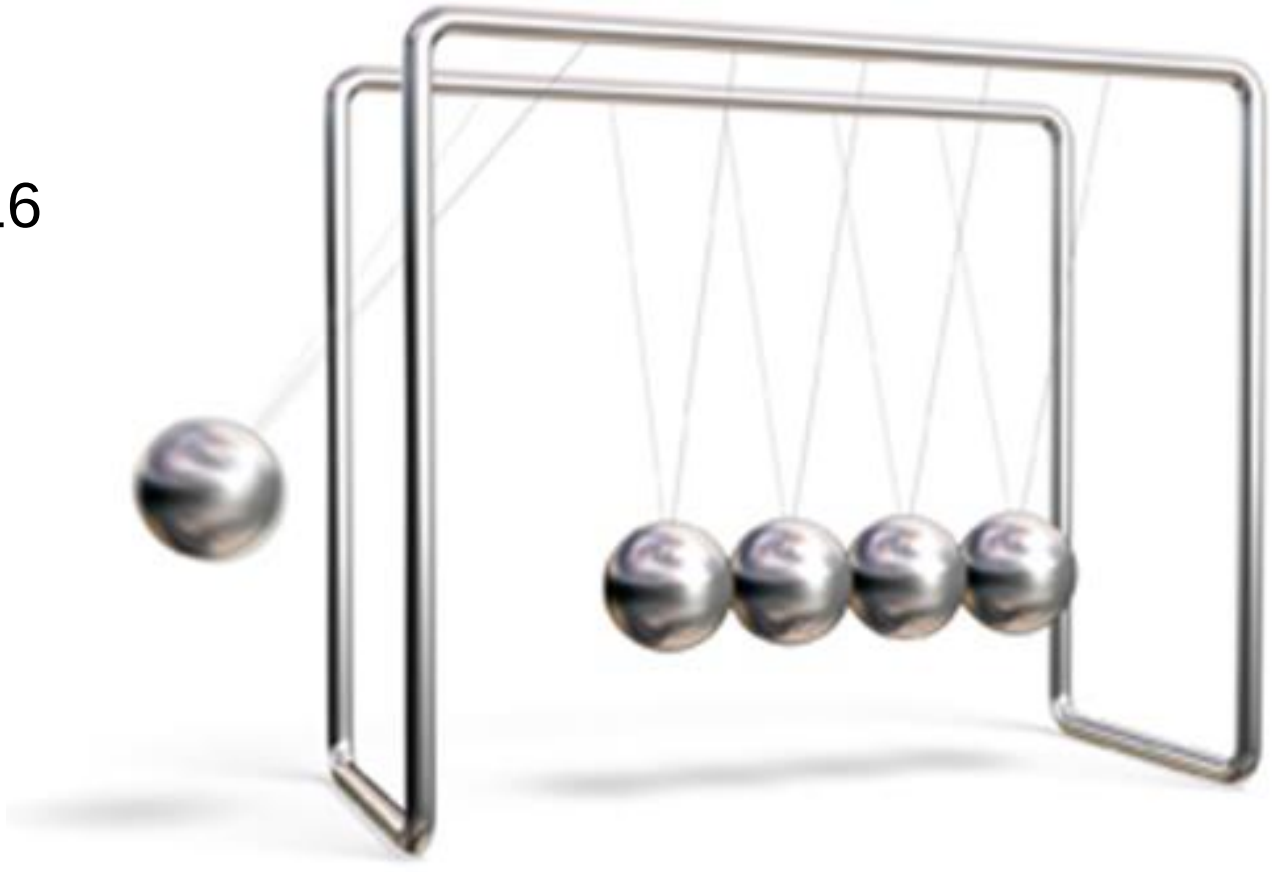
BAKER & McKENZIE

HR Analytics

Impacto en las Relaciones Laborales en la empresa

2016



Todos los derechos reservados

©2016: Baker & McKenzie

No está permitida la reproducción total o parcial de este documento, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro o por otros medios sin el permiso escrito del autor.

HR Analytics

Impacto en las Relaciones Laborales en la empresa

Autores:

Carlos de la Torre, *Of Counsel*, Área Laboral Baker & McKenzie

Raúl Rubio, Socio Área Tecnologías de la Información Baker & McKenzie

Tabla de contenidos

Primera parte

HR Analytics. Entorno jurídico, Relaciones Laborales y Protección de Datos

Primera parte: *HR Analytics*. Entorno Jurídico, Relaciones Laborales y Protección de Datos

Autores:

Carlos de la Torre, *Of Counsel*, Área Laboral Baker & McKenzie

Raúl Rubio, Socio Área Tecnologías de la Información Baker & McKenzie

1. Introducción

HR Analytics consiste en la utilización de técnicas de minería de datos y análisis de negocio aplicados al ámbito de la gestión de datos de recursos humanos, con la ayuda de nuevas tecnologías que permiten el tratamiento masivo de información de una forma rápida y eficiente (big data).

Uno de los objetivos fundamentales del *HR Analytics* es proporcionar a la organización información para una gestión eficaz de los empleados de tal forma que se puedan cumplir los objetivos de negocio de la forma más rápida y eficiente.

El reto de la analítica de recursos humanos es identificar qué datos deben ser capturados y cómo utilizar los datos para modelar y predecir habilidades para la organización que permitan obtener un óptimo rendimiento de su inversión en capital humano.

El *HR Analytics* no sólo se ocupa de recopilar datos sobre la eficiencia de los empleados. Permite correlacionar los datos de negocio y los datos de las personas, con el objetivo de obtener información relevante para cada proceso de negocio que facilite la toma de decisiones con el objetivo de mejorar dicho proceso.

Desde la perspectiva jurídica, el *HR Analytics* implica un uso masivo de información sobre los empleados que puede estar anonimizada o no y cuyo origen puede ser interno o externo a la organización, según sea el caso. Por tanto será esencial tener en cuenta el impacto de la normativa de protección de datos de carácter personal.

En este contexto, *HR Analytics* es una nueva realidad de gestión de datos de empleados por los departamentos de RR.HH. *HR Analytics* y el cuadro de mando no son lo mismo. El cuadro de mando es más una herramienta de planificación estratégica con indicadores mientras *HR Analytics* pone el foco en los datos de los empleados y en la información obtenida sobre las personas en tres niveles: Nivel 1 (datos personales); Nivel 2 (datos de actividad/rendimiento) Nivel 3 (datos de relación con el negocio).

Una cuestión clave para el futuro de esta nueva función en las compañías tiene que ver con la pregunta de por qué es importante *HR Analytics*. En nuestra opinión, creemos que es un modelo de gestión para conocer mejor a los empleados y, también, para mejorar su rendimiento y el desarrollo de negocio con una metodología predictiva del comportamiento y potencial de los empleados. El objetivo de *HR Analytics* no es tener datos de los empleados. El objetivo es poner el foco en las interrelaciones de los datos para utilizarlos de manera ejecutiva (orientados a la acción) para tomar decisiones de negocio.

2. ¿Cómo impacta *HR Analytics* en las relaciones laborales de las empresas? ¿Y en los procesos de recursos humanos?

Como cuestión previa, debemos destacar que en la mayoría de los casos el marco jurídico regulador de las relaciones laborales en su conexión con la normativa de la protección de datos no es capaz de aportar soluciones claras a todos los conflictos laborales que pueden surgir. Hay, sin embargo, un espacio de respeto obligado si se quiere contar con seguridad jurídica para ambas partes (empresas y trabajadores) tanto para la negociación colectiva, si se opta por soluciones bilaterales acordadas, como para protocolos empresariales de regulación unilateral de las condiciones de uso de los medios tecnológicos por los trabajadores y sus representantes y de cumplimiento de las obligaciones relacionadas con el uso de datos de los empleados. Unos y otros –medidas consensuadas con los representantes o protocolos establecidos

unilateralmente- deben tener en cuenta las normas imperativas no disponibles en materia de relaciones laborales y protección de datos tanto internacionales (Convenios de OIT de ámbito laboral y Convenio numero 108 del Consejo de Europa para la Protección de Datos de Carácter Personal y la Recomendación numero 89 que adapta dicho convenio al ámbito del empleo) como las normas nacionales (Estatuto de los Trabajadores y LO 15/1999, de Protección de Datos de Carácter Personal (LOPD), así como la doctrina administrativa que pueda emanar de la propia Administración y las sentencias de los Tribunales internacionales y nacionales de posible aplicación.

Uno de los problemas centrales del impacto de *HR Analytics* en las relaciones laborales reside en que la LOPD es una norma genérica que no dispone reglas específicas para el ámbito laboral. *HR Analytics* parte del reconocimiento del poder de dirección del empresario tanto en su reconocimiento constitucional de la libertad de empresa (art. 38 CE) como en su plasmación en la ley laboral (art. 20.1 ET) y conecta también con el deber básico del trabajador de cumplir "ordenes e instrucciones del empresario en el ejercicio regular de sus funciones directivas". Además, se debe conocer que la celebración de un contrato de trabajo no implica que el trabajador quede privado de sus derechos constitucionales (STCo 106/1996) porque la libertad de empresa no legitima limitaciones injustificadas de los derechos fundamentales y de las libertades públicas (TCo 197/1998 y TCo 98/2000). A la inversa, los derechos fundamentales de los trabajadores es necesario respetarlos tanto en lo que se refiere a la libertad informática (art. 18.4 CE) como al derecho a la intimidad (art. 18.1 CE) aunque no son derechos absolutos, pudiendo ceder ante intereses constitucionalmente relevantes (TCo 99/1994 y 98/2000).

En este contexto, es importante destacar que la capacidad de los departamentos de recursos humanos y, en su caso, de la función de *HR Analytics* para almacenar, cruzar y gestionar datos de los trabajadores no es ilimitada y por ello la propia Constitución establece en su art. 18.4 que la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos como así se ha hecho con la aprobación de la LO 15/1999 (LOPD). Por su parte, el Tribunal Constitucional ha desarrollado una importante doctrina judicial relacionada con este nuevo derecho fundamental consistente en la protección de datos frente al uso indiscriminado de datos personales a través de tecnologías informáticas que es además un derecho instrumental ordenado a la protección de otros derechos fundamentales entre los que se encuentra el derecho a la intimidad (TCo 292/2000). Ese derecho fundamental de la persona (y por extensión de los trabajadores) a la protección de datos extiende su objeto más allá del derecho a la intimidad y entronca con los bienes de la personalidad que pertenecen al ámbito de la vida privada y al respecto de la dignidad personal. El derecho fundamental de protección de datos garantiza en el contexto de una relación laboral al empleado un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado (STCo 292/2000).

En definitiva, lo que esta en juego en el ámbito de las relaciones laborales y el uso de los datos de los empleados es el dilema entre "productividad versus privacidad". Por ello, la función de *HR Analytics* en las empresas debería atender tres reglas básicas para la gestión de los datos de los empleados: (i) Los datos recabados de los empleados deben de ser adecuados, pertinentes y no excesivos en relación al ámbito y a las finalidades para las que se hayan obtenido (art. 4.1 LOPD) puesto que se prohíbe el uso de datos para finalidades incompatibles con su recogida (art. 4.2 LOPD); (ii) Los trabajadores a los que se soliciten datos personales deberán ser informados de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida y de los destinatarios de la

información (art. 5 LOPD); y (iii) el tratamiento de los datos personales del trabajador requerirá el consentimiento inequívoco del mismo (art. 6 LOPD).

Vayamos a analizar cómo puede impactar *HR Analytics* en los procesos de recursos humanos:

En efecto, *HR Analytics* impacta en la selección (con los candidatos); en la contratación (en la formulación de los contratos de trabajo); en el desempeño (en la formulación y ejecución de las políticas retributivas); en la formación y desarrollo (para la planificación de carreras) o en la desvinculación (en el control y vigilancia de la actividad o prestación de trabajo). Con carácter previo al análisis particularizado de cada uno de esos procesos, es importante señalar que en cualquier de esos procesos se debe tener en cuenta el derecho fundamental a la protección de datos pero también otros derechos fundamentales de los empleados (intimidad; privacidad; secretos de las comunicaciones; no discriminación; etc.) aunque no sean derechos ilimitados. La negociación colectiva es un instrumento idóneo para modular los posibles conflictos entre el ejercicio del poder de dirección de las empresas y los derechos fundamentales de los empleados.

Asimismo, el contrato de trabajo puede ser idóneo para incluir aspectos vinculados con el uso y tratamiento de los datos de los empleados por la empresa. Finalmente, es absolutamente crítica la adopción de protocolos empresariales que incluyan indicaciones expresas que prohíban o toleren determinadas conductas de los empleados especialmente cuando puedan tener impacto en procesos de retribución, desempeño o desvinculación.

2.1 Proceso de selección de candidatos

- Es conveniente disponer de modelos de impresos tipo para la formalización del currículum y de un procedimiento de formalización y entrega de los mismos por los candidatos ya que ello permite no solo informar adecuadamente sino definir con precisión el tipo de datos a tratar, establecer las medidas de seguridad, etc.

- En el caso de que para la selección de personal se realice algún tipo de anuncio o convocatoria pública se deberá incluir la información del art. 5 LOPD.

- Es muy conveniente que la cesión de datos contenidos en el currículum cuente con el consentimiento del candidato.

- Una práctica emergente por los departamentos de recursos humanos de las empresas es la creación de redes sociales corporativas para la selección o la consulta de redes sociales profesionales abiertas (LinkedIn, Viageo, etc.) o incluso privadas (Facebook, Twitter, Second Life) para la captación de datos e información de los candidatos para la toma de decisiones final sobre el sentido favorable o desfavorable de la contratación. Es más: en ocasiones está proliferando la práctica de "blacklisting" a través de las redes sociales o la creación de listas negras en base al análisis de los candidatos en las redes sociales que deben abordarse con especial precaución por las compañías para evitar posibles alegaciones de discriminación directa o indirecta en el proceso selectivo para los candidatos excluidos (art. 4.2.c) ET). En esta materia, de nuevo será también importante para la función de *HR Analytics* velar por la calidad de los datos obtenidos y tratados de los candidatos y probablemente evitar como buena práctica su cesión a terceros (piénsese por ejemplo la posibilidad de compartir listas negras con otras empresas del sector por problemas de

desempeño o historial laboral o personal de los candidatos que pueda justificar su exclusión del proceso o no contratación) ya que los datos deben de ser veraces y concederle a los candidatos en caso de utilización la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. Sobre ello, resulta contundente el criterio de la AEPD que señala en su informe jurídico 0201/2010 que "*la inclusión de datos personales en una lista negra requerirá el consentimiento del interesado para ser conforme a lo dispuesto en la normativa de protección de datos*".

2.2 Proceso de contratación

- El contrato de trabajo es el vehículo idóneo para ofrecer información sobre los tratamientos de datos directamente relacionados con la prestación laboral. Hay algunos datos personales que pueden ser recogidos de manera lícita en el contrato (nombre, DNI, domicilio, cónyuge, hijos a cargo, edad del trabajador, etc.) . Sin embargo, hay datos personales cuya recogida puede ser considerada abusiva (número de móvil personal, mail personal, ideología, orientación sexual, etc.).

- También es posible recoger en el contrato los datos relativos a los beneficios sociales que se puedan otorgar a los trabajadores una vez contratados y que puedan conllevar por ejemplo ventajas en compras para el trabajador (ejemplo: tarjetas de descuento), esas decisiones de consumo requerirán que la cesión de datos se documenten en otro formato o medio distinto del contrato de trabajo.

- El mismo supuesto de hecho aplicará a los datos referidos en la contratación de seguros de vida y planes de pensiones de empleados, donde se precisará la cesión de datos de los empleados a la empresa aseguradora o la gestora del plan de pensiones.

- Se debe conocer por la función de *HR Analytics* en las empresas la plena validez y eficacia del contrato electrónico en el ámbito laboral ya que de un lado la Ley 59/2003 de 19 de diciembre de firma electrónica (LFE) dispone que el documento electrónico podrá ser soporte de documentos privados, como lo es el contrato de trabajo y de otro lado, la Ley 34/2002 de 11 de julio de servicios de la sociedad de la información y de comercio electrónico (LSSICE) señala que siempre que la ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en soporte electrónico.

- Del mismo modo, el contrato de trabajo electrónico es reconocido en la normativa de la Inspección de Trabajo (art. 15 del Real Decreto 138/2000 de 4 de Febrero).

2.3 Proceso de retribución

- Es importante garantizar la protección de los datos tanto en el caso de gestión interna de las nóminas como de externalización de la gestión de las nóminas donde aplica la normativa de tratamiento de datos por cuenta de terceros (art. 12 LOPD).

- Además, en esta materia son aplicables las fuertes restricciones para la función de *HR Analytics* que no puede compartir con terceros (otros trabajadores, representantes sindicales, etc.) la información retributiva de sus empleados cuya divulgación precisa de consentimiento expreso del trabajador afectado.

2.4 Proceso de desempeño / formación

- Existe un "equilibrio dinámico" entre la empresa y el trabajador sujeto a circunstancias sobrevenidas de modo que novedades referidas a hechos nuevos (ejemplo, descuento del canon o cuota sindical por afiliación sindical del trabajador con posterioridad a la firma del contrato; instalación de nuevo sistema de control de presencia con sistemas de fichaje informático, control biométrico o huella digital o de video vigilancia, de geolocalización y/o biométricos: uso por trabajadores de tarjetas con banda magnética; etc. requerirán la información previa y el consentimiento del afectado (arts. 5 y 6 LOPD). Por tanto, los registros de tiempo de trabajo que identifican el periodo de trabajo diario y de descanso de cada trabajador son datos personales porque lo identifican o lo hacen identificable (TJUE 30.5.2013 Caso Worten). En estos supuestos, dado que la finalidad de la recogida de datos por la empresa es comprobar el cumplimiento del contrato por parte del trabajador, no se requiere el consentimiento del trabajador pero este sí debe de ser adecuadamente informado (art. 6.2 LOPD). Además, estos sistemas de control del trabajo sí que exigen a las empresas cumplir el trámite de audiencia previa del Comité de Empresa (TS 19.12.2005).

- En las relaciones laborales, hay datos especialmente protegidos según la normativa por su especial sensibilidad –**"datos sensibles"- (art. 7 LOPD)**, entre otros: datos de ideología, religión o creencias; afiliación sindical; origen racial; salud; orientación o vida sexual; salud; raza u origen étnico; comisión de infracciones penales o administrativas; etc. Son datos que pertenecen al núcleo más intimo del trabajador como persona y resultan merecedores de especial protección y el trabajador puede negarse a su comunicación ya que un uso incontrolado puede conllevar consecuencias especialmente negativas para su titular.

- En los sistemas internos de denuncias ("*whistleblowing*") también hay datos sensibles a proteger tanto en relación al denunciado como al denunciante e incluso a los testigos, por lo que habrá que asegurar las medidas que garanticen la adecuada seguridad y confidencialidad.

2.5 Proceso de desvinculación

Un ámbito de especial alcance es el impacto de HR Analytics en los **controles empresariales de la prestación laboral** (e incluso del absentismo laboral) al amparo de lo previsto en el art. 20 ET. Inicialmente HR Analytics no está configurado como un modelo de gestión para el control de la prestación laboral pero si es cierto que las empresas pueden utilizar distintos soportes o medios que puede permitir ese control con el uso de medios tecnológicos, micrófonos, intervención de llamadas, video vigilancia, geolocalización, uso de redes sociales, uso de aplicaciones de mensajería instantánea (Whatsapp; Telegram; Line o Viber), etc. En

este ámbito se entrecruzan los derechos de las empresas derivados del ejercicio del poder de dirección y organización del trabajo (art. 38 CE) y los derechos de los trabajadores de privacidad y de secreto de las comunicaciones (art. 18.1 y 18.4 CE). También están en juego los límites de ambas partes (empresas y trabajadores). De un lado, porque las empresas tienen ciertas restricciones en la utilización de las nuevas tecnologías como parte del poder de dirección y vigilancia; de otro, porque los trabajadores tienen límites en el uso extralaboral de los medios tecnológicos puestos a su disposición por las empresas. Los principios clave a la hora de determinar la licitud de las actuaciones empresariales (y de eventuales pruebas en juicio) vinculadas al proceso de desvinculación o despido y resolver ese conflicto jurídico son, de acuerdo con la normativa aplicable y la doctrina judicial, los siguientes:

- Información previa a los trabajadores (art. 5 LOPD) (STC 29/2013 y STS 13/05/2014);
- Consentimiento del trabajador (art. 6.1 y 2 LOPD) (STS 10/09/2015) y
- Calidad de los datos que permite a los trabajadores corregir o cancelar los datos inexactos o indebidamente procesados y que viene determinada por los principios de legitimación y concurrencia de un fin legítimo, proporcionalidad y congruencia y adecuación a las finalidades previstas en las actividades de vigilancia y control empresarial (art. 4.1.LOPD). La concurrencia de un fin legítimo viene asociada a cuestiones de seguridad, protección del patrimonio empresarial, salud, exigencias del proceso productivo y no cabe "con el único fin de controlar el trabajo" (STSJ C.Valenciana 03/05/2012). Además, es importante la buena fe contractual cuya transgresión ha sido declarada en alguna ocasión por los Tribunales.

2.6 Prevención de riesgos laborales

- Está previsto que el titulo contractual (contrato de trabajo) sean el título para el cumplimiento, desarrollo y control de los datos (art. 6.2 LOPD).
- De particular interés son los reconocimientos médicos cuya regla general es la voluntariedad y en el caso de Servicios de Prevención Propio las empresas son responsables del fichero que se genere para la gestión de la prevención.
- El nivel de seguridad es elevado en el caso de datos de salud con identificación de enfermedades y en el caso de historia clínica del trabajador deben establecerse procedimientos para garantizar los derechos de acceso, rectificación y cancelación de los trabajadores.
- Los datos relativos a la salud de los empleados solo pueden recabarse y tratarse cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. Cabe, no obstante, el tratamiento de los datos de salud de los empleados si resulta necesario para la prevención o para el diagnostico medico. No obstante, el alcance de las facultades de acceso de la empresa a los datos de salud de los trabajadores es muy limitada y en la práctica se limitan a conocer la condiciones de aptitud o no aptitud del trabajador. Además, en materia preventiva, la

normativa habilita y obliga a ceder datos a los delegados de prevención y Comités de Seguridad y Salud laboral.

2.7 Impacto de HR Analytics en las relaciones con los sindicatos y los representantes de los trabajadores

- Exige a las empresas que respeten los derechos de libertad sindical y el conjunto de derechos, competencias y funciones reconocidos a los representantes de los trabajadores (art. 28 CE) y en particular el elenco de derechos y garantías de los representantes (art. 68 ET y 8.2.LOLS) lo que, en la práctica, obliga a tomar decisiones empresariales sobre el uso de tablones sindicales presenciales o digitales y la limitación del acceso de esa información a los representantes legales electos.

- Por ello, la empresa no tiene obligación de garantizar y disponer para uso sindical del correo electrónico pero si ya está implantado un sistema de comunicación informático, la negativa arbitraria de la empresa a la utilización por los representantes vulnera la libertad sindical aunque si hay una utilización abusiva por parte de los sindicatos de las herramientas informáticas estará justificada la negativa empresarial (STCo 7.11.2005).

- El uso sindical de las comunicaciones informáticas a los empleados (tablones electrónicos virtuales; correos o buzones sindicales; etc.) exige un criterio de moderación y una reglas de uso o utilización que pueden ser predeterminadas por las empresas de acuerdo con los siguientes criterios:

    - El uso sindical del correo debe ser solo para transmitir información laboral y sindical;

    - Las comunicaciones electrónicas sindicales a la plantilla no deben perturbar la actividad normal de la empresa; y

    - La utilización de las comunicaciones electrónicas sindicales no deben ocasionar mayores costes a la empresa al servicio de las necesidades sindicales ni entorpecer el uso especifico empresarial de las herramientas informáticas.

- En el ámbito sindical, será importante para la función de HR Analytics decidir el alcance de los datos de los empleados que se comunican a los sindicatos. En principio, únicamente pueden cederse por la empresa datos en aquellos casos que lo exija el cumplimiento de las obligaciones o deberes previstos en el Estatuto de los Trabajadores y/o normas concordantes. El artículo 64.2.d ET reconoce la obligación de la empresa de comunicar datos al Comité de Empresa sobre importantes aspectos, entre otros: las estadísticas sobre el índice de absentismo y sus causas; los accidentes de trabajo y enfermedades profesionales y sus consecuencias; los índices de siniestralidad; o los mecanismos de prevención utilizados. En esta materia, también es importante en cumplimiento de lo previsto en la normativa laboral la gestión de las cesiones de datos personales de los empleados a los sindicatos y de los datos contenidos en TC2, copias básicas de contratos y nóminas tanto de personal propio como de empresas contratistas (art. 44 ET).

2.8 Ejemplos prácticos sobre la gestión de datos de los empleados por la función de *HR Analytics*

Veamos algunos ejemplos prácticos sobre el alcance, los límites y los problemas que plantea la gestión de datos de los empleados por parte de la función de HR Analytics en las empresas cuando se trata de captar datos e información de empleados que permitan verificar su desempeño, medir su productividad o, incluso, justificar procesos disciplinarios o de desvinculación:

- ¿Puede el empresario capturar datos o información relevante a través cámaras de video y micrófonos? Sí, pero exclusivamente en lugares de trabajo y no en dependencias que pueden ser privadas como áreas de descanso, cafeterías, vestuarios, locales sindicales y sin posibilidad que las grabaciones tengan difusión externa. Es recomendable también que esa situación sean conocida previamente por los trabajadores y/o sus representantes (TCO 98/2000 y TSJ de Madrid 17.04.2009).

- ¿Se puede prohibir por el empresario el uso privado de un móvil corporativo? ¿se pueden controlar las llamadas telefónicas del trabajador y utilizar esos datos para justificar sanciones? La empresa tiene libertad plena para prohibir (y por tanto no tolerar) el uso de dispositivos corporativos para usos privados. El control empresarial de las llamadas debe respetar el secreto de las comunicaciones (STS 10.3.1990).

- ¿Es posible captar y gestionar datos de un trabajador recogidos en llamadas telefónicas, correo electrónico o navegación por Internet desde su puesto de trabajo sin vulnerar su privacidad? Sí, pero se le debe advertir al trabajador antes de la fiscalización (Caso Copland, TEDH 3.04.2007).

- ¿Puede el empresario acceder lícitamente a las redes sociales privadas de un trabajador para controlar el envío de mensajes privados con dispositivos corporativos? Sí, siempre que exista información previa y normativa interna que prohíba el uso de recursos tecnológicos facilitados por el empleador para usos privados (Caso Barbulescu, TEDH 12.01.2016).

- ¿Cabe establecer con carácter unilateral una prohibición absoluta del uso personal de las herramientas tecnológicas para usos privados por el trabajador? Sí, ya que es un medio adecuado para descartar cualquier margen de tolerancia por la empresa y rompe toda expectativa de privacidad (STS 6.10.2011). No obstante, es recomendable acompañar esa prohibición con una comunicación general a todos los trabajadores y con la aprobación de un protocolo de uso de herramientas informáticas.

- ¿Es necesario incluir en un convenio colectivo el tipo de infracción de uso extralaboral de herramientas informática? No es necesario aunque si recomendable. Es más: el tipo infractor es un indicio más de la prohibición absoluta de ese uso en la empresa.

- ¿Es conveniente tener un protocolo de uso de los datos de los empleados en los distintos procesos de RRHH? Sí. Los protocolos de control o uso de datos de los empleados no son exigidos por la normativa o los Tribunales nacionales pero el Tribunal Europeo de Derechos Humanos sí sugiere

en muchas sentencias que los trabajadores deben estar informados de las condiciones en que van a ser restringidos sus derechos.

- ¿Puede HR Analytics crear una base de datos de salud de los empleados como registro de bajas médicas por incapacidad temporal sin consentimiento de los empleados? El título empresarial previsto en los artículos 22 y 23 de la Ley de Prevención de Riesgos Laborales que impone la vigilancia periódica de la salud de los empleados y de la conservación de la documentación relativa a los controles sanitarios y de la relación de accidentes de trabajo y enfermedades profesionales no parece suficiente para justificar la concurrencia del interés general si la finalidad de la base de datos no es preservar la salud de los empleados sino controlar su absentismo (STCo 202/1999).

- ¿Puede la empresa utilizar los datos de afiliación sindical en procedimientos de despido disciplinario para comunicar a los delegados sindicales el despido de sus afiliados? El art. 55.1 ET exige audiencia previa a los delegados sindicales cuando al empresario le constara la afiliación y si a la empresa le consta por el descuento de la cuota sindical no parece que existe vulneración alguna del derecho de protección de datos.

- ¿Es lícito comunicar a terceros la productividad o retribución variable de un empleado a sus compañeros sin el consentimiento del trabajador afectado? No. El TCo mantiene que la cesión de datos a terceros para fines distintos de los que motivaron su recogida “supone una nueva posesión y su uso requiere el consentimiento del interesado” (STCo 292/2000).

- ¿Puede la empresa comunicar o proporcionar a los representantes sindicales, unitarios y/o electos en el contexto de un periodo de consultas de reestructuración empresarial o de modificación sustancial de condiciones de trabajo o de inaplicación del convenio, información sobre la productividad de los empleados seleccionados por las medidas laborales? No. La cesión de datos a terceros tiene importantes limitaciones según la normativa de protección de datos.

3. ¿Cómo impacta la función de *HR Analytics* en la gestión de los datos o información corporativa por los empleados? ¿Y en las políticas sobre el uso de los datos en los ordenadores corporativos? ¿Y en las políticas "*Bring your own device*"? ¿Y en las políticas de "*Cloud computing*"?

Con carácter inicial, HR Analytics esta configurada como una función de la empresa para gestionar los datos de los empleados con una metodología que permite conocer información individual del empleado que crea valor al negocio y que puede generar conocimiento valioso para la toma de decisiones en materia de retribución, formación, promoción, movilidad internacional o desvinculación. HR Analytics es una herramienta que va a permitir monitorizar a los empleados, saber quién y por qué tiene un rendimiento destacado, conocer sus gaps o carencias en formación técnica o de negocio, en habilidades o competencias y planificar decisiones o políticas individuales o personalizadas sobre los empleados para optimizar su desempeño, planificar su carrera profesional, reconocer su compromiso y resultados, …. HR

Analytics puede ser la diferencia entre una gestión "hueca" o tradicional de procesos de recursos humanos y una gestión "avanzada" e "inteligente".

A la inversa HR Analytics puede también ser una herramienta que sea un soporte de búsqueda de eficiencia y de productividad y sea también un mecanismo de control y vigilancia del uso correcto de los datos corporativos por los empleados. En esta perspectiva, HR Analytics puede contribuir en la elaboración o en la ejecución de las políticas de limitación del uso de la tecnología que pueda desarrollar y regular aspectos como el uso de los dispositivos informáticos y de comunicaciones de la empresa para fines profesionales y la potestad de control, las condiciones del uso de internet y del correo electrónico con esos dispositivos de la compañía, las limitaciones del uso de las redes sociales o de las aplicaciones móviles de mensajería instantánea, etc.

En el caso de que las empresas opten por razones de optimización de costes y ahorro de gastos de aprovisionamiento electrónico por políticas conocidas como *"Bring your own Device",* práctica a través de la cual los trabajadores emplean sus dispositivos personales (ordenadores, tablets, smartphones, etc.) con interfaz corporativa para el desarrollo de sus actividades laborales, los empleados van a acceder a datos corporativos y a información directamente relacionada con el desempeño de sus funciones. En esas políticas, *HR Analytics* podría asumir un rol preventivo y de control de fugas de información comercial y delimitar los accesos permitidos y no permitidos de un tercero a la información laboral y personal de los empleados, fuera y dentro del horario laboral, extravíos, virus y una larga lista de inseguridades que pueden "encarecer" enormemente esta práctica.

En esa materia, resultará muy recomendable aprobar e implementar un política de uso de dispositivos personales muy restrictiva y con fuertes medidas de seguridad delimitando las fronteras siempre difusas de "transparencia" y "privacidad" de modo que la información laboral y corporativa (y con mayor abundamiento si es comercial o de negocio) pueda estar fuertemente encriptada con contraseñas, bloqueos del dispositivo por inactividad o acceso no autorizado.

Finalmente, los servicios de *cloud computing* (computación en nube) conllevan nuevas ventajas para las empresas y para los trabajadores para la movilidad o acceso compartido a información ya que conlleva ahorro de costes en inversiones en infraestructura tecnológica para el tratamiento de la información al quedar la misma en un proveedor externo. Sin embargo, como toda contratación o externalización a un proveedor, esta contratación externa no está exenta de riesgos legales y las empresas siguen siendo responsables de dicha información. La función de *HR Analytics* debe gestionar los riesgos de la externalización de los datos de los empleados a los proveedores de *cloud computing* y vigilar la transferencias internacionales de datos especialmente a partir de la derogación del programa *Safe Harbour* para la transferencia de datos a Estados Unidos. Por ello, será necesario la previa autorización del Director de la AEPD para realizar dicha transferencia internacional de datos cuando la transferencia de datos personales sea a países no adecuados si el proveedor no es nacional o gestiona esos datos en otros países y jurisdicciones. Sobre ello, es importante recordar que todos los países del Espacio Económico Europeo y algunos otros (Argentina, Canadá, Suiza, etc.) si cuentan con un nivel de protección adecuado para estas transferencias internacionales de datos.

4. Los retos jurídicos del "*big data*" en las relaciones laborales

El "*big data*" se caracteriza por las conocidas **"cinco V": volumen, velocidad, variedad, valor y veracidad**, tal y como defienden los expertos en la materia. Las principales funciones o utilidades del "*big data*" cubren la analítica predictiva, la adecuación y optimización de los procesos.

Aunque muchas de las cuestiones que este tema suscita no se han dilucidado todavía y son objeto de estudio e interpretación legal en la actualidad, conviene destacar el esfuerzo realizado por el Grupo Internacional de Trabajo sobre Protección de datos en el sector de las Telecomunicaciones, también conocido como Grupo de Berlín, que elaboró en 2014 los principios que deben regir el "big data" en un intento por velar por el cumplimiento de las garantías de privacidad y protección de datos de las personas afectadas por el uso de "big data" y que se pueden resumir en los siguientes:

- **Legitimidad y consentimiento**: para que el tratamiento del dato personal sea legítimo, el afectado debe haber prestado su consentimiento inequívoco y cuando esto no sea posible el tratamiento de los datos deberá restringirse al respeto de los límites previamente establecidos;

- **Establecimiento de mecanismos de anonimización robustos**: en la medida en que se pueda decidir que los datos objeto del tratamiento de "*big data*" se traten de forma anónima, bajo seudónimo o manteniéndolos identificables y si se tratan de forma anónima se podrían reducir o incluso eliminar los riesgos asociados a la privacidad;

- **Mayor transparencia y control de la recogida y utilización de los datos**: buscando que todas las personas estén informadas de los datos que se recaban, el tratamiento de los mismos y las finalidades del mismo;

- **"*Privacy by design*" y rendición de cuentas**: es importante que las medidas anteriores se combinen con el diseño de privacidad y la rendición de cuenta para mitigar los riesgos en materia de privacidad y contribuir a generar confianza en los titulares de datos.

Entre los elementos característicos del "big data" se pueden citar la utilización de información ya existente con fines secundarios o alternativos, la consolidación de datos de múltiples fuentes y la creación de nuevas fuentes de datos.

Desde la perspectiva de la regulación de protección de datos se plantean por su parte los siguientes retos:

- **Posibilidad de expansión del ámbito de aplicación de la regulación de datos personales** a este tipo de datos. Elementos como el "profiling" ya están presentes en el nuevo Reglamento Europeo de Protección de Datos teniendo en cuenta la amenaza que supone para las personas la toma de decisiones basada en el análisis automatizado de perfiles personales incluso cuando dicho perfilado se realice con información disociada en la que el individuo haya sido anonimizado.

- **Derecho del titular de los datos a conocer y elegir sobre el tratamiento de sus datos personales**. El uso de herramientas de HR Analytics y big data deberán tener en cuenta estos derechos reconocidos por la legislación europea y que, en la mayoría de los casos implicarán la necesidad de obtener un consentimiento informado del empleado o del candidato para poder tratar la información relevante.

- **Aplicabilidad de los derechos ARCO** (acceso, rectificación, cancelación y oposición) al tratamiento de la información generada en entornos de analítica de recursos humanos.

- **Riesgos asociados a la divulgación de información analítica a terceros.** Será necesario identificar para ello en que supuestos este acceso re lleva a cabo sobre información anonimizada de manera válida a efectos legales o sobre información personal y, en este último caso, si dicho acceso puede tener la consideración de cesión de datos (en cuyo caso será necesario, con carácter general, haber obtenido el consentimiento del afectado) o si se trata de una prestación de servicios o encargo de tratamiento (lo que llevará a la necesidad de regular contractualmente la relación cumpliendo con los requisitos específicos establecidos en la ley).

- **Procedimientos para la disociación de datos.** El criterio actual sostenido por la AEPD exige que la disociación sea irreversible para que la anonimización de datos sea considerada suficiente a efectos de evitar la aplicación de la normativa de protección de datos a dicha información. Sin embargo, la disociación irreversible puede impedir que los datos analíticos o de perfilado puedan ser verificados, pudiendo desplegar efectos injustos o no fundamentados para un empleado o candidato que se vea afectado por las decisiones basadas en dichos criterios analíticos.

- **Restricciones a la cesión de datos y a la transferencia de datos transfronterizos**. La falta de disociación irreversible implica la aplicación plena de la regulación de protección de datos a la información obtenida a partir de procesos de *HR Analytics* limitando la cesión y transferencia internacional de estos datos conforme a la normativa aplicable para la protección de datos de carácter personal.

Una referencia para la protección de los derechos de los individuos desde la perspectiva de la protección de los datos de carácter personal, cuando se utilizan herramientas de *HR Analytics*, es la posible aplicación de los principios de *Privacy by Design*. Estos principios han sido ya reconocidos por el Reglamento Europeo de Protección de Datos y tienen su origen en las guías desarrolladas por la autoridad de protección de datos de Ontario, Canadá (el *Information and Privacy Commissioner of Ontario* o IPC). Estos principios pueden ser aplicables al diseño de aplicaciones informáticas que traten datos personales y se pueden resumir en los siguientes criterios esenciales:

- Protección proactiva y no reactiva. Es mejor prevenir que curar.
- Privacidad por defecto. Las herramientas deben ser diseñadas para proteger la información personal sin que sea necesario configurarlas para ello posteriormente.
- La Privacidad debe estar embebida en el diseño.
- Funcionalidad total sin pérdida de privacidad. El usuario no tiene por qué compensar el acceso a funcionalidades con la pérdida de privacidad innecesaria como moneda de cambio.
- Seguridad de extremo a extremo. Protección de Ciclo de Vida Completo
- Visibilidad y Transparencia – Mantenerlo Abierto. Todos los afectados por el tratamiento de sus datos deben poder verificar el cumplimiento de las declaraciones del responsable. Por esto, el Privacy by Design, establece la obligatoriedad de mostrar de manera visible y transparente a usuarios y proveedores, la información referente a la gestión de la privacidad.
- Respeto por la Privacidad de los usuarios – Mantener un Enfoque Centrado en el Usuario

En el ámbito del "big data" el IPC ha propuesto también unas guías de actuación para aplicar los principios de Privacy by Design que se concretan en las siguientes reglas a incorporar en el diseño de aplicaciones analíticas:

- Atribución completa o plena trazabilidad de la información.
- Anclaje entre la fuente de datos y la información resultante.
- Analytics sobre datos anónimos.
- Existencia de registros de auditoría a prueba de manipulaciones.
- Métodos que favorezcan falsos negativos frente al riesgo de falsos positivos.
- Autocorrección de falsos positivos.
- Control y responsabilidad sobre la transferencia de información.

Por su parte, el artículo 20 del Reglamento Europeo de Protección de Datos establece en cuento a la toma de decisiones automatizadas con respecto a individuos, incluyendo el perfilado, que el interesado tendrá el derecho a no ser objeto de una decisión basada únicamente en un tratamiento automatizado que produzca efectos jurídicos con respecto a él o ella, o que de una manera similar le pueda afectar significativamente.

En este contexto, la regulación europea define el "*profiling*" como cualquier forma de tratamiento automatizado de datos de carácter personal que consista en el uso de esos datos para evaluar determinados aspectos personales correspondientes a una persona física, en particular, para analizar o predecir aspectos relativos al rendimiento de las personas físicas en el trabajo, la situación económica, la

salud, las preferencias personales , los intereses, la fiabilidad, el comportamiento, la ubicación o movimientos.

5. Uso de datos externos por la función de *HR Analytics* en las empresas

El papel de los datos externos es hoy en día esencial para cualquier solución de análisis de recursos humanos. Los datos obtenidos de las redes sociales y sitios externos al ámbito de trabajo son cruciales para la comprensión de la retención, compromiso, y necesidades de carrera de los empleados, pudiendo incluso ser más útiles que los datos obtenidos dentro de la empresa.

Las personas son cada vez más conscientes del valor de sus datos personales pero también están más dispuestas a compartirlos, siempre y cuando consigan algo a cambio. Redes sociales como LinkedIn o Facebook pueden proporcionar una cantidad ingente de información al área de recursos humanos de una compañía pero ¿es éticamente y legalmente correcto utilizar estos sitos web para evaluar a un candidato? ¿Se puede acceder a esta información por parte de la empresa sin consentimiento del candidato o del empleado?

En lo que respecta a España, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) limitaba el concepto de fuentes de acceso público, estableciendo una lista tasada en la que no se encontraba la información contenida en redes sociales. Sin embargo, el Tribunal de Justicia de la Unión Europea declaró en su Sentencia de 24 de noviembre de 2011, en respuesta a las cuestiones prejudiciales planteadas por el Tribunal Supremo, la incorrecta transposición en la normativa española de la Directiva marco de protección de datos.

La Sentencia interpretó la Directiva señalando que pueden obtenerse datos personales, sin el consentimiento del titular de los mismos, siempre que se respeten sus derechos y libertades fundamentales, y sólo si dicha obtención responde a un interés legítimo del responsable del tratamiento o del tercero al que se cedan los datos.

La Directiva 95/46/CE establecía, en su artículo 7.f, lo siguiente (el subrayado es nuestro):

> *"Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:*
>
> *(…)*
>
> *f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva."*

En este sentido, la Sentencia del TJUE referenciada destacó en su fundamento 49 el carácter directo de la aplicación del artículo anterior:

> *"49. Habida cuenta de estas consideraciones, procede responder a la primera cuestión que el artículo 7, letra f), de la Directiva 95/46 debe interpretarse en el sentido de que se opone a una normativa nacional que, para permitir el tratamiento de datos personales necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se*

comuniquen los datos, exige, en el caso de que no exista consentimiento del interesado, no sólo que se respeten los derechos y libertades fundamentales de éste, sino además que dichos datos figuren en fuentes accesibles al público, excluyendo así de forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes."

En base al fallo del TJUE, la Sentencia de 8 de febrero del Tribunal Supremo declaró nulo el artículo 10.2.b del RLOPD, de desarrollo de la LOPD, reconociendo la aplicabilidad directa de las disposiciones de la Directiva 95/46/CE.

A partir de ese momento, diversas modalidades de tratamiento o cesión de datos que anteriormente no estaban amparadas por la LOPD, como la obtención de datos desde ficheros de terceros, podrían posiblemente quedar cubiertas por la normativa europea.

La Sentencia del TJUE declaró la aplicabilidad directa en España del artículo 7.f de la Directiva 95/46/CE, afirmando su carácter exhaustivo y taxativo, así como la inaplicabilidad de las disposiciones nacionales que exijan requisitos adicionales para el tratamiento o cesión de datos, como ocurre también con respecto al artículo 6.2 de la LOPD, en el sentido dado por la definición de "fuentes accesibles al público" (art. 3.j LOPD), aunque no anulado por no resultar jurídicamente posible. También se declararía inaplicable el artículo 10.2.b del RLOPD, de desarrollo de la LOPD.

Por su parte, el Tribunal Supremo no extrajo conclusiones ni estableció directrices sobre los efectos en la interpretación del interés legítimo, de modo que se remite a cada caso concreto la ponderación que deban realizar los responsables del tratamiento o los organismos reguladores; en el caso de España la AEPD, de los derechos y libertades fundamentales de los titulares de los datos personales.

De forma previa al pronunciamiento del Tribunal Supremo sobre la Sentencia del TJUE, la AEPD emitió una nota de prensa en la que defendía la LOPD y su interpretación hasta el momento. La AEPD afirmó que la restricción a las fuentes accesibles al público para el tratamiento de datos sin el consentimiento del interesado formaba parte de la necesaria ponderación entre los derechos del mismo, en contraste con el interés legítimo de la entidad que los trata, en los términos descritos en la Sentencia del TJUE.

Ante la posible aplicabilidad directa del artículo 7.f de la Directiva 95/46/CE, la AEPD condicionó su interpretación a la decisión del Tribunal Supremo, pero desde la publicación efectiva de dicha Sentencia; confirmando en gran medida la Sentencia del TJUE, la AEPD no ha emitido directrices explícitas ni guías de interpretación que faciliten a los responsables del tratamiento la labor de delimitar el alcance de un tratamiento de datos personales realizado a partir de fuentes públicamente accesibles, en su definición no tasada.

Resulta arriesgado, por tanto, realizar un tratamiento de datos personales sólo en base a lo establecido por las sentencias del TJUE y del Tribunal Supremo, asumiendo la aplicabilidad del interés legítimo como argumento universal para llevar a término cualesquiera tratamientos de datos personales, incluido el acceso a la información contenida en redes sociales o, en general en Internet, para evaluar candidatos o trabajadores por parte del empleador, especialmente en vista de la restrictiva interpretación por parte de la AEPD, salvo que se realice a partir de una adecuada ponderación entre los derechos de los titulares de los datos personales y el interés legítimo de la compañía responsable del tratamiento.

Por otro lado, en la actualidad sigue íntegramente en vigor el artículo 6.2 de la LOPD, desarrollado por el artículo 10.2.b del RLOPD anulado, y que mantiene la necesidad de que una fuente de información encaje en alguna de las categorías de fuentes accesibles al público definidas en el artículo 3.j de la LOPD. Cabe hacer constar que el pronunciamiento del Tribunal Supremo no pudo declarar nulos o inaplicables los preceptos de la LOPD en la medida en que quedaron fuera de debate por delimitarse los autos al artículo del RLOPD, y dado que el Tribunal Supremo no es competente para la derogación de preceptos contenidos en una norma de carácter orgánico.

Asumiendo la nulidad implícita de los preceptos señalados y no existiendo pronunciamiento sobre los mismos hasta la fecha, presumiblemente las redes sociales y otros medios públicamente accesibles no se beneficiarían de forma automática de todas las facilidades que la LOPD y su interpretación por la AEPD han venido otorgando a las que actualmente constan en la definición de "fuentes accesibles al público" del artículo 3.j de la LOPD. En esta línea, dispone la AEPD en su Informe 0178/2012:

> *"Por otra parte, es indudable que la Sentencia del Tribunal Supremo ha anulado lo dispuesto en el artículo 10.2 b) del Reglamento de desarrollo de la Ley Orgánica, pero ello no implica necesariamente que del marco establecido por las normas de protección de datos se haya desplazado de forma absoluta el concepto jurídico de fuentes accesibles al público."*

Por tanto, aún no ostentando automáticamente la condición de "fuentes accesibles al público" bajo la definición de la LOPD, sí podrían beneficiarse de las excepciones al consentimiento para el tratamiento o cesión de los datos originados en aquellas redes, siempre que se sustenten en una adecuada ponderación del interés legítimo del responsable del tratamiento y de los derechos de los titulares de los datos, todo ello de conformidad con el artículo 7.f de la Directiva 95/46/CE.

Así lo entiende la Sentencia de la Audiencia Nacional de 31 de mayo de 2012, al referirse a la ponderación prevista en tal artículo 7.f:

> *"Ponderación de intereses en conflicto que dependerá de las circunstancias concretas de cada caso y en la que no obstante, sí puede tomarse en consideración, a efectos de determinar la posible lesión de los derechos fundamentales del afectado, el hecho de que los datos figuren ya, o no, en fuentes accesibles al público. Más ello, simplemente, como un elemento más de ponderación.*
>
> *Es posible, en definitiva, y conforme a dicha Jurisprudencia comunitaria, que existan tratamientos de datos personales que no figuren en una de las que nuestra legislación interna denomina "fuentes de acceso público" (artículo 3.f) LOPD y articulo 7 RLOPD) pero que, sin embargo, no requieran el consentimiento de los titulares de tales datos porque su tratamiento sea necesario para satisfacer un interés legítimo del responsable de los mismos, o del cesionario, siempre que se respeten los derechos y libertades del interesado."*

6. Ponderación del interés legítimo y el tratamiento de datos de fuentes públicas (redes sociales) por parte de la función de *HR Analytics*

La Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 8 de febrero de 2012, parte del objetivo de equiparar e igualar la legislación española con la comunitaria en cuanto a la excepción al consentimiento en el tratamiento de datos de carácter personal.

El supuesto en el que se centraban los demandantes, por entender que no se ajusta al Derecho Comunitario establecido en la Directiva 95/46/CE, es el contenido en el artículo 6.2 de la LOPD y 10.2.b) del RLOPD, que establecen que para estar ante una excepción a la necesidad de recabar el consentimiento del interesado o afectado han de darse tres condiciones:

- que los datos figuren en fuentes accesibles al público,
- que el responsable del fichero o el tercero a quien se comuniquen los datos tenga un interés legítimo para su tratamiento o conocimiento, y
- que no se vulneren los derechos y libertades fundamentales del interesado.

Dado que en la Directiva 95/46/CE no contempla como condición que los datos que van a ser objeto de tratamiento provengan de fuentes accesibles al público, el Tribunal Supremo entendió que la legislación española, en vez de precisar el contenido de la Directiva 95/46/CE al transponerla al derecho interno, modificó el régimen jurídico contemplado en la norma comunitaria.

En este sentido, conforme a la nueva lectura sólo deberán darse dos condiciones para poder recabar datos de carácter personal sin el consentimiento del interesado:

- el respeto a los derechos y libertades fundamentales del interesado, y
- la existencia de un interés legítimo del responsable del fichero prevaleciente sobre los derechos del interesado. Dicho interés legítimo supone un concepto jurídico indeterminado que dependerá del contexto y de la situación en la que nos encontremos, y la Sentencia recuerda que "interés legítimo" no se traduce necesariamente en "interés económico".

La AEPD se pronunció al respecto en varios informes jurídicos (entre otros, Informes Jurídicos 0111/2012, 0112/2012, 0121/2012, 0178/2012 y 0147/2013). En su opinión, la impugnación de estos artículos de las normas españolas no implica que se haya desplazado de forma absoluta el concepto jurídico de fuente accesible al público, pues en sí mismo es un criterio de valoración o ponderación de las reglas establecidas en la Directiva, en su artículo 7.f, si bien la Audiencia Nacional establece en su Sentencia de 31 de mayo de 2012 que se trataría simplemente de un elemento más de ponderación, no el único.

El interés legítimo es el título habilitante y, el hecho de que los datos figuren en fuentes accesibles al público es un requisito adicional, que seguramente ayudará a valorar favorablemente el interés legítimo. Se entiende que prevalece el interés del responsable o del tercero ante el derecho a la protección de datos en particular y a los derechos y libertades fundamentales en un ámbito más amplio. Pero ni la Directiva comunitaria ni la LOPD pueden amparar ningún acceso genérico a datos de carácter personal sin una

adecuada ponderación tanto del interés legítimo de quien accede a los datos como de los derechos y libertades fundamentales del interesado.

Ha de destacarse que los datos recabados que no obren en fuentes accesibles al público, en palabras de la AEPD, ''*implicarán un conocimiento por parte del responsable o el tercero de datos de la vida privada del interesado*'', por lo que la ponderación con los derechos y libertades fundamentales del afectado deberá realizarse en su justa medida, de una manera más meticulosa que en el caso de que nos encontremos ante datos que obren en fuentes accesibles al público.

En definitiva, el tratamiento de datos provenientes de fuentes públicamente accesibles (y no consideradas estrictamente "fuentes accesibles al público") no está exento de controversia. Por una parte, el tratamiento de esta información precisaría, para el mejor cumplimiento de sus finalidades, no depender del consentimiento del interesado, que podría ser otorgado o no. Por otro lado, similares dificultades supone la necesidad de que este tipo de tratamientos esté sujeto a deberes de información de los interesados, dada la rapidez y volumen en que se pueden producir los tratamientos de información y la limitación práctica de cumplir con los deberes formales en este sentido.

A pesar de ello, la evolución en los últimos años del concepto de interés legítimo y su abertura respecto al estatus anterior; sometido a las estrictas excepciones legalmente previstas y a la clasificación en una lista tasada de fuentes accesibles al público, ha facilitado que este tipo de iniciativas, cuya finalidad última es la defensa de derechos y bienes jurídicos protegidos, estén dotadas de una mayor legitimidad de cara a una adecuada puesta en práctica.

De este modo, los pasos a adoptar por parte del empleador en caso de uso de información de empleados o candidatos contenida en redes sociales pueden resumirse como sigue:

- Necesidad de revisión comparativa de las políticas de las distintas redes sociales y medios equivalentes con los protocolos de los mecanismos de control establecidos por el propio empleador.

- Alineación de los medios y sistemas de tratamiento de la información con la normativa aplicable en España, a saber LOPD, RLOPD y legislación sectorial complementaria, adaptando sus protocolos de funcionamiento a la consideración del acceso a la información basándose en la existencia de un interés legítimo, permitiéndose el almacenamiento y conservación de los indicios de la existencia de dicho interés legítimo y su prevalencia sobre los derechos del interesado.

- Adaptación de las cláusulas contractuales existentes con empleados y candidatos para cubrir las necesidades de consentimiento e información aplicables en función del tipo de tratamiento, y remisión de las mismas para su aceptación por parte de los interesados.

- Adaptación de las políticas de uso de los portales internos y externos ofrecidos por el empleador para la posible reutilización de esta información con fines analíticos.

7. Referencias bibliográficas

- BAKER&McKENZIE. "Guía legal sobre Internet. Tecnologías en el trabajo: privacidad y productividad" Editado por Expansión 12 de marzo 2016.
- BAKER &McKENZIE: "Global Data Protection : Enforcement Report" 2016
- SEMPERE NAVARRO, A y SAN MARTIN MAZZUCONI C. “Las TICs en el ámbito laboral”, Claves Prácticas, Editorial Francis Lefebvre 2015.
- DESDENTADO BONETE, A y MUÑOZ RUIZ, “Control informático, Videovigilancia y Protección de Datos”, Editorial Lex Nova, 2012.
- AEPD, “Guía sobre la Protección de Datos en las Relaciones Laborales”.
- AEPD, “Informe jurídico 2009-0006: Legitimación para tratamiento de datos de los trabajadores”.
- AEPD, “Informe jurídico 2002-0000: Utilización del dato de afiliación sindical en los procedimientos de despido”.
- AEPD, “Informe jurídico 2004-0434: Tratamiento de datos conforme a la legislación de prevención de riesgos laborales”.

Segunda parte

Mitos y realidades de *HR Analytics*. Conclusiones

Segunda parte: Mitos y realidades de HR Analytics. Conclusiones

La transformación digital está conllevando profundos cambios en los modelos de negocio de las empresas con la aparición del “Big Data”, “el internet de las cosas” o la aceleración del comercio electrónico y las plataformas virtuales y las tecnologías de la información. En ese nuevo contexto, la función de RR.HH. necesita de un lado, superar la barrera de los factores culturales para la gestión del cambio con sus empleados y anticipar el futuro y las tendencias buscando talento digital y asegurar el desarrollo de habilidades y competencias digitales manteniendo el compromiso y la retención y de otro, afrontar el reto de la gestión masiva de datos personales y profesionales de los empleados provenientes de fuentes internas o externas. En ese camino, emerge también la función de HR Analytics que supone una oportunidad estratégica de la función de RR.HH. para acercarse de nuevo al negocio e introducir un nuevo modelo de gestión y de metodología en la captación y análisis predictivo de los datos de los empleados para mejorar y optimizar los procesos de recursos humanos.

Los empleados tienen la llave para el éxito de la transformación digital de las compañías y la función de HR Analytics debe decidir que datos personales o anonimizados de los empleados es prioritario recoger para su análisis y uso y tratamiento y por qué y como va a utilizar esa información para que se traduzca en conocimiento y permite tomar decisiones fundamentadas y que contribuyan al rendimiento y al desarrollo de negocio. HR Analytics en este nuevo escenario de actuación de la función de recursos humanos para la gestión de datos de los empleados y su optimización en los procesos de selección, contratación, desempeño, formación o desarrollo profesional y desvinculación supone la asunción de nuevas realidades frente a los mitos asumidos sobre esta nueva función en las compañías y también abre una nueva zona de riesgos jurídicos y económicos que es preciso conocer y gestionar con éxito que se pueden consultar en la siguiente figura.

MITOS	REALIDADES
1. HR ANALYTICS es una metodología para la gestión de datos de los empleados cuyo origen y fundamento está en la "matemática de datos" y uso de algoritmos con múltiples variables.	HR ANALYTICS es un modelo de gestión avanzada e inteligente de los datos de los empleados basado en la analítica predictiva para conocer mejor a los empleados y mejorar su rendimiento y el desarrollo de negocio y representa una oportunidad estratégica para volver a tener influencia desde RR.HH. en el negocio y que no se limita a un análisis estricto de variables matemáticas.

2. HR ANALYTICS tiene como reto la obtención del mayor número de datos de los empleados para generar información interna para el Departamento de RR.HH. que es normalmente anonimizada y procede siempre de fuentes internas.	HR ANALYTICS debe tener como reto identificar qué datos de los empleados (personales o no) son relevantes para su captación y para qué los va a utilizar con objeto de garantizar su aplicación práctica y permitir correlacionar los datos de negocio y los datos de las personas que puede estar anonimizada o no pero puede proceder de fuentes internas o externas.
3. HR ANALYTICS tiene que ver exclusivamente con el uso de los datos en la administración de nóminas y beneficios sociales de los empleados.	HR ANALYTICS tiene un uso potencial de los datos (personales o anonimizados) de los empleados mucho más amplio que alcanza a todos los procesos de RR.HH. (selección, contratación, formación, desempeño, retribución y desvinculación) y desde esa perspectiva es una evolución de la función tradicional de administración de personal.
4. HR ANALYTICS parte de conceptos tradicionales de RR.HH. (administración de personal, sistemas de información…) para que los datos disponibles sirvan en la toma de decisiones.	HR ANALYTICS incorpora conceptos nuevos de RR.HH. y de protección de datos ("*Big Data*", "*Cloud Computing*", "*Bring your own device*") que conlleva la necesidad en las empresas de contar con políticas corporativas de recogida, tratamiento y uso de los datos personales de los empleados y de análisis de los mismos y de posible expansión de esas políticas al ámbito de "*Big Data"*.
5. HR ANALYTICS es una herramienta de control de la prestación laboral que tiene su base jurídica en la libertad de empresa (art. 38 CE) y en el poder de dirección del empleador (art. 20.1 ET) para optimizar la productividad por lo que el poder de control sobre los datos de los empleados le corresponde a la empresa y con el único límite la privacidad de los empleados y/o los datos sensibles según normativa (datos de ideología, religión, afiliación sindical, origen racial, salud, orientación sexual, etc.).	HR ANALYTICS es una herramienta de adecuación y optimización de los procesos de recursos humanos y que permite la customización y personalización de las políticas de RR.HH. con los empleados y tiene como límites los derechos fundamentales de los trabajadores tanto en lo que se refiere a la libertad informática (art. 18.4 CE) como al derecho a la intimidad y al secreto de las comunicaciones (art. 18.1 CE) y las empresas deben respetar también el derecho fundamental de los empleados a la protección de datos que les da un poder de control sobre sus datos personales, su uso y su destino para impedir su trafico ilícito y lesivo contra su dignidad.
6. HR ANALYTICS tiene un poder casi absoluto sobre los datos de sus empleados sin que se precise establecer buenas prácticas en la gestión de los procesos de recursos humanos que utilizan los datos de los empleados.	HR ANALYTICS tiene un poder relativo sobre los datos de sus empleados que recoge deben de ser adecuados, pertinentes y no excesivos y su uso vinculado a las finalidades de su recogida y su tratamiento exige el consentimiento inequívoco del trabajador y el respecto de los derechos ARCO de acceso, rectificación, cancelación y oposición

	de los datos por parte de los empleados.
7. HR ANALYTICS está limitado a una dimensión interna relativa a los datos de los empleados y tiende a políticas generales para toda plantilla.	HR ANALYTICS tiene una importante dimensión externa en la gestión de los datos y en el uso y tratamiento de los mismos con terceros (sindicatos, clientes, etc.) que puede requerir importantes restricciones a la cesión de datos y a la transferencia de datos transfronterizos y tiende a políticas personalizadas que pongan el foco en la "experiencia del empleado".
8. HR ANALYTICS tiene una dependencia orgánica y funcional exclusiva del Dpto. de RR.HH.	HR ANALYTICS es una nueva función que, sin perjuicio de la dependencia orgánica del Dpto. de RR.HH., debe estar conectada con otros departamentos y funciones ("Chief Data Officer", "Compliace Officer", etc.)
9. HR ANALYTICS es una función basada exclusivamente en la tecnología para la captación de datos cuantitativos y / o numéricos y no precisa de protocolo empresarial de recogida, tratamiento y uso de los datos de los empleados.	HR ANALYTICS es un gran reto organizacional y funcional para la Dirección de RR.HH. cuya implantación tiene que ser gradual y en todo caso, debe garantizar la calidad de los datos y de los análisis basados en los mismos siendo muy recomendable contar con un protocolo empresarial de recogida, tratamiento y uso de los datos de los empleados que gestione los riesgos jurídicos de orden laboral.

CONCLUSIONES

1. El uso de HR ANALYTICS es una nueva realidad de gestión y de conocimiento con complejidad creciente que debe integrar los datos de los empleados y los datos de negocio para optimizar y mejorar los procesos y el negocio a partir de una análisis lógico y predictivo para anticipar el futuro.
2. La anticipación y planificación para la optimización del HR ANALYTICS es esencial para anticipar problemas jurídicos por lo que es muy recomendable la elaboración de una política corporativa que integre los aspectos laborales y los de protección de datos.
3. HR ANALYTICS ofrece una gran oportunidad para la gestión eficiente de los datos de los empleados y la toma de decisiones y constituye ya una ventaja competitiva.

Baker & McKenzie Madrid, S.L.P.

Paseo de la Castellana, 92
Madrid 28046
España

Tel: +34 91 230 4500

www.bakermckenzie.com