*R.I.T.I. nº 7 Mayo-Agosto 2018*

Revista Internacional TRANSPARENCIA E INTEGRIDAD

# LA ANALÍTICA DE LA CORRUPCIÓN (*)

***Ricard Martínez***
*Director de la Cátedra de Privacidad y Transformación digital*

**RESUMEN**

El uso de herramientas analíticas debería favorecer el desarrollo de metodologías de detección automatizada no sólo de los supuestos de administración ineficiente, o mala gestión sino también de corrupción. En organizaciones complejas las capacidades de control de las personas que desempeñan funciones control pueden verse fácilmente desbordadas. Las herramientas de *machine learning* e inteligencia artificial permiten establecer inferencias y correlaciones que escapan a la lógica usual. También multiplican de modo exponencial la capacidad de revisar grandes volúmenes de información. El Gobierno Valenciano ha realizado una apuesta tecnológica muy interesante legislando y desarrollando un sistema de esta naturaleza. Sin embargo, para el éxito de este tipo de iniciativas se requiere balancear la acción de la administración con el derecho a la vida privada. La protección de datos desde el diseño y por defecto y la evaluación de impacto relativa a la protección de datos prevista en el Reglamento General de Protección de Datos deben ser tenidas en cuenta.

**ABSTRACT**

The use of analytics should encourage the development of automated detection methodologies to verify cases of inefficient administration or mismanagement assumptions, but also of practices of corruption. The human capabilities to perform this controls can easily be overwhelmed. Machine learning and artificial intelligence tools allow us to establish inferences and correlations that are beyond the usual logic. They also exponentially multiply the ability to review large volumes of information. The Valencian Government proposes a very interesting technological commitment by legislating and developing a system of this nature. However, the success of such initiatives requires a balance between government action and the right to privacy. Data protection by design and by default and the data protection impact assessment provided for in the General Data Protection Regulation must be taken into account.

La analítica ofrece cada vez mayores recursos para el tratamiento de información de muy distinta naturaleza. Las posibilidades de alcanzar entornos estructurados y no estructurados de datos, las capacidades de aprendizaje autónomo para la identificación de patrones con técnicas de *machine learning* dirigido o no, y las oportunidades para la toma de decisión debían llegar al análisis de la gestión pública de uno u otro modo.

La contabilidad analítica, la evaluación de políticas públicas o el análisis del desempeño parecen un ambiente natural para la implementación de esta tecnología. El hacerlo para identificar indicios de mala administración o directamente de corrupción significa aceptar un reto de alto riesgo. El Anteproyecto de Ley, de la Generalitat, de Inspección General de Servicios y del Sistema de Alertas para la Prevención de Malas Prácticas en la Administración de la Generalitat y su Sector Público Instrumental, acepta el reto.[1]

[1] Disponible en http://www.transparencia.gva.es/anteproyecto-de-ley-o-proyectos-de-decreto-legislativo

En las próximas líneas se recoge la intervención en el Congreso sobre "Sistema de Alertas contra la Corrupción" organizado por Transparencia Internacional y la Generalitat Valenciana el 13 de noviembre de 2017. En este sentido carecen de la estructura de un artículo académico o informe técnico, pero pretenden conservar la viveza propia de una intervención oral.

Una norma de esta complejidad exige un análisis técnico lo más preciso posible. Uno de los retos para este tipo de normas consiste sencillamente en hacerlas evitando los problemas, discusiones e incluso excusas que después operan como barrera. Ahora es el momento de hacer un balance de intereses, en el que debemos huir de una de las falacias recurrentes en este ámbito consistente en el apriorismo de hacer prevalecer el derecho a la protección de datos. En nuestro país la privacidad fue siempre una gran barrera a la hora de investigar la información de carácter público en procesos de integridad o en procesos de lucha contra la corrupción. Todo era privado, todo era confidencial, y nada era accesible ni siquiera para parlamentarios en el ejercicio de la función de control.

Sin embargo, nuestra ponderación de intereses debería empezar en el artículo 1 de la Constitución. ¿Es posible el Estado de Derecho con corrupción? ¿Es posible un Estado Democrático con corrupción? ¿Es posible que funcione adecuadamente el Estado Social que necesita recursos con corrupción? ¿Es razonable entender que la corrupción detrae recursos al Estado Social? No parece posible concebir un Estado Democrático en el siglo XXI donde no existan mecanismos de control y participación de la acción política a disposición del ciudadano, no es compatible con un sistema donde la corrupción genera injusticia y desigualdad. Parece razonable pensar que cuando hablamos de sistemas de análisis, cuando hablamos de la lucha contra la corrupción, estamos inmersos en la defensa del núcleo esencial del Estado Social y Democrático de Derecho. Es necesario trascender las lecturas formalistas e intencionalmente políticas que instrumentalizan el Estado de Derecho y lo confunden con el principio de legalidad. Y esta relevancia sustancial obliga a un enfoque, no diré que sesgado, pero sí que tenga en cuenta estos valores.

Sin embargo, no puede desconocerse el impacto de la analítica de datos cuando la proyectamos sobre decenas cuando no centenares de sistemas de información relacionales o no relacionales. Y tampoco podemos tener una fe ciega en sus resultados. Todavía estamos aprendiendo de este tipo de herramientas en una fase incipiente de desarrollo. Las métricas aplicadas, los algoritmos, y los resultados exigen de una rigurosa verificación y confiabilidad.

Una ley, y su aplicación, no pueden arriesgarse al falso positivo, concepto que con buen criterio incorpora el proyecto. Y tampoco podemos obviar la directa relación que se producirá con la analítica de recursos humanos en el corto plazo. La analítica del desempeño, o la analítica de social media impactará sin duda a la hora de evaluar la conducta de los profesionales al servicio de determinadas empresas privadas. Si la pretensión de Big Data es el de ser una suerte de estadística del todo capaz de generar resultados relevantes y superar las capacidades del ser humano en la identificación de patrones muy pronto apreciaremos que los límites de la analítica de la corrupción desbordan el contenido de las bases de datos de gestión administrativa o contractual.

Bien pudiera ocurrir que las bases de datos, y los recursos de información externos a la administración pudieran aportar precisamente el elemento que engarza conductas e identifica patrones esenciales para prevenir la corrupción. Especialmente, cuando aquí se cumplirá con toda certeza una de las promesas de esta tecnología: uno sabe lo que busca, pero no lo que encuentra. Hay que estar dispuestos al patrón inesperado o al hallazgo casual.

El razonamiento de la máquina no va a coincidir con el humano en términos estrictos, ni desde la perspectiva de la lógica, ni desde la perspectiva de la rapidez en la obtención de resultados, y ni siquiera en los resultados en si mismos. Ello implica incorporar un cierto nivel de riesgo en la certeza de la información, de contraste entre la finalidad para la que se recabaron los datos e incluso respecto del tipo de nuevos datos que generan. A pesar de su riesgo epistemológico, cada vez hay que apuntar a la teoría de que este tipo de analítica convertirá datos aparentemente inocuos en datos particularmente sensibles. El concepto de sensibilidad de un dato ya no va a depender de su naturaleza, sino del entorno y el contexto en el que se obtiene este tipo de tratamientos.

Para los expertos en medicina poblacional el dato más estratégico, el más sensible es el código postal al que no teníamos por un dato particularmente íntimo. Ante este tipo de sensibilidad sobrevenida y contextual es necesario que adoptemos cautelas que garanticen un funcionamiento adecuado de un sistema como el que se pretende construir.

De la lectura del Anteproyecto lo primero que resulta interesante es la presencia de un embrión de cobertura de algo cercano al whistleblowing o sistemas de denuncias internas, que deberá alinearse en el tiempo con la filosofía que inspira la regulación de esta materia en el sector privado en el Proyecto de Ley Orgánica de reforma de la Ley Orgánica de protección de datos ahora en tramitación. Parece un buen momento para la coordinación interparlamentaria que permita introducir los sistemas de denuncias anónimas en el sector público en la nueva LOPD.

Un elemento que me resulta crucial del Anteproyecto valenciano, que tiene que ver con el ámbito material del mismo, son las metodologías de desarrollo. El marco general, el Reglamento General de Protección de Datos, debe servirnos de inspiración para incorporar dos principios nucleares: el análisis de riesgos y el de protección de datos desde el diseño y por defecto.

Revisado el conjunto de información complementaria asociada a la tramitación del proyecto normativo, y aunque no sea estrictamente obligatorio, parecería conveniente incluir un análisis de impacto en la protección de datos. Desgraciadamente las referencias a la protección de datos son sucintas en el informe de la DGTIC, y los informes de los letrados de la Generalitat únicamente se subraya la necesidad de cumplir con la legislación sobre protección de datos. Por tanto, sería tal vez interesante aprovechar la tramitación parlamentaria para de cierto detalle que nos asegurase que la norma, y el sistema que crea, funcionan perfectamente en este ámbito.

Tengamos en cuenta que el sistema se alimentará de múltiples bases de datos internas que se definen por la norma, y de bases de datos externas que contengan información relevante respecto de la actividad mercantil y financiera de contratistas, personas o entidades proveedoras. Algunas de las cuales sin duda podrían ser sujetos titulares del derecho a la protección de datos. Tengan en cuenta que, con algún leve matiz en el Anteproyecto de Ley de Reforma de la Ley Orgánica de Protección de Datos la exención a las personas físicas que operen como autónomos desaparece y se sustituye por el principio de interés legítimo.

Por otro lado, la normativa sectorial de privacidad y el propio Anteproyecto valenciano afectan tecnológicamente hablando al desarrollo de la aplicación. Puesto que éste ya está en marcha es de esperar que se habrán insertado las metodologías de protección de datos desde el diseño y por defecto, o de la evaluación de impacto si consideramos que existe algún tipo de riesgo. En ese sentido, si se atiende al tenor literal del artículo 45 del Reglamento General de Protección de Datos, cabe pensar que un sistema como el que estamos estudiando aquí, no presenta la necesidad una evaluación de impacto en la protección de datos. Aparentemente no se procesan categorías especiales de datos, ni se evalúa sistemáticamente personas físicas. Sin embargo, esta guía que cuenta con una metodología publicada por la Agencia Española de Protección de Datos, el Information Commissioner de Reino Unido y el Grupo de Trabajo del

Artículo 29, asegura adecuadas condiciones de cumplimiento normativo, de seguridad, de garantía de los derechos e incluso considera el impacto en la reputación. Desde esta perspectiva parece que fuera aconsejable emplearla.

Otra línea estratégica, es la relativa a la garantía de los derechos de los afectados. En sede de disposiciones adicionales se refiere el Proyecto a la vieja LOPD, es necesario apuntar también al Reglamento General de Protección de Datos, formal y materialmente. El último define el nuevo marco general, que la primera completa ejecutando en el ámbito nacional las habilitaciones que contiene el propio Reglamento. En este sentido, llama la atención una referencia el artículo 5.4 la LOPD. Éste se refiere al deber de información, ahora deber de transparencia, cuando los datos no los hemos obtenido del titular de los datos. Y la autorreferencia normativa interna induce a una confusión interpretativa que conviene corregir.

En otro orden de cosas, podemos enfrentarnos a datos especialmente protegidos los datos relacionados con infracciones administrativas o penales. Parece probable inferir que de los trabajos de la Agencia Anticorrupción y de la propia operativa de los tribunales pueda obtenerse información relevante relacionada por ejemplo con antecedentes penales o algún tipo de inhabilitación. Tratar estos datos puede exigir contar con una habilitación legal expresa. Y lo mismo sucede con su comunicación, ya que hoy el artículo 11.2 de la LOPD únicamente se refiere a Ministerio Fiscal, jueces y tribunales, sindicaturas de cuentas y defensorías del pueblo.

En los demás casos la especialidad regulatoria se encuentra en el artículo 21LOPD condenado a desaparecer. Además, es necesario tener en cuenta que en aplicación del criterio del Tribunal Constitucional a las excepciones al deber de información en la recogida de datos deben pensarse con especial cuidado, aunque la regulación europea ofrezca seguramente mayores posibilidades de acción. En este sentido, considera que cuando existan objetivos importantes de interés público general de la Unión o de un Estado miembro se pueden establecer estas excepciones.

Por tanto, no tenemos un problema, ni de legalidad, ni de coherencia con el reglamento, ni de constitucionalidad. Es necesario abordar así de modo estratégico las excepciones a los derechos inspirándonos en leyes preexistentes como por ejemplo las vigentes en materia de prevención del blanqueo de capitales y financiación del terrorismo, que han sido muy precisas a la hora de salvar este tipo de problemas. Y esta recomendación de regular con precisión deriva de que al preverse esta materia en el artículo 23 del Reglamento, el párrafo segundo, establece cuáles son las condiciones exactas de la regulación y creo que tendremos que asegurarnos de cumplir con todas ellas. La previsibilidad es aquí una garantía de los derechos fundamentales ya que eliminamos una expectativa de privacidad. Y como ya viene sucediendo en el ámbito de las relaciones laborales, el caso de la STEDH Barbulescu es paradigmático, puede que la indagación en los sistemas propios afecte a la expectativa de privacidad de los trabajadores de la Administración valenciana. Si se elimina cualquier tipo de duda nuestra capacidad de acción en esta materia se multiplicará exponencialmente y lo mismo sucederá en el caso de personas físicas que operen en el tráfico como autónomos o profesionales.

Adicionalmente hay que considerar todas estas cuestiones desde la perspectiva de los derechos del investigado. Va a ser sometido a actuaciones inspectoras, con pleno ejercicio de la autoridad pública, incluso se plantea la posibilidad de recabar el soporte de terceros e intuyo que esos terceros pueden ser incluso las Fuerzas y Cuerpos de Seguridad bajo ciertas condiciones. De esta manera el investigado se somete a las posibilidades del universo *Big Data*, a lo que la norma define como un falso positivo que incluso podríamos detectar finalizada la investigación. Por ello, las salvaguardas para la persona investigada son muy relevantes ya que esa persona, puede que no tenga comprometida la privacidad y la protección de datos personal, pero si su honor

profesional y su imagen pública. Hay que ser capaces de monitorizar permanentemente el algoritmo y como funciona.

Por último, preocupa que si bien al denunciante se le garantiza la máxima confidencialidad no será un denunciante anónimo. Cabe dar a conocer los datos personales de la persona denunciante cuando sea absolutamente imprescindible para que la persona denunciada pueda ejercer su derecho de defensa en un procedimiento. Si además el artículo 31 considera infracción muy grave las denuncias o comunicaciones de irregularidades manifiestamente falsas cuando causen graves perjuicios la persona denunciada, en la práctica no será un sistema de denuncias anónimas. Y esto operará como elemento disuasorio respecto al denunciante

Y permitan una recomendación final de tipo gremial: apuesten por el delegado de protección de datos. El nivel de complejidad que estamos desarrollando en el ámbito de la transparencia y del control de la corrupción hace que la figura del delegado de protección de datos vaya a ser estratégica.

De algún modo, la recomendación global que deriva de este análisis reside en la necesidad de concebir la protección de datos como problema, no hay que esperar que esto sea así hay que salir al paso y atajar cualquier dificultad desde una regulación basada en el interés público y el principio de proporcionalidad.

(*) La presentación del contenido de este artículo ha recibido financiación a través de la convocatoria pública de la Generalitat Valenciana (DOGV 8064, de 16-6-2017) relativa al Sistema de alertas rápidas en la lucha contra la corrupción.