Universidad Carlos III de Madrid

Máster Universitario en Derecho de las Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información (Curso 2015-2016)

Trabajo Fin de Máster

"Informe a la Dirección General de Migración de la República Dominicana sobre el nivel adecuado de protección a garantizar como receptora de datos PNR de ciudadanos europeos, en virtud de la Directiva 2016/681 de utilización de datos del registro de nombres de los pasajeros"

Francisbel Yanilsa Jerez Castillo

Tutor/a:

María Nieves de la Serna Bilbao

Madrid, 1 de julio de 2016.

Palabras clave: datos PNR, datos API, transferencia internacional de datos, nivel adecuado de protección.

Resumen: el presente informe cumple con el objetivo de dar respuesta a la consulta planteada por la Dirección General de Migración de la República Dominicana, a fin de conocer cuáles son las implicaciones que trae consigo la reciente aprobación la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR), en relación al flujo de datos de ciudadanos europeos, con destino o salida del territorio dominicano. De igual manera, son detalladas las medidas que deben adoptarse en virtud de dicha Directiva para ofrecer las garantías adecuadas que constituyan un nivel equivalente de protección de datos.

ÍNDICE

INTRODUCCIÓN

Es consabido, que el turismo es un sector que ocupa un lugar de alta preponderancia dentro de la economía de la República Dominicana. Cifras oficiales indican que dicho sector representa un aporte superior al 7% del producto interno bruto.[1] Solo en el mes de mayo del presente año, la llegada de pasajeros no residentes a la República Dominicana por vía aérea alcanzó un total de 437,338 viajeros, aumentando en 20,354 pasajeros con respecto al mismo mes del año anterior, lo cual representa una tasa de crecimiento anualizada de 4.9 por ciento, siendo Europa la región que más aportó a esta cifra en términos absolutos, con 6,366 viajeros adicionales (9.1% de crecimiento interanual).[2]

Dentro de las nuevas reformas de protección de datos que han acometido las instituciones de la Unión Europea, se ha dictado una directiva que afecta directamente las transferencias de datos personales ínsitas a todo flujo de pasajeros, se trata de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, (en lo sucesivo, Directiva 2016/681).

El informe que se desarrolla en las páginas que se encuentran a seguidas, ha sido solicitado por el órgano de control fronterizo y migratorio de la República Dominicana, la Dirección General de Migración, con el propósito de conocer las implicaciones y nuevas obligaciones que establece la Directiva 2016/681, a fin de cumplir con las condiciones necesarias para proporcionar las garantías adecuadas que constituyan un nivel equivalente de protección de datos, que inspire confianza y genere seguridad a

[1] Banco Central de la República Dominicana. *Estadísticas turísticas 2015*, Santo Domingo, abril de 2016. Publicación disponible en la web: http://www.bancentral.gov.do/publicaciones_economicas/turisticas/turisticas2015-12.pdf [Fecha de consulta: 1-6-2016]

[2] Banco Central de la República. *Informe del flujo turístico enero - mayo 2016*. Publicación disponible en: http://www.bancentral.gov.do/publicaciones_economicas/informe_turistico/informe_turistico2016-05.pdf [Fecha de consulta: 1-6-2016]

todo visitante que provenga de los países miembros de la Unión, mejorando la marca país y la calidad del turismo como producto.

Para cumplir con tales aspiraciones, hemos elaborado un esquema que parte de los antecedentes de hecho que dieron lugar a la aprobación de la Directiva y al interés del país caribeño por garantizar su cumplimiento. Luego, se identifica el nivel de protección que brinda la legislación dominicana en materia de protección de datos. Consecuentemente, se realiza un examen del contenido de la Directiva (UE) 2016/681, y para finalizar se detallan las medidas que deben ser tomadas para cumplir con los requerimientos de la Directiva (UE) 2016/681.

1. ANTECEDENTES DE HECHO

Hoy más que nunca, es una realidad indiscutible, el asedio al que se encuentra sometida la comunidad internacional por parte de los grupos de criminalidad organizada. En las últimas décadas, se ha registrado una cantidad alarmante de atentados terroristas que mantienen en vilo a las sociedades del mundo. La sensación de inseguridad que generan estas conductas ha traído consigo la adopción de numerosos compromisos internacionales, suscritos con miras a combatir tal realidad, siendo uno de los más recientes el Plan de acción para prevenir la violencia extremista adoptado en diciembre de 2015, por la Asamblea General que congrega a los 193 países miembros de la Organización de las Naciones Unidas.[3]

El hecho de que en los últimos años las ciudades europeas se hayan convertido en el objetivo capital de grupos terroristas radicales, ha propiciado que la Unión Europea dirigiese sus esfuerzos a la prevención, detección, investigación y enjuiciamiento de este tipo de conductas. Así lo revelan instrumentos como la Decisión Marco del Consejo sobre la lucha contra el terrorismo[4], la Declaración sobre la lucha contra el terrorismo[5], la Estrategia Europea para la lucha contra el terrorismo[6], la Comunicación de la Comisión de las Comunidades Europeas para garantizar el espacio de libertad, seguridad y justicia[7], el Programa de Estocolmo para una Europa abierta y segura que sirva y proteja al ciudadano[8], entre otros.

---

[3] Organización de las Naciones Unidas, Plan de acción para prevenir el extremismo violento, Asamblea General, 24 de diciembre de 2015. Disponible en web: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/674&referer=/english/&Lang=S [Fecha de consulta: 1-6-2016]

[4] Consejo de la Unión Europea, DECISIÓN MARCO DEL CONSEJO de 13 de junio de 2002sobre la lucha contra el terrorismo (2002/475/JAI), *Diario Oficial de las Comunidades Europeas,* de fecha 22 de junio de 2002.

[5] Consejo de la Unión Europea, Declaración sobre la lucha contra el terrorismo, Bruselas, de 25 de marzo de 2004. Disponible en la web: http://www.realinstitutoelcano.org/especiales/atentados/docs/declaracterrorUE25304.pdf [Fecha de consulta: 1-6-2016]

[6] Consejo de la Unión Europea, Estrategia Europea sobre la lucha contra el terrorismo de fecha 30 de noviembre de 2005, Disponible en la web: http://register.consilium.europa.eu/doc/srv?f=ST+14469+2005+REV+4&l=es [Fecha de consulta: 1-6-2016]

[7] Comisión Europea, Comunicación de la Comisión de las Comunidades Europeas sobre el espacio de libertad, seguridad y justicia, de fecha 20 de abril de 2010. Disponible en la web: http://eur-

Es innegable que flagelos como el terrorismo ponen en juego la paz, la estabilidad, la seguridad y los derechos fundamentales de las personas, valores universales sobre los cuales se han construido las sociedades democráticas. En la Decisión Marco del Consejo sobre la lucha contra el terrorismo se afirma, que el terrorismo constituye una de las violaciones más graves de los referidos principios democráticos.[9] Asimismo, en los informes de Europol sobre el terrorismo en Europa se ha puesto de relieve que casi todas las campañas terroristas implican desplazamientos internacionales, indicando que los aspectos interior y exterior están íntimamente relacionados y que, para garantizar la eficacia de las medidas destinadas a combatir los actos terroristas, se hace necesaria una estrecha colaboración que refuerce el intercambio de información entre los Estados miembros y sus respectivos servicios, así como con Europol, y si procede, con las autoridades competentes de terceros países.[10]

Sumado a lo anteriormente expresado, huelga decir que los avances tecnológicos que en la actualidad tenemos a nuestro alcance, también han facilitado la perpetración de delitos graves como la trata de personas o el narcotráfico, que involucran y afectan a ciudadanos de todos los países del mundo, lo cual justifica el incremento de medidas tendientes a garantizar la seguridad de los ciudadanos y frenar la consecución de los objetivos de los delincuentes. Habida cuenta de que los miembros de los grupos de delincuencia organizada se valen de todos los canales posibles para cometer actos terroristas o delitos considerados graves, las naciones han establecido sistemas de control fronterizos y migratorios más rígidos, para mitigar la posibilidad de consumación de estos actos deleznables.

En el contexto que hemos venido exponiendo en los párrafos anteriores, ha tenido lugar la aprobación de la Directiva (UE) 2016/681 del Parlamento Europeo y del

---

lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0171&from=ES [Fecha de consulta: 2-6-2016]

[8] Consejo Europeo, Programa de Estocolmo para una Europa abierta y segura que sirva y proteja al ciudadano, *Diario Oficial de la Unión Europea* n˚ C 115/1, de 4 de mayo de 2010.

[9] Decisión Marco del Consejo de 13 de junio de 2002 sobre la lucha contra el terrorismo. *Diario Oficial de las Comunidades Europeas*, n˚ L 164/3, 22 de junio de 2002.

[10] EU Terrorism Situation and Trend Report 2007 citado en Consejo Europeo. *Propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record—PNR) con fines policiales*, 2007. Disponible en web: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/com/com_com(2007)0654_/com_com(2007)0654_es.pdf [Fecha de consulta: 8-5-16]

Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR), para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, cuya fecha límite de transposición es el 25 de mayo de 2018. Este nuevo cuerpo normativo evidentemente contiene disposiciones que regularán la transferencia internacional de los datos PNR a terceros países, y que exigen que se garantice un adecuado nivel de protección de datos personales, tomando como parámetro el derecho de la Unión Europea.

Naturalmente, la aprobación de esta nueva Directiva no se produjo al azar, ya en la Estrategia de la Unión Europea de 2005 para la lucha contra el terrorismo, se asumía como segunda prioridad, la protección de las fronteras exteriores, la mejora de la seguridad de los transportes, la reducción de los objetivos estratégicos y la reducción de la vulnerabilidad de las infraestructuras clave, haciendo el señalamiento de que en ese ámbito, la Unión estaba trabajando en una legislación para regular el uso de los datos del registro de nombres de los pasajeros (PNR), con fines coercitivos.[11]

Hay que tomar en consideración, que con anterioridad a esta Directiva que faculta a los Estados miembros a utilizar los datos del registro de nombre de pasajeros (PNR) con fines represivos, en el año 2004 fue aprobada la Directiva 2004/82/CE del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas, en interés de luchar de manera eficaz contra la inmigración ilegal y mejorar el control fronterizo, así como armonizar, en la medida de lo posible, las sanciones pecuniarias previstas en los Estados miembros, ante los incumplimientos de estas obligaciones.

Posteriormente, en el año 2007 se publicó la Propuesta de Decisión Marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros *(Passenger Name Record--PNR).* Sin embargo, por imperio del Tratado de Lisboa que entró en vigor el 1 de diciembre de 2009[12], esta propuesta quedó obsoleta, no siendo retomada hasta el año 2011, luego de que en el Programa de Estocolmo para una Europa abierta y segura

[11]Consejo de la Unión Europea. *Estrategia de la Unión Europea de 2005 para la lucha contra el terrorismo*, 30 de noviembre de 2005.

[12] El tratado de Lisboa que entró en vigor el 1 de diciembre de 2009 modificó el Tratado de la Unión Europea y el Tratado Constitutivo de las Comunidades Europeas.

se instara a la Comisión Europea a presentar una propuesta sobre la utilización de datos del registro de nombres de los pasajeros (en lo adelante, datos PNR) para prevenir, detectar, investigar y enjuiciar los delitos terroristas y los delitos graves.[13]

Consecuentemente, fue publicada la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves. Sin embargo, esta propuesta no fue acogida, en razón de que las instituciones de la Unión Europea tenían posiciones encontradas por las posibles afectaciones al derecho a la privacidad y a la protección de datos de carácter personal que dicha propuesta contenía.

La ausencia de una regulación armonizada a nivel europeo, no solo perjudicaba a las aerolíneas, al mismo tiempo disminuía la posibilidad de cooperación eficaz entre las autoridades encargadas de prevención y enjuiciamiento de delitos, ello es así porque a lo interno de la Unión, si bien es cierto que la mayoría de los países miembros utiliza los datos PNR para prevenir, detectar, investigar y enjuiciar los delitos graves y los delitos terroristas, sólo un número reducido de ellos ha establecido un sistema PNR, es decir, su utilización se lleva a cabo de forma no sistemática o en virtud de poderes generales conferidos a la policía y otras autoridades.[14] Por otro lado, no existía como tal una disposición que obligara a las aerolíneas a la transferencia de estos datos, todo lo cual generaba incertidumbre.

Todas estas circunstancias hacían necesaria la adopción de estándares que facilitaran la labor de las aerolíneas, que además se enfrentaban a la realidad de que legislaciones de terceros países sí contemplaban la obligación de traslado de estos datos con la imposición de sanciones por su incumplimiento, empero la adopción de las medidas que satisficiesen esas necesidades evidentemente tenía que ser acorde con la garantía de protección de los derechos fundamentales y muy especialmente, el de la protección de datos proporcionado por el derecho comunitario.

[13] Consejo Europeo, Programa de Estocolmo para una Europa abierta y segura que sirva y proteja al ciudadano. Op. cit.

[14] Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, 2011, pág.4.

Independientemente de que previo a la aprobación de la Directiva 2016/681 no existiese un marco legal armonizado sobre la utilización de datos PNR en la Unión, sus normas de protección de datos habían sido bastante claras en la prohibición de transferencia internacional de datos a terceros países que no proporcionasen un adecuado nivel de protección o unas garantías idóneas. Por tanto, cuando en virtud el derecho interno de Estados Unidos, Canadá y Australia, se les solicitó a las compañías aéreas la transmisión de datos PNR sobre vuelos con destino a estos países, las compañías europeas tuvieron que afrontar a una situación muy difícil. Para dar salida a este impasse, la Unión Europea negoció y firmó acuerdos bilaterales de transferencia de datos PNR con cada uno de estos tres países.[15]

La directiva que nos ocupa fue aprobada en vista del escenario descrito precedentemente, y en el entendido de que dentro de la Unión Europea, los objetivos de prevención, detección, investigación, y enjuiciamiento de los delitos de terrorismo y la delincuencia grave a través del tratamiento de datos PNR, no se verían satisfechos por cada Estado miembro de manera aislada y por el contrario, podrían ser alcanzados a escala de la Unión.

Habiendo hecho un recorrido sucinto por los antecedentes que motivaron la aprobación de la Directiva 2016/681, es momento de reseñar las motivaciones por las cuales la República Dominicana, y siendo más específicos, el organismo encargado del control fronterizo y migratorio, la Dirección General de Migración de este país, se inclina por estar al tanto de los requerimientos a observar, a fin de suministrar unas garantías adecuadas de conformidad con la mencionada Directiva 2016/681.

Es incuestionable que la República Dominicana se encuentra en una posición geográfica privilegiada, ya que al ocupar la parte oriental de la isla de Santo Domingo cuenta con salidas directas hacia el océano Atlántico, al mar Caribe, y al Canal de la Mona, lo cual facilita enormemente las conexiones con Norteamérica, Centroamérica y

[15]http://www.consilium.europa.eu/es/policies/fight-against-terrorism/passenger-name-record/

Suramérica, con Europa y con África, más aún cuando el país caribeño cuenta con ocho aeropuertos internacionales en operatividad.[16]

Esta ubicación geográfica privilegiada que la sitúa como uno de los destinos más favorecedores de la región para el transporte de mercancías y personas, con las ventajas comerciales y económicas que esto conlleva, a su vez comporta riesgos muy serios, en la medida de que es considerada por los delincuentes como estratégica y favorecedora para el alcance de sus objetivos, lo que acredita la imperiosa necesidad de contar con unos controles fronterizos y migratorios suficientes, que efectivamente permitan la prevención de delitos graves.

Por lo expuesto anteriormente, Ley No. 285-04 de 15 de agosto del año 2004, General de Migración de la República Dominicana, contiene disposiciones que obligan a las compañías aéreas que realicen vuelos con salida o destino de los aeropuertos de la República Dominicana, a transferir los datos del registro de nombres de pasajeros (PNR), y asimismo en virtud de lo previsto en la misma Ley y en la Resolución No. DGM-04-12 dictada por el propio organismo de control migratorio, son requeridos los datos de información anticipada de pasajeros *(Advanced Passenger Information- API),* sobre los cuales abundaremos más adelante.

La referida Ley No. 285-04 en sus artículos 90 y 91 establece lo siguiente:

> *´´Art. 90.- Antes del arribo de sus aeronaves al país, las compañías de transporte aéreo deberán comunicar a las autoridades migratorias la cantidad de pasajeros que conducen a la República Dominicana, sean éstos en tránsito o de destino, adelantando de ser posible la nómina de los mismos.*
>
> *Art. 91.- El Comandante de la aeronave, o el funcionario designado por la compañía respectiva, deberá entregar antes del desembarco, a las autoridades*

[16]Aeropuerto Internacional de las Américas (SDQ), Aeropuerto Internacional La Isabela (JBQ), Aeropuerto Internacional María Montez (BRX), Aeropuerto Internacional de La Romana (LRM), Aeropuerto Internacional General Gregorio Luperón (POP), Aeropuerto Internacional de Punta Cana (PUJ), Aeropuerto Internacional Presidente Juan Bosch (AZS), y Aeropuerto Internacional del Cibao (STI).

encargadas del control migratorio, la lista de pasajeros y de tripulantes, remitiéndole copia de la misma a la Dirección General de Migración.´´[17]

Otro aspecto a considerar, es el hecho de que las autoridades dominicanas se han caracterizado a lo largo de los años por propender al reforzamiento de los lazos de cooperación con la comunidad internacional, y a la optimización de los instrumentos internacionales de asistencia judicial civil y penal. Las buenas prácticas dominicanas en materia de cooperación internacional, pueden verse reflejadas en la asunción de varios compromisos con países miembros de la Unión Europe en materia de prevención y castigo de las conductas delictivas.[18] Sumado a esto, muy recientemente el Ministerio de Relaciones Exteriores de la República Dominicana, conjuntamente con el Programa de las Naciones Unidas para el Desarrollo (PNUD), publicó el Inventario de Experiencias de Cooperación Internacional de la República Dominicana, que posiciona al Estado dominicano no sólo como receptor de cooperación sino también como oferente.[19]

Como hemos dicho, la economía dominicana depende en gran medida de las divisas generadas por el turismo. El tráfico económico derivado del flujo de pasajeros con entrada o salida del territorio insular ostenta una importancia capital para el sostenimiento de la economía. En vista de que como hemos expresado, las normas de protección de datos de la Unión Europea no permiten que las compañías aéreas que realizan vuelos desde su territorio, transmitan los datos PNR de sus ciudadanos, a terceros países que no garanticen un nivel adecuado de protección, es menester proporcionar las garantías adecuadas que acrediten a la Dirección General de Migración de la República Dominicana, como un organismo que proporciona las

[17] REPÚBLICA DOMINICANA. Ley 285-04, General de Migración *de* 15 de agosto de 2004*, Gaceta Oficial* No. 10291 del 27 de agosto de 2004.

[18] Para ilustrar esta cuestión, a modo de ejemplo, pueden mencionarse los siguientes acuerdos, firmados entre la República Dominicana y países miembros de la Unión Europea: Acuerdo entre la República Dominicana y el Reino de España sobre Cooperación en Materia de Prevención del Consumo y Control del Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas de 15 de noviembre de 2000, el Tratado Bilateral de Cooperación Judicial Penal entre Francia y República Dominicana firmado en Madrid l 15 de septiembre de 2003, el Tratado de Asistencia Jurídica Mutua entre el Reino de España y la República Dominicana firmado en Madrid, el 4 de mayo de 1981.

[19]Cancillería y PNUD publican inventario de buenas prácticas institucionales, *Diario Libre*, 6 de junio de 2016. Disponible en la web:
http://www.diariolibre.com/noticias/cancilleria-y-pnud-publican-inventario-de-buenas-practicas-institucionales-MG3967853 [Fecha de consulta: 6-6-16]

garantías suficientes en el tratamiento de los datos PNR, puesto que por las razones que hemos apuntado *ut supra*, este país no puede permitirse dejar de recabar los datos PNR procedentes de pasajeros europeos.

Del mismo modo, conviene destacar que las autoridades de la República Dominicana no tienen el interés de colocar a las compañías aéreas en la encrucijada de ser multadas por la normativa dominicana, si respetan el derecho comunitario, o de ser sancionadas por el derecho de la Unión si transmiten a las autoridades dominicanas los datos de pasajeros con entrada o salida de sus aeropuertos. Lejos de generar incertidumbre que aleje la inversión extranjera, y el periplo de turistas, las instituciones del país antillano están muy encaminadas a atraerlos a través de la seguridad jurídica, y la garantía de los derechos fundamentales.

Por todas estas razones y antecedentes, es que la Dirección General de Migración de la República Dominicana ha solicitado este informe a fin de que emita mi opinión en derecho sobre la siguiente cuestión esencial para que la economía del país no sufra perjuicios:

¿Cuáles son las medidas a las cuales debe abocarse, de ser necesario, para brindar un nivel equiparable de protección en el tratamiento de datos PNR, por parte de sus autoridades aeroportuarias, en atención a la Directiva 2016/681?

Con carácter previo a emitir la opinión que se me solicita, es preciso partir de conocer cuál es el nivel de protección de datos que contiene la legislación dominicana, tema sobre el cual versa el próximo apartado.

2. IDENTIFICACIÓN DEL NIVEL DE PROTECCIÓN DE DATOS DE LA REPÚBLICA DOMINICANA

A seguidas, nos detendremos a detallar una de las cuestiones neurálgicas para cumplir con las aspiraciones de este informe, y es que antes de referirnos a las medidas que deben ser observadas, en atención a las novedades que contiene la Directiva de utilización de datos del registro de nombre de los pasajeros, resulta lógico identificar el nivel de protección de datos existente en la República Dominicana.

Ello es así, en razón de que en el marco normativo europeo de protección de datos personales, conformado esencialmente por la Carta de los Derechos Fundamentales de la Unión Europea, el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio n˚ 108), el Convenio para la protección de los derechos humanos y de las libertades fundamentales (CEDH) y la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se establece que para permitir la transferencia de datos a terceros países, el tercer país debe proporcionar un adecuado nivel de protección.

A mayor abundamiento, la Directiva 95/46/CE, dispone que la transferencia de datos personales a un país tercero únicamente puede efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la Directiva en cuestión, ese país tercero garantice un nivel de protección adecuado. [20]

La Directiva 95/46/CE también apunta, que el carácter adecuado del nivel de protección se evalúa tomando en cuenta todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, ´´*se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.*´´[21]

Del mismo modo, la Directiva de protección de datos reconoce la facultad a la Comisión Europea de poder hacer constar, que un país tercero garantiza un nivel de protección adecuado a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones a efectos de

[20] DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de las Comunidades Europeas* n˚ L 281/31de23 de noviembre de 1995.
[21] Ídem

protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.[22]

En este punto, resulta imperativo indicar que en fecha 14 de abril del año en curso fue aprobado el **nuevo Reglamento General de Protección de Datos que deroga la Directiva 95/46/CE**, y que será obligatorio en todos sus elementos y directamente aplicable en los Estados miembros de la Unión Europea a partir de 2018. Dicho lo anterior, es de toda lógica informar sobre las implicaciones que tendrá en las materias que atañen a este informe ya que de cara al futuro será lo aplicable.

Las disposiciones del nuevo reglamento en relación a la transferencia internacional de datos mantienen consonancia con las disposiciones fundamentales de la Directiva todavía vigente, tal es así que como principio general instaura que todas las disposiciones del capítulo dedicado a la transferencia de datos a terceros países u organizaciones internacionales, se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el Reglamento no se vea menoscabado[23], es decir que no se menoscabe el nivel adecuado protección, cuando se produzcan dichas transferencias.

No obstante, es menester decir, que el nuevo reglamento ahonda en la ordenación de dichas transferencias pormenorizando con mayor claridad y extensión cómo deben ser llevadas a cabo. En tal sentido y en lo que importa a este trabajo, establece que:

> *´´1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.*
>
> *2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:*
>
> *a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la*

[22] Ídem.

[23] REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO 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), de 14 de abril de 2016, artículo 44.

legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos. b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional […] c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.´´[24]

En adición a ello, dentro del acápite dedicado a la regulación de las transferencias internacionales de datos, el nuevo Reglamento contiene, en su artículo 50, un apartado sobre la cooperación internacional en el ámbito de la protección de datos personales. El referido artículo reza de la siguiente manera:

´´En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para:

a) ***crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales****;*

b) ***prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales****, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales;*

c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

[24] Ibídem, artículo 45.

> *d)* ***promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países****.´´*[25]

Ahora bien, centrándonos en el tema que intitula este apartado, que es el diagnóstico del nivel de protección de datos dentro del sistema jurídico dominicano, hemos de decir que el derecho a la protección de datos personales se encuentra consagrado como derecho fundamental en el artículo 44.2 de la Constitución dominicana en vigor[26]. Dicho artículo estipula que:

> *´´Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos*.´´ [27]

Se observa pues, que en interés de salvaguardar el derecho a la autodeterminación informativa, desde la carta sustantiva de la República Dominicana se le reconoce al titular de los datos el plexo de facultades estandarizado internacionalmente en materia de protección de datos personales, y son elevados a rango constitucional los principios que informan el derecho a la protección de datos.

Asimismo, tal consagración como derecho fundamental legitima su exigencia a través de una acción preferente, sumaria, oral, pública, gratuita y no sujeta a formalidades, encausada ante la jurisdicción constitucional, para exigir la protección inmediata del derecho fundamental, cuando resulte vulnerado o amenazado por la acción u omisión de toda autoridad pública o de particulares, o para hacer efectivo el cumplimiento de una ley o acto administrativo, o para garantizar los derechos e intereses colectivos y difusos. Esta acción instituida en el artículo 70 de la referida Constitución, es la acción de *Hábeas Data*, entendida como el amparo del derecho a la autodeterminación

[25] Ibídem, artículo 50. (Las negritas son nuestras)
[26] República Dominicana, Constitución Política, votada y proclamada por la Asamblea Nacional en fecha 13 de junio de 2015 *Gaceta Oficial* No. 10805 del 10 de julio de 2015.
[27] Ibídem, artículo 44.2.

informativa.[28] Este criterio ha sido además avalado por la más reconocida doctrina dominicana que ha definido la acción de *hábeas data* como el *"derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos."*[29]

En suma, el 13 de diciembre del año 2013, fue aprobada la Ley de Protección de Datos de la República Dominicana[30], (en lo sucesivo, Ley No. 172-13), con el objetivo de proteger de manera integral los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados, así como garantizar que no se lesione el derecho al honor y a la intimidad de las personas, y también facilitar el acceso a la información que sobre las mismas se registre, con arreglo a lo establecido en el artículo 44 de la Constitución de la República Dominicana.[31]

Es importante resaltar, que en ocasión de la evaluación del acuerdo suscrito en 2006 entre Canadá y la Unión Europea sobre la transferencia de datos API /PNR, el Parlamento Europeo estimó que Canadá protegía la privacidad de los titulares de los datos de mejor manera que Estados Unidos, una de las razones para que así fuese, fue la existencia de una legislación de protección de datos de carácter personal canadiense, ya que la misma constituía una condición esencial para cualquier injerencia sobre el derecho a la intimidad[32], lo cual revela la importancia dada desde

[28]Ibídem, artículo 70: "*Hábeas data. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística*."

[29] JORGE PRATS, Eduardo, *Comentarios a la Ley Orgánica del Tribunal Constitucional y de los Procedimientos Constitucionales*, Santo Domingo: IUS NOVUM, Impresión: Amigo del Hogar, 2011, p. 139 citado en JEREZ CASTILLO, Francisbel Yanilsa, *El derecho a la protección de datos personales como límite al derecho a la información*, Santiago de los Caballeros: Pontificia Universidad Católica Madre y Maestra, 2013. (Memoria final para optar por el título de Licenciada en Derecho).

[30] República Dominicana. Ley No. 172-13 de 13 de diciembre de 2013, que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. *Gaceta Oficial* No. 10737 del 15 de diciembre de 2013.

[31] Ibídem, artículo 1.

[32]Informe Final A6-0226/2005, del Parlamento Europeo, sobre la propuesta de Decisión del Consejo relativa a la celebración de un Acuerdo entre la Comunidad Europea y el Gobierno de Canadá sobre el tratamiento de datos procedentes del sistema de información anticipada sobre pasajeros (API) y de los expedientes de los pasajeros (PNR) (COM(2005)0200 – C6-0184/2005 – 2005/0095(CNS)), de 4.07.2005,

las instituciones de la Unión a que el país de destino de los datos cuente con una legislación que regule el derecho a la protección de datos, como es el caso de la República Dominicana.

Volviendo al régimen jurídico de la protección de datos de la República Dominicana, de conformidad con los preceptos constitucionales, en la Ley No. 172-13 son desarrollados los principios de calidad, licitud, lealtad, seguridad y finalidad. La licitud entendida como la prohibición del tratamiento y recogida de datos con finalidades contrarias a las leyes o al orden público. La calidad de los datos, establecida en el sentido de que los datos personales a tratar deben ser ciertos, adecuados y pertinentes en relación al ámbito y finalidad para los que se hubieren obtenido. La seguridad de los datos como la obligación del responsable del archivo de datos personales y en su caso, el encargado del tratamiento, de adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para proteger los datos de carácter personal evitando su alteración, pérdida, tratamiento, consulta o acceso no autorizado. La lealtad concebida como la prohibición de recoger los datos por medios fraudulentos, desleales o ilícitos y en cuanto a la finalidad, la ley ordena que solo se permitirá la recogida de datos cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para los que se hayan obtenido.[33]

La Ley 172-13, también contempla el principio de derecho de información, indicando que cuando se recaben datos personales que requieran del consentimiento de su titular, para ser tratados o ser cedidos después de obtener dicho consentimiento, se deberá informar previamente, a por lo menos uno de los titulares de los datos, en forma expresa y clara, explicando la finalidad, la existencia del registro y la posibilidad de ejercer los derechos de acceso, rectificación y supresión de sus datos.

---

disponible en la web: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML+REPORT+A62005-0226+0+DOC+PDF+V0//ES

[33] Ley No. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. Op. cit., artículo 5.

De igual manera consagra el principio de consentimiento del afectado, señalando que el tratamiento de datos será lícito cuando el titular de los datos hubiere prestado su consentimiento libre, expreso y consciente, que deberá constar por escrito o por otro medio que permita que se le equipare, de acuerdo a las circunstancias, añadido al principio de deber de secreto, que crea la obligación al responsable del archivo de datos y a todo el que intervenga en el tratamiento, de guardar secreto respecto de los mismos subsistiendo con posterioridad a la finalización de relaciones con el titular del archivo de datos o fichero.

En ese tenor, hay que expresar que estos principios guardan correspondencia con el marco de protección europeo. En apoyo a lo dicho, hay que recordar que la Directiva 95/46/CE estableció como principios el de lealtad, licitud, finalidad, calidad y consentimiento. Además del principio de conservación que va de la mano con el de finalidad, el mismo subraya la necesidad de que los datos solo puedan ser conservados de manera que los interesados solo puedan identificarse durante el tiempo necesario para los fines que fueron recogidos, con la excepción de los datos recabados con fines históricos, estadísticos o científicos.

A título ilustrativo, incluimos el siguiente recuadro comparativo donde puede verse con mayor claridad la afinidad de las legislaciones objeto de estudio, en casi todos los casos:

PRINCIPIO	NORMATIVA DOMINICANA	NORMATIVA EUROPEA
Principio de lealtad	Art. 5.7 Ley 172-13: ´´ *Se impone la prohibición de recoger los datos por medios fraudulentos, desleales o ilícitos*´´	Art. 6.1.a) Directiva 95/46/CE: ´´*Los Estados miembros dispondrán que los datos personales sean tratados de manera leal y lícita.* ´´ ***Nuevo Reglamento General de Protección de datos incluye además de la lealtad, el principio de transparencia.**

Principio de calidad	Art. 5.2 Ley 172-13: *´´El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando el principio de calidad […] Los datos deben ser ciertos, adecuados y pertinentes en relación al ámbito y finalidad para los que se hubieren obtenido, exactos y actualizarse en caso de ser necesario.´´*	Art. 6.1.c-d) Directiva 95/46/CE: *´´Los Estados miembros dispondrán que los datos personales sean* adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente exactos y, cuando sea necesario, actualizados. ´´ ***Nuevo Reglamento General hace alusión a la minimización de los datos, en relación al principio de calidad.**
Principio de finalidad	Art. 5.8 Ley 172-13: *´´Los datos solo se recogerán para su tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para los que se hayan obtenido.´´*	*Art. 6.1 b)* Directiva 95/46/CE: *´´Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas. ´´*

Principio de consentimiento	Art. 5.4 Ley 172-13: ´´*El tratamiento y la cesión de datos personales es ilícito cuando el titular de los datos no hubiere prestado su consentimiento libre, expreso y consciente, que deberá constar por escrito o por otro medio que permita que se le equipare, de acuerdo a las circunstancias.* ´´ ***Excepciones relativas a misiones de interés público, fuentes de acceso público, ejecución de un contrato, relaciones laborales, disposiciones legislativas, protección de la vida del interesado, cumplimiento de obligaciones jurídicas.***	Art. 7 Directiva 95/46/CE: *Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si el interesado ha dado su consentimiento de forma inequívoca.* ***Excepciones aplican en caso de que los datos sean necesarios para la ejecución de un contrato, cumplimiento de obligaciones jurídicas, protección del interés vital del titular, misiones de interés público, o satisfacción del interés legítimo perseguido por el responsable del tratamiento.***
Principio de seguridad	Art.5.5 Ley 172-13: ´´*El responsable del archivo de datos personales y en su caso, el encargado del tratamiento, deberán adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para salvaguardar los datos de carácter personal y eviten su alteración, pérdida,*	Art. 5. f) Nuevo Reglamento: *Los datos personales deben ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas*

	tratamiento, consulta o acceso no autorizado.´´	*(«integridad y confidencialidad»).* ***Aunque la Directiva 95/46/CE en su artículo 17 contenía una disposición idéntica a la transcrita *ut supra,* es a partir del nuevo reglamento que se reconoce la seguridad como un principio, a nivel normativo.**
Principio de conservación de los datos	No desarrollado.	*6.1 e) ´´Los datos personales deberán ser conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos´´*

Sin embargo, aunque el nuevo reglamento reconoce que los principios contenidos en la Directiva 95/46/CE siguen siendo válidos, hay que señalar que al momento de su aplicación entrarán en juego nuevos principios, a los cuales hay que prestar especial atención en vista de que el plazo para trasponer la Directiva que importa a este informe, es decir, la Directiva de utilización de datos PNR, es equivalente al de entrada en aplicación del nuevo reglamento. Estos principios son el de transparencia y el de privacidad desde el diseño y por defecto. El primero de ellos exige que sea facilitada al

interesado toda la información complementaria que tienda a garantizar un tratamiento leal y transparente; a modo de ejemplo indica que debe ser informada la posibilidad de elaboración de perfiles y las consecuencias de dicha elaboración.

En cuanto a la protección de datos desde el diseño y por defecto, textualmente, el instrumento normativo explica que:

> *´´El responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.´´*[34]

En cuanto a la diferenciación de los datos en categorías de tratamiento, aspecto de carácter fundamental, la legislación dominicana también distingue los datos que llama sensibles o especialmente protegidos, estableciendo que ninguna persona puede ser obligada a proporcionarlos. Según el artículo 6.8 de la Ley 172-13 se consideran datos sensibles los que *revelen el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.*

En esa línea, la legitimación del tratamiento de los datos sensibles se supedita al consentimiento expreso y por escrito del afectado en todos los casos.[35] Se advierte pues que en relación a esta categoría de datos la legislación dominicana es aún más protectora que la europea, por la inclusión de los datos que revelen convicciones morales, y por exigir que el consentimiento deba constar por escrito en todos los casos. [36]

[34] Reglamento General de Protección de Datos, Op. cit., arts. 25.2 y 25.3
[35] República Dominicana. Ley No. 172-13, op. cit. Art. 76
[36] Se recuerda que las legislaciones de los países miembros de la Unión Europea, exigen el consentimiento por escrito solo en los casos de que se vayan a tratar datos personales que revelen la ideología, afiliación sindical, religión y creencias.

El marco jurídico dominicano además prohíbe la formación de archivos, bancos de datos o registros que se creen con la única finalidad de tratar datos sensibles, sin perjuicio de los ficheros de las iglesias, las asociaciones religiosas, clínicas, hospitales, y las organizaciones políticas y sindicales que podrán llevar registros de sus miembros. Asimismo, reconoce la posibilidad del tratamiento cuando se realice con finalidades estadísticas o científicas y sus titulares no puedan ser identificados.

La referida distinción de los datos especialmente protegidos es capital de cara a este informe y al tratamiento que realiza la Dirección General de Migración, en razón de que la Directiva de utilización de datos PNR, prohíbe expresamente el tratamiento de esta categoría de datos.

De igual manera la norma de protección de datos dominicana, consigna que: ´´*Los datos de carácter personal relativos a la comisión de infracciones penales sólo serán incluidos en archivos de datos personales, y sólo serán tratados o comunicados a los registros públicos, a partir de que haya intervenido una apertura a juicio de conformidad con la ley.* ´´[37] Este precepto es conforme al artículo 7.5 de la Directiva 95/46/CE que ordena lo siguiente: ´´*El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas.*´´[38]

Por último, no es ocioso acotar, que desde la norma suprema de la República Dominicana se dota al titular de los datos personales de la facultad de ejercer los derechos de acceso, rectificación, cancelación, y oposición. Por su parte, la ley 172-13 incluye además el derecho de supresión, y el derecho de indemnización a favor del interesado, cuando sea violentado algún mandato de la misma.

Al igual que en el derecho comunitario europeo, en la esfera de protección de datos personales de la República Dominicana, se explican de forma detallada las condiciones

[37] República Dominicana. Ley No. 172-13, op. cit. Art. 77

[38] Esta disposición es idéntica a la que consta en el Nuevo Reglamento General de Protección de datos sobre esta categoría de datos. Véase el artículo 10 del mismo.

generales para el ejercicio de los derechos del interesado, con establecimiento de plazos y sanciones derivadas del incumplimiento de dichas condiciones.[39]

De igual manera, y como hemos expresado anteriormente, sin perjuicio de los mecanismos establecidos en la Ley 172-13 para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición, supresión e indemnización, todo titular de datos personales podrá ejercer la acción judicial de *hábeas data* de conformidad con la Constitución y la Ley 137-11 Orgánica del Tribunal Constitucional y de los procedimientos constitucionales.

Por otro lado, debemos mencionar que otra de las razones por las cuales se estimó que el acuerdo de transferencia de datos PNR firmado entre la Unión Europea y Canadá, era satisfactorio fue el hecho de que en Canadá existe un marco legal de carácter general en materia de protección de datos que establece criterios aplicables a todo tipo de tratamientos, en comparación con los Estados Unidos donde no existe tal marco legal, lo cual a juicio del Parlamento Europeo constituía una señal peligrosa. [40]

Así también, el Parlamento Europeo se había mostrado inconforme con el acuerdo firmado con los Estados Unidos porque no se había verificado si el acceso a los datos de los sistemas de reserva (datos PNR) tenía una base real en la legislación de los Estados Unidos o se trataba de una interpretación extensiva por parte del Gobierno de este país.[41]

Al igual que como sucede en el caso canadiense, estas señales peligrosas no tendrían lugar al momento de evaluar un acuerdo de transferencia internacional de datos con la República Dominicana, ya que como hemos visto, en el país existe un marco legal de carácter general en materia de protección de datos que establece criterios aplicables a

[39] Véanse los artículos 10 y siguientes de la Ley 172-13 op. cit.

[40] NINO, Michelle, *The protection of personal data in the fight against terrorism. New perspectives of PNR European Unión instruments in the light of theTreaty of Lisbon*, citado en PÉREZ FRANCESCH Joan Lluís, GIL MÁRQUEZ Tomás, GACITÚA ESPÓSITO Alejandro, *Informe sobre el PNR. La utilización de datos personales contenidos en el registro de nombres de pasajeros: ¿fines represivos o preventivos?,* Barcelona: Universitat Autònoma de Barcelona: Working Paper núm. 297, 2011.

[41] Parlamento Europeo. Resolución sobre La transmisión de datos personales por las compañías aéreas en los vuelos transfronterizos. P5_TA (2003) 0097; B5 0187 2003 citado por TEJERINA RODRÍGUEZ, Ofelia, *Seguridad del Estado y privacidad,* Madrid: Editorial Reus, S.A., 2014, ISBN: 9788429017694 p.337 (El paréntesis es nuestro).

todo tipo de tratamientos, y además las solicitudes de datos PNR se encuentran amparadas en una base real en la legislación dominicana (Ley No. 285-04 de 15 de agosto del año 2004, General de Migración de la República Dominicana y Resolución No. DGM-04-12).

En virtud de todo lo anteriormente expresado, podemos convenir entonces que aunque el nivel de protección de datos otorgado por las leyes de la República Dominicana puede mejorarse, específicamente en cuanto a las medidas de seguridad, al desarrollo reglamentario, a la inclusión de principios como el de conservación, el mismo no es desajustado en esencia, y más importante aún, no se verifican contradicciones con el derecho de la Unión Europea.

3. EXAMEN DEL CONTENIDO DE LA DIRECTIVA (UE) 2016/681

Previo a adentrarnos en el estudio de las especificidades de la Directiva (UE) 2016/681 de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, es oportuno esbozar los conceptos clave contenidos en la misma, para propiciar un entendimiento cabal de este informe.

Indudablemente que debemos de iniciar explicando cómo se definen los datos PNR a la luz de la Directiva (UE) 2016/681. Los datos del registro de nombres de pasajeros (PNR, por las siglas en inglés de *Passenger Name Record),* son información no verificada que proporcionan los pasajeros y recogen las compañías aéreas para efectuar las reservas y llevar a cabo el proceso de facturación. Se trata de un registro de los requisitos de viaje de cada pasajero que figura en los sistemas de reservas y control de salidas de las compañías. Contiene las fechas y el itinerario de viaje, los datos del billete, datos de contacto como números de teléfono y dirección, la agencia de viajes, información sobre el pago, número de asiento y datos del equipaje.[42]

[42] Comisión Europea. Comunicación de la Comisión sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países. Bruselas, 2010. Publicación disponible en la web: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0492&from=ES [Fecha de consulta: 19-5-2016]

Expresamente, la Directiva 2016/681 los define como: *´´una relación de los requisitos de viaje impuestos a cada pasajero, que incluye toda la información necesaria para el tratamiento y el control de las reservas por parte de las compañías aéreas que las realizan y participan en el sistema PNR, por cada viaje reservado por una persona o en su nombre, ya estén contenidos en sistemas de reservas, en sistemas de control de salidas utilizado para embarcar a los pasajeros en el vuelo o en sistemas equivalentes que posean las mismas funcionalidades.´´*[43]

Del mismo modo, conviene detenerse en otro tipo de datos que se inscribe dentro de los datos PNR. Se trata de los datos de información anticipada o avanzada de pasajeros (*Advanced Passenger Information- API*), los datos API son los datos biográficos que figuran en la parte de lectura óptica del pasaporte y se refieren al nombre, el lugar de residencia, el lugar del nacimiento y la nacionalidad de la persona.

La Directiva 2016/681 no contiene una definición de esta última categoría de datos, no obstante, la Organización de Aviación Civil Internacional[44] ha explicado que:

> *´´La información anticipada sobre los pasajeros (API) comprende la captura de los datos biográficos y los detalles del vuelo de un pasajero o miembro de la tripulación por parte del explotador de aeronaves antes de la salida. Esta información se transmite en forma electrónica a las agencias encargadas del control fronterizo del país de destino con posterioridad al vuelo. Por lo tanto, las agencias de control fronterizo pueden verificar los datos de los pasajeros, comparándolos con su(s) base(s) de datos e identificar a aquellos que requieren un examen más exhaustivo a su llegada.´´*[45]

[43]DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, *Diario Oficial de la Unión Europea*, n˚ L 119/132*,* de 4 de mayo de 2016.

[44] La Organización de Aviación Civil Internacional (ICAO, por sus siglas en inglés), es una agencia especializada de las Naciones Unidas, establecida en 1944 para velar por el cumplimiento de la Convención de la Aviación Civil Internacional (Convención de Chicago) y promover el entendimiento y la seguridad a través de la cooperación regulatoria. Más información en: http://www.icao.int/

[45] Organización de Aviación Civil Internacional, CONFERENCIA DE ALTO NIVEL SOBRE SEGURIDAD DE LA AVIACIÓN (HLSCA),*INFORMACIÓN ANTICIPADA SOBRE LOS PASAJEROS (API) Y SU FUNCIÓN EN LA SEGURIDAD DE LA AVIACIÓN,* Montreal, septiembre de 2012.

Además, pese a no definirlos, en los considerandos que exponen los motivos por los que se aprueba la Directiva 2016/681, se dice que algunas aerolíneas recogen los datos API como parte de los datos PNR, mientras que otras no lo hacen, instando a aquellas que no los recogen a que los recaben, ya que se plantea que ´´*utilizar los datos PNR junto con los datos API representa un valor añadido para ayudar a los Estados miembros a verificar la identidad de una persona, reforzando así el valor policial de ese resultado y reduciendo al mínimo el riesgo de realizar controles e investigaciones de personas inocentes.*´´ Siendo importante entonces, asegurarse de que cuando las aerolíneas recojan datos API, los transfieran como parte de los datos PNR.[46]

En idéntico sentido, debe aclararse, que con anterioridad de la directiva objeto de examen en este apartado, fue aprobada la Directiva 2004/82/CE, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas, y de conformidad con la misma, en principio podría pensarse que los datos API no están incluidos dentro de la Directiva de utilización de datos PNR, ya que su utilización para fines represivos había sido concebida como una excepción más que una regla[47], sin embargo, desde la óptica de la Directiva 2016/681 se considera su inclusión para ser empleados a fin de prevenir los actos terroristas y de delincuencia grave, como ya hemos señalado.

En adición a ello, el Grupo de Trabajo del Artículo 29 en su Opinión 7/2010 relativa la Comunicación sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países, recalcó que el intercambio de datos PNR no debe ser considerado de forma aislada, por lo tanto el enfoque global debería extenderse a las solicitudes de terceros países para todos los datos de los pasajeros, incluyendo los datos API.[48]

---

[46]DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Op. cit., p.2

[47] Comisión Europea. Comunicación sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países. Op. cit., p. 4.

[48]ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 7/2010 onEuropeanCommission'sCommunicationonthe global approach to transfers of PassengerName Record (PNR) data to thirdcountries, Bruselas: adoptado el 12 de noviembre de 2010. Disponible en la web: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp178_en.pdf [Fecha de consulta: 19-5-2016] (La traducción es nuestra).

Avanzando en el estudio del contenido de la Directiva 2016/681, hemos de referirnos a sus objetivos, los cuales son, entre otras cosas (al decir de la propia directiva), garantizar la seguridad, proteger la vida y la seguridad de los ciudadanos y crear un marco jurídico para la protección de los datos PNR en lo que respecta a su tratamiento por las autoridades competentes, en el entendido de que es imprescindible que los Estados miembros introduzcan disposiciones que impongan la obligación de transferir todos los datos PNR que recojan las compañías aéreas que realizan vuelos exteriores del territorio de la Unión, incluidos los datos API.

Refiriéndose concretamente al tratamiento de los datos PNR, la Directiva 2016/681 estipula que cada Estado Miembro deberá establecer o designar una autoridad competente para la prevención, detección, investigación o enjuiciamiento de los delitos de terrorismo y delitos graves, o una sucursal de esa autoridad para actuar como su unidad única de información (UIP), que se encargará de la recogida, almacenamiento, procesamiento y transferencia de los datos PNR a las autoridades competentes, sean estas pertenecientes a un Estado miembro o a terceros países.[49]

En tanto al ámbito de aplicación, la Directiva 2016/681 indica que los datos PNR podrán tratarse únicamente con fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves, y que para ello deberán ser aplicadas las garantías instituidas en la Carta de los Derechos Fundamentales de la Unión Europea, el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal («Convenio n˚ 108») y el Convenio para la protección de los derechos humanos y de las libertades fundamentales.

En esa misma línea de pensamiento, conforme al nivel de protección que brinda la Carta de los Derechos Fundamentales de la Unión Europea y el Convenio para la protección de los derechos humanos y de las libertades fundamentales, se reconoce expresamente, que en todo caso, deberá permitírsele a los interesados, el ejercicio de los derechos relativos al tratamiento de sus datos, es decir los derechos de acceso, rectificación, supresión y restricción de los datos PNR y el derecho a una

[49]DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Op. cit., p.7

indemnización y a una reparación judicial. Igualmente se consigna que la Directiva 2016/681 deberá aplicarse cuando exista una justificación suficiente y se provean las garantías necesarias para asegurar la legalidad de cualquier tipo de almacenamiento, análisis, uso o transferencia de datos PNR.[50]

Desde la exposición de motivos se delimitan los criterios sobre los cuales pueden elaborarse las listas de datos PNR, especificando que dichas listas no deben basarse en el origen racial o étnico, religión o convicciones, opiniones políticas o de cualquier otro tipo, la pertenencia a un sindicato, la salud, vida u orientación sexual. Los datos PNR solo deberán contener la información sobre las reservas e itinerarios de viaje que permita a las autoridades competentes identificar a los pasajeros por vía aérea que representan una amenaza para la seguridad interior de los países involucrados.[51] A tales efectos, la Directiva se ocupa de establecer un *numerus clausus* de los datos del registro de nombres de los pasajeros que pueden ser recopilados por las aerolíneas y de los delitos que se consideran delitos graves, cuya prevención puede llevarse a cabo tratando los datos PNR. Esa lista taxativa de los datos del registro de nombres de los pasajeros la hemos incluido como **anexo número I.**

En cuanto a la transmisión y el almacenamiento de los datos PNR, se determina que la Comisión Europea respalda las directrices emanadas de la Organización de Aviación Civil Internacional (ICAO), señalando que las mismas se constituyen en la base de los formatos admitidos para la transmisión de los datos PNR. En el artículo 16 es consagrado lo que se transcribe a continuación: *´´Todas las transmisiones de datos PNR por las compañías aéreas a las UIP a efectos de la presente Directiva se efectuarán por medios electrónicos que ofrezcan garantías suficientes en relación con las medidas de seguridad técnicas y las medidas organizativas que rigen el tratamiento de datos que se va a llevar a cabo.[…]Los datos PNR serán transmitidos en un formato de datos admitido que garantice su legibilidad por todas las partes interesadas´´*[52]

Por lo que respecta a la conservación, la Directiva 2016/681 es categórica al implantar un período de conservación de cinco años, contados a partir del momento en el cual

[50] Ibídem, p. 3
[51] DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Op. cit., p.2
[52] DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Op. cit., p.14

los datos PNR son transmitidos a la UIP del Estado miembro en cuyo territorio tenga salida o aterrice el vuelo.

En suma, impone la obligación de despersonalizar todos los datos PNR mediante el enmascaramiento de todos los elementos que permitan identificar directamente a los pasajeros titulares de los datos, cuando hayan transcurrido 6 meses desde la transmisión de los datos PNR a la UIP del Estado miembro en cuyo territorio tenga su punto de salida o aterrizaje el vuelo en cuestión. En este sentido, el artículo 12 contiene una lista de los elementos que podrían servir para identificar directamente al pasajero. Dicha lista se encuentra incluida en el **anexo número II** del presente informe y volveremos sobre la misma en el apartado destinado a las medidas que deberá observar la Dirección General de Migración de la República Dominicana.

Aunado a todo lo anteriormente expresado, el artículo 13 de la Directiva que está siendo examinada, se dedica por entero a la protección de datos de carácter personal, tal y como se verifica en el título que lo acompaña. El referido artículo ordena que: *´´todo pasajero tendrá los mismos derechos de protección de sus datos personales, derechos de acceso, rectificación, supresión y restricción y derechos de indemnización y recurso judicial que los establecidos en el derecho de la Unión y nacional y en aplicación de los artículos 17, 18, 19 y 20 de la Decisión marco 2008/977/JAI.´´*[53]

Por último, es de rigor acotar que el referido artículo 13 prohíbe expresamente el tratamiento de datos PNR que revele el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud, la vida sexual o la orientación sexual de una persona, haciendo la salvedad de que en el caso de que una UIP reciba datos PNR de esa tipología, tendrá que suprimirlos inmediatamente.

Habiendo estudiado las disposiciones generales de la Directiva 2016/681, trataremos a continuación, las condiciones relativas a la transferencia internacional de datos PNR, aspecto primordial en relación con los fines del presente informe.

[53] Ibídem, p. 12

El artículo 11 de la Directiva 2016/681 expresa que las transferencias de datos PNR y del resultado del tratamiento de dichos datos a terceros países podrá tener lugar solo cuando se cumplan las siguientes condiciones:

> *´´a) se cumplen las condiciones establecidas en el artículo 13 de la Decisión marco 2008/977/JAI; b) la transmisión es necesaria para los fines de la presente Directiva a que se refiere el artículo 1, apartado 2; c) el tercer país acuerda transmitir los datos a otro tercer país únicamente si fuera estrictamente necesario para los fines de la presente Directiva a que se refiere el artículo 1, apartado 2, y solo con la autorización expresa del Estado miembro, y d) se reúnen unas condiciones idénticas a las establecidas en el artículo 9, apartado 2.´´* [54]

A fines explicativos, es necesario reproducir el contenido del artículo 14 de la Decisión marco 2008/977/JAI, que a su vez especifica que la transferencia de datos personales a autoridades competentes de terceros países y organismos internacionales solo será posible si son cumplidas las siguientes condiciones:

> *´´a) que sea necesario para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o para la ejecución de sanciones penales; b) que la autoridad receptora del tercer Estado o el organismo internacional receptor sea competente para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales; c) que el Estado miembro que proporcionó los datos haya consentido la transferencia de acuerdo con su Derecho nacional; d) que el tercer Estado u organismo internacional de que se trate garantice un nivel adecuado de protección en el tratamiento de datos previsto.*
>
> *2. La transferencia de datos sin el consentimiento previo de acuerdo con el apartado 1, letra c), solo podrá permitirse si es esencial para la prevención de una amenaza inmediata y grave a la seguridad pública de un Estado miembro o de un tercer Estado o a intereses esenciales de un Estado miembro, y si el consentimiento previo no puede obtenerse a tiempo. Se informará sin demora a la autoridad encargada de otorgar el consentimiento.*
>
> *3. No obstante lo dispuesto en el apartado 1, letra d), podrán transferirse datos personales en cualquiera de los siguientes supuestos: a) que así lo disponga el Derecho nacional del Estado miembro que transfiere los datos por alguno de los siguientes motivos: i) legítimos intereses específicos del interesado, o ii) legítimos intereses superiores, en especial importantes intereses públicos, o b)*

[54] DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Op. cit., p.11

que el tercer Estado o el organismo internacional receptor ofrezca garantías que el Estado miembro de que se trate considere adecuadas de conformidad con su Derecho nacional.

4. La adecuación del nivel de protección a que se refiere el apartado 1, letra d), se evaluará atendiendo a todas las circunstancias que concurran en una operación de transferencia de datos o en un conjunto de operaciones de transferencia de datos. Se tomará en consideración en particular la naturaleza de los datos, la finalidad y la duración de la operación u operaciones de tratamiento previstas, el Estado de origen y el Estado u organismo internacional de destino final de los datos, la normativa, tanto general como sectorial, vigente en el tercer Estado u organismo internacional de que se trate, y las normas profesionales y medidas de seguridad que sean de aplicación.´´[55]

Además, es de reseñar, que sin perjuicio de las disposiciones transcritas en los párrafos que anteceden, de manera excepcional, la Directiva autoriza las transferencias internacionales de datos PNR sin el consentimiento previo del Estado miembro de donde proceden los datos, si se dan las siguientes circunstancias: *´´a) son esenciales para responder a una amenaza específica y real relacionada con delitos de terrorismo o delitos graves de un Estado miembro o de un tercer país, y b) el consentimiento previo no puede obtenerse a su debido tiempo.´´*[56]

Luego de examinar el contenido de la Directiva 2016/681 en todo lo que interesa al organismo que solicita este informe, es tiempo de ocuparnos de las medidas que deben adoptarse para alcanzar sus objetivos de proporcionar las garantías adecuadas en materia de protección de datos.

4. MEDIDAS QUE DEBEN SER ADOPTADAS PARA PROPORCIONAR LAS GARANTÍAS ADECUADAS REQUERIDAS POR LA DIRECTIVA 2016/681

Como hemos visto, en materia de transferencia internacional de datos PNR, la Comisión Europea ha declarado que un tercer país cumple con un adecuado nivel de protección a través de la firma de acuerdos bilaterales de transferencias de tales datos. Se ha dicho que el nivel adecuado de protección de datos puede consagrarse en la legislación del tercer país o proporcionarse en forma de compromisos jurídicamente

[55]DECISIÓN MARCO 2008/977/JAI DEL CONSEJO de 27 de noviembre de 2008 relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, *Diario Oficial de las Comunidades Europeas* n˚ L 350/6, 2008.
[56]DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Op. cit., p.11

vinculantes, es decir un acuerdo internacional que regule el tratamiento de datos PNR.[57]

Tal y como se desprende del intitulado, esta sección será dedicada a la descripción de las medidas que debe adoptar la Dirección General de Migración, con miras a que este organismo esté en condiciones de negociar la firma de un acuerdo que avale la transferencia de datos PNR con los países miembros de la Unión Europea.

Antes de centrarnos en la enunciación de las medidas específicas que deberá adoptar la Dirección General de Migración, se estima pertinente la descripción del panorama actual de recogida, tratamiento, almacenamiento y seguridad de los datos PNR existente en el organismo de control migratorio y fronterizo.

El mencionado panorama, viene dado por las disposiciones de la Ley No. 285-04 de 15 de agosto del año 2004, General de Migración de la República Dominicana y la Resolución No. DGM-04-12 que crea los protocolos para el servicio obligatorio de la información avanzada de pasajeros y tripulantes en todas las operaciones de transporte internacional con destino o desde territorio nacional.

Como hemos expresado previamente, la Ley 285-04 obliga a las compañías aéreas a presentar la lista de pasajeros que transportados ante la autoridad migratoria de control, antes del arribo de sus aeronaves al país, es decir, es solicitada la denominada información anticipada de cada pasajero (API). Las condiciones en las cuales deben ser transmitidos dichos datos son descritas en la Resolución No. DGM-04-12, que en su capítulo I, apartado segundo estipula lo siguiente:

> *´´INFORMACIÓN PASAJERO Y/O TRIPULACIÓN: Todas las aeronaves, naves o vehículos de motor dedicadas al transporte internacional de pasajeros a título público, privado u oficial, de pasajeros o carga, que se dirijan desde el exterior a territorio nacional o, desde territorio nacional hacia el exterior, deberán suministrar, avanzar de manera electrónica a la Dirección General de Migración (DGM) todas las informaciones que se detallan a continuación:*

[57]COMISIÓN EUROPEA. *Comunicación de la Comisión sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países.* Op. Cit.

1.- De cada pasajero, tripulante o conductor: a) Nombre (s) completo (s) (Según figure en el pasaporte), b) Apellido (s) completo (s) (Según figure en el pasaporte), c) Nacionalidad, d) Fecha de nacimiento, e) Lugar de nacimiento, f) Genero/sexo,

2.- Del documento de viaje para acreditar la identidad del pasajero, tripulante o conductor: Pasaporte: Regular, oficial, diplomático, otros., número del pasaporte, fecha de emisión, fecha de expiración, lugar de emisión, país emisor.´´ [58]

En adición a ello la Ley 285-04, en su artículo 117 obliga a las empresas de transporte aéreo internacional, a proveer a todos los pasajeros que arriben o salgan del territorio de la República Dominicana del documento de Embarque/Desembarque e instruirlos en su llenado y entrega. Este documento conocido como tarjeta de Embarque/Desembarque se trata de un formulario donde se recogen datos relativos al itinerario del viaje, y a la identidad de la persona.

Si bien las disposiciones de esta Ley constituyen la base legal de la obligación de transferencia de datos PNR que pesa sobre las empresas de transporte internacional, sus dependencias y sus representantes, nada establecen en materia de protección de datos personales, empero lo cierto es que el derecho a la protección de datos fue reconocido con posterioridad a la aprobación de las leyes migratorias, y por tal razón la Ley de Protección de Datos de la República Dominicana también es ulterior a las mismas, pero ello no quiere decir que no le sean aplicables; las disposiciones de la Ley de Protección de Datos por su especialidad resultan de aplicación ante la generalidad de la Ley migratoria.

Hemos podido comprobar a partir de los estudios de campo realizados, y las reuniones sostenidas con la Consultora Jurídica de este organismo, que a pesar de que en el marco legal migratorio no existen disposiciones expresas dirigidas a la protección de datos de carácter personal, la Dirección General de Migración y específicamente su

[58]REPÚBLICA DOMINICANA. MINISTERIO DE INTERIOR Y POLICÍA. DIRECCIÓN GENERAL DE MIGRACIÓN. *Resolución No. DGM-04-12 que crea los protocolos para el servicio obligatorio de la información avanzada de pasajeros y tripulantes en todas las operaciones de transporte internacional con destino o desde territorio nacional,* Santo Domingo, 2012.

departamento de tecnología, desempeñan sus funciones en base a protocolos respetuosos de la Constitución y las leyes, para el manejo de los datos PNR.[59]

Se trata pues de mejorar los protocolos de actuación existentes, y en tal sentido, nuestra recomendación es que no solo se mejoren de cara al tratamiento de los datos de ciudadanos europeos y en interés de la firma de un acuerdo de transferencias de datos internacionales con la Unión Europea, sino que se establezca para todos los tratamientos de datos PNR sin importar la procedencia del pasajero, las medidas que detallaremos son muy completas en cuanto a la protección efectiva del derecho a la protección de datos se refiere, y compatibles con el marco jurídico general de protección de datos de la República Dominicana, por lo cual no solo podrían ser de aplicación para satisfacer la adecuación a la Directiva 2016/681, sino también al propio marco jurídico de protección de datos de la República Dominicana.

Consideramos además que, en atención al ingente flujo de datos que es tratado por la Dirección General de Migración, es de mayor conveniencia que las modificaciones a introducir en los protocolos de actuación sean recogidas en una resolución cuya publicación sea del conocimiento de todo el personal que tenga acceso a los datos en alguna fase de su tratamiento, lo que indudablemente contribuiría a la cualificación de dicho personal.

En toda lógica, el tratamiento de datos se hará en franco respeto de la legislación dominicana, se trata de establecer medidas ajustadas a la Directiva 2016/681 pero en todo caso, sin ir en contra del derecho interno. El eventual acuerdo internacional se regirá por las leyes dominicanas, que tomando las medidas de lugar llegará a brindar un nivel de protección equivalente a los estándares derivados de la normativa europea.

Para mayor claridad, dividiremos la sección en 2 bloques, el primero destinado al señalamiento de las medidas de carácter general y el segundo, a las medidas específicas en diversas fases del tratamiento, sección que a su vez se subdivide en

[59]LCDA. LAURA LETICIA MARIÑEZ ESPINAL, Consultora Jurídica de la Dirección General de Migración de la República Dominicana.

medidas relativas a la recogida y transmisión, al tratamiento y almacenamiento y a la seguridad de la información.

4.1. Medidas de carácter general

En el protocolo de actuación de la Dirección General de Migración (en lo adelante DGM o la Dirección) deberán consignarse las siguientes medidas generales, de suerte que sirvan de principios:

- Se consignará que deberán preverse las garantías necesarias para asegurar la conformidad de cualquier almacenamiento, análisis, uso o transferencia de datos PNR, con la legislación de protección de datos de la República Dominicana.

- Se reconocerá que todo tratamiento de datos deberá respetar los principios constitucionales de proporcionalidad, razonabilidad y necesidad. Lo que al decir de la Directiva 2016/681 significa que el tratamiento de datos personales PNR debe ser proporcional a los objetivos de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y delincuencia grave.

- Habrá de ser tenido en cuenta que los datos PNR únicamente podrán tratarse con la finalidad de prevenir, detectar, investigar y enjuiciar los actos terroristas y los delitos graves. (En el **anexo número III** se aporta la lista de los delitos que la Unión Europea considera como delitos graves con arreglo a la Directiva 2016/681)

- Se reconocerá que la Dirección será la que correrá con los gastos de uso, conservación e intercambio de datos PNR.

- Se prohibirá expresamente el tratamiento de datos PNR que revele el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la salud, la afiliación sindical, la vida sexual o la orientación sexual de una persona.

- Se reconocerá el derecho de los interesados de ser informados de manera precisa, de fácil acceso y comprensión sobre la recogida de sus datos PNR, de las

condiciones del tratamiento y del ejercicio de sus derechos, todo ello de conformidad con el principio de deber de información contemplado en la normativa de protección de datos dominicana.[60]

- Se establecerá que las listas elaboradas a partir de datos PNR no deberán basarse en el origen racial o étnico, religión y convicciones, opiniones políticas o de cualquier otro tipo, la afiliación sindical, la orientación sexual o la salud.

- Se establecerá un período de conservación de datos PNR de 5 años. En vista de que el marco jurídico de protección de datos dominicano carece de la consagración del principio de conservación de los datos, para efectos del futuro acuerdo se establecerá que: ***´´Los datos personales deberán ser conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.´´***[61]

- Se establecerá que el intercambio de datos PNR entre las autoridades competentes en materia judicial y policial no podrá ir en detrimento del nivel de protección de datos personales que exige la normativa dominicana.

- Se implantará la obligación de que se revise individualmente, por medios no automatizados, todo resultado positivo que se derive del tratamiento automatizado de datos PNR, al momento de que se lleve a cabo una evaluación de pasajeros con la finalidad de identificar a aquellas personas que requieran un

[60] República Dominicana. Ley No. 172-13, op. cit. Art. 5.3: *´´**Derecho de información.** Cuando se recaben datos personales que requieran del consentimiento del titular de los datos, para que se les pueda dar el tratamiento de datos o ser cedidos después de obtener dicho consentimiento, se deberá informar previamente, a por lo menos uno de los titulares de los datos, en forma expresa y clara, explicando: a) La finalidad para la que serán destinados y quiénes pueden ser sus destinatarios o clase de destinatarios. b) La existencia del archivo, registro, banco de datos o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable. c) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.´´*

[61] REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO 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), de 14 de abril de 2016.

examen más a fondo por las autoridades competentes, que en todo caso deberán ser competentes para la prevención, detección, investigación o enjuiciamiento de actos terroristas y delitos graves.

- Se establecerá que los resultados que arroje el tratamiento de datos PNR podrán ser objeto de tratamiento posterior por las autoridades competentes, con la finalidad exclusiva de prevenir, detectar, investigar y enjuiciar los actos de terrorismo y delitos graves.

- Se establecerá que no será adoptada decisión alguna que produzca efectos jurídicos desfavorables para una persona, o que la afecte significativamente, tomando en consideración únicamente el tratamiento automatizado de datos PNR. Asimismo, se establecerá que tales decisiones no deberán basarse en la raza o el origen étnico, la salud, la vida sexual u orientación sexual, las opiniones políticas, la afiliación sindical, y las creencias religiosas o filosóficas.

- Se garantizará en todo caso el ejercicio de los derechos de acceso, rectificación, supresión y restricción de los datos, de conformidad con la normativa, sea a través de los mecanismos establecidos en la propia Ley 172-13 o mediante la acción de *Habeas Data* contemplada en la constitución dominicana, sin perjuicio del derecho a indemnizaciones o reparaciones judiciales que procedan.

- Se velará porque los equipos y medios utilizados por la Dirección para el tratamiento de datos PNR, cumpla con los principios de privacidad desde el diseño y por defecto.

4.2. Medidas específicas

En atención a la tipología individualizada de datos que constituyen los datos PNR, y a las distintas fases del tratamiento de los datos, la Directiva 2016/681 ha trazado directrices específicas que evidentemente deben ser abordadas en este informe, en razón de que su adopción es clave para alcanzar el equiparable nivel de protección que exige para la transferencia internacional de datos PNR.

Huelga decir que estas medidas son perfectamente compatibles con el marco jurídico de protección de datos que provee la legislación dominicana, y muchas de ellas ya vienen siendo aplicadas por el departamento tecnológico de la Dirección General de Migración.

Para una mayor comprensión esta sección a su vez se subdivide en medidas relativas a la recogida y transmisión, al tratamiento y almacenamiento, y a la seguridad de la información.

4.2.1.1. Medidas relativas a la recogida y transmisión de los datos

Como ha sido explicado, la Dirección General de Migración de la República Dominicana tiene acceso a través de dos vías a los datos del registro de nombre de pasajeros. La primera de ellas es la obligada transmisión que hacen las aerolíneas de la lista de pasajeros y la API recopilada, luego del despegue del vuelo, y la segunda vía es a través del formulario de embarque que debe llenar cada pasajero y que la tripulación debe entregar a la Dirección.

En cuanto a la transmisión, hay que mencionar que en la práctica de la aviación internacional, tradicionalmente se ha dispuesto de dos modalidades para la transmisión de los datos PNR, el método *push o* de transmisión, y el método *pull* o de extracción. El método *push o* método de transmisión consiste en el envío por parte de las compañías aéreas a la autoridad solicitante sin permitir a dicha autoridad el acceso a las bases de datos (sistemas de reserva) de las aerolíneas, mientras que en el sistema *pull* o de extracción las autoridades competentes del país que solicita los datos, pueden acceder al sistema de reservas de la aerolínea y extraer una copia de los datos.[62]

Es generalmente admitido dentro de los organismos que regulan la aviación internacional, y las instituciones de la Unión Europea, que el método *push* o de transmisión ofrece un nivel superior de protección de la información en comparación con el método *pull*[63]*.* Así lo ha reconocido la Directiva que en su considerando 16

[62]DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Op. cit., p.2

[63] Véanse: ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL, *Los datos del registro de nombres de los pasajeros (pnr) y su función en la seguridad de la aviación,* Montreal, 2012, Comisión Europea.

estima que este método de transmisión debe ser obligatorio para todas las compañías aéreas, de tal suerte que la primera medida en materia de transmisión es el **mantenimiento del sistema de recogida *push***, ya que hasta el momento la Dirección General de Migración solo accede a los datos vía solicitud y transmisión desde las aerolíneas. En síntesis:

1. La Dirección General de Migración accederá a los datos PNR a través de la solicitud de los mismos, no mediante el acceso a las bases de datos de las compañías aéreas.

2. La Dirección General de Migración adoptará las medidas pertinentes con miras a garantizar que todas las compañías aéreas envíen los datos PNR mediante el método de transmisión *push.*

3. Los formatos de transmisión admitidos para la transmisión electrónica de los datos PNR, serán los que la Organización Civil de Aviación Internacional reconozca al efecto, tal y como establece el Capítulo III, apartado tercero de la Resolución No. DGM-04-12 que establece lo que se transcribe a continuación:

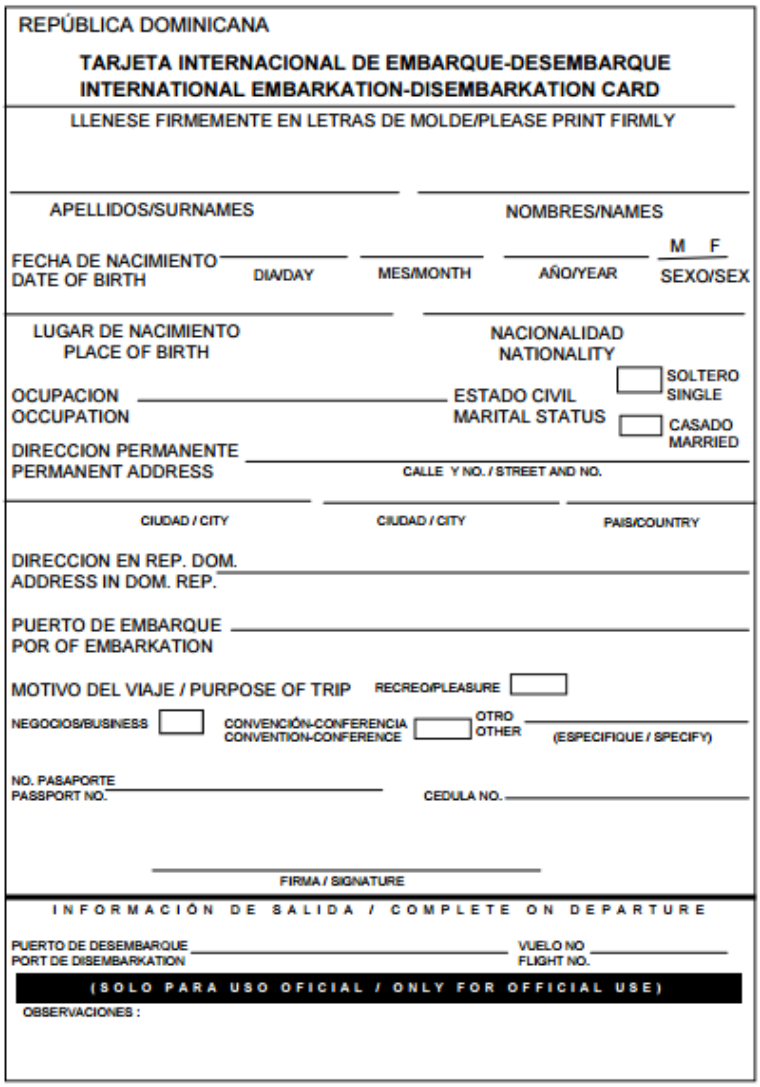
   ´´DE LA NOTIFICACIÓN DE VUELOS COMERCIALES: Toda entidad o persona física propietaria, arrendataria y/o operadora de la aeronave correspondiente, con capacidad de más de doce (12) asientos, sea de manera regular o no, incluidas aquellas que operan como arrendatarias de aeronaves (chárter), que tienen por objeto la explotación comercial del transporte internacional de pasajeros o carga, procederá a servir la información avanzada de pasajeros y/o tripulantes por los medios electrónicos y a través, de los sistemas internacionalmente

---

Comunicación de la Comisión sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países, Op. Cit. ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 7/2010, Op. Cit., Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, *Diario Oficial de la Unión Europea*, n° C 35/16, *9 de febrero de* 2012.

reconocidos que le fueren debidamente indicados por la Dirección General de Migración (DGM). ´´[64]

En cuanto a la recogida de datos mediante el llenado de la tarjeta de embarque/desembarque, entendemos pertinente insertar aquí dicho formulario a fin de explicar las modificaciones que deben hacerse:



REPÚBLICA DOMINICANA

TARJETA INTERNACIONAL DE EMBARQUE-DESEMBARQUE
INTERNATIONAL EMBARKATION-DISEMBARKATION CARD

LLENESE FIRMEMENTE EN LETRAS DE MOLDE/PLEASE PRINT FIRMLY

APELLIDOS/SURNAMES

NOMBRES/NAMES

FECHA DE NACIMIENTO / DATE OF BIRTH — DIA/DAY — MES/MONTH — AÑO/YEAR

M F SEXO/SEX

LUGAR DE NACIMIENTO / PLACE OF BIRTH

NACIONALIDAD / NATIONALITY

OCUPACION / OCCUPATION

ESTADO CIVIL / MARITAL STATUS

SOLTERO / SINGLE

CASADO / MARRIED

DIRECCION PERMANENTE / PERMANENT ADDRESS

CALLE Y NO. / STREET AND NO.

CIUDAD / CITY — CIUDAD / CITY — PAIS/COUNTRY

DIRECCION EN REP. DOM. / ADDRESS IN DOM. REP.

PUERTO DE EMBARQUE / POR OF EMBARKATION

MOTIVO DEL VIAJE / PURPOSE OF TRIP

RECREO/PLEASURE

NEGOCIOS/BUSINESS

CONVENCIÓN-CONFERENCIA / CONVENTION-CONFERENCE

OTRO / OTHER

(ESPECIFIQUE / SPECIFY)

NO. PASAPORTE / PASSPORT NO.

CEDULA NO.

FIRMA / SIGNATURE

INFORMACIÓN DE SALIDA / COMPLETE ON DEPARTURE

PUERTO DE DESEMBARQUE / PORT DE DISEMBARKATION

VUELO NO. / FLIGHT NO.

(SOLO PARA USO OFICIAL / ONLY FOR OFFICIAL USE)

OBSERVACIONES :

Fuente: Dirección General de Migración de la República Dominicana.

Como puede apreciarse, el formulario no cumple con el deber de información y transparencia sobre las finalidades y el destino que tendrán los datos de los interesados, y los derechos que les asisten. Por tanto:

[64]REPÚBLICA DOMINICANA. MINISTERIO DE INTERIOR Y POLICÍA. DIRECCIÓN GENERAL DE MIGRACIÓN. *Resolución No. DGM-04-12, op. Cit.,* p. 4. Esta disposición es compatible por entero con las directrices de la Directiva 2016/681, véase su considerando n˚ 17.

4. **Deberá modificarse la tarjeta de embarque/desembarque** que deben llenar los pasajeros, a fin de que se incluya una cláusula informativa de protección de datos donde se exprese la finalidad de la recogida de los datos, el destino y las formas de ejercer los derechos que les asisten a los interesados. (En el documento anexo **marcado con el número IV** hemos incluido un modelo tipo de clausula informativa que satisface estos requerimientos).

Por último, debemos recordar que la Directiva 2016/681 prohíbe el tratamiento de datos PNR que revelen el origen racial o étnico, las opiniones políticas, las creencias filosóficas o religiosas, la afiliación sindical, la vida sexual u orientación sexual y la 0salud, por lo cual:

5. En caso de que la DGM reciba datos de carácter sensible, **deberá suprimirlos inmediatamente.**

4.2.1.2. Medidas relativas al tratamiento y almacenamiento

En tanto a las medidas relacionadas al tratamiento y el almacenamiento de datos PNR, la Directiva 2016/681 la Dirección deberá tener en cuenta que:

1. En el tratamiento de datos personales de ciudadanos europeos, los datos PNR podrán conservarse por un período máximo de 5 años, pasados los 5 años deberán suprimirse.

2. Se recomienda el nombramiento de un responsable de protección de datos, cuyas funciones sean las de asesoramiento y supervisión del tratamiento de los datos PNR. Dicho responsable tendrá acceso a todos los datos tratados.

3. Luego de pasados 6 meses a contar desde la transmisión, o recogida de los datos PNR, deberán despersonalizarse mediante el enmascaramiento de los elementos que puedan identificar a los interesados.

4. Todo resultado derivado del tratamiento automatizado de datos PNR, deberá ser revisado de forma individual, por medios no automatizados.

5. No se adoptará decisión alguna que produzca efectos jurídicos desfavorables para una persona o que afecte considerablemente, apoyada únicamente en el tratamiento automático de datos PNR.

6. Cuando se considere probable que se produzca una violación de protección de datos PNR que pueda afectar la intimidad de sus titulares, la Dirección, en su caso, comunicará la vulneración al interesado y a la autoridad nacional competente del Estado miembro, de donde sea nacional dicho interesado.

4.2.1.3. Medidas relativas a la seguridad de la información

Una de las cuestiones sobre la cual es enfática la Directiva 2016/681, es la protección de la información. En tal sentido, dice que:

> *´´Todas las transmisiones de datos PNR se efectuarán por medios electrónicos que ofrezcan garantías suficientes en relación* ***con las medidas de seguridad técnicas y las medidas organizativas*** *que rigen el tratamiento de datos que se va a llevar a cabo. En caso de fallo técnico, los datos PNR podrán ser transmitidos por cualquier otro medio adecuado,* ***siempre que se mantenga el mismo nivel de seguridad*** *y que se cumpla íntegramente el derecho de la Unión en materia de protección de datos.´´*[65]

Asimismo, las disciplinas que tienen por objeto el estudio de la seguridad de la información han clasificado las medidas de protección de datos en: medidas legales, técnicas, organizativas y físicas. Se ha señalado igualmente que un régimen de protección que sólo contemple medidas legales resulta insuficiente cuando los datos personales se difunden por todo el mundo a través de las redes de TIC y en su tratamiento intervienen varias jurisdicciones.[66]

---

[65] DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Op. cit., Artículo 16.1

[66] Comisión Europea. Comunicación de la sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad, (*Privacy Enhanced Technology*, PET) referida por RIBAGORDA GARNACHO, Arturo. ´´La protección de datos personales y la seguridad de la información.´´ *Revista Jurídica de Castilla y León*. No. 16, septiembre, 2008.

Para desglosar las medidas relativas a la seguridad de la información utilizaremos como marco de referencia la normativa nacional española, en el entendido de que la misma es la más perfeccionada en este sentido dentro de los países miembros de la Unión Europea. El Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, ha estructurado un sistema acumulativo de protección que divide las medidas de seguridad en tres niveles: básico, medio y alto, contemplando dentro de esos niveles medidas tanto de carácter técnico, como organizativas y físicas.

Esa clasificación por niveles atiende a la naturaleza más o menos sensible de los datos personales que serán objeto de protección[67], los datos PNR al constituir una categoría de datos, cuyo cotejo con otras bases de datos permite evaluar determinados aspectos de la personalidad o del comportamiento de los pasajeros, les serían de aplicación las medidas de nivel medio[68], siendo de aplicación también las medidas de nivel básico, en vista de que como hemos señalado se trata de un método acumulativo de los niveles de las medidas de seguridad.

Tomando como parámetro las medidas que instituye el Reglamento de Desarrollo de la Ley Orgánica 15/1999, para los niveles básico y medio, se recomienda lo siguiente:

1. La Dirección deberá crear un documento de seguridad donde se recojan todas las medidas de seguridad que se han detallado y las que se detallarán, con la debida identificación del personal encargado de cumplimentarlas en cada caso, dicho documento también serviría de guía del personal de la Dirección General de Migración frente a cualquier duda en el tratamiento de los datos PNR.

2. En relación a las funciones y obligaciones del personal, la Dirección deberá definir con claridad las funciones y obligaciones de cada uno de los usuarios que acceda a los datos PNR, así deberá recogerse en el documento de seguridad.

[67]RIBAGORDA GARNACHO, Arturo, ´´La protección de datos personales y la seguridad de la información.´´ *Revista Jurídica de Castilla y León* No. 16, septiembre, 2008.
[68] Véase el artículo 81, f) del Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, *Boletín Oficial del Estado*, núm 17, de 19/01/2008.

3. La DGM hará todo lo necesario para que el personal esté al tanto de las medidas que tiene a su cargo y de las consecuencias que pudiesen derivarse de su incumplimiento.

4. La DGM creará un registro de incidencias donde se consignen las incidencias que afecten los datos PNR, el momento en que se produjeron, y las medidas correctoras tomadas a fin de subsanarlas.

5. La DGM establecerá en sus protocolos, que su personal solo tendrá acceso a los datos que sean necesarios para el desarrollo de sus funciones, se encargará de actualizar la relación de usuarios y perfiles de usuarios y sus autorizaciones, de manera individualizada.

6. La DGM tendrá el deber de evitar que un usuario pueda acceder a recursos para los cuales no está autorizado y únicamente el personal autorizado e identificado en el documento de seguridad podrá conceder, anular, o variar las autorizaciones de acceso.

7. En cuanto a la gestión de documentos y soportes, los mismos deberán inventariarse, identificarse y solo podrán ser accesibles por los usuarios autorizados, excepto en los casos que las particularidades físicas del soporte o documento lo impidan.

8. Cuando la información contenida en soportes y documentos vaya a ser trasladada fuera de los locales de la Dirección, dicho traslado deberá ser autorizado por la persona que se designe como responsable de seguridad y serán adoptadas medidas que no eviten la pérdida, el acceso indebido o la sustracción de los documentos y soportes.

9. Al momento de que vaya a desecharse algún documento o soporte contentivo de datos PNR, se procederá a la destrucción o borrado de dicho documento o soporte adoptando medidas que impidan el acceso a la información o su recuperación posterior.

10. Por lo que respecta a la correcta identificación y autenticación se deberán adoptar mecanismos a fin de garantizar que la identificación se realice de forma personalizada e inequívoca y verificada para todos los usuarios autorizados. Los mencionados mecanismos de autenticación podrán apoyarse en las contraseñas que en todo caso serán asignadas, distribuidas y almacenadas de acuerdo a un procedimiento que vele por la confidencialidad e integridad de las mismas.

11. Se recomienda establecer un período no superior a un año para el cambio de las contraseñas descritas anteriormente.

12. En la medida de lo posible, deberán realizarse copias de respaldo y recuperación de los datos cada semana. De igual manera, serán establecidos procedimientos que aseguren la reconstrucción de de los datos al estado anterior a la pérdida o destrucción.

13. En las pruebas que se lleven a cabo para lograr la medida precedente, no podrán ser utilizados datos reales, a menos de que se garantice el nivel de seguridad acorde al tratamiento efectuado, y se haya realizado una copia de seguridad.

14. Se deberá designar uno o varios responsables de seguridad, a fin de que se encarguen de la coordinación y el control de la aplicación de las medidas de seguridad que hemos venido enunciando. En todo caso, la Dirección será la responsable de cara a terceros sobre las violaciones de protección de datos y no la/s persona/s designadas como responsables de seguridad.

15. Los archivos de datos donde sean almacenados los datos PNR y las instalaciones donde se encuentren estos archivos serán objeto de auditorías internas o externas, al menos cada dos años, en la medida de lo posible. Estas auditorías estarán dirigidas al examen del cumplimiento de los protocolos de actuación en materia de protección de datos y las medidas de seguridad.

16. Los informes que se deriven de las auditorías deberán ser estudiados por el o los responsables de seguridad, que trasladará las conclusiones a los directivos de la DGM, para que en su caso, se ordene la adopción de las medidas correctoras de lugar.

17. Aunado a lo que hemos enunciado sobre los soportes y documentos, se establecerá un sistema para registrar el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos enviados, la modalidad de envío y la persona encargada de su recepción que deberá ser autorizada por la Dirección.

18. En cuanto a las medidas de seguridad físicas, únicamente el personal de la DGM que a tales efectos se designe en el documento de seguridad, podrá acceder a los locales donde se encuentren los sistemas de recogida, almacenamiento y procesamiento de los datos.

19. La DGM tomará las medidas técnicas necesarias para que se limite la posibilidad de intentos repetidos de acceso no autorizado a sus bases de datos.

20. Por último, se creará un registro de incidencias donde tendrán que ser recogidos los procedimientos de recuperación de datos PNR. En caso de que se haya producido una pérdida de datos PNR, en el registro de incidencias deberán consignarse también, los datos recuperados, y la persona ejecutante de la recuperación.

CONCLUSIONES

- El marco jurídico de protección de datos que ofrece la legislación de la República Dominicana, está construido sobre la base de los mismos principios que informan y configuran este derecho a escala de la Unión Europea, de tal suerte ambos marcos normativos son cónsonos en su esencia, y no presentan contradicciones. Sin embargo, en comparación con el derecho europeo, el reconocimiento del derecho a la protección de datos personales en la República Dominicana aún es embrionario, lo cual tiene como consecuencia que el nivel de protección de datos no sea del todo efectivo en atención a algunas carencias como el desarrollo reglamentario de la Ley de Protección de Datos de la República Dominicana.

- A consecuencia de tal situación, el organismo solicitante del presente informe, la Dirección General de Migración de la República Dominicana, tendrá que poner en marcha la adopción de las diversas medidas que han sido expuestas, para situarse a la par de las entidades que tratan los datos PNR dentro de los Estados miembros de la Unión Europea y así proporcionar un nivel equiparable de protección de datos.

- Si las medidas técnicas, organizativas y físicas que han sido señaladas son adoptadas por la Dirección General de Migración, es indudable que la República Dominicana estaría dotada de las condiciones que le permitan negociar un acuerdo de transferencia de datos PNR con la Unión Europea, ya que la institución encargada del tratamiento de esos datos en territorio dominicano, estaría proveyendo las garantías suficientes en materia de protección de datos de carácter personal.

- En concreto, La Dirección General de Migración debe modificar sus protocolos de actuación para el tratamiento de datos del registro de nombre de los pasajeros, incluyendo las medidas de carácter técnico y organizativo que aseguren la garantía real y efectiva del derecho a la protección de datos personales, dotando a su

personal de las herramientas necesarias para no solo brindar un nivel de protección de datos equiparable al europeo.

BIBLIOGRAFÍA

DOCTRINA

BALBUENA BATISTA, PEDRO *et al*, *Constitución Comentada*, 3ra edición, Santo Domingo: Fundación Institucionalidad y Justicia, Inc. (FINJUS), 2012.

BALLESTEROS MOFFA, Luis Ángel. *La tutela jurídica de los datos personales.* Editorial Civitas, SA, Pamplona, 2008.

CAZURRO BARAHONA, Víctor. *Transferencias internacionales de Datos.* Editorial Aranzadi, SA, Pamplona, 2014.

IRUJO AMEZAGA, Mikel. *Seguridad nacional versus derechos fundamentales.* Editorial Aranzadi, SA, Pamplona, 2006.

JORGE PRATS, Eduardo, *Comentarios a la Ley Orgánica del Tribunal Constitucional y de los Procedimientos Constitucionales*, Santo Domingo: IUS NOVUM, Impresión: Amigo del Hogar, 2011.

PALOMAR OLMEDA, Alberto y PÉREZ GONZÁLEZ, Carmen. *La protección de datos: su marco constitucional y el contexto del nuevo Reglamento.* Editorial Aranzadi, SA, Pamplona, 2008.

PÉREZ FRANCESCH, Joan Lluís; GIL MÁRQUEZ, Tomás y GACITÚA ESPÓSITO, Alejandro. *La utilización de datos personales contenidos en el registro de nombres de pasajeros: ¿fines represivos o preventivos? Barcelona:* Institut de Ciencies Polítiques i Socials. Barcelona, 2011.

TEJERINA RODRÍGUEZ, Ofelia, *Seguridad del Estado y privacidad,* Madrid: Editorial Reus, S.A., 2014.

CONVENIOS INTERNACIONALES

Acuerdo entre la Comunidad Europea y el Gobierno de Canadá sobre el tratamiento de datos procedentes del sistema de información anticipada sobre pasajeros y de los expedientes de pasajeros*. Diario Oficial de la Unión Europea* n˚ L 82/15 de 21 de marzo de 2006.

Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos, generados en la Unión Europea, del registro de nombres de los pasajeros (PNR) por las compañías aéreas a los Servicios de Aduanas de Australia. *Diario Oficial de la Unión Europea* n˚ 213/49 de 8 de agosto de 2008.

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL. *Convenio sobre Aviación Civil Internacional.* Novena edición, 2006.

Organización de las Naciones Unidas, Plan de acción para prevenir el extremismo violento, Asamblea General, 24 de diciembre de 2015. Disponible en web: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/674&referer=/english/&Lang=S [Fecha de consulta: 1-6-2016]

LEGISLACIÓN COMUNITARIA

Decisión marco 2008/977/JAI del Consejo de 27 de noviembre de 2008 relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. *Diario Oficial de las Comunidades Europeas* n˚ L 350/6, 2008.

Decisión marco 2008/977/JAI del Consejo de 27 de noviembre de 2008 relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal*, Diario Oficial de las Comunidades Europeas,* 30 de diciembre de 2008.

Decisión marco del Consejo de 13 de junio de 2002 sobre la lucha contra el terrorismo (2002/475/JAI), *Diario Oficial de las Comunidades Europeas*, n˚ L 164/3, 22 de junio de 2002.

Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, *Diario Oficial de la Unión Europea* n˚ L 119/132*,* de 4 de mayo de 2016.

Directiva 2004/82/CE del Consejo de 29 de abril de 2004 sobre la obligación de los transportistas de comunicar los datos de las personas transportadas. *Diario Oficial de la Unión Europea* n˚ L261/2*,* de 6 de agosto de 2004.

Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *Diario Oficial de las Comunidades Europeas* n˚ L 281/31 de 23 de noviembre de 1995.

Reglamento (CE) No. 80/2009 del Parlamento Europeo y del Consejo de 14 de enero de 2009 por el que se establece un código de conducta para los sistemas informatizados de reserva y por el que se deroga el Reglamento (CEE) No. 2299/89 del Consejo. *Diario Oficial de la Unión Europea* n˚ L 35/47 de 4 de febrero de 2009.

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO 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), de 14 de abril de 2016.

LEGISLACIÓN DOMINICANA

República Dominicana. Ley No. 137-11 Orgánica del Tribunal Constitucional y de los procedimientos constitucionales de 13 de junio de 2011 *Gaceta Oficial* No. 10622 del 15 de junio de 2011.

República Dominicana, Constitución Política, votada y proclamada por la Asamblea Nacional en fecha 13 de junio de 2015 *Gaceta Oficial* No. 10805 del 10 de julio de 2015.

República Dominicana. Ley 285-04, General de Migración *de* 15 de agosto de 2004*, Gaceta Oficial No. 10291 del 27 de agosto de 2004.*

República Dominicana. Ley No. 172-13 de 13 de diciembre de 2013, que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. *Gaceta Oficial* No. 10737 del 15 de diciembre de 2013.

República Dominicana. *Reglamento No.285-04 de aplicación de la Ley General de Migración del 15 de agosto de 2004.*

INFORMES Y COMUNICACIONES

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Informe 0076/2009,* 2009.

Banco Central de la República Dominicana. *Estadísticas turísticas 2015*, Santo Domingo, abril de 2016. Publicación disponible en la web: http://www.bancentral.gov.do/publicaciones_economicas/turisticas/turisticas2015-12.pdf [Fecha de consulta: 1-6-2016]

Banco Central de la República. *Informe del flujo turístico enero - mayo 2016*. Publicación disponible en la web: http://www.bancentral.gov.do/publicaciones_economicas/informe_turistico/informe_turistico2016-05.pdf [Fecha de consulta: 1-6-2016]

COMISIÓN DE LAS COMUNIDADES EUROPEAS. *Comunicación de la Comisión. Hacia una estrategia sobre la dimensión exterior del espacio de libertad, seguridad y justicia.* Bruselas, 2005.

Comisión Europea, *Comunicación de la Comisión de las Comunidades Europeas sobre el espacio de libertad, seguridad y justicia*, de fecha 20 de abril de 2010.

COMISIÓN EUROPEA. *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-363/14.* 2015.

COMISIÓN EUROPEA. *Comunicación de la Comisión de las* Comunidades Europeas *al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos. Plan de acción por el que se aplica el programa de Estocolmo.* 2010.

COMISIÓN EUROPEA. *Comunicación de la Comisión sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países,* 2010.

European Union Terrorism Situation and Trend Report 2015, EUROPOL, La Haya, 2015, ISSN 2363-0876.

Informe Final A6-0226/2005, del Parlamento Europeo, sobre la propuesta de Decisión del Consejo relativa a la celebración de un Acuerdo entre la Comunidad Europea y el Gobierno de Canadá sobre el tratamiento de datos procedentes del sistema de información anticipada sobre pasajeros (API) y de los expedientes de los pasajeros (PNR) (COM(2005)0200 – C6-0184/2005 – 2005/0095(CNS)), de 4.07.2005. Disponible en la web: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML+REPORT+A62005-0226+0+DOC+PDF+V0//ES [Fecha de consulta: 1-6-2016]

DICTÁMENES

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo relativa a la celebración del Acuerdo entre los Estados Unidos de

América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (2012/c-35/03), *Diario Oficial de la Unión Europea*, n˚ C 35/16, *9 de febrero de* 2012.

GRUPO DE TRABAJO DEL ARTÍCULO 29. *Dictamen conjunto sobre la propuesta de Decisión marco del Consejo relativa al uso del registro de nombres de los pasajeros ("Passenger Name Record"- PNR) a efectos de la aplicación de la ley, presentado por la Comisión el 6 de noviembre de 20007.* Bruselas, 2007.

GRUPO DE TRABAJO DEL ARTÍCULO 29. *Dictamen 10/2001 relativo a la necesidad de un enfoque equilibrado en la lucha contra el terrorismo.* Bruselas*,* 2001.

GRUPO DE TRABAJO DEL ARTÍCULO 29. *Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries,* Bruselas, 2010.

GRUPO DE TRABAJO DEL ARTÍCULO 29. *Dictamen 10/2011 relativo a la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para prevención, detección, investigación y enjuiciamiento de los delitos terroristas y delitos graves.* Bruselas, 2011

CONFERENCIAS

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL. Conferencia de alto nivel sobre seguridad de la aviación. *Información anticipada sobre los pasajeros (API) y su función en la seguridad de la aviación.* Montreal, 2012.

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL. Conferencia de alto nivel sobre seguridad de la aviación (HLSCA), *información anticipada sobre los pasajeros (API) y su función en la seguridad de la aviación,* Montreal, 2012.

JURISPRUDENCIA

TRIBUNAL DE JUSTICIA DE LAS COMUNIDADES EUROPEAS. *Caso Parlamento/Consejo contra Parlamento/Consejo. (Gran Sala) Caso Parlamento Europeo contra Consejo de la Unión Europea. Sentencia TJCE/2006/146 de 30 de mayo de 2006.*

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. *Caso Comisión/Hungría (Gran Sala). Caso Comisión Europea contra Hungría. Sentencia TJCE/2014/139 de 8 de abril 2014.*

PROGRAMAS Y DECLARACIONES

CONSEJO DE LA UNIÓN EUROPEA, Estrategia Europea sobre la lucha contra el terrorismo de fecha 30 de noviembre de 2005. Disponible en laweb: http://register.consilium.europa.eu/doc/srv?f=ST+14469+2005+REV+4&l=es [Fecha de consulta: 1-6-2016]

CONSEJO DE LA UNIÓN EUROPEA, *Declaración sobre la lucha contra el terrorismo.* Bruselas, 2004. Disponible en la web: http://www.realinstitutoelcano.org/especiales/atentados/docs/declaracterrorUE25304.pdf [Fecha de consulta: 1-6-2016]

CONSEJO EUROPEO, Programa de Estocolmo, Una Europa abierta y segura que sirva y proteja al ciudadano (2010/C-115/01), *Diario Oficial de la Unión Europea* n˚ C 115/1, de 4 de mayo de 2010.

ARTÍCULOS DE PUBLICACIONES EN SERIE

ANCOS FRANCO, Helena. ´´La regulación de las Transferencias Internacionales de Datos de carácter personal como barrera al comercio internacional: de la Directiva 95/46 a los acuerdos UE- terceros Estados.´´ Disponible en la web: file:///C:/Users/yea/Downloads/DialnetLaRegulacionDeLasTransferenciasInternacionalesDeDa-195280.pdf

ARENAS NAON, Pedro M. ´´Los procedimientos administrativos en materia de transferencias internacional de datos de carácter personal.´´ *Revista de Derecho UNED*, núm. 5, 2009.

BLAS, Frédéric. ´´Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales.´´ *Revista Derecho del Estado* No. 23, diciembre de 2009.

GUASCH PORTAS, Vicente. ´´La transferencia internacional de datos de carácter personal.´´ *Revista de Derecho UNED*, No. 11, 2012.

RIBAGORDA GARNACHO, Arturo. ´´La protección de datos personales y la seguridad de la información.´´ *Revista Jurídica de Castilla y León.* No. 16. Septiembre 2008.

RESOLUCIONES

REPÚBLICA DOMINICANA. MINISTERIO DE INTERIOR Y POLICÍA. DIRECCIÓN GENERAL DE MIGRACIÓN. *Resolución No. DGM-04-12 que crea los protocolos para el servicio obligatorio de la información avanzada de pasajeros y tripulantes en todas las operaciones de transporte internacional con destino o desde territorio nacional,* Santo Domingo, 2012.

PÁGINAS WEB

http://www.consilium.europa.eu/es/policies/fight-against-terrorism/passenger-name-record/

http://euroefe.euractiv.es/5533_dosieres/3752304_el-parlamento-europeo-da-luz-verde-a-la-directiva-sobre-registro-de-datos-de-pasajeros-aereos-pnr.html

NOTICIAS

Cancillería y PNUD publican inventario de buenas prácticas institucionales, *Diario Libre*, 6 de junio de 2016. Disponible en la web: http://www.diariolibre.com/noticias/cancilleria-y-pnud-publican-inventario-de-buenas-practicas-institucionales-MG3967853 [Fecha de consulta: 6-6-16]

OTROS

COMISIÓN EUROPEA. *Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, Bruselas,* 2011.

ANEXOS

ANEXO I

Lista de los datos del registro de nombres de los pasajeros recopilados por las compañías aéreas según la Directiva 2016/681:

1. Localizador de registro PNR
2. Fecha de reserva/emisión del billete
3. Fecha(s) fechas de viaje prevista(s)
4. Nombre(s) y apellido(s)
5. Dirección y datos de contacto (número de teléfono, dirección de correo electrónico)
6. Todos los datos de pago, incluida la dirección de facturación
7. Itinerario completo del viaje para el PNR específico
8. Información sobre viajeros asiduos
9. Agencia de viajes/operador de viajes
10. Situación de vuelo del pasajero: confirmaciones, facturación, no comparecencia o pasajeros de última hora sin reserva
11. Información PNR escindida/dividida
12. Observaciones generales (incluida toda la información disponible sobre menores de 18 años no acompañados, como nombre y sexo del menor, edad, idiomas que habla, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de salida y vínculo con el menor, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de llegada y vínculo con el menor, agente en el lugar de salida y de llegada)
13. Información sobre el billete, incluidos el número del billete, la fecha de emisión, los billetes solo de ida y la indicación de la tarifa de los billetes electrónicos (Automatic Ticket Fare Quote)
14. Datos del asiento, incluido el número
15. Información sobre códigos compartidos
16. Toda la información relativa al equipaje
17. Número de viajeros y otros nombres de viajeros que figuran en el PNR

18. Cualquier información recogida en el sistema de información anticipada sobre los pasajeros (sistema API) (incluidos el tipo, número, país de emisión y fecha de expiración de cualquier documento de identidad, nacionalidad, apellidos, nombre, sexo, fecha de nacimiento, compañía aérea, número de vuelo, fecha de salida, fecha de llegada, aeropuerto de salida, aeropuerto de llegada, hora de salida y hora de llegada)
19. Todo el historial de cambios de los datos PNR indicados en los números 1 a 18.

ANEXO II

Lista de los elementos que pueden servir para identificar directamente al pasajero al que se refieren los datos PNR y que deben ser despersonalizados mediante su enmascaramiento, cuando hayan transcurrido 6 meses desde la transmisión o recogida de los datos PNR:

a) nombre(s) y apellido(s), incluidos los de otros pasajeros que figuran en el PNR y número de personas que figuran en el PNR que viajan juntas;

b) dirección y datos de contacto;

c) rodos los datos sobre el pago, incluida la dirección de facturación, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, o a cualquier otra persona;

d) información sobre viajeros asiduos;

e) observaciones generales, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, y

f) toda la API recopilada

ANEXO III

Lista de los delitos considerados como delitos graves según la Directiva 2016/681:

1. pertenencia a una organización delictiva
2. trata de seres humanos
3. explotación sexual de niños y pornografía infantil
4. tráfico ilícito de estupefacientes y sustancias psicotrópicas
5. tráfico ilícito de armas, municiones y explosivos
6. corrupción
7. fraude, incluido el que afecte a los intereses financieros de la Unión
8. blanqueo del producto del delito y falsificación de moneda, con inclusión del euro
9. delitos informáticos/ciberdelincuencia
10. delitos contra el medio ambiente, incluido el tráfico ilícito de especies animales protegidas y de especies y variedades vegetales protegidas
11. ayuda a la entrada y residencia ilegales
12. homicidio voluntario, agresión con lesiones graves
13. tráfico ilícito de órganos y tejidos humanos
14. secuestro, detención ilegal y toma de rehenes
15. robo organizado y a mano armada
16. tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte
17. falsificación y violación de derechos de propiedad intelectual o industrial de mercancías
18. falsificación de documentos administrativos y tráfico de documentos administrativos falsos
19. tráfico ilícito de sustancias hormonales y otros factores de crecimiento
20. tráfico ilícito de materiales radiactivos o sustancias nucleares
21. violación
22. delitos incluidos en la jurisdicción de la Corte Penal Internacional
23. secuestro de aeronaves y buques
24. sabotaje
25. tráfico de vehículos robados
26. espionaje industrial.

ANEXO IV

Modelo tipo de cláusula de protección de datos para ser incluida en la tarjeta de embarque.

De conformidad con lo dispuesto en el art. 5.3 de la Ley No. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. G. O. No. 10737 del 15 de diciembre de 2013., se informa:

Que los datos personales obtenidos a través de este formulario serán incorporados al archivo de datos denominado "Datos del registro de pasajeros´´, titularidad de la Dirección General de Migración de la República Dominicana, y serán tratados con el legítimo fin de realizar las labores de control fronterizo y migratorio. La Dirección General de Migración garantiza que ha adoptado las medidas técnicas y organizativas necesarias para asegurar la seguridad de los datos personales tratados. Todo interesado puede ejercitar sus derechos de acceso, rectificación, y supresión ante esta Dirección localizada en la Autopista 30 de Mayo Esq. Héroes de Luperón, Santo Domingo 10401, República Dominicana.