
Autoridades independientes de control, cooperación, mecanismo de coherencia y Comité Europeo de Protección de Datos

PID_00250224

Antoni Roig

Tiempo mínimo de dedicación recomendado: 2 horas



Antoni Roig

Índice

1. Autoridades independientes de control.....	5
2. Cooperación.....	13
3. Mecanismo de coherencia.....	16
4. El Comité Europeo de Protección de Datos.....	19
Bibliografía.....	23

1. Autoridades independientes de control

1) Características generales

Aunque el Reglamento general de protección de datos introduce el principio de responsabilidad activa (*accountability*), esto no significa que las agencias de protección de datos dejen de tener un papel destacado en la protección de datos¹. El art. 51 RGPD ha afirmado la importancia de las autoridades de control, y prevé que cada Estado miembro encomendará a una o varias autoridades de control –por ejemplo, una agencia de protección de datos– la tarea de supervisar el cumplimiento del RGPD². La importancia de las autoridades de control ha sido también afirmada por la doctrina: «las leyes no se aplican solas y la cultura de la privacidad no puede establecerse eficazmente sin una autoridad reconocible» (Bennet y Raab, 2006; la traducción es nuestra). Las razones esgrimidas para la existencia de autoridades de protección de datos parecen, al menos, seis: la necesidad de armonización de prácticas existentes, la necesidad de ofrecer protección efectiva a los ciudadanos, el conocimiento experto requerido para la supervisión, la necesidad de control sobre los actores privados –pero también sobre los Gobiernos–, la necesidad de independencia política y, finalmente, su flexibilidad a la hora de decidir si conviene investigar o cómo cooperar con otras autoridades de control³ (Hijmans, 2016).

Lecturas complementarias

H. Hijmans (2016). *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFUE*. Berlín: Springer.

P. Craig; G. de Búrca (eds.) (2011). *The evolution of EU law* (2.ª ed.). Oxford: Oxford University Press.

La diferencia con la Directiva reside, entre otros puntos que iremos destacando, en la cooperación acentuada entre autoridades de control⁴. En el caso de tener más de una autoridad de control, el Estado designará una autoridad de control que las represente en el Comité, y asegurará el cumplimiento de las normas adoptadas, de acuerdo con el mecanismo de coherencia (art. 63 RGPD) que veremos más adelante. Se informará a la Comisión de cualquier disposición legal nacional que desarrolle estos aspectos⁵.

⁽¹⁾El Tribunal de Justicia de la Unión Europea los considera los guardianes de la protección de datos (caso C-518/07, Comisión contra Alemania). Se trataría del mantenimiento del modelo continental de protección de datos, según A. Troncoso (2016, págs. 461-512). La regulación de la figura de las autoridades de control independientes es detallada (arts. 51-59 RGPD).

⁽²⁾También veremos que se ha conservado la figura del supervisor europeo de protección de datos, que el Tratado de Ámsterdam de 1997 introdujo en el art. 286 TCE, y se completó con el Reglamento CE 45/2001, de 18 de diciembre del 2000, sobre la protección de los individuos con relación al tratamiento de datos por parte de las instituciones de la Comunidad y sus órganos y sobre el libre movimiento de tales datos.

⁽³⁾De hecho, parece que existe la necesidad de no perder sino, al contrario, ampliar los métodos de control en un momento en el que se pierde el control sobre la información. Podéis ver, al respecto, Craig y de Búrca (2011).

⁽⁴⁾Sobre el origen histórico de las primeras autoridades de protección de datos europeas, así como la evolución posterior, véase González (2014).

⁽⁵⁾Puede verse, al respecto, el título VI de la APLOPD, autoridades de protección de datos, arts. 45-63.

Las autoridades de control actuarán con independencia en el ejercicio de sus funciones⁶. De hecho, su independencia no proviene de ninguna delegación del poder ejecutivo, sino directamente de los tratados, y esto les confiere un estatus constitucional⁷. El estatuto de las autoridades de control es singular en el Derecho europeo: son autoridades públicas independientes y reconocidas en el Derecho originario, a diferencia de la delegación de competencias atribuida a las agencias europeas. Las autoridades de protección de datos no son, así, agentes de ninguna autoridad principal⁸. Más bien, parecen formar parte, de alguna manera, de la Administración europea (Hijmans, 2016). Pues bien, los miembros de cada autoridad de control no deben recibir ninguna orden ni instrucción externa, ya sea de los estados o de las instituciones europeas: el poder de decisión debe ser libre (Balthasar, 2013; véase también art. 130 TFUE). El Tribunal de Justicia de la Unión Europea (TJUE) exige unos requisitos importantes a la hora de reconocer la independencia⁹. Dependiendo de cómo se interpreten en el futuro, podrían incluso llegar a ser más estrictos que los requisitos para ser un órgano jurisdiccional¹⁰. Esto se debe a que la autoridad de control no solo tiene encomendadas tareas de supervisión de actores privados en el mercado europeo, sino también de instituciones europeas y de gobiernos nacionales. En todo caso, la independencia no es un estatuto especial o formal, sino una libertad a la hora de tomar las decisiones. Una reflexión final: la tendencia creciente a reforzar la responsabilidad activa puede suponer una dificultad añadida a la necesidad de preservar la independencia de los órganos de control. Cuando menos, deberán reconciliarse las dos perspectivas¹¹. La relación entre independencia y responsabilidad política ya ha sido abordada por el TJUE¹².

⁽¹¹⁾Hijmans sugiere que las autoridades de control deberían responder ante los parlamentos y ante los órganos jurisdiccionales. Véase Hijmans (2016, pág. 383 y sec. 7.9).

⁽¹²⁾C-614/10, Comisión contra Austria.

Lecturas recomendadas

A. Balthasar (2013). «“Complete Independence” of national data protection supervisory authorities». *Utrecht Law Review* (vol. 9, núm. 3, págs. 26-38).

M. Everson; M. Cosimo; E. Vos (eds.) (2014). *EU agencies in between Institutions and Member States*. Nueva York / Alphen aan den Rijn, Países Bajos: Kluwer Law International.

E. Chiti (2014). «An important part of the EU's institutional machinery: Features, problems and perspectives of European agencies». *Common Market Law Review* (núm. 46, págs. 1395-1442).

Otro aspecto relevante, al respecto, es que los miembros de la autoridad de control no podrán ejercer ninguna actividad profesional, remunerada o no, que sea incompatible con las funciones que se les encomiendan. Cada Estado miembro, además, deberá garantizar la autonomía financiera, técnica y la suficiencia de recursos humanos e infraestructuras para el cumplimiento efectivo de las funciones encomendadas a las autoridades de control¹³. La Comisión no ha llevado a ningún Estado miembro hasta el TJUE por no atribuir suficientes poderes a una autoridad de control, aunque el TJUE ha reconocido que la au-

⁽⁶⁾La importancia de un control independiente para la defensa de los derechos de los individuos ya se encuentra en el considerando 62 de la Directiva 95/46/CE, así como en el preámbulo del protocolo adicional a la Convención para la protección de los individuos en relación con el tratamiento automatizado de datos personales. También el considerando 117 del RGPD señala la importancia de esta independencia.

⁽⁷⁾Así, el art. 16.2 del TFUE prevé este control por parte de autoridades independientes. Puede verse también el art. 8.3 de la Carta de Derechos Fundamentales y el art. 39 TUE.

⁽⁸⁾La metáfora de los agentes se usa, en cambio, en relación con las agencias europeas. Sobre estas últimas, podéis ver Everson, Cosimo y Vos (2014).

⁽⁹⁾Caso C-518/07, Comisión contra Alemania, C-614/10, Comisión contra Austria y C-288/12, Comisión contra Hungría.

⁽¹⁰⁾En efecto, la independencia contemplada en el art. 267 TFUE no es tan estricta como la que el TJUE predica de las autoridades de control. Podéis ver, al respecto, TJUE, caso C-54/96, *Dorch Consult Ingenieursgesellschaft*. Pese a todo, hay muchos puntos de contacto con la independencia de las autoridades de control frente al Ejecutivo: caso C-53/03, *Syfait* y otros. Quizá la menor independencia se da en las agencias europeas, ya que son parte de la Administración y los gobiernos participan en sus comités directivos. Al respecto, véase Chiti (2014).

⁽¹³⁾La falta de efectividad de las autoridades de control por insuficiencia de recursos ha sido defendida en Bamberger y Mulligan (2013). Puede verse también el *Deliverable 1* a cargo de Barnard-Wills y Wright (2105).

⁽¹⁴⁾TJUE, casos acumulados C-293/12 y C-594/12, *Digital Rights Ireland* y *Seitlinger*, respectivamente, y caso C-362/14, *Schrems*.

sencia de poderes de intervención es un problema cuando el tratamiento tiene lugar fuera de la Unión Europea¹⁴. Las autoridades de control podrán tener personal propio. Podrá hacerse un control financiero sin que esto afecte a la independencia de la autoridad de control, que dispondrá de un presupuesto anual público.

El director o presidente de la AEPD será nombrado por el Gobierno, a propuesta del ministro de Justicia (art. 49.2 APLOPD). El Gobierno pondrá en conocimiento del Congreso de los Diputados el nombre del candidato, para que se emita un dictamen sobre su idoneidad. Se requiere que los miembros de la autoridad de control tengan una titulación o experiencia necesaria, en particular, en el ámbito de la protección de datos, para ejercer sus funciones (art. 53 RGPD). Otra garantía formal de independencia es la existencia de una duración mínima de mandato¹⁵. Además, se establece una garantía de inamovilidad: solo podrá destituirse a un miembro de la autoridad de control en caso de conducta irregular o falta de cumplimiento de las funciones encargadas (art. 53.4 RGPD). Por consiguiente, una vez fijado el mandato, no puede existir terminación anticipada, salvo en estos casos excepcionales. Las normas de establecimiento, procedimientos y régimen jurídico de la autoridad de control se adoptarán en una ley. De acuerdo con el art. 50 APLOPD, el presidente de la AEPD estará asesorado por un consejo consultivo. Un estatuto orgánico desarrollará su régimen jurídico. Los miembros de la autoridad de control y el personal propio tendrán el deber de secreto profesional, tanto durante el mandato como después, sobre las informaciones confidenciales que hayan conocido durante el ejercicio de sus funciones¹⁶. Quedará protegida, en este sentido, toda la información recibida de personas en relación con infracciones del RGPD.

⁽¹⁵⁾El mandato tendrá una duración de cinco años, renovable una vez (art. 49.3 APLOPD).

⁽¹⁶⁾Se ha criticado la regulación conjunta de las obligaciones de los miembros de la autoridad de control y del personal, pues genera confusión con normas pensadas para el cese en el empleo aparentemente aplicables a los miembros, y al revés con normas de incompatibilidades durante y después del mandato, aparentemente, también aplicables al personal (Troncoso, 2016, pág. 481).

2) Identificación de la autoridad de control principal y el mecanismo *one-stop shop*

El WP29 ha adoptado una guía para identificar a la autoridad de control principal en supuestos de tratamientos de datos transfronterizos¹⁷. Estos tienen lugar, de acuerdo con el art. 4, 23 RGPD, cuando los establecimientos del responsable o encargado se encuentran en más de un Estado miembro, o bien cuando el responsable o encargado se encuentra establecido en un solo Estado miembro pero, en cambio, el tratamiento afecta de manera sustancial a datos de interesados de más de un Estado miembro. La afectación sustancial se determinará caso por caso, pero se avanzan algunos criterios generales en la guía del WP29:

- Puede producir perjuicios o pérdidas a interesados.
- Puede limitar derechos o provocar pérdida de oportunidades.
- Puede afectar a la salud o al bienestar.
- Puede afectar a la situación económica del interesado.
- Puede producir discriminación.
- Incluye categorías especiales de datos, o de menores.

⁽¹⁷⁾WP29, *Guidelines for identifying a controller or processor's lead supervisory authority*, adoptado inicialmente el 13 de diciembre del 2016, revisado y adoptado de nuevo el 5 de abril del 2017, WP 244 rev. 01.

- Puede provocar cambios significativos en el comportamiento de los interesados.
- Tiene consecuencias imprevisibles o no deseadas.
- Puede dañar la reputación del interesado.
- Incluye el tratamiento de gran cantidad de datos personales.

Este test de «afectación sustancial» es importante, pues las autoridades de control solo deberán colaborar de acuerdo con el mecanismo de coherencia que veremos a continuación, cuando se adopten medidas que produzcan efectos legales sobre tratamientos que afecten a un número significativo de interesados. La autoridad de control principal será la que tendrá la responsabilidad central en el caso de reclamaciones contra tratamientos transfronterizos. Así, coordinará la investigación con las demás autoridades de control interesadas, como veremos. El criterio para identificar a la autoridad de control principal viene establecido en el art. 56 RGPD: se tratará de la autoridad de supervisión del establecimiento principal o del único establecimiento. De acuerdo con el art. 4(16) RGPD, el establecimiento principal del responsable será la sede de Administración central, a menos que las decisiones sobre la finalidad y los medios del tratamiento se adopten en otro establecimiento del responsable. El establecimiento principal del encargado, por su parte, será el establecimiento de la Administración central en la Unión Europea o, al menos, en el cual se desarrollen las actividades de tratamiento principal.

El RGPD pretende que sea una única autoridad de control la competente en los tratamientos transfronterizos. Pese a todo, cuando un responsable tiene una sede que toma de manera autónoma a la sede central decisiones sobre la finalidad y los medios del tratamiento, se requiere identificar con precisión dónde se toman las decisiones. La guía del 2016 del WP29, antes mencionada, nos ofrece unos ejemplos ilustrativos. Así, un banco puede tener su cuartel general en Frankfurt, de manera que todas las actividades de tratamiento de datos personales para la actividad bancaria se llevan a cabo de acuerdo con decisiones tomadas en la sede central. Sin embargo, puede que el departamento central de seguros esté en Viena, de modo que esta segunda sede decide autónomamente sobre el tratamiento necesario para la actividad de seguros. Por consiguiente, la autoridad de control austríaca sería principal en lo concerniente a las transferencias de datos personales para finalidades aseguradoras, mientras que la autoridad de control alemana sería principal para el tratamiento de los datos con fines bancarios, y esto de manera independiente de los interesados.

En los casos en los que no exista una sede administrativa central, se atenderá a elementos fácticos: ¿dónde se toma la decisión final?; ¿dónde se encuentran los que toman tal decisión?; ¿dónde se encuentra registrado el responsable? En todo caso, sería deseable que el propio grupo empresarial fijara cuál es su sede administrativa central, a efectos de dirigirse a la autoridad de control principal correspondiente. Ahora bien, no se permite el *forum shopping* y, por tanto, la supuesta sede central debe tener el poder final de decisión pues, en otro caso, se

atenderá a este elemento de hecho. Las autoridades de control deberán llegar a un acuerdo o, en último caso, el Comité decidirá qué autoridad es principal en el supuesto discutido.

En cuanto a las autoridades de control interesadas, se encuentran en el Estado miembro del responsable o del encargado, o bien de los interesados sustancialmente afectados por el tratamiento o que les ha sido dirigida una reclamación al respecto (art. 4.22 RGPD). Su papel queda entonces supeditado a la propuesta de decisión de la autoridad de control principal, como veremos. Puede suceder, sin embargo, que una autoridad principal decline su responsabilidad en favor de una autoridad interesada. Por ejemplo, este sería el caso de una empresa multinacional, con sede central en Luxemburgo, que lanza un producto cuyos interesados se encuentran en Bélgica. En este supuesto, las autoridades de los dos países pueden acordar que la autoridad belga sea finalmente la que ejerza las responsabilidades de autoridad principal.

Para resumir, una vez que se ha determinado que el responsable o controlador establecido en un Estado miembro lleva a cabo un tratamiento de datos transfronterizo, ya sabemos que la autoridad principal es la del país donde se encuentra la sede central. Si existen varios establecimientos, pero solo hay un responsable, entonces el lugar del responsable indica la Administración central, a menos que se tomen decisiones autónomas sobre la finalidad y los medios en otra sede. Si hay un responsable y un encargado de varios estados miembros, la autoridad principal corresponde a la del país del responsable, y la del encargado es autoridad interesada. Pueden ser autoridades interesadas las que tengan en su territorio a un responsable o un encargado, las de los interesados significativamente afectados, o las que reciban una reclamación al respecto.

3) Funciones de la autoridad de control

Se suele mencionar el cumplimiento de la legalidad y la atribución de competencias claras con los primeros principios del buen gobierno (Ottow, 2015; OCDE, 2014). Quizá el anterior marco legal del art. 16.2 TFEU y del art. 8.3 de la Carta de Derechos Fundamentales no era muy preciso, pues no se mencionaban concretamente cuáles eran las reglas que se debían hacer cumplir. Además, el control del cumplimiento parecía limitarse a la imposición, sin tener en cuenta otras competencias, como las consultivas. El TJUE parece haber ayudado a ampliar las competencias, al menos del supervisor europeo, ya que le ha reconocido la facultad de personarse ante el mismo, por razones de eficacia en la aplicación del antiguo art. 286 TCE¹⁸. La doctrina también empezó a reconocer competencias concretas a las autoridades de control: imposición, investigación, intervención, escuchar reclamaciones y capacidad de

⁽¹⁸⁾Orden del TJUE de 17 de marzo del 2005, en los casos acumulados C-317/04 y 318/04, Parlamento Europeo contra Consejo y Comisión.

⁽¹⁹⁾Otro factor que hay que tener en cuenta es la disparidad de capacidades coercitivas existentes en las distintas autoridades de control nacionales. Normalmente, la reducida capacidad coercitiva de muchas de ellas dificultaba la correcta aplicación de la Directiva 95/46/CE. Sobre las distintas autoridades de control europeas, podéis ver A. Ramiro (2006).

iniciar acciones legales (Peers, Hervey, Kenner y Ward, 2014). Quizá por todo ello, el art. 57 RGPD enumera con más detalle las principales funciones de la autoridad de control¹⁹:

- Aplicar y controlar el cumplimiento del RGPD²⁰.
- Sensibilizar al público, con especial atención a los niños, así como a los responsables y encargados.
- Asesorar a las autoridades nacionales.
- Facilitar información a los interesados sobre sus derechos.
- Resolver las reclamaciones²¹.
- Cooperar con las otras autoridades de control.
- Alentar la elaboración de códigos de conducta y aprobar los que ofrezcan garantías suficientes.
- Fomentar la creación de mecanismos de certificación y marcas.
- Publicar criterios de acreditación de organismos de supervisión de códigos de conducta y de organismos de certificación.
- Autorizar cláusulas contractuales.
- Aprobar normas corporativas vinculantes.
- Llevar registros internos de las infracciones del RGPD.

Lecturas recomendadas

OCDE (2014). *Best Practice Principles for Regulatory Policy*. París: OECD Publishing.

A. Ottow (2015). *Market and competition authorities, good agency principles*. Oxford: Oxford University Press.

S. Peers; T. Hervey; J. Kenner; A. Ward (eds.) (2014). *The EU charter of fundamental rights, a commentary*. Oxford: Hart Publishing.

Se facilitarán formularios de presentación de reclamaciones. La interacción del delegado de protección de datos o del interesado con la autoridad de control será gratuita para estos. Ahora bien, si las solicitudes son manifiestamente infundadas o excesivas, especialmente si son repetitivas, la autoridad de control podrá, en ese caso, establecer una tasa por costes administrativos, o negarse a actuar. Eso sí, la autoridad de control tendrá que demostrar que se trata de una solicitud manifiestamente infundada o excesiva.

⁽²⁰⁾De hecho, las autoridades de control no solo velarán por el cumplimiento del RGPD, sino también de la Directiva 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril del 2016 y de su trasposición nacional.

⁽²¹⁾Sobre la posible existencia de un derecho a obtener una respuesta a la reclamación ante una autoridad de control, podéis ver STJUE, caso C-192/15, Rease y Williams.

Con el fin de llevar a cabo estas funciones, la autoridad de control dispondrá de unas facultades de investigación. Así, de acuerdo con el art. 58 RGPD, podrá:

- Recabar información del responsable o del encargado.
- Llevar a cabo auditorías de protección de datos.
- Revisar certificaciones.
- Notificar infracciones al responsable o al encargado.

Igualmente, la autoridad de control dispondrá de unas facultades sancionadoras y correctivas:

- Sanciones por incumplimiento del RGPD por parte del responsable o del encargado.
- Órdenes a los responsables y encargados de atender a las solicitudes de los interesados.
- Órdenes al responsable de comunicar al interesado una violación de la seguridad de los datos.
- Imponer limitaciones, e incluso prohibiciones de tratamiento.
- Órdenes de rectificar o suprimir datos.
- Retirada de una certificación.
- Imposición de una multa administrativa.
- Suspensión de flujos de datos hacia un país tercero o una organización internacional.

Finalmente, la autoridad de control tendrá poderes de autorización y consulta:

- Asesoramiento al responsable.
- Emisión de dictámenes para las autoridades nacionales y para el público en general.
- Autorización previa de tratamientos, cuando se requiera.
- Aprobación de códigos de conducta y acreditación de organismos de certificación.
- Expedir certificaciones y criterios de certificación.
- Adoptar cláusulas tipo de protección de datos.

- Aprobar normas corporativas vinculantes.

La autoridad de control podrá poner en conocimiento de los tribunales la infracción del RGPD. Por ley, cada Estado miembro podrá ampliar las facultades de sus autoridades de control. Finalmente, la autoridad de control elaborará un informe anual de sus actividades, con los tipos de infracciones notificadas y las medidas adoptadas²². Este informe se presentará a las autoridades nacionales, será público y se pondrá a disposición de la Comisión y del Comité.

⁽²²⁾No se trata de una publicidad de las resoluciones sancionadoras que incluya al infractor, sino de un listado de tipos de infracciones y de medidas (Troncoso, 2016, pág. 511).

2. Cooperación

Ya hemos mencionado anteriormente la importancia de la independencia de las autoridades de control. Otro aspecto definitorio de su función es el creciente valor de la cooperación (Irurzún, 2016). La cooperación internacional es esencial para el correcto cumplimiento de sus funciones. Las autoridades de control cooperarán con las demás autoridades de control (arts. 60-62 RGPD). Siguiendo el nivel de implicación de las autoridades de control, podemos distinguir tres tipos de cooperación (Hijmans, 2016, pág. 396 y sigs.):

a) Intercambio de información entre las autoridades de control. Aunque parece el problema básico de la cooperación procedimental, el TJUE ha defendido que se requiere también aquí una actitud activa en la asistencia a las demás autoridades de control²³ (Hofmann y Tidghi, 2014). Esta cooperación horizontal entre autoridades de control debería verse reforzada con garantías procedimentales para evitar el *forum shopping*, consistente en seleccionar la autoridad de control principal menos exigente (Hofmann, Schneider y Ziller, 2014a,b).

Lecturas recomendadas

H. C. H. Hofmann; M. Tidghi (2014). «Rights and remedies in implementation of EU policies by multi-jurisdiccional networks». *European Public Law* (vol. 20, núm. 1, págs. 147-164).

H. C. H. Hofmann; J. P. Schneider; J. Ziller (2014a). *Research network on EU Administrative Law, ReNEUAL model rules on EU Administrative procedure: introduction to the ReNEUAL model rules. Book I: General Provisions* [documento en línea].

H. C. H. Hofmann; J. P. Schneider; J. Ziller (2014b). *Research network on EU Administrative Law, ReNEUAL model rules on EU Administrative procedure: introduction to the ReNEUAL model rules. Book V: Mutual Assistance* [documento en línea].

b) Red de autoridades de supervisión efectiva en inspecciones o investigaciones. En estos casos, la cooperación tiene una base más regular, y puede deberse a una reclamación o cuando el responsable se encuentra establecido en más de un país. Esta es la tarea que ha llevado a cabo hasta la fecha el WP29²⁴. Por ejemplo, el examen de las políticas de privacidad de Google obligó a crear un grupo informal de trabajo iniciado por el WP29, y varias autoridades de control desde el 2002 al 2013. De ahí, resultaron investigaciones individuales con decisiones separadas (Kloza y Moscibroda, 2014). Hasta la fecha, este proceso de armonización no obligatoria es el cometido principal llevado a cabo por el WP29. Con el Comité, estas redes deberían fortalecerse.

Lectura recomendada

D. Kloza; A. Moscibroda (2014). «Making the case for enhanced enforcement cooperation between data protection authorities: Insights from competition law». *International Data Privacy Law* (vol. 4, núm. 2, págs. 120-138).

Lectura recomendada

F. Irurzún (2016). «Cooperación y coherencia entre autoridades de control». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 513-526). Madrid: Ed. Reus.

⁽²³⁾ Además de Hofmann y Tidghi (2014), véase también el caso C-503/03, Comisión contra España.

⁽²⁴⁾ A diferencia del Comité, el WP29 no ha tenido competencias directas para asegurar la protección transfronteriza, es decir, en la primera capa de cooperación.

c) Grupos de investigación conjuntas²⁵. En este caso, la red de cooperación de autoridades se transforma en una autoridad de protección de datos europea, cuando decida el Comité. Esto no existía con la Directiva 95/46; lo más parecido hasta la fecha son los *joint supervisory bodies*, para Europol y Eurojust.

(25) Esta práctica se formaliza por primera vez con el art. 62 RGPD, pero ya existían experiencias informales de cooperación en operaciones conjuntas con anterioridad.

Una de las grandes novedades del RGPD ha sido la introducción del mecanismo *one-stop shop* y la consiguiente necesidad de identificar a la autoridad principal. Para entender las ventajas de este mecanismo en relación con la situación anterior de varias actuaciones paralelas de distintas agencias, puede valer el siguiente ejemplo: en el 2015, la autoridad de protección de datos belga inició una investigación en relación con el hecho de que Facebook trataba datos personales no solo de sus usuarios, sino también de usuarios de Internet que entraban en contacto con Facebook. Se le recomendó que se abstuviera de usar estos datos personales de no usuarios. En la investigación, colaboraron informalmente las autoridades de protección de datos de Holanda y de Hamburgo, pero no así de Irlanda, donde Facebook tiene su sede en la Unión Europea. Irlanda había investigado anteriormente los mismos hechos, pero había llegado a la conclusión de que no se producía ninguna infracción de la normativa de protección de datos. Evidentemente, Facebook no aceptó la aplicabilidad del derecho de protección de datos belga y la competencia de la autoridad de control de este país.

Estos mismos hechos deberán resolverse cuando se aplique el RGPD de otra manera. En efecto, la autoridad de control principal y las autoridades de control interesadas deberán cooperar e intercambiarán información. Esto se podrá concretar, como veremos, mediante solicitudes de asistencia mutua o bien mediante operaciones conjuntas. En todo caso, la autoridad de control principal transmitirá a las autoridades de control interesadas un proyecto de decisión para obtener un dictamen de las segundas. Si alguna de las autoridades de control interesadas formula, en el plazo de cuatro semanas, una objeción al proyecto de decisión de la autoridad de control principal, pueden darse dos escenarios:

- La autoridad de control principal accede a las objeciones y presenta un nuevo proyecto de decisión revisado.
- La autoridad de control principal no está de acuerdo con las objeciones, y someterá el asunto al mecanismo de coherencia (art. 63 RGPD) que veremos más adelante.

Si no hay objeciones por parte de las autoridades de control interesadas, se entiende que hay acuerdo en el proyecto de decisión. La decisión se adoptará entonces, y se notificará al responsable o encargado del tratamiento. El responsable o encargado deberá adoptar las medidas adecuadas para dar cumplimiento a la decisión, e informar luego a la autoridad de control principal que, a su vez, informará a las autoridades de control interesadas.

Las autoridades de control se prestarán asistencia mutua. Para ello, responderán a las solicitudes de las otras autoridades de control en un plazo máximo de un mes. Pasado el mes sin respuesta, la autoridad de control requirente podrá adoptar una medida provisional, y el Comité decidirá, finalmente, con urgencia (art. 66 RGPD). La autoridad de control solo podrá negarse a responder a la solicitud si no es competente, o si responder a la solicitud supone infringir el RGPD o el Derecho europeo o nacional. Por regla general, la respuesta será por medios electrónicos, utilizando un formato normalizado, y no se cobrará ninguna tasa, salvo indemnizaciones en casos excepcionales, y previstas por normas de indemnización recíprocas. La Comisión podrá adoptar, mediante actos de ejecución, procedimientos de asistencia mutua y formatos normalizados.

Finalmente, las autoridades de control podrán llevar a cabo operaciones conjuntas, ya sean de investigación o de ejecución. Esto ocurrirá cuando el responsable tenga establecimientos en varios estados miembros, o haya un número elevado de interesados de distintos estados miembros: en ese caso, la autoridad de control del establecimiento principal invitará a una autoridad de control de cada uno de los estados miembros a participar en las operaciones conjuntas. Si pasa un mes desde la previsión de actuación conjunta y no hay invitación, entonces las demás autoridades de control podrán adoptar medidas provisionales, y decidirá, finalmente, el Comité. Las autoridades de control del país de acogida podrán conferir poderes a los representantes de las autoridades de control de los países de origen, para que actúen en el país de acogida, bajo el Derecho del país de acogida. La autoridad de control del país de acogida asume la responsabilidad por daños y perjuicios ocasionados por los representantes de las autoridades de control de origen.

3. Mecanismo de coherencia

La cooperación entre autoridades de control se completa con un mecanismo de coherencia (art. 63 RGPD). El Comité Europeo de Protección de Datos, que sustituye al WP29 y tendrá, a diferencia de este, un rol formal en la protección de datos, emitirá un dictamen cuando una autoridad de control pretenda adoptar alguna de las siguientes medidas (art. 63 RGPD):

- Proyecto de una lista de tipos de tratamientos de datos que requieran una evaluación de impacto (art. 35.4 RGPD).
- Proyecto de código de conducta sobre tratamiento de datos en varios estados miembros (art. 40.7 RGPD).
- Proyecto de criterios de acreditación de un organismo de supervisión de códigos de conducta (art. 41.3 RGPD) o de criterios de acreditación de un organismo de certificación (art. 43.3 RGPD).
- Proyecto de cláusulas tipo para transferencias mediante garantías adecuadas (art. 46.2d RGPD) o de cláusulas contractuales tipo para la relación con el encargado (art. 28.8 RGPD).
- Proyecto de cláusulas contractuales para las transferencias mediante garantías adecuadas (art. 46.3a RGPD).
- Aprobación de normas corporativas vinculantes (art. 47 RGPD).

De igual manera, una autoridad de control, el presidente del Comité o la Comisión podrán solicitar que un asunto general o que tenga aplicación en más de un Estado miembro sea examinado por el Comité para que este adopte un dictamen. Esto será de aplicación, por ejemplo, en los casos de incumplimiento de las obligaciones de asistencia mutua o de operaciones conjuntas. El Comité emitirá el correspondiente dictamen en el plazo de ocho semanas, prorrogables seis semanas más, siempre que no se haya emitido ya uno anteriormente sobre el mismo asunto. El dictamen se aprobará por mayoría simple de los miembros del Comité. Para que este mecanismo de coherencia sea efectivo, es necesario que las autoridades de control informen sin dilación por medios electrónicos al Comité, mediante formato normalizado, de los hechos y motivos que justifican la adopción del proyecto de decisión y de las opiniones de las otras autoridades de control interesadas. Igualmente, la autoridad de control deberá tener en cuenta el dictamen del Comité y tendrá que informar de la decisión modificada subsiguiente, mediante formato normalizado. Para

ello, dispone de dos semanas desde la recepción del dictamen del Comité para indicar por medios electrónicos al presidente del Comité si va a mantener o modificar el proyecto de decisión inicial.

Puede darse el caso de que la autoridad de control no prevea seguir, en todo o en parte, el dictamen del Comité. En este caso, se aplicará el mecanismo de resolución de conflictos (art. 65 RGPD). El Comité adoptará entonces una decisión vinculante, así como en los siguientes supuestos:

- Cuando una autoridad de control interesada manifieste una objeción motivada a un proyecto de decisión de una autoridad de control principal, o esta última haya rechazado la objeción, por considerarla no motivada.
- Cuando existan diferencias sobre cuál es la autoridad de control competente para el establecimiento principal.
- Cuando una autoridad de control competente no solicite el dictamen preceptivo, de acuerdo con el art. 64 RGPD, o cuando no lo siga y se haya emitido en virtud de este mismo artículo.

El Comité dispone de un mes para adoptar la decisión vinculante, prorrogable otro mes más, a partir de la remisión del asunto. La decisión se adoptará por mayoría de dos tercios de los miembros del Comité, y se remitirá a las autoridades de control principal e interesadas. Asimismo, la decisión se publicará en el sitio web del Comité. Si pasan los dos meses, la decisión podrá adoptarse por mayoría simple, y decidirá el voto del presidente en caso de empate. Mientras, las autoridades de control no tomarán ninguna decisión, a la espera de la decisión del Comité. Una vez adoptada esta última, la autoridad de control principal o, en su caso, la autoridad de control ante la cual se presentó la reclamación, adoptarán la decisión definitiva en el plazo de un mes desde la notificación, e informarán de la misma al Comité para su publicación en el sitio web del mismo, así como al responsable y al encargado. Se adjuntará, a la misma, la decisión del Comité.

Una excepción al mecanismo de coherencia es lo contemplado en el art. 66 RGPD como procedimiento de urgencia. Así, cuando una autoridad de control considere que es urgente intervenir para proteger derechos de los interesados, podrá adoptar inmediatamente medidas provisionales con efectos en su territorio, por un plazo máximo de tres meses. Estas medidas serán inmediatamente comunicadas a las demás autoridades de control interesadas, al Comité y a la Comisión. La Comisión, mediante actos de ejecución, podrá concretar las modalidades de intercambio de información por medios electrónicos entre autoridades de control, y entre esta y el Comité, y establecerá un formato normalizado.

Si se requiere la adopción de medidas definitivas, entonces la autoridad de control podrá solicitar, motivando esta solicitud, y con carácter urgente, un dictamen o una decisión vinculante al Comité. De hecho, cualquier autoridad de control puede pedir este dictamen o decisión vinculante urgente cuando una autoridad de control competente no ha tomado ninguna medida en un supuesto urgente para proteger derechos de los interesados. Estos dictámenes o decisiones vinculantes urgentes se adoptarán en el plazo de dos semanas, por mayoría simple de los miembros del Comité.

Como valoración final del mecanismo de coherencia, cabe mencionar que tiene dos capas. Así, en primer lugar, es un procedimiento de resolución en los casos en los que distintas autoridades de control tienen perspectivas diferentes en un caso concreto, es decir, cuando una autoridad de control tiene serias objeciones a la propuesta de decisión de otra autoridad de control (art. 64 RGPD). En segundo lugar, se pretende también armonizar con este mecanismo la aplicación de la normativa de protección de datos en el ámbito de la Unión Europea, como una suerte de casación jurisdiccional (art. 65 RGPD). Se trata de un mecanismo vinculante de resolución de conflictos, cuando no se llega a un acuerdo. Tanto el WP29, como el supervisor europeo de protección de datos, han criticado esta segunda atribución de competencias²⁶. De todos modos, el punto débil de todo el sistema se encuentra en la capacidad de la autoridad de control de decidir discrecionalmente involucrar o no al Comité (Hijmans, 2016, pág. 407). La práctica indicará el valor real de este mecanismo a la hora de proteger los datos personales. Convendría haber puesto más claramente de relieve la ventaja de la segunda capa del mecanismo de coherencia para la protección de los derechos de los ciudadanos. Ahora, no parece este el motivo principal de su adopción.

⁽²⁶⁾ El WP29 critica la participación de la Comisión en el mecanismo de coherencia, y pretende limitar el efecto de casación. Podéis ver, al respecto, su opinión 01/2012, sobre las propuestas de reforma relativas a la protección de datos (WP 191). En un sentido parecido, el supervisor europeo de protección de datos también prefería limitar el mecanismo a la primera capa, en su opinión de 7 de marzo del 2012, sobre el paquete de reformas sobre protección de datos. Incluso la enmienda 167 del Parlamento Europeo, con un nuevo art. 58a, parecía ir en la misma dirección. El Consejo Europeo tampoco parece querer ir más allá de un mecanismo de resolución de conflictos en casos concretos.

4. El Comité Europeo de Protección de Datos

1) Características generales

Una de las novedades destacadas del RGPD es la creación del Comité Europeo de Protección de Datos (Cervera, 2016). Hemos tenido ocasión de mencionarlo anteriormente, y ahora veremos con más detalle este organismo dotado de personalidad jurídica (art. 68 RGPD). Dispone de un presidente y lo componen los directores de una autoridad de control de cada Estado miembro y el supervisor europeo de protección de datos, o sus representantes. En el caso de existir más de una autoridad de control nacional de protección de datos, se nombrará a un representante común, de acuerdo con el Derecho nacional. La Comisión será informada de las actividades del Comité y participará en las reuniones mediante un representante, aunque sin derecho a voto. En lo relativo a las decisiones vinculantes, el supervisor europeo de protección de datos solo votará en las decisiones que afecten a las instituciones, órganos y organismos de la Unión Europea. El Comité actuará con total independencia de la Comisión, pese a asesorar a esta última o atender las solicitudes de asesoramiento por parte de la Comisión.

2) Competencias

La Unión Europea, a diferencia de Estados Unidos, ha sido hasta ahora reticente a otorgar competencias reguladoras a los órganos expertos, cosa que sí se da en el caso de la Federal Trade Commission (FTC) americana²⁷. Sin embargo, el Comité parece tener unas competencias que podrían ser reguladoras en la práctica. Las principales competencias del Comité vienen mencionadas en el artículo 70 RGPD:

- Garantizar el cumplimiento del RGPD en los supuestos de los arts. 64 y 65 RGPD, antes descritos.
- Asesorar a la Comisión sobre cuestiones relativas a la protección de datos y a propuestas de modificación del RGPD.
- Asesorar a la Comisión sobre el formato y los procedimientos para intercambiar información entre responsables, encargados y autoridades de control en relación con las normas corporativas vinculantes.
- Emitir directrices, recomendaciones y buenas prácticas para la supresión de vínculos, copias o réplicas de los datos personales procedentes de servicios de comunicación a disposición pública (art. 17.2 RGPD); sobre decisiones basadas en perfiles (art. 22.2 RGPD); en las violaciones de seguridad

Lectura recomendada

L. Cervera (2016). «El Comité Europeo de Protección de Datos». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 527-538). Madrid: Ed. Reus.

⁽²⁷⁾La competencia de la FTC se aplica a casos de prácticas injustas o fraudulentas en el ámbito de la privacidad del consumidor. Esta autoridad proviene del art. 5 de la *FTC act*.

de los datos (arts. 33.1, 33.2 y 34.1 RGPD); y en transferencias basadas en normas corporativas vinculantes (art. 47 RGPD), entre otros.

- Alentará la elaboración de códigos de conducta, mecanismos de certificación de protección de datos, sellos y marcas de protección de datos.
- Acreditará organismos de certificación (art. 43 RGPD), llevará un registro de los organismos acreditados (art. 43.6 RGPD) y de los responsables o encargados acreditados en terceros países (art. 42 RGPD), y especificará los requisitos de la acreditación (arts. 42 y 43.3 RGPD).
- Facilitará a la Comisión un dictamen sobre los requisitos de certificación (art. 43.8 RGPD), sobre los iconos (art. 12.7 RGPD) y sobre la adecuación del nivel de protección de un tercer país, parte del mismo o una organización internacional.
- Emitirá dictámenes sobre proyectos de decisión de las autoridades de control, como ya hemos visto anteriormente.
- Promoverá acuerdos de cooperación y programas de formación entre autoridades de control europeas e intercambios de información y legislación con autoridades de control de todo el mundo.
- Emitirá códigos de conducta a escala de la Unión Europea (art. 40.9 RGPD).
- Llevará un registro electrónico público de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados de acuerdo con el mecanismo de coherencia.

Lecturas recomendadas

Sobre la posición institucional de la Federal Trade Commission americana, podéis ver:

FTC (2012, 26 de marzo). «FTC Issues Final Commission Report on Protecting Consumer Privacy» [documento en línea].

D. J. Solove; W. Hartzog (2014). «The FTC and the new common law of privacy». *Columbia Law Review* (vol. 114, pág. 583 y sigs.).

D. C. Valadeck (2015). «A US perspective on narrowing the U.S.-EU privacy divide». En: A. Rallo; R. García (eds.). *Hacia un Nuevo derecho europeo de protección de datos (Towards a new European Data Protection Regime)*. Valencia: Tirant lo Blanch.

3) Organización y funcionamiento

El Comité elaborará un informe anual sobre el tratamiento de datos en la Unión y, si procede, en terceros países y organizaciones internacionales. El informe se hará público y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión, e incluirá también un estudio de la aplicación práctica de las directrices, recomendaciones y buenas prácticas, así como de las decisiones vinculantes.

El Comité tomará sus decisiones por mayoría simple, salvo que el reglamento indique lo contrario. Este reglamento interno se adoptará por mayoría de dos tercios de sus miembros. El Comité elegirá por mayoría simple a un presidente y dos vicepresidentes, con un mandato de cinco años, renovable una vez. El Comité distribuirá las funciones entre el presidente y los vicepresidentes en su reglamento interno. Las funciones del presidente vienen determinadas en el art. 74 RGPD:

- Convocar las reuniones del Comité y preparar su orden del día.
- Notificar las decisiones a la autoridad de control principal y a las autoridades de control interesadas.
- Garantizar el cumplimiento de las funciones del Comité y, de manera destacada, del mecanismo de coherencia.

El supervisor europeo de protección de datos se encargará de la secretaría, siguiendo las instrucciones del presidente del Comité²⁸. El personal del supervisor que desempeñe estas funciones dependerá de un superior jerárquico distinto del resto del personal del supervisor. El Comité, en consulta con el supervisor, elaborará un memorando para esta colaboración, que será de aplicación al personal en esta situación. La secretaría presta apoyo al Comité, y sus competencias son las siguientes (art. 75.6 RGPD):

- Asuntos corrientes.
- Comunicación entre miembros del Comité, presidente, Comisión, otras instituciones y el público en general.
- Gestión de los medios electrónicos para la comunicación interna y externa.
- Traducción de la información.
- Preparación y seguimiento de las reuniones.
- Preparación, redacción y publicación de los dictámenes, decisiones y otros acuerdos adoptados por el Comité.

Los debates del Comité serán confidenciales cuando se considere necesario, de acuerdo con su reglamento interno. Por otro lado, el acceso a los documentos presentados en el Comité se regirá por el Reglamento (CE) 1049/2001.

⁽²⁸⁾El WP29, antecesor del Comité, y formado por las autoridades de control nacionales y el supervisor europeo, propuso, sin éxito, que el supervisor fuera vicepresidente del Comité (opinión 01/2012, sobre las propuestas de reforma de protección de datos, adoptado el 23/03/2012, WP 191). La propuesta final no menciona esta vicepresidencia, limita el poder de voto del supervisor y aísla al personal de la secretaría de la dirección directa del supervisor.

Bibliografía

- Arenas, M.** (2006). *El derecho fundamental a la protección de datos personales en Europa*. Valencia: Tirant lo Blanch.
- Balthasar, A.** (2013). «“Complete Independence” of national data protection supervisory authorities». *Utrecht Law Review* (vol. 9, núm. 3, págs. 26-38).
- Bamberger, K. A.; Mulligan, D. K.** (2013). «Privacy in Europe: Initial Data on Governance Choices and Corporate Practices». *Georges Washington Law Review* (vol. 81, pág. 1529 y sigs.).
- Barnard-Wills, D.; Wright, D.** (2015, julio). «Co-ordination and co-operation between Data Protection Authorities» [documento en línea]. <<http://www.phaedra-project.eu/?s=Co-ordination+and+co-operation+between+Data+Protection+Authorities>>.
- Bennet C. J.; Raab, C.** (2006). *The Governance of Privacy, Policy Instruments in Global Perspective*. Cambridge, MA: MIT Press.
- Cervera, L.** (2016). «El Comité Europeo de Protección de Datos». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 527-538). Madrid: Ed. Reus.
- Chiti, E.** (2014). «An important part of the EU’s institutional machinery: Features, problems and perspectives of European agencies». *Common Market Law Review* (núm. 46, págs. 1395-1442).
- Craig, P.; Búrca, G. de (eds.)** (2011). *The evolution of EU law* (2.ª ed.). Oxford: Oxford University Press.
- Everson, M.; Cosimo, M.; Vos, E. (eds.)** (2014). *EU agencies in between Institutions and Member States*. Nueva York / Alphen aan den Rijn, Países Bajos: Kluwer Law International.
- FTC** (2012, 26 de marzo). «FTC Issues Final Commission Report on Protecting Consumer Privacy» [documento en línea]. <<http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy>>.
- González, G.** (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Berlín: Springer.
- Hijmans, H.** (2016). *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFUE*. Berlín: Springer.
- Hofmann, H. C. H.; Schneider, J. P.; Ziller, J.** (2014a). *Research network on EU Administrative Law, ReNEUAL model rules on EU Administrative procedure: introduction to the ReNEUAL model rules. Book I: General Provisions* [documento en línea]. <http://www.reneual.eu/images/Home/ReNEUAL-Model_Rules-Compilation_BooksI_VI_2014-09-03.pdf>.
- Hofmann, H. C. H.; Schneider, J. P.; Ziller, J.** (2014b). *Research network on EU Administrative Law, ReNEUAL model rules on EU Administrative procedure: introduction to the ReNEUAL model rules. Book V: Mutual Assistance* [documento en línea]. <http://www.reneual.eu/images/Home/ReNEUAL-Model_Rules-Compilation_BooksI_VI_2014-09-03.pdf>.
- Hofmann, H. C. H.; Tidghi, M.** (2014). «Rights and remedies in implementation of EU policies by multi-jurisdiccional networks». *European Public Law* (vol. 20, núm. 1, págs. 147-164).
- Irurzún, F.** (2016). «Cooperación y coherencia entre autoridades de control». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 513-526). Madrid: Ed. Reus.
- Kloza, D.; Moscibroda, A.** (2014). «Making the case for enhanced enforcement cooperation between data protection authorities: Insights from competition law». *International Data Privacy Law* (vol. 4, núm. 2, págs. 120-138).
- OCDE** (2014). *Best Practice Principles for Regulatory Policy*. París: OECD Publishing.
- Ottow, A.** (2015). *Market and competition authorities, good agency principles*. Oxford: Oxford University Press.
- Peers, S.; Hervey, T.; Kenner, J.; Ward, A. (eds.)** (2014). *The EU charter of fundamental rights, a commentary*. Oxford: Hart Publishing.

Solove, D. J.; Hartzog, W. (2014). «The FTC and the new common law of privacy». *Columbia Law Review* (vol. 114, págs. 583 y sigs.).

Troncoso, A. (2016). «Autoridades de control independientes». En: J. L. Piñar (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 461-512). Madrid: Ed. Reus.

Valadeck, D. C. (2015). «A US perspective on narrowing the U.S.-EU privacy divide». En: A. Rallo; R. García (eds.). *Hacia un Nuevo derecho europeo de protección de datos (Towards a new European Data Protection Regime)*. Valencia: Tirant lo Blanch.