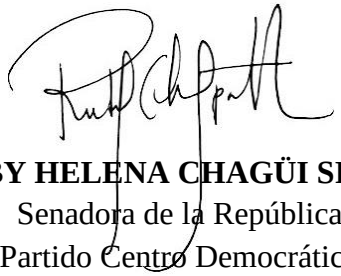
PROPOSICIÓN

Elimínese el Art. 265 del informe de ponencia para segundo debate del proyecto de ley 409/20Cámara – 234/20Senado Por la cual se expide el código electoral colombiano y se dictan otras disposiciones.

~~*ARTÍCULO 265. Ninguna entidad privada podrá recolectar información biométrica de los colombianos, salvo una autorización legal para ello.*~~

~~*Parágrafo Transitorio: Las empresas privadas que hayan recolectado la información biométrica de los colombianos deberán eliminarla, pudiendo mantener solamente el nombre, número de cédula y datos no sensibles.*~~



RUBY HELENA CHAGÜI SPATH
Senadora de la República
Partido Centro Democrático

JUSTIFICACIÓN

La Ley Estatutaria 1581 de 2012 contiene reglas sobre recolección, uso y tratamiento de datos biométricos como categoría de datos sensibles. Esa ley fue revisada y avalada por la Corte Constitucional (C-748 de 2011)

- La Constitución ni la Ley 1581 de 2012 no prohíben que los datos sensibles biométricos solo pueden ser recolectados y usados por las entidades públicas
- La propuesta impediría que entidades como las siguientes no pudiesen tener datos biométricos (huellas dactilares, fotos, tipo de sangre, ADN): hospitales, empresas de seguridad privada, bancos, aeropuertos. Esto afectaría, entre otros, los sistemas de seguridad de muchas organizaciones.
- No es conveniente que mediante el Código Electoral se modifique la Ley General de carácter estatutaria como lo es la ley de Datos Personales (Ley 1581 de 2012) porque el tema no debe verse únicamente desde la perspectiva de las elecciones o desde la funciones de la Registraduría Nacional del Estado Civil.

Los datos biométricos expresamente están catalogados como datos sensibles por el artículo 5 de la Ley 1581 de 2012 y por lo tanto sujetos a lo dispuesto en la misma, en el

decreto 1377 de 2013 y en la jurisprudencia de la Corte Constitucional. La información biométrica[1] incluye datos sobre las características físicas (rostro, huella dactilar, palma de la mano, retina, ADN, tipo de sangre) y "comportamentales" (forma de firmar, tono de voz) sobre las personas[2].

En el numeral 14 del artículo 4 del Reglamento Europeo de Protección de Datos[3] se definen en los siguientes términos:

"datos biométricos»: 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;"

Se suma a la anterior las múltiples definiciones sobre biometría que tienen como común denominador el uso de características físicas o comportamentales de los individuos. Para Grijpink[4], por ejemplo, la expresión "biometrics" es la identificación de los individuos basada en sus características físicas utilizando tecnologías de información. Furnell[5], trayendo a colación la definición del International Biometric Group, señala que biometrics es el uso automatizado de las características físicas y de comportamiento de una persona para determinar o verificar su identidad. Finalmente, Yue Liu[6] menciona que "*biometrics*" y "*biometric technology*" son mecanismos de medición de comportamiento o las características físicas de los seres humanos con mira a determinar o autenticar su identidad.

---

[1] Buena parte de lo que menciono a continuación es tomado de: GOMEZ CORDONA, Ana Isabel. REMOLINA ANGARITA, Nelson. 2011. *Los sistemas de identificación biométrica y la información biométrica desde la perspectiva de la protección de datos personales.* En Derecho & TIC 10.0. Bogotá: Ediciones Uniandes y Editorial Temis. Pp 223-268

[2] Saini, Nirmala y Sinha, Aloka. *Soft biometrics in conjunction with optics based biohashing* . Optics Communications, Volume 284, Issue 3, pag. 756. February 2011.

[3] Cfr. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) . Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[4] Grijpink, Jan. *Biometrics and privacy*. Computer Law & Security Report, Volume 17, Issue 3, Pag 154. May 2001.

[5] Furnell, Steven y Clarke Nathan. *Biometrics: no silver bullets*. Computer Fraud & Security, Volume 2005, Issue 8, Pag. 9. August 2005.

[6] Liu, Yue. The principle of proportionality in biometrics: Case studies from Norway. Computer law & security review. Volume 25, Issue 3, Pag 237, 2009.

El uso de datos biométricos incrementa cada día por parte de los gobiernos, los organismos de seguridad o investigación de delitos, las empresas de seguridad privada, los clubes sociales, la banca, los organismos de inmigración instalados en los aeropuertos, las empresas privada, la instituciones de salud y en general cualquier persona. De hecho, los sistemas biométricos serán por excelencia los mecanismos de identificación del siglo XXI, reemplazando, en buena medida, medios tradicionales como las tarjetas de identificación, los códigos de barras, los password, las firmas digitales y los números secretos de identificación, gracias a que las características biométricas son más difíciles de violar en términos de seguridad.

Con los mecanismos biométricos de identificación se captura, procesa y almacena información relacionada, con los rasgos físicos de las personas (huellas dactilares, el ADN, la forma o silueta de la mano, patrones de la retina o el iris, aspectos faciales) para poder establecer o "autenticar" la identidad de cada sujeto[7]. De acá surgen los sistemas de autenticación humana o HAS (Human Authentication System) y los sistemas biométricos de autenticación o BAS (Biometric Authentication System). En los primeros (HAS), quien efectúa la autenticación compara, entre otras, la cara, el pelo, la voz de una persona frente a la información que previamente tiene almacenada sobre ella en una base de datos. El resultado de la autenticación depende del juicio de valor de la persona que realiza la comparación. En los segundos (BAS), el reconocimiento es automático sin la intervención de una persona que perpetra la comparación como sucede en los HAS.

Los sistemas biométricos representan un mecanismo de identificación y verificación basados en las características biológicas, morfológicas, anatómicas o rasgos de comportamiento de las personas[8], las cuales tienen un carácter intransferible e irrepetible. Precisan Bhatnagar, Lall y Patney que esta información es "natural" y casi única a cada persona[9]. Estas particularidades generan algunas ventajas sobre los métodos tradicionales de identificación[10] como, por ejemplo, el hecho que estos mecanismos no se extravían ni se olvidan como sí puede suceder con una tarjeta de identificación con código de barras y las claves secretas. Por eso se considera que los sistemas biométricos

---

[7] Ver Woodward, John. "Biometric Scanning, Law & Policy: Identifying the concerns-drafting the biometric blueprint". University of Pittsburgh Law Review. 1997

[8] Anil, Jain y otros. Introduction to biometrics. Capítulo de libro publicado en la obra "Biometrics: personal identification in networked society". Boston: Kluwer Academic Publishers, pág. 1-41, 1999; Jain A, Ross, and Prabhakar,. Biometrics-Based Web Access, Michigan State University, Technical Report TR98-33, November 1998; Newham, E. The Biometric Report. New York: SBJ Services, 1995.

[9] Bhatnagar, Jay; Lall, Brejesh y Patney, R. *Performance Issues in Biometric Authentication Based on Information Theoretic Concepts: A Review*. IETE Technical Review, Vol. 27, Issue 4, p 274. Jul-Aug 2010. Delhi, India.

[10] Cfr. Nalini, Ratha and Bolle, Ruud. "*Smartcard based authentication*". pp. 369-384. En: Jain,ob cit.; Saini, Nirmala y Sinha, Aloka. Soft biometrics in conjunction with optics based biohashing . Optics Communications, Volume 284, Issue 3, pag. 762. February 2011.

contribuyen a aumentar el nivel de precisión de identificación de los individuos y permiten combatir el fraude de identidad[11].

Los datos sensibles, por su parte, son aquellos que por su naturaleza están relacionados con aspectos muy íntimos de la persona o que pueden ser nicho de discriminaciones o comprometer los derechos y libertades de las personas. Jurisprudencialmente se ha catalogado esta información como secreta. La información genética, los "datos sensibles" o relacionados con la ideología, la inclinación sexual son ejemplos de Información denominada por la Corte Constitucional como "reservada o secreta" porque guardan *"estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones"* [12].

Los datos sensibles fueron definidos en la ley 1581 de 2012 y en el decreto 1377 de 2013 como **"** *aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los* ***datos biométricos***"[13].

[11] Cfr. Davies, Simon. "*Touching Big Brother: How biometric technology will fuse flesh and machine*". Information Technology & People, Vol. 7, No. 4 1994.

[12] Cfr. Corte Constitucional, sentencia T-729 de 2002, C-336 de 2007 y C-334 de 2010

[13] Artículo 5 de la ley 1581 de 2012, repetido en el numeral 3 del artículo 3 del decreto 1377 de 2013