

Título	Privacidad y protección de datos
Documento	Doc. Prel. N.º 10 de agosto de 2021
Autor	Oficina Permanente
Punto de la agenda	Punto 10.i.
Mandato(s)	C&R N.º 36 del CAGP de 2019
Objetivo	Exponer los posibles problemas relacionados con la privacidad y la protección de datos en el funcionamiento del Convenio sobre la Apostilla
Medida que debe adoptarse	Decisión <input checked="" type="checkbox"/> Aprobación <input type="checkbox"/> Para debate <input type="checkbox"/> Acción / finalización <input type="checkbox"/> Para información <input type="checkbox"/>
Anexos	No constan
Documentos relacionados	No constan

Índice

I.	Introducción.....	1
II.	Marco del Convenio e implicaciones prácticas.....	1
III.	Propuesta de la Comisión Especial	3

Privacidad y protección de datos

I. Introducción

- 1 Cuando se elaboró el Convenio sobre la Apostilla, las complejas cuestiones de privacidad y protección de datos a las que se enfrenta la comunidad mundial en la actualidad no podían contemplarse. La utilización cada vez mayor de las tecnologías de la información sigue generando cantidades de datos sin precedentes, que deben ser recogidos, tratados y conservados. Esto ha impulsado a reforzar los marcos normativos en materia de privacidad y a elaborar nuevos regímenes normativos en materia de protección y conservación de datos¹.
- 2 Estas tendencias jurídicas y tecnológicas afectan a todos los sectores y disciplinas, y el funcionamiento del Convenio sobre la Apostilla no constituye ninguna excepción. Estos avances son especialmente importantes en el contexto del Programa de la Apostilla electrónica (e-APP), ya que con la expedición de e-Apostillas y el mantenimiento de e-Registros se recogen, tratan y conservan datos de forma digital.
- 3 Durante la reunión de mayo de 2021 del Grupo de Expertos sobre el e-APP y las nuevas tecnologías, el Grupo abordó el tema de la privacidad y la protección de datos en relación con el e-APP y señaló que la posible interacción entre los marcos normativos y las disposiciones del Convenio podría justificar la continuación del debate en la Comisión Especial².
- 4 Si bien se reconoce que el cumplimiento tanto del Convenio como de los marcos normativos aplicables es responsabilidad y prerrogativa de cada una de las Partes contratantes, el presente documento expone una serie de cuestiones que deben tenerse en cuenta en cada etapa del proceso de expedición y verificación de la Apostilla.

II. Marco del Convenio e implicaciones prácticas

- 5 Las Apostillas no contienen ninguna información personal. Los 10 términos estándar numerados están relacionados con el documento en cuestión y con la autoridad certificadora. Sin embargo, el proceso de expedición requiere naturalmente que se recojan algunos datos adicionales, lo que puede suscitar ciertos problemas en materia de privacidad y protección de datos.
- 6 Para expedir una Apostilla conforme al artículo 3, la Autoridad Competente recoge información del solicitante, tanto de carácter personal como sobre el documento público que debe apostillarse. Si bien la Autoridad Competente tiene la facultad de determinar cómo hacerlo, la recogida, el tratamiento y la conservación de los datos tal vez se rijan por regímenes de protección de datos, independientemente de que las solicitudes se presenten por vía electrónica o en papel.
- 7 Para certificar el origen del documento público en cuestión, la mayoría de las Autoridades Competentes utilizan una base de datos con muestras de firmas, sellos y timbres, con las que se puede verificar el origen del documento público³. La información personal del firmante que se conserva con este fin suele estar relacionada únicamente con quienes actúan en calidad de funcionarios, por lo que es poco probable que suscite problemas en materia de privacidad o protección de datos.

¹ Véase, p. ej. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Unión Europea).

² Véase el Doc. Prel. N.º 6 de mayo de 2021, "Informe de la presidencia del Grupo de Expertos sobre el e-APP y las nuevas tecnologías", Anexo I, párr. 12.

³ Véase el Doc. Prel. N.º 2 de agosto de 2021, "Resumen de respuestas al Cuestionario sobre la Apostilla", párr. 26 y sig.

- 8 Una vez expedida, la Apostilla no debe compartirse con más personas que el solicitante. En el caso de las solicitudes presenciales, esto se traduce en la verificación de la identidad del solicitante. En un contexto electrónico, puede suponer un procedimiento de entrega o transmisión segura.
- 9 Una vez expedida la Apostilla, el artículo 7 exige que las Autoridades Competentes consignen en un "registro o fichero" cierta información sobre las Apostillas que expiden:
- a. el número de orden y la fecha de la Apostilla; y
 - b. el nombre del signatario del documento público y la calidad en que haya actuado o, para los documentos no firmados, la indicación de la autoridad que haya puesto el sello o timbre.
- 10 En la actualidad, las Autoridades Competentes de más de un tercio de las Partes contratantes llevan e-Registros que permiten la verificación de Apostillas en línea⁴. La mayoría lleva registros que no están disponibles al público ni en formato electrónico ni en papel. Independientemente de la forma del registro o de su accesibilidad, el ingreso y la conservación de los datos a efectos del artículo 7 pueden dar lugar a una serie de consideraciones en materia de privacidad y protección de datos.
- 11 La primera consideración se refiere al tipo de información que se registra (es decir, los datos que se conservan). Los requisitos de registro del artículo 7(1)(a) son de carácter general y los del artículo 7(1)(b) están relacionados con las personas que actúan en calidad de funcionarios, ninguno de los cuales plantea problemas en cuanto a la privacidad o la protección de datos. Sin embargo, las Autoridades Competentes pueden registrar información adicional sobre la solicitud y/o el solicitante. Por ejemplo, puede que algunas Autoridades Competentes conserven una imagen o copia del documento público en cuestión. Aunque esta práctica facilita la experiencia del usuario del e-Registro, el documento público tal vez contenga información personal o delicada⁵. Dependiendo de la naturaleza de la información, esto puede dar lugar a problemas en materia de privacidad o protección de datos, por ejemplo, si el solicitante debe prestar su consentimiento expreso para la recogida y conservación de sus datos personales (y si ese consentimiento puede ser revocado y de qué manera).
- 12 La segunda consideración de importancia es la seguridad. Si bien el texto del artículo 7(2) invita a solicitar la verificación de la Apostilla a "cualquier interesado", en la práctica generalmente se considera que esto se refiere al solicitante y al destinatario o destinatarios de la Apostilla. El registro no debería poder ser consultado por personas que no tengan acceso a la Apostilla en cuestión ni la necesidad de verificar su autenticidad. En este contexto, el Foro sobre el e-APP ha destacado la importancia de evitar la "caza de información" (*fishing expeditions*) (es decir, intentos de los usuarios de un e-Registro de obtener acceso a Apostillas que no han recibido o información sobre las mismas) mediante numeración aleatoria o la exigencia de un código independiente⁶.
- 13 La tercera consideración trata del período de conservación de los datos. El Convenio no impone ningún plazo en cuanto a la validez de una Apostilla, ni tampoco impone un plazo determinado para la conservación de datos en el registro. Esto significa que las Apostillas no caducan y son válidas mientras permanezcan identificables y unidas al documento público en cuestión⁷. En consecuencia, los registros que llevan las Autoridades Competentes deben poder ofrecer la verificación de estas Apostillas. En la Comisión Especial se ha señalado anteriormente que

⁴ Véase la "Tabla de puesta en práctica del e-APP" en la Sección Apostilla del sitio web de la HCCH < www.hcch.net >.

⁵ La relevancia de las leyes de protección de datos en el contexto de la visualización de los documentos públicos (y/o Apostillas) en un e-Registro fue señalada ya en el 2012 en el Foro sobre el e-APP (véase 11(c) del Séptimo Foro (Esmirna)), y ha sido reiterada en múltiples ocasiones desde entonces: véase, por ejemplo, la CyR N.º 28 del Décimo Foro (La Haya) (refrendada por la C&R N.º 21 de la CE de 2016).

⁶ Véase la CyR N.º 29 del 10.º Foro (La Haya) (refrendada en la CyR N.º 21 de la CE de 2016).

⁷ El hecho de que las Apostillas no caducan ha sido reconocido por el Foro sobre el e-APP. Véase CyR N.º 23 del 10.º Foro (La Haya) (refrendada en la C&R N.º 21 de la CE de 2016).

corresponde a cada Parte contratante formular criterios objetivos sobre el tiempo que deben conservarse los registros de Apostillas⁸. Con la introducción de los e-Registros, la recomendación ha evolucionado, por lo que se anima a las Partes contratantes a dar acceso a los registros en línea durante "el mayor tiempo posible"⁹.

- 14 Esta conservación semipermanente de los datos puede plantear problemas en materia de protección de datos si el registro contiene el documento público en cuestión, en particular en las jurisdicciones en las que la conservación de los datos privados de una persona está prohibida si no media consentimiento expreso. Puede surgir un problema semejante en el marco de regímenes de protección de datos en los que una persona puede revocar su consentimiento, como en el contexto del "derecho de supresión" o "derecho al olvido" del Reglamento General de Protección de Datos de la Unión Europea¹⁰.
- 15 Al menos una Parte contratante ha señalado que los posibles conflictos en este contexto se resuelven permitiendo a los solicitantes de Apostillas decidir si el contenido del documento público será o no visible en el registro y, en caso afirmativo, precisar que se lo debe eliminar después de determinado tiempo¹¹.
- 16 En resumen, si bien las Apostillas en sí no contienen información personal del solicitante, pueden estar asociadas a información confidencial, dependiendo de las prácticas de las Autoridades Competentes. Las Partes contratantes deben considerar cuidadosamente qué información deberá registrarse a efectos de archivo interno, cuál será accesible al público a través de un e-Registro, durante cuánto tiempo se conservarán esos registros, así como las implicaciones en materia de privacidad o protección de datos en la jurisdicción pertinente.

III. Propuesta para la Comisión Especial

- 17 Se invita a la Comisión Especial a que estudie si se necesitan orientaciones adicionales en relación con la intersección del funcionamiento del Convenio y de los regímenes de privacidad y protección de datos vigentes.
- 18 Se invita a las Partes contratantes a que informen a la Oficina Permanente de los desafíos que hayan surgido en el contexto de la privacidad y la protección de datos, así como de las prácticas o procedimientos que se hayan establecido para resolverlos.

⁸ Véase la CyR N.º 21 de la CE de 2003. Cabe señalar que este debate se produjo en el contexto de las Partes contratantes que llevaban registros en papel, o registros electrónicos en discos compactos con capacidad limitada.

⁹ Véase la CyR N.º 33 del 10.º Foro (La Haya) (refrendada en la CyR N.º 21 de la CE de 2016).

¹⁰ Reglamento General de Protección de Datos, art. 17. El RGPD también prevé un número limitado de excepciones al derecho de supresión (véase el art. 17(3)).

¹¹ Estonia informó de esta práctica durante la reunión de mayo de 2021 del Grupo de Expertos sobre el e-APP y las nuevas tecnologías. Para más información, véase la Cámara de Notarios de Estonia, *What is an e-Apostille, Certification of Public Documents by Apostille* (Qué es una Apostilla electrónica, certificación de documentos públicos mediante Apostilla), disponible en el sitio: < <https://www.notar.ee/en/teabekeskus/apostille> >.