Parlamento Europeo
2014-2019

Comisión de Libertades Civiles, Justicia y Asuntos de Interior

1.4.2019

SEXTO DOCUMENTO DE TRABAJO (B)

sobre la propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal (2018/0108 (COD)) – Salvaguardias y vías de recurso

Comisión de Libertades Civiles, Justicia y Asuntos de Interior

Ponente: Birgit Sippel

Coautor: Romeo Franz

II. Salvaguardias *ex ante*

Una vez analizada la propuesta en lo que se refiere a la notificación del interesado, el presente documento de trabajo examinará las salvaguardias que deben garantizarse antes de que se obtengan y se transfieran los datos al Estado solicitante (las salvaguardias *ex ante*).

Dado que la cuestión de la autenticación previa del EPOC-PR por parte del proveedor de servicios (que garantiza que una autoridad judicial competente ha emitido realmente un EPOC-PR) ya se ha examinado en profundidad en el tercer documento de trabajo[1], este documento solo se centrará en las garantías *ex ante* con respecto a terceros y en las relacionadas con el procedimiento de ejecución.

1. Terceros afectados[2]

Es casi inevitable que incluso una utilización de EPOC específicos conlleve una recopilación accidental de datos de las personas con las que se haya comunicado la persona afectada inicialmente, es decir, el sospechoso o el acusado. Algunos de estos datos pueden ser pertinentes para la investigación, mientras que otros no lo serán. En consecuencia, se deben aplicar unas normas estrictas, que garanticen el pleno respeto de los derechos fundamentales y de los principios en materia de protección de datos, a la conservación, entrega y difusión no solo de los datos de los interesados, sino también de los datos de terceros (incluida la seguridad de los datos). Sin embargo, hasta la fecha no se han tenido en cuenta ni se han abordado adecuadamente las cuestiones relativas a la conservación, la difusión y la seguridad de los datos recopilados. Además de acordar un enfoque común elemental con miras a proteger adecuadamente los datos frente a piratas informáticos y otros agentes malintencionados, es necesario establecer un conjunto claro de normas y procedimientos que determinen la duración de la conservación de los datos recopilados, con quién pueden compartirse y con qué fines, antes de que los datos se recopilen y transfieran al Estado solicitante.

2. Notificación y posible reacción de las autoridades en el Estado de ejecución

Otro elemento importante en relación con las salvaguardias *ex ante* es la cuestión de una mayor participación de las autoridades del Estado de ejecución, incluida una notificación exhaustiva sobre un EPOC-PR y la posibilidad de una reacción significativa, o incluso de una autorización previa. Esta cuestión ya se ha destacado en varios de los documentos de trabajo precedentes. Este derecho automático de la autoridad de ejecución a reaccionar no está previsto actualmente en la propuesta de Reglamento. Si bien en el artículo 14, apartado 4, letra f), y apartado 5, letra e), se establece que un proveedor de servicios podría no cumplir un EPOC-PR si «se desprende que es claramente contrario a la Carta de los Derechos Fundamentales de la Unión Europea o manifiestamente abusivo», estas disposiciones presuponen que el proveedor de servicios no ha cumplido un EPOC-PR. Solo en ese momento

[1] Véase también el Dictamen n.º 28/2018 del Bundesrechtsanwaltskammer (BRAK - Colegio de Abogados Federal), que hace referencia también a la necesidad de transmitir más datos a los proveedores a tenor de lo dispuesto en el artículo 5 de la Directiva OEI.

[2] El acceso a datos de terceros que no sean sospechosos debe producirse en condiciones aún más estrictas y debe limitarse a casos excepcionales, por ejemplo, en relación con la protección de intereses vitales de seguridad nacional, defensa o seguridad pública.

desempeñarían un papel activo las autoridades del Estado de ejecución.

No obstante, la única solución lógica para garantizar el respeto de la jurisprudencia actual del Tribunal Europeo de Derechos Humanos (TEDH) y de las obligaciones de los Estados miembros parece ser una mayor participación del Estado de ejecución[3]. Esa posibilidad de notificación y reacción podría seguir el modelo del artículo 31 de la Directiva OEI y de los motivos de denegación del reconocimiento enumerados en el artículo 11 de dicha Directiva, y podría adaptarse a las distintas categorías de datos.

Por lo que se refiere a los datos de los abonados y los datos relativos al acceso, esta mayor participación podría estipular que un EPOC-PR deba enviarse de forma automática y al mismo tiempo al proveedor de servicios y a la autoridad del Estado de ejecución; esta dispondría de un plazo determinado para formular objeciones al EPOC-PR sobre la base de los motivos de denegación del reconocimiento contemplados en el artículo 11 de la Directiva OEI[4]. De esta forma, en lugar de solicitar la confirmación de un EPOC-PR por las autoridades del Estado de ejecución, los EPOC-PR sobre los datos de los abonados y los datos relativos al acceso otorgarían al Estado de ejecución el derecho a reaccionar negativamente.

Por lo que se refiere a las categorías de datos más sensibles, es decir, los datos de transacciones y los datos de contenido, un régimen de participación reforzado puede exigir obligaciones más estrictas, por ejemplo una decisión favorable y, por lo tanto, una confirmación del Estado de ejecución de un EPOC-PR con anterioridad a la entrega o la conservación de los datos[5].

Por otra parte, por lo que respecta al texto de la cláusula sobre los derechos fundamentales, no debe utilizarse la formulación muy imprecisa de la propuesta de la Comisión, a saber, «es claramente contrario a la Carta de los Derechos Fundamentales de la Unión Europea», sino la definición contemplada en el artículo 11, apartado 1, letra f), de la Directiva OEI: «cuando existan motivos fundados para creer que la ejecución de la medida de investigación indicada en la OEI sería incompatible con las obligaciones del Estado de ejecución de conformidad con el artículo 6 del TUE y la Carta».

Es esencial retomar la misma formulación de la Directiva OEI para poner fin al mosaico actual de cláusulas de los distintos instrumentos jurídicos de reconocimiento mutuo de la UE y la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE)[6]. Aunque, con el tiempo, se ha puesto de manifiesto que una cláusula sobre los derechos fundamentales clara es

[3] Véase el documento de trabajo n.º 3.

[4] Por lo que respecta al recurso al artículo 11 de la Directiva OEI, véase también la posición del Consejo de la Abogacía Europea (CCBE), de 19 de octubre de 2010, sobre la propuesta de la Comisión.

[5] La orientación general del Consejo no resuelve el problema con la introducción de un nuevo artículo 7 bis, que prevé la notificación para los datos de contenido si la persona en cuestión es nacional del Estado de ejecución. No prevé una prerrogativa clara del Estado de ejecución para intervenir, ya sea de forma negativa (plazo determinado para reaccionar) o de forma favorable (decisión de autorización). El Estado de emisión solo podrá tener en cuenta las posibles objeciones en un número muy limitado de casos. Véanse también las recomendaciones del CCBE, de 28 de febrero de 2019, sobre las pruebas electrónicas.

[6] Véanse, por ejemplo, tan solo una referencia general en el artículo 1, apartado 3, de la Decisión Marco 2002/584/JAI sobre la orden de detención europea y las cláusulas explícitas en el marco de su transposición en varios Estados miembros; el artículo 20, apartado 3, de la Decisión Marco 2005/214/JAI, de 24 de febrero de 2005, relativa a la aplicación del principio de reconocimiento mutuo de sanciones pecuniarias; el artículo 11, apartado 1, letra f), de la Directiva OEI; el artículo 8, apartado 1, letra f), y el artículo 19, apartado 1, letra h), del Reglamento (UE) 2018/1805 sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso, y los asuntos acumulados C-404/15 y C-659/15 PPU, Aranyosi y Căldăraru, y el asunto C-216/18 PPU, Minister for Justice and Equality/LM.

esencial para garantizar el respeto de las obligaciones en materia de derechos fundamentales, en la práctica se ha procedido más bien a introducir cláusulas diferentes para cada instrumento de reconocimiento mutuo, con la clara intención de limitar o impedir su aplicación[7]. Por lo tanto, la formulación de la cláusula sobre los derechos fundamentales debe ser lo suficientemente amplia como para permitir que un juez la utilice en caso necesario (tiene la obligación de proteger los derechos fundamentales), y debe hacer referencia a todos los derechos (y no solo a un catálogo de derechos)[8] y al artículo 6 del TUE[9]. Solo de esta manera se podrán evitar futuros recursos y tensiones en materia de derechos fundamentales[10].

3. Notificación del Estado afectado

El enfoque de la propuesta de la Comisión, consistente en otorgar a las autoridades del Estado de emisión competencias jurídicas directas sobre los proveedores de servicios (y, por ende, sobre los datos de los ciudadanos) con una notificación tan solo limitada o tardía a la persona afectada, se traduce en una situación en la que la persona afectada no tiene la posibilidad efectiva de impugnar la legalidad, proporcionalidad o necesidad de una orden ante un órgano jurisdiccional al que tenga acceso en su Estado de residencia, lo que afecta directamente al derecho a un proceso equitativo y al derecho a la defensa. Por ello, en la propuesta de la Comisión no se incluye el parámetro «localización de la persona afectada», por el que se debe tener en cuenta, además del lugar del enjuiciamiento, la ubicación del interesado[11].

Una manera de garantizar el ejercicio efectivo de los derechos fundamentales de la persona afectada, incluidas las inmunidades y privilegios (por ejemplo, en el caso de periodistas, médicos o abogados), consistiría en crear un mecanismo de notificación mediante el cual el Estado de emisión pueda informar o solicitar la aprobación del Estado afectado antes de emitir una orden destinada al Estado de ejecución y al prestador de servicios. De esta forma se adecuaría la protección de los derechos fundamentales a las normas aplicables en materia de

---

[7] Por ejemplo, utilizando los términos «denegación flagrante de justicia» (un concepto del CEDH utilizado principalmente en relación con la extradición a terceros países), rechazados expresamente por el PE en las negociaciones de la OEI debido a sus extremadas limitaciones.

[8] Algunos Estados miembros querían limitar las categorías de derechos cubiertos por este motivo en lo que respecta al reconocimiento mutuo de las resoluciones de embargo y decomiso. Sin embargo, el PE se opuso firmemente a una limitación a determinados derechos. Véase también Comité Europeo de Protección de Datos (CEPD), ibídem (p. 17): *Incluso el motivo de denegación de la ejecución de una orden porque violaría la Carta parece superior al umbral clásico en relación con una violación de los derechos fundamentales de la persona afectada. Por consiguiente, [...] en la propuesta de Reglamento se debe prever al menos la excepción clásica mínima por la que, si existen motivos sustanciales para creer que la ejecución de una orden vulneraría un derecho fundamental del interesado y que el Estado de ejecución incumpliría sus obligaciones en materia de protección de los derechos fundamentales [...]*.

[9] Es importante incluir una referencia al artículo 6 del TUE, ya que en él se hace referencia a los tres pilares de la protección de los derechos fundamentales, a saber, el CEDH, la Carta y las tradiciones constitucionales comunes. Gracias a esa referencia se podrá evitar un potencial conflicto del tipo «Solange» entre las constituciones nacionales y el Derecho de la UE en lo que respecta a la protección de los derechos fundamentales.

[10] En los Estados miembros, los instrumentos de reconocimiento mutuo se transponen en muchos casos con una ley especial. No tiene sentido y para un juez no es viable que, para cada procedimiento de reconocimiento mutuo, se utilice una cláusula sobre los derechos fundamentales distinta (más amplia o limitada), por ejemplo, una para la orden de detención europea, otra para los decomisos y otra para las pruebas. Los jueces no trabajan y no evalúan los asuntos de esta forma: o bien ven un riesgo para los derechos fundamentales o bien no lo ven.

[11] Véase, por ejemplo, el documento WK 3901/2017 del Consejo, que contiene la propuesta belga relativa a un método de trabajo en la que se afirma que, a su entender, se trata del «factor de conexión» más importante, aparte del motivo del enjuiciamiento, y en la que se propone el concepto de «localización del uso habitual del servicio por la persona afectada».

cooperación judicial y se permitiría que el Estado afectado cumpla sus obligaciones en materia de protección de los derechos fundamentales.

No obstante, se plantea una pregunta fundamental, a saber: ¿a qué Estado se notificará? ¿Al Estado en el que se almacenan los datos, al Estado en el que se ha nombrado al representante legal del proveedor de servicios, al Estado de residencia[12] de la persona afectada o al Estado de su nacionalidad[13]? La cuestión se complica aún más con el concepto de representante que se introduce en la Directiva paralela, en virtud del cual dicho representante podría diferir de la sede del proveedor en la UE y del lugar en el que se almacenan los datos en la UE[14]. En teoría, parece que, para respetar las obligaciones en materia de derechos fundamentales y de protección de datos de la UE y del CEDH, todos ellos tendrían que ser informados. Para reducir al mínimo las acciones necesarias, una opción podría consistir en estipular el nombramiento de un representante legal únicamente para los proveedores de terceros Estados; para los proveedores de la UE podría ser más conveniente el sistema actual, según el cual, en principio, sirven de punto de contacto la sede del proveedor o la ubicación de los datos. A este respecto, es discutible que la orientación general del Consejo sobre la Directiva sobre pruebas electrónicas, de 8 de marzo de 2019[15], intente ampliar, al parecer, el concepto de representante legal (y todo lo relacionado con esta cuestión en lo que respecta a la notificación) a otros instrumentos existentes, como la OEI. Esa posible ampliación pondría en tela de juicio el eficaz sistema de trabajo establecido actualmente en lo que respecta a los proveedores de la UE[16].

Además de la cuestión de decidir quiénes deben ser los destinatarios de una notificación completa, también es importante examinar las posibles consecuencias de dicha notificación. Al menos para algunas categorías de datos, esa notificación debe incluir la posibilidad de reaccionar, como mínimo de forma negativa (por ejemplo, bloquear la medida dentro de un plazo determinado sobre la base del modelo del artículo 31 de la Directiva OEI), a fin de

---

[12] Véase, para esta opción, T. Christakis, CBDF, «Big divergence of opinions on e-evidence in the EU Council: A proposal in order to disentangle the notification knot» (Gran divergencia de opiniones sobre las pruebas electrónicas en el Consejo de la UE: propuesta destinada a solucionar el problema de la notificación).

[13] Ibídem.

[14] Véase el artículo 3 de la propuesta de Directiva sobre pruebas electrónicas: «El representante legal deberá residir o estar establecido en uno de los Estados miembros en los que el proveedor esté establecido u ofrezca los servicios». Este sistema sería lógico para los proveedores no establecidos en la UE pero que ofrezcan servicios en la UE. Sin embargo, para los proveedores establecidos en la UE introduce un cambio en las prácticas vigentes y en un sistema de cooperación eficaz. Esta cuestión fue planteada por la Federación Alemana de Jueces (Deutscher Richterbund) en su dictamen n.º 6/18.

[15] Documento 6946/19 del Consejo.

[16] Véase el considerando 8 de la orientación general mencionada, en el que se indica lo siguiente: *El representante legal en cuestión deberá servir de destinatario de las órdenes y resoluciones nacionales y de las órdenes y resoluciones en virtud de los instrumentos jurídicos de la Unión adoptados en el ámbito de aplicación del título V, capítulo 4, del Tratado de Funcionamiento de la Unión Europea a efectos de recabar pruebas para procesos penales, incluso cuando dichas órdenes y resoluciones se transmitan en forma de certificado. Esto incluye tanto los instrumentos que permiten la notificación directa de órdenes en situaciones transfronterizas al proveedor de servicios o a su representante legal, como el [Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal («Reglamento»)], como otros instrumentos para la cooperación judicial aplicable entre los Estados miembros, en particular los que entran en el ámbito de aplicación del título V, capítulo 4, como la Directiva sobre la orden europea de investigación y el Convenio relativo a la asistencia judicial en materia penal de 2000. El recurso al representante legal debe realizarse de conformidad con los procedimientos establecidos en los instrumentos y la legislación aplicables a los procedimientos judiciales. Las autoridades competentes del Estado miembro en el que resida o esté establecido el representante legal deben actuar de conformidad con el papel que se les asigne en el instrumento respectivo en caso de que se prevea una participación.*

permitir al Estado de ejecución ejercer sus responsabilidades en el marco del sistema del CEDH, así como tener en cuenta el carácter sensible de algunos datos en consonancia con la jurisprudencia del TJUE (especialmente en lo que se refiere al umbral muy bajo utilizado por la Comisión, por ejemplo, en los datos de tráfico)[17].

4. Distintas salvaguardias para distintas categorías de datos (artículo 2)

La Comisión ha introducido cuatro categorías de datos en su propuesta: a) datos de los abonados, b) datos relativos al acceso, c) datos de transacciones y d) datos de contenido. La propuesta prevé diversos requisitos en función de las categorías a las que pertenezcan los datos solicitados por las autoridades competentes. Mientras que en el caso de los datos de los abonados y los datos relativos al acceso solo se exige la validación por un fiscal y se puede acceder a ellos para todas las infracciones penales, solo se puede acceder a los datos de transacciones y los datos de contenido previa validación por un juez y únicamente para las infracciones penales punibles con una pena máxima de privación de libertad de al menos tres años, para las infracciones armonizadas en la Decisión marco 2001/413/JAI del Consejo, la Directiva 2011/93/UE y la Directiva 2013/40/UE, y para los delitos de terrorismo enumerados en la Directiva 2017/541/UE.

La nueva clasificación de los datos plantea dos problemas: 1) las definiciones se solapan parcialmente (véanse las definiciones de los datos relativos al acceso y los datos de transacciones) y pueden impedir el uso legítimo de los instrumentos por parte de las autoridades policiales y judiciales; 2) la clasificación se aparta tanto de las definiciones de las categorías de datos contempladas en la legislación europea vigente[18] en el ámbito de la protección de datos y la privacidad de las comunicaciones electrónicas, como de los tratados internacionales[19], lo que conlleva riesgos de desajuste y de incompatibilidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos[20].

[17] El CEPD ha criticado el razonamiento «simplista» de la Comisión en los casos relativos a la conservación de los datos, conforme al cual considera que está autorizado todo lo que no haya sido mencionado o prohibido expresamente por el Tribunal. Dictamen 23/2018 del CEPD (p. 14): *El CEPD lamenta especialmente que el umbral mínimo que prevé la posibilidad de que las autoridades policiales y judiciales soliciten acceso a datos de los abonados y a datos relativos al acceso para cualquier delito se fundamente en una interpretación a contrario de la jurisprudencia del TJUE [...].*Véanse asimismo el Dictamen n.º 6/18 de la Deutscher Richterbund y el Dictamen del CEPD sobre las pruebas electrónicas, en los que se solicita una notificación significativa con una posible reacción dentro de un plazo determinado.

[18] Artículo 10, apartado 2, letra e), de la Directiva 2014/41/UE (Directiva OEI) y artículo 4, apartado 3, letra c), de la propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (COM(2017)0010).

[19] Convenio del Consejo de Europa sobre la Ciberdelincuencia.

[20] Para más información, véase el documento de trabajo n.º 2 sobre el ámbito de aplicación, especialmente en lo que se refiere a las direcciones IP dinámicas.