FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

El Reglamento Europeo (UE) 2016/679: análisis de un claroscuro

*Marcel Moritz** y *Valentin Gibello***

RESUMEN

La Directiva 95/46/CE del 24 de octubre de 1995 fue el primer instrumento jurídico para la regulación de la protección de datos en la Unión Europea. Esta Directiva será sustituida por el Reglamento (UE) 2016/679, a partir del 28 de mayo de 2018.

Este artículo aborda de manera crítica el nuevo Reglamento Europeo, se presentan sus objetivos, y se destaca la importancia de crear un Reglamento en lugar de una nueva Directiva sobre protección de datos personales. Además, se describe el fortalecimiento de la protección de datos personales en la Unión Europea, al tenor de los desafíos tecnológicos de la actualidad. Sin embargo, varios analistas consideran que el nuevo Reglamento genera dudas por cuanto pretende beneficiar a los responsables del tratamiento de datos a través de la aplicación de una metodología de análisis de riesgos. Este doble enfoque genera muchas incertidumbres jurídicas que se discuten a lo largo del texto.

Palabras clave: datos personales, protección de datos, privacidad, derechos fundamentales, derecho al olvido, Unión Europea, análisis de gestión de riesgos.

ABSTRACT

The Directive 95/46/CE from October 24th 1995 was the first legal instrument for the regulation of data protection in the European Union. This directive will be replaced by the Regulation (UE) 2016/679, from May 28th 2018.

This paper abords in critical way this new European Regulation, presents its purposes, and the importance of creating a Regulation instead of a new data protection directive. Furthermore, this paper describes the strenghtening of european data protection law in relation to the challenges of today's technology.

Nevertheless, some analysts consider that the new Regulation generates many doubts because it aims to benefit data controllers by establishing a risk based

* Director del Máster en Derecho Digital, Université Lille 2 Droite et Santé, CERAPS.

** Candidato a doctor, Université Lille 2 Droite et Santé, CERAPS.

approach. This double perspective creates many ambiguities that are discussed along the contents of this paper.

KEYWORDS: personal data, data protection, privacy, fundamental rights, right to be forgotten, european union, risk based approach.

FORO

INTRODUCCIÓN

Conscientes de la transición hacia una economía centralizada en los datos, la Comisión Europea anunció la creación del mercado único digital (digital single market)[1] en mayo de 2015. La Comisión presidida por *Jean-Claude Junker* tuvo la prioridad de agregar a la economía digital dentro de los objetivos de la Unión, a través de la creación de un mercado interno de libre competencia de acuerdo con los valores de la Unión, y en particular, con la protección de los derechos humanos.

En esta perspectiva, y paralelamente al establecimiento de medidas de regulación de esta economía (enmarcado de las tarifas de itinerancia, umbral común del IVA, etc.), la Comisión ha acelerado el proceso de adopción de una importante reforma de la Directiva 95/46/CE del 24 de octubre de 1995, la cual se basa en las leyes nacionales de los estados miembros. La reforma que fue propuesta en 2012 es crucial para los actores de este mercado único digital, y ha sido objeto de intensas negociaciones durante todo el proceso legislativo, hasta su publicación en el Diario Oficial de la Unión Europea el 4 de mayo de 2016.[2]

Plasmado en un Reglamento, este tiene la intención de poner fin a las disparidades que aparecieron como resultado de la transposición de la Directiva a las leyes nacionales de los veintiocho (28) estados miembros, e instaurar en todos ellos el mismo alto nivel de protección de los datos personales y derecho a la vida privada.[3]

---

1. La página oficial de esta prioridad de la Unión, disponible en ‹https://ec.europa.eu/priorities/digital-single-market_en›. Consulta: 15 de enero de 2017.
2. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 relativo a la protección de personas físicas con respecto al tratamiento de datos de carácter personal y la libre circulación de estos datos. Disponible en ‹http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC›.
3. Cuya protección está garantizada por el artículo 8 de la Convención Europea de Derechos Humanos

Este ambicioso texto reafirma los principios preexistentes en una nueva forma jurídica, aportando innovaciones significativas, pero a la vez dando nacimiento a algunas ambigüedades.

UN REGLAMENTO CON OBJETIVOS AMBICIOSOS[4]

En un primer momento, el objetivo del Reglamento aparece más en la forma que en la materialidad de sus disposiciones (a). Sin embargo, un análisis más detallado permite descubrir cambios que pueden engendrar consecuencias significativas (b).

Una evolución ampliamente formal de la legislación europea

La contribución más importante de la solución radica probablemente en su naturaleza jurídica. En efecto, al contrario de una Directiva Europea que no obligaba al cumplimiento de sus objetivos por parte de los estados miembros, por suponer únicamente la transposición de sus textos en el derecho interno, el Reglamento pretende ser una ley uniforme. De acuerdo con el artículo 288 del Tratado de funcionamiento de la Unión Europea, un Reglamento "será obligatorio en todos sus elementos y [...] es directamente aplicable en todos los Estados miembros". Por lo tanto, la regulación "produce efectos inmediatos y es, como tal, capaz de crear derechos individuales que los órganos jurisdiccionales nacionales tienen la obligación de proteger".[5]

Este es un punto de gran importancia, dado que una de las debilidades del derecho europeo de protección de datos personales ha sido justamente el estar basado en una Directiva. La Directiva que será reemplazada por el Reglamento desde el 25 de mayo de 2018, no ha generado hasta la fecha una perfecta armonización de las leyes nacionales. Según se especifica en el preámbulo del Reglamento:

> Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en

---

y Libertades Fundamentales del Consejo de Europa, y por el artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea.

4. Primera parte dirigida por Marcel Moritz, MCF HDR.
5. CJCE, 14 de diciembre de 1971, aff. 43/71, Politi; CJUE, 10 de octubre de 1973, aff. 37/73, Fratelli Variola.

> particular en relación con las actividades en línea. Las diferencias en el nivel de protección de los derechos y libertades de las personas físicas, en particular del derecho a la protección de los datos de carácter personal en lo que respecta al tratamiento de dichos datos en los Estados miembros, pueden impedir la libre circulación de los datos de carácter personal en la Unión.[6]

En el fondo, no es sorprendente que muchas disposiciones del Reglamento hayan sido copiadas directamente de la Directiva 95/46/CE. Tal es el caso, por ejemplo, del campo de aplicación material del texto,[7] ya que el Reglamento se aplica al tratamiento de datos personales automatizados, en todo o en parte, así como para los ficheros no automatizados. Pero no se aplica ni para la persecución y sanción de actividades delictivas, ni para la seguridad pública, ni para las actividades domésticas de un individuo.

Las principales definiciones[8] (datos personales, procesamiento, archivo, controlador, etc.) no contienen cambios significativos en comparación con la Directiva de 1995,[9] pues muchos de estos principios han sido transcritos de la Directiva. A modo de ejemplo, el contenido del artículo 5 del Reglamento sobre los principios para el tratamiento de los datos personales no causan sorpresa. Encontramos los principios de legalidad, imparcialidad, transparencia, la limitación, los objetivos, la minimización de datos, precisión, seguridad. Todos estos principios ya fueron instituidos en la Directiva de 1995, y ya constan en las leyes nacionales, en particular el artículo 6 acerca de la calidad de los datos.

Por lo tanto, debemos remarcar a título preliminar una precisión importante: a pesar de que el Reglamento contiene ciento setenta y tres (173) considerandos y noventa y nueve (99) artículos, no constituye un texto que sea en su mayor parte *inédito*. Gran parte de estas disposiciones han estado desde hace mucho tiempo plasmadas en el derecho positivo de los estados miembros de la Unión Europea. La doctrina tiende en consecuencia a limitar el aporte del Reglamento.

> Se detecta en el nuevo Reglamento de la UE, pocas novedades respecto a la orientación previa en la determinación de los derechos de las personas implicadas, y las obligaciones impuestas a los administradores de procesamiento de datos. La armonización europea de-

6. Cons. 9 del Reglamento.
7. Art. 2 del Reglamento.
8. Art. 4 del Reglamento.
9. Sin embargo, hay que tener en cuenta la introducción del concepto de seudonimización, definido en el art. 4 del Reglamento como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

> seada parece más inspirada por el deseo de promover "flujo transfronterizo de datos" entre Estados miembros –entre los cuales en general no existen límites. E incluso a terceros países, con iniciativas de refuerzo para la protección de datos.[10]

En este conjunto muy amplio que constituye la normativa, sí es posible destacar una serie de aportes importantes.

Innovaciones jurídicas con efectos antagónicos

La lectura de los ciento setenta y tres (173) considerandos del Reglamento permite comprender de mejor manera las finalidades del texto, las que podríamos resumir de la siguiente manera: "asegurar un nivel equivalente de protección de personas físicas, y la libre circulación de datos personales a través de la Unión".[11] Esta fórmula ilustra perfectamente el desafío que enfrenta el Reglamento, debiendo a la vez proteger los datos personales de los individuos, y la vitalidad del mercado único en el que estos datos son un recurso valioso.

En consecuencia, el resultado no solo es la afirmación de nuevos derechos para los individuos, sino también el surgimiento de oportunidades sin precedentes para las empresas que en gran medida prestaron su pluma para la redacción de este reglamento.[12] A continuación abordaremos ambos enfoques.

En cuanto a los nuevos derechos asignados a los individuos, el Reglamento refuerza la protección de los "niños",[13] ya que en el entorno de los servicios de la sociedad de la información[14] el consentimiento para un menor de 16 años (o 13 años si la ley del Estado miembro lo permite) debe ser lícito y autorizado por su representante legal.

Más allá de esta categoría específica de personas, el Reglamento instituye varias medidas de protección, particularmente el derecho a la supresión[15] de datos, igualmente calificado por el texto –para nosotros de manera un poco excesiva– como *dere-*

---

10. E. Derieux, "Protection des données à caractère personnel et activités de communication publique Apports du règlement européen du 27 avril 2016 au regard de la précédente directive du 24 octobre 1995 et de la loi française du 6 janvier 1978 (révisée par celle du 6 août 2004)", *Revue Lamy Droit de l'Immatériel*, No. 128 (2016): 15.
11. Cons. 170 del Reglamento.
12. V. especialmente: Y. Eudes, "Très chères données personnelles", en *Le Monde*, 2 de junio de 2013.
13. Art. 8 del Reglamento.
14. Definido conforme a la Directiva No. 98/34/CE: "todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios".
15. Art. 17 del Reglamento.

cho al olvido. Este derecho es aplicable cuando los datos ya no son necesarios, cuando la persona retira su consentimiento, cuando ejerce su derecho de oposición,[16] cuando el tratamiento es ilícito, o cuando la ley impone la supresión de datos en causa.

Entre los aportes significativos podemos citar la consagración de un derecho a la portabilidad de datos,[17] que permite a un individuo exigir la restitución en un formato explotable de los datos que hayan sido transmitidos al responsable del tratamiento automatizado de datos, o aquellos que hubiesen sido transmitidos directamente de un responsable del tratamiento a otro, siempre y cuando sea técnicamente posible. Sin embargo, esta disposición se reserva los derechos y libertades de terceros, por cuanto podrían limitar su aplicación en otras áreas jurídicas, como por ejemplo la propiedad intelectual.

El artículo 22 del Reglamento es igualmente interesante, por cuanto prohíbe –salvo excepciones– que una persona sea objeto de "una decisión basada únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produjeren efectos jurídicos en él, o le afecten de manera significativa de modo similar".[18] El futuro nos revelará cual es el significado preciso de estas disposiciones, las cuales bien podrían ser un límite importante para las actividades de algunas empresas, siempre y cuando una interpretación restrictiva no neutralice su potencial.

Además de las disposiciones enfocadas en proteger a los individuos, algunas de los cuales se acaban de describir brevemente, el Reglamento también establece en muchos aspectos cierta flexibilidad para los responsables del tratamiento. Como se subraya en la doctrina, "una de las principales diferencias entre la directiva de 1995 y el Reglamento radica en la reducción de cargas administrativas para los responsables del tratamiento de datos: las formalidades previas han sido eliminadas en la mayoría de los casos".[19] Es sobre la base de esta lógica que el Reglamento establece el mecanismo de análisis de impacto para tratamientos susceptibles de engendrar un riesgo elevado que afecte los derechos y libertades de las personas físicas,[20] el nombramiento de un delegado para la protección de datos,[21] o también el desarrollo de códigos de conducta[22] y mecanismos de certificación,[23] ambos fuertemente promovidos en el texto.

---

16. Este derecho de oposición está previsto por el art. 21 del Reglamento.
17. Art. 20 del Reglamento.
18. Art. 22 del Reglamento.
19. F. Mattatia, "Synthèse du futur règlement européen sur les données personnelles", *Revue Lamy Droit de l'Immatériel*, No. 126 (2016): 42.
20. Art. 35 del Reglamento.
21. Art. 37 y 39 del Reglamento.
22. Art. 40 y 41 del Reglamento.
23. Art. 42 y 43 del Reglamento.

En resumen, el Reglamento pone gran énfasis en la responsabilidad de los actores económicos que, se supone, deben estar más involucrados en el cumplimiento de sus tratamientos. Si bien es comprensible que "es importante, en particular, que el responsable del tratamiento esté obligado a implementar medidas adecuadas y eficaces, y ser capaz de demostrar que las operaciones son conformes a las establecidas en el presente Reglamento",[24] también es relevante preguntarse si es que asumir una forma de autocontrol podría ser peligroso. La ambigüedad del Reglamento podría abrir la puerta para posibles incertidumbres jurídicas.

UN REGLAMENTO FUENTE DE INCERTIDUMBRES JURÍDICAS[25]

La voluntad de asegurar un nivel excepcional de protección en los veintiocho (28) estados, pero sin comprometer el desarrollo de los mercados clave para la Unión, dio lugar a un texto ambiguo, que afecta tanto al alcance del texto (a), como su función unificadora del Derecho (b).

Un texto en el que el radicalismo frecuenta un enfoque basado en el riesgo

La primera parte de este estudio demostró que el Reglamento tiende a desarrollar un nivel muy elevado de protección, añadiendo nuevos derechos y obligaciones al edificio construido por la Directiva de 1995, los cuales son ahora directamente aplicables en los estados miembros.

La consagración de un "derecho al olvido" (art. 17),[26] el reconocimiento de un principio de minimización de los datos recogidos (art. 5-1, c), o la protección de datos desde el diseño (art. 25), así como penas más severas, bien podrían revelar una postura radical[27] en algunos de los redactores del Reglamento. Si bien, a priori, este enfoque pretender hacer de la Unión Europea un territorio excepcional de protección

24. Cons. 74 del Reglamento.
25. Segunda parte dirigida por Valentin Gibello, doctorante (CERAPS, UMR 8026).
26. De hecho, es una variación del derecho a la supresión de datos que ya incluía la directiva de 1995.
27. Sobre la concepción maximalista de la protección de derechos fundamentales, ver: E. Brems, "Droits humains, étrangers et multiculturalisme: pour une approche maximaliste et inclusive des droits fondamentaux", *Revue Trimestrielle des Droits de l'Homme*, vol. 82 (2010): 237-49.

del derecho a la vida privada, algunos ya están preocupados por la posibilidad de que el Reglamento no esté a la altura de sus propias ambiciones.[28]

Pero, sin prejuzgar los futuros efectos del Reglamento y de los méritos de este enfoque, es conveniente encontrar la esencia real del texto, con la finalidad de investigar su verdadero alcance más allá de la enunciación de principios. Sin embargo, una ambigüedad importante radica en la coexistencia, por un lado, del reconocimiento de un vasto conjunto de derechos y obligaciones, y por el otro, de la implementación de métodos de gestión de riesgos.

De esta manera, el responsable del tratamiento está obligado a proceder a la supresión de datos "teniendo en cuenta la tecnología disponible, y el coste de su implementación" (art. 17-2). Del mismo modo, los principios cardenales del Reglamento, el de responsabilidad (art. 24), de protección de datos desde el diseño (art. 25), o los de seguridad del tratamiento (art. 32), se ejercen "a la luz de su naturaleza, su alcance, su contexto y los propósitos del tratamiento así como sus riesgos, considerando que su nivel de probabilidad y gravedad varía de acuerdo a los derechos y libertades de las personas físicas".

Estas limitaciones, así como la importancia que el Reglamento otorga a las nociones de "responsabilidad" y "análisis de riesgos" (art. 35),[29] revelan la opción tomada por sus redactores de utilizar un enfoque de riesgos (risk-based approach), una opción que no es neutral para la protección efectiva del derecho fundamental a la vida privada.

Unánimemente adoptada por todas las delegaciones que contribuyeron a la elaboración del texto, y al tenor de los instrumentos de trabajo interinstitucionales,[30] el enfoque fundado sobre los riesgos es directamente una copia del modelo legislativo anglosajón. Desarrollado en el Reino Unido en los años 1990,[31] bajo la presión correguladora de las empresas, sobre todo del sector financiero, la cual permanece en el corazón de la política legislativa británica desde la New Labour.[32]

---

28. G. Desgens-Pasanau, "RGPD: entre incertitudes et occasions manquées", *Dalloz IP/IT*, No. 77 (2016): 335-9.
29. La cual debe contener "una evaluación de los riesgos para los derechos y libertades de los interesados [...]" y "las medidas previstas para afrontar los riesgos [...]".
30. Consejo de la Unión Europea, Secretaría General del Consejo, Archivo Interinstitucional 2012/0011 (COD), 2 de septiembre de 2014, Bruselas. Disponible en ‹http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012267%202014%20REV%202›. Consulta: 10 de enero de 2017.
31. Ver en M. Moran, "Understanding the Regulatory State", *British Journal of Political Science* 32, No. 2 (2002): 391-413.
32. Ver el reporte encargado por el Gobierno, P. Hampton, *Reducing administrative burdens: effective inspection and enforcement*, HMSO, 2005, cuyos principios han sido integrados en el Código Re-

Esta concepción de cómo hacer el Derecho presume el fracaso de las regulaciones clásicas, las cuales contemplaban una carga insoportable de formalidades para las empresas, y por lo tanto constituirían un impedimento importante para el desarrollo económico. Este elemento de discurso, que hizo consenso durante las negociaciones, es cuestionable por varias razones. En primer lugar, cabe considerar que la realidad misma de las potenciales economías[33] no es suficientemente establecida,[34] y el argumento es frecuentemente manejado por los grupos de presión a favor de una regulación "dúctil" y "flexible", en pocas palabras, menos restrictiva.

La transición hacia un enfoque basado en el riesgo es promovida por el Reglamento, incluyendo requisitos de documentación, y llevar a cabo evaluaciones de impacto, lo cual lógicamente incrementaría los costos de desarrollo.[35] Sobre la base de esta hipótesis, el *risk-based approach* recomienda dejar a los actores económicos modular la intensidad de sus obligaciones, de acuerdo a los riesgos de una actividad dentro de un contexto definido.

Traducido al derecho a la protección de datos personales, esto significa que será necesario que el responsable de un tratamiento de datos que presente riesgos elevados que atenten contra el derecho de la vida privada de las personas, esté obligado a invertir más recursos para su cumplimiento (mayor seguridad, protección de datos por diseño, nombrar a un RPD, análisis de impacto, etc.).

En contraste, el tratamiento de datos con menor riesgo conlleva a un menor peso de obligaciones para el responsable del tratamiento. ¿Es tal enfoque realmente adaptable a la protección de un derecho fundamental como es el derecho a la vida privada? En nombre del pragmatismo, ¿ha cedido el Reglamento ante grupos de poder comprometiendo la posibilidad de llegar a establecer una protección eficaz y uniforme del derecho a la vida privada en la Unión?

Podemos preocuparnos acerca de si este método es adecuado para asegurar la protección del derecho individual a la vida privada, al no involucrar al Estado.[36] El cumplimiento basado en el riesgo deja que los responsables del tratamiento evalúen los

---

gulador. Disponible en ‹https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/300126/14-705-regulators-code.pdf›. Consulta: 10 de enero de 2017.

33. 2,3 millones de euros de economía para los actores económicos, según la Comisión, ver: London Economics, *Implications of the European Commission's proposal for a general data protection regulation for business - Final report to the Information Commissioner's Office*, mayo de 2013, vii.
34. Lo demuestran las conclusiones del informe de la agencia de protección de datos inglesa, l'ICO, ibíd.
35. Los "*compliance costs*", como se destacó por parte de la delegación holandesa en el mencionado documento de trabajo: Council of the European Union, 97.
36. Recordando el rol principal del Estado en la protección del derecho a la vida privada: J. J. Lavenue,

riesgos de las personas afectadas, a pesar de que el enfoque de riesgos tal como se utiliza en todas otras áreas, consiste en identificar los riesgos para la propia empresa y responder con los recursos disponibles. Determinar los riesgos de la privacidad de las personas afectadas es un asunto discutido, pero no sin consecuencias. De hecho, los riesgos son diferentes en su naturaleza y el alcance de manera individual, y cada persona tiene la facultad de determinar los límites de su vida privada.[37]

Es también lamentable que el Reglamento se fundamente en la búsqueda de un compromiso entre el derecho a la vida privada y las prioridades económicas de las empresas. Si bien es necesario establecer un equilibrio, este debería ser entre el derecho fundamental específico y otros derechos fundamentales con los cuales podría entrar en conflicto, incluida la libertad de expresión o el derecho a la información. En términos más generales, podemos evaluar este cambio como una transición sutil del derecho a la vida privada, hacia un derecho a la *privacy*, y su lógica anglosajona de carácter mercantil, que sugiere la vacilación constante entre el Reglamento y el enfoque patrimonial y extra patrimonial de la noción sobre los datos de carácter personal.[38]

Acerca de las objeciones presentadas en contra de este método, el grupo de trabajo del artículo 29 (G29) tuvo la precaución de contestar el 30 de mayo de 2014,[39] destacando por encima de todo, lo que ya estaba presente en la Directiva de 1995.[40] Sin embargo, el G29 defiende un diseño totalmente diferente al de las fuerzas del *lobbying*, y considera al enfoque basado en el riesgo como la forma de *aumentar* las obligaciones del responsable del tratamiento de riesgos, aplicando lo mismo para los tratamientos que juzga como "de bajo riesgo".[41]

Además de estar –a partir de ahora– impuesto a los estados miembros, y generalizado en todo el derecho de protección de datos, el enfoque basado en el riesgo que irriga el Reglamento, no logró de alguna manera disuadir los votos de la G29. Está previsto por ejemplo, que las obligaciones ante cualquier violación de los datos personales (art. 33 y 34) no se apliquen a los tratamientos de bajo riesgo. Dada la falta

---

C. Codron, N. Desrumeaux y G. B. Hamerel, "Privacy by design ou Privacy by law", *Revue Droit international, Commerce, Innovation et Développement*, No. 2 (2012): 77-104.

37. Ver sobre este punto: B. Beigner y J. Antippas, "La protection de la vie privée", en *Libertés et droits fondamentaux* (París: Dalloz, 2015), 239.
38. Sobre esta diferencia, ver: C. Wolf y M. Winston, "So Close, Yet o Far Apart: The EU and US Visions of a New Privacy Framework", *Antitrust* 26, No. 3 (2012).
39. Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", No. 14/EN WP 218, adoptado el 30 de mayo de 2014.
40. Principalmente en las obligaciones de seguridad de datos del art. 17.
41. Art. 29 Data Protection Working Party, ibíd.

de definición del concepto de "riesgo" en el Reglamento,[42] ya se puede cuestionar el alcance real de muchos de los derechos y obligaciones establecidos.

En la práctica, las consecuencias para la protección de la vida privada dependerán del equilibrio necesario entre el deseo de pragmatismo que promueva el control a posteriori, de los mecanismos de regulación menos verticales, y la fuerza vinculante del Reglamento, que representan el aumento de las sanciones y la supervisión del rol de las agencias de protección de datos. Otra ambigüedad mayor será la capacidad de armonizar el derecho de este Reglamento Europeo, directamente en peligro por su contenido mismo.

Una voluntad de armonización contradicha en el texto

De hecho, a pesar de la extrema longitud del texto (173 considerandos, 99 artículos) y las redundancias que contiene, persisten muchas incertidumbres cuya resolución necesita de un trabajo consistente de interpretación.

En primer lugar, los estados pueden introducir en diversos entornos, normas nacionales diferentes a las del Reglamento, en el sentido de una mayor protección de las personas afectadas. Las disposiciones relativas al tratamiento de los datos biométricos son un ejemplo notable, tomando en cuenta el gran crecimiento de su utilización (seguridad de pagos, lucha contra el terrorismo, identidad digital).

Desde el punto de vista económico, el Reglamento se aplica para establecer un régimen *a minima*, según el cual los datos biométricos adoptan la calificación de los datos sensibles en el sentido del artículo 9, y, por lo tanto, su tratamiento está en principio prohibido. Este principio de prohibición va acompañado inmediatamente de una decena de excepciones, incluyendo el consentimiento explícito de la persona interesada. En este punto, el Reglamento ya admite que la legislación nacional de un Estado miembro pueda neutralizar dicha excepción.[43]

Además de obtener el consentimiento, el responsable de un tratamiento de datos biométricos deberá, a priori, cumplir con el procedimiento de "consulta previa" sobre la base del análisis de impacto requerido por el artículo 36 e interpretado por el delegado de protección de datos, cuyo nombramiento se hace entonces obligatorio (art. 37). Esto sin tomar en cuenta el artículo 9-4, que añade: "Los Estados miembros podrán mantener o establecer condiciones adicionales, incluyendo limitaciones, en

42. A lo sumo, el considerando 75 establece algunas indicaciones.
43. Art. 9-2, a) del Reglamento.

cuanto al tratamiento de datos genéticos, datos biométricos o datos relativos la salud". En otras palabras, los legisladores nacionales pueden añadir otros requisitos, tales como, prohibir por completo el procesamiento de datos biométricos.

Esta disposición lejos de ser una oportunidad para mejorar la protección del derecho a la vida privada en relación a los riesgos del uso de la tecnología, conlleva a renunciar al efecto de la unificación del Derecho propio de este instrumento. La capacidad de la Unión Europea para edificar un frente común en materia de protección de datos personales condiciona directamente la efectividad de esta protección. Por otra parte, una flexibilidad de tal magnitud allana el camino para la adopción de disposiciones nacionales imprecisas y ambiguas, como es el caso de las iniciativas francesas recientes.[44]

Además de estas disposiciones sobre la biometría, existe la posibilidad de que los estados miembros se desvíen del Reglamento con respecto a las reglas de licitud del tratamiento (art. 6), las disposiciones aplicables al trabajo (art. 90), la definición de tratamiento que requiere de una evaluación de impacto (art. 35-3), el uso del número de identificación nacional (art. 87), o la edad de consentimiento para menores al tratamiento de sus datos (art. 8-1).

Por otra parte, el Reglamento es objeto de críticas tanto de representantes y especialistas de la industria digital, en cuanto la falta de precisión de ciertas nociones[45] cuya importancia operativa es grande. Así que ¿cuáles son los criterios para evaluar la noción de "alto riesgo", que se utiliza en varios lugares de la conciliación? ¿Desde qué momento es implementado un tratamiento de datos "a gran escala", e impone nuevas responsabilidades al responsable del tratamiento? ¿Se pretende aplicar el derecho al olvido establecido en el artículo 17 a los motores de búsqueda, en la línea que marcó la sentencia del 13 de mayo de 2014 en el caso de Google España?[46] ¿Cuál es el perímetro del nuevo derecho a la portabilidad de los datos establecido en el artículo 20?

---

44. De hecho, la aprobación en el Senado de la ley "*pour une République numérique*" vio un nuevo intento de introducir medidas restrictivas para el tratamiento de datos biométricos, los cuales, mal concebidos, conllevarían en definitiva a bajar el nivel de protección de los franceses con respecto a la biometría, dicha "*de service*".
45. Tomaremos como prueba las contribuciones a la consulta abierta por la CNIL en vista de los trabajos para la aplicación del Reglamento en 2018. Ver la síntesis en esta dirección: ‹https://www.cnil.fr/sites/default/files/atoms/files/resultats_de_la_consultation_publique_reglement_0.pdf›. Consulta: 11 de enero de 2017.
46. CJUE, grande chambre, 13 de mayo de 2014, *Google Spain SL*, C-131/12. E. Brunet, "Règlement général sur la protection des données à caractère personnel-Genèse de la réforme et présentation globale", *Dalloz IP/IT*, No. 12 (2016): 567-72.

CONCLUSIONES

El Reglamento Europeo (UE) 2016/679 deja muchas interrogantes que requerirán de un largo trabajo de interpretación, lo que determinará su alcance real y su función armonizadora. El riesgo es que este trabajo se realice en primer lugar a nivel nacional y que se mantengan las diferencias en los enfoques que existían entre las agencias europeas de protección de datos en el ámbito de la Directiva de 1995. No obstante, la duda permanecerá acerca de su capacidad para lograr una concepción unificada y protectora del derecho a la vida privada en todos estos puntos, mediante el establecimiento del Comité Europeo de Protección de Datos creado en el artículo 68.

Cabe agregar que el equilibrio de este nuevo marco legal se fundamenta en la disuasión y el carácter verosímil de las sanciones que proporciona. Está diseñado para evitar abusos en la aplicación del principio de la responsabilidad y la lógica de control a posteriori. Por otro lado, existen pocas garantías para protegerse contra las diferencias excesivas en la aplicación de sanciones económicas por parte de las agencias de protección de datos. No hay ninguna indicación de que el Reglamento pondrá fin a la situación actual, en la cual coexisten en la Unión Europea algunas agencias reacias, como es la CNIL francesa,[47] o, por el contrario, más flexibles como la Agencia Española de Protección de Datos (AEPD).

Aparte de las sanciones, el Reglamento se apoya fuertemente en el proceso de certificación (etiquetas, códigos de conducta), que constituyen de igual manera una clave para la aplicación efectiva del principio de protección de datos. No obstante, podemos dudar de las posibilidades de lograr una política armonizada en la materia, por cuanto la regulación mantiene un nivel de certificación nacional (art. 42).

De manera más general, por la falta de éxito de la certificación nacional hasta el momento, y la falta de incentivo real para usarlo en la regulación, la armonización de la política de certificación podría incluso llegar a ser un asunto secundario.[48]

El nuevo Reglamento General sobre la protección de datos, que estará vigente a partir del 25 de mayo de 2018, la ley común de la Unión Europea en esta materia, está

---

47. Según el reporte anual de 2016, solamente tres sanciones pecuniarias han sido pronunciadas por la CNIL, que prefiere un enfoque pedagógico basado en gran parte sobre la actividad informática correspondiente y las libertades, que reemplazarán al *oficial de protección de datos*.
48. Sobre este punto, ver: O. Tambou, "L'introduction de la certification dans le règlement général de la protection des données personnelles: quelle valeur ajoutée?", *Revue Lamy droit de l'immatériel* 5, No. 126 (enero 2016): 43-48; E. Lachaud, "Why the certification process defined in the General Data Protection Regulation cannot be successfu", *Computer Law & Security Review* 32, No. 6 (diciembre de 2016): 814826.

impregnado de tantas ambigüedades como ambiciones. Una lectura profunda de sus numerosas disposiciones, altamente protectoras a priori del derecho fundamental a la vida privada, revela un pragmatismo de concesiones hechas a los actores económicos. Será misión de las instituciones de protección de datos nacionales y europeas, el encontrar la manera de evitar abusos a través de un arduo trabajo de interpretación en la práctica.

BIBLIOGRAFÍA

Beigner, B., y J. Antippas. "La protection de la vie privée". *Libertés et droits fondamentaux*. Paris (2015).

Brems, E. "Droits humains, étrangers et multiculturalisme: pour une approche maximaliste et inclusive des droits fondamentaux". *Revue Trimestrielle des Droits de l'Homme*, vol. 82 (2010).

Derieux, E. "Protection des données à caractère personnel et activités de communication publique Apports du règlement européen du 27 avril 2016 au regard de la précédente directive du 24 octobre 1995 et de la loi française du 6 janvier 1978 (révisée par celle du 6 août 2004)". *Revue Lamy Droit de l'Immatériel*, No. 128 (2016).

Desgens-Pasanau, G., "RGPD: entre incertitudes et occasions manquées". *Dalloz IP/IT*, No. 7 (2016).

Lachaud, E., "Why the certification process defined in the General Data Protection Regulation cannot be successful". *Computer Law & Security Review* 32, No. 6 (2016).

Lavenue, J.-J., C. Codron, N. Desrumeaux y G. B. Hamerel. "Privacy by design ou Privacy by law". *Revue Droit international, Commerce, Innovation et Développement* (2012).

London Economics. *Implications of the European Commission's proposal for a general data protection regulation for business - Final report to the Information Commissioner's Office*, 2013.

Mattatia, F. "Synthèse du futur règlement européen sur les données personnelles". *Revue Lamy Droit de l'Immatériel*, No. 126 (2016).

Wolf, C., y M. Winston. "So Close, Yet o Far Apart: The EU and US Visions of a New Privacy Framework". *Antitrust* 26, No. 3 (2012).

Fecha de recepción: 7 de febrero de 2017
Fecha de aprobación: 31 de mayo de 2017