Credit scoring y consentimiento en la protección de datos

Carlos Alonso Martínez

Recientemente ha surgido la polémica de la regulación de los *scoring* en relación con las normas de protección de datos, planteándose la problemática de la necesidad de recabar el consentimiento del interesado para realizar estos tratamientos. El objeto de este artículo es realizar una primera aproximación al problema, para lo cual voy a exponer en qué consisten estos tratamientos, cuál es la postura de la Agencia de Protección de Datos, cuál es el marco regulador del consentimiento en la Ley Orgánica, para, por último, dar un primer criterio de evaluación.

EL RIESGO DE CRÉDITO Y LOS SISTEMAS AUTOMÁTICOS DE EVALUACIÓN

Los sistemas automáticos de evaluación –*credit scoring*– han permitido simplificar y objetivizar los sistemas tradicionales de análisis del riesgo de crédito basados en la experiencia profesional de las personas de una determinada entidad de crédito, a las que la organización confía la implantación de las políticas de riesgos y los niveles que la entidad esta dispuesta a asumir por riesgo de crédito. Se trata, por tanto, frente a una solicitud de riesgo determinada, de aplicar los conocimientos que el analista de riesgo tiene del prestatario, combinando factores objetivos y subjetivos. Los sistemas automáticos de evaluación son una herramienta de apoyo para el analista de riesgo, ya que en la mayor parte de los supuestos –podrían quedar fuera de este supuesto los créditos de bajo importe–, las entidades no han prescindido de que las decisiones finales de concesión estén sometidas a los analistas, sino que, por el contrario, han diseñado herramientas que permiten simplificar el trabajo de éstos, pero dejando la decisión final a su criterio. Es por esta causa por la que la mayoría de los *scoring* ofrecen resultados de aprobación, análisis experto y denegación, y cuando se producen las dos últimas circunstancias son sometidos a la decisión de un analista que emite un dictamen aplicando las políticas de concesión del crédito en la entidad.

Antes de comenzar a explicar el *credit scoring*, es conveniente poner de manifiesto qué se entiende por riesgo de crédito. Ramón Tamames y Santiago Gallego en su *Diccionario de economía y finanzas* definen el riesgo de crédito o riesgo crediticio como "*la probabilidad de que los intereses o el principal, o ambos, de un crédito no sean repagados*". Es por tanto una de las principales actividades de las entidades de crédito la valoración y asunción de riesgos, siendo así imprescindible conocer en todo momento el riesgo asumido, y el riesgo que están dispuestas a asumir, función que orgánicamente desempeñan los analistas de riesgos con apoyo de determinadas herramientas, como el denominado *credit scoring*. Como indica Carlas Cerdá en el manual *Herramientas de medición del riesgo de crédito*, la valoración del riesgo asumido o a asumir depende de múltiples factores, como son: el estado de la economía, la profesionalidad de las personas y de los equipos directivos responsables del estudio y concesión de operaciones, y el grado de dispersión de los riesgos asumidos.

Una vez realizada una aproximación al riesgo de crédito, es conveniente definir el *credit scoring*. Acudiendo nuevamente al *Diccionario de economía y finanzas* de Ramón Tamames y Santiago Gallego, estos autores definen el *credit scoring* como: "*Método de decisión, utilizado en banca y por las compañías de tarjeta de crédito, sobre el riesgo de solicitudes de crédito y tarjetas de particulares. Se basa en modelos matemáticos que operan en función de un conjunto de muestras*". Esta definición es completamente válida, en el sentido de que la esencia del *credit scoring* es,

tal como indican estos autores, la utilización de modelos matemáticos operando en función de unas muestras, si bien, a efectos del tema que se pretende analizar, conviene aclarar que actualmente no sólo se utiliza para concesión de operaciones, sino en todas las fases del ciclo del riesgo: concesión, seguimiento, recuperación, etcétera.

El *credit scoring* comporta una serie de ventajas frente a los sistemas tradicionales de evaluación de riesgos por los analistas:

- trata de realizar científicamente lo que el responsable de créditos hace por intuición, con la ventaja de que, utilizando procedimientos estadísticos modernos, se consideran global y simultáneamente todas las variables y datos del binomio operación-cliente;

- parte de los datos y experiencias del pasado para predecir, por medio de una puntuación de conjunto de la solicitud, si este crédito, una vez otorgado, resultará una pérdida o no para la entidad financiera.

En resumen, simplifica la realización de cálculos matemáticos complejos, que se producen en las dos fases de desarrollo de un *credit scoring*:

Primera fase. Aplicación de unos coeficientes de ponderación sobre las variables socioeconómicas, que permiten obtener una puntuación global de una solicitud.

Segunda fase. La puntuación global de la solicitud es traducida a una probabilidad de impago o probabilidad de morosidad. Esta probabilidad, comparada con los márgenes tolerables por la entidad financiera, determina el dictamen de la operación (conceder, rechazar, análisis manual, etcétera).

A fin de cumplir el objetivo de examinar la repercusión del *credit scoring* en la protección de datos, considero necesario realizar una aproximación a un desarrollo de un modelo automático de decisión. Las fases de desarrollo de un *credit scoring* son las siguientes:

1) Extracción de la información y auditoría.

2) Análisis de variables.

3) Análisis discriminante y determinación del poder estadístico del modelo matemático.

4) Calibración de la probabilidad de morosidad.

Primera fase. Extracción de la información

En esta fase se trata de definir la información histórica de operaciones de la entidad en la que se va a implantar el sistema automático de decisión, tratando de que la muestra contemple todo el ciclo de la vida de las operaciones de crédito, incidiendo de forma especial en el comportamiento de pago de éstas. La información se trata de forma disociada. Se intenta obtener una muestra del comportamiento histórico de las operaciones de una entidad con el mayor número de datos posible, es decir, con datos que se generaron en la concesión de la operación y posteriormente en su comportamiento. Esta muestra debe de ser suficiente basándonos en tres criterios fundamentales:

— Profundidad histórica o madurez.

— Cantidad de casos.

— Cantidad de variables.

Parte del éxito de esta fase consiste en realizar una auditoría de calidad de la información, si bien este dato es inocuo a efectos del presente análisis. Hay un elemento, por el contrario, que sí puede influir en el análisis posterior en cumplimiento de las normas de privacidad, y es que en esta primera fase se tienen en cuenta de forma disociada datos socioeconómicos del solicitante de la operación. Al seleccionar datos históricos de las operaciones sobre las que se van a analizar datos de su comportamiento de pago, se tienen en cuenta datos socioeconómicos como el estado civil, la edad, número de hijos, propiedad o no de la vivienda, junto a otros de vinculación con la entidad financiera, comportamiento de pago, etc. Lo que es importante reflejar es que este conjunto de datos, como he indicado en líneas anteriores, son datos disociados, cuyo concepto expondré en el apartado correspondiente a la evaluación en protección de datos.

Segunda fase. Análisis de las variables

En esta fase se trata de construir la variable dependiente (morosidad o no de una operación) y de preparar el conjunto de variables que actuarán como potenciales indicadores de la propensión o no a la morosidad. Pueden existir diversos tipos de variables. En esta línea, nos podemos encontrar variables categóricas (por ejemplo el estado civil) y variables continuas (por ejemplo la edad); adicionalmente, la combinación de variables puede dar lugar a nuevas variables (variables derivadas). Las continuas se transforman en nuevas variables categóricas (por ejemplo, distribuir la edad por tramos: hasta 25 años, hasta 40

años, etc.). A su vez, cada categoría de una variable queda convertida en una variable binaria, de forma que si generamos, a modo de ejemplo, cuatro categorías de edades, sólo una de ellas toma valor "uno", y el resto toman valor "cero" de cara al sistema de evaluación que estamos generando. En esta fase la información continua disociada.

Tercera fase. Análisis discriminante y determinación del poder estadístico

En la determinación de la función discriminante sobre la base de una muestra (por ejemplo, 2.000 operaciones con correcto funcionamiento de pago y 1.000 con morosidad), se trata de decidir cuáles son las mejores variables predictoras y sus coeficientes (edad entre 25 y 45, peso –0,140) mediante determinados métodos de selección. Una vez que se ha obtenido la función discriminante, se determina el poder estadístico, que es, en resumen, cuantificar la predecibilidad del modelo.

Cuarta fase. Medición de la probabilidad de mora de la operación

En esta fase, una vez determinado el modelo matemático que determina la puntuación global para una solicitud de crédito, se puede clasificar la cartera de riesgos bajo criterios de mayor o menos propensión a la morosidad. En esta fase entran en juego las políticas de concesión de crédito de la entidad, de forma que se trata de obtener una frontera de aprobación o denegación con base en la morosidad que una entidad esta dispuesta a asumir, siendo el objetivo determinar dónde se encuentra el punto de corte en términos de negocio, en función de la morosidad esperada o asumida.

El resultado de las cuatro fases anteriores es la obtención del algoritmo de evaluación automática.

En las líneas anteriores se define, de una forma muy básica, en qué consiste un *credit scoring*. Esta descripción se da únicamente a los efectos de poder evaluar cuál es la problemática actual de estos tratamientos en aplicación de la Ley Orgánica de Protección de Datos (a partir de ahora LOPD), por lo cual, asumiendo que se iba a realizar una descripción deficiente para un técnico en riesgos, he considerado necesario realizar esta extracción para tratar de situar el diagnóstico en protección de datos.

Antes de pasar a la descripción de problemática en protección de datos, conviene destacar la tendencia de las entidades a no generar un modelo de *scoring* para un determinado producto, sino a desarrollar varios en función de los mismos, y a realizar lo que se denominan sistemas automáticos de evaluación avanzados, en los que se integran diferentes *credit scorings* para alcanzar políticas de crédito conjuntas en el marco de una compañía. En el mundo anglosajón se conocen estas técnicas como APPS, que responde a la denominación de *application processing systems*.

LA OPINIÓN DE LA AGENCIA DE PROTECCIÓN DE DATOS

La Agencia de Protección de Datos se ha pronunciado recientemente sobre los *scoring*, hecho que ha ocasionado preocupación en determinados sectores de la actividad económica. El director de la Agencia de Protección de Datos, en su comparecencia ante el Congreso de los Diputados el 14 de diciembre de 2000 indicó: "*últimamente han aparecido técnicas que a mi modo de ver son un paso más de invasión a la intimidad como son el* scoring, *el* data mining *y el* data warehouse, *que ya permiten sacar perfiles del individuo, es decir, sabiendo lo que yo gasto en unos determinados bienes, sabiendo lo que gano, sabiendo a quién contribuyo, se pueden llegar a obtener perfiles del ciudadano. Esto es un paso más dentro de la intimidad de los ciudadanos, así tiene consideradas la Agencia estas prácticas. A no ser que estén expresamente consentidas por el ciudadano, están absolutamente prohibidas. Son prácticas graves porque son invasoras de la intimidad del ciudadano*", y posteriormente, después de referirse a la problemática general del sector bancario, finalizó este tema en la mencionada comparecencia ante el Congreso de los Diputados diciendo: "*Como ya he manifestado, todas esas prácticas de un paso más dentro de la intimidad, a mi modo de ver están absolutamente prohibidas, a no ser que exista consentimiento expreso del ciudadano, aunque en algunos supuestos hemos detectado que estas prácticas se están llevando a cabo sin consentimiento, no en el caso concreto de los bancos, sino en el caso concreto de compañías dedicadas a la telefonía móvil. Y por supuesto en esos casos hay varias resoluciones de la Agencia sancionando rigurosamente una práctica que, como digo, va más allá de la simple intimidad de los datos generales, si no es entrar ya a conocer incluso nuestros comportamientos*".

De estas líneas surge una parte de la problemática que en este trabajo analizo, y es el requerir el consentimiento expreso del interesado para estos tratamientos. Por tanto, y con carácter previo a la evaluación del problema, voy a tratar de sintetizar en

el apartado siguiente lo que implica el principio del consentimiento en protección de datos.

Con independencia del análisis a realizar, sí quiero dejar constancia respecto a la opinión de la Agencia de Protección de Datos que debe verse con cierta cautela de la comparecencia ante el Congreso de los Diputados, en tanto que del contexto en el que se produce se puede llegar a pensar que no se trata de una opinión de carácter general para todo *scoring*, sino para algún *scoring* concreto que planteara esa problemática.

CONSENTIMIENTO EN LA PROTECCIÓN DE DATOS. EXCEPCIONES AL CONSENTIMIENTO REVOCACIÓN DEL CONSENTIMIENTO

El principio del consentimiento se regula en el artículo 6 de la LOPD, al disponer que el tratamiento de datos de carácter personal requerirá el *consentimiento inequívoco* del afectado, salvo que la Ley disponga otra cosa, regulación que pone de manifiesto la necesidad de que el interesado deba prestar su consentimiento para cada uno de los tratamientos. Una vez otorgado el consentimiento, el interesado podrá revocarlo en cualquier momento, siempre que exista una causa justificada, y sin que tenga efectos retroactivos.

La Ley determina diversas formas para recabar el consentimiento, en función de los datos que se recogen, y refuerza el consentimiento en los casos en los que el tratamiento se refiera a datos especialmente protegidos. Con base en lo anterior, podemos realizar una primera clasificación, que ya he utilizado en anteriores trabajos y que, en función de los datos, ayude a determinar en cada momento cómo debe recabarse el consentimiento.

Consentimiento expreso (art. 7.3); sólo podrán ser tratados, recabados y cedidos siempre y cuando medie este consentimiento los datos que hagan referencia a origen racial, salud y vida sexual.

Consentimiento expreso y por escrito (art 7.2); sólo podrán ser objeto de tratamiento los datos que revelen ideología, afiliación sindical, religión y creencias.

Consentimiento para el resto de tratamientos; se le podría denominar "consentimiento general", y se utiliza en el resto de supuestos de la LOPD. Se entiende que no es necesario que sea consentimiento expreso, ni consentimiento expreso y por escrito, ya que esta regulación sólo comprende los denominados datos sensibles.

Siguiendo esta clasificación del consentimiento, vamos a exponer las excepciones al mismo:

Consentimiento general del artículo 6

No se requiere cuando lo disponga una Ley, cuando los datos se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias, cuando se refiera a las partes de un contrato o precontrato, de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento, cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Consentimiento expreso del artículo 7.3

Se exceptúa cuando lo disponga una Ley por razones de interés general; cuando resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento se realice por un profesional sanitario sujeto a secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto. Así mismo, cuando sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado este física o jurídicamente incapacitado para dar su consentimiento.

Consentimiento expreso y por escrito del artículo 7.2

Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros.

Un caso especial es la *excepción al consentimiento para la comunicación de datos del art. 11*; la comunicación de datos a un tercero para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario no requerirá el consentimiento del interesado cuando la cesión esté autorizada por Ley, se trate de datos recogidos de fuentes accesibles al público, el tratamiento responda

a la libre y legítima (siempre que se limite a la finalidad que la justifique) aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros, o la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los jueces y tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

Tampoco es necesario el consentimiento en el supuesto de que se produzca entre administraciones públicas y tenga por objeto el tratamiento con fines históricos, estadísticos o científicos; cuando la cesión de datos relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica, o cuando la comunicación se efectúe previo procedimiento de disociación.

Al margen de estas excepciones, conviene nuevamente resaltar que toda la regulación de protección de datos gira en torno al principio del consentimiento, en la medida en que es el titular de datos el que debe decidir en todo momento cuál es el tratamiento que admite para éstos, incluyendo en el concepto de tratamiento la cesión de los datos a un tercero.

La anterior afirmación no supone para el responsable del fichero que una vez ha recogido el consentimiento del interesado para el tratamiento cesen sus obligaciones respecto al dato, ya que tienen que cumplirse todos y cada uno de los principios de la LOPD, y a su vez el principio del consentimiento no puede interpretarse de forma aislada, sino en relación con el resto de principios, y muy especialmente con el de finalidad, principio por el cual todo tratamiento tiene una finalidad que es eje, junto al consentimiento, sobre el que giran el resto de los principios.

DIAGNÓSTICO DEL *SCORING* EN TÉRMINOS DE PROTECCIÓN DE DATOS Y RESPECTO AL PRINCIPIO DEL CONSENTIMIENTO

Una vez expuesta la aproximación al concepto de *scoring* y el planteamiento general del consentimiento en términos de protección de datos, voy a evaluar la opinión del director de la Agencia de Protección de Datos en la comparecencia ante el Congreso de los Diputados de 14 de diciembre de 2000, relativa a *scoring*, por su tenor literal, ya que, como he indicado anteriormente, es posible que la opinión no sea tan radical, y pueda tener algunos matices. A efectos de entrar en su diagnóstico, la postura literal se pueden resumir en:

— El *scoring* es un paso más de invasión de la intimidad, al permitir obtener perfiles del individuo.

— Estos perfiles se obtienen sabiendo lo que una persona gana, gasta en determinados bienes y a quién contribuye.

— Son prácticas prohibidas, salvo que expresamente estén consentidas por el ciudadano.

La primera crítica tiene que realizarse con carácter general, y debe ser frente a esa afirmación tan contundente que se dio ante el Congreso de los Diputados de que el *scoring* requiere el consentimiento expreso. En mi opinión, no todo *scoring,* conforme a la definición que hemos realizado, requiere el consentimiento, aunque algunos por evaluaciones que realicen, perfiles obtenidos, tipología de datos que se tengan en cuenta, etc., pueden requerir el consentimiento, e incluso en la línea expuesta por el director, algunos de ellos pueden requerir el consentimiento expreso.

Partiendo de lo anterior, vamos a analizar un supuesto teórico basado en la definición de *credit scoring* que hemos mantenido: "Método de decisión, utilizado en banca y por las compañías de tarjeta de crédito, sobre el riesgo de solicitudes de crédito y tarjetas de particulares. Se basa en modelos matemáticos que operan en función de un conjunto de muestras obtenidas de datos disociados. Con esta definición podemos llegar a tres elementos de análisis, que, a su vez, responden a un gran número de los sistemas implantados en la banca, éstos son:

1) El *scoring* se confecciona a partir de datos estadísticos.

2) Al *scoring* se le incorporan las políticas de crédito de una entidad.

3) El *scoring* facilita un dato de predicción de mora de una operación.

Respecto a la primera afirmación. Si el *scoring* se confecciona a partir de datos estadísticos, no se puede requerir el consentimiento del interesado en tanto que se considera únicamente dato de carácter personal cualquier información concerniente a personas físicas identificadas o identificables, (art. 3

apartado a) de la Ley orgánica de Protección de Datos), y la mencionada Ley sólo es de aplicación a los datos de carácter personal. En este sentido, se muestra también la regulación para la comunicación de datos que, en el apartado 6 del artículo 11, aparece regulada como una excepción al consentimiento, al indicar: "*Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores*". El procedimiento de disociación aparece definido en el apartado f) del artículo 3 de la LOPD, donde se encuentran las definiciones, y se define este procedimiento como "*todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable*". En consecuencia, si partimos de información disociada para confeccionar el *scoring*, en esta fase no debe existir ningún problema de protección de datos, ni, por descontado, requerir el consentimiento de aquellas personas que componen la base histórica de la entidad y cuyos datos disociados de la entidad van a componer el *scoring*.

Respecto a la segunda afirmación. Al *scoring* se le incorporan las políticas de crédito de una entidad. Nuevamente aquí no estamos ante ningún dato de carácter personal. Una entidad decide sus políticas de aprobación de riesgos con independencia de que el proceso se encuentre automatizado. Cuando se automatiza el proceso, se llevan estas políticas a la herramienta de evaluación. Cabría pensar si alguna de estas políticas fuera discriminante hacia el individuo o atacara frontalmente su intimidad. En la práctica, no será frecuente encontrar este tipo de supuestos, pero, en el caso de encontrarse, la consideración en términos de protección de datos no vendría por el tratamiento consistente en implantar sistemas de evaluación, sino por solicitar datos del interesado que pudieran calificarse como excesivos en función de la finalidad para la que son recabados: concesión o denegación de una operación con base en las políticas definidas.

Respecto a la tercera afirmación. El *scoring* facilita un dato de predicción de mora de una operación. El resultado del *scoring* no da una evaluación del perfil del individuo, ya que ofrece un resultado de la operación, aprobando o denegando ésta con base en la probabilidad de que esa operación supere los márgenes tolerados de mora por la entidad.

No obstante, pueden existir en el mercado sistemas automáticos de evaluación en cuyos resultados se dé una evaluación del individuo o la emisión de un perfil. En estos supuestos, sí coincido con el director de la Agencia de Protección de Datos en que el responsable del fichero debe recabar el consentimiento, o, en todo caso, encontrarse en disposición de acreditar estar inmerso en una causa de excepción a la recogida del consentimiento en los términos del artículo 6.2, y por supuesto recabar el consentimiento expreso de los interesados si estamos en algún supuesto encuadrable en el artículo 7 de la Ley Orgánica de Protección de Datos.

En consecuencia: ¿Dónde se encuentra la problemática de los sistemas de evaluación? He tratado en las líneas anteriores de acreditar que la herramienta de trabajo que implica un *scoring* no tiene per se un problema de protección de datos. En términos de protección de datos, lo que se debe evaluar es si los datos personales, ya sean pedidos directamente al interesado o en cualquier otro supuesto, que se recaban para una determinada finalidad –aprobar o denegar una operación de préstamo, determinar si el Banco le concede descubiertos en cuenta, etc.–, requieren, o no, del consentimiento del interesado, con independencia de que se utilice o no una herramienta automática de evaluación, y en este sentido:

Sólo requerirán el consentimiento expreso del interesado si los datos recabados son especialmente protegidos.

Sólo requieran el consentimiento siempre que no se encuentren en una de las excepciones del artículo 6.2, y, en estos casos, la excepción que previsiblemente se puede aplicar al mayor número de supuestos será la de referirse a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa, y sean necesarios para su mantenimiento o cumplimiento.

Por tanto, respecto a los datos recabados lo importante y definitivo es acreditar que no se han recabado datos sensibles, y que estos datos son necesarios para el mantenimiento o cumplimiento de la relación contractual o precontractual. En esta línea, cada sector de la actividad económica debe tener justificaciones a la "necesariedad" que pide el artículo 6.2 de la LOPD, y debe tenerse en cuenta, en este sentido, que tras la sentencia del Tribunal Constitucional de 30 de noviembre de 2000, cualquier excepción al consentimiento puede ser interpretada con carácter restrictivo.

Queda por analizar el supuesto de si, como resultado de los datos recabados, se llega a emitir una evaluación o un perfil del individuo. En este sentido, hay que tener en cuenta la reciente sentencia del Tribunal Supremo, que ha llegando a la conclusión de que las evaluaciones son un dato de carácter personal, y por tanto hay que evaluar si requieren el consentimiento y

qué tipo de consentimiento. Entiendo que nuevamente es plenamente aplicable lo expuesto en el párrafo anterior, si la finalidad de la obtención es necesaria para mantener o cumplir un contrato o precontrato, no requerirán el consentimiento.

En conclusión, mi opinión sobre si los sistemas automáticos de evaluación requieren el consentimiento expreso del interesado es:

— El *scoring* per se, en tanto que es una herramienta de trabajo, no requiere el consentimiento.

— La decisión de riesgo de una entidad, se utilice o no un *credit scoring*, sólo requiere el consentimiento expreso del interesado cuando se recaben datos sensibles o se obtengan nuevos datos consistentes en evaluaciones o perfiles del individuo derivadas de los mismos, o que en su resultado constituyan un dato especialmente protegido.

— La decisión de riesgo de una entidad, se utilice o no un *credit scoring*, sólo requiere el consentimiento del interesado si el responsable del fichero, en función de la finalidad, no puede acreditar encontrarse ante una de las excepciones del artículo 6.2 de la Ley Orgánica de Protección de Datos.

Por último, con base en los tres criterios anteriores, en mi opinión la postura del director de la Agencia de Protección de Datos en la comparecencia ante el Congreso de los Diputados debería ser matizada, y la evaluación en protección de datos no debe conducir a una respuesta general, sino al análisis individual de las políticas de la entidad para conceder el riesgo de crédito y, en su caso, de la herramienta de trabajo que se utiliza para esta finalidad, a la que en el mercado se la conoce como *credit scoring*.

RESUMEN

- El *scoring* es una mera herramienta, cuya finalidad básica es la realización de cálculos matemáticos complejos para la mente humana.

- El *scoring*, al ser una mera herramienta, no debe ser el problema en sí, ya que se limita a reflejar las políticas de riesgos de la entidad concreta donde se encuentra aplicado.

- En términos de protección de datos, no se debe dar una respuesta global para el *scoring*, ya que las conclusiones pueden ser diferentes en función de cómo se haya realizado su desarrollo, basado en las políticas de crédito.

- En determinados sectores de la actividad, los datos que se recaban pueden ser necesarios para el mantenimiento o control de la relación precontractual o contractual.

- El sector financiero, por sus normas específicas, puede acreditar esta "necesidad", aunque este extremo debe ser acreditable por cada entidad ante un hipotético requerimiento de la Agencia de Protección de Datos.

- Aquellos *scoring* que, en función de las políticas de concesión de riesgos de la entidad, no puedan acreditar la "necesidad" indicada requerirán el consentimiento del interesado.

- Sólo requerirán el consentimiento expreso aquellos *scoring* que, en función de las políticas de concesión de riesgos de la entidad, utilicen datos de carácter sensible, y que se encuentran definidos en el artículo 7 de la Ley Orgánica de Protección de Datos.