



Comisión de Libertades Civiles, Justicia y Asuntos de Interior

Lunes 25 de noviembre de 2019 de las 19.00 a las 22.30 horas
en el Parlamento Europeo
ESTRASBURGO

Comparecencia del candidato Yann PADOVA

1. ¿Podría exponer las razones por las que presenta su candidatura a este puesto y explicar por qué se considera cualificado para el mismo?

Mi trayectoria profesional me ha permitido adquirir un **conocimiento completo sobre la protección de datos**, ámbito en el que trabajo **desde hace 20 años**. Primero, desde la Asamblea Nacional, abordé dicha materia como legislador, ya que trabajé en la transposición de la Directiva 95-46, así como en otros proyectos de ley, como en el de creación de un fichero de seguimiento de los autores de infracciones sexuales. En la Asamblea Nacional, como **administrador** sujeto a una **estricta obligación de neutralidad**, aprendí a trabajar con diputados electos de **todos los espectros políticos** y a negociar soluciones transaccionales sobre los textos legislativos. Volví a desempeñar esa tarea en la Comisión Europea trabajando en las primeras versiones del RGPD. Esta **experiencia de asesor del Legislador** me parece especialmente pertinente para el puesto de Supervisor Europeo de Protección de Datos (SEPD) en su labor ante el Parlamento y el Consejo.

Posteriormente, como secretario general de la Autoridad Francesa de Protección de Datos (CNIL) creé la «nueva CNIL», resultante de esta transposición, con nuevas competencias reforzadas y variadas. **Se modificaron la organización y los procedimientos de la CNIL, así como el ejercicio del poder coercitivo y de control protegido, y se establecieron nuevos servicios y mecanismos para los usuarios desarrollados**, etc. Para explicar estas nuevas competencias, puse en marcha una ambiciosa política de comunicación, también a nivel europeo. Habida cuenta las nuevas tareas del SEPD, **esta experiencia en la introducción de cambios**, de dirección, de establecimiento de nuevas competencias, de **gestión presupuestaria rigurosa**, de despliegue de herramientas y una fuerte política de **comunicación** me parecen esenciales para desempeñar con éxito la función de SEPD.

Como comisario en la Comisión Reguladora de la Energía, supervisé la redacción del informe sobre la gestión de datos por los operadores de redes de energía. Las tareas de estos operadores de redes evolucionan rápidamente con el despliegue de «redes inteligentes» y la recogida masiva de datos resultante. Están surgiendo nuevas oportunidades, pero también aparecen nuevos riesgos, como la ciberdelincuencia. También en esta ocasión, me resultará útil para el SEPD la experiencia de construir un nuevo marco regulador en un **sector industrial estratégico**, en **beneficio del consumidor final** y de la **confianza digital**.

En la actualidad, como asesor estratégico de la ICO (Oficina del Comisionado de Información, Reino Unido), **estoy trabajando en el vínculo entre la normativa y la innovación**. Desde 2016, mi función consiste en proponer la creación de un «sandbox» (campo de pruebas) y acompañar a la ICO en este proceso hasta su despliegue operativo. Este debate sobre la innovación al servicio del bien público deberá producirse a nivel europeo, sobre todo **en el Parlamento**, en particular tras conocerse las ambiciones europeas en materia de inteligencia artificial. Mi reflexión sobre esta cuestión, así como mi actividad docente y mis publicaciones académicas, resultarán de utilidad para asesorar al Parlamento.

Y, por último, ejerzo como abogado en un despacho internacional. Asesoro a las empresas, en materia de datos personales, en la elaboración y gestión de proyectos innovadores. La problemática de la protección de datos se está convirtiendo en uno de los impulsores de la competitividad y la diferenciación de las empresas. Constituye también un factor de riesgo más elevado, habida cuenta del importe de las sanciones previstas en el RGPD. Así pues, hoy en día mi labor de asesoramiento es más estratégica y abarca diferentes ámbitos jurisdiccionales. **Considero que el conocimiento de los desafíos y el funcionamiento de las empresas desde dentro**, así como las limitaciones y objetivos de su transformación digital, es una **condición necesaria** para ejercer **adecuadamente** las tareas asignadas al SEPD.

Esta experiencia diversificada garantiza no solo una competencia técnica multidisciplinaria, una visión estratégica de las cuestiones, una apertura internacional, sino que también es muestra de pragmatismo. Mi recorrido demuestra **mi capacidad para construir «puentes»: entre ámbitos** jurídicos diferentes, **entre el Derecho y la tecnología**, **entre el Derecho y la economía**, entre **sistemas jurídicos de distintos países**, entre **las instituciones y los sujetos, incluidos los políticos, a veces con intereses divergentes**, entre **culturas**. Esta experiencia también ilustra **mi vinculación con el diseño europeo de la protección de datos**, mi capacidad para defender y **promoverlo** a nivel internacional. Esta vinculación también está relacionada con **mis orígenes personales**, de ascendencia sueca por mi madre, originario de los territorios orientales polacos por mi padre y portador del nombre de una ciudad italiana en la que mis antepasados hallaron refugio.

Para acabar, me gustaría añadir que **mi vida profesional gira en torno a la independencia**. Lo estuvo cuando decidí incorporarme a la CNIL y a la CRE, autoridades independientes. Lo está ahora en mi profesión de abogado, en forma de obligación deontológica. Pero la independencia se mide por mis actos: tal como ponen de manifiesto **mis artículos** académicos sobre el derecho al olvido, en sintonía con la sentencia del Tribunal de Justicia de la Unión Europea (C-507/17), o mi reciente **alegato ante el TJUE** sobre el control que efectúa el Estado (C-511/18). La independencia es una disciplina exigente. Debe incluir **el diálogo con todas las partes interesadas**, de lo contrario, se convierte en una autarquía inaccesible. El SEPD necesitará una concepción semejante de la independencia, exigente pero **constructiva, abierta pero firme**, y que yo quiero poner a **su servicio**.

2. ¿Podría describir su visión del futuro de la autoridad cuya dirección tendría que asumir en calidad de SEPD, incluidos los posibles desafíos que prevea y sus prioridades para esta autoridad independiente?

Con el rápido desarrollo de la **inteligencia artificial (IA)**, el autoaprendizaje de algoritmos y la internet de las cosas, Europa se enfrenta a **retos éticos sin precedentes**. En un momento en el que el volumen de datos se duplica cada veinticuatro meses, ¿cómo pueden regularse unos

algoritmos que cambian por sí mismos y que, en ocasiones, parecen escapar al control de sus creadores? ¿Cómo podemos garantizar la transparencia y la comprensión de estos instrumentos que invaden nuestra vida cotidiana? ¿Cómo podemos garantizar su objetividad y medir su sesgo? ¿Cómo corregirlos cuando son discriminatorios? Estos retos son más importantes en la medida que **Europa se halla atrapada entre dos modelos de regulación**: el modelo de Estados Unidos, donde no existe una legislación federal transversal sobre los datos, y es el juez, o el regulador sectorial, quien actúa *a posteriori*, y el modelo de China, caracterizado por una hipercentralización estatal del acceso a los datos.

En este **contexto geopolítico de los datos**, en un mundo digital en construcción, **Europa debe convertirse** en el nuevo actor principal. La Comisión ha anunciado su intención de presentar una propuesta sobre la IA en un plazo de cien días. Europa **dispone de unos medios acordes con sus ambiciones**, ya que dispone de un sólido marco jurídico sobre el que **construir** esta nueva regulación: **el RGPD**. Este texto recoge una serie de principios pertinentes, como la rendición de cuentas, la transparencia, el derecho de las personas a no ser objeto de una decisión adoptada únicamente sobre la base de un tratamiento automatizado. Basándose en el RGPD, Europa puede y debe **lograr un uso ético de la IA, responsable, beneficioso para las personas y para la sociedad en su conjunto**. Y en la **construcción** de este enfoque **europeo y humanista de la inteligencia artificial**, el **SEPD** tiene que desempeñar un papel esencial, **prestando asesoramiento** y presentando **propuestas** pragmáticas e innovadoras al **Parlamento que es el lugar privilegiado** en el que construir **democráticamente** esta vía europea. En cuanto al fondo, podría preverse la introducción de un enfoque en función de los riesgos que podría basarse en el derecho a la experimentación, de mecanismos de certificación, corrección y transparencia reforzados, e incluso de una trazabilidad de los datos y los algoritmos utilizados (¿hacia «un pasaporte» para los datos? Este es un primer desafío importante que también deberá **abordarse a nivel internacional**. Y el **SEPD** deberá ser **el portavoz de esta vía europea**.

El segundo desafío estratégico del SEPD se deriva del **creciente valor de los datos, la complejidad y el carácter evolutivo de la economía de los datos**. La comprensión de la cadena de valor y **la identificación de las tendencias** emergentes, así como de los nuevos actores, se han convertido en requisitos previos para prestar un asesoramiento pertinente, **ágil y proactivo**, y no solo reactivo. Para ello, el SEPD **deberá aumentar** los mecanismos de **cooperación** operativa con las autoridades europeas responsables de la **competencia** y con las **autoridades nacionales de protección de datos**, y desarrollar acuerdos de asociación con centros de investigación en materia de **economía, ciberseguridad, sociología** sobre los usos de la tecnología. Pero, sobre todo, el SEPD tendrá que mejorar su propia capacidad de análisis de la **perspectiva tecnológica** y de intervención, **mediante la diversificación del perfil de sus agentes, lo que reforzará su independencia**.

Yo dispongo de esa **experiencia en la construcción de una capacidad de análisis de la perspectiva tecnológica**, puesto que creé, dentro de la CNIL, **el laboratorio de conocimientos técnicos**, uno de los primeros de Europa, aumentando el efectivo de ingenieros del 3 % al 10 % en seis años. La protección de los datos ya no puede funcionar **de forma aislada**. Para ser un asesor **pertinente, proactivo y multidisciplinario para el Parlamento, el Consejo y la Comisión**, el **SEPD** debe abrirse más y agruparse en torno a un **nuevo proyecto estratégico**. Me comprometo a **participar en la construcción** de ese proyecto, mediante la consulta a las **partes interesadas** y en un plazo de 6 meses desde mi incorporación al cargo, ya que **la independencia no es autarquía**.

El tercer desafío se refiere a la cuestión del intercambio y transferencia de datos entre Estados, incluidos los terceros países, por motivos de lucha contra la delincuencia. El **TJUE y el Parlamento han adoptado posturas firmes** en las que el SEPD podrá apoyarse a la hora de desarrollar sus tareas consultivas y de control (véase la pregunta n.º 3).

El último reto al que se enfrentará el SEPD se deriva de su **función como supervisor** de las instituciones europeas. El SEPD debe llevar a cabo su labor de control de forma **previsible, justa y creíble**. Para ello, debe seguir acompañando a las instituciones europeas en la adecuación a las normas, **ayudándolas en su proceso de maduración**, por ejemplo, ofreciéndoles **nuevos instrumentos** de rendición de cuentas, como los modelos de contratos de subcontratación, o las herramientas de autoevaluación, las **guías prácticas** temáticas y las formaciones exhaustivas en ciberseguridad. El SEPD también deberá mejorar su **capacidad de control** sobre el terreno o con arreglo a documentación, labor que requiere **competencias específicas**. Soy consciente de esta cuestión por **haber creado el servicio de control de la CNIL**. Así pues, el SEPD deberá **publicar su programa anual de controles e informar sobre su ejecución**, en especial **ante el Parlamento**. De ello también depende su **credibilidad**, tanto dentro como fuera de la UE.

A fin de hacer frente a todos estos retos, **el SEPD necesitará el pleno apoyo del Parlamento** para obtener un aumento de sus recursos que siguen siendo insuficientes para hacer frente a sus tareas y desafíos.

3. ¿Cómo se propone desempeñar el cometido que se ha atribuido legalmente al SEPD en materia de supervisión de las agencias de justicia y de asuntos de interior, y cuál es su opinión sobre los intercambios de datos personales que tienen su origen o su destino en dichas agencias, concretamente en relación con la supervisión de las transferencias de datos personales a terceros países?

Para supervisar eficazmente las operaciones de tratamiento de datos por parte de las autoridades europeas encargadas de hacer cumplir la ley, **es preferible conocer el funcionamiento del sistema penal**, las instituciones judiciales y los servicios responsables de la lucha contra la delincuencia. A este respecto, mi experiencia en la Comisión de Leyes de la Asamblea Nacional y en la CNIL (autoridad francesa de protección) me parece especialmente pertinente.

En la Comisión de Leyes me responsabilicé del seguimiento del presupuesto de la administración penitenciaria y de las cuestiones relativas al Derecho penal y al Derecho en materia de datos personales. En este contexto, durante siete años me correspondió tratar todos los textos penales, y en particular la creación de una base de datos y un sistema de seguimiento de los autores de infracciones sexuales graves (fichero «FIJ AIS»).

En cuanto a la CNIL, durante mucho tiempo fue una de las pocas autoridades de protección de datos en Europa que disponía de un control *ex ante* y *ex post* de los expedientes policiales y judiciales. Esta es la razón por la que, como secretario general, organicé, en 2008 y 2009, **el primer control general de los archivos de la policía judicial** (STIC), llevado a cabo por los fiscales competentes. Cuando se realizó ese control, el STIC contenía datos de más de 36 millones de personas. El control duró más de un año, dio lugar a 19 inspecciones en el terreno, al envío de cuestionarios a 34 tribunales que representaban el 50 % de la actividad penal en Francia, así como a solicitudes técnicas sobre las medidas de seguridad y la trazabilidad de las conexiones. Además, el derecho de acceso de las personas al tratamiento de los datos personales

por parte de agentes de la policía solo se hizo valer de forma «indirecta», es decir, la CNIL ejerció ese derecho en nombre del solicitante, tal como también puede hacer el SEPD, en virtud del artículo 84 del Reglamento n.º 2018/1725. **Esta experiencia única de control y de ejercicio del derecho de acceso indirecto** (unas 4 000 solicitudes anuales a la CNIL) me resultará especialmente útil en el SEPD.

En efecto, el SEPD interviene en un **marco jurídico complejo** y que evolucionará durante su próximo mandato. A pesar de la aprobación del Reglamento (CE) n.º 2018/1725 y de su capítulo IX, las competencias del SEPD siguen siendo variables, ya que se basan en varios instrumentos jurídicos especiales. Tal como ocurre con el tratamiento de datos operativos llevado a cabo por Europol, Eurojust o la Fiscalía Europea. Las competencias del SEPD son diferentes, ya que no puede imponer una multa administrativa, ni ordenar la suspensión de los flujos internacionales de datos, ni dirigir un requerimiento a la Fiscalía Europea. Tampoco puede imponer una prohibición de tratamiento de datos a Eurojust, ni a la Fiscalía Europea, a diferencia de Europol.

Sin embargo, los sistemas jurídicos actualmente en vigor permiten al **SEPD ejercer un estricto control sobre estas agencias, control absolutamente esencial teniendo en cuenta los riesgos inherentes al tratamiento** de dichos datos y **la perspectiva de interoperabilidad** de determinados sistemas de información. Los riesgos más elevados se refieren a la transferencia de datos, en particular a terceros países, y por ese motivo el control debe ejercerse con el máximo rigor. A falta de una decisión de adecuación adoptada por la Comisión con arreglo a la Directiva 2016/680, el papel del SEPD será crucial.

Este control ya existe para los acuerdos celebrados entre la Unión y terceros países para las transferencias de datos por parte de Europol, y tendrá que continuar con un nivel máximo de exigencia. En cuanto a Eurojust y la Fiscalía Europea, el supervisor tendrá que asumir las competencias de control que le son conferidas para garantizar que las **transferencias de datos se llevan a cabo de conformidad con las normas establecidas en los reglamentos aplicables y de acuerdo con las exigencias del TJUE**. El riesgo de que los datos transferidos sean utilizados para otros fines en terceros países es real y, a ese respecto deberá efectuarse un control estricto.

Con el fin de **evitar la fragmentación** de los sistemas de control y, por lo tanto, el debilitamiento del nivel de protección de los datos de las personas en este ámbito especialmente sensible, el artículo 98 del Reglamento (UE) 2018/1725 prevé una «cláusula de aplazamiento» (a más tardar el 30 de abril de 2022). Con arreglo a esta cláusula, la Comisión revisará los actos jurídicos especiales para evaluar su coherencia con la Directiva (UE) 2016/680 y detectar las divergencias que puedan dar lugar a dicha fragmentación. La función del SEPD será aquí decisiva para hacer valer su experiencia y asesorar a la Comisión, al Consejo y al Parlamento.

Para ello, considero **esencial que el SEPD**: i) elabore desde principios de 2020 un **programa plurianual de controles**, que se refleje dentro de su programa anual (véase la respuesta a la pregunta n.º 2); ii) aumente sus **competencias**, así como los recursos disponibles para realizar controles sobre el terreno; iii) desarrolle una **coordinación** reforzada con las **autoridades nacionales de protección de datos**, teniendo en cuenta la naturaleza «mixta» de los datos tratados por dichos organismos; iv) **proporcione información** de manera más explícita e independiente de su labor de supervisión y v) desarrolle **mecanismos de acompañamiento** y de adecuación específicos, en colaboración con los equipos de esos organismos.

