

# La protección de los datos personales en la Europa de Schengen

ALVARO SÁNCHEZ BRAVO

*Facultad de Derecho de la Universidad de Sevilla  
Dpto. de Filosofía del Derecho*

## LOS ACUERDOS DE SCHENGEN. DETERMINACION DE SU NATURALEZA JURIDICA.

La firma del **Acuerdo de Schengen** entre los gobiernos de los Estados del Benelux (Luxemburgo, Países Bajos y Bélgica), de la República Federal de Alemania y de la República Francesa tuvo lugar el 14 de junio de 1985 en la localidad fronteriza luxemburguesa que da nombre al Acuerdo.<sup>1 2</sup>

Las Partes Contratantes reconocen como su misión la de contribuir a la supresión de los controles de personas en las fronteras exteriores y facilitar la libre circulación de mercancías.

La estructura Schengen ha nacido de la creencia de considerar la puesta en marcha del programa comunitario como provocador de un déficit de seguri-

- 1 Cfr. LAZARO MORENO, F., **El Acuerdo de Schengen y la libre circulación de personas en la CEE**, Cuadernos de Europa, nº 2, Diputación de Zaragoza (Comisión de Europa), Zaragoza, 1993.
- 2 Como antecedentes de este Acuerdo pueden citarse, tal y como se desprende de los propios antecedentes explicitados en su texto, los siguientes hechos:
  - Conclusiones de la Reunión de Neustadt/Naaisch, de 31 de mayo de 1984, de los Ministros de Transportes de los Estados del Benelux y la República Federal de Alemania.
  - Declaración del Consejo Europeo de Fontainebleau, de los días 25 y 26 de junio de 1984, relativa a la supresión en las fronteras interiores de las formalidades de policía y de aduanas para la circulación de personas y mercancías.
  - Acuerdo de Sarrebruck, de 13 de julio de 1984, entre la República Federal de Alemania y la República Francesa, para la eliminación de los controles aduaneros entre ambos países.
  - Memorandum de los Gobiernos del Benelux, de 12 de diciembre de 1984, remitido a los gobiernos de la República Federal de Alemania y la República Francesa.Debe hacerse hincapié en la frenética actividad desplegada en ese año 1984, y que tuvo como protagonistas a los mismos países que pocos meses más tarde firmaron el Acuerdo de Schengen.

dad. Es cierto, en efecto, que abandonando la iniciativa del proceso a las instituciones comunitarias, los seis corrían el riesgo de quedar en una situación comprometida, si la supresión de los dispositivos de protección del orden público en las fronteras interiores no coincidía con la aplicación simultánea e integral de dispositivos de seguridad en las fronteras exteriores y con la unificación de los procedimientos represivos y de colaboración policial. Sin duda, es la fragilidad de la voluntad política de la Europa de los doce lo que se cuestiona y la ineptitud del proceso decisional comunitario para realizar unas medidas que necesitan la aplicación coordinada de los Estados miembros.<sup>3</sup>

Una de las principales razones de estas dificultades, señaladas por la Comisión en su **Quinto Informe sobre la realización del Libro Blanco**, aparece porque los procedimientos comunitarios ofrecen múltiples ocasiones de bloqueo o retardo.

El Acuerdo de 1985 distingue entre medidas aplicables a corto ( Título I) y a largo plazo ( Título II). El objetivo a cumplir claramente indicado: suprimir los controles en las fronteras comunes ( y no las fronteras mismas como parecía suponer el artículo 8.A del Tratado de Roma ) para concentrarlos en las fronteras exteriores, supone pues dos órdenes de medidas previas. Las primeras necesitan de la técnica clásica, "de armonización de las disposiciones legislativas y reglamentarias"<sup>4</sup>. Las otras medidas son las denominadas complementarias<sup>5</sup>.

Entre las medidas que deberían realizarse a corto plazo destaca la necesidad de mejorar el intercambio de información entre los Estados miembros, así como proceder a su reforzamiento en todos aquellos datos que sean necesarios para la lucha contra la criminalidad<sup>6</sup>. La información, y la necesidad de su transmisión, se revela ya desde los orígenes como un elemento fundamental, imprescindible, para llevar a buen puerto la "nueva Europa" que se pretende construir.

Este acuerdo de 1985 hacía referencia en numerosos preceptos a una convención ulterior, destinada a completarlo y precisar su contenido. Este fue el objeto del **Convenio de Aplicación del Acuerdo de Schengen**, firmado el 19 de junio de 1990.

■ 3 Weckel, P., *La convention additionnelle a l'Accord de Schengen*, *Revue Generale de Droit International Public*, Tome 95/1991/2, pp. 422-423.

■ 4 Cfr. arts. 19 y 20 del Acuerdo de Schengen de 14 de junio de 1985, relativo a la supresión gradual de controles en las fronteras comunes, B.O.E. nº 181, de 30 de julio de 1991.

■ 5 Cfr. art. 18 del Acuerdo de Schengen..., cit.

■ 6 Cfr. **Art. 9 del Acuerdo de Schengen**, cit..

Su propia estructura evidencia la pluralidad de sectores que se verán afectados por esta regulación<sup>7</sup>, y que pueden sistematizarse en los dos grandes objetivos a conseguir:

1. Cooperación policial, judicial y aduanera.
2. Armonización de la política de visados y del derecho de asilo.

Es preciso llamar la atención sobre el hecho de que el Convenio de Aplicación de Schengen responde precisamente a la finalidad de suprimir los controles en las fronteras interiores y toma como punto de referencia la existencia de un “**espacio interior común**”. Impone un especial deber de diligencia sobre aquellos Estados cuyas fronteras son calificadas de “exteriores”, ya que a través de las mismas van a entrar en territorio común extranjeros que podrán desplazarse **de facto** en este espacio interior como consecuencia del juego de la libre circulación de personas<sup>8</sup>.

La obtención de un espacio interior sin controles no se concibe sin que se transfiera a la frontera exterior un modo uniforme de controlar el cruce en interés de todos los Estados miembros<sup>9</sup>.

Desde las primeras reuniones intergubernamentales para el desarrollo del objetivo del espacio interior sin controles en las fronteras comunes ha estado patente que los problemas del terrorismo, el tráfico de drogas, los problemas de otros delitos de delincuencia organizada, tráfico ilícito de obras de arte, etc. y los problemas de la inmigración clandestina no deben desviar a la Comunidad del objetivo de la libre circulación interior. Pero al mismo tiempo ese objetivo no puede generar déficit de seguridad; debe ser compatible con la necesidad de combatir el terrorismo, el tráfico de drogas y otras formas graves de delincuencia internacional.

- 7 El Convenio de Aplicación del Acuerdo de Schengen presenta la siguiente estructura:

Título I: Definiciones (Art. 1)

Título II: Supresión de controles en las fronteras interiores y circulación de personas (Arts. 2-38)

Título III: Policía y Seguridad (Arts. 39-91)

Título IV: Sistema de Información de Schengen (Arts. 92-119)

Título V: Transporte y Circulación de mercancías (Arts. 120-125)

Título VI: Protección de los Datos de carácter personal (Arts. 126-130)

Título VII: Comité Ejecutivo (Arts. 131-133)

Título VIII: Disposiciones Finales (Arts. 134-142)

- 8 Cfr. ESCOBAR HERNANDEZ, C., **El convenio de Aplicación del Acuerdo de Schengen y el Convenio de Dublín: Una aproximación al asilo desde la perspectiva comunitaria**, Revista de Instituciones Europeas, Vol. 20, núm. 1, 1993, pp. 69-70.
- 9 Cfr. DE MIGUEL ZARAGOZA, J. y BLANCO DE CASTRO, A., **El Título VI del Tratado de la Unión: Cooperación en asuntos de Justicia e Interior**, Gaceta jurídica de la C.E.E. y de la Competencia, GJ 115, Serie D, núm D-18, Septiembre de 1992, p. 202.

La sustitución de los controles internos, además de medidas de armonización legislativa y de mejora de la asistencia judicial internacional en materia penal, hace necesario un mejor intercambio en la información<sup>10</sup>.

Con objeto de conseguir ese mejor intercambio de información se introduce una de las principales innovaciones de este convenio: un complejo sistema informático, denominado Sistema de Información de Schengen, constitutivo del soporte para la transmisión automatizada de los datos necesarios para la consecución de los precitados objetivos. Al estudio de este Sistema y a los riesgos que presenta para los derechos de los ciudadanos, especialmente para su intimidad, dedicaremos el contenido de nuestra exposición.

Respecto a su contenido material, debemos hacer constar como las materias que regulan estos convenios se refieren a cuestiones que bien pudieran encontrarse dentro del campo de las competencias comunitarias. Como ya señalamos previamente, esto conduce a la necesidad de determinar cual es la naturaleza jurídica de estas normas, que generadas en el marco de lo que se conoce como "cooperación intergubernamental", sin embargo pueden constituir una suplantación de la actividad de las instituciones comunitarias en la regulación de determinados competencias que le son propias.

Ello nos invita, por tanto, a reflexionar sobre las relaciones entre este "derecho subregional" y el derecho comunitario.

Mucho se ha debatido, y se continúa debatiendo, en torno a cual es la verdadera naturaleza jurídica de estos acuerdos. Al respecto, y sin ánimo de ser exhaustivos, sí que conviene indicar cuales son las principales orientaciones; que pueden agruparse en tres categorías:

1. Consideración como textos de Derecho Comunitario General. Acuerdos que los Estados, en uso de su soberanía y su capacidad jurídica para obligarse internacionalmente, concluyen para regular determinados sectores comunes. Las obligaciones y derechos que se generan de tales acuerdos sólo serían directamente exigidos y exigibles por los Estados miembros, tal y como deriva de la técnica normal de conclusión de estos textos.

2. Se trataría de un Derecho especial, sui generis, más concreto que el que suele derivar de acuerdos internacionales "strictu sensu". La peculiar natu-

■ 10 Cfr. DE MIGUEL ZARAGOZA, J. y BLANCO DE CASTRO, A., *El Título VI del Tratado de la Unión Europea: Cooperación en asuntos...*, cit., pp. 212-213.

raleza de las materias que regula, y el concreto y restringido número de Estados destinatarios, hace que deba considerarse como un " derecho intermedio ", de naturaleza vinculante, pero no susceptible de ejecución obligatoria.

3. Los Acuerdos de Schengen son Derecho Comunitario. Apoya esta consideración la naturaleza comunitaria de las materias que regula, así como el carácter comunitario de los Estados a los que va dirigido. La conclusión en forma que parezca un convenio internacional, no es, como ya se ha indicado, más que una treta para burlar el control que debería haberse ejercitado por las instituciones comunitarias. Constituirían auténticos " **actos en fraude de ley comunitaria** ".

Seguro que no faltarán argumentos en apoyo de unas u otras consideraciones. Baste ahora dejarlos indicados, y proceder a escrutar que pueda extraerse del propio articulado del Convenio.

La Convención de Schengen prevé, en numerosas disposiciones, su inserción en el derecho comunitario. No impone ser tomada como modelo por los otros Estados miembros, pero este movimiento ya ha comenzado.

La inserción de los acuerdos de Schengen en el derecho comunitario responde a un cierto número de principios, no expresados en estos términos por la Convención, pero de hecho todos manifestados. Es primeramente el *principio de exclusividad* que se deduce del **art. 140** del Convenio, a tenor del cual: " **Todo Estado miembro de las Comunidades Europeas podrá convertirse en Parte contratante del presente Convenio** ". Es seguidamente el *principio de solidaridad* de los signatarios actuales en las negociaciones, discusiones y mecanismos de elaboración del derecho comunitario, en numerosas ocasiones expresado a propósito de la libre circulación de mercancías especialmente. En el Acuerdo son los **arts. 21, 22, y 24**: " **Las Partes adoptarán iniciativas comunes en el seno de las Comunidades Europeas..**", " **se esforzarán, tanto entre ellas, como en el seno de la Comunidades Europeas..**". En la Convención deben citarse los siguientes Considerandos:

" **Considerando que el Tratado constitutivo de las Comunidades Europeas, completado por el Acta Unica Europea, dispone que el mercado interior implicará un espacio sin fronteras interiores**",

"**Considerando que la finalidad perseguida por las Partes Contratantes coincide con el citado objetivo, sin perjuicio de las medidas que se adopten en aplicación de las disposiciones del Tratado**".

Especial consideración, sin perjuicio de la importancia evidente que revisten los textos anteriormente reseñados, merecen los arts.120.4 y 122.2.2: “...las Partes Contratantes colaborarán estrechamente (...) en el marco de las Comunidades Europeas”; “se esforzarán por adaptar una posición común en lo referente a la modificación de las directivas comunitarias (...) y para el establecimiento de actos comunitarios”.

Esta manifestación de las evidentes relaciones entre Schengen y Comunidades Europeas constituye el punto central de nuestra argumentación. Tal y como se deduce del propio Convenio de Aplicación, se consolida el reconocimiento del **principio de subordinación** del “Derecho de Schengen” con respecto al Derecho Comunitario. Dos artículos expresan clara y contundentemente este principio transcendente en orden a la determinación de la naturaleza jurídica de este “nuevo orden europeo”. Respecto al derecho comunitario *strictu sensu*, es el art. 134: “**Las disposiciones del presente convenio únicamente serán aplicables en la medida en que sean compatibles con el Derecho comunitario**”. Se evidencia en este precepto la *primacía* otorgada por el propio Convenio al Derecho comunitario. Respecto al derecho comunitario fruto de convenciones particulares firmadas por los Doce, se recoge en el art. 142 : “**Cuando se suscriban convenios entre los Estados miembros de las Comunidades europeas con vistas a la realización de un espacio sin fronteras interiores, las Partes Contratantes acordarán las condiciones en las que las disposiciones del presente Convenio serán sustituidas o modificadas en función de las disposiciones correspondientes de dichos convenios... Las disposiciones que sean contrarias a las acordadas entre los Estados miembros de las Comunidades Europeas se adaptarán en cualquier caso**”.

Llama la atención el hecho de que unas normas elaboradas en el marco de la cooperación intergubernamental de los Estados miembros, “percibidas” socialmente como comunitarias y cuyo fin es garantizar la efectiva aplicación de un objetivo comunitario, queden al margen de los controles judiciales y de los mecanismos institucionalizados de solución de controversias previstos en el ordenamiento jurídico comunitario.

Es cierto, que al no tratarse de una regulación comunitaria en sentido estricto, su control escapa al Tribunal de Justicia, que carece de competencia automática al respecto. Nada impide, sin embargo, que se le pueda atribuir dicha competencia mediante acuerdo entre los Estados Partes en el convenio. Solución que viene a ser confirmada por el propio Tratado de la Unión Europea, que contempla la posibilidad de que se puedan atribuir competencias al T.J.C.E. respecto de aquellos Tratados cuya finalidad sea poner en marcha la cooperación en el ámbito de la justicia y de los asuntos de interior.

Se han indicado las deficiencias del Acuerdo de Schengen y de su Convenio de Aplicación y, lo que constituye lo más grave, fuera de métodos propiamente comunitarios, dejando al margen del proceso normativo a las instituciones comunitarias, acudiendo a la cooperación intergubernamental para el logro de un objetivo, la libre circulación de personas, que constituye uno de los pilares básicos del sistema comunitario .

## **EL SISTEMA DE INFORMACION SCHENGEN ( S.I.S.)**

### **Naturaleza y Funciones. Estructura**

Este fichero “contrapunto necesario a la supresión de los controles en las fronteras”, constituyó el tema central de los debates del acta adicional.

Considerado como un gran riesgo de atentado a las libertades individuales, almacenará globalmente 800.000 señalamientos de personas buscadas y 6.000.000 de objetos<sup>11</sup>.

Aparece regulado en el **TITULO IV** del Convenio de Aplicación, que aparece integrado por los siguientes **Capítulos**:

**Capítulo Primero: Creación de Sistema de Información Schengen.**

**Capítulo 2: Explotación y uso del Sistema de Información de Schengen.**

**Capítulo 3: Protección de los datos de carácter personal y seguridad de los datos en el marco del Sistema de Información de Schengen.**

**Capítulo 4: Reparto de los costes del Sistema de Información de Schengen.**

El art. 92 establece la creación del referido sistema de información<sup>12</sup>, articulado en torno a una doble estructura organizativa:

- *Parte Nacional del S.I.S.*. Cada Parte contratante creará y mantendrá, por sus cuenta y riesgo, su parte nacional. No obstante, los Estados parte en el refe-

■ 11 Cfr. *NEEL, B., L'Europe sans frontières intérieures: l'Accord de Schengen*, Actualité juridique. Droit Administratif, 1991, núm. 10, p. 664.

■ 12 En la elaboración y gestión del S.I.S. han participado tres poderosas empresas de electrónica, “Bull”, “Siemens” y la “Sociedad de Servicios Informáticos francesa (SEMA)”.

rido Convenio no podrán actuar independientemente, estando sometidos a un doble condicionamiento:

a) Los ficheros de las Parte Nacional de todos los Estados miembros deberán ser idénticos. Para ello el propio Convenio establece que será la unidad de apoyo técnico la que deberá proceder a tal unificación.

b) Cada Parte Contratante deberá ajustarse, al elaborar su parte nacional, a los protocolos establecidos en común por las Partes contratantes. Especificaciones técnicas que, como indica el propio art. 93 en su párrafo 2, servirán al objetivo de permitir una transmisión rápida y eficaz de los datos. Ahora bien, cabe también preguntarse, ¿y una transmisión segura?. Con posterioridad intentaremos dar respuesta a esta cuestión. Sirva ahora meramente indicarla.

- *Unidad de Apoyo Técnico.* Será creada y mantenida por las Partes en común. Este fichero estará instalado en Estrasburgo, y la responsabilidad sobre el mismo corresponderá a la República Francesa. Tal y como establece el propio Convenio en su **art. 92.3** dicha unidad de apoyo técnico comprenderá un fichero de datos que garantizará la identidad de los ficheros de datos de las Partes nacionales. Se erige así esta unidad de apoyo técnico en elemento unificador de los datos incluidos en el propio Sistema, evitando de esta manera una desmesurada inclusión de datos personales que no respondan a necesidades reales.

Sirve también a esta criterio delimitador y restrictivo el hecho de que, según se desprende del artículo que venimos estudiando, sólo se incluirán en el fichero de datos de la unidad de apoyo técnico las descripciones de personas y objetos, siempre que las referidas descripciones afectan a todas las Partes Contratantes. Se trata con ello de evitar un descontrol de las autoridades nacionales en los señalamientos, que escapen a un verdadero interés unitario del Grupo.

Por último y respecto a esa Unidad de Apoyo de Técnico, se establece una restricción **ratione materiae**: no se incluirán otros datos que los mencionados en el presente apartado y en el apartado 2 del artículo 113<sup>13</sup>.

■ 13 Dicho artículo, en su párrafo 2, establece:

**“ 2. Los datos suprimidos se conservarán un año más en la unidad de apoyo técnico. Durante dicho período sólo podrán consultarse para comprobar a posteriori su exactitud y la licitud de su integración. Después deberán ser destruidos”.**

Resulta sorprendente lo que establece este párrafo. La conservación de los referidos datos sólo se efectuará por razones técnicas, y siempre a posteriori. Así pues unos datos incorrectos, erróneos o excesivos habrán desplegado sus nocivos y peligrosos efectos durante su inclusión en el fichero de datos, sin que, y según se desprendería del precitado párrafo, nadie se haya cuestionado o haya reparado en tales peligros. Se consagra una especie de **“ enjuague moral”** para lamentarse a posteriori de lo incorrecto, innecesario a abusivo del uso de determinados datos. Reiteramos, esto resulta cuanto menos sorprendente.

Este Sistema, mediante un procedimiento de consulta automatizado, permitirá que las Autoridades designadas por las Partes Contratantes<sup>14</sup>, dispongan de descripciones de personas y de objetos, en el territorio de cada uno de los Estados<sup>15</sup>. Dichas descripciones sólo figurarán siempre y cuando las mismas afecten a todas las Partes Contratantes. Este criterio “restrictivo”, digno de ser indicado, impedirá que mal entendidas necesidades o intereses particulares de alguno/os Estado/s Miembro/s ponga en peligro la función y el funcionamiento uniforme y unificado del sistema.

### **“ La salvaguarda del orden y la seguridad públicos “.**

El S.I.S. tiene como finalidad, de acuerdo a lo preceptuado en el **art. 93.**, **preservar el orden y la seguridad públicos, incluida la seguridad del Estado.**

Constituye esta finalidad, junto a la consecución de un espacio común interior, la piedra angular en torno a la cual se articula todo el Convenio. Se erige no sólo como criterio u objetivo a conseguir, sino también como fundamental argumento para la realización de las políticas que se consagran en el Convenio.

Este concepto genérico, de difíciles e imprecisos contornos, nos remite no obstante a un planteamiento excesivamente individualista que rememora los intereses particulares de los Estados, en contra del proyecto común que quiere llevarse a efecto con el Convenio. Se evidencia así que los Estados nacionales, se muestran reacios, o al menos incómodos, con una eventual transferencia de su

- 14 Respecto a la determinación de las autoridades competentes, conviene remitirse a lo establecido en el **art. 101** donde se establece la enumeración de aquéllas a las que se reconoce los “derechos” de acceso y consulta a los datos integrados en el Sistema de Información de Schengen.

Dicho artículo señala:

“ **El acceso a los datos...., así como el derecho de consultarlos directamente estará reservado exclusivamente a las autoridades competentes para:**

**a. los controles fronterizos**

**b. las demás comprobaciones de policía y de aduanas realizadas dentro del país, así como la coordinación de las mismas.”** Asimismo se reconoce tales facultades, acceso y consulta, “ **a las autoridades competentes para la expedición de visados, ... autoridades centrales competentes para el examen de las solicitudes de visado y por las autoridades competentes para la expedición de permisos de residencia y para la administración de extranjeros...**”

Será Cada Parte Contratante la que facilitará al Comité Ejecutivo la lista de las referidas “ autoridades competentes”.

Al respecto cabe hacer dos breves consideraciones:

1. La determinación de dichas autoridades se hace de manera genérica, en consideración a la tarea a desarrollar. Esta generalidad supone un evidente riesgo de ampliación cuantitativa de aquellas personas o entidades que tendrán acceso a los datos, con el evidente riesgo de peligro para la intimidad de los ciudadanos. Máxime cuando no se establece ningún control para tal determinación.

2. Resulta sorprendente la exclusión de las autoridades judiciales de la enumeración señalada. Parece que sólo las autoridades policiales y administrativas poseen tales facultades. Este “olvido” supone un manifestación de la consolidación de esta “ **Europa policial** “, que parece va perfilándose.

- 15 Cfr. *NEEL, B., L' Europe sans frontières intérieures: l'Accord de Schengen*, cit., p. 665.

soberanía, que se manifestaría en la progresiva pérdida de control sobre su espacio geográfico, y más concretamente del control de sus fronteras.

Surge de nuevo ese fantasma que se ha manifestado en todo el proceso de lo que se ha denominado "construcción europea". Éste no es más que las reticencias nacionales a un verdadero proceso de integración, de llevar a efecto unos objetivos y conseguir unos resultados comunes, al margen de malentendidos nacionalismos.

Se impone por lo tanto, y llegados a este punto, el proceder a una delimitación de este concepto. Como venimos indicando el Convenio no procede a esta delimitación, erigiéndose en lo que la ciencia jurídica denomina como "concepto jurídico indeterminado".

Como señala el pfsr. Martín-Retortillo y Baquer " el "orden público" en cuanto límite de derechos y libertades- con todas las técnicas de potenciación y respeto - está claro que lo que se formula desde la perspectiva de los límites, habrá de ser, por supuesto, objeto de interpretación restrictiva" <sup>16</sup>.

La seguridad a que se hace referencia no es la del derecho administrativo o laboral que se definen como la tranquilidad o la ausencia de accidentes, nociones todas ellas clásicas. El concepto utilizado esta más próximo a la seguridad militar o de las alianzas diplomáticas. Tiene un aire guerrero. Guerra contra los traficantes de drogas, después guerra contra los terroristas, combates que se entremezclan cuando los terroristas son asimilados a los delincuentes comunes y cuando los traficantes devienen " narco-terroristas ". Guerra contra la inmigración clandestina, en la que pueden meterse unos y otros, cuya estrategia es ahora definida en estrecha relación con las medidas de prevención y de represión de la criminalidad. El concepto de seguridad interior es así el fruto de una " evolución globalizante ", de una " ideología de la amenaza del Sur " y de una labor de profesionales tendente a " despolitizar y burocratizar cuestiones sensibles como el terrorismo". <sup>17</sup>

Será necesario recurrir a textos de derecho comparado para proceder a la delimitación de este concepto.

Resulta interesante, en torno a la concreción del concepto de seguridad pública, tener en consideración lo señalado por el Tribunal Europeo de Derechos

■ 16 Cfr. MARTÍN-RETORTILLO Y BAQUER, L., *Bajo el signo de la Constitución (Estudios de Derecho Público)*, Instituto de Estudios de Administración Local, Madrid, 1983, pp.407-440.

■ 17 Cfr. MASSÉ, M., *L 'espace Schengen. II. - Développements de l'entraide répressive internationale*, en *Revue de Science Criminelle et Droit Pénal Comparé*, 4, oct.-déc. 1992, p. 801.

Humanos, caso Klass y otros, sentencia de 6 de septiembre de 1978, serie A, núm 28, donde señala que “ el poder de vigilar en secreto a los ciudadanos no es tolerable según el convenio más que en la medida estrictamente necesaria para la salvaguarda de las instituciones democráticas” 18.

Por su parte el Consejo de Europa, en la Memoria Explicativa, número 56, del Convenio para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal establece que “ la noción de seguridad del Estado deberá entenderse en el sentido tradicional de protección de la soberanía nacional contra amenazas internas o externas, incluida la protección de las relaciones internacionales del Estado “ 19.

Las Comunidades Europeas, en una regulación más parca, consideran como tal “ la protección de la soberanía nacional contra amenazas internas y externas “ 20.

### Categorías de Datos. Problemática.

La categoría de los datos que se incluirán en el Sistema de Información de Schengen se establece de acuerdo a dos criterios:

- 18 Vid. sobre ello: **Tribunal Europeo de Derechos Humanos: 25 años de Jurisprudencia 1959-1983**, Cortes Generales, Madrid, 1981, pp. 469-485.
- 19 Vid. sobre ello: **Protección de datos. Convenio del Consejo de Europa de 1981**, Servicio Central de Publicaciones. Presidencia del Gobierno, Madrid, 1983, p. 36.
- 20 Vid. **Propuesta modificada de Directiva del Consejo, de 15 de octubre de 1992, 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**, COM (92) 422 final-SYN 287.

Conforme a los arts. 48.3, 56.1 y 66 del TCEE los Estados Miembros están facultados para introducir limitaciones en la libre circulación de trabajadores y el derecho de establecimiento, siempre que dichas limitaciones estén justificadas por motivos de orden público y/o seguridad pública. Para evitar que los Estados Miembros dieran una interpretación excesivamente amplia y divergente el Consejo dictó una Directiva (Directiva 64/221), que prevé la coordinación de las medidas vigentes para los extranjeros.

Los Estados Miembros no pueden desviarse de las normas comunitarias por motivos de orden público y/o de seguridad pública, si con las medidas limitativas de hecho se persiguen objetivos económicos, o si las medidas no se basan exclusivamente en el comportamiento personal del interesado. En consecuencia, las condenas criminales no pueden ser motivo, sin más, sino que también debe tenerse en cuenta el número y la gravedad de los delitos cometidos y sus consiguientes penas.

El Tribunal de Justicia de las Comunidades Europeas ha interpretado esta Directiva en una extensa e interesantísima jurisprudencia. En caso de expulsión de ciudadanos de otros Estados Miembros no deben influir las consideraciones preventivas generales (Asunto 67/74, *Bonsignore c. Oberstadtdirektor der Stadt Köln*, Recueil 1975, p. 297). Debe tratarse de una amenaza real y deben tenerse en cuenta los derechos humanos y las libertades del Convenio (Asunto 36/75, *Rutilli c. Ministerio del Interior*, Recueil 1975, p. 1219). Según el Tribunal sólo puede

hablarse de una alteración del orden público cuando se trata de una amenaza real y suficientemente grave que afecta a un interés fundamental de la sociedad (Asunto 30/77, *Regina c. Boucherau*, Recueil 1977, p. 2203). Cfr. *BRINKSHORST, L. J., Líneas Básicas del Derecho Europeo*, Editorial Praxis, Barcelona, 1986, p. 133.

a. Categorías de datos aportados por cada una de las Partes Contratantes (ratione personae).

b. Dichos datos deben ser necesarios para los fines señalados en los artículos 95 a 100 (ratione materiae) <sup>21</sup>.

Respecto a la necesidad de la introducción de los datos en el Sistema, será cada Parte Contratante la que determinará si la importancia del caso justifica la introducción de la descripción. Se deja por tanto a cada Estado la facultad absoluta de proceder a esa ponderación. Ello es coherente con el carácter proteccionista para los intereses de los Estados que consagra el Convenio, así como con las facultades que los Estados mantienen en orden a la determinación de su política de seguridad y de orden público. Lo que no se acierta a comprender es como se conseguirá alcanzar esa "unidad" que el Convenio pretende, si se mantienen esos amplios márgenes de autonomía.

Además como indicamos anteriormente sólo se introducirán aquellas descripciones que afecten a todas las Partes Contratantes, por lo cual deberá procederse a una clara delimitación de cuando nos encontramos ante esa "afección común".

Para arrojar más incertidumbre en esa diatriba - intereses nacionales-consecución objetivos comunes -, el propio Convenio concede la facultad a cualquiera de las Partes Contratantes de añadir posteriormente a la introducción de una descripción una indicación destinada a que la ejecución de la medida pertinente no se realice en su territorio<sup>22</sup>.

La categoría de los datos que se introducirán en el S.I.S. aparecen indicados en el párrafo 2 del artículo 94, si bien su desarrollo pormenorizado se efectúa en los artículos siguientes ( art. 95 - 100 ).

Dichas categorías de datos son:

**a. personas descritas.**

■ 21 Artículo 94 Convenio de Aplicación.

■ 22 Art. 93.4

Dicha indicación se introducirá cuando se estima que la referida inscripción no es compatible con el Derecho nacional, obligaciones internacionales o intereses nacionales esenciales de la Parte Contratante.

El Propio Convenio manifiesta así la falta de coordinación que existe entre los Estados Miembros en orden a la aproximación y unificación tanto de sus políticas en materia de seguridad, como en sus "productos legislativos".

Tal indicación restrictiva sólo podrá llevarse a efecto cuando la identificación se haya realizado de conformidad con los artículos 95, 97 ó 99. A saber: **Personas buscadas para su detención a efectos de extradición; personas desaparecidas o personas que, en interés de su propia protección o para la prevención de amenazas, deban ser puestas a salvo provisionalmente; personas o vehículos a efectos de vigilancia discreta o control específico.**

## b. objetos y vehículos.

Con referencia a las personas, el Convenio permite la introducción de todo un elenco de datos personales, en una enumeración excesivamente prolija, y que en algunos supuestos pueden presentar evidentes problemas para la intimidad de los individuos afectados. Dichos datos son: nombre y apellidos; alias en su caso, que se registrarán por separado; rasgos físicos particulares, objetivos e inalterables; primera letra del segundo nombre; fecha y lugar de nacimiento; sexo; nacionalidad; indicación de que el interesado va armado o es violento; el motivo de la inscripción; y la conducta a observar.

No obstante, no podrán registrarse sin limitación alguna datos sobre los interesados. El límite se encuentra en los denominados "datos sensibles", a los que el propio Convenio hace referencia por remisión al art. 6 del Convenio 108 del Consejo de Europa para la protección de las personas en lo referente al tratamiento automatizado de los datos de carácter personal<sup>23</sup>.

El registro de las condenas criminales anteriores no se incluye, puesto que no figuran en la proposición primera del art. 6 del Convenio 108 y además condicionan algunas de las situaciones de las personas buscadas ( en especial es supuesto contemplado en el art. 96 )<sup>24</sup>

■ **23 El art. 6 del Convenio 108 del Consejo de Europa establece:**

**" Los datos de carácter personal que revelaren el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán ser elaborados automáticamente a menos que el Derecho interno previera las oportunas garantías. La misma regla se aplicará a los datos de carácter personal referentes a condenas criminales".** Vid. sobre ello: **Protección de datos. Convenio del Consejo de Europa**, cit...

Establece así el Convenio la prohibición del tratamiento automatizado de esta clase de datos, en función de las potencialidades lesivas que presentan para los derechos e intereses de los individuos. Discrepamos en este punto de la opinión manifestada por Manuel Heredero ( **La protección de datos personales en manos de la policía: reflexiones sobre el Convenio de Schengen**, en la obra colectiva **" La protección de los datos personales. Regulación internacional de la seguridad informática "**, Monografies i Documents, 8, Centre d'Investigació de la Comunicació i Universitat Pompeu Fabra, Generalitat de Catalunya, Barcelona, 1993, p. 38 ) en orden a que el Convenio 108 no prohíbe el tratamiento de estas clase datos, sino que lo condiciona a la adopción en el Derecho interno de unas garantías apropiadas. Estimamos que lo que el precitado Convenio establece es la prohibición de dicho tratamiento con carácter general, permitiendo algunas excepciones a esta regla en virtud de la naturaleza protectora de las medidas que se arbitren en el Derecho interno. Lo general, por lo tanto, es la prohibición, y no la excepción. Como señala el propio Consejo de Europa la lista que contiene el artículo 6 no deberá considerarse exhaustiva. El grado de sensibilidad de los datos dependerá del contexto jurídico y sociológico del respectivo país.

Por su parte, la Comunidad Europea en el **art. 8 de la Propuesta modificada de Directiva relativa a la protección de las personas física en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos** establece:

**" Los Estados miembros prohibirán el tratamiento de datos que revelen el origen racial y étnico, la opinión política, las convicciones religiosas, filosóficas o morales, la afiliación sindical, así como las informaciones relacionadas con la salud y la vida sexual"**.

Como establece la propia Propuesta Modificada de este apartado se deduce que, por regla general, el tratamiento automatizado de datos especiales ( sensibles ) está prohibido.

Vid sobre ello: **Propuesta modificada...**, cit..

En España la **L.O.R.T.A.D.** establece también en su **art. 7**, una protección reforzada para este tipo de datos, que enumera bajo la denominación genérica de "datos especialmente protegidos".

■ **24 Cfr. HEREDERO HIGUERAS, M., La protección de datos personales en manos de la policía: reflexiones sobre el Convenio de Schengen**, en la obra colectiva **La Protección de los datos personales. Regulación Internacional de la seguridad informática**, Monografies i Documents, núm. 8, Centre d'Investigació y de la Comunicació i Universitat Pompeu Fabra, Generalitat de Catalunya, Barcelona, 1993.

Conviene detenerse brevemente en uno de los supuestos recogidos en la enumeración que acabamos de indicar. Se trata de “ **los rasgos físicos particulares, objetivos e inalterables** “. La no determinación de que deba entenderse por tales rasgos constituye un supuesto de evidente indefinición e inseguridad. La inclusión dentro de tal concepto de datos como el color de la piel o el origen étnico, podría dar lugar a una peligrosa antinomia, al vulnerar la prohibición establecida en el propio Convenio en orden a la no inclusión en el Sistema Informático de datos sensibles.

Estimamos, que lo que se establece es la posibilidad de introducir datos pertenecientes a la referida categoría, siempre y cuando aquéllos no tengan la naturaleza de sensibles. Sería una determinación residual por exclusión, en la cual entrarían supuestos tales como cicatrices, minusvalías físicas, etc... Obviamente, otras interpretaciones pueden darse a esta problemática, nosotros indicamos la que estimamos más acorde a lo que parece derivarse del propio precepto y del conjunto del Convenio.

Las categorías de datos son ampliamente reguladas en los artículos 95 a 100, de acuerdo a los diferentes datos que son necesarios o se derivan del cumplimiento de los fines que se establecen en el Convenio. Pasemos a analizarlas.

**a. Datos relativos a personas buscadas para su detención a efectos de extradición.**<sup>25</sup> su introducción en el Sistema sólo se realizará cuando medie un requerimiento de la autoridad judicial competente para conocer de tal procedimiento.

Se conculca de esta manera la autonomía de las referidas autoridades judiciales en orden a la ordenación del procedimiento, por cuanto su requerimiento no surte un efecto automático, sino que se difiere a la “ aprobación “ de otras e indefinidas autoridades nacionales ( por no decir policiales ).

Podría parecer, que estas medidas constituyen una salvaguarda para la protección de los datos personales que se solicitan. Nada más lejos de la realidad. Si el Poder Judicial tiene encomendado en los Estados de Derecho la salvaguarda de los derechos e intereses de los ciudadanos, no se acierta a comprender como se le desposee de tales facultades, y se sustituye por un control de oportunidad o interés nacional, que responden a intereses ciertamente políticos y no jurídicos.

■ 25 Art. 95.

Junto a los datos personales que se integrarán en la descripción, el precepto establece que deberán aportarse una serie de información suplementaria, calificada como “esencial”, y que deberá ser simultánea a la descripción. Estas menciones formales, o más concretamente procedimentales son: autoridad que pide la detención; existencia de una orden de detención o de un documento que tenga la misma fuerza, o de una sentencia ejecutoria; carácter y calificación legal de la infracción; descripción de las circunstancias en que se cometió la infracción, incluidos el momento, el lugar y el grado de participación de la persona mencionada; en la medida de lo posible, las consecuencias de la infracción.

Nada se dice acerca de las garantías que deben incorporarse a esta transmisión de carácter técnico, que revestirá casi con toda probabilidad la forma de transmisión automática informatizada, y que además el propio Convenio exceptúa de las garantías referentes a la protección de los datos personales, según se desprende de lo señalado en los arts. 126 y 127.

No olvidemos que las referidas “menciones formales”, incorporarán una serie de datos personales, que por esta vía escaparán a las ya de por sí escasas garantías que presenta el Convenio.<sup>26</sup>

#### **b. Datos relativos a extranjeros que estén incluidos en la lista de no admisibles.**<sup>27</sup>

La introducción de los referidos datos se hará sobre la base de una descripción, que deberá atemperarse a los procedimientos legalmente establecidos para la adopción de las correspondientes decisiones de no admisión en el territorio nacional.<sup>28</sup>

En este supuesto, a diferencia del anterior, si parecen tener un efecto directo las decisiones adoptadas, cuya sola concurrencia posibilita la introducción de la descripción en el Sistema. Ahora bien, en este supuesto, no sólo serán

■ 26 Sobre esta materia, vid. **Convenio Europeo de Extradición, de 13 de diciembre de 1957**, así como su **Protocolo Adicional de 15 de octubre de 1975** y su **Segundo Protocolo Adicional de 17 de marzo de 1978**.

■ 27 **Art. 96**.

■ 28 No obstante el **art. 25** del Convenio de Aplicación establece la posibilidad de expedir, por una Parte Contratante, un permiso de residencia a un extranjero incluido en la lista de no admisible. Tal expedición sólo podrá tener lugar, como indica el precepto, por “motivos serios”, especialmente de carácter humanitario o derivados de obligaciones internacionales.

Esta expedición conllevará la retirada de la descripción del S.I.S.

Esta excepción implica una manifestación más de la falta de unidad entre los Estados Miembros, y la descoordinación que ello conllevará en el otorgamiento de los permisos de residencia.

La salvaguarda de la “autonomía” de los Estados se manifiesta como principal obstáculo para la consecución de una política común en este ámbito.

las decisiones adoptadas por las autoridades judiciales, sino también las realizadas por las autoridades administrativas; entiéndase por tales las que tienen encomendadas el control y la administración de extranjeros.

La determinación de esta categoría de personas suscita evidentes inquietudes. Los extranjeros señalados a efectos de no admisión, que son objeto de una negativa de entrada sobre el territorio de uno de los nueve Estados, pueden serlo porque tal decisión esté basada en la falta de presentación de uno de los documentos exigidos por la legislación nacional. Dicha prohibición se aplicará al conjunto del territorio común.

Esta decisión, como señala el profsr. **Julien-Laferriere**, aparte de suponer un atentado a la soberanía de los Estados, que son tributarios de decisiones adoptadas por autoridades extranjeras, revela una desproporción evidente entre el hecho imputable al extranjero y las consecuencias que se derivan de él<sup>29</sup>.

Dos son las razones que pueden justificar una decisión tal:

a. Amenaza para el orden público o la seguridad nacional, si bien aquí matizados por el peligro que pueda suponer la presencia de un extranjero sobre el territorio nacional. Respecto a la determinación de los conceptos de orden público y seguridad nacional sirva lo indicado anteriormente.

El artículo establece dos supuestos o categorías concretas, como señeras de los que debe entenderse por tal "amenaza":

1. Extranjero condenado por una infracción sancionada con pena privativa de libertad de un año como mínimo.

La discrecionalidad del supuesto, y su vulneración de los postulados de la seguridad jurídica, es evidente. Lo determinante es que la pena sea privativa de libertad, obviando otra serie de sanciones penales que, pese a que no incorporan tal privación, pueden considerarse también como graves y que merecen el reproche social. Pero quizás lo más polémico será el hecho de la aplicación extraterritorial de los efectos o consecuencias de una determinada ley penal nacional. La existencia en los diversos Estados Miembros de legislaciones penales diferentes, con tipificaciones legales, procedimientos y órganos jurisdiccionales diversos, complica aún más el esclarecimiento de este supuesto.

■ 29 Cfr. **JULIEN-LAFERRIERE, F.**, *L'Europe de Schengen: de la disparition des frontières aux transferts des contrôles (commentaire de la loi n° 91 - 737 du 30 juillet 1991 autorisant l'adhésion de la France à la Convention d'application de l'accord de Schengen)*, Actualité Législative Dalloz, n° 13, 1993, p. 129.

Pensemos en una infracción tipificada como delictiva en un Estado Miembro y sancionada de acuerdo a su peculiar procedimiento, pero que sin embargo no constituye tal categoría, de acuerdo a la legislación penal de otra Parte. Surge entonces la pregunta: ¿Podrá considerarse vinculado un Estado soberano, por decisiones adoptadas por otros Estados, también soberanos, y verse compelido a la adopción de determinadas acciones, que ni siquiera puede fiscalizar?. La respuesta práctica es la cierta vinculación, que llevará a que el extranjero incluido en tal "lista" no puede acceder al conjunto del territorio del "espacio Schengen". Nuevamente se revela la necesidad de proceder a una armonización de las legislaciones penales y administrativas de los Estados Miembros, que tanta incidencia tienen sobre los ciudadanos. La generalización que parece derivarse del Convenio es ciertamente peligrosa <sup>30</sup>.

2. Extranjero sobre el cual existan razones serias para creer que ha cometido hechos delictivos graves, o sobre el cual existan indicios reales de que piensa cometer tales hechos en el territorio de una Parte Contratante.

Nuevamente se vuelve a echar mano de conceptos jurídicos indeterminados, de estricta valoración subjetiva, y que por ello son difícilmente fiscalizables por las autoridades encargadas de su aplicación. Ello constituye un evidente peligro de vulneración de las garantías establecidas para las personas en los Estados Social y Democrático de Derecho.

Será por lo tanto preceptivo analizar la situación caso por caso, teniendo en cuenta las circunstancias particulares que concurren en un supuesto, para no establecer una generalización sancionatoria, por el simple hecho de proceder de determinados países, étnias o grupos sociales.

Parece desprenderse del texto, que serán las autoridades policiales, las que procederán a esa determinación, y obviamente lo harán de acuerdo a sus propios medios de investigación. Medios de investigación de naturaleza ciertamente represiva, en su consideración de lucha contra la delincuencia, pero que necesitará de un adecuado control, para evitar extralimitaciones amparándose en la salvaguarda de una mal entendida preservación del orden o la seguridad nacional.

■ 30 Respecto a la necesidad de unificación del Derecho Penal Europeo, cfr. RUIZ VADILLO, E., *¿ Que puede esperarse razonablemente de un Derecho Penal Europeo Comunitario ? (Consideraciones Generales)*, Actualidad Penal, nº 34, 1993, pp. 507 - 530. Mi agradecimiento a D. Juan José Medina Ariza, por la sugerencia y búsqueda de esta obra.

Cfr, también DIEZ SANCHEZ, J.J., *El Derecho Penal*

*Internacional (Ambito espacial de la ley penal)*, Colex, Madrid, 1990.

b. Extranjero que ha sido objeto de una medida previa de alejamiento, devolución o expulsión.

Se trata de la vulneración de las legislaciones nacionales en materia de entrada y/o residencia de extranjeros.

**c. Personas desaparecidas o personas que, en interés de su propia protección o para la prevención de amenazas, deban ser puestas a salvo provisionalmente.** <sup>31</sup>

Este precepto se introduce como medio para preservar la vida e integridad de las personas. Parece estar pensándose en la actividad de grupos terroristas u organizaciones criminales, cuya forma de actuación incluye fundamentalmente la amenaza, la extorsión, el chantaje; cuando no, y desgraciadamente, el asesinato.

La introducción de los datos tiene en este supuesto un carácter preventivo, de salvaguarda. El fin es posibilitar que las autoridades policiales comuniquen el lugar de residencia de dichas personas y ponerlas así a salvo. Cuando dichas personas se encuentren en tránsito, el objetivo consistirá en impedirles la prosecución del viaje, y evitar que se consuma un hecho atentatorio.

La coordinación de la policía, así como la rápida transmisión de la información, se revela fundamental en esta tarea.

Se hace un especial hincapié en la necesidad de protección de los menores y de aquellas personas que deban ser internadas por resolución de una autoridad competente. Se trata de sectores, cuyo riesgo de desprotección y desvalidamiento aumenta considerablemente, en función de sus peculiares circunstancias. Puede constituir éste un buen procedimiento para luchar contra una situación habitual en nuestros días: la desaparición de menores.

**d. Testigos, personas citadas para comparecer ante las autoridades judiciales en el marco de un procedimiento penal para responder sobre hechos por los cuales hayan sido objeto de diligencias, o personas a las que se deba notificar una sentencia represiva o un requerimiento para que se presente a fin de ser sometido a una pena privativa de libertad.** <sup>32</sup>

▪ 31 Art. 97

▪ 32 Art. 98

Esta larga enumeración recoge ciertos supuestos que pueden surgir en el marco de la cooperación y asistencia judicial en materia penal.<sup>33</sup>

La descripción, que se hará a instancias de las autoridades judiciales nacionales de los Estados Miembros, tendrá por objeto facilitar el lugar de residencia o el domicilio de las precitadas personas.

La inclusión de los datos referentes a personas a quienes se deba comunicar una sentencia represiva o que deban someterse a una pena privativa de libertad, parece constituir una primera fase del procedimiento general de extradición. La localización del sujeto, en un determinado territorio, permitirá solicitar a las autoridades nacionales competentes, con base en los referidos datos, su extradición para ser juzgado por los hechos que se le imputan o para cumplir la pena que previamente ha quebrantado.

**e. Personas o vehículos, a efectos de vigilancia discreta o de control específico.**<sup>34</sup>

Dos son los objetivos que justifican la introducción de los referidos datos:

**1. represión de infracciones penales y prevención de amenazas para la seguridad pública.** Tal actividad preventiva se basa no obstante, como ya señalamos al tratar de los datos referentes a extranjeros incluidos en lista de no admisibles, en datos no siempre constatados, sino en simples presunciones atentatorias contra las libertades individuales. Se utilizan así conceptos tan indeterminados como “**indicios reales que permitan presumir**” o “**apreciación global del interesado**”. Pero lo más delicado es la posibilidad de utilización de datos personales por la única causa de que el afectado haya cometido hechos delictivos anteriores, y se suponga que va a cometer en el futuro hechos de extrema gravedad. Esto constituye un supuesto de “estigmatización”, que implica un desbordamiento de los límites marcados por el principio de culpabilidad y responsabilidad penal.

**2. prevención de una amenaza grave que proceda del interesado, o de otras amenazas graves para la seguridad interior y exterior del Estado.** En este supuesto los riesgos se personalizan en la actuación del “interesado”, si bien, y coincidiendo con el anterior, vuelve a basarse en “indicios”. Ciertamente que la

■ 33 En materia de asistencia judicial penal, vid. Capítulo 2, Título III (Policía y Seguridad), arts. 48-53, del Convenio de Aplicación. Vid. también **Convenio Europeo sobre Asistencia Judicial en Materia Penal, de 20 de abril de 1959**, en **Normas Españolas de Derecho Penal Internacional**, Secretaría General Técnica, Centro de Publicaciones del Ministerio de Justicia, Madrid 1989.

■ 34 Art. 99

actividad policial debe basarse en una serie de investigaciones previas, de averiguaciones, pero ello no debe constituir “ título suficiente ” para la inclusión de determinados datos personales en el S.I.S.

#### **f. Objetos buscados con vistas a su encautación o como pruebas en un procedimiento penal.<sup>35</sup>**

Esta categoría de datos parece, en primera instancia, no incidir sobre la “ intimidad ” de los ciudadanos. No obstante, si se comprobara la existencia de la descripción de un objeto encontrado se procederá a contactar con la autoridad informadora a los efectos de adoptar determinadas medidas a seguir. Y es para la adopción de estas medidas, para lo que sorprendentemente se establece la posibilidad de transmitir datos personales.

Si se trata de datos relativos a objetos, que se buscan a los efectos precisados, no se entiende el porqué de la inclusión de datos personales. Estos sólo podrían introducirse si se procediera a su subsunción bajo alguna de las categorías que a los mismos hacen referencia<sup>36</sup>, y siempre que fueran estrictamente imprescindibles para la realización de las medidas a seguir. Nuevamente el Convenio vuelve a posibilitar un uso “ arbitrario ” de datos personales, cuya única salvaguarda reside en la referencia genérica a su adecuación “ con el presente Convenio ”.

Para concluir este recorrido por las principales características del Sistema de Información de Schengen, conviene hacer una breve referencia al criterio establecido para el reparto de los costes originados por la instalación, gestión y uso del Sistema Informático.

Regulado en el **art. 119**, se articula en torno a un doble criterio, emanación de la propia estructura funcional del Sistema:

a) Costes de la Unidad de Apoyo Técnico: los costes de instalación y uso de esta unidad se sufragarán en común por todas las Partes Contratantes. En dichos costes se incluirán los de las líneas de comunicación de las partes nacionales del Sistema con la unidad de apoyo técnico.

■ **35 Art. 100**

■ 36 Ello implicaría la necesidad de una doble descripción, producida por la concurrencia de sujeto y objeto en el mismo supuesto. De otra forma debería procederse a la modificación de la descripción, por referencia al sujeto de la actuación ilegal, dejando la descripción del objeto como elemento accesorio, material, de la misma. De igual forma que el **art. 107** permite la integración de descripciones referentes a personas, creemos que, **mutatis mutandi**, podría operarse una tal integración para este supuesto que estamos contemplando.

Como es notorio, no todos los países miembros tienen la misma capacidad y disponibilidad económica, y es por ello que el propio precepto establece un reparto de los costes mediante la atribución de unas determinadas cuotas a cada Parte Contratante. Dichas cuotas se establecerán de acuerdo a lo preceptuado en la Decisión del Consejo de las Comunidades Europeas de 24 de junio de 1984 relativa al sistema de recursos propios de las Comunidades<sup>37</sup>.

b) Costes de la Parte Nacional: serán sufragados individualmente por cada Parte Contratante. Ello es congruente con el uso exclusivo que cada Parte tiene sobre su Parte Nacional del S.I.S. <sup>38</sup>.

## PROTECCION DE LOS DATOS PERSONALES

Estructurado el Convenio en torno a la creación y eficacia del Sistema de Información de Schengen, es necesario por lo tanto articular un sistema de garantías para los eventuales afectados por la recogida, almacenamiento, tratamiento y transmisión de los datos personales.

La existencia de estas garantías se revelan como imprescindibles para la articulación de un tratamiento automatizado de los datos que responda a las exigencias de un Estado Social y Democrático de Derecho. Es precisamente la extensión, la delimitación de estas garantías la que señalará el punto de encuentro, de equilibrio, entre las necesidades de información de los órganos y autoridades estatales y un escrupuloso respeto a los derechos y libertades de los ciudadanos.

Y es por ello que la vulneración de las mismas, no sólo supone un ataque frontal a los intereses del concreto afectado, sino que menoscaba la propia estructura democrática del sistema, convirtiendo la actuación estatal en arbitraria, y ajena a la estricta observancia de los principios de legalidad, congruencia y oportunidad de actuación.

- 37 Tal cuota se determinará sobre la base de la tasa de cada Parte Contratante en la base imponible uniforme del impuesto sobre el valor añadido. Concretamente la letra c) del párrafo primero establece: " **la base imponible de un Estado miembro que deberá tomarse en cuenta, a los efectos de la presente Decisión, no podrá ser superior al 55 % de su P.N.B.** ".

La referencia a un texto de Derecho comunitario europeo evidencia esa dependencia y vinculación del Convenio respecto a la actividad normativa de los órganos comunitarios. Se manifiesta así nuevamente la naturaleza " comunitaria " de las disposiciones emanadas de esa " norma convencional internacional ".

Por su parte el art. 92.3 del Convenio de Aplicación señala: " **Las Partes Contratantes crearán y mantendrán por cuenta y riesgo de todas ellas, la unidad de apoyo técnico del Sistema de Información de Schengen** ".

- 38 El art. 92.2 del convenio de Aplicación establece: " **Cada Parte Contratante creará y mantendrá, por su cuenta y riesgo, su parte nacional del Sistema de Información de Schengen ...** ".

El derecho a la intimidad, del que el ciudadano es titular, aunque sólo en una concepción teórica, se ve despojado de las garantías que le son propias, vaciándolo de contenido y quedando relegado a una mera declaración grandilocuente sin ninguna virtualidad práctica. El derecho debe ser tal, no sólo por que se tenga como titular, sino porque, llegado el caso, pueda ejercitarse.

La forma en que el Convenio aborda esta materia es ciertamente insatisfactoria. Los textos, extremadamente numerosos, consagrados a la protección de los datos adolecen de una manera manifiesta de haber sido introducidos tardíamente y aparecen dispersos a lo largo de la Convención sin otras directrices más que una serie de reiteraciones y una serie de exclusiones en cascada. Pese a ello se han alzado voces, tanto en la doctrina española como extranjera, defendiendo el acierto de tal regulación<sup>39</sup>. No obstante la opinión mayoritaria se muestra ciertamente crítica y preocupada. No es para menos, tal y como iremos viendo en la disección que del Convenio pretendemos hacer en las reflexiones siguientes.

### **1. Marco Jurídico Regulador: Derecho aplicable**

La protección de los datos personales aparece, como ya señalamos, dispersa a lo largo del texto. Tres momentos pueden apreciarse en dicha regulación:

- a. Protección de los datos personales generados e intercambiados en el examen de una solicitud de asilo<sup>40</sup>.
- b. Protección de los datos de carácter personal y seguridad de los datos en el marco del Sistema de Información de Schengen<sup>41</sup>.
- c. Protección de los datos de carácter personal<sup>42</sup>.

Los autores del Convenio han consagrado así una artificiosa diferenciación en la protección de los datos. No se acierta a comprender como las mismas categorías de datos, y por lo tanto, sujetas a los mismos riesgos, son trata-

■ 39 Cfr. entre otros, *HEREDERO HIGUERAS, M., La protección de los datos personales en manos de la policía*, cit..., y *GAUTIER, Y., La coopération policière: les perspectives ouvertes par le traité sur l'Union européenne du 7 février 1992*, en *Europe*, 3 année - N° 4, Avril 1993.

■ 40 **Art. 38** del Convenio de Aplicación.

■ 41 **Capítulo 3 del Título IV** del Convenio de Aplicación.

■ 42 **Título VI** del Convenio de Aplicación.

das de manera tan diversa, llegando incluso a excepcionarse el régimen de garantías<sup>43</sup>. Como ya vimos al tratar sobre la naturaleza jurídica del Convenio, el derecho aplicable se manifiesta confuso, obedeciendo a una superposición<sup>44</sup> de órdenes normativos, algunos de los cuales no presentan ni una conexión directa, ni aún clara, con la regulación establecida en el Convenio.

La gran autonomía, por no decir casi la absoluta primacía, que se otorga a las legislaciones nacionales de las Partes Contratantes para la articulación de las medidas protectoras sobre los datos personales automatizados, evidencia la naturaleza restrictiva de la unificación<sup>45</sup> que se pretende llevar a efecto.

Surge de nuevo una contraposición dialéctica: Vamos a construir un proyecto común, pero vamos a hacerlo como a cada uno convenga o según nuestros propios criterios. La incongruencia es manifiesta.

- 43 Así se observa en el **CAPÍTULO VI** titulado “**PROTECCION DE LOS DATOS DE CARACTER PERSONAL**”, que incorpora una derogación casi absoluta de las garantías. Excluye de su ámbito de aplicación la mayor parte de las políticas del Convenio para las cuales se revela imprescindible el tratamiento automatizado de los datos personales. Y lo efectúa en aquellos sectores que carecen de medidas protectoras en la parte del Convenio que los regula, y para los cuales parecería estar pensada la genérica protección de los datos que se articula en este Capítulo.

Así el **Art. 126** establece, concretamente en su **apartado 3**, la necesidad de aplicación de una serie de principios de protección por lo que se refiere al tratamiento de datos personales transmitidos en aplicación del presente Convenio. Así, debe determinarse la finalidad de los datos, al igual que las personas que puedan utilizarlos; los datos deberán ser exactos, etc..

Tras proclamar estos principios, el propio artículo consagra esa excepción generalizada, esa derogación fáctica de las garantías. Y así señala: “ **4. El presente artículo no se aplicará a la transmisión de datos prevista en el Capítulo 7 del Título II y en el Título IV. El apartado 3 no se aplicará a la transmisión de datos prevista en los Capítulos 2, 3, 4 y 5 del Título III** “. Tras esta remisión se incluyen, y por lo tanto se excepcionan: Examen de las solicitudes de asilo; Sistema de Información de Schengen; Asistencia Judicial en materia penal;

Aplicación del principio non bis in idem; Extradición; Transmisión de la ejecución de sentencias penales.

Como observamos, a casi nada se aplica este artículo. Queda vacío, sin ninguna eficacia práctica. Notable argucia de los autores del Convenio.

En iguales términos, y con las mismas excepciones, debemos manifestarnos respecto a los **Arts. 127** ( que extiende las medidas del artículo anterior a datos procedentes de ficheros no automatizados o introducidos en un fichero no automatizado. Desgraciadamente el acierto de este precepto queda obviado por las referidas excepciones de aplicación ) y **128** ( que difiere la transmisión de los datos hasta que las Partes contratantes afectadas encarguen a una autoridad de control nacional que ejerza un control independiente sobre el cumplimiento de los dispuesto en los arts. 126 y 127. Lo señalado en este artículo, a diferencia de los anteriores, sí se aplica al sistema de Información de Schengen ).

Se consagra así que a iguales garantías, iguales excepciones.

Lo realmente relevante de este régimen de excepciones, y ahí estriba su potencialidad lesiva, es que no se limita a los principios de protección de los datos, sino que se extiende a los mecanismos de control independientes, ajenos a los concretos intereses públicos o privados, y que constituyen el mecanismo de la defensa de los intereses y de la salvaguarda de los derechos de los ciudadanos.

- 44 Como caso paradigmático de esta superposición, puede señalarse el contemplado en el **art. 115.1**, cuando regula la creación de la autoridad de control encargada del control de la unidad de apoyo del S.I.S. : “.. **El control se ejercerá de conformidad con lo dispuesto en el presente Convenio, en el Convenio del Consejo de Europa de 28 de enero de 1981..., teniendo en cuenta la Recomendación R (85) de 17 de septiembre del Comité de Ministros del Consejo de Europa... y con arreglo al Derecho nacional de la Parte Contratante responsable de la unidad de apoyo técnico** “.
- 45 La unificación, más que en el sentido positivo de homogeneización de criterios, debe entenderse en el sentido de una auténtica *reformatio in peius*.

Por otro lado, y como por todos es sabido, la protección de los datos personales es objeto de diferentes enfoques en los Estados Miembros; diversidad resultante, por una parte, de la carencia de legislación de algunos Estados miembros, y por otra, del diferente contenido de la legislación existente en aquellos que la poseen. Estas normas internas, aunque presentan un objeto idéntico, la protección de las personas afectadas adopta diferentes soluciones por la gran variedad de opciones posibles para asegurar tal protección. Además los progresos técnicos pueden llevar a los Estados a adoptar diferentes pautas de actuación y acentuar, si cabe aún más, las diferencias.

No olvidemos que el Convenio sólo exige una armonización de las normas técnicas del Sistema Informático, tal y como se desprende del **párrafo 2 del art. 92**. Para la protección de los datos los autores del Convenio creen que basta con una genérica remisión a los preceptos que en la materia ha elaborado el Consejo de Europa. Concretamente la **Convención 108 para la protección de las personas respecto al tratamiento automatizado de los datos de carácter personal de 28 de enero de 1981**, y la **Recomendación N<sup>o</sup> R (87) del Comité de Ministros del Consejo de Europa a los Estados Miembros tendente a reglamentar la utilización de datos personales en el sector de la policía**.

Tres son los ordenes normativos que confluyen para la regulación de los datos personales en el Convenio, y que contribuyen a dar la imagen de “ inseguridad normativa ” que venimos manifestando.

#### **A. Derecho Nacional de las Partes Contratantes.**

Las legislaciones nacionales relativas al tratamiento de datos personales deben tener por objeto asegurar el respeto de los derechos y libertades fundamentales, particularmente el derecho a la intimidad reconocido en el artículo 8 del Convenio Europeo para la Protección de los derechos fundamentales, así como en los principios generales del derecho comunitario<sup>46</sup>.

La diferencia entre los niveles de protección de los derechos y libertades de las personas, y en concreto de la intimidad, garantizados en los Estados Miembros se debe a la diferencia existente entre las disposiciones legales, reglamentarias y administrativas existentes en los referidos Estados.

Esta disparidad supone un serio obstáculo a la realización de esa finalidad protectora perseguida. Es por ello que se impone que el nivel de protección sea equivalente en todos los Estados Miembros. Pero ese objetivo no puede

■ 46 Cfr. *SANCHEZ BRAVO, A., La Interpretación en el Derecho Comunitario Europeo. Relevancia de los Principios Generales del Derecho*, en curso de publicación en el Boletín de la Facultad de Derecho de la UNED.

lograrse mediante la simple actuación de los Estados Miembros, de ahí la necesidad de coordinar dichas legislaciones para que el flujo de datos sea regulado de forma coherente.

Para ello hubiera sido necesario que los Estados miembros se plantearan seriamente estos obstáculos y no hubieran obviado su regulación.

Como señalamos, la naturaleza “convencional” del Acuerdo se manifiesta en esa remisión casi constante a la necesaria actividad normativa estatal<sup>47</sup>.

Esta iniciativa nacional, que aparentemente parece loable por implicar el dotar a los Estados de un amplio margen para atemperar las exigencias del texto a su realidad política, social o cultural, presenta como contrapartida la diferente regulación nacional a la que antes aludimos, y todo ello fruto de una mal entendida salvaguarda de los “intereses nacionales”.

Pero esta disparidad no sólo supone un riesgo de inseguridad en la actuación estatal frente a los ciudadanos, sino que ya está suponiendo *de facto* una paralización del Convenio de Aplicación, una de cuyas causas fundamentales<sup>48</sup> es la ausencia en dos Estados Miembros (Italia y Grecia) de una norma

- 47 Sin ánimo de ser exhaustivos, indicaremos a continuación la materia concreta que se deja a la normación estatal, en el ámbito de la protección de los datos personales, con referencia al concreto precepto donde se recoge:  
El Derecho nacional de la parte informadora se aplicará a la descripción (art. 104.1); aplicación del derecho nacional a los datos introducidos en la parte nacional del S.I.S. (art. 104.2); ejecución de la medida pertinente solicitada de acuerdo al derecho nacional de la parte contratante que la ejecute (art. 104.3); el ejercicio del derecho de acceso se efectuará respetando el derecho nacional de la Parte ante la que se hubiere alegado (art. 109.1); la autoridad nacional de control se designará respetando el derecho nacional (art. 114.1); la petición de solicitud de control por la autoridad de control nacional se regulará por el derecho nacional (art.114.2); la determinación de la responsabilidad por daños causados con motivo de la explotación del fichero de la parte nacional del Sistema Informático se regirá por el derecho nacional (art. 1116.1).  
Muchas otras referencias podrían señalarse. Sirvan estas como indicativo de lo que venimos señalando. No debe olvidarse que esta remisión a las legislaciones nacionales internas no tiene como objeto el obligar a los Estados Miembros a observar sus propias normas internas sobre protección de datos, sino dejar en sus manos la resolución de los múltiples problemas que van a generarse. Problemas que seguramente tendrán unas soluciones diversas, e incluso contradictorias.
- 48 La entrada en vigor de los acuerdos de Schengen inicialmente estuvo prevista para enero de 1993, luego se retrasó a julio y posteriormente a diciembre. Tampoco ha sido cumplida la última fecha prevista del 1 de febrero de 1994. Carencias de orden presupuestario e informático parecen ser la causa de este retraso.  
Francia ha manifestado sus reticencias respecto a la efectiva puesta en práctica del Sistema de Información.  
Portugal, en fecha reciente, ha renunciado a ostentar la Presidencia del grupo de Schengen, debido tanto a dificultades presupuestarias como a las fricciones surgidas entre los Ministerios de Exteriores y de Interior. Vid. sobre ello ABC, Miércoles 16-2-94, Sevilla, p. 30.  
Respecto a España la primeras pruebas de interconexión del N.S.I.S. y C.S.I.S. tuvieron lugar en la segunda mitad del año 1992. La determinación y mantenimiento de los datos, que por parte española se integran en el S.I.S., así como la realización del N.S.I.S. español, están exigiendo un esfuerzo de adaptación muy importante por parte de los departamentos afectados. Esos esfuerzos han planteado dos esfuerzos inmediatos:  
1. La realización de un estudio sobre el diseño funcional y operacional del N.S.I.S. español. Esta actividad se está llevando a cabo mediante un grupo de trabajo, compuesto por la Dirección General de Política Interior, el Servicio de Informática de la Dirección General de la Policía y la Comisaría General de Documentación de la misma institución.  
2. La participación en los gastos comunes relacionados con el C.S.I.S. (asumidos por el Ministerio de Asuntos Exteriores) y la realización de importantes inversiones nacionales para la puesta en marcha del N.S.I.S., asumidas por el Ministerio del Interior. Vid. respecto a España: LAZARO MORENO, F., **El Acuerdo de Schengen y la libre circulación de personas en la CEE**, Cuadernos de Europa, nº 2, Diputación de Zaragoza (Comisión de Europa), Zaragoza, 1993.

interna reguladora de la protección de los datos personales.

En la lucha integración vs. autonomía nacional, esta última, por el momento gana la partida.

La propia estructura funcional del Sistema, con la existencia en cada Estado Miembro de una Parte Nacional del S.I.S., conectado con la Unidad Central, hace que sean los Estados los encargados de regular esa "unidad nacional"<sup>49</sup>.

Es la ubicación del fichero del sistema la que determina el criterio de atribución de competencia territorial.

Pero las referidas "unidades nacionales" no son independientes, sino que su relevancia y eficacia esta en función del papel central asignado a la Unidad Central, que le sirve como referente y justificación.

Los datos personales no sólo van a quedar integrados en los ficheros nacionales, sino que tras su integración en la Unidad Central, se posibilitará el acceso a los referidos datos a las autoridades policiales, administrativas y judiciales de los Estados Miembros.

Así pues este criterio "nacional" no es correcto. El Convenio olvida problemas que podrían presentarse, tales como un conflicto positivo o negativo de dos o más Estados Miembros en torno a la titularidad de determinados datos o a la competencia de sus autoridades para utilizarlos. Ello podría generar, en el fragor del conflicto, la eliminación de las garantías para los ciudadanos, al no

■ 49 Recientemente se ha conocido, que esa "excesiva" autonomía nacional, es la causante de la falta de operatividad del S.I.S. y por ende del Convenio.

Un problema en el lenguaje informático de los sistemas informáticos de los Estados Miembros, ha impedido así que el pasado día 1 de febrero fueran efectivas las medidas entorno a la libre circulación de personas y la eliminación de las fronteras interiores en el "espacio Schengen".

Se trabaja arduamente para readaptar el lenguaje de las computadoras y la velocidad de la información. Se ha formado lo que han denominado una "célula de crisis" integrada por cinco expertos - un español, un holandés, un alemán, un francés y un belga - que deberán "rediseñar" el lenguaje de las computadoras de cada país y el ordenador central.

Estos nuevos datos evidencian la improvisación de los autores del Convenio. Articulado el texto en torno a la efectividad del sistema Informático, resulta sorprendente como se ha incurrido en un error tan sorprendente, al no tener en consideración lo que debería haber sido el inexcusable punto de partida; a saber, la compatibilidad de los sistemas informáticos.

poder determinarse cual sea la legislación nacional protectora que deba aplicársele<sup>50</sup>.

Sirva indicar, y como conclusión, que la referencia a los ordenamientos jurídicos nacionales o internos como marco regulador de la protección de los datos personales, no se articula convenientemente en el texto. Más que aclarar lo que hace es complicar la búsqueda del verdadero criterio a seguir para la protección de la intimidad de las personas frente al tratamiento automatizado de sus datos personales.

### **B. Convenio 108 del Consejo de Europa, de 28 de Enero de 1981 sobre la protección de las personas en lo referente al tratamiento automatizado de los datos de carácter personal.**

La alusión a este Convenio es constante, aunque de una manera desordenada, y sin entrar a determinar claramente cual es el papel que le corresponde en la articulación de las medidas protectoras a adoptar.

Desde un punto de vista estrictamente lingüístico-sintáctico, observamos como el Convenio puede responder a una triple función:

**1. Función Delimitadora:** “...legislación aplicable... que *cumpla* los principios del Convenio del Consejo de Europa...” (Art. 38.12).

**2. Función Vinculante:** “El control se ejercerá *de conformidad* con lo dispuesto en... el Convenio del Consejo de Europa...” (Art. 115.1).

- 50 En este sentido resulta más correcta la regulación establecida por la Comisión de las Comunidades Europeas en la **Propuesta Modificada de Directiva...**, cit.... Recoge una pormenorizada regulación de cual va a ser la legislación nacional aplicable al tratamiento automatizado de los datos personales. Como a interconexión de ficheros nos estamos refiriendo, se fijan los criterios necesarios para determinar cual es la legislación nacional aplicable a los tratamientos que entren dentro del ámbito de la Directiva.

Ello responde a un doble objetivo:

1. Que el interesado carezca de protección, en particular debido a una elusión de responsabilidad.
2. Que un mismo tratamiento se vea sometido a la aplicación de varias legislaciones nacionales.

Concretamente su art. 4 establece:

“ 1. Los Estados miembros aplicarán las disposiciones nacionales adoptadas en aplicación de la presente Directiva a todos los tratamientos de datos personales:

(a) cuyo responsable esté establecido en su territorio o esté sometido a su jurisdicción;

(b) cuyo responsable no esté establecido en el territorio de la Comunidad, cuando dicho responsable utilice medios, automatizados o no, localizados en el territorio de dicho Estado miembro para el tratamiento de datos personales.

2. En el caso mencionado en la letra b) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, que se subrogará en los derechos y obligaciones del responsable.”

**3. Función Inspiradora:** “... un nivel de protección de los datos de carácter personal que sea al menos igual al resultante de los principios del Convenio del Consejo de Europa...” (Art.117.1);

“... un nivel de protección de los datos de carácter personal que sea al menos igual al que se desprende de los principios del Convenio del Consejo de Europa...” (Art. 126.1).

Este marasmo de significaciones nos remite a cuestionarnos cual es el verdadero valor de estas declaraciones; cual la importancia de una norma internacional ajena al Convenio, pero que constituye uno de sus referentes.

Estimamos que, al igual que sucede en la Comunidad Europea, al carecer los Estados miembros de una legislación unificada, uniforme sobre la materia, se pretende conseguir dicha homogeneización de manera indirecta. Y se pretende conseguir vinculándose al único instrumento de Derecho Internacional existente en este ámbito. Instrumento que, no obstante, no ha limitado esta disparidad, ya que por una parte permite elegir entre un gran número de opciones para la aplicación de los principios básicos que define y, por otro sólo ha sido ratificada por cuatro países miembros (Alemania, España, Francia y Luxemburgo).

Se observa como esa aparente vinculación, lo es sólo desde un punto de vista nominal o referencial, pero que en la práctica se muestra inoperante, tanto por las propias limitaciones del Convenio 108, como por la peculiar naturaleza y objetivos del Convenio Schengen.

Que duda cabe que este Convenio 108 habrá servido de referente<sup>51</sup> para la adopción de determinados principios reguladores. De ahí a afirmar que existe una vinculación directa va un abismo.<sup>52</sup>

Preocupados por salvaguardar su autonomía y su libertad de actuación, como iba a tolerarse una dependencia de una organización internacional, ajena

■ 51 Como también lo habrán sido, seguramente, principios recogidos en las legislaciones de los Estados Miembros.

■ 52 El Parlamento Europeo ha señalado recientemente:

“ Considera que no basta con declarar que una posible convención es conforme a las convenciones internacionales en vigor, sino que todos los Estados miembros están obligados a respetarlas, y que esto debe comprobarse antes de redactar el texto. “

Cfr. Resolución, de 22 de febrero de 1991, sobre la armonización de las políticas de acceso a los territorios de los Estados miembros de la CE, con vistas a la libre circulación de las personas (art. 8 del Tratado CEE) y la elaboración de una convención intergubernamental entre los doce Estados miembros de la Comunidad, D.O.C.E. Nº C 72/213 de 18.03.1991.

a los objetivos que persigue el Convenio Schengen, dotada de unos órganos y estructuras diferentes, y con unos objetivos diametralmente opuestos: en el Convenio 108 asegurar una esfera de protección uniforme para los ciudadanos frente al tratamiento automatizado de sus datos personales; en Schengen lograr una Europa policial fuerte, impermeable, para cuya consecución la transmisión y circulación de datos personales se revela como imprescindible.

Puede afirmarse que la apelación al Convenio 108 del Consejo de Europa, sirve como justificación para no profundizar en el tema de la protección de los datos personales. La alusión a otro texto normativo internacional parece ser suficiente, y se elude así el afrontar seria y adecuadamente una cuestión de capital importancia para los ciudadanos. Pero, como ya sabemos, no existe, en este campo, esa voluntad política seria y responsable.

### **C. Recomendación Nº R (87) 15 de 17 de septiembre de 1987 del Comité de Ministros del Consejo de Europa dirigida a regular el uso de los datos de carácter personal en el sector de la policía.**

La aparición de esta Recomendación en el texto del Convenio se produce en tres concretos momentos, pareciendo responder a una triple función, al menos tal y como se formula en el propio articulado:

1. Como **norma inspiradora** en la regulación del ejercicio del control que sobre la Unidad de Apoyo Técnico del S.I.S. corresponde ejercer a la Unidad de Control Común que crea el Convenio<sup>53</sup>.

2. Como **norma delimitadora** de los principios a los que debe atemperarse la transmisión de los datos de carácter personal transmitidos en aplicación del Título IV ( referente al S.I.S.), a más tardar en el momento de la entrada en vigor del Convenio Schengen<sup>54</sup>.

3. Como **norma vinculante** respecto a los principios que deben cumplir

- 53 “ Se creará una autoridad de control común encargada del control de la unidad de apoyo técnico del Sistema de Información de Schengen.... El control se ejercerá.... *teniendo en cuenta* la Recomendación R (87) 15 de 17 de septiembre de 1987 del Consejo de Europa dirigida a regular la utilización de datos de carácter personal en el sector de la policía...” ( Art. 115.1 ).
- 54 “ Por lo que se refiere al tratamiento de los datos de carácter personal que se transmitan en aplicación del presente Título, cada Parte Contratante adoptará a más tardar en el momento de la entrada en vigor del presente Convenio, las disposiciones nacionales necesarias para conseguir un nivel de protección de los datos de carácter personal... y respetando la Recomendación R (87) 15 de 17 de septiembre de 1987 del Comité de Ministros del Consejo de Europa...” ( Art. 117.1 ).

las Partes Contratantes en la transmisión de los datos personales necesarios para la cooperación policial constituida por el Convenio<sup>55</sup>.

Al igual que en el supuesto anterior la virtualidad práctica de esta Recomendación<sup>56</sup> es escasa. Si bien, debe indicarse que presenta más conexión con ciertas materias propias que regula el Convenio Schengen. La razón estriba en el hecho de que el Convenio hace referencia o regula determinadas actuaciones policiales, y por ello se ha creído conveniente la referencia a la Recomendación del Consejo de Europa como regulación específica de la protección de los datos generados o utilizados en el curso de actividades policiales. Sería un apelación al principio de primacía de la **lex specialis** sobre la **lex generalis**; teniendo en cuenta lo ya apuntado respecto al restringido papel que cumplen en el Convenio.

De lo expuesto no puede extraerse, como apresuradamente ya ha hecho algún autor<sup>57</sup>, una vinculación directa e inmediata; sólo por el hecho de que exista una coincidencia en la formulación de determinados principios o garantías.

Principios y/o garantías que deben recogerse, no por que se inspiren o por que se busque el respeto a un " ideal texto internacional ", sino por que son estrictamente necesarios, imprescindibles para la salvaguarda de los derechos de los ciudadanos, y fundamentalmente de su derecho a la intimidad.

El no haber recogido estos principios o garantías hubiera supuesto el colmo del despropósito.

## **2. Principios relativos a la protección de los datos personales.**

Los principios de protección de los datos personales deben aplicarse a todos los tratamientos de datos personales. Dichos principios tienen su expresión, por una parte, en las distintas obligaciones que incumben a los órganos o autoridades que efectúen tratamientos - obligaciones relativas, en particular, a la calidad de los datos, seguridad técnica, notificación a las autoridades de control,

- 55 " Por lo que se refiere a la transmisión de datos de carácter personal en aplicación del Capítulo 1 del Título III, las Partes Contratantes se comprometen,... a conseguir un nivel de protección de los datos de carácter personal **que cumpla** los principios de la Recomendación R (87) 15 de 17 de septiembre del Comité de Ministros del Consejo de Europa... " (Art. 129 ).
- 56 Esta Recomendación va dirigida a los Estados Miembros para que "adecuen" sus legislaciones a las pautas marcadas por el referido texto. El objeto de esta regulación aparece claramente explicitado: "... **la necesidad de conciliar el interés de la sociedad por la prevención y la represión de infracciones penales y el mantenimiento del orden público y, de otra, el interés del individuo y el derecho al respeto de su vida privada** " .
- 57 Cfr. *HEREDERO HIGUERAS, M., La protección de los datos personales en manos de la policía...*, cit... Asimismo *LAZPI- TA GUTURBAY, M., La protección de los datos personales en la Comunidad Europea*, Revista de Estudios Europeos, núm. 9, 1993, especialmente su nota 12.

fundamentos de los tratamientos - y por otra parte, en los derechos otorgados a las personas, cuyos datos serán objeto de tratamiento, de ser informados acerca de tales datos, de poder acceder a ellos, de solicitar su rectificación o incluso de oponerse a su tratamiento.

El articulado del Convenio manifiesta la alegación de una serie de principios de protección de los datos personales, lo cual no prejuzga una regulación o contenido satisfactorios de los referidos principios. Estos principios aparecen diseminados a lo largo de su articulado, en un intrincado laberinto de denominaciones y menciones. Incluso, un mismo principio se menciona de formas diversas, cuando realmente hace referencia a lo mismo.

Ha sido por lo tanto necesario acometer una labor de sistematización y de reconstrucción de ese " puzzle " normativo. Este desorden evidencia el carácter asistemático y de "avanzar como impulsos" que presenta la regulación de la protección de los datos personales. Ello no es más que la consecuencia de la introducción tardía de estas cuestiones en el texto del Convenio, y de haberlo hecho con escasa confianza respecto a su eficacia.

#### **A. Principio de Especificación de la Finalidad. Principio de Restricción de Uso.**

El objeto de la recogida de datos personales debe determinarse, esto es, la finalidad de la recogida y la utilización de los datos deberá definirse de la manera más concreta posible. Una definición o una descripción vagas del objeto del tratamiento no es acorde con este principio, que constituye un mecanismo de salvaguarda importante, impidiendo una desviación, abuso o un uso torticero de los datos personales.

Con referencia al Convenio, debe indicarse que este principio no se cumple, pese a que se hace alegación del mismo, en la primera aparición que hace en el texto.

Proclamado en el **apartado 5 del art. 38**, referente a las solicitudes de asilo, cuando se establece que los datos intercambiados únicamente podrán utilizarse para los fines previstos en el apartado 1, su determinación queda relegada a lo que establece el referido precepto<sup>58</sup>.

- 58 " 1. Cada Parte Contratante comunicará a toda otra Parte Contratante que lo solicite las informaciones que posea acerca de un solicitante de asilo y que sean necesarias para:
  - determinar la Parte Contratante responsable del examen de la solicitud de asilo;
  - el examen de la solicitud de asilo;
  - el cumplimiento de las obligaciones derivadas del presente Capítulo.
- 5. Los datos intercambiados únicamente podrán utilizarse para los fines previstos en el apartado 1... " ( Art. 38 ).

Precepto cuya amplitud es manifiestamente desorbitante, no sólo desde el punto de vista material - de sus contenidos -, sino desde el punto de vista subjetivo. Cualquiera Parte podrá "comunicar" a cualquier otra parte que lo solicite (ámbito subjetivo) las informaciones que posea acerca de.... y que sean necesarias para.... (ámbito material).

Como vemos los datos no sólo podrán utilizarse para el examen de una concreta solicitud de asilo, sino que también se posibilita un uso generalizado, y creemos que indiscriminado, amparándose en el cumplimiento genérico de las obligaciones del Capítulo; relativo a la responsabilidad del examen de las solicitudes de asilo.

Proclamado en el **art 32**<sup>59</sup> que cada Parte contratante examinará conforme a su derecho interno las solicitudes de asilo, ello implicará que será cada Estado miembro el que determinará unilateralmente que datos son necesarios, de acuerdo a su peculiar legislación, para un correcto examen de las solicitudes de asilo. Si a ello unimos el amplio elenco de datos<sup>60</sup> que podrán tratarse con este objeto, observamos como este principio se difumina y disuelve en ese marasmo de remisiones y vacíos normativos.

Iguales criterios se establecen en el **art. 102**<sup>61</sup> respecto a la determinación de la finalidad en el uso de las categorías de datos señalados en los arts 95 a 100. Lo ya apuntado anteriormente cuando estudiamos la formulación y

■ 59 " La Parte Contratante del examen de la solicitud de asilo lo llevará a cabo con arreglo a su Derecho nacional" ( Art. 32 )

■ 60 El **art. 38.2** hace referencia, de forma sorprendente y parece que irónicamente, a que " *los datos sólo podrán referirse a:* ". La enumeración es extremadamente exhaustiva, conteniendo supuestos de discrecionalidad e indeterminación lesivos y peligrosos, y como casi siempre en detrimento de los derechos de los ciudadanos. Así puede citarse la letra c., donde después de enumerar en letras anteriores toda una serie de datos personales, posibilita que puedan comunicarse datos relativos a "los demás elementos necesarios para identificar al solicitante", consagrando un supuesto de absoluta discrecionalidad.

Así se expresa la enumeración de las referidas categorías de datos:

" 2. Dichos datos sólo podrán referirse a:

- a. la identidad (nombre y apellidos, en su caso apellido anterior, apodos o seudónimos, lugar y fecha de nacimiento, nacionalidad actual y anterior del solicitante de asilo y, en su caso, de los miembros de su familia;
- b. los documentos de identidad y de viaje (referencia, período de validez, fechas de expedición, autoridad que los haya expedido, lugar de expedición, etc.);
- c. los demás elementos necesarios para identificar al solicitante;
- d. los lugares de estancia y los itinerarios de viaje;
- e. los permisos de residencia o los visados expedidos por una Parte Contratante;
- f. el lugar en que se haya presentado la solicitud de asilo;
- g. en su caso, la fecha de presentación de una solicitud de asilo anterior, la fecha de presentación de la solicitud actual, el estado actual del procedimiento y el contenido de la decisión adoptada. "

■ 61 " Las Partes Contratantes sólo podrán utilizar los datos previstos en los artículos 95 a 100 con los fines enunciados para cada una de las descripciones mencionadas en dichos artículos ". ( Art.102.1 )

amplitud de estas descripciones, obvia cualquier otro comentario. Tampoco en este supuesto se salvaguarda este principio<sup>62</sup>.

Más sorprendente resulta la regulación que se establece en la letra a. del apartado 3 del art. 126<sup>63</sup>, cuando, tras proclamarse la salvaguarda del principio de especificación de la finalidad, se exceptiona rápidamente recogiendo la posibilidad de utilizar los referidos datos con fines distintos. El recoger esta excepción abre las puertas a toda una serie de usos de diferente etiología, que consecuentemente escapan a todo control, y por supuesto a todo conocimiento de los afectados. Además se formula de una manera genérica, amplia, sin establecer la más mínima cortapisa material respecto a las diferentes finalidades a las que potencialmente tal desviación pueda tender<sup>64</sup>.

Eso sí, nuevamente el Convenio pretende adornarlo con un requisito formal, consistente en el previo acuerdo o consentimiento entre Estados, y a la adecuación a sus legislaciones internas. Las peculiares materias y tareas que contempla el Convenio ( terrorismo, crimen organizado, armas, etc. ) hace que esta posibilidad abra un amplio campo para el tratamiento de datos personales, como un elemento para luchar contra todas conductas o situaciones que puedan tener una conexión con las referidas materias. No debe olvidarse, por otra parte, que la mayoría de las legislaciones internas contemplan un generoso régimen de excepciones de las garantías, en el supuesto de tratamiento de datos personales realizados por los diferentes Cuerpos y Fuerzas de Seguridad del Estado.

Cuando de lucha contra el crimen y la delincuencia organizada estamos hablando, que Parte negará a otra que haga un uso diferente de los datos que

■ 62 Y no puede hacerlo, por que a renglón seguido establece dos posibilidades ciertamente contradictorias con el principio que proclama:

1. Posibilidad de duplicar los datos, amparándose, eso sí, en "razones técnicas".

2. Posibilidad de pasar de una descripción a otra cuando así lo exijan, por enésima vez, "el orden y la seguridad públicos, una amenaza grave o la prevención de una amenaza grave".

Todo ello, cuando al final proclamà "solemnemente":

" **Toda utilización de datos que no sea conforme con los apartados 1 a 4 se considerará como una desviación de la finalidad respecto al Derecho nacional de cada Parte Contratante** ".

Paradójicamente se habla de desviación de poder, cuando ésta se incluye en la propia regulación. Será "otra" desviación de poder.

■ 63 " **3.a la Parte contratante destinataria únicamente podrá utilizar los datos para los fines previstos en el presente Convenio para la transmisión de dichos datos; la utilización de los datos con fines distintos sólo será posible previa autorización de la Parte Contratante que transmita los datos y en cumplimiento de la legislación de la Parte contratante destinataria; podrá concederse la autorización siempre y cuando el Derecho nacional de la Parte Contratante que transmite los datos lo permita** ". ( Art. 126.3.a. )

■ 64 La Comisión de las Comunidades Europeas establece, a este respecto, que : " **Una modificación posterior de la finalidad de un tratamiento sólo será legítima en la medida que sea compatible con la finalidad principal... En la medida en que la finalidad de la conservación y utilización de datos personales debe ser legítima, las finalidades potenciales de un tratamiento son limitadas. Dicho tratamiento sólo puede crearse y utilizarse para un objeto que se ajuste a las disposiciones de la Directiva y de las legislaciones nacionales de los Estados Miembros** ".

Cfr., *Propuesta modificada de Directiva...*, cit. pp. 15 - 16.

originariamente le transmitió, si con ello lograra hacer frente a los ataques al “orden y/o la seguridad públicos”.

Este principio de especificación de la finalidad aparece conectado, como si del reverso de una misma moneda se tratara, con el **principio de restricción de uso**.

Si el tratamiento automatizado de los datos personales para ser leal y lícito debe contener la indicación previa de las finalidades a las cuales se dirige, ello implica la consagración efectiva de un uso restrictivo de aquellos por parte de las personas u órganos autorizados a utilizarlos<sup>65</sup>.

Por tanto, el tratamiento debe referirse a datos pertinentes y no excesivos en relación con los objetivos perseguidos; objetivos que como ya se han indicado deben ser legítimos y explicitados previamente. De nada serviría que se exigiera, por parte de la legislación reguladora, el respeto del principio de especificación de la finalidad, si paralelamente no se limitara el uso que de los datos pueda hacerse.

En dos grupos pueden clasificarse las menciones que respecto a este principio realiza el Convenio:

**a) Restricción de Acceso.** Intenta garantizar que sólo las autoridades competentes y para el cumplimiento de específicas tareas tengan acceso a un determinado conjunto de datos personales:

**1. “ Los usuarios podrán consultar únicamente los datos que se a n necesarios para el cumplimiento de su misión”**

( Art.101.3 )<sup>66</sup>.

■ 65 Sobre este particular el propio Convenio establece :

“ 4. Cada Parte Contratante facilitará al Comité Ejecutivo la lista de las autoridades competentes que estén autorizadas a consultar directamente los datos integrados en el Sistema de Información de Schengen. En dicha lista se indicará, para cada autoridad, los datos que puede consultar y para que misión “. ( Art. 101.4 )

■ 66 Este mismo precepto en sus párrafos 1 y 2 procede a la enumeración de los referidos usuarios:

“ 1. El acceso a los datos integrados en el Sistema de Información de Schengen, así como el derecho de consultarlos directamente, estará reservado a las autoridades competentes para:

a. los controles fronterizos;

b. las demás comprobaciones de policía y de aduanas realizadas dentro del país, así como la coordinación de las mismas  
2. Además, el acceso a los datos introducidos de conformidad con el artículo 96, así como el derecho a consultarlos directamente, podrán ser ejercidos por las autoridades competentes para la expedición de visados, por las autoridades centrales competentes para el examen de las solicitudes de visado y por las autoridades competentes para la expedición de permisos de residencia y para la administración de los extranjeros en el marco de la aplicación de lo dispuesto en el presente Convenio sobre la circulación de personas... ”.

2. “ Los datos únicamente podrán ser utilizados por las autoridades judiciales, los servicios y los órganos que realicen una tarea o cumplan una función en el marco de los fines contemplados en la letra a ” ( Art. 126.3.b ).

b) **Restricción de Uso.** Pretende articular garantías para que el uso de los datos se haga de acuerdo con las finalidades previamente determinadas:

1. “ Los datos no podrán ser utilizados con fines administrativos. Como excepción, los datos introducidos con arreglo al artículo 96 sólo podrán utilizarse, de conformidad con el Derecho nacional de cada Parte Contratante, para los fines que se definen en el apartado 2 del artículo 101 ” ( Art. 102.4 ).

Nuevamente se observa la derogación casi automática de la garantía que el precepto pretende establecer, y se lleva a cabo de una forma embrollada, demostrando una manifiesta ausencia de técnica legislativa, mediante la remisión a otros preceptos del Convenio.

Tal posibilidad podrá aplicarse a aquellos datos relativos a extranjeros incluidos en la lista de no admisibles (art. 96), y para el cumplimiento de comprobaciones de policía y de aduanas realizadas dentro del país, así como para la coordinación de las referidas actividades.

Parece consagrarse la equiparación entre infracciones penales y administrativas con respecto al tratamiento de los datos personales. Aun cuando se utilicen, apartándose de la finalidad original, no deben servir para arrojar más elementos de culpabilidad o de sospecha sobre los individuos afectados.

El dejar el control de esta posibilidad a la legislación de los Estados Miembros puede producir soluciones de lo más diverso, por cuanto el cumplimiento o no de determinadas formalidades administrativas implicará la introducción automática del extranjero en la lista de no admisibles, o bien simplemente se le pedirá la subsanación de tal falta en tiempo y forma oportunos.

La calificación de una persona como deseable o indeseable puede quedar limitada al cumplimiento de determinados requisitos formales, obviando las peculiares situaciones personales, familiares, culturas o políticas que coadyuven a la determinación de su particular estado y circunstancia. Lo contrario es reducir al hombre a un mero objeto de procedimiento, y no considerarlo sujeto del mismo.

2. “ La Parte Contratante destinataria sólo podrá utilizar los datos para los fines indicados por la Parte Contratante que los proporcione, y debe-

**rá hacerlo cumpliendo las condiciones impuestas por dicha Parte Contratante” ( Art. 129.a. ).**

La articulación de este principio, que se incardina en un precepto general relativo a la transmisión de los datos, se hace recaer sobre el acuerdo entre Estados. Será la Parte transmisora la que señalará tanto las finalidades como las condiciones de uso a las que deberá ceñirse la Parte receptora. Ahora bien, no siempre será posible esa adecuación. Y no lo será por que no se quiera, sino simplemente por que no se pueda; por que la legislación interna del Estado receptor le impida o dificulte el cumplimiento de ciertas condiciones, o bien por que regule supuestos no contemplados en su norma patria. La situación se agravaría si nos encontramos con Estados que no posean una norma interna reguladora de la protección de los datos personales automatizados.

Además, se echa de menos el establecimiento de un mecanismo de garantía efectivo que asegure esa adecuación. ¿ Como un Estado soberano va a poder controlar el uso que internamente otro Estado, también soberano, ha hecho de determinados datos, aunque aquel se los haya transferido ?; aun cuando fuera posible, ¿ como controlar, y mucho menos evitar o impedir, determinados usos desviados ?. Preguntas, ciertamente, de difícil resolución.

Si como parece establecer el Convenio, se tiende a un espacio único, a una legislación única por que no se han establecido unas normas unificadas para regular el flujo de datos entre Estados Partes, máxime cuando de transmisión de datos estamos hablando.

Ello nos conduce a formularnos otras preguntas. ¿ Que resultado se deduciría de un eventual incumplimiento por el Estado receptor ?; ¿ de acuerdo a que legislación se deduciría tal responsabilidad ?, ¿ podría imponerse una sanción ?; ¿ de que naturaleza ?. Preguntas sin respuestas en el Convenio.

La salvaguarda de la autonomía nacional condena a estas correctas declaraciones, al menos en lo que de deseo expresan, al papel de meras expresiones grandilocuentes, vacías de contenido.

## **B. Principio de Calidad de los Datos.**

La naturaleza de los datos debe corresponderse con el objetivo perseguido. Ello implica que los datos deberán ser adecuados, pertinentes y no excesivos con relación a los fines que se persiguen. Los datos deben ser exactos y, cuando sea necesario, deben actualizarse. En el supuesto de que hubiera datos

incorrectos o incompletos con respecto a los fines para los que fueron recogidos, debe preverse la posibilidad de su supresión o rectificación.

La calidad de los datos supone el criterio protector genérico, en torno al cual se articulan una serie de garantías, que contribuyen a perfilar su concreto contenido. Pero criterios como la pertinencia, la exactitud o cualquier otro, no deben entenderse aisladamente, sino que forman parte integrante de esa calidad, de esa esencia misma de los datos personales.

Este principio supone la consagración de un criterio objetivo, sin cuya escrupulosa concurrencia no deben nunca ser objeto de tratamiento automatizado los datos personales. La calidad se perfila así en su acepción negativa, pues se predica en lo que de garantía tiene para los ciudadanos, y no de la “calidad” que deben reunir determinados datos para posibilitar su tratamiento. La concurrencia de sus contenidos supone una protección, no una habilitación a los agentes que tratan los datos para que procedan a tal operación.

Volviendo al contenido del Convenio, de este tenor se expresa el **párrafo 6 del artículo 38** <sup>67</sup>:

**“ La Parte Contratante que transmita los datos velará por su exactitud y su actualidad.**

**En el supuesto de que dicho Estado miembro facilitara datos inexactos o que no hubieran debido transmitirse, se informará inmediatamente de ello a las Partes Contratantes destinatarias, las cuales estarán obligadas a rectificar dichas informaciones o a eliminarlas** <sup>68</sup>.

La eficacia de este principio se articula, como se extrae del propio precepto, en torno a un doble principio:

1. La Parte que transmita los datos debe, y aunque nada dice el texto

- 67 Centramos el estudio en este precepto por ser de contenido idéntico al resto de los que se refieren a este principio, presentando una problemática idéntica, que es la general del Convenio. Al resto de preceptos se irá haciendo referencia en el desarrollo de nuestro viaje por este principio.
- 68 En iguales términos se expresa el **artículo 126.3.c.**, si bien aquí consagra una importante novedad digna de reseñar. Las comprobaciones acerca de la calidad y de la exactitud de los datos no sólo se deja a la Parte transmitente, sino que también la persona interesada podrá solicitar que se proceda a tal verificación de calidad. Esta posibilidad directa para los individuos constituye un notable acierto del Convenio, pues implica el dotar a los interesados de la posibilidad de conocer que existe un tratamiento automatizado sobre sus datos personales, y además cual es el contenido exacto, tanto del proceso, como de los mismos datos. Incorpora el reconocimiento a los afectados de su derechos de acceso, rectificación y cancelación sobre sus datos personales. Supone una consagración de ese **derecho a la autodeterminación informativa**.

debe entenderse que antes<sup>69</sup> y durante la transmisión, velar por la exactitud y la actualidad de los datos. Pero su responsabilidad no finaliza ahí. Si efectuada la transmisión se evidencia que los datos son incorrectos o no pertinentes debe comunicarlo inmediatamente a la Parte contratante que los hubiera recibido. Sorprende como al Estado transmisor, causante del error, sólo se le exige un deber de comunicación, y no cualquier otra conducta que tienda a evitar o al menos atenuar los resultados perniciosos que de un uso no correcto de los datos personales puedan derivarse.

Podrá objetarse que los datos están en poder de un tercer Estado, con lo cual escapan al control del Estado transmisor; por otra parte, ese tercer Estado puede haber hecho uso de los datos recibidos de “buena fe”, antes de recibir la comunicación de que los datos son incorrectos o no pertinentes, y consecuentemente después de haberse generado un perjuicio para los individuos afectados.

¿ En que puede concluir este galimatías ?. La solución parece ser una exoneración de responsabilidad por parte de los Estados intervinientes, unos por que cuando comuniquen los defectos que sufren los datos, tal vez ya se haya hecho uso de ellos; los otros por que han procediendo a la utilización de los datos confiando en su regularidad<sup>70</sup>. Serán los individuos afectados los que sufran las consecuencias. Volveremos sobre esta cuestión posteriormente al abordar el estudio del Principio de Responsabilidad por Infracción.

2. La Parte que reciba los datos deberá, si por la Parte transmisora se le comunica que los datos son incorrectos o no pertinentes, proceder inmediatamente y “ex officio” a su rectificación o cancelación. Nada indica el precepto

- Esta afirmación tiene apoyatura en el hecho de que el propio Convenio exige a las Partes Contratantes que se proceda a la verificación de exactitud y actualidad de los datos en el momento de la introducción de los datos en el S.I.S., y por supuesto, en un momento anterior a que la transmisión de datos a otros Estados se efectúe. Se recoge la posibilidad de un control interno, previo por y para cada Estado, que tendrá como límite inexcusable el momento en que se proceda a la introducción de los datos en el Sistema común. Control que de no efectuarse deparar las responsabilidades a que haya lugar.

Así se expresa el **Art. 105**:

**“ La Parte Contratante informadora será responsable de la exactitud, actualidad y licitud de la introducción de los datos en el Sistema de Información de Schengen ”.**

- Sí se establece la posibilidad de un conflicto entre Estados miembros en torno a la concurrencia o no de errores de hecho o de derecho que desvirtúen esa calidad que de los datos deba predicarse; ello no implica que exista un conflicto en torno a la delimitación o atribución de responsabilidades. Se trata de un conflicto anterior a la eventual depuración, y por tanto atribución de responsabilidades. Los Estados discrepan acerca de el contenido de los datos, no de las consecuencias derivadas de un uso o transmisión posterior.

El **párrafo 3 del art. 106** así se expresa:

**“ Si las Partes Contratantes no pudieran llegar a un acuerdo, la Parte Contratante que no hubiere dado origen a la descripción someterá el caso para dictamen a la autoridad de control común mencionada en el apartado 1 del artículo 115 ”.**

si tales fallos son constatados por la Parte receptora de los datos; es decir si constata tales deficiencias antes de hacer uso de los mismos. La solución nos la proporciona el propio Convenio cuando señala el deber de informar a la Parte informadora, la cual procederá inmediatamente a la comprobación de las posibles deficiencias, y constatadas éstas debe proceder a la rectificación o cancelación de los datos<sup>71</sup>.

Supone la otra manifestación del fenómeno estudiado anteriormente, si bien aquí, regulado con evidente acierto. Creemos que constituye un efectivo remedio para evitar perniciosos efectos o consecuencias para los ciudadanos, derivados de una falta de diligencia por parte de los Estados Miembros, cuando procedan al tratamiento de sus datos personales. Observamos como el precepto que venimos estudiando hace referencia a dos categorías que engloban ese principio genérico de la calidad pero que no obstante no deben confundirse. Aunque complementarios, no pueden identificarse, pues responden a dos presupuestos diferentes:

a) Contenido Material: Datos Exactos.

b) Contenido Temporal: Datos Actuales.

Así datos exactos en este momento, devendrán inexactos por el transcurso del tiempo y por las variaciones de las circunstancias en las que se apoyan debido a ese caminar del tiempo. Igualmente la afirmación del carácter actual de los datos, no prejuzga su exactitud.

El estudio que estamos realizando vuelve a complicarse cuando, con respecto a las obligaciones de los Estados referentes a la salvaguarda de los datos, se hace referencia, por un lado a *datos inexactos*; y por otro a una nueva categoría, *datos que no hubieran debido transmitirse*.

Para nada se hace mención a la otra categoría: la actualidad. No se hace referencia a datos “ antiguos “, “ no actualizados “, o cualquier otra mención semejante.

Bien pudiera entenderse que aparecería englobada en la categoría de datos que no debieron transmitirse, pero eso mismo podría predicarse de la

■ 71 De esta manera se expresa el Art. 106 en su párrafo 2 :

“ Si una de las Partes Contratantes que no haya hecho la descripción dispusiera de indicios que hagan presumir que un dato contiene errores de hecho o de derecho, informará de ello lo antes posible a la Parte Contratante informadora, la cual deberá comprobar la comunicación y, en caso necesario, corregir o suprimir sin demora el dato “.

exactitud. La concepción de un dato como no transmisible es una consideración genérica que engloba aquellos supuestos en que los datos no presentan la calidad suficiente para ser transmitidos, independientemente de que sea por falta de exactitud o de actualidad.

La referencia es a un criterio objetivo, previo, genérico

- el carácter intransmisible de los datos -, y no a una cualidad concreta de los datos - la actualidad -.

No se acierta a comprender esta diferenciación. Acaso nos encontremos ante un "lapsus legislatoris" o realmente se pretenda hacer referencia a algo diferente. Baste ahora indicarlo.

Para concluir, debemos hacer referencia a otro criterio, que aunque no explicitado en el texto del Convenio, si puede deducirse del mismo. Este es la **integridad** de los datos.

La salvaguarda de un correcto uso de los datos personales debe incluir el que los datos sean utilizados en su integridad, tanto formal como material. Es decir, en lo referente a su expresión en los textos o documentos que le sirven de soporte, y en el contenido concreto que los referidos datos se pretende expresar.

La apelación a la integridad en la utilización de los datos, no debe entenderse como un propuesta a favor de la utilización masiva de los mismos, sino todo lo contrario. Lo que se pretende salvaguardar es una utilización racional y no parcelada, que impida una versión desvirtuada de los hechos y de las circunstancias que confluyen en las personas. En muchas ocasiones será más lesivo, para el ejercicio y disfrute de los derechos, un uso parcial o una imagen parcial de una determinada situación, que un uso no estrictamente correcto de los datos.

Los datos en su utilización deben atemperarse al criterio de la integridad, para posibilitar así un conocimiento completo y unos efectos también completos; entendidos estos últimos como garantías para los afectados.

No debe tolerarse que un aspecto parcial se equipare al conjunto; que una persona quede reducida a la manifestación concreta de un aspecto de su personalidad.

En el Convenio, de manera indirecta como ya indicamos, se recoge

cuando establece que será la Parte informadora la única autorizada para completar los datos que hubiera introducido<sup>72</sup>.

Se da por supuesto que podrán introducirse datos incompletos, de ahí que sea necesario otorgar esta facultad “reparadora” a los Estados.

Lo que debería haberse establecido es la prohibición absoluta de tratar datos incompletos, por el perjuicio que puede deparar para los afectados. Además esta facultad de completar los datos no se concede al resto de Partes Contratantes, si apreciaran una deficiencia en el contenido de los datos, sino que sólo se otorga a al Parte informante. Se aparta así del criterio señalado anteriormente con respecto a la posibilidad de modificación de datos inexactos o que no hubieran debido transmitirse.

### C. Principio de Conservación Limitada de los Datos.

La conservación de los datos personales en una forma que permita la identificación del interesado, sólo debe quedar autorizada durante un período que no exceda del necesario para los fines para los que fueron registrados. Esta limitación pretende a garantizar lo que se ha denominado *derecho al olvido*.

Los datos deben tener una vigencia estricta, en lo afectante a su uso y transmisión, para impedir que situaciones concretas y circunstanciales, supongan un elemento de estigmatización social para los afectados.

Constituye un medio de poner freno a ese afán devorador de datos que presentan actualmente, tanto las administraciones públicas como grandes multinacionales de los sectores de comunicación e información.

En el Convenio, también se recoge este principio en la forma que venimos señalando<sup>73</sup>, estableciendo un procedimiento de verificación y examen respecto a la necesidad de conservar los datos.

Siendo capital el reconocimiento del principio, su efectividad se manifestará en el mecanismo que se ponga en práctica para aplicarlo a los supuestos concretos que se presenten, así como las actuaciones que deberán desarrollar las autoridades u órganos encargados de la conservación.

■ 72 Cfr. Art. 106.1.

■ 73 “ Los datos transmitidos se conservarán durante un período no superior al necesario para los fines para los que se hubieren intercambiado...” ( Art. 38.9 ).

“ Los datos de carácter personal introducidos en el Sistema de Información de Schengen a efectos de la búsqueda de personas sólo se conservarán durante el tiempo necesario para los fines para los que se hubieren facilitado los datos...” ( Art. 112.1 ).

La regulación a este respecto es bastante dispar, atendiendo a un doble criterio: datos referentes a personas y cualesquiera otros datos. Esta diferenciación genera importantes diferencias respecto al período máximo de examen y conservación de las diferentes categorías de datos.

#### 1. Datos referentes a personas.

Si de datos personales referentes a solicitantes de asilo se trata, el Convenio no establece ningún criterio respecto al período máximo de conservación de los datos<sup>74</sup>, y ni siquiera se hace referencia a un plazo razonable para proceder al examen de la oportunidad o no de conservar los datos.

El haber regulado estos datos como una categoría especial, aparte, con su peculiar régimen de garantías, hace que en este caso la desprotección y la arbitrariedad sea máxima. ¿ Como puede establecerse una regulación con semejante deficiencia, cuando de asilo, de desarraigo familiar, social y cultural, estamos hablando ?. Quizás por eso, por que no se espera una crítica, ni siquiera una súplica de “unos pobres sin hogar”.

De esta manera se expresa el Convenio, a este respecto:

**“ La Parte Contratante de que se trate estudiará a su debido tiempo la necesidad de conservarlos ”**<sup>75</sup>.

Como indicamos, más indeterminación es imposible. ¿ Que entender por su debido tiempo ?. Creemos que aquí sí la respuesta es clara: cuando los Estados quieran, con absoluta independencia.

Mejor y más completa es la regulación que se establece respecto a los datos referentes a personas incluidas en las categorías señaladas en los arts. 95 a 99.<sup>76</sup>

Tampoco se establece un período máximo de conservación, pero lo que sí se incluye el plazo en el cual deberá procederse al examen acerca de la necesidad de conservar los datos. El plazo general es de 3 años, que queda reducido a 1 en el supuesto de datos relativos a personas a efectos de vigilancia discreta o de control específico. Este plazo comienza a correr desde el momento de introducción de los datos.

▪ 74 En ningún caso debe ser superior a la conclusión del examen de una solicitud de asilo, y por tanto a su resolución.

▪ 75 Art. 38.9

▪ 76 Art. 112.

Pero lo realmente relevante de esta regulación es que constituye un mínimo inexcusable. Aquí los Estados no podrán obviar estos plazos, y ello en virtud de dos criterios:

1. Los Estados no podrán ampliar este período. A sensu contrario, lo que sí podrán es establecer unos plazos más cortos para efectuar dicho examen.

2. La Unidad de Apoyo Técnico del S.I.S. procederá, en caso de que los Estados no le comuniquen el mantenimiento de la descripción, a la supresión de los datos. Esta supresión se comunicará con un mes de antelación a la Parte Contratante afectada. Esta supresión automática es una importante novedad, que garantiza que los Estados no puedan mantener *sine die* la descripción en el Sistema, alegando que no se han cuestionado la necesidad o no de conservación.

Como venimos señalando, estas garantías no impiden que la descripción siga manteniéndose, si el Estado informador considera que sigue siendo necesaria para el cumplimiento de los fines que motivaron su introducción<sup>77</sup>. El mantenimiento implica que nuevamente vuelve a correr el plazo de 3 años, o de 1 en su caso, a cuya conclusión deberá procederse a un nuevo examen. La Unidad de Apoyo Técnico deberá ser informada de este mantenimiento.

## 2. Datos referentes a objetos.<sup>78</sup>

A diferencia de las categorías anteriores, estos datos están sujetos a un período máximo de conservación, sin necesidad de una actividad de examen por parte de los Estados miembros acerca de la necesidad o no de conservación de los datos.

La eliminación se produce de manera automática, una vez transcurrido el período de vigencia de los datos.

El tiempo máximo de conservación se determina en cascada:

1. Se conservarán durante un período máximo de 10 años los datos distintos de los mencionados en el artículo 112. Deberán incluirse los datos personales, no incluidos en la categoría anterior, que se transmitan para la comproba-

■ 77 Vid. lo ya señalado anteriormente respecto a la problemática que plantea el Convenio respecto a la delimitación de las finalidades que motivan el tratamiento automatizado y uso de los datos personales.

■ 78 Art. 113.

ción de una descripción de un objeto encontrado<sup>79</sup>.

2. Como máximo durante 5 años, los datos relativos a documentos de identidad expedidos y billetes de banco registrados.

3. Los referentes a vehículos de motor, remolques y caravanas, como máximo durante 3 años.

Estos datos suprimidos se conservarán durante un año más en la Unidad de Apoyo Técnico, con el sólo fin de consultarlos para comprobar a posteriori su exactitud y la licitud de su integración.

#### **D. Principio de Responsabilidad por Infracción.**

La inclusión de este principio entre los que deben garantizar la protección de los datos obedece a una doble consideración: En primer lugar, antes de proceder al tratamiento automatizado de los datos, debe especificarse en las legislaciones correspondientes que el Estado será responsable de los perjuicios que ocasione. Se trata de una obligación positiva que deben asumir los Estados. Para los individuos, supone el concederle un ámbito de protección y de restitución en sus legítimos derechos e intereses que hayan podido verse afectados por el tratamiento en forma automatizada de sus datos personales.

Y es una consecuencia que no debe extraerse del proceso global de tratamiento, ni considerarse sólo como un derecho de los afectados. Es una de las posibles consecuencias del proceso de tratamiento, y por lo tanto debe estudiarse unitariamente en el mismo.

Las Partes contratantes serán responsables de cualquier daño ocasionado a una persona como consecuencia de la explotación de su parte nacional del S.I.S.<sup>80</sup>. Esta responsabilidad se determinará en cada Estado de acuerdo a su derecho interno. Ello implica que se producirán disfuncionalidades en este sistema de atribución de responsabilidades. Conductas que en un Estado serán consideradas como causa de responsabilidad, en otro no lo serán. Incluso en aquellos en que lo sea de manera igualitaria, su nivel de intensidad variará considerablemente. No debe olvidarse que este principio no se recoge en todas las legislaciones internas que para la protección de los datos se han promulgado en los Estados miembros<sup>81</sup>.

■ 79 Art. 100.2. Vid. sobre ello, *HEREDERO HIGUERAS, M., La protección de los datos personales en manos de la policía: Reflexiones...* cit., p. 40.

■ 80 " Toda Parte Contratante será responsable, con arreglo a su derecho nacional, de cualquier daño ocasionado a una persona como consecuencia de la explotación del fichero nacional del Sistema de Información de Schengen... " ( Art.116.1 ).

■ 81 Se recoge especialmente en Alemania y en España (art. 17 de la LORTAD). Vid. sobre ello: *HEREDERO HIGUERAS, M., La protección de los datos personales en manos de la policía: Reflexiones...*, cit., p.40.

Creemos que hubiera sido más conveniente el regular una responsabilidad general, conjunta, pues de una organización y actividades conjuntas estamos hablando; y dejar a los Estados Miembros las concretas formas de satisfacción a los administrados por los perjuicios irrogados de acuerdo a sus peculiares instituciones y a su tradición jurídica.

El ámbito de responsabilidad incluye todos los que daños que se irroguen a una persona. Criterio ciertamente amplio del que precisamente tampoco podrá hacerse un uso desmesurado o no acorde con la peculiar naturaleza de la institución. Estos daños deben ser consecuencia de la explotación de la parte nacional del Sistema, y por lo tanto deben incluirse cualquier operación o conjunto de operaciones aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo o supresión.<sup>82</sup>

Ya indicamos anteriormente que en esta cuestión de atribución de responsabilidades los principales obstáculos podrían derivar de un enfrentamiento entre Estados miembros en orden a cual corresponde tal responsabilidad, y quien debe, consecuentemente, hacer frente a las prestaciones que se deriven del daño causado.

El Convenio hace frente a esta cuestión estableciendo unos criterios de determinación del Estado responsable:

a) La asunción de responsabilidad corresponde como regla general a todo Estado Miembro.

b) Si los daños son consecuencia de la transmisión de datos que contengan errores de hecho o de derecho, la responsabilidad será imputable a la Parte Contratante informadora. No obstante, la Parte que usó los datos transmitidos no podrá alegar que se le transmitieron datos incorrectos si, con arreglo a su Derecho interno, le corresponde la responsabilidad con respecto de una persona perjudicada<sup>83</sup>. Se trata de evitar que se produzca una elusión de responsabilidad alegando una eventual norma de conflicto, en menoscabo de una norma interna de carácter imperativo.

■ 82 Tal como se recoge en el apartado b) del artículo 2 de la *Propuesta modificada de Directiva del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales...*, cit., p. 69.

■ 83 Art. 126.3.d.

c) Si la demanda de responsabilidad se plantea contra la Parte Contratante destinataria y ésta viene obligada a reparar el perjuicio causado y a hacer frente a la correspondiente indemnización, la Parte Contratante informadora deberá, previa petición, proceder al reembolso integro de las cantidades satisfechas por la Parte destinataria. Este derecho de reembolso encuentra su límite en el supuesto de que la Parte destinataria, demandada, hubiese hecho uso de los datos incumpliendo el Convenio.

### **3. Derechos de la persona interesada.**

Ante el tratamiento automatizado de sus datos personales toda persona debería poder:

- obtener a intervalos razonables y sin plazos o gastos excesivos, la confirmación de la existencia o no en el fichero automatizado de datos personales que le afecten, así como la comunicación de los mismos de forma inteligible,
- obtener, si hubiera lugar, la rectificación de dichos datos o su cancelación si hubieran sido tratados violando aquellas normas que aseguran y hacen efectivos los principios básicos de protección de los datos personales,
- disponer de un recurso si no se da curso a una solicitud de confirmación o, en su caso, de rectificación o cancelación.

Corresponde a los Estados miembros establecer como deben ofrecerse estas informaciones al interesado.

El **apartado 1 del art. 109**, que regula el *derecho de acceso*<sup>84</sup>, nos remite al Derecho nacional de la Parte contratante ante la que se hubiese alegado el derecho. Su ejercicio queda diferido hasta que la autoridad de control nacional establezca las modalidades en que deberá hacerse efectivo el derecho, si así lo prevé la legislación interna.

El derecho de acceso puede ejercerse previa solicitud. El interesado tendría derecho a obtener información sobre el origen y sobre la utilización de los datos personales en cuestión.

■ 84 " El derecho de toda persona a acceder a los datos que se refieran a ella y estén introducidos en el Sistema de Información de Schengen se ejercerá respetando el Derecho de la Parte Contratante ante la que se hubiese alegado tal derecho. Si el Derecho nacional así lo prevé la autoridad nacional de control prevista en el apartado 1 del artículo 114 decidirá si se facilita información y con arreglo a qué modalidades ".

En idénticos términos se expresa el art. 127.2.c. :

" el acceso a los datos y las condiciones en que se concederá dicho acceso estarán regulados por el Derecho nacional de la Parte Contratante a la que la persona interesada presente su solicitud ".

Cuando la solicitud de acceso se ejercite ante una Parte contratante que no haya realizado la descripción, aquella no podrá facilitar información respecto a los datos que se le solicitan. Supone una derogación de este derecho, que se ampara en la responsabilidad que corresponde a cada Estado por la introducción de descripciones en el Sistema. Además como ya vimos, según se desprende del art. 105, sólo la Parte Contratante informadora será responsable de la introducción de los datos, y consecuentemente ante ella debería ejercerse el derecho de acceso.

No obstante esta imposibilidad no presenta caracteres absolutos. Si se ha concedido a la Parte informadora la posibilidad de manifestarse respecto a dicha solicitud de acceso, la Parte destinataria si podrá conceder la información sobre los datos solicitados. Supone una manifestación, *mutatis mutandi*, del principio administrativo del silencio positivo.

Pero el derecho de acceso aparece limitado en su ejercicio. Corresponde a los estados Miembros decidir en qué medida deben incluirse estas excepciones, a no ser que vengan impuestas por el Convenio. Tal es el caso de las descripciones integradas con vistas a una vigilancia discreta, en el que se denegará siempre el derecho de acceso, a al menos mientras no concluya tal actividad y se proceda a la modificación de la descripción.<sup>85</sup>

La introducción de excepciones deben limitarse a aquellas que sean necesarias para la salvaguarda de los valores indispensables para una sociedad democrática.

La relación de los intereses que deben salvaguardarse no es nada exhaustiva. Dos razones justifican tales excepciones:

1. Cumplimiento de la tarea legal consignada en la descripción. Se exige el requisito suplementario de que el comunicar información al interesado pueda ser perjudicial para el cumplimiento de tal tarea. De ahí que, sí pese a comunicarse información, tal tarea legal no sufre perjuicio o menoscabo, no pueda en ningún caso negarse el derecho de acceso.

Las cuestiones fundamentales surgen al intentar determinar que sea dicha tarea legal. Para ello es necesario remitirse a cada una de la categorías de descripciones que se señalan en el Convenio ( arts.95-100 ), para determinar cual

■ 85 Se trata con ello de evitar que se entorpezca gravemente el cumplimiento de una función de investigación por los órganos policiales. Este interés que debe salvaguardarse no debe constituir, no obstante, una vía por la cual se pueda derogar el control que sobre sus propios datos debe otorgarse a los ciudadanos.

es la actividad a desarrollar por las autoridades y órganos competentes en cada supuesto. Cuestiones que tienen su referente en esa función general que no es otra que el preservar el orden y la seguridad públicos. De ahí que deban estimarse estas tareas en sus justos límites y con relación a cada supuesto concreto, y no establecer una generalización ampliadora, que olvida la naturaleza concreta del caso en cuestión y las también concretas medidas a aplicar.

## 2. Protección de los derechos y libertades de terceros.

Al ser equivalente al derecho de acceso del interesado debe considerarse como un motivo válido para limitar el derecho de acceso. Aparte del ejercicio de los derechos fundamentales por terceros, deberán incluirse entre las causas que dan lugar a esta limitación<sup>86</sup> las siguientes: secretos de negocios de terceros; normas del secreto profesional a que están sometidas las profesiones jurídicas o médicas; derecho de un tercero a elaborar su propia defensa; y la defensa de los derechos humanos.

Si el interesado no puede tener acceso a datos que le conciernen y que figuren en el fichero del S.I.S., la autoridad nacional de control debe, previa solicitud, proceder a las verificaciones necesarias para la comprobación de los datos y la licitud de los tratamientos y uso con relación a los fines para los que introdujeron los datos. El procedimiento se acomodará a lo establecido por la normativa interna del Estado ante el que se presente la solicitud. Si el Estado que introdujo los datos fuera otro diferente al que se ha presentado la solicitud, se exige una colaboración entre las autoridades de control de ambos Estados para proceder a tal control<sup>87</sup>.

El **artículo 110** recoge el *derecho de rectificación y supresión o cancelación*. El derecho de rectificación se ejercerá sobre datos que contengan errores de hecho. El de supresión sobre aquellos que contengan errores de derecho. No creemos sea este el criterio más correcto para fundamentar el ejercicio de los derechos. Máxime cuando serán los hechos los que determinarán el Derecho aplicable; a tales circunstancias tal marco jurídico regulador. No se acierta a comprender el porqué de esta división artificiosa. Debería ser la intensidad del error, y su influencia en la valoración de las situaciones que se presenten, la que determinara la rectificación o la cancelación, y no la naturaleza del error. En muchas ocasiones será una incorrecta apreciación de los hechos la que supondrá una mayor lesión, al otorgar a las personas una imagen desvirtuada y alejada de su realidad

■ 86 Vid sobre ello: **Propuesta modificada de Directiva del Consejo relativa a la protección de las personas en lo que respecta al tratamiento de datos personales...**, cit., p. 25.

■ 87 Art. 114.2 .

cotidiana. El Derecho vendrá después para establecer el régimen jurídico al que debe someterse e imponer, si así se establece, la sanción correspondiente.

Debe ponerse el acento en las consecuencias del error y no en la etiología del mismo.

El *derecho de ejercicio de acciones* se reconoce en el **artículo 111**. Se reconoce el Derecho a acudir ante los órganos competentes de los Estados miembros para solucionar los conflictos que pudieran plantearse con respecto al ejercicio de los derechos de información (acceso), rectificación, supresión o indemnización<sup>88</sup>. La distinción entre órganos jurisdiccionales y otras autoridades se debe, como señala **Herederó**, a la diversidad de los sistemas de control existentes en las legislaciones nacionales<sup>89</sup>. Corresponde a las legislaciones nacionales otorgar estas facultades de recurso a los interesados para permitirles que defiendan de una manera amplia todos los derechos que les reconoce el Convenio.

Esta protección de los interesados, y la resolución de las respectivas acciones, debe concluir, además de en una restitución en los derechos afectados, en que las demás Partes Contratantes reciban una notificación de rectificación, supresión o bloqueo de los datos con objeto de que puedan rectificar, suprimir o bloquear los datos en cuestión; tal y como se establece en el art.106.

#### **4. Autoridades de Control.**

En el marco del Convenio son varias las autoridades que pueden integrarse dentro de esta categoría. Ello se debe a la propia estructura funcional del Sistema, articulada entorno a una Unidad Central y, a una Parte Nacional en cada Estado Miembro. También confluye el intento por preservar todos los intereses en conflicto; la salvaguarda de la autonomía de los Estados Miembros, el respeto por los derechos de las personas afectadas y la consecución de unos objetivos comunes.

Conviene señalar que la existencia en cada uno de los Estados Miembros de una autoridad nacional encargada de ejercer un control independiente sobre los datos personales constituye requisito previo e inexcusable para cualquier transmisión de datos personales, y por tanto para poner en marcha el propio Convenio<sup>90</sup>.

- 88 Respecto al derecho de indemnización vid. lo ya apuntado anteriormente cuando abordamos el estudio del principio de responsabilidad por infracción.
- 89 Cfr. **HEREDERO HIGUERAS, M., La protección de datos personales en manos de la policía...**, cit., p. 42.
- 90 Arts. 38.12 y 128.1

Para una mejor comprensión de estos órganos, sistematizaremos nuestra exposición, aludiendo a los concretos perfiles que presenta cada uno.

a) Autoridad con competencia sobre la Parte Nacional del S.I.S.<sup>91</sup>

Es un órgano de naturaleza evidentemente técnica, que ostenta la competencia central sobre dicho fichero nacional y que desarrolla las siguientes funciones:

- Competencia exclusiva sobre la introducción de las descripciones. Será esta autoridad la que procederá a la introducción efectiva de los datos en el Sistema, cuando así le sea solicitado por los órganos judiciales y/o administrativos competentes, dependiendo de la naturaleza de la descripción que se pretenda. Igualmente le corresponderá la competencia para decidir acerca de la modificación de una descripción solicitada por otro Estado miembro<sup>92</sup>, así como para la integración de descripciones<sup>93</sup>.

- Será responsable del correcto funcionamiento de la Parte Nacional del Sistema. Supervisará que todas las operaciones realizadas por y en dicha Parte Nacional se hagan de acuerdo a los protocolos reglamentarios y técnicos establecidos por el Convenio, evitando usos indeseables o torticeros.

- Adopción de medidas necesarias para garantizar el cumplimiento del Convenio. Incluye las funciones organizativas, de material y equipos, así como todas las operaciones técnicas para asegurar una correcta y fluida comunicación entre la Unidad Central y la parte nacional del fichero.

- Órgano de comunicación con los restantes Estados Miembros, en orden al funcionamiento del S.I.S.

Nada se dice acerca del nombramiento de dicha autoridad. Las funciones a desarrollar y su naturaleza, nos inducen a pensar que será un órgano nombrado por los Gobiernos de los Estados Miembros, como encargados gubernamentales de la parte que les corresponde en el S.I.S.<sup>94</sup>.

■ 91 Art. 108

■ 92 Art. 102.3

■ 93 Art. 107

■ 94 La utilización de la expresión " designará ", parece indicar un mayor *quantum* de vinculación con la actividad gubernamental. Nos remite más a una facultad exclusiva del Gobierno, que a un procedimiento de elección y posterior nombramiento.

b) Autoridad Nacional de Protección de los Datos. <sup>95</sup>

Se dispone el establecimiento en cada Estado Miembro de una autoridad de control independiente dotada de medio de investigación y de intervención. Aquellos Estados que aún no tengan esta autoridad deberán proceder a nombrarla, so pena de no poder participar en la transmisión de datos a través del S.I.S. Sus funciones fundamentales son:

- Ejercer un control independiente sobre el fichero de la Parte Nacional del S.I.S.. Control referido a la licitud y legalidad de los tratamientos.

- Comprobar que el tratamiento de la utilización de los datos no lesionan los derechos de las personas afectadas. Constituye su función capital, y cuyo efectivo desarrollo o no evidencia el grado de independencia que las legislaciones nacionales han otorgado a este órgano.

- Conocer de las acciones que, en los supuestos en que no estén atribuidas al conocimiento de autoridades judiciales, correspondan a las personas afectadas respecto a la titularidad, ejercicio y defensa de sus derechos de acceso, rectificación, supresión e indemnización.

La facultad de control tiene por objeto permitir a la autoridad de control que recabe de los responsables del tratamiento los datos necesarios para el cumplimiento de su cometido. Esta competencia se manifiesta en concreto en el acceso a los datos que son objeto de tratamiento. Acceso que deberá hacerse respetando la confidencialidad que a los datos concede el derecho interno, para respetar los derechos de las personas afectadas.

c) Autoridad de Control Común. <sup>96</sup>

Su introducción responde a la búsqueda de un elemento homogeneizador, buscando esa unidad de acción y de objetivos que se pretende.<sup>97</sup>

Su función primordial es efectuar un control sobre la unidad de apoyo técnico del S.I.S. Control acerca de la legalidad y de la correcta ejecución de las

▪ 95 Art. 114

▪ 96 Art. 115.

▪ 97 Su estructura, funcionamiento y competencias son muy similares a las que en el ámbito del Derecho comunitario se atribuirán, salvo una nueva modificación de la Propuesta, al denominado *Grupo de Protección de las Personas frente al Tratamiento de Datos Personales*. Vid. sobre ello: **Propuesta modificada de Directiva del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales...**, cit., concretamente sus arts.31 y 32.

disposiciones del Convenio, y de las actividades desarrolladas por la Unidad Central. Pero dicho control no podrá ejercerse de cualquier manera, sino teniendo en cuenta determinadas regulaciones protectoras de los datos personales, y concretamente el Convenio 108 y la Recomendación R (87) 15, ambas del Consejo de Europa.

Para el cumplimiento de esta misión estará facultada para acceder a los datos integrados en la Unidad de Apoyo Técnico. Este acceso se revela imprescindible para que dicha autoridad pueda ejercer correctamente su función, conociendo directamente los fallos y disfuncionalidades del sistema.

Esta función genérica se manifiesta en las siguientes atribuciones:

- Competencia para analizar las dificultades de interpretación y aplicación que surjan con la explotación del S.I.S.. Se le atribuye competencia para la resolución de controversias entre Estados Miembros acerca de la existencia o no de errores en determinados datos que hayan sido objeto de transmisión.<sup>98</sup> Igualmente se le atribuye competencia para emitir un dictamen, si así se lo solicita alguna Parte Contratante acerca de las dificultades de interpretación y aplicación de las medidas contempladas en el art.126

- Procederá al estudio de los problemas que pudieran surgir en el ejercicio del derecho de acceso y del control independiente efectuado por las autoridades nacionales de protección de datos. Estos estudios y la efectiva consideración de sus conclusiones pueden contribuir a constituirlo de manera indirecta en una especie de "segunda instancia" para la protección de los datos, al poner de manifiesto las trabas planteadas por la aplicación de las legislaciones nacionales e indicar los nuevos caminos por los que seguir avanzando.

- Elaboración de propuestas armonizadas con vistas a encontrar soluciones comunes a los problemas planteados. Se tratará naturalmente de propuestas normativas, que pueden contribuir a corregir las múltiples deficiencias que presenta el Convenio.

La composición de esta autoridad está limitada a los representantes de las autoridades nacionales de control. Cada Estado designará 2 representantes, pero sólo dispondrá de un voto deliberativo.

▪ 98 Art. 106.3

La conclusión de sus estudios y propuestas se harán mediante informes, que deberán ser transmitidos a las autoridades de control nacionales, así como a todos los organismos a los cuales las autoridades nacionales remiten sus propios informes. Como nada se indica, abogamos por que al menos anualmente esta autoridad elabore un informe, que debe ser publicado, acerca del funcionamiento del Sistema Informático de Schengen, poniendo de manifiesto todas las actividades desarrolladas, los problemas suscitados, así como la actitud y cumplimiento de las garantías por parte de los Estados Miembros.

## **5. Seguridad de los Datos.**

La seguridad de la información ( protección de datos conservados, tratados y transmitidos electrónicamente ) contra todo tipo de amenazas es esencial para el ejercicio efectivo de los derechos de las personas en lo referente al tratamiento automatizado de datos personales. La seguridad constituye un requisito imprescindible para la protección de personas y bienes que hacen necesarios el desarrollo de una política común tanto en el campo normativo como en el tecnológico.<sup>99</sup>

Los peligros que amenazan al derecho a la intimidad del interesado no provienen tan sólo del responsable del tratamiento. El derecho está también amenazado si los datos los utiliza con fines diferentes un tercero que no esté autorizado a acceder a ellos ni a utilizarlos.

Es por ello que se obliga a los Estados miembros a tomar las medidas técnicas y organizativas apropiadas y necesarias para la protección contra la destrucción accidental o ilícita, contra la pérdida accidental, así como contra la alteración, la comunicación y cualquier otro tratamiento no autorizado de datos personales.

Esta obligación general de seguridad se concreta en el Convenio<sup>100</sup> en una pormenorizada enumeración de medidas técnicas y de gestión que deberán llevarse a efecto.<sup>101</sup>

Dichas medidas pueden agruparse atendiendo a cuatro criterios fundamentales:

- 99 Cfr. *SANCHEZ BRAVO, A., El Tratamiento Automatizado de las Bases de Datos en el marco de la Comunidad Económica Europea: Su Protección*, en Actas del III Congreso Iberoamericano de Informática y Derecho (Volumen I), Revista Informática y Derecho, Vol. 4, UNED. Centro Regional de Extremadura, Mérida, 1994.
- 100 Art. 118.
- 101 Dichas medidas deberán ser adoptadas por Francia, en su calidad de Parte Contratante responsable de la Unidad de Apoyo Técnico, y respecto a esta unidad.

- Controles personales: Para el tratamiento de datos personales sólo podrá designarse a personas especialmente cualificadas y que estén sometidas a controles de seguridad. Estas personas autorizadas sólo deben disponer de acceso a los datos que sean de su competencia (control de acceso). Estas medidas tiende a impedir que los sistemas de tratamiento de datos puedan ser utilizados por personas no autorizadas haciendo uso de las instalaciones de transmisión de datos (control de la utilización).

- Control de Instalaciones: Deben adoptarse medidas para impedir que personas no autorizadas accedan a las instalaciones utilizadas para la transmisión de datos ( control de acceso a las instalaciones). Se pretende con ello salvaguardar también la integridad de los soportes de datos, y evitar que cualquier persona no autorizada, una vez que haya accedido a las instalaciones pueda leer, copiar, modificar o retirar los soportes de datos (control de los soportes de datos). Dichas medidas deben extenderse a las situaciones en que se produzca un transporte de los soportes de datos ( control del transporte).

- Controles en el tratamiento: Las medidas deben tender a impedir la introducción, información, comunicación o retirada de datos sin autorización (control de la introducción de los datos). Asimismo debe poder comprobarse y verificarse posteriormente al tratamiento que datos han sido introducidos, por qué personas y en qué momentos ( control de verificación de la introducción de datos).

- Controles en la transmisión: Tendrá que impedirse que los datos sean leídos, copiados, modificados o suprimidos sin autorización durante la transmisión de los datos. Deberá establecerse la posibilidad de verificar y comprobar a que autoridades se remiten datos de carácter personal a través de instalaciones de transmisión de datos.<sup>102</sup>

Las medidas de seguridad deberán reforzarse especialmente cuando la transmisión de datos se efectuó a servicios situados fuera del territorio de las Partes Contratantes. Las medidas adoptadas se comunicarán a la autoridad de control.

■ 102 Se recoge la obligación para los Estados miembros de dejar constancia de la transmisión y recepción de las informaciones intercambiadas, cuando de datos referentes a solicitudes de asilo (**Art. 38.8**) o de datos personales transmitidos en aplicación del Convenio (**Art. 126.3.e**) se trate.

Cuando se transmitan datos procedentes de un fichero no automatizado que se introduzcan en otro fichero no automatizado, la transmisión y recepción de datos de carácter personal quedará registrada por escrito (**Art. 127.2.a**).

## **BIBLIOGRAFIA.**

- *ALAUX, J. P., En Europe:« sécurité » d'abord*, Le Monde Diplomatique, juillet 1993.

- *BADILLO O'FARRELL, P., ¿ Que Libertad ?. Entorno al concepto de libertad en la actual Filosofía Política Británica*, Tecnos y Fundación Cultural Enrique Luño Peña, Madrid, 1991.

- *Compétences des Communautés Européennes.- Coopération dans le domaine des affaires intérieures et judiciaires.- Accords de Schengen.- Convention d'application.- Processus de ratification.*, Europe, núm. 7, juillet 1993.

- *Compétences des Communautés Européennes.- Coopération dans le domaine des affaires intérieures et judiciaires.- Accords de Schengen.*, Europe, núms. 8-9, août-septembre 1993.

- *Consejo Europeo de Bruselas*, Comunidad Europea Aranzadi, núm. 13, enero 1994.

- *CHOCHEYRAS, L., La convention d'application de l'Accord de Schengen*, Annuaire Français de Droit International, XXXVII - 1991.

- *DE MIGUEL ZARAGOZA, J., Los Pactos de Schengen. La Cooperación Judicial*, Boletín de Información del Ministerio de Justicia, suplemento al núm. 1676, 5 de julio de 1993.

- *DE MIGUEL ZARAGOZA, J. y BLANCO DE CASTRO, A., El Título VI del Tratado de la Unión: Cooperación en asuntos de Justicia e Interior*, Gaceta Jurídica de la C.E.E. y de la competencia, núm. GJ 115, Serie D, núm. D-18, septiembre 1992.

- *DENNINGER, E., El Derecho a la autodeterminación informativa*, en *Problemas Actuales de la Documentación y la Informática Jurídica (Actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986)*, ed. a cargo de A.E. Pérez Luño, Tecnos, Madrid, 1987.

- *ESCOBAR HERNANDEZ, E., El Convenio de Aplicación del Acuerdo de Schengen y el Convenio de Dublín: Una aproximación al asilo desde la perspectiva comunitaria*, Revista de Instituciones Europeas, Vol. 20, núm. 1, enero-abril 1993.

- *FROSINI, V., Cibernética, Derecho y Sociedad*, Tecnos, Madrid, 1989.
- *GARCIA RODRIGUEZ, I., La Ley aplicable y el Orden Público Comunitario*, Revista de Instituciones Europeas, Vol. 20, núm. 3, septiembrediciembre 1993.
- *GAUTIER, Y., La coopération policière: les perspectives ouvertes par le traité sur l'Union européenne de 7 février 1992*, Europe, núm. 4, avril 1993.
- *GAUTIER, Y., Les accords de Schengen et le droit d'asile à l'épreuve du débat constitutionnel*, Europe, núm. 12, décembre 1993.
- *GONZALEZ-TABLAS SASTRE, R., La Informática Jurídica. Un análisis experimental desde la Filosofía del Derecho*, Sevilla, Tesis Doctoral, 1986.
- *HEREDERO HIGUERAS, M., La protección de datos personales en manos de la policía: reflexiones sobre el Convenio de Schengen*, en la obra colectiva *La protección de los datos personales. Regulación Internacional de la seguridad informática*, Monografies i Documents, núm. 8, Centre d'Investigació de la Comunicació i Universitat Pompeu Fabra, Generalitat de Catalunya, Barcelona, 1993.
- *JULIEN-LAFERRIERE, J., L'Europe de Schengen: de la disparition des frontières aux transferts des contrôles ( commentaire de la loi n° 91-373, du 30 juillet 1991 autorisant l'adhésion de la France à la Convention d'application de l'accord de Schengen )*, Actualité Législative DALLOZ, núm. 13, julio 1992.
- *LAZARO ROMERO, F., El Acuerdo de Schengen y la libre circulación de personas en la CEE*, Cuadernos de Europa, núm. 2, Diputación de Zaragoza (Comisión de Europa), Zaragoza, 1993.
- *LAZPITA GUTURBAY, M., La protección de los datos personales en la Comunidad Europea*, Cuadernos Europeos de Deusto, núm. 9, 1993.
- *LOSANO, M., Curso de Informática Jurídica*, Tecnos, Madrid, 1987.
- *LOSANO, M., Los orígenes de la "Data Protection Act" inglesa de 1984*, en la obra colectiva *Libertad Informática y Leyes de Protección de los Datos Personales*, Centro de Estudios Constitucionales, Madrid, 1989.
- *LUCAS MURILLO DE LA CUEVA, P., El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática*, Tecnos, Madrid, 1990.

- *LUCAS MURILLO DE LA CUEVA, P.*, **Informática y protección de los datos personales (estudio sobre la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal)**, Centro de Estudios Constitucionales, Madrid, 1993.

- *MASSE, M.*, **L'espace Schengen. I.- Textes et contexte, figures de l'intégration dans l'Europe communautaire**, Revue de Science Criminelle et Droit Pénal Comparé, núm. 2, avril-juin 1992.

- *MASSE, M.*, **L'espace Schengen. II.- Développements de l'entraide répressive internationale**, Revue de Science Criminelle et Droit Pénal Comparé, núm. 4, octobre- décembre 1992.

- *MASSE, M.*, **L'Organisation Internationale de Police Criminelle (O.I.P.C.-INTERPOL)**, Revue de Science Criminelle et Droit Pénal Comparé, núm. 2, Avril -juin 1989.

- *NEEL, B.*, **L'Europe sans frontières intérieures: l'Accord de Schengen**, Actualité juridique. Droit administratif, núm. 10, 1991.

- *PEREZ LUÑO, A. E.*, **Derechos Humanos, Estado de Derecho y Constitución**, 4ª Edic., Tecnos, Madrid, 1991.

- *PEREZ LUÑO, A. E.*, **Comentario Legislativo: La LORTAD y los derechos fundamentales**, en Derechos y Libertades. Revista del Instituto Bartolomé de las Casas, 1993, Febrero-Octubre, núm. 1, Universidad Carlos III y Boletín Oficial del Estado.

- *PEREZ LUÑO, A. E.*, **Intimidación y protección de Datos personales: Del Habeas Corpus al Habeas Data**, en el vol. col. Estudios sobre el Derecho a la Intimidación, edic. a cargo de L. García San Miguel Rodríguez-Arango, Tecnos, Madrid, 1992.

- **Portugal no asumirá la Presidencia de Schengen**, en ABC, Sevilla, 16-2-94, p. 30.

- **Question écrite n° 2707/92 de Marco Taradash et Mme Djida Tazdait (V) au Conseil des Communautés européennes (29 octobre 1992) (93/C 101/76)**, Revue Trimestrelle de Droit Européen, núm. 3, juillet- septembre 1993.

- *SANCHEZ BRAVO, A.*, **El tratamiento automatizado de las Bases de Datos en el marco de la Comunidad Económica Europea: su protección**, en

Actas del III Congreso Iberoamericano de Informática y Derecho (Volumen I),  
Revista Informática y Derecho, Vol. 4, UNED. Centro Regional de Extremadura  
- Mérida, 1994.

- **TONIATTI, R., Libertad Informática y Derecho a la Protección de los Datos Personales: Principios de Legislación Comparada**, trad. cast. A. Saíz Arnaiz, en Revista Vasca de Administración Pública, 1991, enero-abril, nº 29.

- **VEDEL, G., Schengen et Maastrich (a propos de la décision nº 91-294 DC du Conseil Constitutionnel du 25 juillet 1991)**, Revue Française de Droit Administratif, núm 2, mars-avril 1992.

- **WECKEL, F., La Convention Additionnelle a l'Accord de Schengen**, Revue Générale de Droit Internationale Public, núm. 2, 1991.

.- Relación de documentos de las Instituciones Comunitarias:

- COMISION DE LAS COMUNIDADES EUROPEAS:

- **Propuesta de Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales**, COM (90) 314 final - SYN 288.

- **Propuesta modificada de Directiva del Consejo 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**, COM (92) 422 final - SYN 287.

- **Propuesta de Decisión, basada en el artículo K.3 del Tratado de la Unión Europea, por la que se aprueba el Convenio sobre el paso de las fronteras exteriores de los Estados miembros**, COM (93) 684 final, D.O.C.E. Nº C 11/6 de 15.1.94.

- **Propuesta de Reglamento, basado en el artículo 100 C del Tratado constitutivo de la Comunidad Europea, por el que se determinan los terceros países cuyos nacionales deben estar provistos de un visado al cruzar las fronteras exteriores de los Estados miembros**, COM (93) 684 final, D.O.C.E. Nº C 11/15 de 15.1.94.

- COMITE ECONOMICO Y SOCIAL:

- **Dictamen sobre la propuesta de Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales**, D.O.C.E. Nº C 159/38 de 17.6.91

- PARLAMENTO EUROPEO:

- **Dictamen del Parlamento Europeo sobre la propuesta de la Comisión al Consejo referente a una directiva relativa a la protección de las personas en lo referente al tratamiento de datos personales**, D.O.C.E. Nº C 94/198 de 13.4.92.

- **Resolución, de 23 de noviembre de 1993, sobre la firma del Acuerdo adicional de Schengen**, D.O.C.E. Nº C 323/98 de 27.12.89.

- **Resolución, de 15 de marzo de 1990, sobre la libre circulación de las personas en el mercado interior**, D.O.C.E. Nº C 96/274 de 17.4.90.

- **Resolución, de 14 de junio de 1990, sobre el Acuerdo de Schengen y el Convenio relativo al derecho de asilo y al estatuto de los refugiados del Grupo ad hoc sobre inmigración**, D.O.C.E. Nº C 175/170 de 16.7.90.

- **Comisión de Investigación del Racismo y la Xenofobia. Informe sobre las Conclusiones**, Oficina de Publicaciones Oficiales de las Comunidades Europeas, Luxemburgo, 1991.

- **Resolución, de 22 de febrero de 1991, sobre la armonización de las políticas de acceso a los territorios de los Estados miembros de la CE, con vistas a la libre circulación de las personas (art. 8 del Tratado CEE) y la elaboración de una convención intergubernamental entre los doce Estados miembros de la Comunidad**, D.O.C.E. Nº C 72/213 de 18.03.91.

- **Resolución sobre la entrada en vigor de los Acuerdos de Schengen**, D.O.C.E. Nº C 337/214 de 21.12.92.

- **Recurso interpuesto el 18 de noviembre de 1993 contra la Comisión de las Comunidades Europeas por el Parlamento Europeo (Asunto C-445/93)**, D.O.C.E. Nº C 1/12 de 4.1.94.

- **Fichas Técnicas sobre el Parlamento Europeo y las actividades de la Unión Europea**, Parlamento Europeo. Dirección General de Estudios, Luxemburgo, 1994.