

# USO DE LA TECNOLOGÍA BIOMÉTRICA EN LA RELACIÓN DE TRABAJO

*Felipe Miguel Carrasco Fernández<sup>28</sup>*

**Sumario:** Palabras Clave. Introducción. 1. Concepto de tecnología biométrica. 2. Reseña Histórica. 3. Clasificación de datos biométricos. 4. Control de la relación de trabajo a través de tecnología biométrica. Conclusiones. Bibliografía.

**Palabras Clave:** Tecnología Biométrica. Datos Biométricos. Relación de Trabajo. Datos Personales. Derechos Fundamentales

## Introducción

La tecnología biométrica consiste en el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o rasgos físicos intrínsecos del individuo, este desarrollo está siendo utilizado regularmente a nivel mundial. Cabe destacar que desde hace mucho tiempo la humanidad ha buscado los mecanismos para poder identificar a cada ser humano como alguien único, y tratar de hacerlo con la mayor exactitud posible utilizando las técnicas de biometría se ha podido llegar hasta un punto en el que es posible realizarlo.

La inclusión de estas técnicas biométricas para controlar el acceso físico a cualquier inmueble o utilización de un servicio es indispensable hoy en día, porque cotidianamente se presentan hurtos, ingresos no deseados o uso no autorizado de los recursos que se encuentran en un área designada o de confianza, la cual puede almacenar objetos o información valiosa para un individuo o empresa.

Mediante estas técnicas biométricas como lo indica Velásquez: “es posible determinar la identificación de un individuo y asegurar que se trata de este, que no se están haciendo suplantaciones, la gran ventaja con esta tecnología es que no es necesario cargar llaves, tarjetas

---

<sup>28</sup> Profesor investigador de la Facultad de Derecho de la Universidad Popular Autónoma del Estado de Puebla (UPAEP)

o algún otro mecanismo y que a su vez pueda ser extraviado y aprovechando esta situación extraer los objetos de valor del inmueble”<sup>29</sup> o acceder a determinadas áreas de la empresa.

Para Tolosa, “todos los seres humanos tenemos características morfológicas únicas que nos diferencian. La forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital, son algunos rasgos que nos diferencian del resto de seres humanos.”<sup>30</sup>

Si bien el desarrollo de este tipo de tecnología y su implementación en los diversos sistemas automatizados de datos puede traer grandes beneficios para el desarrollo social y para los gobiernos en la medida que facilita la identificación indubitable de la persona, es imprescindible no dejar de tener en consideración que muchas veces implican una serie de riesgos a las personas naturales, afectando, amenazando y privándolas del ejercicio de algunos derechos fundamentales.

Por lo tanto, resulta necesario crear sistemas normativos de protección que sean capaces de conjugar estas relaciones entre datos personales y derechos fundamentales, creando condiciones para que el uso de esta tecnología ayude a satisfacer derechos sin afectar negativamente el ejercicio de otros, o al menos puede anhelarse afectarlos en la menor medida posible, y sólo bajo circunstancias en las que resulte realmente necesario.

## 1. Concepto de tecnología biométrica

La palabra biometría tiene su origen en las siguientes palabras: *bio*, que significa vida, y *metron* que significa medida. De esta forma, la biometría vendría a ser una especie de medición de la vida, por lo que, en otras palabras, los dispositivos biométricos buscan medir o identificar características que son propias de los seres vivos. Pato y Millet definen el uso de datos biométricos como “el reconocimiento automático de los individuos en base a sus características biológicas y de comportamiento.”<sup>31</sup>

---

<sup>29</sup> Velásquez Valencia, Jorge Eduardo y Linares Jaramillo, Álvaro Andrés. “Soluciones Inteligentes para el control de acceso físico mediante el uso de tecnología biométrica”. Universidad Tecnológica de Pereira. Facultad de Sistemas. Ingeniería de Sistemas y Computación Pereira. 2013. En Línea: <http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4090/0053682V434.pdf;jsessionid=BD2069D6A97A5B9F4536E2847DCDE383?sequence=1> p. 12

<sup>30</sup> Tolosa Borja, César y Giz Bueno, Álvaro. “Sistemas Biométricos”. En Línea: [https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web\\_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf](https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf) p. 1

<sup>31</sup> Pato y Millet citado por Muñoz Gallardo, Sebastián Andrés. “Datos Biométricos y Derechos Fundamentales”. Facultad de Derecho. Departamento de Derecho Procesal. Universidad de Chile. Santiago, 2017. En Línea:

La biometría para Soto, se puede definir como “la ciencia que estudia los métodos automatizados de identificación de los sujetos y en el ámbito de la tecnología de la información se utilizara el término autenticación biométrica que se basan en características físicas/anatómicas (reconocimiento facial, geometría de la mano, iris) o rasgos conductuales/dinámicos (firma, dinámica de teclado, voz)”<sup>32</sup> las técnicas biométrica poseen ventajas y desventajas comparativas, las cuales deben tenerse en consideración al momento de decidir que técnica utilizar para alguna aplicación específica.

De acuerdo a la naturaleza de la información que configura un dato biométrico, es posible identificar que se trata de información sobre una persona, o más bien de ella misma en el sentido de describir una característica unida esencialmente a ella. En concordancia con lo anterior podemos establecer a priori que se tratan de datos personales.

El concepto de dato personal conlleva implícito dos ideas. En primer lugar, la idea del dato, que es información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho. Por otro lado, se encuentra el carácter de personal, en virtud del cual existe una conexión de este dato con una persona identificada o identificable.

En caso de no existir tal relación, la información contenida en esos datos será anónima y por lo tanto no será merecedora de protección por parte del ordenamiento jurídico.

El reconocimiento biométrico responde a un sistema automático basado en la inteligencia artificial y el reconocimiento de patrones, que permite la identificación y/o verificación de la identidad de personas a partir de características morfológicas o de comportamiento, propias y únicas del individuo, conocidas como autenticadores. Asimismo, la naturaleza del tipo de característica, morfológica o de comportamiento, se encuentra directamente relacionada con el grado de variación de las mismas con el paso del tiempo.

La biometría es una de las formas más eficaces para trabajar en seguridad empresarial, ya que un individuo cuenta con rasgos únicos que lo hacen diferente a cualquier otra persona,

---

<http://repositorio.uchile.cl/bitstream/handle/2250/145203/Datos-biom%C3%A9tricos-y-derechos-fundamentales.pdf?sequence=1> p. 11

<sup>32</sup> Soto Aravena, Patricia Paola. “Impacto en los trabajadores por la implantación de un sistema biométrico en la automatización de los tiempos y control de asistencia”. Máster en Dirección de Recursos Humanos. MÁSTERES de la UAM. Facultad de Psicología. Ediciones UAM. Año Académico 2010-11. En Línea: <http://docplayer.es/7158217-Impacto-en-los-trabajadores-por-la-implantacion-de-un-sistema-biometrico-en-la-automatizacion-de-los-tiempos-y-control-de-asistencia.html> p. 13

de esta manera se pueden utilizar dichas características para brindar el acceso a un recinto, donde solo esta persona pueda tener acceso, y que, de igual manera, así se puede solucionar el problema de extraviar llaves o tarjetas las cuales son usadas para poder ingresar a un sitio de la empresa.

Para Velásquez, los beneficios que trae consigo la tecnología biométrica “es el incremento de la protección de identidad, la disminución de los riesgos de privacidad, la protección de derechos civiles y a la libertad civil, es por eso que en un mundo donde la tecnología avanza rápida y constantemente, la solución a esto requiere el desarrollo de sistemas complejos y robustos.”<sup>33</sup>

Cada día agencias gubernamentales, entidades, empresas, instituciones académicas confían más en la tecnología biométrica gracias a sus sistemas de seguridad que utilizan características morfológicas de cada individuo, contribuyendo así al no uso de tarjetas que son extraviadas con facilidad.

La biometría ya ha sido definida y abordada en el paradigma de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), al propiciar una reflexión en cuanto a su regulación y los derechos de las personas. De esta forma, dicho organismo ha señalado que la biometría consiste en características únicas y medibles de rasgos en los seres humanos que sirven para automáticamente reconocer o verificar una identidad. La relevancia de la biometría hoy en día está dada por el gran aumento de sistemas automatizados para identificar a las personas, ya sea por los gobiernos o las empresas privadas. En la misma línea, otros autores agregan más elementos a considerar en la biometría: no sólo se trataría de características o rasgos físicos, sino además de comportamientos que permitirían una identificación. Así las cosas, la biometría se entenderá para Korja “como aquellos mecanismos automatizados para determinar la identidad de una persona basada en sus aspectos fisiológicos o conductuales.”<sup>34</sup>

Las tecnologías que se han utilizado han sido creadas de acuerdo a las diferentes técnicas de identificación o de recolección de información biométrica tales como las huellas digitales, la voz, el rostro, los ojos y otras más que constantemente se desarrollan como evolución y mejoramiento de estas herramientas. Por lo tanto como lo indica Velásquez: “hoy

---

<sup>33</sup> Velásquez Valencia, Jorge Eduardo y Linares Jaramillo, Álvaro Andrés *op. cit.* p. 13

<sup>34</sup> Korja citado por Garrido Iglesias, Romina y Becker Castellaro, Sebastián. “La biometría en Chile y sus riesgos”. Revista Chilena de Derecho y Tecnología, Vol. 6 Núm. 1, 2017. En Línea: <https://rchdt.uchile.cl/index.php/RCHDT/article/view/45825/48403> p. 3

en día se puede aprovechar completamente la funcionalidad de estas herramientas para la identificación plena de un individuo evitando así la suplantación de identidad y al utilizarlas adecuadamente dentro de un entorno donde sea necesario un sistema de seguridad para salvaguardar algo en específico se puede garantizar que solo las personas indicadas puedan tener acceso a este.”<sup>35</sup>

La identificación biométrica es utilizada para verificar la identidad de una persona midiendo digitalmente determinados rasgos de alguna característica física y comparando esas medidas con aquéllas de la misma persona guardadas en archivo en una base de datos o algunas veces en una tarjeta inteligente que lleva consigo la misma. Las características físicas utilizadas son huellas digitales, huellas de la voz, geometría de la mano, el dibujo de las venas en la articulación de la mano y en la retina del ojo, la topografía del iris del ojo, rasgos faciales y la dinámica de escribir una firma e ingresarla en un teclado.

El funcionamiento de estos sistemas para Tolosa, “implica de la necesidad de un potente software con unas fases diferenciadas en las cuales intervienen diferentes campos de la informática, como son: el reconocimiento de formas, la inteligencia artificial, complejos algoritmos matemáticos y el aprendizaje. Éstas son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos.”<sup>36</sup>

Los escáneres de huellas digitales y equipos de medición de geometría de la mano son los dispositivos más utilizados. Independiente de la técnica que se utilice, el método de operación es siempre la verificación de la identidad de la persona para una comparación de las medidas de determinado atributo físico.

Los datos biométricos tienen dos características fundamentales:

- Son obtenidos por tratamientos automatizados para verificar o determinar la identidad de personas a través de características fisiológicas o conductuales.

- Reconocen características fisiológicas, físicas, conductuales o psicológicas: las características fisiológicas o físicas se definen como medidas o mediciones a parte o partes del cuerpo humano (escáner al iris o huellas dactilares, patrones geométricos del rostro u orejas, reconocimiento de voz, etcétera).

---

<sup>35</sup> Velásquez Valencia, Jorge Eduardo y Linares Jaramillo, Álvaro Andrés. *op. cit.* p. 34

<sup>36</sup> Tolosa Borja, César y Giz Bueno, Álvaro. *op. cit.* p. 4

Para Korja, los datos biométricos para que puedan cumplir la función de identificar a las personas o bien autentificarlas, deben reunir las siguientes características:

- a) Medibles: la facilidad por la cual es posible leer el dato.
- b) Robustos: en cuanto a cómo el dato individual va modificándose con el tiempo.
- c) Aceptables: deben mostrar aspectos positivos del individuo.
- d) Universales: que toda población tenga aquel dato que se extrae del individuo.
- e) Distintivos: debe mostrar una gran variabilidad sobre el resto de la población para asegurar la individualidad del dato en cuestión.<sup>37</sup>

Los datos biométricos para la Asociación por los Derechos Civiles pueden clasificarse en tres grandes grupos:

- Datos estáticos: aquéllos que se extraen de las características físicas de cualquier individuo. Suelen ser huellas dactilares, imagen del rostro, iris de los ojos, etcétera, y se recolectan a través de programas de reconocimiento facial; por ejemplo, es posible identificar a una persona de acuerdo a las distancias que hay entre su nariz, su boca y sus ojos, y con ellas generar modelos geométricos de rostro para la identificación posterior.

- Datos dinámicos: aquéllos que se concentran en el comportamiento, forma de caminar, manera en la que firma o utilización del teclado de un computador, entre otras. Estos mecanismos detectan patrones de conducta para vincularlas con una persona en particular.

- Datos mixtos: Combina ambas técnicas ya mencionadas, como por ejemplo el patrón de voz o comportamientos de discurso.<sup>38</sup>

Los datos biométricos son principalmente usados para la identificación de personas, la que puede ser a través de autentificación (o verificación) de identidad o a través de identificación.

La autentificación o verificación de identidad se da cuando en una primera fase es realizada la recopilación de uno o más datos biométricos (por ejemplo, la muestra del iris, huella digital o rostro de una persona) para que sea procesado y almacenado en una base de datos biométricos. Esta fase del proceso se llama inscripción y elaboración de una planilla biométrica. Posteriormente, se compara la plantilla biométrica con el dato entregado; si coinciden, será verificada la identidad de aquella persona.

Los datos biométricos están siendo utilizados hoy día para garantizar rigurosos estándares de seguridad al entrar a sistemas de información altamente seguros o lugares comunes como trabajos, escuelas, estadios u otros; sirven para facilitar la autentificación a usuarios en internet y realizar compras. En la actualidad existe autentificación con huellas

---

<sup>37</sup> Korja citado por Garrido Iglesias, Romina y, Becker Castellaro, Sebastián. *op. cit.* p. 3

<sup>38</sup> Asociación por los Derechos Civiles citada por Garrido Iglesias, Romina y Becker Castellaro, Sebastián. *op. cit.* p. 68

digitales o reconocimiento facial, tecnologías que han permitido mayor seguridad en las industrias; incluso se utiliza para entrar a un puesto de trabajo.

Para la OCDE, la biometría en sí no implica necesariamente un aspecto dañino o benigno para la privacidad, sino que deviene necesariamente de los usos que se le den y cómo hacemos frente a sus desafíos para la privacidad de las personas. De este modo, sugiere que, con diseños y políticas apropiadas al respecto, no es necesario escoger entre privacidad o seguridad, sino que es posible encontrar soluciones que permitan mejorar los aspectos económicos y sociales de los países.

El marco regulatorio por el cual deben ceñirse las empresas es sumamente débil, y el que existe no consta que se esté cumpliendo, a pesar de que extraer huellas dactilares implica que hay riesgos de divulgaciones no autorizadas, flujos de datos biométricos interempresas, discriminación en la entrega de servicios, robo de identidades, etcétera. Todos estos riesgos conllevan que puedan existir múltiples identidades digitales, vulneraciones a derechos humanos y otras lesiones a los derechos de las personas.

Los principios de la Unión Europea establecen como fundamental el consentimiento expreso para la utilización de datos biométricos. En caso de que no existan autorizaciones correspondientes por las personas dueñas de los datos biométricos, su derecho fundamental a la privacidad u otros derechos fundamentales será vulnerado. Para Garrido, “todos los individuos tienen derecho a tener el control de sus datos personales y, en la medida que éstos sean transferidos o divulgados sin su consentimiento, existe una vulneración a los derechos de las personas.”<sup>39</sup>

La mayoría de los sistemas biométricos funcionan con arreglo a un modelo general que consiste en dos pasos. El primer paso es el registro de la persona en el sistema. Durante el proceso de registro, el sistema captura el rasgo característico de la persona, como por ejemplo la huella digital, y lo procesa para crear una representación electrónica llamada modelo de referencia.

De acuerdo con la teoría tradicional en biometría, el segundo paso depende de si la función del sistema biométrico consiste en verificar la identidad de la persona o identificar a la persona. En el caso de verificación, la persona le informa al sistema cuál es su identidad, ya sea presentando una tarjeta de identificación o introduciendo alguna clave especial. Se captura

---

<sup>39</sup> Garrido Iglesias, Romina y Becker Castellaro, Sebastián. *op. cit.* p. 83

el rasgo biométrico y se compara con el modelo de referencia de la persona. Si ambos modelos coinciden, la verificación se realizó con éxito, si no es fallida.

En caso de que sea identificación, la persona no le informa al sistema biométrico cuál es su identidad. El sistema tan sólo captura el rasgo biométrico y lo compara con un conjunto de modelos de referencia para determinar la identidad de la persona.

Existe una gran variedad de tecnologías biométricas, tantas como características biométricas. Muchas de ellas se están aplicando en la vida real y otras están en proceso de estudio. Algunas características biométricas que se utilizan actualmente son: voz, huellas dactilares, cara, iris, retina, venas de la mano, forma de la mano, forma de la oreja, forma de andar, forma de escribir en un teclado, firma, ADN y olor. Partiendo de estas características se han desarrollado dispositivos que han tenido mayor o menor éxito en el mercado. En la actualidad, los sistemas comerciales más usados son:

- a) Reconocimiento facial
- b) Lector de impresión digital por medio de huella dactilar.
- c) Reconocimiento de manos que puede hacerse en dos o tres dimensiones, la primera busca patrones en las líneas de la palma de la mano, y el de tres dimensiones funciona a través de la medición de la mano, el largo de los dedos, la altura de la mano, etc.
- d) Sistema de autenticación biométrica de las venas de la palma de la mano y de los dedos
- e) Sistema de identificación mediante el iris basada en los patrones de la retina
- f) Sistema de reconocimiento de firmas mediante un sistema de bolígrafo que contiene varios sensores.
- g) Sistema de Reconocimiento de voz que detecta el espectro de la frecuencia de voz de una persona.

El costo de los sistemas biométricos va reduciéndose progresivamente mientras que su fiabilidad y precisión cada vez va en aumento. Existen diversos tipos de enfoques de autenticación como lo expone Areitio:

Lo que uno sabe (una contraseña o password, responder a preguntas, passphrases, etc.), lo que uno lleva (una tarjeta inteligente con PIN), lo que uno es (biometría), donde se encuentra geográficamente (en base a localización GPS o etiquetas RFID ocultas dentro del cuerpo humano), etc. Para que la autenticación sea usable se requiere que cumpla propiedades como que sea memorizable, entendible, no vulnerable al phishing, aceptable psicológicamente, que

haga uso de las capacidades cognoscitivas de las personas, por ejemplo que se base en el reconocimiento en vez de tener que recordar.<sup>40</sup>

Algunos de los beneficios que ofrece la tecnología biométrica como lo cita Areitio, son:

- (1) La biometría vincula un evento a un individuo concreto no a una contraseña o dispositivo que lleve como tarjeta inteligente o llave criptográfica USB.
- (2) Puede considerarse una tecnología conveniente ya que no se tiene que recordar.
- (3) Es el mismo independiente donde se encuentre el individuo.
- (4) No puede averiguarse, robarse, transferirse, compartirse, delegarse, perderse, olvidarse o copiarse fácilmente.
- (5) Previene la suplantación (protege contra robo de identidad y posee un alto grado de no repudio).
- (6) Mejora la privacidad (protege contra acceso no autorizado a información personal).
- (7) Es complementario con otros mecanismos de autenticación (como tarjetas inteligentes con PIN y PKI).<sup>41</sup>

La revolución en la tecnología de la información ha producido un rápido incremento en el uso de PINS y contraseñas. Por esto en palabras Tobías “es necesario restringir el acceso a datos personales. Las técnicas biométricas, que sustituyen el uso de PINS y contraseñas, son más prácticas para el usuario y pueden prevenir con mucha más efectividad el acceso sin autorización o uso fraudulento de teléfonos móviles, ordenadores, sistemas y redes informáticas, tarjetas de identificación, contraseñas y PINS.<sup>42</sup>

En la actualidad se utilizan varios tipos de sistemas biométricos para la identificación en tiempo real. Los más populares son la geometría facial y huella digital. Un sistema biométrico en general consta de componentes tanto hardware como software necesario para el proceso de reconocimiento.

Dentro del hardware se incluyen principalmente los sensores que son los dispositivos encargados de extraer la característica deseada. Una vez obtenida la información del sensor, será necesario realizar sobre ella las tareas de acondicionamiento necesarias, para ello se emplean diferentes métodos dependiendo del sistema biométrico utilizado. Por ello se han descrito los principales tipos de sistemas biométricos existentes que según Tolosa, son:

---

<sup>40</sup> Areitio, Javier y, Areitio, Teresa. “Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación”. Control de Accesos. Mayo 2007. En Línea: <https://es.scribd.com/document/13156295/Biometricos> p. 52

<sup>41</sup> *Ídem*. p. 54

<sup>42</sup> Tobías Martínez, Miguel Ángel. “Análisis de factibilidad de la implementación de un sistema de asistencia a clase mediante huella dactilar en la Facultad de Ingeniería Arturo Narro Siller”. Centro Universitario Tampico – Madero, noviembre de 2010. Facultad de Ingeniería Arturo Narro Siller. Universidad Autónoma de Tamaulipas. En Línea: <https://es.scribd.com/document/299912324/TESIS> p. 11

“Reconocimiento de la huella dactilar; Reconocimiento de la cara; Reconocimiento de iris/retina; Geometría de dedos/mano; Autenticación de la voz; Reconocimiento de la firma.”<sup>43</sup>

Entre las ventajas de la biometría, Olivares, considera las siguientes “Reduce la posibilidad de fraude; Es imposible olvidar su huella; Es imposible perder la huella; La huella no se puede prestar a nadie; Es prácticamente imposible de falsificar; ahorra tiempo al contabilizar; Fácil de usar y aprender; Bajo costo de inversión; No requiere consumibles; Rápido retorno de inversión.”<sup>44</sup>

## **2.- Reseña Histórica**

Aunque se podría pensar en la biometría como una ciencia-ficción futurista, los principios básicos de la biometría eran comprendidos y utilizados miles de años antes. Está comprobado, que, en la época de los faraones, en el Valle del Nilo (Egipto) se utilizaban los principios básicos de la biometría para verificar a las personas que participaban en diferentes operaciones comerciales y judiciales.

Muchas son las referencias de personas, que, en la antigüedad, han sido identificados por diversas características físicas y morfológicas como cicatrices, medidas, color de los ojos, tamaño de la dentadura. Esta clase de identificación se utilizaba, por ejemplo, en las zonas agrícolas, donde las cosechas eran almacenadas en depósitos comunitarios a la espera de que sus propietarios dispusieran de ellas. Los encargados de cuidar estos depósitos debían identificar a cada uno de los propietarios cuando estos hicieran algún retiro de su mercadería, utilizando para esta tarea principios básicos de biometría como eran sus rasgos físicos.

Luego, en el siglo XIX hubo un gran interés por parte de investigadores en criminología, cuando intentaron relacionar características físicas con tendencias criminales. Esto resultó en una variedad de equipos de medición y gran cantidad de datos recogidos. Los resultados no eran concluyentes, pero la idea de medir las características físicas de un individuo parecía efectiva y el desarrollo paralelo de la identificación de huellas digitales se

---

<sup>43</sup> Tolosa Borja, César y Giz Bueno, Álvaro. *op. cit.* p. 1

<sup>44</sup> Olivares Morales, Alejandro. “Automatización del proceso de control de asistencia del personal académico en tiempo real a través de reconocimiento biométrico”. Facultad de Ingeniería. Universidad Nacional Autónoma de México. Marzo 2010. En Línea: <http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/1188/Tesis.pdf> p. 51

convirtió en la metodología internacional para identificación utilizada por las fuerzas policiales de todo el mundo.

Los orígenes de la biometría se remontan a los años setenta, cuando la empresa NEC comienza a trabajar junto al FBI en algunos estudios de como automatizar biométricamente algunas características del ser humano. De esa forma se comienzan a desarrollar una serie de algoritmos matemáticos con la finalidad de representar, por ejemplo, una huella dactilar.

No es sorprendente que por muchos años haya existido una fascinación con la posibilidad de usar la electrónica y el poder de microprocesadores para automatizar la verificación de identidad por parte de individuos y organizaciones tanto en el ámbito militar como comercial. Varios proyectos fueron comenzados para ver el potencial de la biometría, y uno de estos proyectos eventualmente llevó a la creación de un abultado y extraño lector de geometría de mano.

El éxito de su funcionamiento motivó a sus diseñadores a refinar el concepto. Eventualmente, una pequeña compañía y un mucho más pequeño y más desarrollado lector de geometría de mano fueron introducidos al mercado y se convirtió en uno de los pilares de la industria biométrica.

Paralelamente, otras metodologías biométricas como la verificación de huellas digitales eran constantemente mejoradas y refinadas al punto de convertirse en equipos confiables y fácilmente desplegados, como lo expone Tolosa “en años recientes, también se ha visto interés en el escaneo de iris y reconocimiento facial, técnicas que ofrecen el potencial de no necesitar contacto.”<sup>45</sup>

### **3.- Clasificación de datos biométricos**

Existen diversas clasificaciones respecto de los datos biométricos, entre las que encontramos las siguientes:

**A.- Datos Biométricos Estáticos.** Son aquellos datos que se relacionan en mayor medida con características físicas o estructurales de las personas y que, por lo tanto, son en general permanentes en el tiempo, ya que se relacionan directamente con órganos o sistemas anatómicos humanos. Dentro de este tipo de datos se encuentran los datos respecto al ADN,

---

<sup>45</sup> Tolosa Borja, César y Giz Bueno, Álvaro. *op. cit.* p. 2

las huellas dactilares, el color del iris, los rasgos faciales, la piel o la composición química del cuerpo.

B. Datos Biométricos Dinámicos. En contraposición a las formas estáticas, los datos biométricos dinámicos se determinan en relación con características funcionales o del comportamiento de las personas. Este comportamiento se diferencia de los datos estáticos, debido a su naturaleza no sólo tiene aptitud para mutar, sino que es muy probable que ocurra durante la vida del individuo. Dentro de este tipo de datos encontramos información relativa a la forma de caminar, el comportamiento al firmar, el ritmo al hablar, forma de teclear, o gestos y movimientos corporales.

C.- Datos biométricos mixtos. Este tipo de datos corresponden a aquellos que utilizan y entremezclan tanto datos estáticos como dinámicos. Un ejemplo de esta tercera categoría es el discurso de un individuo, que mezcla características fisiológicas, como lo son las que producen un determinado tono de voz, y datos dinámicos, como el ritmo al hablar. En estos casos el sistema, mediante un algoritmo que intenta simular la capacidad del cerebro humano de aprender y tomar decisiones, sería capaz de unir diferentes métodos de identificación biométrica como el color de los ojos, la forma de la cara o las huellas dactilares de una persona. El algoritmo también puede aprender patrones biométricos asociados a diferentes conjuntos de información, permitiendo combinar datos, tales como las huellas dactilares, la voz, o la forma de andar, en lugar de depender de un único sistema biométrico.

#### **4.- Control de la relación de trabajo a través de tecnología biométrica**

Henri Fayol, el padre de la teoría moderna de la administración operacional, señaló que todos los procedimientos que desarrollan las actividades de las empresas se dividen en seis operaciones: Técnicas (producción, fabricación, transformación de insumos), Comerciales (compras, ventas, intercambios, búsqueda de mercados), Financieras (captación y gerencia o administración de los capitales), Seguridad (protección de los bienes y de las personas), Contabilidad (inventario, balance, previsión de costo, estadística, precios, etc.), Administrativas o de Gerencia (previsión, organización, mando o dirección, coordinación y Control). En las actividades de gerencia se encuentra la función de control, que procura la vigilancia para que todo se desarrolle de acuerdo a las reglas establecidas y a las órdenes dadas. Lo importante es verificar que todo acontezca conforme al programa adoptado a personas,

actos y cosas en cuanto a las órdenes y principios impartidos, con el propósito además de señalar, reparar y evitar los errores y su futura duplicación.

La función administrativa de control, tratar de asegurar que las diversas unidades de la organización marchen de acuerdo con lo previsto. Existe el control en la función administrativa, que mide, evalúa y corrige lo que ha sido planificado, organizado y dirigido por el nivel organizacional (control estratégico) a nivel intermedio (control táctico) o a nivel operativo (control operativo) para alcanzar los objetivos y las metas previstas. El control en la regulación de estándares, se regula automatizadamente constante el funcionamiento dentro de los estándares deseados. Finalmente, el control para Chiavenato “en la función restrictiva y limitadora, se utiliza el expediente de los empleados para mantener el mismo patrón de conducta.”<sup>46</sup>

Las fases del proceso de control y los criterios para impulsar una conducta autónoma del trabajador deben conciliarse con los medios para que personas permanezcan dentro de los estándares establecidos, en una conducta normalizada y predecible a través de un proceso exitoso de socialización. Entre los medios que incluyen el control social están las jerarquías de autoridad, estatutos, leyes y procedimientos, establecimiento de objetivos, medios de comunicación, etc.

Respecto del sistema de control en el área de recursos humanos debemos considerar que el valor del capital humano para el cumplimiento de un plan estratégico es un factor clave sobre todo por la adaptación a los nuevos cambios para ser cada vez más competitivos en la sociedad actual a nivel tecnológico, sociológico, comercial, político y económico. Lo anterior repercute indudablemente en las relaciones laborales, la estructura organizativa y en los sistemas de gestión.

El subsistema de control es una tendencia actual en la mayoría de las empresas para optimizar cada vez más sus procesos internos de gestión. La deficiencia de ellos provoca tareas repetitivas, pérdidas de tiempo laborales en la productividad, absentismo laboral, sobre costos por tiempo facturado no laborado, errores humanos por liquidación manual.

En la Edad Media los controles de acceso físicos estaban dirigidos por los señores feudales, reyes, emperadores que a través de sus fortalezas regulaba quien entraba a sus moradas. En la Revolución Industrial se controlaba la asistencia de la mano de obra artesanal

---

<sup>46</sup> Chiavenato citado por Soto Aravena, Patricia Paola. *op. cit.* p. 7

de manera verbal, pronunciando su nombre y registrando al empleado según el criterio del dueño en un libro su cumplimiento al trabajo. En la Época Moderna se utilizaba el libro de registro de personal, donde el funcionario tenía que firmar y anotar su nombre, con la fecha y hora de entrada y salida de su trabajo. En la actualidad, a partir de la década de los años 90 del siglo pasado, se empiezan a utilizar el reloj de marcado con tarjetas magnéticas, los números de identificación para controlar al personal, no ha siendo hasta ahora 100% seguros ni validos en sus resultados, ya que es fácil que en esta tecnología exista la marcación fraudulenta de un trabajador frente a otro compañero de trabajo para poder facturar tiempo no laboral o entrar en un área restringida.

Las herramientas no han evolucionado mucho hace 40 años y el impacto de las nuevas tecnologías juega un papel fundamental, así como en todo proceso tecnológico tienen mayor transcendencia las que provienen de estudios y casos de éxito en campos gubernamentales o militares, tal como lo fue a su vez la tarjeta, el reloj o ID. Es así como en el año 1982 el FBI marcó las primeras directrices para establecer un concurso público para animar a investigadores a dotar de automatización a un sistema universalmente expandido como era la dactiloscopia. Así es como nació el *Automated Fingerprint Identification System (AFIS)* Sistema Automatizado de Identificación Dactilar. Dicho concurso fue ganado por la empresa *Morphosistemas* empresa subsidiaria del Líder Mundial de sistema de Comunicaciones *Sagem Defense Et Securite*. La efectividad del sistema permitió a instancias del propio FBI, la expansión y estandarización del propio sistema a los diferentes Estados para el intercambio de información en materia de inmigración y terrorismo. Sin embargo, no fue hasta mediados del año 2000 cuando dicha tecnología fue liberada para el sector civil, tras los atentados del 11 de septiembre y con una clara intención de popularizar su uso hasta lo que conocemos hoy en día como los sistemas biométricos.

En el último tiempo se han perfeccionado exitosamente los procedimientos de control de accesos y de asistencia a los empleados. Así, ha sido la evolución de los libros de registro a los distintos tipos de relojes de control de trabajo. Encontrándose, los relojes de marcado (mecánicos y eléctricos), relojes de fichar informatizados (con tarjeta chip, con microprocesador incorporado sin necesidad de conexión a PC y los de tarjeta magnética) y

finalmente los relojes de fichar mediante huella dactilar, con la función de medir exactamente los tiempos de producción y la remuneración real por hora trabajada.<sup>47</sup>

Desde un punto de vista empresarial el propósito central del sistema biométrico es integrar y consolidar todas las áreas de seguridad y presencia en un mismo patrón tecnológico.

Así a través de la tecnología biométrica se permite realizar un exhaustivo control del tiempo de presencia y/o ausencia de los empleados; calendario laboral, jornada de trabajo, motivos de ausencia, horas extras, vacaciones, capacitación, convenios y los contratos laborales utilizando los mismos dispositivos que para el control de seguridad. Las tecnologías biométricas son usadas extensivamente para proporcionar la autenticación fuerte de un usuario y evitar las brechas en la seguridad de las tarjetas, añadiendo una movilidad, ergonomía y facilidad en el uso con el simple acto de posicionar el dedo en un sensor, el efecto diferenciador y de evolución tecnológica está garantizado.

La gestión de control en el área de recursos humanos se programa el dispositivo para su tratamiento de entrada, salida o ambos a la vez, como también en relación a las fechas del calendario laboral, se actualiza la ficha del empleado con todos los antecedentes apellidos, nombre, cargo, país, fecha de alta, horas permitidas en la jornada, duración de la jornada y hora de inicio de la jornada laboral. En los tratamientos de incidencias se registran todos los motivos especiales adicionales a la jornada normal de trabajo, indicando su duración en el calendario laboral, la hora de comienzo de la incidencia como sus observaciones en las enfermedades comunes, enfermedades laborales, días festivos, capacitación y vacaciones. Para Soto “los informes del personal están estipulados por filtros del ID del usuario, su fecha de inicio y fin, el mes y año para elegir el tipo de resumen que necesita tanto en horas individuales, horas globales, accesos individuales como del calendario mensual individual.”<sup>48</sup>

Dentro de las ventajas en la implementación del control de acceso biométrico en el ámbito laboral encontramos como lo indica Gutiérrez, que este sistema:

- a) Elimina suplantaciones de identidad de los empleados, controlando el ingreso de personas no autorizadas a la entidad.
- b) Organiza las horas de ingreso y salida de los empleados.
- c) Disminuye costos de funcionamiento.
- d) No existe riesgo de falsificación.
- e) El medio de identificación es única y personal.
- f) Método seguro de identificación, pues no existe dos huellas digitales iguales en el mundo.

---

<sup>47</sup> Soto Aravena, Patricia Paola. *op. cit.* p. 10

<sup>48</sup> *Ídem.* p. 27

- g) Bajo costo de implementación permitiendo instalaciones en ciertas etapas interactuando con otros tipos de controles de seguridad.<sup>49</sup>

Los datos biométricos representan en la sociedad de las últimas décadas, una total transformación a nivel global motivada por el desarrollo de nuevas formas de tecnología. Estas transformaciones han llegado, en gran medida, a simplificar tareas que históricamente han sido costosas en términos económicos y temporales. Los datos biométricos surgen dentro de este contexto, como lo indica Muñoz “pues las tareas de identificación y verificación juegan importantes roles en el mundo moderno, y vienen a reemplazar en la mayoría de los casos, mecanismos de seguridad bastante más rudimentarios e inseguros, contribuyendo a eliminar en gran medida el porcentaje de incertidumbre que estos mecanismos rudimentarios conllevan.”<sup>50</sup>

Es importante precisar que la captura de datos biométricos por parte de la empresa derivada de la relación laboral que tiene con los trabajadores, estos tienen la protección de la legislación correspondiente a protección de datos personales en relación a este tema podemos encontrar que la legislación de diversos países en materia laboral es omisa respecto a reglamentar los datos personales de los trabajadores y su protección jurídica dentro del contexto de la normativa jurídica laboral, haciendo caso omiso o una total ausencia legislativa al respecto.

Otro grupo de países si bien son omisos respecto a los datos biométricos en las relaciones laborales, y no se encuentra reglamentada en forma específica en dicha reglamentación si tienen leyes protectoras respecto a los datos personales de los trabajadores, por lo tanto, gozan de la protección jurídica los trabajadores en relación a sus datos personales cuando esos son propiciados al patrón con motivo de su contrato o relación de trabajo.

Y un tercer grupo considera los datos biométricos como datos sensibles y por lo tanto gozan de las garantías jurídicas del derechos de protección de datos personales, considerándolos como sensibles en virtud de que identifican fácilmente a una persona en específico, como consecuencia de lo anterior, la implicación jurídica que tiene el uso de la tecnología biométrica en los centros de trabajo es comprobada para controlar la actividad

---

<sup>49</sup> Gutiérrez Ricardo, Jorge Enrique. “Estudio de factibilidad para el control de acceso biométrico, en una empresa empleando lectores de huella digital”. Universidad De La Salle. Bogotá D. C. 2007. En Línea: <http://repository.lasalle.edu.co/bitstream/handle/10185/2158/T91.07%20G985e.pdf?sequence=1&isAllowed=y>  
p. 21

<sup>50</sup> Muñoz Gallardo, Sebastián Andrés. *op. cit.* p. 37

laboral de los empleados y lograr su máximo rendimiento durante la jornada laboral pero el patrón debe ser sumamente cuidados respecto a la utilización de la biometría ya que deberá salvaguardar los derechos de los trabajadores y reconocer la protección de datos personales de éstos en virtud de que el tratamiento de dichos datos son un bien jurídico tutelado por el derecho y en consecuencia los datos biométricos gozan de la protección jurídica de datos personales que se encuentra ligada a la idea de intimidad o privacidad; por lo tanto, la evolución tecnológica e informática si bien facilita la interacción de datos, su tratamiento y transferencia, debe ser de sumo cuidado por el sector patronal toda vez que podría presentar una colisión de derechos entre el derecho de control de la actividad laboral por parte del empleador en relación al trabajador y por parte del derecho de protección de datos del trabajador.

Aldunate, define colisión de derechos como la situación en que “el efecto jurídico de la protección iusfundamental alegada por un sujeto es incompatible con el efecto jurídico perseguido por otro sujeto a partir de un alegato de protección iusfundamental”.<sup>51</sup>

Si bien existen diversas formas de solución al conflicto producido cuando chocan dos o más derechos fundamentales, nos centraremos en el método de la ponderación; ésta para Bertelsen consiste en “la opinión emitida por el tribunal que analiza un problema constitucional mediante la identificación de los intereses implicados en el caso, y llega a una decisión o construye una regla de derecho constitucional, mediante la asignación explícita o implícita de valores a los intereses previamente identificados”.<sup>52</sup>

Es importante precisar que estos conflictos no son de naturaleza irreconciliable, Muñoz, considera que “pueden ser subsanados de acuerdo a una serie de principios y resguardos normativos, que sean capaces de garantizar que los derechos fundamentales no sean perturbados, o que esta perturbación ocurra en la menor medida posible, y solo si las circunstancias lo ameritan.”<sup>53</sup>

En relación a las implicaciones jurídicas que tiene la utilización de datos biométricos de los trabajadores por parte de la empresa para tener un control más eficiente del desempeño laboral durante la jornada de trabajo tiene aplicación en México la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de 2017, ya que en su artículo 3 fracción III, establece como definición lo siguiente:

---

<sup>51</sup> Aldunate citado por Muñoz Gallardo, Sebastián Andrés. *op. cit.* p. 63

<sup>52</sup> Bertelsen citado por Muñoz Gallardo, Sebastián Andrés. *op. cit.* p. 64

<sup>53</sup> Muñoz Gallardo, Sebastián Andrés. *op. cit.* p. 65

Artículo 3. Para los efectos de la presente Ley se entenderá por:

...

III. Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

Asimismo, las fracciones IX y X de dicho precepto legal establecen el concepto de dato personal y dato personal sensible. Si bien es cierto en las tres fracciones anteriores no especifica los datos biométricos podemos deducir de una interpretación hermenéutica respecto a la fracción X del artículo número 3 de dicha ley que los datos biométricos se consideran sensibles ya que son datos personales que permiten a una persona ser identificable y pueden revelar su origen racial o étnico o información genética o estado de salud ya que dependiendo el sistema de datos biométricos que utilice la empresa, los cuales pueden ser como lo hemos anotado en líneas anteriores, huellas digitales, el contorno de la mano, el registro de la retina del iris, voz, cara, venas de la mano, forma de la mano, forma de la oreja, forma de andar, forma de escribir en un teclado, firma, ADN y olor; por tal motivo la persona sería fácilmente identificable, en consecuencia los datos biométricos de los trabajadores pasarían a ser datos sensibles de acuerdo con la legislación que se comenta.

A mayor abundamiento el artículo 22 fracción V de dicho ordenamiento legal, establece que el responsable del tratamiento de los datos personales no está obligado a recabar el consentimiento del titular de los datos personales, mismo que a la letra dice:

Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:

...

V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.

En relación a la aplicación de esta excepción del numeral antes citado, para los trabajadores no es aplicable ya que se trata de datos personales sensibles, por lo tanto, si es aplicable lo dispuesto en los artículos 20 y 21 de la multicitada ley que a la letra dicen:

Artículo 20. Cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la presente Ley, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

I. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;

II. Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, e

III. Informada: Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

Artículo 21. El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.

Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de esta Ley.

En consecuencia, podemos decir que los datos biométricos son sensibles y por lo tanto requieren el consentimiento expreso del titular de estos, es decir, de los trabajadores. A mayor abundamiento el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares establece en su artículo 2 fracción VIII el concepto de persona física identificable:

Artículo 2. Además de las definiciones establecidas en el artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para los efectos del presente Reglamento se entenderá por:

...

VIII. Persona física identificable: Toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información. No se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas;

Por lo tanto, a través de los datos biométricos que utilice la empresa derivada de la relación laboral y en virtud de que los trabajadores son personas físicas identificables, no tiene aplicación el artículo 5 fracción III del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la empresa deberá tener el consentimiento de acuerdo a lo establecido en el artículo 12 de dicho Reglamento que a la letra dice.

Artículo 12. La obtención del consentimiento tácito o expreso deberá ser:

I. Libre: sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular;

- II. Específica: referida a una o varias finalidades determinadas que justifiquen el tratamiento, y
- III. Informada: que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento. El consentimiento expreso también deberá ser inequívoco, es decir, que existan elementos que de manera indubitable demuestren su otorgamiento.

A mayor abundamiento con los datos biométricos se crean bases de datos personales sensibles y en consecuencia tienen aplicación los artículos 9 y 56 del citado reglamento que a la letra dicen:

Artículo 9. De acuerdo con lo previsto en el artículo 6 de la Ley, los responsables deben cumplir con los siguientes principios rectores de la protección de datos personales:

- I. Licitud;
- II. Consentimiento;
- III. Información;
- IV. Calidad;
- V. Finalidad;
- VI. Lealtad;
- VII. Proporcionalidad, y
- VIII. Responsabilidad.

Asimismo, el responsable deberá observar los deberes de seguridad y confidencialidad a que se refieren los artículos 19 y 21 de la Ley.

Artículo 56. En términos de lo previsto en el artículo 9, segundo párrafo de la Ley, sólo podrán crearse bases de datos que contengan datos personales sensibles cuando:

- I. Obedezca a un mandato legal;
- II. Se justifique en términos del artículo 4 de la Ley, o
- III. El responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

Como conclusión podemos decir que, respecto a la utilización de datos biométricos de los trabajadores en las relaciones laborales por parte del patrón, los empleados cuentan con la protección de la referida Ley Federal de Datos Personales en Posesión de Particulares de México y su Reglamento, ya que sus datos personales son considerados, a través de una interpretación hermenéutica, como datos sensibles, porque es una persona identificable. Lo ideal sería una reforma a la referida Ley Federal de Protección de Datos Personales en Posesión de los Particulares, específicamente en el artículo 3 fracción X, adicionándola en forma específica para que incluya datos biométricos, ya que estos se refieren a la esfera más íntima de su titular o sea de los trabajadores.

Entre las implicaciones jurídicas que tiene el tratamiento de datos biométricos en la empresa para el control de la relación de trabajo ha generado la idea del derecho de autodeterminación informativa que tiene el titular de los datos personales o sea el trabajador,

en relación al uso y destino que les dará el empleador, por lo tanto, se ha considerado que el sector empresarial debe respetar los datos biométricos de los trabajadores y proporcionar información a estos sobre el uso que se les dará a los mismos.

En la actualidad algunos países consideran los datos biométricos como datos sensibles o sea elevando su protección a una categoría superior a los datos en general de las personas ya que a través de los datos sensibles se podrían realizar prácticas ilegales como sería la discriminación entre otros.

## **Conclusiones.**

1. La empresa que utilice datos biométricos de los trabajadores para obtener un mayor control y eficiencia durante la relación de trabajo por parte de los empleados, debe respetar los principios que se utilizan para el tratamiento de datos personales o sea el principio de respeto a la privacidad, el principio de proporcionalidad y el de consentimiento.
2. Los datos biométricos deberían tener la protección de los derechos fundamentales en la actual sociedad, por lo tanto, las implicaciones jurídicas son varias y se recomienda tener cuidado por parte del personal administrativo, ejecutivo y abogados de la empresa para salvaguardar los derechos del empleado en este rubro.

## **Bibliografía:**

- Aguilera Portales, Rafael Enrique y López Sánchez, Rogelio. “Los derechos fundamentales en la teoría jurídica garantista de Luigi Ferrajoli”. En Línea <http://biblio.juridicas.unam.mx/libros/6/2977/4.pdf>
- Areitio, Javier y, Areitio, Teresa. “Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación”. Control de Accesos. Mayo 2007. En Línea: <https://es.scribd.com/document/13156295/Biometricos>
- Castells, Manuel citado por Vidal Salazar, Michael. “Los derechos laborales fundamentales frente a la globalización y la flexibilización laboral”. En Línea: <http://vufind.uniovi.es/Record/oai:doaj.orgarticle:3fcc461a3c4e47129ffa425aeea345d/Details>

- Garrido Iglesias, Romina y, Becker Castellaro, Sebastián. “La biometría en Chile y sus riesgos”. Revista Chilena de Derecho y Tecnología, Vol. 6 Núm. 1, 2017. En Línea: <https://rchdt.uchile.cl/index.php/RCHDT/article/view/45825/48403>
- Gutiérrez Ricardo, Jorge Enrique. “Estudio de factibilidad para el Control de Acceso Biométrico, en una empresa empleando lectores de huella digital”. Universidad De La Salle. Bogotá D. C. 2007. En Línea: <http://repository.lasalle.edu.co/bitstream/handle/10185/2158/T91.07%20G985e.pdf?sequence=1&isAllowed=y>
- Kahale Carrillo, Djamil Tony. “Las Nuevas Tecnologías en las Relaciones Laborales: ¿Avance o Retroceso?”. En Revista de Derecho, julio, número 025, de la Universidad del Norte, Barranquilla, Colombia. En Línea: <http://redalyc.uaemex.mx/pdf/851/85102508.pdf>
- Laguna Quiroz, Rosa. “El Trabajo en la Era Digital de la Relación Contractual”, Alfa-Redi, Revista de Derecho, Numero 78, Enero, 2005, En Línea: <http://www.alfaredi.org/rdi-articulo.shtml?x=986>
- Medina Castillo, J. Enrique. “Las nuevas tecnologías en las relaciones laborales. Del empleo a la participación en la innovación”. En Línea: [file:///C:/Users/Propietario/Downloads/archivoPDF%20\(2\).pdf](file:///C:/Users/Propietario/Downloads/archivoPDF%20(2).pdf)
- Meseguer González, Juan de Dios. “Derechos fundamentales afectados por la geolocalización”, En ElDerecho.com. En Línea: [http://www.elderecho.com/tribuna/www-elderecho-com/Derechos-fundamentales-afectados-geolocalizacion\\_11\\_567055001.html](http://www.elderecho.com/tribuna/www-elderecho-com/Derechos-fundamentales-afectados-geolocalizacion_11_567055001.html)
- Muñoz Gallardo, Sebastián Andrés. “Datos Biométricos y Derechos Fundamentales”. Facultad de Derecho. Departamento de Derecho Procesal. Universidad de Chile. Santiago, 2017. En Línea: <http://repositorio.uchile.cl/bitstream/handle/2250/145203/Datos-biom%C3%A9tricos-y-derechos-fundamentales.pdf?sequence=1>
- Murillo De La Cueva, Pablo Lucas. “Derechos fundamentales y avances tecnológicos. Los Riesgos del Progreso”. Boletín Mexicano de Derecho Comparado, Nueva Serie, Año XXXVII, Núm. 109, Enero-Abril de 2004
- Olivares Morales, Alejandro. “Automatización del proceso de control de asistencia del personal académico en tiempo real a través de reconocimiento biométrico”. Facultad de Ingeniería. Universidad Nacional Autónoma de México. Marzo 2010. En Línea: <http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/1188/Tesis.pdf>

- Pérez Luño, Antonio Enrique. “Los derechos humanos en la sociedad tecnológica”, En Cuadernos Electrónicos de Filosofía del Derecho, No. 27, 2013. En Línea: [file:///C:/Users/Propietario/Downloads/2337-8164-1-PB%20\(1\).pdf](file:///C:/Users/Propietario/Downloads/2337-8164-1-PB%20(1).pdf)
- Perozo, Edinson y, Nava, Ángel. “El impacto de la gestión tecnológica en el contexto empresarial”, Revista Venezolana de Ciencias Sociales, Vol. 9, Núm. 2, Diciembre, 2005, Universidad Nacional Experimental Rafael María Baralt, Cabimas, Venezuela. En Línea: <http://www.redalyc.org/pdf/309/30990214.pdf>
- Rodríguez Crespo, María José. “El Derecho a la Intimidad Informática del Trabajador: Un Límite más al Poder de Dirección del Empresario”. Sentencia del Tribunal Superior de Justicia de Madrid de 21 de marzo de 2014. Poder de Dirección. Universidad de Córdoba. Temas Laborales Núm. 128/2015. En Línea: <https://www.juntadeandalucia.es/empleo/carl/carlportal-portlets/documentos?nombre=4b82f8e7-5ed0-48bb-881d-76f9e2eacc23.pdf>
- Soto Aravena, Patricia Paola. “Impacto en los trabajadores por la implantación de un sistema biométrico en la automatización de los tiempos y control de asistencia”. Máster en Dirección de Recursos Humanos. MÁSTERES de la UAM. Facultad de Psicología. Ediciones UAM. Año Académico 2010-11. En Línea: <http://docplayer.es/7158217-Impacto-en-los-trabajadores-por-la-implantacion-de-un-sistema-biometrico-en-la-automatizacion-de-los-tiempos-y-control-de-asistencia.html>
- Stella Rodríguez, Gladys. “El software libre y sus implicaciones jurídicas”. Revista de Derecho, Núm. 30, Diciembre, 2008, pp. 164-169. Universidad del Norte. Barranquilla, Colombia. En Línea: <http://www.redalyc.org/pdf/851/85112306007.pdf>
- Tobías Martínez, Miguel Ángel. “Análisis de factibilidad de la implementación de un sistema de asistencia a clase mediante huella dactilar en la Facultad de Ingeniería Arturo Narro Siller”. Centro Universitario Tampico – Madero Noviembre de 2010. Facultad de Ingeniería Arturo Narro Siller. Universidad Autónoma de Tamaulipas. En Línea: <https://es.scribd.com/document/299912324/TESIS>
- Tolosa Borja, César y Giz Bueno, Álvaro. “Sistemas Biométricos”. En Línea: [https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web\\_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf](https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf)

- Ugarte Cataldo, José Luis. “La tutela de Derechos fundamentales y el Derecho del trabajo: de erizo a zorro”. En Línea: <http://www.scielo.cl/pdf/revider/v20n2/art03.pdf>
- Velásquez Valencia, Jorge Eduardo y Linares Jaramillo, Álvaro Andrés. “Soluciones Inteligentes para el control de acceso físico mediante el uso de tecnología biométrica”. Universidad Tecnológica de Pereira. Facultad de Sistemas. Ingeniería de Sistemas y Computación Pereira. 2013. En Línea: <http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4090/0053682V434.pdf;jsessionid=BD2069D6A97A5B9F4536E2847DCDE383?sequence=1>
- Viegas, María José. “Impacto de las tecnologías en las relaciones laborales”. En Línea: <http://mjv.viegasociados.com/wp-content/uploads/2011/05/Impacto-de-las-tecnologias-en-las-relaciones-laborales.pdf>

### **Legislación**

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Federal del Trabajo