Parlamento Europeo
2014-2019

Comisión de Libertades Civiles, Justicia y Asuntos de Interior

1.4.2019

6º DOCUMENTO DE TRABAJO (C)

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

III. Salvaguardias ex post

1. Vías de recurso efectivas (art. 17)

El documento de trabajo ya ha puesto de relieve que es muy probable que la información de los usuarios solo llegue en una fase muy tardía de la investigación. Por lo tanto, es muy dudoso que el interesado, en un estado tan tardío de la investigación, aún pueda solicitar realmente unas vías de recurso efectivas. Dado que esto plantea, una vez más, serias dudas en cuanto al principio de igualdad de armas y el principio de contradicción como parte del derecho a un juicio justo (artículo 6 del CEDH), esta parte del documento de trabajo abordará con más detenimiento el artículo 17 de la propuesta de Reglamento, que se refiere a las «vías de recurso efectivas».

El artículo 17, apartado 1, del Reglamento sobre pruebas electrónicas propuesto otorga al sospechoso o acusado el «derecho a vías de recurso efectivas contra [la] orden [europea de entrega] durante el proceso penal para el que se haya emitido la orden».[1] No se aplicará a las órdenes de conservación (EPOC-PR). El artículo 17, apartado 2, estipula además lo siguiente: «Cuando la persona cuyos datos se hayan obtenido no sea un sospechoso o acusado en un proceso penal para el que se haya emitido la orden, dicha persona tendrá derecho a vías de recurso efectivas contra una orden europea de entrega en el Estado emisor». «Este derecho a una tutela judicial efectiva se ejercerá ante un órgano jurisdiccional en el Estado emisor con arreglo a su legislación nacional y deberá incluir la posibilidad de impugnar la legalidad, la necesidad y la proporcionalidad de la medida» (véase el artículo 17, apartado 3).

Con ello, la propuesta no prevé ningún derecho a una tutela judicial efectiva cuando se trata de EPOC-PR, ni para el sospechoso o acusado, ni para los terceros implicados. Así pues, como ya se ha indicado anteriormente, en los casos en que una EPOC no sigue a una EPOC-PR, el interesado no sabe que sus datos se han conservado, por lo que no tiene acceso a ninguna vía de recurso.

Se plantea otro problema por lo que se refiere al lugar donde se puede interponer un recurso. La propuesta establece que, en el caso de los sospechosos y acusados, los recursos solo podrán interponerse «durante el proceso penal (...) en el Estado emisor» (artículo 17, apartado 1) y, en el caso de terceros (artículo 17, apartado 2), los recursos solo podrán interponerse «en el Estado emisor (...) con arreglo a su legislación nacional», por lo que resulta dudoso que el interesado pueda interponer efectivamente tal recurso. En cambio, por lo que se refiere al carácter transfronterizo del instrumento de prueba electrónica propuesto, es muy probable que la tutela judicial efectiva se vea claramente obstaculizada, debido a la distancia física con respecto al Estado emisor, a posibles problemas lingüísticos, a la falta de comprensión del otro sistema jurídico, así como a dificultades financieras para interponer recurso en otro Estado miembro.[2] Por tanto, se plantea la cuestión de si el usuario no debe poder impugnar

[1] Se afirma que esto se entiende sin perjuicio de las medidas de protección de datos y sin perjuicio de las vías de recurso disponibles en virtud de la Directiva (UE) 2016/680 y del Reglamento (UE) 2016/679.

[2] Véanse también los comentarios del Comité Meijers, CM 1809, de 18 de julio de 2018, en los que se afirma que, con arreglo al mecanismo propuesto, es muy probable que se produzca una situación en la que la persona implicada —ya sea sospechosa o no— resida en un Estado miembro distinto del Estado emisor y del Estado en cuyo territorio está ubicado el representante legal o el establecimiento del prestador de servicios. *El Comité Meijers se pregunta si esto no generaría una incertidumbre en el marco del acervo de derechos fundamentales o de otro tipo, en cuanto al país en el que la persona interesada pueda presentar una reclamación. ... Por lo tanto,*

asimismo la legalidad ante los tribunales de su propio Estado miembro (o, al menos, en el Estado miembro de ejecución, dado que fue allí donde se ejercieron las competencias).[3]

Además, la propuesta no especifica las vías de recurso, por lo que corresponde a los Estados miembros determinar con arreglo a la legislación nacional las consecuencias de una violación de las normas de procedimiento en la obtención de datos electrónicos. Teniendo en cuenta los anteriores instrumentos de reconocimiento mutuo a escala de la Unión, como la OEI, pero también las directivas sobre garantías procesales, debe admitirse que se trata de un problema general. Hasta ahora, dichas directivas sobre derechos procesales, así como la OEI, carecen de una referencia clara a un recurso armonizado o solo utilizan un lenguaje muy vago que se refiere, por ejemplo, a los «derechos de defensa y equidad del procedimiento».[4]

2. La cuestión de la admisibilidad de los datos como prueba

Empíricamente, desde la posición del interesado, el único recurso efectivo parece ser el derecho a impugnar la admisibilidad de las pruebas recabadas.[5] Esto también podría ayudar a prevenir las prácticas ilegales de aplicación de la legislación, es decir, un uso indebido del instrumento de pruebas electrónicas. La cuestión mencionada se refiere a la cuestión de la admisibilidad de pruebas en relación con la norma de exclusión.[6] En la actualidad, los Estados miembros de la Unión difieren significativamente en su enfoque con respecto a los dos conceptos mencionados, que varía desde una ausencia completa de normas de admisibilidad hasta unas normas muy estrictas de admisibilidad y exclusión.[7] Según los profesionales, en lo

---

el Comité Meijers propone que se considere seriamente la posibilidad de permitir expresamente a las personas que presenten sus reclamaciones ante un tribunal de su Estado de residencia.

[3] Véanse los artículos 50 y 52 de la Directiva 2016/680 («Directiva sobre la protección de datos destinada a los servicios de seguridad»: el derecho a presentar una reclamación ante una autoridad de control única que el interesado elija, y transmisión a la autoridad de control competente).

[4] El Reglamento sobre pruebas electrónicas da un paso más en el artículo 18 en lo que se refiere a garantizar los privilegios e inmunidades, así como los intereses fundamentales del estado de ejecución, pero solo para los datos de transacciones o de contenido. Sin embargo, solo es el órgano jurisdiccional del Estado emisor el que garantizará durante el proceso penal para el que se emitió la orden que estos motivos se tengan en cuenta en las mismas condiciones que si estuvieran previstos en su legislación nacional al evaluar la pertinencia y la admisibilidad de las pruebas en cuestión. En vista de los diferentes sistemas, las consecuencias podrían ser sustancialmente diferentes y no las mismas que las que se darían en el estado de ejecución. La orientación general del Consejo suprimió el artículo 18.

[5] Véanse, por ejemplo, a modo de comparación, las sentencias del Tribunal Supremo de los Estados Unidos en el asunto Wolf / Colorado , 338 U.S. 25 (1949), en las que se optaba por un sistema divergente de sanciones en los Estados federados, y revocadas en Mapp / Ohio , 367 U.S. 643 (1961), por la que se introducía la norma de exclusión como un recurso efectivo común en todos los Estados federados para evitar violaciones de la 4ª Enmienda, que prohíbe los registros e incautaciones ilegales. Véase también el documento sobre pruebas electrónicas presentado por Fair Trials International (febrero de 2019), p. 1, donde se afirma que: *«Durante el juicio (o poco antes, tras la obtención de las pruebas) se lleva a cabo un control fundamental de la legalidad de la recogida de pruebas por parte de las autoridades con funciones coercitivas. Se trata de la facultad del acusado de impugnar la admisibilidad de pruebas en las que el Estado pretende basarse para obtener una condena. El acusado debe tener derecho a impugnar la solicitud y el uso de datos en el juicio, así como a buscar las vías de recurso adecuadas cuando se hayan obtenido pruebas electrónicas de forma ilegal. Y con el fin de estar en condiciones de ejercer el derecho a impugnar, las personas acusadas deben poder obtener la divulgación de las fuentes de las pruebas electrónicos.»*

[6] Los dos conceptos están conectados, pero no son idénticos. La admisibilidad se refiere a la posibilidad de basar la sentencia en determinadas pruebas o no. La norma de exclusión, además, exige que, en principio, el juez que resuelva el asunto en la fase del juicio no esté en contacto con pruebas inadmisibles, ya que esto podría provocar su contaminación psicológica.

[7] Véase, por ejemplo, S. C. Thaman, *Exclusionary Rules in Comparative Law*, 2012.

que respecta a su aplicación, pueden incluso variar considerablemente de un órgano jurisdiccional a otro y de un juez a otro. Y también a escala de la Unión, no existe un marco jurídico claro en lo que respecta a la admisibilidad de las pruebas, lo que dificulta el funcionamiento del principio de reconocimiento mutuo. En la actualidad, la única base común se deriva de la jurisprudencia del TEDH, según la cual se han establecido normas claras sobre violaciones del artículo 3 del CEDH (prohibición de la tortura y de los trato inhumanos y degradantes).[8] Sin embargo, por lo que se refiere al derecho a un juicio justo (véase el artículo 6 del CEDH, incluidos, entre otros, el derecho a guardar silencio, el derecho a un abogado, el derecho a la defensa, etc.[9]) o el derecho a la intimidad (véase el artículo 8 del CEDH), las normas son mucho menos claras y solo se refieren a un principio de ponderación sobre la «equidad del procedimiento en su conjunto» sobre las violaciones de los derechos mencionados. Incluso la jurisprudencia pertinente sobre el artículo 8 del CEDH (en relación con la admisibilidad y el juicio justo en el artículo 6 del CEDH), tal como ha sido desarrollada por el TEDH, se basa en criterios vagos que son muy inferiores a las normas actuales en varios Estados miembros.[10]

En consecuencia, el nuevo mecanismo debe especificar qué recurso se aplica cuando se han obtenido pruebas electrónicas de forma ilegal. Además, con el fin de evitar que las autoridades policiales se beneficien de pruebas obtenidas ilegalmente (por ejemplo, si se obtiene una condena únicamente sobre la base de las pruebas obtenidas ilegalmente), los nuevos instrumentos propuestos deben permitir una revisión de la manera en que se han recopilado las pruebas. A tal fin, la fuente subyacente de los datos electrónicos debe revelarse al tribunal de revisión y a la defensa para permitir una evaluación en cuanto a la legalidad de la recopilación de datos y al modo en que pueden obtenerse pruebas exculpatorias. Si se ha demostrado que se han obtenido pruebas de forma ilegal, deben introducirse nuevas normas en lo que respecta a la inadmisibilidad de estas pruebas o, al menos, cierta armonización de las normas nacionales de admisibilidad/exclusión.[11]

3. Prohibición de tratamiento ulterior y posterior transferencia de pruebas

Debe introducirse la prohibición de utilizar las pruebas al margen del procedimiento de investigación y, en particular, la prohibición de divulgar los datos a las autoridades investigadoras que no estén asociadas al caso. La transferencia de datos con fines de seguridad pública debe estar claramente regulada. El sistema propuesto es un sistema de Derecho penal y no debe utilizarse con fines de inteligencia debido a la tendencia en algunos Estados miembros a difuminar la línea divisoria entre la aplicación de la ley y la inteligencia.

[8] Véanse, por ejemplo, TEDH, Gäfgen / Alemania , n.º 22978/05, sentencia de 1 de junio de 2010, y El Haski / Bélgica , n.º 649/08, sentencia de 25 de septiembre de 2012.

[9] Además, las mencionadas normas del CEDH son mucho más bajas que las normas constitucionales de los Estados miembros y que las normas de la Unión. Por ejemplo, el derecho a guardar silencio es solo un derecho relativo según la jurisprudencia del TEDH (véase, por ejemplo, John Murray / Reino Unido, n.º 18731/91, sentencia de 8 de febrero de 1996) pero un derecho absoluto en la Unión Europea (véanse la Directiva 343/2016 y algunas constituciones nacionales). Véase, por ejemplo, Bykov / Rusia , n.º 4378/02, sentencia de 10 de marzo de 2009, por lo que se refiere a los criterios para evaluar la equidad del procedimiento por una posible violación del derecho a guardar silencio.

[10] Véanse, por ejemplo, TEDH, Malone / Reino Unido , n.º 8691/79, sentencia de 2 de agosto de 1984, Schenk / Suiza , n.º 10862/84, sentencia de 12 de julio de 1988, Kopp / Suiza, n.º 23224/94, sentencia de 25 de marzo de 1998 , Khan / Reino Unido , n.º 35394/97, sentencia de 12 de mayo de 2000, etc.

[11] El Parlamento Europeo ya adoptó este enfoque en su posición interna para las negociaciones por lo que se refiere a determinados aspectos de la presunción de inocencia que proponen una estricta no admisibilidad en caso de violación del derecho a guardar silencio (procedimiento legislativo sobre la Directiva 2016/343).

Esto es necesario en los casos en que una persona encausada haya podido obtener una resolución de que una EPOC ha sido emitida de forma improcedente (artículo 17). Si los datos cuya obtención ilegal se hubiera descubierto posteriormente ya hubieran sido transmitidos, su supresión apenas puede efectuarse y controlarse.

Habría que crear procedimientos distintos para la recuperación y la transferencia en los casos en los que la investigación aún está en curso y la medida sigue estando oculta. En este caso, los órganos jurisdiccionales del Estado miembro de ejecución deben tomar tales decisiones en lo que se refiere a las transferencias ulteriores y a la divulgación de información. En particular, antes de transmitir los datos a las autoridades de terceros países, es indispensable que los órganos jurisdiccionales del Estado de ejecución adopten una resolución judicial.[12]

4. Compensación financiera y sanciones

Además, debe evaluarse si las vías de recurso efectivas también podrían incluir la compensación financiera para el interesado, si está cubierta por la base jurídica. Con este régimen de compensación, también las terceras personas que no estén encausadas/acusadas, en cuyo caso la cuestión de la admisibilidad de las pruebas no es relevante, podrían beneficiarse de la tutela judicial efectiva. Aparte de la cuestión de la admisibilidad, con el fin de evitar que las autoridades policiales obtengan pruebas de forma ilícita, podría ser conveniente examinar la posibilidad de prever también sanciones para las autoridades emisoras que solicitaron ilegalmente datos (véase a este respecto, por ejemplo, el artículo 57 de la Directiva sobre la policía), si están cubiertas por la base jurídica.

5. Recurso para los prestadores de servicios

Como entidades privadas, los proveedores de servicios están bastante poco equipados y no tienen ningún incentivo intrínseco para proteger los derechos fundamentales de sus usuarios. Por tanto, los proveedores de servicios no pueden ni deben verse en una situación en que tengan que sustituir a las autoridades públicas por lo que se refiere a la protección de los derechos fundamentales.

No obstante, las partes interesadas han señalado la importancia de dar a los proveedores de servicios la oportunidad realista de rechazar la ejecución de una EPOC o una EPOC-PR si tienen motivos razonables para creer que tal orden puede ser ilegal.[13] Se ha cuestionado por qué solo una infracción «manifiesta» debe constituir uno de los motivos de denegación, y no simplemente «una infracción». Asimismo, para que esto funcione, los proveedores de servicios necesitarían tiempo suficiente para evaluar una solicitud y no deberían verse amenazados por ello de forma unilateral con unos plazos extremadamente cortos y unas sanciones financieras.

[12] Deutscher Richterbund, ibidem.
[13] Documento de EDRi

IV. Supervisión efectiva y responsabilidad pública

1. Supervisión efectiva y sistémica del uso de las medidas

Si los nuevos instrumentos se utilizan de forma equitativa y proporcional, es más probable que mantengan la confianza de los ciudadanos en los sistemas judiciales penales y en las autoridades con funciones coercitivas. Unos mecanismos de supervisión eficaces tendrán que garantizar un blindaje contra el riesgo de uso indebido y, de este modo, ayudar a proteger tanto la reputación de la actividad legítima de los servicios con funciones coercitivas como a quienes podrían convertirse en víctimas de abuso de los instrumentos. Con este fin, los organismos de supervisión para la presentación transfronteriza de pruebas deben participar como parte de un marco institucional adecuado (modelo de la OEI, modelo del CEPD, modelo del GCPC o, quizás, modelos nacionales), incluidas las competencias reales de supervisión.

2. Transparencia y responsabilidad

El artículo 19 de la propuesta de Reglamento se refiere a la cuestión del «seguimiento y presentación de informes», que establece obligaciones concretas para la Comisión y los Estados miembros a fin de hacer el seguimiento de los resultados y las repercusiones de la propuesta de Reglamento y recopilar una amplia variedad de datos. Esta disposición presenta un valor añadido.

Las estadísticas son un problema recurrente en el ámbito del Derecho penal de la Unión, ya que los Estados miembros en las negociaciones legislativas a menudo quieren un conjunto más limitado de datos estadísticos en comparación con el Parlamento Europeo y la Comisión.[14] Sin embargo, estos datos son esenciales para abordar, entre otras cosas, los problemas potenciales con órdenes excesivas e infundadas, y para poder evaluar el funcionamiento de los instrumentos existentes. Por consiguiente, los Estados miembros no solo deben recopilar y notificar estadísticas a la Comisión (según lo previsto en el artículo 19, apartado 2), sino que estos datos estadísticos también deben publicarse. Además, parece necesario ampliar el artículo 19, apartado 2, para incluir también información más detallada:

- el número de EPOC(-PR) emitidos e indicación de los Estados miembros destinatarios,

- la indicación del tipo de delito para el que se emitió la EPOC(-PR),

- y el número de condenas en los casos en que se recurrió a las EPOC(-PR).

V. Limitaciones de las salvaguardias y el llamado «derecho a la seguridad»

[14] Compárese, por ejemplo, las propuestas iniciales de la Comisión y los textos legislativos finales del artículo 11 de la Directiva 2014/42/UE, sobre el embargo y el decomiso de los instrumentos y del producto del delito en la Unión Europea, y el artículo 35 del Reglamento (CE) n.º 2018/1805, sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso.

En su evaluación del impacto de la propuesta sobre pruebas electrónicas, pero también en otras propuestas desde la entrada en vigor de la Carta de los Derechos Fundamentales de la Unión Europea, la Comisión afirma que, sobre la base del artículo 6 de la Carta, existe un «derecho a la seguridad» y que tal derecho, según parece, tendría que equilibrarse con otros derechos y salvaguardias individuales.[15]

No obstante, esta argumentación debe rechazarse enérgicamente, ya que cualquier referencia al artículo 6 de la Carta es engañosa y errónea. No existe ningún «derecho a la seguridad» legalmente reconocido ni en el marco del CEDH ni en el de la Carta. El mencionado artículo no introduce dos derechos distintos, como afirma la Comisión, a saber, el derecho a la libertad y el derecho a la seguridad, que deben ser equilibrados. Por el contrario, el artículo 6 de la Carta es un mero reflejo del artículo 5 del CEDH (con exactamente el mismo título), que establece claramente el derecho a la protección contra las detenciones ilegales por parte del Estado. Así pues, no existe un derecho a la seguridad legalmente reconocido.[16] Existe la seguridad como una necesidad humana básica[17], pero no es un derecho fundamental reconocido desde el punto de vista jurídico ni en virtud del CEDH ni en virtud de la Carta.

En el CEDH, en determinados artículos, solo existe el concepto de obligaciones positivas de las Partes Contratantes, por ejemplo en el artículo 2 (derecho a la vida)[18] o el artículo 3 (prohibición de la tortura, las penas y los tratos inhumanos o degradantes)[19], en virtud del cual, en algunos casos particulares, las Partes en el Convenio pueden ser responsables de la violación de tales obligaciones positivas. Sin embargo, tales obligaciones no constituyen una clase de «derecho a la seguridad» alternativo. Además, el artículo 52, apartado 3, de la Carta establece que «[e]n la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio». Esta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa.» Por consiguiente, los derechos y las garantías no pueden quedar por debajo del nivel de la Carta. Sin embargo, la referencia de la Comisión a su «derecho a la seguridad» artificial e inexistente se utiliza en la propuesta para equilibrar esos derechos y garantías a un nivel diferente y posiblemente inferior al CEDH.

Es importante aclarar esta cuestión, ya que parece que, debido a la utilización de este término legalmente inexistente por la Comisión, entre otros, el equilibrio de los derechos y garantías

[15] En las pruebas electrónicas está relacionado con la cuestión de las víctimas. Sin embargo, en otros documentos de la Comisión, parece un derecho autónomo. Véase, por ejemplo, el Documento de trabajo de los servicios de la Comisión sobre la Evaluación de impacto que acompaña al documento Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión marco 2001/413/JAI del Consejo

[16] Esto lo señaló claramente la FRA, así como por la Red de expertos independientes de la Unión en materia de derechos fundamentales («Durante la redacción del artículo 6 de la Carta en el Convenio, el término «seguridad» condujo en repetidas ocasiones a controvertidos debates, y algunos miembros propusieron que simplemente se suprimiera, ya que podría dar lugar a diferentes interpretaciones en algunos Estados miembros de la Unión, como Francia, Italia y Alemania. Sin embargo, la Convención decidió mantener el término en la interpretación restrictiva de la jurisprudencia de Estrasburgo en virtud del artículo 5 del CEDH.»)

[17] Véase A. Maslow, *Motivation and Personality*, 1954.

[18] Véase, por ejemplo, TEDH, Osman / Reino Unido, n.º 23452/94, sentencia de 28 de octubre de 1998.

[19] Véase, por ejemplo, TEDH, Z. y otros / Reino Unido, n.º 9292/95, sentencia de 10 de mayo de 2001.

(como un derivado de derechos individuales, como el derecho a la tutela judicial efectiva, al acceso a un tribunal, a un procedimiento justo, las limitaciones de la intimidad, el derecho a ser informado sobre los cargos, el principio de igualdad o de las partes, etc.) empezó a verse afectado en comparación con las normas del CEDH.[20]

Conclusión

- Los recursos ex-ante deben incluir unas condiciones estrictas para la emisión de las EPOC(-PR), como la obtención de un determinado nivel de las pruebas y un determinado nivel de proporcionalidad debidamente evaluado, en virtud de lo cual el proveedor también debe poder realizar un determinado ensayo.

- Para que la persona afectada pueda hacer uso de los recursos disponibles, debe conocer la medida y el hecho de que sus datos han sido producidos/conservados, con el fin de garantizar el derecho a la defensa y a un juicio justo. Por lo tanto, debe realizarse una notificación mucho más significativa, al menos en el estado de aplicación, incluida una cláusula de derechos fundamentales basada en el ejemplo de la EOI. La confidencialidad debe ser la excepción, no la regla, y debe regirse por unas condiciones estrictas.

Por lo que se refiere a las posibles infracciones de las normas establecidas en el presente Reglamento, el texto también tiene que prever el acceso a unas vías de recurso eficaces. En consecuencia, unas normas más armonizadas sobre los recursos disponibles en el Estado emisor, así como sobre la admisibilidad de las pruebas recogidas ilegalmente y la norma de exclusión, como medidas de acompañamiento. Además, el acceso a las vías de recurso en el país en el que se hayan producido o conservado los datos o en el Estado miembro en el que reside el sospechoso o tercero, así como la imposición de sanciones a las autoridades que emitan ilegalmente una EPOC(-PR), podría ser necesario para permitir realmente una tutela judicial efectiva.

- La cuestión de que el representante legal puede disociarse del lugar de establecimiento del proveedor del servicio debe analizarse más a fondo, ya que tiene un impacto significativo en el otro Estado miembro que debe notificarse. Debe aclararse asimismo si este sistema es también necesario para los proveedores de servicios establecidos en la Unión Europea (o si no solo sería necesario para los proveedores de servicios basados en

[20] Véase también TJUE, asunto C-601/15 J.N . / Staatssecretaris van Veiligheid en Justitie, sentencia de 15 de febrero de 2016, apartado 45 («las explicaciones relativas al artículo 6 de la Carta [...] dejan claro que los derechos establecidos en el artículo 6 de la Carta corresponden a los garantizados por el artículo 5 del CEDH»). Lamentablemente, el propio TJUE ha creado cierta confusión por referencias poco claras en el dictamen 1/2015 y en los asuntos C-293/12 y C-594/12 Digital Rights Ireland y Seitlinger y otros. En el futuro, el TJUE deberá ser más prudente a este respecto no dar lugar a malentendidos con consecuencias negativas para la conformidad de la Carta con el mínimo del CEDH. Véase también X. Tracsol, dictamen 1/15 de la Gran Sala — Revisión de la seguridad informática 34 (2018) (« La confianza de la Gran Sala en el artículo 6 de la Carta en este contexto específico no es convincente y sus implicaciones no son claras»).

terceros países), en particular en lo que respecta a los instrumentos de cooperación existentes, así como al CEDH y a los derechos fundamentales de la Unión y al marco de protección de datos.

- El seguimiento y la recogida de estadísticas públicos y transparentes deben formar parte del sistema.

- No existe un «derecho a la seguridad» reconocido legalmente en virtud de los artículos 5 del CEDH y del artículo 6 de la Carta, y cualquier prueba de sopesamiento en relación con los derechos fundamentales no deberá vincularse a un derecho inexistente de este tipo.