que aportan a sus operaciones.

Esta dinámica ha generado en el sector humanitario un impulso tangible para el uso de la biometría destinada al registro de beneficiarios y a la distribución de la asistencia. El personal en el terreno ve que otras organizaciones utilizan la biometría e informan sobre sus diversos beneficios, por lo que es lógico que deseen emplear las mismas herramientas. La administración quiere que sus operaciones sean lo más eficientes y «ágiles» posibles. Asimismo, hay una presión implícita de los donantes, que, cada vez más, exigen «la posibilidad de auditar de extremo a extremo» y condicionan el financiamiento humanitario a procesos comprobables de lucha contra el fraude y de rendición de cuentas. Si bien los donantes no exigen en forma explícita el uso de la biometría, estos sistemas aparentemente ofrecen –y, de hecho, se los publicita así– como la forma más atractiva de cumplir con los múltiples requisitos de los programas humanitarios. La biometría desempeña, además, un papel central en la intensificación de los programas de transferencias monetarias, y muchos proveedores de servicios financieros la perciben, en consecuencia, como una herramienta que, de manera sencilla, les permite cumplir con los requisitos en materia de identificación de clientes y otros requisitos jurídicos de diligencia debida.

Independientemente de la distribución de asistencia, al CICR también le interesa la tecnología relativa a la biometría, como el análisis de ADN, para contribuir a la identificación de restos humanos en el proceso de determinación del paradero de las personas desaparecidas. Asimismo, actualmente evalúa el potencial de utilizar tecnología de reconocimiento facial en su programa de restablecimiento del contacto entre familiares para ubicar a personas que sus familiares procuran encontrar luego de separaciones forzosas como consecuencia de emergencias humanitarias. A raíz de la frecuente presencia de esta tecnología en las noticias, e incluso de la existencia de *proveedores que exigen que se la reglamente*, resulta palpable la necesidad de contar con una política general sobre biometría que minimice los riesgos para los beneficiarios y, por ende, para la reputación del CICR.

Biometría y protección de datos

La sensibilidad de los datos biométricos es reconocida, tanto en la legislación como en la práctica. El *Reglamento general de protección de datos de la Unión Europea* –que ha cohesionado a jurisdicciones de todo el mundo en la adopción, revisión, propuesta o consideración de sus propias leyes sobre protección de datos– considera los datos biométricos como una «categoría especial», lo que conlleva la aplicación de límites más estrictos para la obtención y protección de los datos. La Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos, el «modernizado» Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y muchas otras leyes nacionales sobre privacidad también incluyen normas especiales que restringen el procesamiento de datos biométricos. Si bien estas normas no se aplican al CICR (que ha adoptado *Normas* sobre protección de datos personales que reflejan su carácter de organismo internacional), los principios esenciales que las fundamentan son los mismos.

La Conferencia Internacional de Comisarios de Protección de Datos y de la Privacidad (ICDPPC, por su sigla en inglés) fue la primera en plantear inquietudes sobre la biometría en una resolución del año 2005 en la que advierte que «el uso extendido de la biometría tendrá una enorme incidencia en la sociedad mundial» y que «por lo tanto, debería ser objeto de un debate abierto a nivel mundial». En 2012, las orientaciones de los organismos de supervisión de protección de datos de la Unión Europea advirtieron que «el uso de las tecnologías biométricas también está ampliando gradualmente su ámbito de aplicación: de la identificación y autenticación al análisis del comportamiento, la vigilancia y la prevención del fraude». En el informe de Privacy International del año 2013, titulado «*Aiding Surveillance*«, se plantean inquietudes respecto del uso de la biometría en diversos entornos humanitarios. En dicho informe, se sostiene que ha habido «una falta sistemática de análisis crítico de los potenciales efectos negativos de la aplicación de tecnologías en iniciativas humanitarias y del ámbito del desarrollo; lo mismo puede decirse de la consideración de protecciones jurídicas y técnicas necesarias para respetar los derechos de las personas que viven en el mundo en desarrollo» (pág. 7). En 2015, la ICDPPC aprobó una resolución sobre privacidad y acción internacional humanitaria que destacó también, entre otras cuestiones, los riesgos de la biometría y de los sistemas de identificación.

La biometría y la protección de los beneficiarios de la asistencia humanitaria

Independientemente de los regímenes jurídicos aplicables, los datos biométricos son particularmente «sensibles» en las emergencias humanitarias, ya que si, una vez obtenidos, se los retiene, ello da origen a un registro permanente e identificable de una persona. Esto podría resultar problemático para los beneficiarios de asistencia humanitaria, que quizás no desean que se los pueda identificar para siempre, en particular, si existe el riesgo de que los datos se filtren o que terceros no autorizados puedan acceder a ellos. En el caso de sistemas de gestión de identidad biométrica, existe, además, un riesgo significativo de que con el paso del tiempo se desvirtúe su uso, lo que abre la posibilidad de que en última instancia los datos se utilicen de formas que los usuarios no comprenden o desean, o para las que no han dado su consentimiento.

Si bien las políticas de protección de datos y los sistemas sólidos de seguridad de datos pueden atenuar estos riesgos, el uso de tecnologías biométricas por parte de las organizaciones humanitarias plantea además importantes cuestiones éticas. En diversos contextos humanitarios a gran escala, las poblaciones afectadas han manifestado su seria preocupación por el uso de la biometría y la posibilidad de que las organizaciones no humanitarias accedan a los datos, en particular, para fines de seguridad y de control migratorio *[1]*. Dado que los datos biométricos resultan atractivos para estos propósitos, los Estados ya han presionado a estas organizaciones para que los revelen. Además, estos datos son vulnerables a las ciberoperaciones por parte de actores estatales y no estatales que procuran acceder a los datos sin autorización.

En el caso del CICR, la protección de datos personales –cuya revelación podría poner en riesgo a sus beneficiarios, o cuyo uso para fines distintos de los previstos durante su recolección– representa un medio integral de preservar la neutralidad, imparcialidad e independencia de la Institución, además de la naturaleza exclusivamente humanitaria de su labor.

Determinar la legitimidad y el propósito

La Política del CICR sobre biometría, aprobada por la Asamblea del CICR en agosto de 2019, fue el corolario de 18 meses de un exhaustivo trabajo de investigación, análisis, consulta y reflexión. Este proceso incluyó una revisión de todas las situaciones y los casos en los que el CICR procesa datos biométricos o considera la utilización la biometría, una evaluación de las «razones legítimas» y de los fines específicos del procesamiento, así como la identificación de protecciones organizacionales, técnicas y jurídicas.

No resulta difícil determinar que existen razones legítimas cuando el CICR procesa datos biométricos de conformidad con objetivos específicos vinculados a su cometido –como la identificación de personas como parte de su labor de restablecimiento del contacto entre familiares y la determinación de la suerte o el paradero de las personas desaparecidas– y en casos en los cuales, sin la biometría, no es posible concretar objetivos específicos. En este caso, el CICR procesa los datos biométricos como una cuestión de «interés público» (en la implementación del cometido del CICR).

La cuestión resulta mucho más compleja en lo que respecta al uso de la biometría para la gestión de beneficiarios y la distribución de asistencia, casos en los que el procesamiento de datos puede no ser considerado como parte integral de una actividad establecida en el cometido del CICR que requiera la identificación de personas. Dado que en este caso el propósito está vinculado fundamentalmente con la eficiencia, y en tanto la asistencia pueda distribuirse (y durante mucho tiempo se ha distribuido) sin necesidad de recurrir a la biometría, el CICR debería determinar que el «interés legítimo» que tiene en poner en práctica un sistema de identidad biométrica no supera la posible incidencia que esto puede tener en los derechos y las libertades de las personas afectadas. Esta prueba de equilibrio es típica de la legislación sobre protección de datos toda vez que un controlador de datos funda el procesamiento en los intereses de estas personas.

En su análisis, el CICR determinó, no obstante, que era posible lograr un equilibrio que permitiera a la Institución aprovechar las ventajas de la autenticación biométrica en cuanto a su eficiencia y eficacia, y propiciar una rendición de cuentas de extremo a extremo en sus tareas de distribución de asistencia y, al mismo tiempo, minimizar los riesgos a los que estarían expuestos sus beneficiarios.

Este equilibrio depende de operaciones dispuestas a utilizar los datos biométricos en el registro y la verificación de beneficiarios que limitan el procesamiento a un sistema basado en *tokens*. En la práctica, significa, por ejemplo, la posibilidad de extender una tarjeta a los beneficiarios que almacene, en forma segura, sus datos biométricos, pero que el CICR no recabará, retendrá ni procesará (y que por ende no constituirán una base de datos biométricos).

Es posible utilizar el *token*/la tarjeta para verificar la identidad de los beneficiarios durante distribuciones de asistencia a fin de que esta llegue a sus destinatarios previstos, pero no para ningún otro uso. Si el beneficiario desea retirar o eliminar sus datos biométricos no tendrá más que devolver la tarjeta, o destruirla. Si las autoridades buscan obligar a las organizaciones humanitarias de un país dado a entregar los datos biométricos de los beneficiarios, el CICR estará exento de esta presión ya que, de hecho, no contará con esta clase de datos.

¿Y el consentimiento?

El CICR ha asumido el compromiso, ante sus beneficiarios y poblaciones afectadas, de procesar los datos con la mayor transparencia posible, pero no considera que el consentimiento constituya un fundamento jurídicamente válido para el procesamiento de datos en muchas situaciones de emergencia.

Esto se debe a que el consentimiento no puede considerarse válido si la persona no tiene otra opción, por ejemplo, cuando la prestación de asistencia depende en efecto de que suministre información personal, en cuyo caso es poco probable que el consentimiento se «otorgue por la propia voluntad». Además, como consecuencia del desequilibrio de poder y de la situación de los beneficiarios, probablemente estos no tengan una verdadera «opción» y se vean inducidos a aceptar lo que una organización humanitaria propone. Asimismo, cuando se trata de la biometría, resulta en extremo difícil garantizar que el consentimiento sea genuinamente «informado», ya que en muchas situaciones la población afectada no estará en condiciones de comprender en profundidad la tecnología, los flujos de información, los riesgos o los beneficios que subyacen al procesamiento de sus datos biométricos.

En consonancia con las Normas del CICR en materia de protección de datos personales, la Política sobre biometría exige que la Institución explique a sus beneficiarios los fundamentos y los fines del procesamiento de datos, incluidos los acuerdos sobre intercambio de datos, independientemente de los motivos que justifican el procesamiento. Además, el CICR procura favorecer que los beneficiarios tengan la oportunidad de formular preguntas y objetar el procesamiento de los datos si así lo desean, en particular, cuando existe la posibilidad de estos datos se transmitan a terceros. Si las personas no desean suministrar sus datos biométricos u otros datos personales, o que, con fines humanitarios, su información se transmita a los asociados, el CICR respetará su voluntad.

Qué significa la Política para el CICR

En primera instancia, el CICR puede confiar en haber identificado un «fundamento legítimo» para utilizar la biometría en sus actividades operacionales y programas y, conforme a la implementación de las protecciones organizacionales, técnicas, jurídicas contenidas en la Política, elaboró protecciones adecuadas para preservar a su personal y a los beneficiarios de los riesgos que puedan presentarse.

Los responsables de programas que deseen utilizar la biometría deberán cerciorarse de que los fines y las modalidades de procesamiento cumplan con la Política. Todo nuevo caso de uso deberá ser objeto de una evaluación de impacto relativa a la protección de datos y se deberán elaborar protecciones adecuadas para los beneficiarios. La Política del CICR sobre biometría dispone además que, antes de poner en práctica cualquier solución en la materia, se realice una evaluación de riesgos y se consulte a las poblaciones afectadas.

En la Política también se deja en claro que el CICR solo utilizará los datos biométricos cuando ello mejore la capacidad de la Institución de cumplir con su cometido humanitario, y que, bajo ninguna circunstancia, compartirá esos datos con terceros, incluidas las autoridades, que puedan utilizarlos para fines no humanitarios. Incluso si es posible identificar razones puramente humanitarias para intercambiar datos biométricos, de todos modos se deberá cumplir con estrictas condiciones antes de que el CICR pueda transferir tales datos.

Por último, en virtud de esta Política, el CICR se compromete a utilizar la biometría en forma transparente. Su publicación en el sitio web del CICR y su explicación en este documento son parte de ese esfuerzo.

Con miras al futuro

El CICR se ha comprometido a trabajar con las últimas tecnologías de modo tal que, siempre que resulte posible, ello depare beneficios comprobables para sus actividades y sus beneficiarios, lo que significa que analizará los avances respecto de la disponibilidad, la seguridad, el costo, la eficacia y los efectos de la tecnología biométrica. Asimismo, cuando resulte pertinente, revisará su propia Política sobre biometría al menos cada tres años a fin de evaluar los nuevos casos de uso y las nuevas tecnologías.

Esta revisión tiene por objeto mantenerse al tanto de los avances tecnológicos que podrían conllevar que el uso de una biometría específica planteara un riesgo significativamente mayor o menor en el futuro respecto del que se considera que hoy plantea. En consecuencia, se continuará revisando la decisión de no crear por el momento una base de datos biométricos para la gestión de identidad.

Además, el CICR procurará determinar cuál es la percepción de los beneficiarios respecto de la forma en que se utiliza la biometría. La Política puede modificarse, de ser necesario, a fin de ampliar el alcance del uso de la biometría, o para incluir nuevas protecciones.

***

[1] V., por ejemplo, *'Yemen's Houthis and WFP dispute aid control as millions starve'* (Reuters, 4 de junio de 2019), *'Rohingya Refugees Protest, Strike Against Smart ID Cards Issued in Bangladesh Camps'* (Radio Free Asia, 26 de octubre de 2018) y *'Over 2,500 Burundi Refugees in Congo Seek Shelter in Rwanda'* (Voice of Africa News, 8 de marzo de 2018).

***

Otros blogs sobre este tema

- *Digital risks for populations in armed conflict: Five key gaps the humanitarian sector should address*, Delphine van Solinge, 12 de junio de 2019
- *The price of virtual proximity: How humanitarian organizations' digital trails can put people at risk*, Tina Bouffet y Massimo Marelli, 7 de diciembre de 2018
- *Protecting the digital beneficiary*, Gus Hosein, 12 de junio de 2018
- *Humanitarian experimentation*, Katja Lindskov Jacobsen, Kristin Bergtora Sandvik y Sean Martin McDonald, 28 de noviembre de 2017
- *The data divide: Overcoming an increasing practitioner-academic gap*, Larissa Fast, 2 de noviembre de 2017