MI HUELLA POR UN VOTO

Acerca de la identificación biométrica en elecciones

por los Derechos Civiles

Asociación por los Derechos Civiles

Abril 2019

Este trabajo fue realizado como parte de un proyecto financiado por **Ford Foundation.**

Mi huella por un voto. Acerca de la identificación biométrica en elecciones *

Resumen ejecutivo

El siguiente reporte indaga en la relación entre la biometría y los derechos humanos a través de un caso específico: la identificación de votantes antes de la emisión del sufragio. El uso de tecnologías biométricas para acreditar la identidad de electores es justificada en base a su mayor precisión, seguridad y rapidez. Sin embargo, se sostendrá que un examen más cuidadoso de dichos sistemas demuestra que aquello no es necesariamente el caso. Los métodos de identificación biométricos pueden resultar en errores, son susceptibles de ser engañados y pueden retardar el proceso electoral. Al mismo tiempo, se argumentará que los biométricos -género al cual pertenece la huella dactilar- son datos sensibles y por lo tanto debe existir previo a la implementación de estas tecnologías un conjunto de garantías robustas para resguardar el derecho a la privacidad y a la protección de datos personales.

* El presente documento fue escrito por Eduardo Ferreyra, analista de políticas públicas de la ADC adcdigital.org.ar | adc.org.ar. Encargado de diseño y diagramación: Matías Chamorro.

Introducción

No importa la concepción que se tenga de la democracia, la elección de las autoridades gubernamentales por parte del pueblo es un componente esencial. A partir de ahí, se puede complejizar el análisis y requerir otros elementos. Ciertamente una concepción "sustantiva" del proceso democrático buscaría ensanchar la idea de democracia hasta incluir el goce, por parte de la población, de derechos básicos como la salud, la educación o la vivienda. Así, una sociedad que tuviera elecciones periódicas pero cuya mayoría de habitantes padeciera graves carencias sociales sufriría un profundo déficit democrático. A su vez, una concepción "formalista" no necesita limitarse solo a la celebración de elecciones sino que puede incorporar otros mecanismos, como referendos revocatorios, consultas populares o un robusto proceso de deliberación previo a la toma de decisiones. En cualquiera de ambos casos, no obstante, resulta claro que el voto es una condición necesaria para la existencia de un régimen democrático.

Lo fundamental del voto nos exige, entonces, que dirijamos nuestra atención hacia las condiciones en las que se desarrolla dicho acto. Es preciso, por lo tanto, hablar del proceso eleccionario. Está claro que el mero acto de introducir el sobre en la urna no implica que tal conducta haya sido ejemplo de un libre ejercicio del derecho al sufragio. Varios hechos podrían haber sucedido antes, durante o después de la emisión del voto. Por ejemplo, la persona podría haber sufrido intimidación para que elija a un determinado candidato. O quizás no existieron amenazas pero sí ofrecimientos de dinero. Por otro lado, al momento de ingresar al cuarto oscuro la persona puede observar una gran cantidad de boletas con múltiples candidatos para elegir, con la salvedad de que todos ellos pertenecen al oficialismo, ya que vive en un país con régimen de partido único. Finalmente, el día de los comicios tal vez transcurrió con normalidad, pero luego del cierre de la votación, se produce un fraude electoral y resulta ganador el candidato que cosechó menos sufragios. Como puede verse, existen numerosas instancias a lo largo de todo el proceso que pueden poner en riesgo la integridad de las elecciones. En este caso, nos ocuparemos de una de ellas: el procedimiento de identificación de los votantes.

La identificación como garantía de una elección transparente

El deber de asegurar que la persona que emitió el voto es efectivamente aquella que figura en el padrón electoral resulta indispensable por diversas razones.

En primer lugar, es una manera de respetar el principio de "una persona = un voto". El derecho de participación política tiene que ser ejercido de modo equitativo por todos los ciudadanos. Esto significa que los individuos deben contar con una única oportunidad para votar. Si una persona puede influir con más de un voto, se viola la igualdad ante la ley, componente esencial de una sociedad sin privilegios. En este sentido, la identificación ayuda a lograr este objetivo, ya que permite que haya registro de la persona que ya sufragó. De esta manera, se evita que en otro momento del día se presente esa misma persona y quiera votar de nuevo.

En segundo lugar, es una forma de asegurar que la elección de las autoridades encargadas de tomar las decisiones políticas estará a cargo de las personas que serán afectadas por ellas. Por lo general, los individuos están habilitados a votar en un determinado distrito electoral, porque allí es su lugar de nacimiento o de residencia. De esta manera, se garantiza que exista un vínculo entre la persona y el territorio sobre el cual va a ejercer el acto eleccionario. La identificación evita, entonces, que personas sin relación con el lugar tengan influencia en la elección de sus autoridades políticas.

Por último, el voto es una herramienta fundamental para el ejercicio de los derechos políticos en una democracia. Más allá de su real probabilidad de influir decisivamente en el resultado electoral, el sufragio resulta parte esencial de la condición de ciudadano. Como tal, representa la confianza que la comunidad depositó en la persona para hacerla partícipe -aunque sea de manera indirecta- en la deliberación de sus cuestiones políticas más trascendentales. Por lo tanto, la identificación también sirve para que cada elector reafirme su dignidad política al evitar que otras personas ejerzan ilegalmente por ella el derecho al voto.

La biometría como mecanismo de identificación

La necesidad de asegurar una identificación certera de los votantes ha llevado a los gobiernos a elaborar distintos mecanismos de control de identidad. El más usual suele ser la presentación por parte del votante de un documento que demuestra que él es quien dice ser. Sea a través de la exhibición de un documento nacional de identidad, una tarjeta de votación u otro instrumento (pasaporte, licencia de conducir, carné del seguro social, etcétera), las personas se acreditan y luego de un chequeo por parte de las autoridades, son autorizadas para votar.

Sin embargo, existe una tendencia cada vez mayor a utilizar la biometría para llevar adelante esta tarea. Gobiernos de diversas partes del

mundo han implementado o están empezando a implementar tecnologías biométricas para identificar a sus votantes[1]. Las razones esgrimidas son múltiples.

En primer lugar, se afirma que este método aumentará de modo significativo la eficiencia de la identificación de los votantes en los centros electorales. De este modo, las chances de que haya suplantación de identidad se reducirán considerablemente y los votos emitidos corresponderán efectivamente a quienes debían votar.

En segundo lugar, se sostiene que la biometría es útil para evitar el fraude electoral. En efecto, al no requerirse la presentación de algún instrumento, queda neutralizada la posibilidad de ejecutar ciertas formas de engaño como ser la duplicación o adulteración de documentos. Sumado a las supuestas ventajas de una identificación más precisa, la adopción de biometría llevaría a transparentar el proceso eleccionario.

Por último, el uso de tecnologías biométricas agregaría simplicidad y rapidez al acto eleccionario. El proceso de identificación sería más veloz y así las personas no tendrían que hacer largas filas. Como consecuencia, las elecciones contarían con más probabilidad de finalizar en el horario establecido y, por lo tanto, los resultados estarían disponibles más rápidamente.

En base a estos argumentos, varios Estados del mundo han comenzado a imitar a los precursores en el uso de biometría y manifestaron su intención de adoptar, para identificación electoral, este tipo de tecnologías. La Argentina es uno de ellos. En 2017, la Cámara Nacional Electoral (CNE) anunció la realización de una prueba piloto de utilización de herramientas de identificación biométrica para la comprobación de la identidad de electores[2]. Esta prueba tuvo lugar en las elecciones legislativas de aquel año y fue circunscripta a determinadas provincias. Asimismo, para las elecciones legislativas y presidenciales de 2019, está previsto que se realice nuevamente la prueba piloto[3].

Así, se vuelve necesario analizar los sistemas biométricos de identificación electoral. Además de los ya mencionados, existen otros motivos

1 Según la base de datos del Institute for Democracy and Electoral Assistance, 53 países usaron datos biométricos para identificar votantes. Ver https://www.idea.int/data-tools/question-view/739 (último acceso: 22-04-19)
2 Cfr. ADC Digital. "Prueba biométrica en las PASO: la Cámara Electoral respondió a ADC", 18 de Octubre de 2017, disponible en https://adcdigital.org.ar/2017/10/18/prueba-biometrica-las-paso-la-camara-electoral-respondio-adc/ (último acceso: 22-04-19)
3 Según respuesta de la Cámara Nacional Electoral a una solicitud de información de la ADC, que se encuentra en archivo.

Primero, por la eventualidad de que en algún momento este tipo de tecnología pueda ser implementada de manera definitiva para la identificación electoral. Si no es utilizada para las de este año, puede intentarse para una futura elección. En definitiva, la adopción de las pruebas pilotos es evidencia de que al menos hay un interés -en el corto o mediano plazo- en explorar este tipo de tecnologías para el acto eleccionario.

Segundo, el uso de estas tecnologías está cada vez más extendido en América Latina. Bolivia, Brasil, Colombia, Costa Rica, República Dominicana y Venezuela son algunos de los países que utilizan o utilizaron, en algún momento, sistemas de identificación biométrica[4]. Por lo tanto, la importancia del análisis no se limita a lo nacional sino que es relevante para la región.

Tercero, los principios que deben guiar la evaluación del uso de biometría para la identificación electoral pueden ser adaptados para analizar otros usos de la misma tecnología. Sea para combatir la inseguridad, garantizar la confiabilidad de una transacción bancaria o controlar la migración, la biometría se expande cada vez más como herramienta de identificación. De esta forma, aquello que podamos expresar acerca de la identificación electoral puede ayudar al análisis que se haga en otros campos en donde también existe un uso intenso de las tecnologías biométricas.

Bajo este contexto, en este trabajo presentaremos diversas objeciones desde el punto de vista de los derechos humanos hacia la identificación biométrica de electores. En primer lugar, cuestionaremos las ventajas que supuestamente traerían este tipo de tecnologías al proceso eleccionario. Luego, describiremos los riesgos vinculados al empleo de datos biométricos. Como conclusión, sostendremos que la decisión de utilizar tecnologías biométricas para la identificación de electores no puede tomarse sin antes evaluar su necesidad y conveniencia en relación a los métodos tradicionales. Asimismo, afirmaremos que cualquier implementación de esta herramienta requiere la existencia de un fuerte marco normativo de garantías de derechos, un esquema de control robusto y medidas de seguridad adecuadas que eviten que el tratamiento de datos tan sensibles de los individuos, se transforme en un ejercicio de abuso de sus derechos.

No se trata de una respuesta por sí o por no

La biometría es un ejemplo clásico del discurso sobre el "progreso tecnológico". La aparición de esta forma de identificación es promovida por sus partidarios como una superación más precisa y confiable

4 Cfr. nota 1

de los métodos tradicionales para reconocer a una persona. Sin embargo, un examen profundo de la cuestión nos habilita a dudar de tan tajante afirmación.

Pongamos un ejemplo para empezar. Imaginemos a alguien llamada Lucía. Lucía es fanática de la obra de Jorge Luis Borges. Su pasión por él es tan grande que decide fundar un grupo de discusión acerca del célebre autor. Su objetivo es conocer lectores que también posean ese fervor, para así poder compartir análisis de textos, charlas u otras actividades. Para asegurarse que el grupo esté efectivamente conformado por fanáticos de Borges, Lucía establece un requisito de ingreso: todos los interesados deben llevar a las reuniones del grupo un libro borgiano. Luego de los primeros encuentros, Lucía se siente decepcionada. Si bien entre los participantes pudo encontrar varios eruditos de la obra del escritor, muchos de los asistentes eran personas que solo conocían, de manera superficial, apenas algunos de los cuentos del creador de *El Aleph*.

Frustrada por su fallido intento, Lucía rápidamente encuentra la solución. Llega a la conclusión de que el requisito de ingreso era demasiado amplio y entonces establece la siguiente regla: todos los que quieran ingresar al grupo deberán traer todos los libros escritos por Borges y, además, rendir un examen de cien preguntas acerca de la obra del autor. Lucía se vuelve tan estricta que no permite que haya error alguno en la prueba.. Un solo equívoco y la persona será rechazada para integrar el grupo. Lo mismo con los libros: si al postulante le falta solo uno de los títulos de Borges, tampoco podrá ser admitido como miembro. Satisfecha con su nueva regla, Lucía ahora si se siente segura de que finalmente podrá compartir su pasión con personas de gustos literarios afines. Tristemente, lo estricto de sus requisitos hizo que nadie superara la prueba (incluso gente que efectivamente poseía un gran conocimiento de Borges) y así ella quedó como la única miembro del grupo.

Este ejemplo hipotético nos permite sacar varias conclusiones.

En primer lugar, los criterios de selección elegidos por Lucía resultaron muy defectuosos, debido a que en ambos casos no se pudo lograr el fin deseado. Sin embargo, las razones del fracaso fueron distintas. En la primera situación, la regla identificó a más personas de las adecuadas. Junto a los expertos en Borges, se sumaron al grupo varias personas que no conocían en profundidad la obra del escritor. En el segundo caso, la regla seleccionó a menos personas de las debidas. Numerosos fanáticos de Borges no consiguieron acceder al grupo porque no superaron los estrictos requisitos exigidos.

En segundo lugar, resulta prácticamente imposible diseñar un criterio cuya aplicación permita seleccionar a todas las personas que lo merecen y no seleccione a aquellas que no. Está claro que las reglas de Lucía fueron demasiadas permisivas en un caso y demasiadas estrictas en el otro. Resulta obvio además que existen varios criterios en el medio que podrían haber sido utilizados para hacer más eficiente el proceso de identificación. De todas maneras, por más pulido y perfeccionado que sea el criterio, siempre existirán casos en que se elegirá a personas equivocadas y/o no se seleccionará a personas indicadas.

Por último, la influencia del factor humano es decisiva, ya que el diseño del criterio de selección tendrá consecuencias en los resultados a alcanzar. Si Lucía opta por un enfoque más permisivo, seguramente su grupo estará compuesto por muchas personas pero quizás la calidad de la discusión no será muy elevada. Por el contrario, si Lucía elige ser más restrictiva, el debate quizá sea de mayor nivel pero la posibilidad de conocer gente y compartir experiencias -otra de las metas que llevan a la creación de estos grupos- se verá ampliamente reducida.

Se trata en suma de qué concesiones y arreglos se consideran convenientes realizar para lograr un determinado resultado. No hay una fórmula mágica que nos permita realizar una división infalible. Toda proceso de selección tendrá errores que producirán consecuencias injustas.

Pues bien, el proceso de identificación en base a biometría se asemeja bastante a la tarea llevada a cabo por Lucía para seleccionar a los integrantes de su grupo literario. Lejos de lo que nuestros preconceptos sobre el rol de la tecnología nos impulsan a pensar, no se trata de una operación sencilla mediante la cual se nos dará un sí o no a nuestras dudas sobre la identidad de una persona. En realidad, la tarea es más compleja y requiere una intervención decisiva del factor humano. Citemos al Dr. Hugo Scolnik, especialista en seguridad informática: "Todos los métodos de identificación proceden primero a recoger información de un individuo (huellas dactilares, características de la cara como distancia entre ojos, forma de la boca, nariz, etcétera) y luego determinan una 'distancia' a los datos existentes en una base. Se decide si una persona se corresponde con una identidad si esa 'distancia' es menor que una 'tolerancia'. Entonces queda claro que los resultados dependen de ambos conceptos, y de ahí los posibles errores, pues con una 'tolerancia' grande se aumenta el número de 'coincidencias' y con una chica probablemente no haya ninguna, pues todo depende de, por ejemplo, la luz, el ángulo con el que se toma la fotografía, los colores de fondo, etcétera"[5].

5 Asociación por los Derechos Civiles. *La identidad que no podemos cambiar. Cómo la bio-*

Lo que nos señala Scolnik es que al final de cuentas, el funcionamiento del sistema dependerá de la decisión del desarrollador o implementador de la tecnología. Si existe un margen de tolerancia grande, es probable que el sistema emita mayores resultados coincidentes que si se establece un margen más estricto. Pero el lado negativo de un sistema más tolerante es que es probable que parte de esas coincidencias sean falsas, debido a la mayor laxitud con que se consideró la distancia. Por el contrario, un sistema que exige un mayor grado de coincidencia es más eficiente en evitar errores de identificación. Pero a su vez, la probabilidad de que efectivamente pueda identificar se reduce de manera considerable, ya que una diferencia con los datos existentes en la base puede suponer que el sistema no reconocerá a dicha persona.

De este modo, todo sistema de identificación biométrica tiene que ponderar entre los casos de identificación certeros que se producirán y los errores que se cometerán. Por lo tanto, la afirmación de que la implementación de un procedimiento de este tipo aumentará *per se* la eficiencia del sistema resulta meramente dogmática. Sobre todo, si no se hace una evaluación integral del sistema y no se lo compara con los procedimientos utilizados en la actualidad. En este sentido, la identificación por huella dactilar suele tener un grado de confiabilidad mayor que otros sistemas, como ser el de reconocimiento facial. Sin embargo, es muy pronto para celebrar. Como veremos a continuación, existen diversos métodos para engañar a los sistema biométricos que identifican a la gente por medio de su huella dactilar.

No es un método infalible contra el fraude electoral

La identificación por huella dactilar no previene de manera infalible el fraude electoral. Cierto es que ya no se corre el peligro de que se adultere o falsifique el documento nacional de identidad. Pero en verdad, lo que se está haciendo es suplantar un riesgo por otro. Las huellas dactilares pueden ser copiadas, simuladas o capturadas para burlar al sistema. Prestemos atención a una noticia reciente en Argentina. A principios de abril de 2019, nos enteramos que Aerolíneas Argentinas (AA) había despedido a seis empleados luego de haber sido descubiertos en una maniobra fraudulenta para simular su asistencia a su lugar de trabajo[6]. La empresa tenía un sistema de control biométrico para

---

metría afecta nuestros derechos humanos. Pág. 8 Buenos Aires, 2017. Disponible en https://adcdigital.org.ar/wp-content/uploads/2017/06/La-identidad-que-no-podemos-cambiar.pdf (último acceso: 22-04-19)

6 Infobae. "Echaron a empleados de Aerolíneas Argentinas que falsificaban su ingreso con dedos de silicona". 9 de Abril de 2019. Disponible en https://www.infobae.com/sociedad/2019/04/09/echaron-a-empleados-de-aerolineas-argentinas-que-falsificaban-su-ingreso-con-dedos-de-silicona/ (último acceso: 22-04-19)

asegurar la presencia de sus trabajadores. Sin embargo, los empleados recurrieron a un dispositivo de dedos de silicona para sortear el control. Uno de los implicados se encargaba de llevar un artefacto de color blanco que contaba con las huellas impresas de sus otros cinco compañeros. De esta manera, el sistema registraba la presencia de todos los implicados cuando en realidad solo uno había asistido a trabajar.

Este ejemplo es uno solo de los varios que existen en el mundo y que han demostrado los riesgos de los sistemas de identificación por huella dactilar. Para mencionar otros: captación de huellas de una persona a través de fotografías de ella, creación de copias de huellas con o sin consentimiento de la personas, falsificación de huellas para acceder a un dispositivo, uso de huellas de gelatina para simular huellas reales, entre otros[7]. Como se ve, las modalidades de engaño que pueden adoptarse son diversas. Seguramente, algunas de ellas serán más eficaces que otras para un hipotético intento de fraude electoral. De todos modos, lo relevante es señalar -en línea con el argumento anterior- que la adopción de un mecanismo de identificación biométrica por huella dactilar no es garantía automática de que la posibilidad de fraude se desvanecerá. Tal como acabamos de ver, existen métodos por los cuales se puede burlar al sistema.

No es obvio que agilice el proceso electoral

A pesar de ello, existe otra promesa que la identificación biométrica pareciera cumplir: aumentar la velocidad del proceso. Uno de los aspectos que genera mayor molestia en las votaciones es el tiempo que lleva emitir el sufragio. Largas colas y extensos momentos de espera vuelven fastidiosa la experiencia. De este modo, cualquier iniciativa que asegure una estadía más breve en el centro de votación será vista con aprobación. La tecnología biométrica supone la eliminación del proceso de verificación manual del documento de identidad y, en consecuencia, la agilización del trámite de identificación. Sin embargo, este análisis supone necesariamente que no se producirá ninguna circunstancia que altere el sistema durante la jornada electoral. En cambio, si pensamos en algunas situaciones que pueden suceder durante la votación, nos daremos cuenta que la identificación biométrica puede ser un factor que alargue el tiempo de espera. Por ejemplo, consideremos los casos de aquellas personas que no pueden participar del sistema debido a que no poseen suficientes propiedades biométricas para ser consideradas. En el

7 Asociación por los Derechos Civiles. *La identidad que no podemos cambiar. Cómo la biometría afecta nuestros derechos humanos.* Pág. 7. Buenos Aires, 2017. Disponible en https://adcdigital.org.ar/wp-content/uploads/2017/06/La-identidad-que-no-podemos-cambiar.pdf (último acceso: 22-04-19)

caso de las huellas dactilares, nos referimos a personas con los dedos vendados, que perdieron un dedo o cuyas huellas no pueden ser captadas debido a que fueron dañadas o se encuentran degradadas. En estas situaciones, seguramente se producirá una interrupción del sistema ya que el afectado protestará, habrá incertidumbre entre las autoridades acerca de lo sucedido, se intentará nuevamente la identificación, etc. Por otro lado, pueden presentarse fallas tecnológicas que también paralicen el funcionamiento del proceso. Así, la biometría se transforma en un factor que puede demorar o incluso detener el desarrollo del acto eleccionario[8].

En definitiva, una vez que examinamos la situación en detalle, nos damos cuenta de que la identificación biométrica no necesariamente es más eficaz, certera, segura o rápida que otros métodos alternativos. En este sentido, un defensor de la biometría sostendría que los riesgos de este tipo de tecnologías pueden ser mitigados a través de un correcto diseño e implementación del sistema. Pero similar argumento vale para sostener la permanencia de los actuales medios de identificación. Mayores medidas de seguridad en los documentos de identidad y un aumento en la capacitación de las autoridades de mesa para detectar falsificaciones también pueden reducir los riesgos asociados a su utilización. Es por ello que el análisis no debe realizarse de manera ligera. Por el contrario, se vuelve indispensable una evaluación integral de todos los pros y contras de los distintos métodos de identificación para poder decidir cuál conviene implementar. Parte imprescindible de esa tarea supone considerar la magnitud de los peligros específicos de cada proceso de identificación. En este sentido, la identificación biométrica presenta ciertas características que deberían impulsar a una actitud cautelosa antes de proponer su aplicación.

La naturaleza del dato biométrico

Existen tres formas principales de comprobar la identidad de una persona: a través de algo que se tiene, a través de algo que se sabe o a través de lo que uno es. En el primer caso, nos referimos a documentos, tarjetas, llaves o algún otro instrumento cuya posesión por parte de la persona es prueba de que esta es quien dice ser. En nuestro sistema electoral, es el medio utilizado para acreditar la identidad de las votantes. Cada vez que una persona acude a un centro de votación en Argentina, se le exige la presentación del documento nacional de identidad previo a la entrega del sobre en el cual se depositará el voto.

8 Ver el ejemplo de Kenya en Privacy International. Biometrics. Friend or Foe of privacy?, pág. 3. 2017. Disponible en https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf (último acceso: 22-04-19)

En el segundo caso, estamos hablando de contraseñas, claves o secretos. Es el medio de identificación utilizado para entrar a sitios web, acceder a dispositivos electrónicos o contactarse con nuestro colega espía, al menos si nos guiamos por lo que nos muestran los libros o las películas. En el último caso, nos encontramos con el dato biométrico. A través de una parte de nuestro cuerpo (rostro, mano, huella dactilar) o mediante un específico comportamiento (forma de caminar o de escribir), somos identificados, ya que se trata de rasgos únicos que no se replican de manera exacta en otro ser humano. La aparición del dato biométrico produjo un salto cualitativo, ya que en este caso se refiere a nuestra propia corporalidad. Una contraseña o un documento es un objeto externo pero un rostro o una huella no. Precisamente, esta característica es utilizada para justificar la adopción de biometría, debido al -supuesto- mayor grado de exactitud que permite esta tecnología. Sin embargo, esto es solo observar una cara de la moneda. Vinculados a la precisión, están los riesgos que un mal tratamiento del dato biométrico puede ocasionar a los derechos de las personas. Al respecto, destacaremos dos características especiales del dato biométrico que sirven de base para nuestras precauciones.

La primera característica es la publicidad del dato biométrico. Podemos guardar nuestros documentos de identidad en un cajón para que no puedan ser vistos. También podemos memorizar una contraseña y después romper el papel. Sin embargo, resulta más difícil ocultar nuestros cuerpos de los demás. Utilizar un pasamontaña cada vez que salimos a la calle para que no reconozcan nuestros rostros no parece ser una solución muy atractiva. Quedarnos encerrados de por vida en nuestras habitaciones tampoco parece ser viable para evitar ser reconocidos por nuestras formas de caminar. Incluso la huella dactilar no se salva de la publicidad, si recordamos los casos en que se las pudo reconstruir a partir de una fotografía.

La segunda característica es que el dato biométrico es insustituible. Podemos cambiar una contraseña. Podemos pedir que se nos extienda otro documento de identidad. Sin embargo, hasta ahora es imposible o extremadamente difícil conseguir una nueva cara o una nueva huella dactilar. Este rasgo resulta importante de considerar en vista de la seguridad. Si una contraseña es robada u olvidada, podemos generar otra y recuperar la seguridad perdida. Sin embargo, si nuestras huellas dactilares son comprometidas de algún modo, no tenemos opción de volver a nuestro nivel de seguridad previo, ya que no podemos reemplazarla por otra diferente.

Como consecuencias de estas características, la legislación ha establecido requisitos estrictos para el tratamiento de este tipo de datos.

La sensibilidad del dato biométrico[9]

Dentro del conjunto de datos personales, existe una categoría especial conformada por aquellos datos que por sus características merecen mayor protección. La razón es que su tratamiento puede llegar a ocasionar serios riesgos para el goce de derechos y libertades fundamentales. A esta clase de datos se lo ha llamado "sensibles" precisamente para remarcar los peligros de un mal uso de los mismos. La decisión sobre qué se considera dato sensible pertenece a la legislación de cada país o región. En este caso nos enfocaremos en la normativa argentina y la europea.

Según la definición de la ley argentina, se considera dato sensible a los "datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual" (art. 2)[10]. La norma fue sancionada en el año 2000 y, por lo tanto, no considera la preponderancia que el dato biométrico posee hoy. De allí, su no mención explícita. Sin embargo, no resulta complicado llegar a la conclusión de que nuestra norma cubre los casos analizados. Pensemos en las huellas dactilares, que a los fines de este trabajo es el ejemplo más importante a considerar.

En 2015, una investigación de las universidades de Carolina del Norte y Washington (EE. UU.) descubrió que las huellas dactilares podrían brindarnos pistas para conocer el origen étnico de una persona[11]. Los investigadores analizaron las huellas dactilares del índice derecho de 243 personas de origen afro-americano o europeo-americano y hallaron diferencias significativas en las bifurcaciones del dedo entre las personas pertenecientes a ambas etnias. Los propios científicos afirmaron que era necesaria una muestra mayor de personas y un análisis de etnias más diversas para obtener una conclusión definitiva. Sin embargo, calificaron de promisorios los primeros resultados en el sentido de que

---

9 Esta sección está basada en Asociación por los Derechos Civiles. *Desafíos de la biometría para la protección de los datos personales. Reflexiones sobre el caso SIBIOS.* 2017. Disponible en https://adcdigital.org.ar/wp-content/uploads/2017/06/ADC-Biometria-y-proteccion-de-datos-personales.pdf (último acceso: 22-04-19)

10 Ley 25.326 de protección de datos personales. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm (último acceso: 22-04-19)

11 Gray, Richard. "Fingerprints reveal whether you're black or white: Distinctive patterns show whether a person is of African or European descent". Mail Online, 29 de septiembre de 2015, disponible en http://www.dailymail.co.uk/sciencetech/article-3253295/Fingerprints-reveal-black-white-Distinctive-patternsperson-African-European-descent.html (último acceso: 22-04-19)

indican una alta posibilidad de que las huellas dactilares reflejen patrones propios de una etnia específica. Debido a que nuestra legislación considera dato sensible a aquellos que revelen "origen racial y étnico", no es descabellado concluir que la huella dactilar podría ser incluida dentro de esa categoría especial.

Esta afirmación encuentra respaldo en las legislaciones más modernas. El Reglamento General de Protección de Datos de la Unión Europea (RGPD) fue sancionado en 2016 y entró en vigencia en 2018[12]. Su reciente aparición lo ha vuelto uno de los instrumentos normativos clave para pensar la protección de datos frente a la masificación de las tecnologías digitales. Es por eso que conviene repasar cómo es considerado el dato biométrico en dicha legislación.

A diferencia de nuestra normativa, el RGPD sí contempla expresamente al dato biométrico. El art. 4 inc. 14 lo define como "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Como se puede observar, la huella dactilar está mencionada como un ejemplo de dato biométrico. Por otro lado, al momento de determinar su calificación jurídica, el Reglamento lo ubica dentro de las "categorías especiales de datos personales", que es el nombre que la norma le da a los datos sensibles. Es por ello que como regla general el RGPD sostiene en el art. 9 que "quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial (...), datos biométricos dirigidos a identificar de manera unívoca a una persona física..." Sea porque es un dato que podría revelar la etnia de una persona o porque se trata de un dato biométrico que tiene como objetivo identificar de manera inequívoca a una persona, la huella dactilar es considerada de manera especial por el ordenamiento jurídico y, por eso, su tratamiento está sujeto a requisitos más estrictos que un dato personal común.

La caracterización de la huella dactilar como un dato sensible -en tanto es un dato biométrico- provee a aquellos de fuertes restricciones en lo que respecta a su utilización por parte de terceros. En ese sentido, podría decirse que la regla general es la prohibición de todo tipo de tratamiento de datos sensibles. Esta lectura encuentra su apoyo en dos disposiciones que se encuentran en el art. 7 de la ley argentina de protección de datos personales. La primera, presente en el inc. 1, establece que "ninguna persona puede ser obligada a proporcionar datos sensibles". La segunda se encuentra en el inc. 3 cuando se dispone que

12 El Reglamento General de Protección de Datos está disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf (último acceso: 22-04-19)

“queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles”.

Cierto es que la propia ley establece excepciones. El inc. 2 del recién mencionado artículo determina que “los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley”. Esta disposición debe ser considerada con mucho cuidado, ya que una mala interpretación puede romper todo el esquema protectorio creado para salvaguardar los derechos de las personas. Efectivamente, bastaría que el Estado diga que una cuestión es de interés general para que no se apliquen las garantías previstas.

Es por ello que una lectura que se ajuste a un régimen democrático y republicano de gobierno debe siempre tratar de limitar el accionar estatal a fin de respetar los derechos de los individuos. Por fortuna, el ordenamiento jurídico argentino dispone de las herramientas para llevar a cabo esa tarea con éxito.

En primer lugar, la propia ley 25.326 establece que las razones de interés general deben ser “autorizadas por ley”. Al momento de desentrañar el significado de “ley”, la Corte Interamericana de Derechos Humanos ha expresado que si la misma tiene por objeto la restricción de un derecho o libertad, debe entenderse que se trata de una “norma jurídica de carácter general (…) emanada de los órganos legislativos constitucionalmente previstos y democráticamente elegidos…”. Por lo tanto, no resulta admisible el dictado de decretos u otros instrumentos de similar naturaleza, ya que el Poder Legislativo no puede intervenir. Así, todo intento de implantar un régimen de identificación biométrica en Argentina debería estar consagrado mediante una ley en sentido formal. Un reglamento, una resolución administrativa o una acordada no es suficiente.

En segundo lugar, no olvidemos que el sistema de protección de datos personales está conformado por un conjunto de principios que deben ser respetados al momento de realizar un tratamiento de datos. Si consideramos que estos principios deben ser cumplidos en el caso de datos personales en general, con más razón se aplican cuando los datos revisten el carácter de sensibles, tal como lo son los datos biométricos. Por lo tanto, al momento de examinar la legalidad del tratamiento, se debe exigir un cumplimiento estricto de los requisitos de licitud, exactitud, finalidad o calidad.

A pesar de esto, se hace necesaria una actualización de la legislación. La ausencia de un marco normativo preparado para afrontar el desafío de la biometría es una característica no solo de Argentina sino de gran

parte de los países en vías de desarrollo. Las tecnologías de biometría se expanden cada vez más en todo el mundo. En este contexto, los países desarrollados ya han diseñado reglas para evitar daños a los derechos de las personas. El RGPD de la Unión Europea es un ejemplo. Sin embargo, en países como Argentina todavía no existen normas que aseguran una protección robusta a sus ciudadanos. Si a esto, le sumamos el hecho de que la precisión y efectividad de estos sistemas es algo que aún está por probarse, el resultado puede ser un escenario de pérdida de derechos sin que se consigan los beneficios prometidos.

Conclusión

El funcionamiento de la democracia se sostiene en la confianza de los ciudadanos. A su vez, la columna vertebral del sistema son las elecciones. Por lo tanto, no puede haber una régimen democrático saludable si el proceso electoral genera escepticismo en la población. La biometría es presentada como una herramienta útil para transparentar el proceso de votación ya que impediría suplantaciones de identidad y así evitaría maniobras de fraude electoral. Sin embargo, el uso de estas tecnologías sin un marco normativo robusto de regulación puede traer más perjuicios que beneficios.

La ausencia de una legislación pensada para abordar este fenómeno es una característica de Argentina así como de otros países de América Latina y el Caribe. De esta manera, los ciudadanos pueden verse en riesgo de que sus datos sean utilizados para fines no previstos o que la falta de medidas de seguridad adecuadas desemboque en alguna filtración que exponga sus datos a terceros no autorizados. A su vez, la falibilidad aún existente seguramente provocará que haya errores de identificación o intentos de engaño al sistema.

Es por eso que como paso previo a cualquier implementación de un sistema biométrico de identificación electoral, deberían establecerse ciertas garantías.

En primer lugar, todo cambio debería hacerse a través de una ley del Congreso de la Nación. La sensibilidad de los datos involucrados y la importancia del proceso electoral exige una deliberación razonada por parte de los representantes de las ciudadanas frente a cualquier modificación que implique riesgos para la privacidad o los datos personales. En segundo lugar, debería establecerse de manera expresa al dato biométrico como dato sensible. Si bien la legislación actual ya posibilita

justificar esta afirmación, una mención clara al respecto sería útil para despejar cualquier duda.

En tercer lugar, la identificación biométrica no debería ser obligatoria sino solo una alternativa frente a la cual el ciudadano podría optar por rechazarla y elegir otro método de identificación.

Por último, los principios existentes en materia de protección de datos deben ser respetados de manera robusta: consentimiento expreso e informado, desarrollo de fuertes medidas de seguridad, límites estrictos al acceso a los datos, utilización exclusiva para el fin propuesto y destrucción del dato cuando ya no es necesario su uso son restricciones típicas que cobran mayor valor cuando el dato es sensible.


por los Derechos Civiles