

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Estrasburgo, 19 de agosto de 2016

T-PD(2016)18rev

**COMITÉ CONSULTIVO DEL CONVENIO PARA LA
PROTECCIÓN DE LAS PERSONAS EN RELACIÓN CON
EL TRATAMIENTO AUTOMATIZADO DE DATOS DE
CARÁCTER PERSONAL
(T-PD)**

**Opinión sobre las implicancias de la protección
de datos en relación con el tratamiento de
Registros de Nombres de Pasajeros
(PNR)**

Director General de Derechos Humanos y Estado de Derecho

Índice

1. Introducción	2
2. Descripción de datos en relación con los PNR	3
3. Legalidad.....	4
4. Necesidad y proporcionalidad	5
5. Aplicación de los principios y salvaguardias	6
6. Conclusiones	12

El Comité Consultivo del Convenio para la Protección de las Personas en Relación con el Tratamiento Automatizado de Datos de Carácter Personal (ETS 108, en adelante el “Convenio 108”),

Recordando al Convenio Europeo de los Derechos Humanos (ECHR) y en especial los artículos 8 (derecho al respeto de la vida privada) y 13 (derecho a un recurso efectivo), de la forma elaborada por la jurisprudencia del Tribunal Europeo de Derechos Humanos y el artículo 2 (libertad de movimiento) del Protocolo N°4,

Vistos el Convenio 108 y demás instrumentos pertinentes del Consejo de Europa en el ámbito de la protección de datos, tales como la Recomendación (87)15 que regula el uso de los datos de carácter personal en el sector de la policía y la Recomendación (2010)13 sobre la protección de las personas en relación con el tratamiento automatizado de datos de carácter personal en el ámbito de la elaboración de perfiles,

Observando la rápida propagación a nivel global de los sistemas de tecnologías de la información y de las legislaciones que refieren a la transmisión de datos personales de pasajeros por parte de transportistas aéreos a las autoridades públicas en pos del cumplimiento de la ley y con el propósito de mantener la seguridad nacional,

Decidió apoyar el respeto a los derechos humanos en relación con el tratamiento de los datos de naturaleza personal en el ámbito del transporte aéreo por parte de las autoridades públicas responsables de la prevención, detección, investigación y procesamiento ante delitos terroristas y crímenes graves,

Adoptando la presente opinión:

1. Introducción

La XXXII Reunión Plenaria (1 al 3 de julio de 2015) del Comité Consultivo del Convenio 108 adoptó, en virtud de las crecientes preocupaciones emanadas por las reacciones contra los recientes ataques y amenazas terroristas, a preparar esta opinión, habiendo considerado en profundidad los temas tratados en el informe “Los registros de nombres de pasajeros (PNR), la minería de datos y protección de datos: la necesidad de salvaguardias fuertes”¹¹.

La Mesa del Comité, durante las reuniones XXXVI, XXXVII y XXXVIII del 6 al 8 de octubre de 2015, del 9 al 11 de diciembre de 2015 y del 22 al 24 de marzo de 2016, respectivamente, trabajó en la preparación de la Opinión, la cual fue estudiada en la XXXIII Reunión Plenaria del Comité del Convenio 108 luego de la consulta por escrito a las delegaciones y a las partes interesadas.

El Comité del Convenio 108 entiende que, en el reciente contexto de la acumulación de amenazas de ataques terroristas, la lucha contra el terrorismo debe reforzarse. Subraya la importancia de combatir el terrorismo de una manera eficiente y efectiva a la vez que se asegure el respeto por los derechos humanos, el estado de derecho y los valores comunes que defiende el Consejo de Europa. El Comité señala la voluntad de los gobiernos por establecer sistemas que permitan el estudio de los datos personales en relación con los

¹¹ Informe redactado por el Dr. D. Korff con la contribución de la Sra. M. Georges:
[http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD\(2015\)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf)

pasajeros aéreos como uno de los medios para evitar el terrorismo y otros delitos graves, siendo este un elemento en el esfuerzo para garantizar la seguridad de la población. En este marco, el Comité considera necesario recordar los principios de protección de datos aplicables a dichos sistemas, subrayando que la interferencia con los derechos humanos, incluido el derecho a la protección de la vida privada y a la protección de los datos personales, solo puede ocurrir una vez cumplidas las condiciones necesarias.

El artículo 8 del ECHR y el artículo 9 del Convenio 108 han establecido las condiciones que deben respetarse al considerar limitaciones a los derechos a la vida privada y a la protección de datos. Una limitación así debe estar en consonancia con una legislación clara y debe ser necesaria en una sociedad democrática con una finalidad legítima (como la seguridad nacional, seguridad pública o la prevención del delito).

2. Descripción de datos en relación con PNR

Existen varios tipos de datos sobre los pasajeros. A los efectos del presente documento de opinión, el Comité se centrará en los Registros de Nombres de Pasajeros (PNR).

Los PNR son registros que se utilizan en la industria del transporte aéreo con fines comerciales y operativos cuando se ofrecen servicios de transporte aéreo. Los PNR son creados por las compañías aéreas y las agencias de viaje², y están relacionados a las reservas de viaje para permitir el intercambio de información entre ellos y de acuerdo con las solicitudes de los pasajeros. Dichos registros son captados mediante diversas formas, dado que las reservas³³ pueden hacerse a través de sistemas de distribución globales (GDS), sistemas de reservas informáticos (CRS), o utilizando el sistema de reservas propio de cada aerolínea. Los datos ingresados en un Sistema de Control de Salidas (DCS) de una aerolínea luego de que el pasajero realiza el check-in (o sea la información sobre el asiento y el equipaje) también pueden agregarse automáticamente a un PNR cuando el CRS y el DCS están integrados en uno solo.

Si bien los PNR fueron introducidos originalmente para utilizarse en el caso de viajes aéreos, los CRS actualmente pueden usarse para reservar hoteles, alquilar vehículos, y para reservar viajes marítimos y férreos.

El formato y contenido de un PNR, debido a las necesidades comunes de los múltiples actores, han ido armonizándose progresivamente, estandarizándose a través de la Asociación Internacional de Transporte Aéreo (IATA), la cual proporciona apoyo durante el diseño de los programas para datos de los pasajeros.

La información de los PNR se toma de los pasajeros y contiene algunos o todos los siguientes puntos:

- Nombre completo⁴
- Domicilio e información de contacto (número telefónico, dirección de correo electrónico, dirección IP)
- Tipo de documento con el que viaja, número, país donde fue emitido y fecha de

² En el futuro, "los operadores económicos no transportistas", (o sea las agencias de viaje y los operadores turísticos) posiblemente estén obligados a proporcionar los datos de PNR a las autoridades nacionales competentes.

³ Entre los sistemas de distribución global tradicionales, Amadeus es el único ubicado en Europa, con su sede central en España, su centro de datos en Alemania y el centro de investigación y desarrollo en Francia. Sus propietarios y principales usuarios son Air France, Iberia, Lufthansa, British Airways y Scandinavian Airlines y más de 60 otros transportistas en todo el mundo están afiliados a dicho sistema.

⁴ Información verificada contra la información del pasaporte presentado por el pasajero.

- vencimiento⁴
- fecha y país de nacimiento⁴
- nacionalidad⁴
- país de residencia
- itinerario de viaje (fechas, lugar de salida y llegada)
- dirección donde se alojará durante la primera noche en el país de destino
- método de pago utilizado, incluida la dirección de facturación y los detalles de la tarjeta de crédito
- datos concernientes a viajero frecuente y beneficios (suba de categoría o boletos gratuitos)
- un espacio libre para observaciones generales ("Solicitud de Servicio Especial", "Instrucciones sobre Servicios Opcionales" o "Información sobre otros servicios") tales como la información disponible sobre menores de edad que viajan solos, requisitos médicos o en cuanto a la dieta, preferencias referentes al asiento, idiomas, detalles sobre incapacidades y otras solicitudes similares.
- una referencia individual (código de ubicación del PNR)
- información sobre la agencia/el agente de viajes
- información sobre el boleto (número, fecha de la reserva, fecha de emisión, boletos sólo de ida)
- detalles tarifarios y las restricciones que posiblemente corresponden a dicha tarifa (y los impuestos relacionados)
- nombres y cantidad de otros pasajeros que viajan juntos en un mismo PNR
- situación del viaje del pasajero, incluidas confirmaciones, estado del check-in, información sobre "no show" o "go show";
- número de asiento y demás información relativa al asiento
- información sobre el código compartido
- información dividida (en los casos de itinerarios diferentes de varios pasajeros en un mismo PNR, los cambios deben integrarse a la reserva de un pasajero en un PNR existente)
- información sobre el equipaje
- el histórico de todos los cambios realizados al PNR sobre la información mencionada anteriormente.

En la práctica, el contenido de cada PNR variará en gran medida, dado que la cantidad y naturaleza de campos a completar dependerá del itinerario (por ej. en el caso de un itinerario circular que cubra varias ciudades en el mismo país o en varios países), la oferta de servicios ofrecidos por las aerolíneas y el sistema de reservas utilizado (en algunos casos más de 60 campos a completar).

El hecho de que la información recolectada es proporcionada por los pasajeros, o por otros en su nombre, y que dicha información no sea verificada sistemáticamente (con excepción por ejemplo de la información proporcionada por las aerolíneas y la información del pasaporte, cuando este último no es falso), también debe tenerse en cuenta en relación con el principio de precisión de la información. Hay lugar para el error: un PNR puede contener información incorrecta sobre una persona, lo cual, en algunos casos, podría levantar sospechas.

Las aerolíneas podrán estar obligadas a transferir la totalidad o parte de los datos de los PNR a las autoridades públicas competentes para identificar a las personas que se sospeche están implicadas en actividades terroristas o delitos graves.

3. Legalidad

Si bien es posible que los PNR beneficien a las autoridades públicas competentes en la

consecución de una finalidad legítima, es necesario que se cumplan algunas condiciones para que sea permitida la interferencia con los derechos a la vida privada y a la protección de datos.

De conformidad con la jurisprudencia emanada del Tribunal Europeo de Derechos Humanos, en relación con el artículo 8 del ECHR, dicha interferencia solo será permisible cuando se haga de acuerdo a derecho y sea estrictamente necesaria y proporcional al fin legítimo que persiga.

Aun cuando la evaluación de la necesidad de la interferencia y la proporcionalidad de las medidas consideradas deben ser estudiadas cuidadosamente a la luz de una variedad de elementos, el Comité recordará brevemente lo que el ECHR considera estar cubierto por la condición de legalidad. El requisito de que cualquier interferencia esté ‘en concordancia con la ley’ (o ‘prevista en la ley’ tal como se indica en el artículo 9 del Convenio 108) solamente se considerará cumplido cuando se satisfagan tres condiciones:

- la medida debe estar fundada de alguna manera en la legislación nacional,
- dicha legislación debe ser lo suficientemente clara y precisa como para ser accesible para la persona en cuestión (obviamente debe ser pública), y
- debe tener consecuencias predecibles (lo cual permitiría a la persona, de ser necesario y con el adecuado asesoramiento, regular su conducta y actuar en consecuencia)⁵.

En el contexto del tratamiento de PNR a través de las autoridades a cargo del cumplimiento de la ley, el criterio de la calidad de la ley implica una definición muy precisa y estricta de la finalidad legítima que se persigue.

4. Necesidad y proporcionalidad

Cualesquiera medidas prescritas o consideradas sobre el tratamiento de datos de un PNR por parte de las autoridades públicas competentes, en vista de la interferencia que podría acarrear frente a los derechos de los titulares de los datos, estarán sujetas al análisis de su necesidad y proporcionalidad. El Comité invita al análisis de elementos objetivos que permitan evaluar dicha necesidad, la proporcionalidad de las medidas prescritas así como también la eficiencia y eficacia del sistema (que debe ser demostrable en los casos en que dicho sistema ya exista).

El tratamiento de datos de un PNR – siempre y cuando el único beneficio al que conduzca el identificar a las personas en cuestión – sea el estudio general e indiscriminado de todos los pasajeros por parte de diversas autoridades competentes, incluidos quienes no sean sospechosos de delito alguno, y refiera a datos recolectados inicialmente por entidades privadas con fines comerciales. En virtud del grado de interferencia sobre los derechos a la vida privada y a la protección de datos que podría darse a partir de dicho procesamiento, el hecho de que el mismo es una medida necesaria en una sociedad democrática con una finalidad legítima, debe quedar claramente demostrado y deberá contarse con las salvaguardias adecuadas. Es necesario contar con una demostración específica de la necesidad de recolectar y luego utilizar datos de PNR.

El Tribunal Europeo de Derechos Humanos subrayó que “si bien el adjetivo ‘necesario’ [...]

⁵ ECHR Kennedy c. el Reino Unido, § 151; Rotaru c. Rumania, 28341/95, §§50, 52 y 55; Amann c. Suiza, § 50; Iordachi y otros c. Moldavia; Kruslin c. Francia, § 27; Huvig c. Francia, § 26; Asociación para la Integración de Europa y los Derechos Humanos y Ekimdzhiev c. Bulgaria, § 71; Libertad y otros c. el Reino Unido, § 59, etc.

no es sinónimo de 'indispensable', ninguno de los dos tiene la flexibilidad de expresiones como 'admisible', 'común', 'útil', 'razonable' o 'deseable'.”⁶

El Estado tiene un cierto margen de apreciación para elegir los medios necesarios para lograr su finalidad legítima y necesaria. No obstante, debe evaluar si la interferencia creada por dichas medidas se corresponde con una 'necesidad social apremiante'⁷⁷. La evaluación de la proporcionalidad de la excepción debe estar apoyada en el análisis de una gran variedad de elementos tales como la definición de finalidades claras y delimitadas, del alcance de la aplicación del sistema, de la naturaleza de los datos en cuestión, la naturaleza del tratamiento, las formas de acceso a los datos y de su conservación, etc.

Durante la definición al respecto de la validez de la Directiva sobre la Conservación de Datos (relativa a la conservación de datos de comunicaciones), el Tribunal de Justicia de la Unión Europea subrayó⁸ que “las excepciones a la protección de datos de carácter personal y las limitaciones de dicha protección deben establecerse sin sobrepasar los límites de lo estrictamente necesario”.

Cuando existan sistemas de procesamiento de datos de PNR de las autoridades públicas competentes, se deberá velar por una mayor transparencia al momento de evaluar la eficacia de dichos sistemas en pos de permitir una evaluación independiente sólida de la necesidad del sistema. En tanto la mencionada transparencia debe ser detallada, no deberá anteponerse a la finalidad legítima. Es decir, la información objetiva y cuantificable sobre los resultados obtenidos, tales como la cantidad de personas arrestadas, de amenazas terroristas que se evitaron, de otros efectos disuasorios, la modificación del comportamiento de delincuentes (como podría ser dejar de participar de delitos originalmente planificados), la probabilidad de que los costos y las dificultades de perpetrar un delito sean mayores (como en el caso de los ataques terroristas), contribuiría a evaluar si es necesario un sistema para PNR.

La necesidad de un sistema para PNR deberá revisarse regularmente a intervalos periódicos para adecuadamente justificar en tiempo su existencia.

5. Aplicación de los principios y salvaguardias

(a) Limitación de la finalidad

En virtud del nivel de la interferencia sobre los derechos a la vida privada y a la protección de datos que supone el procesamiento de datos de un PNR por parte de las autoridades públicas competentes, las finalidades deben ser claras y estar predefinidas con precisión por ley, sustentadas en criterios objetivos limitantes de la transmisión de los datos solamente hacia las autoridades con competencia en la materia, así como también del uso adicional de dichos datos.

Los sistemas para PNR generalmente están justificados sobre la base de la prevención, detección, investigación y procesamiento ante delitos terroristas y otros crímenes graves (como narcotráfico, trata de personas o tráfico de niños, lavado de dinero), u otros delitos internacionales (como crímenes de lesa humanidad, torturas o genocidios). Es necesario

⁶ Handyside c. Reino Unido, 5493/72, §48.

⁷ Olsson c. Suecia, 10465/83.

⁸ Digital Rights Ireland, C-293/12 del 8 de abril de 2014, §52.

contar con una delimitación clara de las finalidades legítimas y de las correspondientes nociones para circunscribir el uso de dichos sistemas de una manera estricta.

Las definiciones de 'terrorismo' y 'delitos terroristas' tienen una complejidad particular (véanse los correspondientes Convenios de la ONU, el Convenio del Consejo de Europa sobre la prevención del terrorismo de 2005 y su protocolo adicional de 2015). Ante la ausencia de una delimitación clara, esta terminología deberá ser interpretada de manera restrictiva. De no ser así, la finalidad del sistema para el PNR sería demasiado vaga y el principio de proporcionalidad no se estaría respetando.

En casos excepcionales, la prevención de amenazas graves al público (por ejemplo la prevención de la propagación de una enfermedad contagiosa peligrosa) también podría justificar el uso de datos de un PNR.

(b) Autoridades competentes

Para garantizar la proporcionalidad de la interferencia sobre los derechos de las personas en cuestión, las autoridades públicas que reciban los datos del PNR deberán ser las autoridades responsables de las finalidades legítimas previamente definidas.

Asimismo, el establecimiento de unidades de coordinación dedicadas (como las 'Unidades de Información de Pasajeros' en el esquema de la UE) contribuye a evitar una mezcla de actividades judiciales y de vigilancia pero las competencias de dichas unidades deben estar definidas de manera rigurosa y precisa, y ser públicas.

Las autoridades competentes nacionales legalmente autorizadas para procesar datos de un PNR deben estar enumeradas y ese listado debe estar públicamente disponible.

(c) Datos de naturaleza personal de los pasajeros

Los datos transmitidos y procesados posteriormente por las autoridades públicas competentes deben ser pertinentes, adecuados y no excesivos (artículo 5 del Convenio 108) en relación con las finalidades para las cuales se procesen. Los datos transmitidos deben estar claramente definidos (los elementos del PNR a transmitir deben estar exhaustivamente enumerados) sustentados en criterios objetivos y también deberán establecerse límites en relación con el uso adicional posterior de dichos datos.

Los PNR contienen información necesaria para facilitar el viaje del pasajero, y es posible que incluyan una cierta cantidad de datos sensibles que podrían servir para indicar el origen racial, opiniones políticas o convicciones religiosas o de otra índole, o datos relativos a la salud o a la orientación sexual de una persona, no solo mediante ciertos datos 'codificados' sino también en el campo abierto donde se incluyen las observaciones generales (como requisitos médicos o relativos a la dieta, o el hecho de que una asociación política o religiosa accedió a tarifas reducidas que utilizó en los viajes de sus miembros) lo cual podría conducir a discriminación directa.

Si bien las autoridades competentes que reciben los datos de los PNR pueden tener permitido el tratamiento en circunstancias excepcionales y estrictamente justificadas (no es

posible realizar una evaluación en base a criterios que tengan conexión con cualquier tipo de datos sensibles), el Comité considera que la prohibición del uso sistemático de dichos datos sensibles debe estar establecido como principio.

(d) Transmisión de datos

Hay dos métodos para transmitir datos desde el sector comercial a las autoridades competentes del sector público:

- por el método de 'extracción', donde las autoridades públicas directamente ingresan ('acceden') al sistema de reservas y toman ('extraen') de allí una copia de los datos necesarios;
- por el método de 'empujar', en el cual el operador transmite ('empuja') los datos requeridos de los PNR hacia la base de datos de la autoridad que los solicita.

El Comité entiende que debe preferirse el método de 'empujar', donde el operador es completamente responsable de la calidad de los datos y de las condiciones de transmisión, ya que ofrece mayores salvaguardias a la protección de los datos que el método de 'extracción'.

(e) Emparejamiento y minería de datos

El tratamiento de datos de carácter personal puede afectar a todos los pasajeros y no solo a las personas marcadas como sospechosas de estar implicadas en delitos o de suponer una amenaza inmediata sobre la seguridad nacional o el orden público.

Los datos de PNR pueden ser comparados ('emparejamiento de datos') con bases de datos⁹ de las autoridades competentes de conformidad con la ley (por ejemplo de personas con condenas por delitos graves, de personas que están siendo investigadas como sospechosas de actividad terrorista, de pasaportes extraviados o robados), para identificar sospechosos o criminales, así como también personas relacionadas con dichos sospechosos o criminales potenciales ('encadenamiento de contactos').

Los datos de los PNR también pueden procesarse con la intención de identificar a cualquier persona que 'podría' estar implicada en actividades delictivas, o que 'podría en un futuro' estar relacionada con actividades delictivas tales y como las define la ley que determina la difusión de los PNR ante las autoridades competentes, por ej. en el caso de personas en viaje para convertirse en combatientes terroristas extranjeros. Esto es posible mediante 'minería de datos' utilizando selectores o según algoritmos predictivos.

Esta evaluación de pasajeros mediante minería de datos puede hacer surgir el tema de la predictabilidad, en especial cuando se opera basado en algoritmos predictivos utilizando criterios dinámicos que podrían evolucionar constantemente a la luz de las capacidades de auto aprendizaje.

El desarrollo de algoritmos de minería de datos debe estar fundado en los resultados de evaluaciones regulares del posible impacto del tratamiento de datos sobre los derechos y las libertades fundamentales de los titulares de los datos.

⁹ Bases de datos creadas, operadas y actualizadas de conformidad con la ley.

La estructura básica de los análisis debería estar asentada sobre indicadores de riesgo predefinidos que hayan sido identificados claramente con anterioridad.

La pertinencia de los resultados individuales de dichas evaluaciones automáticas debe ser analizada cuidadosamente, caso por caso, por una persona y de una manera no automatizada.

(f) Conservación de los datos

El período de retención de los datos del PNR debe estar claramente especificado y limitado al tiempo absolutamente necesario para la finalidad prescrita y debe estar “sustentado por criterios objetivos para asegurar que está limitado a lo estrictamente necesario”¹⁰. Dichos criterios deben estar disponibles al público.

El enmascaramiento¹¹ de algunos elementos de los datos que identifican al pasajero, pasado un período de tiempo predeterminado y tan breve como sea posible, puede mitigar los riesgos que conlleva un período de conservación más largo de los datos de todos los pasajeros, como sería por ejemplo el acceso abusivo.

Es necesario que se recuerde que los datos enmascarados aún permiten la identificación de las personas y como tales, continúan constituyendo datos de naturaleza personal. Su conservación también entonces debe limitarse en el tiempo de modo de evitar la vigilancia permanente y general.

(g) Derechos a la información, al acceso, a la rectificación y a la supresión

El Comité recuerda que de conformidad con el artículo 1 tanto del ECHR como del Convenio 108, los derechos a la privacidad y a la protección de datos deben estar garantizados para todas las personas dentro del ámbito de competencia de las partes contratantes, independientemente de su nacionalidad o lugar de residencia.

La persona cuyos datos de los PNR están siendo transmitidos a las autoridades competentes tiene derecho a saber qué tratamiento están dando dichas autoridades a esos datos (naturaleza de los datos, finalidad y manera, lapso), tiene derecho al acceso y a solicitar la rectificación o supresión de los datos personales.

Si bien dichos derechos pueden estar limitados por las condiciones restrictivas mencionadas previamente (en consonancia con la legislación y necesario en pos de los intereses de una finalidad legítima), el Comité recomienda que las personas que no estén bajo sospecha de haber cometido un delito terrorista u otro delito grave o bajo sospecha de estar por cometerlo, goce del pleno ejercicio de esos derechos. Las personas que se sospeche han cometido o están por cometer dichos delitos podrán al menos solicitar la corrección de datos imprecisos y la supresión de datos ilegales.

Cualquier limitación en relación con esos derechos debe ser informada a los pasajeros al momento en que sus datos son recolectados y durante todo el proceso de tratamiento por parte de las autoridades públicas competentes.

¹⁰ Digital Rights Ireland, C-293/12 del 8 de abril de 2014 §64.

¹¹ ‘Enmascarar’ significa hacer invisible ciertos elementos de los datos que permiten la identificación de una persona.

En los casos en que se hayan recolectado datos sobre un pasajero sin que este lo supiera, y a no ser que los datos se supriman, esa persona deberá ser informada sobre el hecho, cuando sea posible, tan pronto como el objeto de la finalidad de la recolección ya no sea potencialmente perjudicable.

Las personas en cuestión deben ser informadas sobre cómo ejercer sus derechos y saber qué recursos tienen a disposición.

(h) Seguridad

Según el artículo 7 del Convenio 108, es requisito tomar las medidas de seguridad adecuadas para proteger los datos personales. Principalmente, esto implica que el sistema de los PNR se mantenga en un entorno físico seguro, con controles de intrusión de alto nivel y un estricto control de acceso (limitado a ciertas personas), con características como inicios de sesión con autenticación adicional y la generación de un registro de acceso con auditoría. Asimismo, la comunicación de los datos en los PNR a las autoridades competentes deberá estar protegida con medios técnicos y procedimentales (por ej. cifrados complejos, procedimientos efectivos de gestión de claves, etc.).

(i) Flujo de datos transfronterizo

El Comité recuerda que cualquier transferencia de datos de PNR a Estados que no sean Parte del Convenio 108 debe cumplir con las condiciones establecidas para garantizar la protección adecuada de los titulares de los datos en dichos Estados.

(j) Recursos

Es requisito esencial de la jurisprudencia emanada del Tribunal Europeo de Derechos Humanos que existan “recursos efectivos” contra la vulneración de los derechos fundamentales y que los mismos estén disponibles para las personas (y no solamente para quienes tienen la nacionalidad del país en cuestión). En tanto el Tribunal de Justicia de la Unión Europea menciona expresamente el requisito de la reparación ante un tribunal, el Tribunal Europeo de Derechos Humanos dictaminó¹² que la ausencia de control judicial no constituye necesariamente una vulneración a los derechos en juego siempre y cuando se proporcione otras salvaguardias fuertes por parte de la legislación (por ejemplo supervisión independiente de autoridades investidas con las suficientes potestades y competencias para ejercer un control efectivo y continuo).

El artículo 10 del Convenio 108 requiere que las Partes “establezcan sanciones y recursos convenientes contra las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos” enunciados en el Convenio.

El Comité apoya la necesidad de ofrecer una reparación efectiva a las personas, la cual debería cubrir tanto el recurso administrativo como el judicial. El Comité además pone énfasis en la importancia, como condición previa a un recurso efectivo, de que la persona en cuestión esté completamente informada en relación con el tratamiento de sus datos personales, y subraya las dificultades que existen para ofrecer recursos efectivos sobre

¹² Klass y otros c. Alemania, §§ 55-56; Kennedy c. el Reino Unido, § 167.

decisiones tomadas en base a algoritmos e interferencias problemáticas, al estar estas basadas en análisis de datos (con medidas discriminatorias como falsos positivos y otras).

(k) Supervisión y transparencia

Se desprende claramente de la jurisprudencia del Tribunal Europeo de Derechos Humanos que la supervisión a las autoridades responsables de vigilar debería ser llevada a cabo por un organismo independiente y externo.

El Comité subraya el papel de las autoridades competentes en la protección de datos, las cuales no solo deberían ser consultadas durante el proceso normativo ante la adopción de las leyes y reglamentos relacionados, sino que también podrían evaluar el cumplimiento de un sistema para PRN en cuanto a las reglas de protección de datos en base a reclamos individuales que podrían recibir, o como iniciativa propia.

Otras autoridades independientes especializadas (como podría ser una comisión parlamentaria) encargadas de supervisar el cumplimiento de la legislación y las agencias de inteligencia también pueden controlar el alcance de aplicación del sistema, su eficiencia, y realizar controles caso a caso sobre los fundamentos detrás de la conservación de datos de pasajeros y la duración de dicha conservación.

La supervisión realizada por autoridades independientes en protección de datos, a través de autoridades independientes especializadas encargadas de supervisar el cumplimiento de la ley y las agencias de inteligencia, así como también a través de evaluaciones independientes de la eficiencia por parte de las mismas autoridades competentes, podrían conducir a mayores niveles de transparencia y rendición de cuentas de las capacidades y competencias de un sistema de PNR.

Adicionalmente, dentro de las autoridades competentes que realicen el tratamiento de datos de PNR debería designarse personal dedicado a la protección de los datos para asegurar el cumplimiento y la adecuada respuesta del sistema (con evaluaciones regulares de los riesgos en juego y auditorías sistemáticas de los PNR), del procesamiento de datos y de la comunicación de los datos, su actualización y supresión, así como la información suministrada a los pasajeros. Los funcionarios encargados de la protección de datos también podrían desempeñarse como puntos de contacto en caso de reclamos o solicitudes de las personas en cuestión. Se los anima a crear conciencia sobre las “buenas prácticas”.

6. Conclusiones

En vista de la especial interferencia sobre los derechos a la protección de datos y a la privacidad que podrían representar las medidas sobre los PNR, la legalidad, proporcionalidad y necesidad de un sistema para PNR deben ser estrictamente respetadas y demostradas, lo cual implica principalmente lo siguiente:

- comprobación transparente y de manera medible de la necesidad y proporcionalidad del sistema a la luz de la finalidad legítima que se persiga;
- son necesarias las definiciones precisas y rigurosas de la finalidad legítima perseguida y el tratamiento de datos de PNR solo está permitido ante el trasfondo limitado definido (prevención, detección, investigación y procesamiento ante delitos terroristas y otros crímenes graves, o en casos excepcionales, la prevención de amenazas graves al público);
- publicidad de las autoridades públicas competentes (idealmente con unidades de coordinación dedicadas);
- transmisión de datos utilizando el ‘método de empujar’, con una definición clara del lapso inicial de mantenimiento y de las medidas de seguridad adecuadas;
- prohibición del uso sistemático de datos sensibles;
- minería de datos limitada a indicadores de riesgo previamente definidos, con análisis caso a caso no automatizado de la pertinencia de los resultados;
- limitaciones legales y solo necesarias a los derechos de las personas a la información, al acceso, a la rectificación y a la supresión de datos;
- competencia de las autoridades de protección de datos (para ser consultadas y con capacidad para evaluar al sistema para PNR así como para atender reclamos personales);
- disponibilidad de recursos efectivos administrativos y judiciales para las personas;
- supervisión independiente y externa del sistema para PNR;
- revisión periódica de los sistemas para PNR por parte de las autoridades competentes.