Autoridades europeas de protección de datos: clave de salvaguarda de la privacidad

Francisco Javier Carbayo

Noemí Brito Izquierdo

Miembros del Comité Operativo del Data Privacy Institute (ISMS Forum Spain)

La ciudadanía y las empresas, por lo general, suelen tener la falsa percepción de que las funciones y competencias de las autoridades de control en materia de protección de datos se circunscriben a procesos sancionadores y a la imposición de multas. Sin embargo, la primera y principal misión de estas autoridades es la de velar por el cumplimiento de la legislación sobre protección de datos, más allá de la mera sanción en caso de incumplimiento, lo que supone la existencia y el ejercicio de otras tantas e importantes funciones en materia de información, concienciación, atención al responsable de tratamiento y al ciudadano, etc.

Y no es fácil para estas autoridades convencer de que la privacidad no es una "moda pasajera", sino algo consustancial al desarrollo mismo de lo digital, donde el ciudadano se erige en protagonista respecto a la protección de sus propios derechos.

Asimismo, el actual contexto mundial, los constantes flujos globales de información, así como los últimos y lamentables incidentes terroristas, implican nuevos desafíos para la protección de la privacidad por parte de tales autoridades, las cuales están abocadas a adoptar un renovado papel en la sociedad, quizás mucho más activo si cabe, aunque siempre en coherencia y en difícil equilibrio, con otros tantos derechos e intereses igualmente protegibles.

En este ámbito, la reciente sentencia del Tribunal de Justicia de la Unión Europea (TJUE), de 6 de octubre (http://curia.europa.eu/juris/documents.jsf?num=C-362/14), más conocida por anular la Decisión de la Comisión Europea por la que se declaraba que Estados Unidos garantizaba un nivel de protección adecuado de los datos personales transferidos *(Safe Harbor)*, destaca por valorizar las competencias de dichas autoridades al declarar que éstas deben ser ejercidas con total independencia, si que deban quedar cercenadas en modo alguno por las Decisiones de la Comisión Europea.

Esto supone un importante espaldarazo a las autoridades de control, que deben aprovecharlo para impulsar su actuación, haciendo cada vez más partícipes en tales procesos a ciudadanos, empresas y profesionales, y reforzando la coordinación y cooperación entre las mismas, tal y como apunta el próximo Reglamento Europeo de Protección de Datos.

En este sentido, podría ser posible una aproximación a las actuales competencias, funciones y tareas de las autoridades de control en protección de datos basada en la habitual configuración por círculos concéntricos: ámbito local, ámbito europeo y ámbito global.

Por supuesto, no es una configuración perfecta, sino más bien susceptible de varios y diversos matices, entre otros los que pudieran venir por las diferentes materias en que hay que dividir la protección de datos, por los *stakeholders* implicados, por la situación de reconocimiento y la madurez de cada autoridad, por la propia capacidad financiera de cada una ellas, etcétera.

Elementos básicos

Sin duda, un número significativo de variables, que inducen más a un formato de gráfico radial. Pero antes de llegar ahí, pasemos por la proposición de los elementos básicos de cada uno de los círculos, en concreto:

- Ámbito local: no debemos olvidar que, a día de hoy, la normativa de protección de datos es, dentro de la Unión Europea, homogénea sólo de facto (o en todo caso no tan homogénea como se le habría de suponer) y heterogénea en la práctica.

La reacción de diferentes autoridades de protección de datos ante la sentencia europea sobre 'Safe Harbor' pone de manifiesto la diversidad y diversificación en esta materia

Es decir, tenemos (todavía) un marco de base constituido por la Directiva 95/46/CE, como argumento para la homogeneidad; pero tenemos una realidad de cuestiones diferenciales y diferenciadoras en la trasposición a cada país, diferentes países con diferentes momentos de incorporación a la UE, países con diferentes sensibilidades en protección de datos, diferentes regímenes sancionadores en cada país, diferentes capacidades prácticas y grados de intensidad en la aplicación de tales regímenes sancionadores, diferentes factores políticos, económicos, etcétera, que de manera coyuntural varían la situación en algunos países... En definitiva, supuestamente la misma receta, pero diferente plato sobre la mesa, en realidad.

La reacción de diferentes autoridades ante la sentencia TJCE sobre *Safe Harbor* mencionada, pone de manifiesto la diversidad y diversificación. Porque, aunque parezca que todas las autoridades han reaccionado en el sentido de "bueno, pues cláusulas-tipo si no se puede ir por alguna de las otras vías, ¿no?", como siempre el diablo está en los detalles, y éstos nos dicen que la situación puede no ser tan simple (que no simplista).

No obstante, en ese ámbito local, de manera general y al menos en ciertos casos de todos conocidos, entre los que se encuentra nuestra Agencia Española de Protección de Datos, las autoridades nacionales de protección de datos han contribuido de manera principal y esencial a que la protección de datos haya alcanzado el crecimiento, lugar e importancia que ahora tiene (y esto, en el fondo, no ha hecho más que empezar). Esa labor antes pionera y ahora de liderazgo debería ser una constante, más allá de configuraciones jurídicas concretas.

- Ámbito europeo: en los días en que nos encontramos no hay charla, evento, mentidero, etcétera, sobre protección de datos que no hable de la llegada de aquello que ya se divisa en el horizonte, el Reglamento Europeo de Protección de Datos. Y, sin duda, uno de los temas que genera más dudas y curiosidades es la configuración que se va a proponer de las autoridades nacionales de protección de datos.

  La primera cuestión no por obvia hay que evitarla: ¿existirán las autoridades nacionales tras el Reglamento? Parece que no hay duda de que sí, como no podía ser de otra manera. ¿Seguirán tal y como los conocemos? Parece que no, en el sentido de que el impacto del Reglamento en la regulación de la protección de datos y la privacidad requiere de unas autoridades nacionales adecuadas a la nueva realidad que viene. Sin lugar a dudas, el Reglamento quiere autoridades reales, independientes en todos los sentidos, y activas.

  Pero, al mismo tiempo, la opción por el modelo de *one-stop-shop* puede acarrear serias dificultades para una coordinación entre autoridades en términos de igualdad y cordialidad, al tiempo que la aproximación de cada autoridad a la determinación de las sanciones puede conllevar grandes y graves diferenciaciones que distorsionen el modelo de regulación única que promueve el Reglamento.
- Ámbito global: por una u otra causa (globalización económica, redes sociales que se usan en cualquier país y por cualquier persona del mundo, comunicaciones con capacidad gigantesca y creciente de transportar información en tiempos menguantes, etc.), la privacidad es una materia globalizada.

  Para muestra un par de ejemplos. El primero, un artículo de un medio asiático sobre el incremento de poderes que podría conllevar el acuerdo UE-USA sobre *Safe Harbor 2.0*, (ver http://www.channelnewsasia.com/news/business/international/eu-wants-to-give-national/2300616.html). ¿Por qué es importante esta noticia para un medio asiático? Quizá porque el "APEC Cross-Border Privacy Rules (CBPR) system" puede verse afectado o, al menos, influenciado. Quizá porque la privacidad ha llegado hasta la negociación del Acuerdo de Libre Comercio entre la UE y Estados Unidos, siendo que el Acuerdo de Libre Comercio entre Estados Unidos y Asia ya existe.

  El segundo, una pregunta realizada en el contexto del World Economic Forum, de gran vigencia y plena actualidad en estos días: *"Can you have both security and privacy in the internet age?"* –¿Se puede tener seguridad y privacidad a la vez en la era de Internet?– (ver https://agenda.weforum.org/2015/07/can-you-have-both-security-and-privacy-in-the-internet-age/).

En definitiva, más que nunca, las autoridades de protección de datos deberían tomar muy en consideración ese "viejo" aforismo de Internet de "actúa local, piensa global". Las necesidades en protección de datos y privacidad son crecientes en volumen e importancia, así como acuciantes y urgentes en algunos casos. Las autoridades de protección de datos han sido, son y seguramente sigan siendo pieza clave, motor y lubricante del engranaje de protección y cumplimiento. ■