ECONOMÍA DIGITAL

GUSTAVO ENRIQUE VELESQUEN SAENZ

C.A.B.A.

Resumen.

El avance de la economía digital ha producido profundas transformaciones en aspectos fundamentales de las condiciones de trabajo, y en este contexto, la facultad de organización y dirección empresaria, potenciada por la implementación de estas tecnologías en los sistemas de selección, gestión y control de personal, puede tener el potencial de afectar los derechos a la intimidad y privacidad de los trabajadores y trabajadoras.

Resulta pues imperioso analizar las consecuencias derivadas de ello en relación al tratamiento dado a su respecto en la actual Ley de Protección de Datos Personales y su proyecto de reforma, para así asegurar una adecuada tutela sobre los datos personales de los dependientes frente a su recopilación y tratamiento en forma masiva por medio de algoritmos e inteligencia artificial en los procesos de gestión, así como su uso para el perfilamiento y el control empresarial ejercido por medio de la utilización de herramientas de monitoreo digitales.

En el presente trabajo se procurará brindar una aproximación a las nuevas formas de selección, control y gestión de los trabajadores y trabajadoras, los datos que se generan en el marco de la relación laboral y las particularidades de este vínculo en relación a la adquisición de esos datos, como así también analizar las implicancias derivadas de ello, en el marco del Proyecto de Ley de Protección de Datos Personales, formulando algunos aportes que permitan asegurar el respeto de los derechos a su intimidad y privacidad en el ámbito laboral.

Conclusiones.

La gestión, control y dirección de personal por medios digitales y el procesamiento automático de datos es ya una realidad que abre una posibilidad cierta de discriminación directa o indirecta, y de amenaza de violación de la intimidad y privacidad de los dependientes, que debe regularse adecuadamente.

El Proyecto de Ley de Protección de Datos Personales (PLPDP) no aborda este tópico, colocando a trabajadores y trabajadoras en una situación de vulnerabilidad, agravada por su débil posición negocial dentro del contrato de trabajo, por lo que debiera

dispensárseles un tratamiento diferenciado.

Debe establecerse como regla el principio de prohibición de recopilación y procesamiento automático de datos sensibles de los dependientes, marcándose las excepciones que pudieren ser estrictamente necesarias en forma taxativa en la propia ley.

El consentimiento como vía de excepción a esta regla en estos casos no resulta idóneo ni razonable, toda vez que, derivado de su posición negocial, no puede decirse que estemos en presencia de una voluntad expresada libremente. Por otro lado, no puede dejar de señalarse de su parte la falta del debido conocimiento respecto del alcance, importancia e implicancias que tienen sus datos y metadatos, aún los generados durante la prestación laboral, manifestación ésta de la consabida brecha digital.

Resulta necesario que participen las asociaciones sindicales activamente en la protección de los datos personales de sus representados, y que ello esté contemplado desde el diseño mismo de la norma, pudiendo contarse con un homólogo de la figura del delegado de protección de datos.

I. Introducción.

Las tecnologías de la Información y las comunicaciones (en adelante las TICs) han transformado irreversiblemente la interrelación entre las personas. Del mismo modo, estas tecnologías digitales han irrumpido de manera revolucionaria en el campo de la producción de bienes y prestación de servicios, habiéndose acelerado su adopción debido a la crisis derivada de la pandemia de Covid-19, impactando en el mundo del trabajo.

El avance de la economía digital está configurando un ecosistema empresarial en el que los procesos industriales se caracterizan por la adopción de robots y sistemas inteligentes automatizados e interconectados, por el trabajo por medio de plataformas digitales, el uso de algoritmos e Inteligencia Artificial, no solo para el proceso de selección de personal, sino también para su gestión.

Estos cambios han producido profundas transformaciones en aspectos fundamentales de las condiciones de trabajo, como la dependencia, el concepto de horario y lugar de trabajo, lo que plantea serios riesgos de exclusión de la tutela de las normas laborales y pone en crisis conceptos fundamentales del derecho del trabajo.

En este contexto, la digitalización de los puestos de trabajo y el fenómeno del trabajo remoto, junto con el desarrollo de sistemas de selección, control y gestión de personal basados en algoritmos e inteligencia artificial otorgan una importancia superlativa a la protección de los datos de los trabajadores y trabajadoras.

Lamentablemente, el proyecto de reforma de la Ley 25.326 de Protección de datos personales no ha previsto la incorporación de normas y principios que den un tratamiento diferenciado a este colectivo, como sí lo ha hecho respecto de los NNyA[1].

En el presente trabajo, dada su limitada extensión, se pretende esbozar una aproximación a las nuevas formas de selección, control y gestión de los trabajadores y trabajadoras, los datos que se generan en el marco de la relación laboral y las particularidades de este vínculo en relación a la adquisición de esos datos, las implicancias de ello, y un análisis somero del tratamiento que se le da a esta cuestión en el Proyecto de Ley de Protección de Datos Personales (en adelante PLPDP), formulando algunos aportes para su incorporación y tratamiento.

II. El problema de las facultades de control y dirección empresaria en relación al procesamiento automático de datos.

La protección de los datos personales en el ámbito del derecho laboral es un tema de notoria actualidad debido al impacto que las tecnologías de la información y la comunicación (TICs), la robotización, la minería de datos, el análisis avanzado de *big data*, el internet de las cosas, los algoritmos y la inteligencia artificial han tenido en el modelo productivo actual. Como mencionáramos, estos avances tecnológicos han afectado un sin número de los principios del cuerpo normativo laboral, lo que plantea la necesidad de actualizar y ampliar las tutelas propias, que fueron concebidas en el contexto social y económico de fines del siglo XIX y principios del XX. Y si bien se han aprobado normas específicas que procuran regular aspectos concretos de este fenómeno, como la ley 27.555 de Teletrabajo, nuestro derecho del trabajo tiene pendiente una regulación más abarcativa que tutele adecuadamente la exposición de los trabajadores y trabajadoras a estas nuevas

tecnologías.

Por su parte, la actual ley 25.326 de Protección de Datos Personales -sancionada hace ya más de 20 años- tampoco contemplaba nada en este punto, siendo que incluso les exceptúa de la necesidad de prestar consentimiento a los fines de tratar los datos en estos casos (art. 5 inc. d). Si bien les mantiene amparados bajo la prohibición general del tratamiento de datos sensibles. Pero es una realidad que al tiempo de sanción de la ley 25.326 no se había alcanzado un desarrollo tecnológico que permitiera la injerencia en la privacidad e intimidad como la que permite hoy día los sistemas tecnológicos utilizados en la selección y gestión de personal dependiente, tal como se explicará más adelante.

Ya en el año 2019, se aprobó por ley 27.483 el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Sin embargo, en este convenio tampoco se contemplan las cuestiones

---

[1] Así como aquí se plantea la necesidad de establecer un tratamiento diferenciado respecto de los trabajadores y trabajadoras, también debería considerarse ello respecto de aquellas personas contempladas en la Resolución 139/2020 de la secretaría de Comercio (B. O. 28/05/2020).

relativas al tratamiento de datos en el marco de una relación laboral. Es importante destacar que en su artículo 6 se establece que “Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas”. Esto ciertamente deja abierta una posibilidad para que sean objeto de tratamiento este tipo de datos por medios automatizados, generando una notoria ambigüedad en un tema de especial sensibilidad, supeditando ello a que en las normas internas se encuentre vedado.

La facultad de organización y dirección prevista en los artículos 64 y 65 de la LCT, potenciada por la implementación de estos sistemas de gestión y control, tiene la potencialidad de afectar los derechos a la intimidad y privacidad de los trabajadores y trabajadoras. Por ello, en el contexto de la digitalización de las empresas, por los posibles riesgos de afectación de los derechos enunciados que esta conlleva, imponen el reconocimiento de la protección de los datos personales de los dependientes frente a su recopilación y tratamiento en forma masiva por medio de algoritmos e inteligencia artificial en los procesos de gestión, así como su uso para el perfilamiento y el control empresarial ejercido por medio de la utilización de herramientas de monitoreo digitales y de seguimiento por medio de geolocalización, entre otras, deben enmarcarse en la salvaguarda del derecho a la intimidad y privacidad.

Este enfrentamiento entre el interés legítimo de la empresa en vigilar y controlar la actividad laboral y el respeto a los derechos fundamentales de los trabajadores debe analizarse necesariamente anteponiendo la dignidad de la persona humana, el derecho a la privacidad, a la intimidad, a no ser discriminado, derechos humanos fundamentales que, entre muchos otros, siguen constituyendo piedra basal sobre la que se cimenta la protección de las personas en general y de los trabajadores y trabajadoras en particular. En consecuencia, resulta necesario que las regulaciones se actualicen y adapten a esta nueva realidad para de tal modo garantizar en forma más extensa la protección de estos derechos en el ámbito laboral.

Estas tensiones, que se añaden a la inherente propia de los intereses históricamente en pugna intrínsecos de la relación laboral, imponen la necesidad de extremar los esfuerzos normativos para reequilibrar el ejercicio de la libertad empresarial con los derechos humanos fundamentales. En este sentido, es importante recordar que los trabajadores y trabajadoras no deben ver limitada su dignidad como personas humanas por el mero hecho de formar parte de una organización empresarial productiva. Recordemos que, según lo reconocido por nuestro máximo tribunal, el trabajador y la trabajadora deben ser objeto de una tutela preferente y, por lo tanto, protegidos en todo momento[2].

Esto nos obliga a abordar la cuestión desde el reconocimiento de los matices

particulares que presenta la relación laboral, la cual por sus características justamente se constituye como un ámbito propicio para la afectación de esos derechos fundamentales, agravado ello por la digitalización de los puestos de trabajo y el uso masivo por parte de las empresas de información personal relativa a sus empleados, ya sea suministrada u obtenida por la mera forma de estructurarse el trabajo.

Ante ello, el primer límite o requisito al control tecnológico debería constituirse en el deber de información en su implementación. Es esencial asegurar que los dependientes sean informados de manera clara, completa y transparente sobre la existencia y el funcionamiento de estas herramientas de control digital, y se les proporcione una explicación detallada de qué datos generarán, cómo se procesarán y a qué efectos. Pero

---

[2] En ese sentido Vizzoti, Carlos Alberto c. Amsa S.A. - 14/09/2004-Cita Online: AR/JUR/1979/2004 y Pérez, Aníbal Raúl c/ Disco S. A. 1/09/2009 Id SAIJ: FA09000086, entre otros.

aún en caso de cumplirse ello, siempre el eje rector debiera ser el respeto de la dignidad de la persona humana.[3]

Otro límite que obedece al respeto de la intimidad humana es la de establecer un claro límite a la posibilidad de realizar controles fuera del lugar y horario de trabajo. La jurisprudencia[4] señala que las posibilidades del empresario de violar el derecho a la intimidad fuera del lugar y horario de trabajo son mucho mayores, máxime en el caso de la implementación de controles por medio de herramientas digitales y ante el tratamiento automatizado de tales datos Y por ello, resulta imperiosa la necesidad de reducir las posibilidades de control fuera del mismo.

Dado que la empresa tiene la posición de control y dirección de la actividad laboral, la digitalización de los sistemas de gestión y control les ha permitido acceder a un incontable volumen de datos personales de sus dependientes, obtenidos por diferentes medios tecnológicos. Estos medios tecnológicos pueden materializarse de las más diversas formas, tales como programas de registro de teclas, seguimiento de los movimientos y clics del mouse, capturas aleatorias de pantalla de los medios informáticos utilizados, capturas aleatorias de la cámara, registro de sonidos recibidos por el micrófono, control de los movimientos de los ojos y gestos faciales, seguimiento de la actividad en línea del empleado, supervisión del uso del correo electrónico empresarial, la agenda y mensajería empresarial, análisis del rendimiento de las aplicaciones y programas ejecutados por el empleado, y la utilización obligatoria de *wereables* para controlar el desplazamiento físico, ya sea por RFID[5], GPS[6] u otros sistemas.

Es importante tener en cuenta que, como regla general, la operación de estas herramientas de control digital implica el procesamiento de datos personales de los empleados. Considerando que la esencia inherente de dichos sistemas radica en el control, registro y análisis de los trabajadores y trabajadoras, su funcionamiento implica la recopilación y tratamiento de sus datos personales, incluso llegando a involucrar datos sensibles. Por lo tanto, es necesario evaluar en cada caso si ello puede llegar a constituirse en un tratamiento automatizado de datos y qué tipos de datos serán utilizados.

Si el sistema únicamente genera directrices o información que posteriormente es analizada por una persona humana dentro de la organización empresarial, quien es el responsable último de tomar las decisiones basadas en los resultados proporcionados por

---

[3] Desde el caso “Villarruel, Roxana I. c/ Vestiditos S.A. s/ despido, CNTRAB, Sala X, 17/11/03, la jurisprudencia ha establecido que el empleador puede monitorear el uso del correo electrónico laboral, siempre y cuando se cumplan ciertos criterios objetivos: a) la expectativa de privacidad del trabajador ha sido eliminada; b) los métodos de control son razonables y no violan los derechos fundamentales del trabajador; c) los métodos de control son generales y no se dirigen a trabajadores específicos; d) las sanciones en los reglamentos internos

son razonables y cumplen con los requisitos legales (como contemporaneidad y proporcionalidad); y e) la empresa aplica las sanciones de manera efectiva y respeta la igualdad de los empleados. Ahora nos encontramos con un flujo de datos que excede sobremanera el caso regulado pretorianamente.

[4] Es de interés el análisis que se formula en el caso Florindo de Almeida Vasconcelos Gramaxo v. Portugal - 26968/16

Fecha de sentencia 13/12/2022, Corte Europea de Derechos Humanos. En el presente caso se analizó analizando la pertinencia de los registros digitales llevados por la empresa respecto del trabajador y que sirvieron para justificar un despido sanción por el uso indebido de un vehículo de la empresa en lugares ajenos al desarrollo de las tareas encomendadas. Los datos que se registraron fueron distancias recorridas, las horas en que el vehículo arrancó y se detuvo, y la velocidad a la que fue conducido. No se permitió a los empleados desactivar el sistema de GPS, por lo que permitió obtener datos de geolocalización durante horas de trabajo y fuera de las horas de trabajo. En este caso la Corte dictaminó que el despido no resultó discriminatorio, pero limitó a que se tuvieran en consideración solamente las distancias recorridas, por cuanto los demás datos resultaban una intromisión abusiva en la vida personal del trabajador.

[5] Acrónimo de *radio-frequency identification* (identificación por radiofrecuencia) y se refiere a una tecnología mediante la cual los datos digitales codificados en etiquetas RFID o etiquetas inteligentes son capturados por un lector RFID a través de ondas de radio.

[6] En inglés *Global Positioning System* ó Sistema de Posicionamiento Global, es un sistema que permite a un dispositivo receptor localizar su propia posición sobre la Tierra con una precisión de metros a centímetros.

el sistema, se podría argumentar que la decisión no se basó exclusivamente en el procesamiento automatizado de datos. No obstante, en el caso de que estos sistemas emitan instrucciones autónomamente a las personas, sin intervención humana, en función de un análisis de su comportamiento laboral, y esto tenga un impacto significativo, nos encontraríamos, en efecto, frente a un procesamiento automático de datos.

Para establecer un umbral claro en esta distinción, la participación humana debe ser relevante y no simplemente una mera formalidad que busque dar un cumplimiento normativo aparente. Por lo tanto, resulta necesario considerar cómo se utilizará la información y, en consecuencia, asegurar que las acciones o decisiones relacionadas con los trabajadores y trabajadoras, basadas en los datos procesados, cuenten con una participación adecuada, real y debidamente documentada de una persona humana. Asimismo, dicha decisión debe tener un impacto suficientemente significativo en la persona empleada, como podría ser en el caso de la aplicación de sanciones de manera expresa o implícita[7].

En esencia, determinar en cada caso si nos enfrentamos a una toma de decisiones automatizada o no, puede depender de circunstancias y matices sumamente específicos, por lo que resulta imprescindible contar con un análisis detallado antes de implementar este tipo de sistemas, y luego proceder a su revisión periódica. Pues en su caso, ello impondría la aplicación de las normas que regulan el supuesto (tal como lo establece el PLPDP). Y más aún en el caso de tratarse de datos sensibles, donde sería necesario evaluar también la pertinencia y razonabilidad de estos datos para el cumplimiento de las obligaciones laborales y los fines propuestos, y si se están procesando de una manera adecuada y acorde con las normas de protección de datos personales establecidas para estos casos.

En definitiva, ante esta nueva realidad laboral hasta aquí esbozada, donde la selección de personal puede gestionarse por medio del procesamiento automático de datos, donde el poder de dirección y control de la empresa no requieren ya de una supervisión directa e independiente del presentismo, del rendimiento ni del comportamiento de los trabajadores y trabajadoras, ya que estos aspectos son cubiertos por sistemas de control digitales y procesamientos automatizados de datos, es necesario que el ordenamiento jurídico se adapte para que los principios, derechos y garantías elaborados durante más de un siglo, propios del Estado social de derecho en general y del derecho del trabajo en particular, cobren nueva vitalidad, poniendo el foco sobre la dignidad humana por encima de las reglas al servicio de la lógica económica.

Por ello, el Proyecto de Ley de Protección de Datos Personales (PLPDP) ofrece una valiosa oportunidad de incorporar salvaguardas eficaces que permitan asegurar el derecho a la intimidad y la privacidad de las y los trabajadores como colectivo especialmente vulnerable, asegurando la plena vigencia de los derechos humanos. Es importante destacar

que esto no implica forzar la creación de nuevos derechos digitales absolutamente ajenos a los derechos fundamentales ya reconocidos o a los principios y derechos laborales ya consolidados, sino dotar de un marco normativo claro que contemple este fenómeno disruptivo que presentan las nuevas tecnologías, evitando subterfugios técnicos y zonas grises que se conviertan en medios propicios para vulnerar derechos laborales.

---

[7] Ciertos sistemas de organización y control empresario, como en el caso de trabajadores de plataformas, presentan la particularidad que el sistema bloquea el acceso a la App. ante supuestos incumplimientos del dependiente, por lo que esto implica una sanción sin que se explicite la causa, violentando de tal manera el ordenamiento jurídico y afectando garantías esenciales que goza toda persona humana por el solo hecho de serla.

III. La protección de los datos de los trabajadores en el Proyecto de Ley de Protección de Datos Personales (PLPDP).

La situación de los trabajadores y trabajadoras en el marco del Proyecto de Ley de Protección de Datos Personales (PLPDP) plantea ciertas consideraciones relevantes.

Luego de transitar por la definición de ciertos conceptos a los fines de la ley (art. 2) y la enunciación de principios generales (arts. 3 a 12 y cc.), el diseño normativo del PLPDP establece en su artículo 13 que el tratamiento de datos personales solo puede llevarse a cabo si se cumple al menos, entre otras, la siguiente base legal en relación al contrato de trabajo: "... d) que sea necesario para la ejecución de un contrato en el que el Titular de los datos sea parte, o para la aplicación de medidas precontractuales...". Esto implica que, por un lado, desde antes del inicio de la relación laboral, los trabajadores y trabajadoras pueden estar sujetos al posible tratamiento de sus datos y, en segundo lugar, que sus empleadores cuenten con la venia jurídica de poder dar tratamiento a sus datos, ya sea en forma directa o por un tercero. Y también quedan habilitadas para ello las Aseguradoras de Riesgos de Trabajo.

Sin embargo, esta disposición genera cierta ambigüedad, especialmente en el caso de las agencias de selección de personal, ya que estas entidades no serían las futuras empleadoras y, por lo tanto, la posibilidad de tratamiento de datos a través de esta vía quedaría en principio prohibida, sin perjuicio de lo establecido en los arts. 37[8] y cc. Del PLPDP. En consecuencia, sería aplicable el principio general de que el titular deba otorgar su consentimiento expreso para uno o varios fines específicos, tal como se establece en el inciso “a” del mismo artículo 13. Este consentimiento debería cumplir con las estipulaciones del artículo 14, que requiere que sea "expreso, previo, libre, específico, informado e inequívoco" para que pueda enmarcarse en los principios de licitud, lealtad y transparencia (artículo 6), finalidad (artículo 7) y minimización de datos (artículo 8).

Esto plantea una segunda lectura relacionada con la posición de los trabajadores y trabajadoras frente a esta situación: ¿hasta qué punto puede decirse que existe una voluntad libre para prestar su consentimiento en estos casos? Este aspecto será retomado más adelante.

El artículo 16 establece los requisitos mínimos de información que deben proporcionarse al titular de los datos antes de la recopilación, los cuales deben ser concisos, transparentes, comprensibles y de fácil acceso, utilizando un lenguaje claro y sencillo.

De particular interés es el siguiente artículo, que establece los parámetros en relación con los datos sensibles, que fueran definidos en el artículo 2 como "aquellos que se refieren a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen étnico; creencias o

convicciones religiosas, filosóficas y morales; afiliación sindical u opiniones políticas; datos relativos a la salud, discapacidad, preferencia u orientación sexual, datos genéticos o biométricos cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para su titular y que estén dirigidos a identificar de manera unívoca a una persona humana".

Es así que en el art. 17 se establece el principio general de prohibición de tratamiento de esta categoría de datos. Sin embargo, en lo que respecta a los trabajadores y trabajadoras, se establece una excepción a este principio que desorbita todo el sistema a su respecto, y que se consagra en el inciso “g” con la siguiente formulación: "…fuera necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular de los datos en el ámbito del derecho laboral y de la seguridad, la salud pública y la protección social". O sea que automáticamente los datos sensibles de los trabajadores y trabajadoras quedan exceptuados de todo límite a su

[8] El encargado de tratamiento es la persona humana o jurídica, pública o privada, que trate datos personales por cuenta del Responsable del tratamiento (conf. Art. 2).

tratamiento. Es importante destacar la evidente asimetría y desequilibrio en relación con los derechos de cualquier otra persona humana, lo cual importa otorgar a la empresa un poder que claramente excede las necesidades propias de la relación laboral y resulta violatorio de la dignidad de los trabajadores y trabajadoras.

Resulta fundamental limitar esta facultad desmedida y establecer parámetros objetivos para la identificación de los datos sensibles que puedan ser objeto de tratamiento. Aunque se pueda argumentar que se deben cumplir los principios rectores de licitud, lealtad y transparencia; de finalidad; de minimización; y de exactitud, resulta preocupante la permisiva laxitud de la norma en este sentido.

Pero, inclusive, tampoco debería admitirse el tratamiento irrestricto de estos datos, aún en el supuesto que se hubiere brindado el consentimiento. En relación a esto, retomo lo ya manifestado en el sentido que, dada la particular posición negocial de los trabajadores y trabajadoras, su voluntad no puede considerarse totalmente libre. La inherente desigualdad en las partes del contrato de trabajo implica que la negativa a proporcionar cualquier dato solicitado, incluso datos sensibles, podría conducir a reducir sus oportunidades laborales.

Por lo tanto, sería adecuado considerar como principio general la indisponibilidad de los datos sensibles dentro de la esfera del orden público laboral, incluso en el caso de manifestarse una voluntad en sentido contrario, en consonancia con el principio de irrenunciabilidad que rige en el ámbito laboral y que, con las diferencias correspondientes, guarda sintonía con el espíritu del artículo 34 del PLPDP en cuanto a la irrenunciabilidad de los derechos consagrados proyectados en esta ley. Si bien algunas categorías de datos sensibles podrían justificar su tratamiento (por ejemplo, cuestiones relacionadas con la salud, estado civil, maternidad y paternidad, etc.) para poder cumplir con las leyes aplicables, e incluso en temas sindicales, en la mayoría de las categorías de datos sensibles enunciados, ni siquiera con el consentimiento se debería levantar la prohibición de tratamiento.

Esto se debe a que resulta cuestionable la pertinencia de recopilar y tratar datos sobre ideología, religión, sexo, orientación sexual, creencias u origen racial o étnico, ya que su conocimiento por parte del empleador parece más propenso a ser fuente de discriminación que a cumplir con un propósito legítimo. Aun reconociendo que el artículo 31 del PLPDP, en su último párrafo, establece que "El Responsable del tratamiento no puede llevar a cabo tratamientos automatizados o semiautomatizados de datos personales que tengan como efecto la discriminación en detrimento de los Titulares de los datos, particularmente si se encuentran basados en alguna de las categorías de datos contenidas en la definición de datos sensibles del artículo 2 de la presente ley", esto no constituye un impedimento a la recopilación y tratamiento de este tipo de datos, siendo que se prohíbe

cuando el efecto sea discriminatorio. Cuestión que deberá, en su caso, denunciarse, tanto en lo referente al tratamiento de los datos, como así también al resultado discriminatorio en perjuicio de la persona, lo que lejos se encuentra del principio de prevención del daño.

Además de ello, no se establece ningún criterio respecto de la valoración de la prueba en el supuesto que se denuncie una discriminación con base en el tratamiento automatizado de los datos, atento la dificultad teconlógica que se suma a la ya de por sí dificultosa prueba en estos casos, siendo que bien podría haberse incluido en forma expresa para estos casos el estándar elaborado por la CSJN en los casos “Pellicori” y “Sisnero”[9].

---

[9] Pellicori, Liliana Silvia c/ Colegio Público de Abogados de la Capital Federal s/ amparo, 15 de Noviembre de 2011, Id SAIJ:FA11000149; Sisnero, Mirtha Graciela y otros c/ Taldelva SRL y otros s/ amparo, 20 de Mayo de 2014, Id SAIJ:FA14000071, donde se estableció como estándar probatorio que resulta suficiente para la parte que afirma ser víctima de una acto discriminatorio, con la acreditación de hechos que, prima facie evaluados, se presenten idóneos para inducir su existencia, caso en el cual corresponderá al demandado a

En relación con los datos sensibles, surge el problema de la ambigüedad del término "alto riesgo" en el sistema establecido en los artículos 40 y siguientes sobre el tratamiento de datos que, debido a su naturaleza, alcance, contexto o finalidades, pueda conllevar un riesgo significativo para los derechos de los titulares de los datos protegidos por la presente ley. Esta ambigüedad abre la posibilidad de litigios y requiere que la afectación se evalúe en cada caso concreto.

Esto adquiere particular importancia en los procesos de selección de personal, donde la información recopilada requiere un tratamiento especial por sus posibles usos. Es preocupante la ausencia de una regulación específica al respecto dentro del PLPDP, ya que estos procesos tienen el potencial de afectar los derechos humanos fundamentales y generar resultados discriminatorios o desiguales. Estos riesgos no son meramente imaginarios, sino que han tenido y, desafortunadamente, siguen teniendo una presencia real. El caso paradigmático es el algoritmo de selección de personal desarrollado por Amazon[10], que ha demostrado la posibilidad concreta de obtener efectos discriminatorios no previstos.

Estos riesgos, no siempre atribuibles a una decisión deliberada de discriminar a ciertos grupos, son resultado de sesgos algorítmicos y derivados de los datos utilizados para la toma de decisiones, que en muchos casos son incompletos y sesgados. Esto se relaciona con las disposiciones del artículo 41, inciso a, y del artículo 42, inciso d del PLPDP, que prevén la prevención de dichos riesgos a través de sistemas de evaluación de impacto en el caso de tratamiento de datos que puedan generar discriminación en perjuicio de los titulares de los datos, como ocurre en los procesos de selección de personal. No obstante, atravesado el umbral de esa evaluación, siempre quedará latente el posible desarrollo de un resultado discriminatorio, por lo que se impone una revisión constante de estos sistemas.

En este sentido, resulta positiva la revisión por parte de una persona humana, como establece el artículo 31 del PLPDP, como medida de salvaguarda. Sin embargo, esto no elimina el riesgo de que el algoritmo utilice datos sensibles de manera discriminatoria, lo que priva a los trabajadores de garantías suficientes y a los empleadores de seguridad jurídica. Además de las posibles indemnizaciones por reparación integral del daño causado al titular de los datos que haya sido objeto de una decisión discriminatoria, los empleadores también pueden enfrentar sanciones derivadas de esta situación. Y debe reiterarse la necesidad que esta revisión no se constituya en una mera apariencia tendiente a dar visos de cumplimiento normativo, y resulte una real revisión.

Por ello, en el caso de los datos sensibles, resulta evidentemente necesario adoptar una interpretación restrictiva del poder empresarial. Esto brindaría una mayor seguridad jurídica y contribuiría a prevenir adecuadamente casos de discriminación en el ámbito laboral. De lo contrario, aunque siempre se pueda establecer la ilegalidad de la recopilación

y tratamiento de estos datos debido a la violación de los principios mencionados anteriormente, ello siempre será posterior a los hechos, cuando el daño ya estaría producido.

---

quien se reprocha la comisión del trato impugnado, la prueba de que éste tuvo como causa un motivo objetivo y razonable ajeno a toda discriminación.

[10] Discriminación de género algorítmica que se detectó en el sistema de selección de personal automatizado de Amazon llevado a cabo por algoritmos de aprendizaje automático para analizar currículums y seleccionar a los candidatos más adecuados para un trabajo en particular. El algoritmo había sido entrenado con datos históricos de la compañía. Y como en el pasado Amazon había contratado a un mayor número de hombres que de mujeres en puestos técnicos y ejecutivos, el algoritmo alimentado con esos datos aprendió a dar preferencia a los currículos de los hombres por sobre los de las mujeres. Incluso se producía una realimentación de datos, ya que el sistema de toma de decisiones era alimentado a su vez con los datos de estas nuevas selecciones, con lo que el problema, lejos de morigerarse, se agravó con el tiempo creándose un círculo vicioso. Ello evidenció un proceso de selección de personal discriminatorio, pero en el que en apariencia era objetivo y neutral por realizarse por medio de un sistema algorítmico. Amazon finalmente decidió dejar de utilizar el algoritmo y rediseñar sus sistemas automatizados de selección de personal para garantizar que no se produzca más discriminación de género.

Además, es importante considerar que el ejercicio de los derechos de oposición, supresión, limitación y otros establecidos en el PLPDP (artículos 27, 28, 29, 30) presuponen, por un lado, un conocimiento adecuado de los datos que están siendo tratados y, por otro lado, la posibilidad real de ejercer dichos derechos. Sin embargo, en el contexto de la relación asimétrica entre las partes del contrato de trabajo, esto se convierte en una mera ficción. Vale reiterar que, en el ámbito de los derechos humanos, los Estados deben primordialmente velar por prevenir los daños.

Por otra parte, también resulta relevante el derecho a la portabilidad de datos personales contemplado en el artículo 31 del PLPDP. Según este artículo, cuando los datos personales son tratados mediante medios electrónicos o automatizados, el titular de los datos tiene derecho a obtener una copia de los datos que ha proporcionado o que están siendo tratados, en un formato que le permita utilizarlos posteriormente. Esto reviste una gran importancia en los sistemas en los que la reputación digital del trabajador o trabajadora dependa, en alguna medida, de su capacidad para resolver problemas o manejar diversas situaciones, que van más allá de lo contemplado en un certificado de trabajo u otros documentos establecidos en el artículo 80 de la Ley de Contrato de Trabajo (LCT) y que pueden incluir en esa calificación evaluaciones realizadas por el usuario y/o destinatario de la actividad desarrollada. Sin embargo, para el caso de las relaciones laborales, las excepciones planteadas en los puntos a, c, d y el párrafo final del artículo propuesto resultan limitantes y contrarias al propósito mismo de este derecho.

IV. Conclusión.

En el contexto de la digitalización de los puestos de trabajo, la gestión de los datos personales de los trabajadores y trabajadoras por parte de las empresas presenta particularidades que requieren especial atención y que motivan un tratamiento diferenciado en la norma objeto de estudio.

Esto se debe a que los empleadores tienen acceso y procesan una gran cantidad de información que, en el ámbito laboral, puede trascender los límites de la funcionalidad y adentrarse en la privacidad e intimidad del trabajador de manera más intrusiva que en el común de los ciudadanos, debido a su posición dominante en la relación contractual laboral. Además del poder de dirección, la empleadora también posee capacidad sancionadora en la ejecución del trabajo, una facultad ausente en otros actores. Lamentablemente, la normativa aplicable no muestra una sensibilidad particular para proteger los derechos fundamentales de este colectivo en las diferentes etapas de la relación laboral, incluyendo la selección de personal, la gestión y el control durante el desarrollo de la relación laboral, y su terminación.

Pretender aplicar a estos casos, en aras de las facultades de dirección y control

empresariales, el principio de consentimiento para la cesión de datos ya sea en forma explícita o implícita, sería ignorar la intrínseca desigualdad y la débil o nula posibilidad de oposición de los trabajadores y trabajadoras frente a la empresa, quedando en entredicho la existencia misma de un genuino consentimiento libre e informado.

Surge evidente la tensión entre intereses y derechos, ya que los datos personales recopilados con fines aparentemente estrictamente profesionales pueden estar asociados, mediante su análisis masivo, con otros datos que también pueden tener relevancia laboral. Esto genera preocupaciones sobre la falta de neutralidad y objetividad de los resultados, así como la posibilidad de discriminación directa o indirecta, y la potencial violación de la intimidad y privacidad.

El uso de inteligencia artificial y algoritmos en la toma de decisiones empresariales no excluye la posibilidad de intromisiones en la vida privada con consecuencias negativas en el ámbito laboral, lo que resalta la importancia de establecer garantías tanto en la recopilación de datos, para evitar intrusiones ilegítimas o desproporcionadas en la información obtenida, como en el uso de la información seleccionada.

Esto se ve agravado en los casos que se utilicen elementos de hardware y software propiedad de los empleados, tal como admite el artículo 9 de la Ley 27.555, ya que los sistemas de control y tratamiento de datos representan un riesgo cierto y grave de afectación del derecho a la privacidad e intimidad, atento que compartirán funciones laborales y personales. Máxime si esos elementos son, a su vez, utilizados por otros miembros de la familia de los dependientes.

Por lo demás, no puede dejar de señalarse las serias falencias en lo referente al conocimiento por parte de los trabajadores y trabajadoras del alcance, importancia e implicancias que tienen sus datos, manifestación ésta de la consabida brecha digital, redundando ello también en la afectación del consentimiento en tanto este debe ser informado.

Desde ya que no se trata de cubrir con un manto de sospechas la utilización del tratamiento de datos automatizados por la empresa, sino de reconocer el inmenso flujo de datos (y metadatos) que proporcionan los trabajadores y trabajadoras al desarrollar sus tareas, las posibilidades de control análisis de estos por parte de la empresa, y el que la toma de decisiones referentes al control y dirección empresario basadas en tratamientos automatizados de datos sea hoy una realidad. Y, que, en multiplicidad de casos, se ha evidenciado la existencia de sesgos algorítmicos y resultados discriminatorios que deben ser conjurados.

Justamente esa finalidad preventiva del daño es lo que reclama un mejor diseño y mayor desarrollo de la legislación en el sentido señalado, otorgando a los trabajadores y trabajadoras un tratamiento diferenciado que reconozca su particular posición. Puesto que la digitalización de los puestos de trabajo y los medios de control digitales no pueden constituirse en vehículo para pulverizar las garantías de los derechos y la protección de los datos personales en el ámbito laboral, sino que muy por el contrario reclaman nuevos medios que permitan asegurarlos.

Por ello pareciera una consecuencia natural involucrar a las asociaciones sindicales de los trabajadores y trabajadoras a tomar participación activa en la protección de los datos personales de sus representados, y que ello esté contemplado desde el diseño mismo de la norma. En este sentido no puede dejar de señalarse que, ante la figura del delegado de protección de datos (arts. 44 y 45 PLPDP), resultaría idóneo una contraparte de la representación sindical. Posibilidad cierta que bien podría encausarse dentro de las medidas propuestas en el art. 48[11] PLPDP.

Mientras que las normas brindan un marco genérico de orden público, la negociación colectiva se presenta como un recurso especialmente valioso en un mercado de trabajo digitalizado y tecnológico, permitiendo una regulación más detallada que atienda a las especificidades de los distintos sectores, garantizando un adecuado equilibrio de intereses.

El diálogo social y la negociación colectiva deben asumir un rol preponderante en la construcción de un entorno digital que permita asegurar el debido control sobre los medios, el contenido y los tipos de datos que recaba la empresa cuando esos datos serán objeto de un tratamiento automatizado.

---

[11] En el marco del PLPDP se establecen mecanismos de regulación vinculantes tales como códigos de ética, de buenas prácticas, normas corporativas vinculantes, sellos de confianza, certificaciones u otros mecanismos que coadyuven a contribuir a los objetivos señalados.