BOLETÍN DEL MINISTERIO DE JUSTICIA

Año LXXVII · Núm. 2.261 · Marzo de 2023

ESTUDIO DOCTRINAL

LA TRANSFERENCIA INTERNACIONAL DE DATOS EN EL NUEVO MARCO DE COOPERACIÓN PENAL HISPANO-MARROQUÍ

Antonio Evaristo Gudín Rodríguez-Magariños

GOBIERNO DE ESPAÑA · MINISTERIO DE JUSTICIA

ISSN: 1989-4767
NIPO: 051-15-001-5
https://revistas.mjusticia.gob.es/index.php/BMJ

Enlaces de contacto

Contacto Boletín
Normas de publicación en el Boletín del Ministerio de Justicia

LA TRANSFERENCIA INTERNACIONAL DE DATOS EN EL NUEVO MARCO DE COOPERACIÓN PENAL HISPANO-MARROQUÍ

ANTONIO EVARISTO GUDÍN RODRÍGUEZ-MAGARIÑOS

*Doctor en Derecho. Letrado de la Administración de Justicia adscrito al Servicio Común de Ejecutorias de la Audiencia Nacional**

RESUMEN

La protección de datos constituye un aspecto fundamental para el entendimiento de las normas de cooperación en materia penal. Las nuevas tecnologías de la información habilitan un tratamiento automatizado de los datos personales que permite el acceso a los investigadores a todos los rincones de la intimidad de un importante conjunto de la población. La normativa europea en materia de protección de datos es consciente de esta realidad y exige que el tratamiento de la información obtenida en una investigación penal se lleve a efecto sobre la base de elementos objetivos y no discriminatorios, limitado a lo estrictamente necesario en orden a la prosecución del delito. Tales exigencias tienen enormes consecuencias en materia de cooperación internacional con otros países. En el caso de Marruecos, las autoridades de aquel país son conscientes de la necesidad de avanzar en estas materias, razón por la cual se han sumado al Acuerdo 108 del Consejo de Europa para la protección de las personas respecto del tratamiento automatizado de carácter personal y al segundo protocolo del Convenio de Budapest de Lucha contra la Ciberdelincuencia. A estos acuerdos se suma la ratificación recientemente del Convenio en materia de seguridad y de lucha contra la criminalidad de 13 de febrero de 2019. Se procede en el presente estudio al examen del estado de la cuestión con especial atención a los progresos llevados a efecto por este país en los últimos años en esta materia.

PALABRAS CLAVE

Marruecos-UE, cooperación internacional penal, datos de carácter personal, protección de datos, transferencia internacional de datos.

ABSTRACT

Data protection is a fundamental aspect for the understanding of the rules of cooperation in criminal matters in the European Union. New information technologies enable an automated processing of personal data that allows investigators access to all corners of the privacy of a large part of the population. European data protection law is aware of this reality and requires that the processing of information obtained in a criminal investigation be carried out based on objective and non-discriminatory elements, limited to what is strictly necessary for the prosecution of the crime. Such requirements have enormous consequences for international cooperation with other countries. In the case of Morocco, the Moroccan authorities are aware of the need to make progress in these matters, which is why they have joined the Council of Europe's Agreement 108 for the Protection of Individuals regarding Automatic Processing of Personal Data and the Second Protocol to the Budapest Convention on Combating Cybercrime. These agreements have been supplemented by the recent ratification of the Convention on Security and Combating Crime of 13 February 2019. This study examines the state of play with a particular focus on the progress made by the country in this area in recent years.

KEY WORDS

Morocco-EU, cross-border cooperation in criminal matters, personal data, data protection, international data transfer.

ABSTRACT

La protection des données est un aspect fondamental pour la compréhension des règles de coopération en matière pénale. Les nouvelles technologies de l'information permettent un traitement automatisé des données personnelles qui permet aux enquêteurs d'accéder à tous les recoins de la vie privée d'une grande partie de la population. Le droit européen de la protection des données est conscient de cette réalité et exige que le traitement des informations obtenues dans le cadre d'une enquête pénale soit effectué sur la base d'éléments objectifs et non discriminatoires, limités à ce qui est strictement nécessaire à la poursuite de l'infraction. De telles exigences ont des conséquences énormes sur la coopération internationale avec d'autres pays. Dans le cas du Maroc, les autorités marocaines sont conscientes de la nécessité de progresser dans ces domaines, c'est pourquoi elles ont adhéré à l'Accord 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et au deuxième protocole à la

Fecha de recepción: 4-11-2022. Fecha de aceptación: 15-2-2023

Convention de Budapest sur la lutte contre la cybercriminalité. Ces accords ont été complétés par la récente ratification de la Convention sur la sécurité et la lutte contre la criminalité du 13 février 2019. Cette étude examine l'état des lieux en mettant l'accent sur les progrès réalisés par le pays dans ce domaine ces dernières années.

MOTS CLÉS

Maroc-UE, coopération pénale internationale, données personnelles, protection des données.

CONTENIDO

ABREVIATURAS

ANRT	Agencia Nacional de Regulación de las Comunicaciones.
Art.	Artículo.
BOE	*Boletín Oficial del Estado*.
BORM	*Boletín Oficial del Reino de Marruecos*.
coord.	Coordinado.
T-CY	Cybercrime Convention Committee.
CNDP	Comisión Nacional para el Control de la Protección de Datos Personales.
CNDH	The National Human Rights Council of Morocco.
DGED	Direction générale des études et de la documentation Marocain.
DGST	Direction générale de la surveillance du territoire.
DOI	Digital Object Identifier.
DOUE	*Diario Oficial de la Unión Europea*.
LECrim	Ley de Enjuiciamiento Criminal.
núm.	Número.
NLSI	National Law School of India Review.
p.	Página.
REEI	*Revista Electrónica de Estudios Internacionales*.
RGDP	Reglamento General de Protección de Datos 639/2016/UE.
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea.
UE	Unión Europea
vol.	Volumen.

1. LA PROTECCIÓN DE DATOS Y EL NUEVO DE MARCO DE COOPERACIÓN INTERNACIONAL CON MARRUECOS

La cooperación jurídica internacional entre las autoridades españolas y el Reino de Marruecos ha sido siempre una cuestión central en materia de política criminal del Estado español[1]. Pese a las dificultades habidas por cuestiones externas, como puede ser el asunto del Sáhara o la soberanía de las plazas de Ceuta y Melilla, las autoridades de ambos países han sabido estar por encima de cualesquiera dificultades asumiendo una política de pragmatismo, respecto de algo en que ambos países se encuentran igualmente interesados[2]. Cuestiones tales como el terrorismo, el narcotráfico o la trata de seres humanos[3] son aspectos que no se concibe que puedan abordarse sin una

*Debo agradecer el apoyo y la atención para con este letrado del anterior magistrado de enlace José María Fernández Villalobos durante el lustro en que estuvo colaborando como magistrado de enlace de España en Marruecos con el Juzgado Central de Instrucción n.º 6. Su tiempo y dedicación me han permitido sumergirme en el entendimiento de un ordenamiento jurídico tan desconocido y complejo como es el de Marruecos. Vaya para él mi agradecimiento.

1 Como explica por testimonio de primera mano del que fuera magistrado de enlace de España Ángel Llorente, la estrategia de las autoridades de ambos países partía básicamente de la constatación de tres elementos: 1) la necesidad de establecer con Marruecos una línea rápida y eficaz para conseguir una cooperación judicial efectiva; 2) la existencia de una inequívoca voluntad política de colaboración del Gobierno marroquí, y 3) superar el alto grado de desconocimiento de los sistemas jurídicos de ambos países por los actores de la cooperación, es decir, jueces y fiscales. LLORENTE, Á., «La cooperación judicial antiterrorista entre España y Marruecos», Real Instituto El Cano, Área de Terrorismo Internacional, ARI 174/2010, 20/12/2010, p. 5.

2 En este sentido, el Tratado de auxilio judicial y cooperación en materia Penal constituyó en su momento uno de los instrumentos más avanzados en materia de cooperación internacional, muchas de cuyas previsiones como el traslado temporal de detenidos o el seguimiento de cuentas bancarias fueron traspuestas a la Directiva 141/2014 de la Orden Europea de Investigación. Las novedades más importantes que se encuentran en el régimen son la limitación de las causas de denegación por razones de orden público, la posibilidad de traslado de las autoridades de ambos países para la práctica de diligencias, la simplificación del régimen de comunicaciones entre ambos países, el régimen de remisión de solicitudes complementarias y la regulación detallada de traslado de personas detenidas. Esta última previsión constituye un referente en el ámbito de la cooperación internacional y viene precedida del acuerdo entre la Audiencia Nacional española y sus homólogos marroquíes en el caso de Hassan el Haski en el año 2009, y se reproduce en el artículo 23 la Decisión marco 2014/141/UE (BARRENECHEA, L., «Los otros "efectos colaterales" del 11 de septiembre», *Revista de Derecho Migratorio y Extranjería*, 2007, núm. 14 p. 225). Otra de las novedades es la posibilidad de la ejecución condicionada. Se previene que, cuando la solicitud no pueda ser ejecutada, o no pudiera ser ejecutada en su totalidad, las autoridades de la parte requerida informarán de ello a la mayor brevedad y las partes harán un seguimiento del caso. Este régimen de aceptación condicionada se acomoda también a la normativa existente en el Reglamento de Decomiso 2018/1805.

3 En el ámbito judicial los mecanismos de cooperación bilateral se han fortalecido considerablemente a raíz de los atentados del 11-M. Siguiendo a Barrenechea, entre estas mejoras cabe destacar: a) la creación de la figura de los magistrados de enlace; b) la reforma de los tratados bilaterales de extradición y de asistencia judicial en materia penal; c) la creación del «Cuatripartito» entre fiscalías especializadas, entre ellas la de la Audiencia Nacional y la de la Corte de Apelación

mutua colaboración a ambos lados del Estrecho[4]. Por otro lado, España y Marruecos participan de un modelo judicializado de investigación criminal en el que resulta fundamental la figura del juez instructor[5]. Ambos países reconocen también la existencia de tribunales especializados en diversas materias, como pueda ser el terrorismo, y admiten la depuración de las responsabilidades civiles en vía penal[6].

Existen también claras divergencias particularmente en razón del carácter aconfesional del Estado español frente a la oficialidad de la religión musulmana —lo que se ha traducido en la distinta visión de la situación de la mujer y en materia de discriminación sexual— y a un entendimiento propio de la naturaleza y límites del principio de seguridad y orden público[7]. También es relevante la importancia que tienen en aquel ordenamiento la equidad y la jurisprudencia de los tribunales, que se constituyen en verdadera fuente del derecho, lo que les separa del derecho continental. Con todo, la

---

de Rabat, d) el incremento del nivel de interlocución entre los diferentes actores de la cooperación judicial hispano-marroquí. BARRENECHEA, L., «Mecanismos e iniciativas de cooperación hispano-marroquí contra el terrorismo», *Revista electrónica de estudios internacionales* (REEI), 2016, núm. 31 p. 28.

4 Véase también VILCHES DE MORAGUES, P., «Ser juez en Marruecos y España». *Seminario Fundación CIDOB*. Barcelona, España, p. 130.

5 La organización judicial presenta dos niveles según la importancia del asunto: de una parte, la jurisdicción municipal, jueces comunales (municipales) y *arrondissement* (distrito) para asuntos menores, y, de otra parte, los jueces de instancia para los casos más graves. Los primeros tenían carácter temporal y eran designados por el Consejo Superior de la Magistratura por tres años, y los tribunales de primera instancia, que contaban con un presidente, varios jueces, uno de los cuales con funciones de vicepresidente, un miembro del ministerio fiscal, un secretario judicial y la secretaria de la fiscalía; por encima de esta organización se encuentran los tribunales de apelación y la Corte de casación o Corte Suprema. Existen una jurisdicción especializada administrativa y mercantil y una jurisdicción militar de excepción.

6 El modelo tradicional, que sigue en gran parte la organización judicial existente durante el protectorado, ha sido recientemente modificado por la Ley 38.15, aprobada el 24 de febrero de 2022 y publicada en el *Boletín Oficial del Estado del Reino de Marruecos* el 14 de julio de 2022 (*BORM* 7108). Esta reforma ha entrado en vigor en enero 2023 y viene precedida de una larga polémica como consecuencia de la derogación del texto primitivo por el Tribunal Constitucional en Sentencia de 8 de febrero de 2019. La piedra angular de este poder es ahora el Consejo Superior del Poder Judicial (المجلس الأعلى للسلطة القضائية), que sustituye al Instituto Superior de la Magistratura y al que la Constitución dedica el artículo 109 y los artículos 113 a 116 del texto constitucional. Es destacable la autonomía no solo del Poder Judicial, sino de la Fiscalía, tanto en cuestiones administrativas como presupuestarias. Véase https://www.chambredesrepresentants.ma/sites/default/files/loi/rapport-2l-38.150.pdf.

7 Para una aproximación a estas cuestiones véase MAKULILO, B. A, «Data Protection Regimes in Africa: too far from the European 'adequacy' standard?», *International Data Privacy Law*, 2013, vol. 3, núm. 1, pp. 42-50. Según el citado autor, resulta sorprendente que el legislador haya reconocido el carácter sensible de los datos relativos a las creencias filosóficas y religiosas, mientras que el procesamiento de este tipo de datos se presenta de ordinario en una variedad de situaciones en Marruecos (véase MAKULILO, B. A., «African Data Privacy Laws», Bremen: Springer, 2016, p. 42).

reciente firma de la Cumbre de Estambul sobre prevención y lucha contra la violencia de género ha puesto de manifiesto que ninguna de estas dificultades es insalvable, siempre que se traten dentro de un ámbito de respeto y de entendimiento de las relaciones multiculturales de la sociedad actual[8].

Estas dificultades se suman al nivel de exigencia que la Unión Europea está imponiendo en materia de protección de datos, que como veremos constituye hoy el eje de las políticas en materia de cooperación internacional en el ámbito de la investigación penal. Ciertamente, y como luego expondremos, esta protección no se refiere a todo tipo de datos personales, sino tan solo a aquellos que o bien son objeto de tratamiento automatizado, o bien, no existiendo tal tratamiento automatizado, los datos personales se vinculan con otros mediante la incorporación a un sistema informativo o archivo (art. 2 RGPD). Tal como sostienen Ustaran y García, el simple tránsito de información no supone una transferencia internacional de datos personales, para que pueda haber una transferencia internacional debe existir un tratamiento de los datos personales en el tercer país[9]. El hecho es que en las modernas investigaciones resulta esencial el acceso a bases de datos, seguimientos y controles telemáticos. Por otra parte, la incorporación de la información obtenida a archivos policiales y judiciales implica de suyo una grave restricción de los derechos de la ciudadanía y en particular al principio de presunción de inocencia[10]. Todas estas razones han determinado una regulación específica y ajustada a las circunstancias de orden público de la investigación penal constituida hoy por la Directiva 680/2016, normativa coetánea a la regulación del Reglamento General de Protección de Datos y la Ley Orgánica 7/2021, de 26 de mayo, de trasposición de aquella directiva, que imponen restricciones específicas a la transferencia internacional de datos a terceros países, como es el caso de Marruecos.

---

8 Avance que, irónicamente, no ha impedido que, habiendo sido Turquía el primer país firmante del tratado, haya sido también el primero en retirarse de este. Un decreto publicado el 20 de marzo de 2021 anunció la retirada formal de Turquía del referido Convenio. https://www.coe.int/en/web/commissioner/-/turkey-s-announced-withdrawal-from-the-istanbul-convention-endangers-women-s-rights.

9 USTARÁN, E. y GARCÍA, P., «Transferencias internacionales de datos». *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* / coord. por Artemi Rallo Lombarte, 2019, p. 459.

10 Ruiz Tarrías cita en este sentido la STJUE en el asunto Bodil Lindqvist, en la que se aborda la incorporación de información a una página web: «El concepto de "tratamiento" de dichos datos que utiliza el artículo 3, apartado 1, de la Directiva 95/46, éste comprende, con arreglo a la definición del artículo 2, letra b), de dicha Directiva, "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales". Esta última disposición enumera varios ejemplos de tales operaciones, entre las que figura la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos. De ello se deriva que la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole». RUIZ TARRÍAS, S., «La sentencia del Tribunal de Justicia de la Unión Europea en el Caso Schrems II o cómo los datos personales pueden terminar viajando sin equipaje». *Revista Española de Derecho Europeo,* núm. 76 | octubre-diciembre de 2020, núm. 76. p. 117. DOI:10.37417/num_76_2020_532.

Pese a todas estas dificultades, parece que se empiezan a observar pasos decididos en orden a equiparar a ambos ordenamientos jurídicos en lo referente a la protección de datos[11].

En este contexto de aproximación entre las legislaciones de ambos países, el pasado día de 7 de abril de 2023 se publicó el acuerdo hispano-marroquí en materia de seguridad y de lucha contra la delincuencia[12]. Este acuerdo se enmarca en la línea de colaboración que entre ambos países se ha abierto en los últimos meses y viene precedido, además, por la ratificación por Marruecos en mayo de 2023 del Segundo protocolo de lucha contra la cibercriminalidad[13].

En el caso del acuerdo en materia de seguridad, resultan especialmente novedosas las previsiones contenidas en su artículo noveno, en el que, luego de condicionar el uso de los datos únicamente para el fin y según las condiciones determinadas por la parte requerida, se prevé en su apartado segundo que las partes asegurarán la protección de los datos ofrecidos frente al acceso, modificación, divulgación o destrucción no permitidos de acuerdo con su legislación nacional. Asimismo, se comprometen a no ceder los datos personales a ningún tercero distinto del órgano solicitante de la parte requirente, o, en caso de solicitarse por esta, solo podrán transmitirse previa autorización del requerido. Se establece, por último, que cualquier parte podrá aducir, en cualquier momento, el incumplimiento por la parte requirente, como causa para la suspensión inmediata de la aplicación del Convenio y, en su caso, de la terminación automática de aquel[14].

El otro gran reto de las autoridades marroquíes es la incorporación de Marruecos al segundo protocolo del Convenio de Budapest de lucha contra la cibercriminalidad y su protocolo adicional sobre xenofobia y racismo. Como luego se expondrá, este Convenio al tiempo que facilita el acceso a los datos de las comunicaciones, exige un alto nivel de garantías en materia de protección de datos.

---

11 En 2018, la Comisión Nacional de Control de la Protección de Datos Personales de Marruecos (CNDP) presentó los resultados de un estudio que lideró con la delegación de la Unión Europea en Marruecos. Este estudio recomendaba un escenario que pretende una integración «moderada» en el esquema del Reglamento General de Protección de Datos. Este esquema implicaría un cierto número de enmiendas a la ley para reducir las lagunas que la legislación marroquí presenta en el momento actual, teniendo en cuenta, al mismo tiempo, las particularidades locales (BOSSI, M., «Processing data to Third Countries or International Organizations», *Arribat – International Journal of Human Rights,* septiembre de 2021, vol. 1, cuestión 2, pp. 176-186 y 139.

12 Convenio entre el Reino de España y el Reino de Marruecos sobre cooperación en materia de seguridad y de lucha contra la delincuencia, hecho en Rabat el 13 de febrero de 2019. Disposición 5595, del *BOE* núm. 83, de 7 de abril de 2022.

13 Accesible desde: https://www.coe.int/fr/web/rabat/-/renforcement-de-la-cooperation-et-de-la-divulgation-de-preuves-electroniques.

14 Convenio entre el Reino de España y el Reino de Marruecos sobre cooperación en materia de seguridad y de lucha contra la delincuencia, hecho en Rabat el 13 de febrero de 2019, *BOE* núm. 83, de 7 de abril de 2022.

Dichos acuerdos son consecuencia de un esfuerzo de las autoridades de aquel país para integrarse en el complejo ordenamiento de la Unión Europea en materia de protección de datos, voluntad que se ha concretado en la ratificación por Marruecos del Convenio 108 del Consejo de Europa para la protección de las personas respecto del tratamiento automatizado de datos de carácter personal[15].

Las autoridades de España y Marruecos son conscientes de que la extensión y alcance de la cooperación en la lucha contra la criminalidad exigen un marco de confianza para hacer posible el traslado de grandes volúmenes de información de carácter sensible, cuya entrega a otro país sin las debidas garantías puede poner en riesgo los derechos y libertades de sus ciudadanos.

En lo que se refiere al ordenamiento español, el acuerdo viene precedido además por la aprobación de la Ley 7/2021, de 26 de mayo, texto legal largamente esperado, que desarrollaba las previsiones contenidas en la Directiva de protección de datos, desarrollo legal que a la postre ha permitido la ratificación de un acuerdo que se remonta a tres años antes y que se encontraba ciertamente paralizado en su tramitación[16].

---

15 Debe recordarse, sin embargo, que existe un salto cualitativo en materia de protección de datos entre la normativa del Convenio 108 del Consejo de Europa. Como se señala en el *Manual de Legislación Europea en Materia de Protección de Datos*, la Carta no solo garantiza el respeto a la vida privada y familiar (artículo 7), sino que también establece el derecho a la protección de datos (artículo 8), elevando explícitamente el nivel de dicha protección al de derecho fundamental en el derecho de la UE: «No importa si los datos personales en cuestión tienen que ver con la vida privada de una persona física, si son sensibles o si se ha molestado a los interesados de algún modo. Para que sea lícita, la injerencia ha de cumplir todas las condiciones establecidas en el artículo 52, apartado 1, de la Carta» (*Manual de Legislación Europea en Materia de Protección de Datos*, Oficina de Publicaciones de la Unión Europea, 2018, p. 48). Y es que, a diferencia de la legislación del Consejo de Europa, la cual se haya orientada exclusivamente a la protección del derecho a la privacidad, la legislación de la Unión Europea en materia de protección de datos se proyecta y se extiende no solo a la protección de la intimidad de las personas, sino también a cualesquiera otros derechos o intereses difusos, estando directamente vinculada a la dignidad de la persona. Nos encontramos ante la protección del individuo frente a la detentación y manipulación del dato identitario, entendido este como elemento de dominación e interferencia en la vida privada de las personas, particularmente en aquellos supuestos en que es objeto de un tratamiento automatizado. Es por esto por lo que presenta un carácter marcadamente instrumental, siendo objeto de una protección específica y concreta por agencias independientes de carácter administrativo y solo indirectamente a través de los tribunales.

16 Ante esta laguna normativa, la disposición transitoria cuarta de la Ley 3/2018, de 5 de diciembre, había previsto que el tratamiento de datos personales para fines de la investigación del delito continuara rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al derecho español. Estos preceptos contenían una prohibición de las investigaciones prospectivas, distinguiendo el acceso a datos sensibles según la acción policial se dirija a la investigación de un delito o al mantenimiento del orden público en general y la seguridad pública que se regulan ahora con carácter restrictivo en el artículo 13 de la Ley 7/2021, que contiene una remisión normativa a otras normas con rango de ley salvo aquellos supuestos de concreto peligro para intereses vitales y derechos fundamentales.

Se observa de igual modo, en estos últimos años, una extensión generalizada de las previsiones de protección de datos en todos los textos legales que afectan al proceso penal, véase el caso del Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, por el que se establece una cooperación reforzada en orden a la creación de la Fiscalía Europea que dedica a esta materia los artículos 47 a 89, una cuarta parte de los ciento veinte que contiene la ley. Este novedoso texto legal hace prever que en los próximos años los aspectos relativos a la protección de datos asuman un rol dominante en el derecho procesal penal. Constituyendo el objeto de la protección de datos, el tratamiento de la información relativa a una persona física identificada o identificable, resulta manifiesto que este objeto coincide cabalmente con los fines propios de la investigación criminal, que no son otros que la identificación de los responsables de las acciones penales[17].

Por todas estas razones, la legislación de protección de datos se sitúa, así, en el epicentro de la cooperación jurídica internacional, hecho que no es desconocido por las autoridades marroquíes, las cuales han apostado de forma firme y decidida por el desarrollo normativo en estas materias, pero en el que, como veremos, habremos de encontrar numerosos aspectos originales que deberán ser tenidos también en cuenta en orden a prestar la adecuada reciprocidad.

El objeto del presente trabajo se centrará en la extensión y límites de las transferencias internacionales de datos entre Marruecos y la Unión Europea, así como las posibilidades que los nuevos instrumentos de cooperación ofrecen para llevar a efecto estas transferencias. Se tratará en particular de las transferencias de información electrónicamente almacenada a la vista de la reciente firma por ambos países del segundo protocolo adicional al convenio de Budapest de cibercriminalidad.

17 Como hemos expuesto en otras ocasiones, las cuestiones de protección de datos atienden fundamentalmente a un derecho prestación de carácter instrumental que se proyecta sobre la dignidad de la persona y sobre el resto de los derechos fundamentales. Su tutela se sitúa en sede administrativa y se reconduce a los derechos de acceso, rectificación, cancelación, supresión y limitación. Así resulta expresamente de lo previsto en el expositivo 16 del Reglamento de Protección de Datos, que expresamente excluye la regulación de la protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con actividades excluidas del ámbito del derecho de la Unión, como las actividades relativas a la seguridad nacional. Véase GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información», *La Ley Penal* núm. 125, Sección Estudios, abril-marzo de 2017, p. 3..

2. LA COOPERACIÓN EN MATERIA PENAL Y LA PROTECCIÓN DE DATOS DE LOS CIUDADANOS DE LA UNIÓN EUROPEA MÁS ALLÁ DE SUS FRONTERAS

La cooperación internacional en materia penal viene condicionada en gran medida por la extensión y alcance de la transmisión de información, y muy en particular por las políticas de protección de datos que está marcando la Unión Europea. En el caso de Marruecos, su aprobación del segundo protocolo del Convenio 108 del Consejo de Europa ha supuesto un paso decidido en orden a la equiparación de su normativa interna con la existente en la Unión Europea[18], pero no agota todas las exigencias de la normativa europea. El Convenio 108 se orienta fundamentalmente a la protección de los datos personales en relación con la privacidad de las personas, mientras que el legislador europeo en el art. 8 CDFUE ha dotado a la protección de datos del carácter de un derecho fundamental autónomo dirigido a la tutela de las personas frente a la detentación y manipulación del dato identitario, particularmente en aquellos supuestos en que los datos son objeto de un tratamiento automatizado[19].

Como he sostenido en otros foros, nos encontramos ante un derecho-prestación o de carácter instrumental que se proyecta no solo sobre el derecho a la privacidad, sino sobre cualquier otro derecho subjetivo. El derecho a la protección de datos presenta un carácter instrumental en la medida en que el solo dato identitario carece de por sí de un contenido propio para hacerlo objeto de protección. La identidad que proporcionan los datos de carácter personal es el medio que permite reconocer al resto de los derechos fundamentales dotándoles de la exterioridad propia de cualquier derecho o interés legítimo y hacerles merecedores de un tratamiento particularizado. Se entiende, así, que la protección de datos admite una distinta protección según cual sea la sensibilidad del dato objeto de tratamiento. Este entendimiento justifica también que su ejercicio se haga valer ante un órgano administrativo como es la Agencia de

18 La Comisión ha señalado indirectamente su apoyo a la estrategia sugerida, declarando que «la adhesión al Convenio 108 es un factor importante que la Comisión Europea debe tener en cuenta en su evaluación de la adecuación», de conformidad con el artículo 45 del RGPD. También ha señalado, en efecto, su apoyo al Convenio del Consejo de Europa en sentido más amplio, declarando oficialmente que «alienta la adhesión de terceros países al Convenio 108 del Consejo de Europa y a su Protocolo adicional» y «promoverá activamente la rápida adopción» del Convenio 108 «con vistas a que la UE sea parte». Además, la Comisión reconoce el «papel crucial» que el Convenio ya ha desempeñado «en la difusión del "modelo europeo de protección de datos" a nivel mundial», y predice que el impacto práctico que de aquel puede esperarse sea mucho mayor. Comunicación de la Comisión al Parlamento Europeo y el Consejo, «Exchanging and Protecting Personal Data in a Globalised World», COM(2017) 7 final, 10 de enero de 2017, pp. 11-12. Sobre este particular véase BYGRAVE, L., «The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects», *Computer Law & Security Review*, abril de 20211 vol. 40, Norwegian Research Center for Computers and Law, Department of Private Law, University of Oslo, Norway, p. 12.

19 GONZÁLEZ FUSTER, G., *The Emergence of Personal Data Protection as a Fundamental Right of the European Union, Law, Science, Technology and Society*, Brusssels: Springer, 2014, p. 256..

Protección de Datos y que la habilitación a su acceso se haga extensiva no solo a las autoridades judiciales, sino también a la Fiscalía, a la Agencia Tributaria e incluso a las fuerzas y cuerpos de seguridad del Estado en orden al cumplimiento de los fines que les son propios. Solo cuando es reconocible una conexión del dato identitario con un derecho fundamental superior se hace precisa la intervención de las autoridades judiciales[20].

Este nivel de exigencia se encuentra especialmente presente en la jurisprudencia del TJUE en los casos Schrems I y II. En estas resoluciones, el alto tribunal europeo declaró que es responsabilidad del transferente de los datos como del receptor evaluar si el nivel de protección exigido por la legislación de la UE se respeta en el país tercero de que se trate, determinando en particular si las garantías proporcionadas por ese tercer Estado pueden cumplirse en la práctica. En caso contrario, deberá evaluar si pueden proporcionarse medidas complementarias para garantizar un nivel de protección equivalente al establecido en el marco europeo, y si la legislación del país tercero no afectará a estas medidas adicionales para evitar su efectividad[21]. Como trataremos luego más extensamente, esta pretensión es exorbitante en un mundo virtual en el que es difícil conocer el alcance de la jurisdicción y en que el principio de ubicuidad es la regla general en orden a la investigación de los delitos como consecuencia del carácter compartido de la información que es objeto de tratamiento.

La normativa europea en relación con la transferencia internacional de datos en el ámbito de la investigación penal presenta, además, particularidades propias que son consecuencia de los compromisos internacionales en materia de cooperación judicial. Estas son tratadas en un instrumento *ad hoc*, diferenciado y distinto del Reglamento 679/2016, de 30 de marzo (en adelante, RGDP), cual es la Directiva 680/2016, de la misma fecha, promulgada al tiempo de aquel.

El principio fundamental establecido en la directiva no es distinto del establecido en el artículo 44 del RGDP, según el cual la divulgación de datos personales a terceros países no deberá menoscabar el nivel de protección garantizado por la legislación de protección de datos europea. Sin embargo, tratándose de datos especialmente dirigidos a la investigación del delito, el ordenamiento jurídico reconoce un conflicto inmanente entre el hecho de la investigación de los hechos y los derechos de las personas afectadas por el tratamiento. Dicho conflicto se concreta en materia de cooperación judicial, además, en las exigencias de cumplimiento de los compromisos asumidos por los Estados y la propia Unión Europea en orden a la lucha frente a la criminalidad.

---

20 GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información», *La Ley Penal*, núm. 125, Sección Estudios, marzo-abril de 2017, p. 4.

21 STJUE de 16 de julio de 2020, Schrems II (C-311/18, ECLI:EU:C:2020:559), epígrafe 91, y 6 de octubre de 2015, Schrems I (C-362/14, EU:C:2015:650), epígrafe 72.

Es por esto por lo que, en materia de investigación penal, las transferencias de datos a terceros países o a organizaciones internacionales, como es el caso de Marruecos, se hacen depender de un doble condicionante. De una parte, los compromisos asumidos para la lucha contra el delito —compromisos que no son distintos a los establecidos en el orden interno por la propia directiva—, y por el reconocimiento de un nivel de protección garantizado por los Estados miembros.

El primer condicionante atiende al principio de necesidad, esto es, que el acceso y tratamiento a la información sea estrictamente necesario para la realización por la autoridad competente de la actividad que le es propia, al objeto de asegurar la prevención, investigación, detección o enjuiciamiento de infracciones penales respecto de hechos que son constitutivos de delito, y la prevención frente a las amenazas frente a la seguridad pública[22].

La segunda de las exigencias requeridas para una transferencia internacional de datos es que existan garantías adecuadas en orden al tratamiento de los datos, bien mediante una decisión de adecuación que dictamine que el ordenamiento en cuestión ostenta un nivel de garantías adecuado, bien mediante la prestación de las garantías bastantes, o bien mediante el reconocimiento de una situación jurídica particularizada.

Concretamente, el expositivo 64 de la directiva señala que «dichas transferencias pueden tener lugar en los casos en que la Comisión haya decidido que el tercer país o la organización internacional en cuestión garantizan un nivel adecuado de protección, o cuando se hayan ofrecido unas garantías apropiadas o se apliquen excepciones para situaciones específicas. Cuando los datos personales sean transferidos desde la Unión a responsables y encargados del tratamiento u otros destinatarios de terceros países u organizaciones internacionales, no debe verse menoscabado el nivel de protección de las personas físicas que se garantiza en la Unión mediante la presente Directiva, ni tampoco en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados del tratamiento del mismo u otro tercer país u organización internacional»[23].

De este modo, la transferencia internacional de datos para un proceso de investigación penal en aquellos países que no tienen un sistema jurídico integrado en la Unión Europea vendrá directamente condicionada por el grado de desarrollo de un sistema de garantías en materia de protección de datos. En el caso de Marruecos, al carecer de una declaración de adecuación, exige un examen particularizado para cada acción de cooperación, como ha sucedido en el caso del convenio hispano-marroquí en materia de seguridad de 13 de febrero de 2019. En este se establece por adelantado un

22 En estos casos se distingue si estos datos son directamente accesibles, por haberlos hecho públicos el propio interesado o si este ha excluido su acceso a tercero (art. 13.1.c de la LO 7/2021). Solo en este último caso, datos excluidos, estamos ante datos que afectan estrictamente a la privacidad de las personas (véase art. 588 *ter* i LECrim). Estas previsiones deben completarse con las contenidas en el art. 39 de la directiva, en relación con los principios de proporcionalidad y adecuación de la medida.

23 Directiva de Protección de Datos, Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *DOUE* 4/5/2016, L 119/89.

régimen al que habrán de sujetarse la recepción y transmisión de esta clase de información que afecte a la seguridad. Condicionantes de los que el Tratado de Auxilio y Cooperación judicial en material penal se encuentra ausente.

Sin embargo, como luego veremos, el segundo protocolo de Budapest va a establecer un régimen de excepción, que determinará como garantías bastantes y adecuadas para el acceso a los datos de un entorno virtual de otro Estado las establecidas en el propio convenio. La delimitación de este entorno virtual se fundamenta en el principio de que no puede haber espacios vacíos a la acción de los Estados y exige un compromiso mutuo en orden a la lucha contra el delito en la red, lo que habilita ciertas excepciones al principio de territorialidad, excepciones que, como veremos, van mucho más allá del concepto tradicional de cooperación judicial hasta hoy conocida.

Ciertamente, la aplicación del protocolo admite un diferente conjunto de salvaguardias, según si el tercer país destinatario de los datos se encuentra dentro de un ordenamiento jurídico integrado como es la Unión Europea. Sin embargo, tales condicionantes no pueden extenderse a un régimen más restrictivo respecto a la protección de datos que el establecido en el artículo 14 del Convenio. Este precepto establece un sistema de garantías de mínimos respecto de la información obtenida en la red, propio y distinto al establecido en la normativa general de protección de datos. En este sentido, el apartado 226 señala que el objetivo del artículo 14 es establecer las garantías mínimas adecuadas que permitan la transferencia de datos personales entre las partes, pero no impone la armonización de los marcos jurídicos nacionales para el tratamiento de datos personales en general, ni del marco para el tratamiento de datos personales a efectos de la aplicación de la ley penal. No autoriza, en concreto, a que las partes puedan imponer requisitos adicionales para las transferencias de datos más allá de los permitidos específicamente en el propio acuerdo.

Esto no impide, sin embargo, que las partes, con fundamento en el protocolo, hagan reservas o exijan garantías de protección de datos más estrictas que las previstas en los apartados 2 a 15, pero siempre con una habilitación expresa realizada al tiempo de firmar el protocolo[24]. En este sentido, el informe explicativo al segundo protocolo, —teniendo en mente quizás, la jurisprudencia del caso Schrems II— significa como ejemplo que una Parte no puede condicionar la transferencia en un caso individual a que la Parte solicitante tenga el equivalente a una autoridad de protección de datos especializada. Resultará bastante el cumplimiento de las exigencias que en materia de protección de datos se contienen en el protocolo[25].

En uno y otro caso resultará decisivo el entendimiento del sistema de protección de datos en orden a la valoración del alcance y extensión de las garantías exigidas por un país tercero que recabe la cooperación conforme a los tradicionales instrumentos de cooperación.

---

24 Explanatory Report, apartado 226, accesible: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b.

25 Explanatory Report, apartado 230, accesible: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b.

3. LA LEGISLACIÓN MARROQUÍ EN MATERIA DE PROTECCIÓN DE DATOS

Las autoridades de Marruecos, como venimos indicando, se encuentran seriamente concienciadas en esta materia. La reforma constitucional de julio de 2011 reafirmó el compromiso de Marruecos para la construcción de un Estado de derecho democrático y moderno que proteja los derechos humanos y las libertades individuales y colectivas. Entre estos derechos se encuentra el derecho a la intimidad. En su artículo 24, la nueva Constitución del Reino de Marruecos reconoce este derecho fundamental en los siguientes términos: «Toda persona tiene derecho a la protección de su vida privada». El preámbulo de la Constitución marroquí de 2011 establece que el Reino de Marruecos se compromete a proteger y promover las medidas de derechos humanos y el derecho internacional humanitario «en su indivisibilidad y universalidad». Por su parte el artículo 27 de la Constitución marroquí señala que «el derecho a la información sólo puede ser limitado por la ley, con el fin de garantizar la protección de todo lo que concierne a la defensa nacional, la seguridad interior y exterior del Estado, así como la vida privada de las personas, para evitar la violación de los derechos y libertades establecidos en esta Constitución»[26].

La adhesión de Marruecos a la legislación internacional sobre el derecho a la protección de los datos personales, particularmente al Convenio 108 del Consejo de Europa, y la consagración de este derecho en la Constitución conforman una base real para la armonización de su derecho interno con los principios y disposiciones establecidos en estos textos[27].

La legislación en la materia se contiene en la Ley 09-08 promulgada por el Dahir 1-09-15, de 18 de febrero de 2009 (22 safar 1430), relativa a la protección de las personas en lo que respecta al tratamiento de sus datos (*BORM* 5714, 5 de marzo 2009). Se establecen en esta norma los principios fundamentales en la materia y los medios de aplicación de la protección de las personas en lo que respecta al tratamiento de datos de carácter personal. Esta ley se completa con el Decreto 2-09-165, de 21 de mayo de 2009, que sirve de norma de desarrollo.

Desde su promulgación, el legislador marroquí ha venido estableciendo un régimen jurídico de protección de los datos personales mesdiante la adopción diversas normas que desarrollan la Ley 09-08, pero que no quiebran los principios fundamentales recogidos en aquella norma[28]:

---

26 Dahir 1-11-91 du 27 Chaabane 1432 (29 de julio de 2011).

27 El preámbulo afirma que los tratados internacionales debidamente ratificados tienen la primacía sobre el derecho nacional. Este principio, sin embargo, resulta bastante relativo, pues lo es en el marco de las disposiciones de la Constitución y las leyes del Reino, con respecto a su identidad nacional inmutable. Esta ambigua redacción, tal como como sostiene Benchemsi, hace que la afirmación de la supremacía de los tratados internacionales sobre el derecho nacional sea poco clara. Véase BENCHEMSI, A., «Morocco: Outfoxing the Opposition», *Journal of Democracy* enero de 2012, núm. 57, p. 61. http://www.journalofdemocracy.org/sites/default/files/Benchemsi-23-1.pdf.

28 Véase, WALLE, E., «Le Maroc adopte une loi sur la protection des données personnelles». *Gazette du Palais*, 21/22 de octubre de 2009, p. 2935.

— Ley 31-08, promulgada por el Dahir 1-11-03, de 18 de febrero de 2011, 14 Rabii 1432, promulgando medidas de protección (*BORM* 5932, 7 de abril de 2011).

— Ley 132-13, por la que se aprueba el protocolo adicional al del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como la protección de las personas en relación con el tratamiento automatizado de datos personales, promulgado por el Dahir 1-14-136, 3 Chaoual 1435 (31 de julio de 2014) (*BORM* 6288, 4 de septiembre de 2014).

— Ley 88-13, promulgada por el Dahir 1-16-122, de 10 de agosto de 2016, 6 Kaada 1437, relativa a la prensa y publicaciones (*BORM* 6522, 1 de diembre de 2016).

Es también de tener en cuenta la Ley 53-05, promulgada por el Dahir 1-07-129, de 30 de noviembre de 2007, 19 Kaada 1428, relativa a intercambio electrónico de datos jurídicos (*BORM* 5584, 6 de diciembre de 2007). Estas normas se encuentran inspiradas en la normativa europea vigente entonces, concretamente la Directiva 95/46/CE del Parlamento Europeo y del Consejo, la cual reproduce en sus aspectos fundamentales. Se echan en falta, no obstante, previsiones fundamentales respecto al derecho actualmente vigente constituida, por el Reglamento 679/2016 y la Directiva 680/2016, tanto en materia de derecho al olvido como en lo relativo a la transferencia internacional de datos.

Respecto a la definición de los datos de carácter personal, se tienen por tales toda información de cualquier naturaleza, independientemente del soporte, incluidos el sonido y la imagen, sobre persona física identificada e identificable. En lo que se refiere a los datos personales recogidos y tratados con fines de prevención y represión de los delitos y las faltas, la aplicación de la legislación de protección de datos debe limitarse a las condiciones establecidas por la ley o el reglamento que establece el fichero en cuestión. En particular, el artículo 6 de la ley, en su apartado a), limita el derecho de información de la recogida de datos a los supuestos datos personales cuya recogida y tratamiento son necesarios para la defensa nacional, la seguridad interior o exterior del Estado, la prevención o la represión de la delincuencia

De este modo, y a diferencia del contexto europeo, en el que existe una normativa específica y de carácter general para la protección de datos en la investigación penal —constituida, hoy, por la Directiva 680/2016, de 30 de marzo, y en España por la Ley Orgánica 7/2021, de 26 de mayo—, en el caso de Marruecos dependerá no de una regulación general, sino de una regulación particular para cada tipo de fichero. La norma de creación del fichero determinará el responsable del tratamiento, la condición de legitimidad del tratamiento, la finalidad o las finalidades del tratamiento, la categoría o las categorías de personas afectadas y los datos o las categorías de datos que les conciernen, el origen de los datos, los terceros o las categorías de terceros a los que pueden comunicarse los datos y las medidas que deben adoptarse para garantizar la seguridad del tratamiento. Se someterá al dictamen previo de la Comisión Nacional de Protección de Datos (CNPD)[29].

29 Señala el apartado 2 del artículo 4: «Aux données à caractère personnel recueillies et traitées dans l'intérêt de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat. Elle ne

Esta ley no se aplica tampoco a los datos personales recogidos y tratados en interés de la defensa nacional y la seguridad interior o exterior del Estado, previsiones que se corresponden con las contenidas en el artículo 2.2.b del Reglamento y en el artículo 2 apartado c) de la Ley Orgánica 3/2018, de 5 de diciembre, sin embargo, no existen previsiones específicas en lo que se refiere al tratamiento y conservación de datos sensibles relativas al proceso comunicativo similares a las contenidas en el artículo 15, apartado 1, de la Directiva 2002/58.

Esta legislación deberá interpretarse a luz de la Convención 108 del Consejo de Europa y sus protocolos adicionales, normativa ratificada por Marruecos el 1 de septiembre de 2019, que exigirá una modificación de estas normas particularmente en orden a reforzar la capacidad del Centro Nacional de Protección de Datos (CNPD)[30] y en relación con las garantías que deban adoptarse para la transferencia internacional de datos[31].

El tratamiento se define en la Ley 09-08 como «toda operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, aplicadas a datos personales, como la recogida, registro, organización, modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de puesta a disposición, cotejo o interconexión, así como el bloqueo, la supresión o la destrucción» (art. 1, párrafo 2). Con esta definición, el legislador ha querido abarcar todas las posibilidades de tratamiento que pueden aplicarse a los datos personales para ofrecer la protección más adecuada a los ciudadanos.

---

s›applique aux données à caractère personnel recueillies et traitées à des fins de prévention et de répression des crimes et d´lits que dans les conditions fixées par la loi ou le règlement qui crée le fichier en cause; ce règlement précise le responsable du traitement, la condition de légitimité du traitement, la ou les finalités du traitement, la ou les catégories de personnes concernées et les données ou les catégories de données s'y rapportant, l'origine de ces données, les tiers ou les catégories de tiers auxquels ces données peuvent être communiquées et les mesures à prendre pour assurer la sécurité du traitement. Il est soumis à l'avis préalable de la Commission nationales». A los datos personales recogidos y tratados en interés de la defensa nacional y la seguridad interior o exterior del Estado. Se aplicará a los datos de carácter personal recogidos y tratados con fines de prevención y represión de delitos y las faltas, únicamente en las condiciones establecidas por la ley o el reglamento por el que se cree el fichero en cuestión; el reglamento especificará el responsable del tratamiento, la condición de legitimidad del tratamiento, la finalidad o finalidades del tratamiento, la categoría o categorías de interesados y los datos o categorías de datos relativos a estos, el origen de los datos, los terceros o categorías de terceros a los que pueden comunicarse los datos y las medidas que deben adoptarse para garantizar la seguridad del tratamiento. Se someterá al dictamen previo de la Comisión Nacional.

30 Véase El Hourri, A., «Protection des donées pesonnelles: le Maroc vers la ratification de la "Convention 108"», *Medias* 24, publicado el 14/02/2022, modificado el 16/02/2022, https://medias24.com/2022/02/14/protection-des-donnees-personnelles-le-maroc-ratifie-la-convention-108/ (consulta: octubre de 2022).

31 https://rm.coe.int/16806c1abe.

El eje central de esta materia viene constituido por la información y el consentimiento. El consentimiento es una expresión de voluntad libre, específica e informada por la que el interesado acepta que se traten los datos personales que le conciernen. De este modo, y al igual que la normativa europea, el silencio o la inacción no deben equipararse al consentimiento. De acuerdo con el artículo 4 de la Ley 09-08, los datos personales solo pueden ser tratados si el interesado ha dado su consentimiento inequívoco a la operación o las operaciones previstas[32].

El tratamiento de datos personales debe tener una finalidad claramente definida. Al igual que sucede en la Unión Europea, solo podrá recogerse para fines específicos y no podrá ser objeto de un tratamiento posterior incompatible con dichos fines.

La recogida de los datos está también limitada por los principios de proporcionalidad y equidad:

— El principio de proporcionalidad implica que los datos personales recogidos deben ser adecuados para la finalidad del tratamiento. Así, los datos deben ser «adecuados, pertinentes y no excesivos en relación con los fines para los que se tratan» (Ley 09-08, art. 3, párrafo 1.c).

—Junto con el principio de proporcionalidad el legislador marroquí, siguiendo el orden de fuentes que es propio de este ordenamiento jurídico recoge el principio de equidad en el tratamiento de datos. Este es un principio fundamental que debe subyacer a cualquier operación de tratamiento de datos personales. Supone garantizar que los datos se recogen de forma justa, es decir, que los interesados están bien informados y que se respetan sus derechos. También es necesario garantizar la protección de los datos contra cualquier violación que pueda provenir de terceros, poniendo los recursos humanos y técnicos adecuados.

Para la obtención de estos objetivos, el legislador marroquí ha establecido una serie de derechos semejantes a los derechos «ARCO» contenidos en la derogada legislación española de 1999 en materia de protección de datos de carácter personal:

— Consentimiento. El derecho del interesado a dar o negar su consentimiento permite a las personas mantener el control sobre su intimidad y sus datos personales y es manifestación del ámbito de autodeterminación personal que corresponde a toda persona.

32 Una de las peculiaridades del ordenamiento marroquí es la prohibición de la realización de ofertas prospectivas. La Ley 09-08 se opone expresamente a este tipo de prácticas abusivas y regula el modo de presentar ofertas no solicitadas al consumidor de forma restrictiva al objeto de proteger la intimidad de los ciudadanos frente a intromisiones inoportunas en su espacio privado (teléfono, correo electrónico, etc.). Así, el artículo 9 permite a cualquier persona cuyos datos personales sean tratados oponerse, de forma gratuita, a la utilización de sus datos con fines de prospección comercial. Además, el artículo 10 afirma este derecho al prohibir la comercialización directa por medio de aparatos de llamada automática, fax o correo electrónico o tecnología similar que utilice, en cualquier forma, los datos de contacto de una persona física que no haya expresado su consentimiento libre y específico para recibir comercialización directa por ese medio.

— Derecho a la información en el momento de la recogida. Toda persona cuyos datos personales vayan a ser tratados tiene derecho a ser informada de forma precisa, expresa e inequívoca sobre el uso o almacenamiento de sus datos. Este derecho a la información abarca también al organismo que recoge la información y a los destinatarios. Además, cuando la persona responde a un cuestionario, debe ser informada de si la respuesta a una determinada pregunta es obligatoria o facultativa.

— Derecho de acceso. Este derecho está reconocido por el artículo 7 de la Ley 09-08. Permite a cualquier persona acceder a la información sobre ella para asegurarse de que es exacta. Dicho derecho está directamente relacionado con la obligación de los responsables de tratamiento a que los datos se recopilen y procesen de manera justa, legítima y transparentes conforme a las previsiones contenidas en el artículo 23 de la ley a las que luego aludiremos.

— Derecho de rectificación. Como complemento del derecho de acceso, este derecho permite a los interesados exigir la rectificación de los datos que les conciernen, especialmente cuando son inexactos o incompletos. Este derecho se ejerce mediante una solicitud dirigida al responsable del tratamiento, que está obligado a responder en un plazo de 10 días, sin imponer ningún coste.

Como contrapartida se enuncian las obligaciones de los responsables del tratamiento de datos:

— Obligación de obtener el consentimiento del interesado. Se trata de una obligación que se deriva del derecho de los interesados a la protección de sus datos personales y es un requisito previo indispensable para cualquier tratamiento previsto.

— Declaración previa. Salvo en determinados casos que no requieren autorización previa, el tratamiento de datos personales debe ser objeto de una declaración previa ante la Comisión Nacional de Control de la Protección de Datos Personales (CNDP). Esta declaración previa permite a la CNDP supervisar la protección de los datos personales y asegurarse de que el responsable del tratamiento cumple las disposiciones de la Ley 09-08.

— Autorización previa. Algunas operaciones de tratamiento, debido a su especificidad, no requieren una declaración previa del responsable del tratamiento, sino una autorización previa emitida por la CNDP y, en su caso, la previa comunicación al interesado (art. 5.4 Ley 09-08). Este es el caso, en particular, del tratamiento de «datos sensibles», como sería el tratamiento de datos relativos a delitos, condenas o medidas de seguridad, así como el tratamiento de datos que contengan el número del documento nacional de identidad del interesado.

— Obligaciones de confidencialidad, seguridad del tratamiento y secreto profesional. En virtud de lo dispuesto en el artículo 23 de la Ley 09-08, el responsable del tratamiento está obligado a aplicar todas las medidas técnicas y organizativas

para proteger los datos personales con el fin de evitar que sean dañados, modificados o utilizados por un tercero no autorizado a acceder a ellos. Estas medidas deben reforzarse en el caso de los datos sensibles o de los datos relativos a la salud, de conformidad con lo dispuesto en el artículo 24 de la ley. Se aplican no solo al responsable del tratamiento, sino también a cualquier encargado del tratamiento en el que se deleguen las tareas del responsable. Además, el artículo 26 impone una obligación de secreto profesional al responsable del tratamiento de datos personales y a las personas que, en el ejercicio de sus funciones, tengan conocimiento de datos personales.

— Derecho a oponerse a la comercialización directa (art. 59 Ley 09-08). La comercialización o *marketing* directo es el envío de cualquier mensaje destinado a promover, directa o indirectamente, bienes, servicios o la imagen de una persona que vende bienes o presta servicios. Este es un punto en el que la legislación marroquí se presenta más tajante que la europea, proscribiendo en absoluto cualquier tipo de práctica indiscriminada tendente a la captación de clientes.

Esta legislación se muestra hoy obsoleta en relación con el RGPD (Reglamento General de Protección de Datos) que entró en vigor en 2018, el cual añadió una serie de nuevos derechos que asisten a los individuos para la protección de sus datos personales. Estos son fundamentalmente el derecho de portabilidad, la limitación del tratamiento y el derecho al olvido, que sustituye al de cancelación, y que constituye hoy en día la piedra angular de la nueva ordenación en materia de protección de datos[33].

El derecho a la portabilidad reconoce al interesado la facultad de obtener los datos que ha proporcionado a un tercero en un formato estructurado, de uso común y de lectura mecánica, supone una consecuencia necesaria del derecho de acceso a la información. Lo mismo cabe decir de la limitación del tratamiento, que se encuentra implícita también en las obligaciones generales del responsable del tratamiento tal como se contienen en el artículo 23 de la Ley 09-08.

Cuestión distinta es la relativa al derecho al olvido, que exige una conducta activa de los responsables de las grandes empresas en orden al tratamiento automatizado de la información y que exigen un cierto desarrollo técnico que puede resultar una carga excesiva en ciertos contextos. Como luego veremos, los programas Data Tika han supuesto un notable avance, estableciendo un diseño particularizado, apropiado a los medios y objetivos de cada empresa o situación jurídica particularizada.

33 Conforme al artículo 26 de la LO 7/2021, el ejercicio de estos derechos, en el caso de datos afectados a la investigación penal, se llevará a cabo de conformidad con lo dispuesto en la LOPJ, principalmente art. 263 *bis* a *nonies*, en las normas procesales y en el Estatuto del Ministerio Fiscal.

4. DIVERGENCIAS EN EL TRATAMIENTO DE DATOS CON LA LEGISLACIÓN DE LA UNIÓN EUROPEA

En julio de 2018, se produjo en Rabat un seminario entre responsables de la Unión Europea y de Marruecos en el que se procedió a analizar las diferencias entre ambos ordenamientos. Los resultados revelaron varios ámbitos de convergencia, como las definiciones, el ámbito de aplicación material de la ley, los principios del tratamiento de datos, los principios aplicables a las transferencias transfronterizas y la misión de la autoridad de control. Sin embargo, también se identificaron otros ámbitos en que se apreciaban soluciones dispares a los problemas planteados. Así, la ausencia de referencias a los datos biométricos o a la orientación sexual, así como la falta de desarrollo de los derechos de los interesados, como puedan ser la ausencia de derecho al olvido, la ausencia de derecho a la portabilidad de los datos, la ausencia de condiciones detalladas relativas a la validez del consentimiento, la falta de requisitos para notificar a la autoridad las violaciones de los datos, la ausencia de un principio de minimización de los datos, y los límites de los poderes concedidos a la CNDP[34].

Las autoridades marroquíes han promocionado también la intervención de terceros de confianza (*tiers de confiance*). Recientemente el presidente de la Comisión Nacional para el Control de la Protección de Datos Personales se refirió a una deliberación de la Comisión, en 2020, que sentó las bases para las directrices sobre una arquitectura de identificadores que abogan por la separación de los lugares de almacenamiento de los datos de uso y de los de los datos de autenticación[35].

La CNDP también ha propuesto el establecimiento de un tercero nacional de confianza dedicado a la autenticación para evitar que cada proveedor de servicios (banca, seguros, logística, administración, etc.) tenga una base de datos biométrica interna[36]. Las autoridades de Marruecos han insistido en la necesidad de gestionar adecuadamente la gestión de la identidad digital, abogando por el establecimiento de

34 Sobre este particular, el apartado 4 del artículo 14 del segundo protocolo de Budapest señala: «[...] los datos personales que revelen el origen racial o étnico; las opiniones políticas, las convicciones religiosas o de otro tipo, o la afiliación sindical; los datos genéticos; los datos biométricos considerados sensibles por los riesgos que entrañan; o los datos personales relativos a la salud o a la vida sexual». Según el apartado 236 del informe explicativo incluiría tanto la orientación como las prácticas sexuales. *Cfr.* CHENAOUI, H., «Morocco data protection law: Moving to align with EU data protection». https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection/ (consulta: julio de 2022).

35 Véase SEGROUHNI, O., «La protection des données à caractère personnel : Une contribution marocaine à l'universel», *Boletín CNDP,* núm. 1, Tiers de Confiance Numérique, disponible en: https://www.cndp.ma/images/bulletin/Bulletin-CNDP_Tiers-de-Confiance-Num%C3%A9rique-N01.pdf.

36 Véase la Deliberación 478-2013, de 1 de noviembre de 2013, sobre las condiciones necesarias para la utilización de dispositivos biométricos para el control de acceso, accesible desde: https://www.cndp.ma/images/deliberations/deliberation-n-478-2013-01-11-2013.pdf.

un «marco internacional» dedicado a la gestión de la identidad para acercar las visiones legales entre los distintos Estados[37].

Debe tenerse presentes las consecuencias que se están produciendo respecto a la identificación biométrica para el seguimiento de la inmigración ilegal[38], cuestión que se aborda en el Reglamento (UE) del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados, y que habilita el almacenamiento de una plantilla biométrica en que se combinan las huellas dactilares y el reconocimiento facial de las personas.

En los últimos años los esfuerzos de la Comisión Nacional de Protección de datos se han centrado en la promoción de los programas Data Tika[39]. Estos programas surgieron en julio de 2020, y pretenden acoger una suerte de compromiso de buenas prácticas que va mucho más a allá de las exigencias requeridas por la ley. Se establecen tres fórmulas posibles, en función de si van dirigidos a empresa, instituciones públicas u organizaciones no gubernamentales.

Estos programas se hicieron también extensivos al sector de la justicia por un acuerdo firmado el 26 de febrero de 2021 entre la CNDP y el Ministerio de Justicia[40]. Dichos programas de carácter voluntario imponen restricciones en el tratamiento de datos que recogen nuevos compromisos adaptados a las exigencias de la Unión Europea en esta materia.

37 Véase, en este sentido, la comunicación publicada en la revista digital *Maroc diplomatique*, que se hace eco del posicionamiento de las autoridades de Marruecos sobre esta materia: «L'expérience marocaine en matière de protection des données personnelles mise en exergue à Tunis», https://maroc-diplomatique.net/lexperience-marocaine-en-matiere-de-protection/ (consulta: 2 de junio 2022).

38 TASSINARI, F., «The Externalization of Europe's Data Protection Law in Morocco: an Imperative Means for the Management of Migration Flows», *Peace & Security – Paix et Sécurité Internationales*, 2021, núm. 9, p. 19.

39 Véase el comunicado de prensa remitido por la CNDP el 9 de julio de 2020. https://www.cndp.ma/images/commpresse/CNDP_Communique_de_presse_DATATIKA_20200709.pdf.

40 https://www.cndp.ma/fr/actualite/711-programme-data-tika-signature-d-une-convention-de-partenariat-entre-la-cndp-et-le-minist%C3%A8re-de-la-justice.html.

5. ESPECIAL REFERENCIA A LOS DATOS DE TRÁFICO ASOCIADOS AL PROCESO COMUNICATIVO EN LA LEGISLACIÓN MARROQUÍ

Hasta la entrada en vigor del nuevo Código de Procedimiento Penal revisado y corregido por la Ley 03-03, sobre la lucha contra el terrorismo, la legislación marroquí ignoraba oficialmente las escuchas telefónicas, y menos aún tenía en consideración la protección de los datos de tráfico.

La ausencia de una regulación hasta el año 2003 no significó que la práctica judicial haya ignorado este tipo de investigación. Para ilustrar este punto, se suele citar el antiguo artículo 86 del Código de Procedimiento Penal que permitía al «juez de instrucción proceder, de conformidad con la ley, con todos los actos de información que considere útiles para la demostración de la verdad», y entre estos actos, la doctrina incluía las escuchas telefónicas[41]. Sin embargo, el artículo 6 de la Constitución garantiza «el secreto de la correspondencia». La reforma no ha querido dejar lugar a la duda sobre este punto, declarando solemnemente el primer párrafo del artículo 108 del Código de Procedimiento Penal el principio de la prohibición de «escuchas telefónicas, interceptación de comunicaciones, grabación, descifrado o transcripción». Desde mayo de 2003, las escuchas ilegales están reguladas por los artículos 108 a 116 del nuevo Código de Procedimiento Penal (CPP).

Conforme al artículo 108, el legislador otorga al juez de instrucción el poder de ordenar tales audiencias al objeto de proceder a la intervención de las comunicaciones. Junto con aquel el fiscal puede promover y ordenar las intervenciones de las comunicaciones, después de obtener la autorización del presidente del Tribunal de Apelación. Su realización sigue estando sujeta a ciertas condiciones: el delito objeto de la investigación debe estar bajo la seguridad del Estado, crimen terrorista, organización criminal, homicidio intencional, envenenamiento, secuestro y toma de rehenes, falsificación de moneda y bonos del tesoro, drogas y estupefacientes, armas, municiones o explosivos, o la protección de los asuntos relacionados con la salud.

El fiscal, de forma excepcional en caso de emergencia extrema (riesgo de pérdida de pruebas, por ejemplo), puede también autorizar directamente escuchas telefónicas sin previo aviso al primer presidente del Tribunal de Apelación, por temor a la desaparición de los medios de prueba, siempre que se trate de delitos que afecten a la seguridad del Estado o un delito terrorista o relacionado con estupefacientes y sustancias psicotrópicas, armas, municiones y explosivos, secuestro o toma de rehenes. En tales casos, el cuarto párrafo del artículo 108 prevé que deberá solicitarse su ratificación en el término de 24 horas después de la decisión del fiscal. A la vista de lo cual el presidente del tribunal podrá cancelar, aprobar o reducir el alcance de este procedimiento, resolución que no es susceptible de recurso.

---

41 Al-Husseini, A. A., مدى مشروعية التسجيل الصوتي بالهواتف النقالة كدليل في الاثبات الجنائي (La legalidad de la grabación de voz en teléfonos móviles como prueba en la prueba penal). *Ahl al-Bayt*, 2009, núm. 8, pp. 166-203.

En lo que se refiere a los datos de tráfico, el artículo 114 del Código de Procedimiento Penal señala que para realizar las operaciones de captación de comunicaciones autorizadas, grabación de estas, toma de copias de estas y embargo, es posible obtener la información y los documentos necesarios para identificar la comunicación que se tomará de cualquier usuario de una red pública o de una autoridad de telecomunicaciones a la que se refiere la Ley 24.96, relativa al correo y las comunicaciones.

La ley de telecomunicaciones marroquí reconoce también el carácter confidencial de las comunicaciones y prevé en el artículo 26 que los operadores de redes públicas de telecomunicaciones, los proveedores de servicios de telecomunicaciones y sus empleados estarán obligados a respetar el secreto de la correspondencia electrónica y las condiciones de protección de la intimidad y los datos personales de los usuarios, bajo pena de las sanciones previstas en el artículo 92 siguiente. Por su parte, el artículo 24 modificado por el artículo 1 de la Ley 55-01, promulgada por el Dahir 1-04-154, 21 Ramadán 1425 (4 de noviembre de 2004). Conforme a lo previsto en esta norma, las personas jurídicas que explotan redes de telecomunicaciones o prestan servicios de telecomunicaciones están obligadas a poner a disposición de la Agencia Nacional de Regulación de las Comunicaciones (en adelante, ANRT), en los plazos fijados por el director de dicho instituto, la información o los documentos necesarios para comprobar si cumplen las obligaciones que les imponen las leyes y los reglamentos y la licencia que se les ha concedido. La ANRT está facultada para llevar a cabo investigaciones de las mismas personas, incluidas las que requieren una intervención directa o la conexión de equipos externos a sus propias redes. La información que posee la ANRT se transmite a la autoridad gubernamental competente y a cualquier otra autoridad administrativa que lo solicite. El ANRT podrá hacer pública la información que le facilite el explotador, a excepción de la información que haya sido identificada de mutuo acuerdo entre el operador y el ANRT como confidencial o datos comercialmente sensibles. Podrá solicitar, asimismo, que cualquier información que se le facilite sea verificada por un experto.

En lo que respecta a la conservación de los datos personales, la Ley 08-09, de protección de datos, al definir la calidad de los datos de carácter personal, previene que estos deberán conservarse en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos. A petición del responsable del tratamiento, y si existe un interés legítimo, la Comisión podrá autorizar el almacenamiento de datos personales con fines históricos, estadísticos o científicos más allá del período estrictamente necesario. Sin perjuicio de lo cual, y conforme al artículo 28 de la propia ley, la Comisión Nacional de Protección de Datos está también autorizada para habilitar la conservación de aquellos datos más allá del periodo inicialmente previsto. No se dice qué criterios deben ser tenidos en cuenta para la conservación de los datos, pero se sobreentiende —atendida la obligación de colaborar con la Administración de Justicia de los titulares de los datos de carácter personal—, que la investigación de los delitos y la aportación

de pruebas al proceso se encuentran también implícitamente previstas entre los fines del tratamiento.

Durante este tiempo se debe garantizar que los datos personales se recopilen y procesen de manera leal, legítima y transparente. También debe tener una finalidad precisa y legítima que se comunica a los interesados en el momento de la recogida de sus datos personales y a la CNDP en el momento de la notificación del tratamiento. El cambio de finalidad está sujeto a la autorización previa de la CNDP.

Más polémico ha sido el acceso a los datos por motivos de seguridad nacional al margen de la investigación de los delitos. El informe del Comité de Derechos Humanos se muestra bastante crítico en este punto[42]. Como hemos señalado anteriormente, la ley de 2009 no se aplica a los datos personales recogidos y tratados en interés de la defensa nacional y la seguridad interior o exterior del Estado. No existen, sin embargo, previsiones específicas en lo que se refiere al tratamiento y conservación de los datos sensibles, tales como los que afectan al proceso comunicativo, semejantes a las contenidas en el artículo 15, apartado 1, de la Directiva 2002/58.

Según señala en el Comité Internacional de Derechos Humanos, existen al menos ocho organismos gubernamentales que pueden vigilar potencialmente las comunicaciones[43]. Concretamente, y bajo la autoridad del Ministerio del Interior, se encuentran los *Renseignements généraux marocains* (también conocidos como Direction Générale de Sûreté Nationale), que forman parte de la policía nacional, y la Direction Générale de la Surveillance du Territoire (DGST), que se ocupa del contraespionaje y la lucha antiterrorista y es, sin duda, el organismo con más recursos. Dependiente de la autoridad del Ministerio de Defensa, la Direction Générale des Études et de la Documentation (DGED) y el Service de Renseignement de la Gendarmería Real Marroquí. Estos servicios operan con una cierta falta de transparencia, quedando habilitado su funcionamiento en razones de orden público superior, sin que exista un organismo independiente, como sucede en España, encargado de velar por el cumplimiento de las garantías constitucionales[44].

42 International Submission to Human Rights Committee. The Right to Privacy in Morocco (2016), p. 2. Accesible desde: https://privacyinternational.org/sites/default/files/2017-12/HRC_morocco.pdf (consulta: octubre de 2022).

43 International Submission to Human Rights Committee. The Right to Privacy in Morocco (2016), p. 2. Accesible desde: https://privacyinternational.org/sites/default/files/2017-12/HRC_morocco.pdf (consulta: octubre de 2022).

44 Sobre este particular, véase el informe anual *Amnesty International Annual Report 221 - Morocco/Western Sahara Report* (2021), disponible en: https://www.amnesty.org/en/location/middle-east-and-north-africa/morocco-and-western-sahara/report-morocco-and-western-sahara/.

6. LA TRANSFERENCIA INTERNACIONAL DE DATOS ENTRE LA UNIÓN EUROPEA Y MARRUECOS. EVOLUCIÓN Y SITUACIÓN ACTUAL

Expuesta la situación de la legislación que en materia de protección de datos existe en el país vecino, es posible entender el alcance y límites de las transferencias internacionales de datos en materia de cooperación. Como ha quedado expuesto, es inherente a la cooperación jurídica internacional, particularmente en el ámbito de materia penal, la transferencia de datos de carácter sensible que puede comprometer los derechos e intereses de los ciudadanos.

Es por esto por lo que la exposición de la Directiva 680/2014/UE previene que los Estados miembros deben velar por que las transferencias de datos a terceros países o a organizaciones internacionales solo se lleven a cabo si resultan necesarias para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública, y si el responsable del tratamiento en el tercer país u organización internacional de que se trate es una autoridad competente en el sentido de lo dispuesto en la propia directiva.

La normativa de la UE estableció restricciones a la transacción internacional de datos de sus ciudadanos fuera de sus fronteras, prohibiendo las transferencias a un tercer país u organización que no cuente con un nivel adecuado de protección de datos. Sin embargo, como señala Sobrino García[45], ni la directiva anterior y ni el actual RGPD han establecido qué debe entenderse por nivel adecuado de protección de datos, quedando en manos de la jurisprudencia del Tribunal de Justicia de la UE y de guías de buenas prácticas de carácter interno[46].

En el caso de Marruecos, siempre tuvo una relación privilegiada con la Unión Europea, pero el carácter autoritario de la monarquía alauita en el último cuarto de siglo de la precedente centuria no permitió grandes avances en materia de cooperación. El Acuerdo de Asociación Euromediterránea celebrado entre la UE y Marruecos en 1996 marcó un punto de inflexión para el establecimiento de un estatus avanzado de Marruecos. De hecho, el diálogo intergubernamental incluyó la mejora de las relaciones en varios frentes: político, económico, financiero, social y cultural. En esa ocasión, la UE promovió sus valores básicos y principios fundamentales insertando una cláusula democrática que incluía la protección de los derechos humanos, incluyendo una lista

45 Véase SOBRINO GARCÍA, I., «Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Los Estados Unidos», *Revista de Derecho Comunitario Europeo*, Centro de Estudios Políticos y Constitucionales, enero-abril de 2021, núm. 6, p. 230.

46 Véase la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y posteriormente el Reglamento (UE) 2016/679 y la Directiva 680/2020, de 30 de marzo.

de principios de protección de datos aplicables a las relaciones comerciales entre la UE y Marruecos[47].

Estos principios eran básicamente un calco de la Directiva de Protección de Datos, una norma europea que Marruecos aceptó en su legislación interna por la Ley 09-2008 y en la que el legislador marroquí pretendió una adecuación a la legislación europea. A pesar de estos esfuerzos, en 2010 la ley marroquí no superó la prueba de adecuación de la Comisión Europea que habría permitido la libre circulación de datos en virtud del artículo 36 de la Directiva de Protección de Datos[48]. Con todo, la divergente normativa marroquí remite a un sistema jurídico subyacente construido sobre su propio conjunto de principios y valores que deben igualmente ser respetados dentro de los límites de la necesaria reciprocidad[49]. Tal como apunta Tassinari, la Ley 09-2008, por ejemplo, se hace eco de la religión musulmana, al no incluir las cuestiones de género y la orientación sexual dentro de la definición de datos sensibles, omisiones que no eran asumibles desde la perspectiva europea[50].

En el Plan de Acción UE-Marruecos (2013-2017), ambas partes se comprometieron a realizar «un espacio de valores compartidos» en el que Marruecos, en particular, habría hecho más esfuerzos para «sensibilizar a todas las partes y actores implicados a nivel nacional sobre la importancia de seguir los principios y valores establecidos por el Convenio Europeo de Derechos Humanos del Consejo de Europa, la Carta de Derechos Fundamentales de la UE, los Acuerdos Parciales del Consejo de Europa y las directivas pertinentes de la UE»[51].

47 MARTÍNEZ DE CAPDEVILA, C., «El "estatuto avanzado" de Marruecos en la Unión Europea», *Revista de Derecho Comunitario Europeo*, septiembre/diciembre de 2009, núm. 34, p. 903.

48 MAKULILO, A. B., «Data Protection Regimes in Africa: too far from the European 'adequacy' standard?», *International Data Privacy Law*, 2013, vol. 3, núm. 1, pp. 42-50.

49 Renteln ha sostenido que la comparación de los sistemas de derechos humanos debe basarse en una evaluación de intercultural, mediante la identificación de aquellos valores universales respecto de los que existe un consenso en la comunidad internacional. RENTELN, Alison Dundes, *International Human Rights: Universalisma Versus Relativism*. Quid pro books, 2013, Kindel Edition, p. 115.

50 TASSINARI, F., «The Externalization of Europe's Data Protection Law in Morocco: an Imperative Means for the Management of Migration Flows», *Peace & Security – Paix et Sécurité Internationales*, 2021, núm. 9, p. 7.

51 Propuesta conjunta de Decisión del Consejo (Eur Lex 52013JC0006) relativa a la posición de la Unión en el seno del Consejo de Asociación instituido por el Acuerdo Euromediterráneo por el que se crea una Asociación entre las Comunidades Europeas y sus Estados miembros, por una parte, y el Reino de Marruecos, por otra, con vistas a la adopción de una recomendación relativa a la ejecución del Plan de Acción UE-Marruecos de ejecución del Estatuto Avanzado (2013-2017) /* JOIN/2013/06 final - 2013/0107 (NLE) */.

Se instó entonces a Marruecos a que adoptara el modelo europeo y, especialmente, a que se adhiriera al Convenio 108 del Consejo de Europa[52], lo que finalmente hizo en enero de 2019[53]. Mientras tanto, la Directiva de Protección de Datos, en vigor desde el 25 de mayo de 2018, aunque mantiene el modelo de transferencia internacional de datos de la precedente Directiva de Protección de Datos, introduce cambios significativos que estimulan el flujo de información entre la UE y terceros países y organizaciones internacionales[54].

Esta es también la opinión expresada por la Comisión belga de protección de la intimidad en relación con las transferencias de datos al Reino de Marruecos en el marco de un acuerdo de cooperación policial y judicial. En dicho informe se concluye: «[...] debido a la existencia del Acuerdo de Cooperación de 6 de mayo de 1999 sobre la lucha contra la delincuencia organizada [...], la transferencia de datos personales puede realizarse a Marruecos porque "se hace legalmente obligatoria para la protección de un interés público importante" (art. 22, § 1, 4° de la Ley de Privacidad); [...] deben proporcionarse ciertas garantías adicionales para que las personas afectadas puedan seguir beneficiándose de los derechos y garantías fundamentales en relación con el tratamiento de sus datos en Bélgica, una vez transferidos a Marruecos»[55].

El acuerdo internacional en materia de seguridad que ahora se aprueba servirá también para legitimar la transacción internacional de datos respecto de actuaciones de prevención y aseguramiento, en que no exista todavía un procedimiento judicial abierto. Con todo, se observan deficiencias en la regulación de las políticas de género, datos de tráfico comunicativo, derecho al olvido, y, particularmente, en las situaciones de excepción por razones seguridad y defensa nacional que se alejan bastante del régimen establecido en el derecho europeo[56]. No existen, sin embargo, las dificultades

52 CHENAOUI, H., «Morocco data protection law: Moving to align with EU data protection». https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection/ (consulta: julio de 2022).

53 Véase el comunicado de prensa de 27 de junio de 2019: «Joint declaration the European Union and Morocco for the fourteenth meeting of the association Council». Accesible desde: https://www.consilium.europa.eu/en/press/press-releases/2019/06/27/joint-declaration-by-the-european-union-and-the-kingdom-of-morocco-for-the-fourteenth-meeting-of-the-association-council/.

54 Declaración conjunta de la Unión Europea y Marruecos tras la 14.ª reunión del Consejo de Asociación UE-Marruecos. Véase: https://www.consilium.europa.eu/fr/press/press-releases/2019/06/27/joint-declaration-by-the-european-union-and-the-kingdom-of-morocco-for-the-fourteenth-meeting-of-the-association-council/.

55 Comisión (belga) para la Protección de la Privacidad, Dictamen 22/2009, de 2 de septiembre de 2009, sobre la compatibilidad de la ley marroquí con la Ley de Privacidad en el marco del procedimiento de ratificación del Acuerdo de cooperación de 6 de mayo de 1999 entre el Reino de Bélgica y el Reino de Marruecos en materia de lucha contra la delincuencia organizada.

56 Véase el informe del Comité de Derechos Humanos en su 116.ª sesión, *The Right to Privacy in Morocco* 2016, p. 2, disponible en https://privacyinternational.org/sites/default/files/2017-12/HRC_morocco.pdf (consulta: octubre de 2021).

que se han presentado con el derecho norteamericano respecto a la falta de control judicial o por una autoridad administrativa independiente de los titulares de los datos, existiendo una autoridad de control que presenta todas las garantías de independencia, y sobre todo la posibilidad de acudir a los tribunales para obtener la tutela de los derechos relativos a la protección de datos en términos semejantes a los existentes en la Unión Europea.

7. TRANSFERENCIA INTERNACIONAL DE DATOS MEDIANTE UNA DECISIÓN DE ADECUACIÓN

El nuevo Reglamento General de Protección de Datos y la directiva establecen una regulación más flexible que la ordenación precedente al establecer nuevos instrumentos para legitimar las transferencias internacionales y suprimir los requisitos burocráticos que obstaculizaban los intercambios internacionales. En concreto, se habilita la realización de tales transferencias sin la necesidad de una autorización específica, y sin que sea imprescindible que los responsables o encargados del tratamiento tengan que notificar a la autoridad de control cualquier operación o conjunto de operaciones de tratamiento total o parcialmente automáticas.

Estas transferencias, como hemos visto, pueden fundarse, bien en una decisión de adecuación que reconozca en un determinado ordenamiento jurídico un nivel de protección similar al que tiene en la Unión Europea, bien en el otorgamiento de garantías apropiadas a cada caso en concreto, o bien en supuestos específicos mediante un reconocimiento de situaciones particularizadas. En el caso de Marruecos, los artículos 43 y 44 de la Ley 08-09, de protección de datos, siguen casi a la letra las previsiones contenidas en la directiva de 1995, en que, a falta de una decisión de adecuación o del consentimiento del interesado, se estima bastante para el reconocimiento de una transferencia internacional de datos la existencia de razones de orden público o la salvaguardia del ejercicio o defensa de una reclamación legal[57].

Tanto el RGPD como la Ley marroquí 08-09 propugnan las decisiones de adecuación como el canal preferible para la transferencia de datos personales, ya que este instrumento exige que se realice por las respectivas agencias de protección de datos un análisis en profundidad del ordenamiento jurídico y los compromisos internacionales con terceros países, incluido el respeto de los principios del Estado de derecho y los derechos fundamentales. Sin embargo, como señala Sobrino García, ni la directiva anterior ni el actual RGPD han establecido qué debe entenderse por nivel adecuado de

57 Artículo 44. No obstante lo dispuesto en el artículo 43 anterior (existencia de una resolución de adecuación), el responsable del tratamiento podrá transferir datos personales a un Estado que no cumpla las condiciones establecidas en el artículo anterior, si la persona a la que se refieren los datos ha consentido expresamente su transferencia o si el traslado es necesario a) para salvaguardar la vida de esa persona; b) proteger el interés público; c) el cumplimiento de obligaciones para garantizar el establecimiento, el ejercicio o la defensa de reclamaciones legales; d) la ejecución de un contrato entre el responsable del tratamiento y el interesado, o de medidas precontractuales adoptadas a petición del interesado; e) la celebración o ejecución de un contrato celebrado o por celebrar, en interés del interesado, entre el responsable del tratamiento y un tercero, y f) la prevención, el diagnóstico o el tratamiento de enfermedades. Aparte de este supuesto, se contempla el caso de que la transferencia se realiza en virtud de un acuerdo bilateral o multilateral del que el Reino de Marruecos es parte. En último caso, se prevé la posibilidad de la autorización expresa y motivada de la Comisión Nacional, si el tratamiento garantiza un nivel adecuado de protección de la intimidad y de los derechos y libertades fundamentales de las personas, en particular por a las cláusulas contractuales o de las normas internas a las que está sometido.

protección de datos, quedando en manos de la jurisprudencia del Tribunal de Justicia de la UE y de diversos informes oficiales de orden interno que no presentan carácter vinculante. Hoy por hoy, constituyen un ámbito de inseguridad jurídica ante los elevados niveles de exigencia del TJUE, que ha procedido a derogar por dos veces las sucesivas decisiones de adecuación con Estados Unidos[58].

Por otra parte, se ha criticado a la Unión Europea en su intento de imponer sus valores al resto del mundo[59], exigiendo un nivel de exigencia que no se corresponde con la reciprocidad que es propia en el tratamiento de las cuestiones en materia de cooperación internacional y sobre todo desconociendo el principio de ubicuidad que es esencial para el entendimiento del alcance[60] y efecto de la jurisdicción en materia de información electrónicamente almacenada[61]. Conforme a su formulación primitiva contenida en el Código Penal alemán (sección 9 §1 Alt. 3 y 4 del *Strafgesetzbuch*), el principio de ubicuidad (*Ubiquitätsprinzip*) establece que el delito se considera ocurrido en el lugar de la acción del autor o en el lugar donde se produjo el daño[62]. La restricción de los efectos en orden a la transmisibilidad de los datos limita igualmente las posibilidades de extender la jurisdicción a otros Estados al restringir notablemente el objeto de la investigación. Debe tenerse en cuenta que el entorno virtual es en muchos casos una entelequia compartida en que no es asumible la imposición unilateral de exigencias de orden público sin chocar con los modelos propios de otros países[63].

El hecho es que a día de hoy la Unión Europea solo tiene aceptadas decisiones de adecuación de datos con Japón y el Reino Unido, este último acuerdo consecuencia colateral del *Brexit*, así como con Noruega e Islandia, que, de hecho, integran en su ordenamiento la Directiva de Protección de Datos. Las otras decisiones de adecuación existentes con otros países son anteriores al Reglamento General de Protección de

---

58 Véase SOBRINO GARCÍA, I., «Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y los Estados Unidos», obra cit., p. 227.

59 Véase en este sentido BRADFORD, A., «The Brussels Effect: How European Union Rules de World», OUP 2020, Kindle Edition, p. 132.

60 Como veremos, el protocolo al que ahora se adhiere Marruecos va a dar una nueva vuelta de tuerca a estas cuestiones al fijar las condiciones y garantías de los derechos de los usuarios dentro del entorno virtual; este hecho condicionará también el efecto expansivo del principio de ubicuidad. Véase GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E.. «El nuevo protocolo del Convenio de Budapest de lucha contra la cibercriminalidad», (RI §425241) *Revista General de Derecho Procesal*, septiembre 2022, núm. 58, pp. 18-19.

61 Véase MILIART, J. B., «The limits of subjective territorial jurisdiction in the context of cybercrime», *Era fórum*, 2019, p. 375.

62 Sobre el contenido y alcance de la cibercriminalidad, ver BROWN, Cameron S. D., «Investigating and prosecuting cybercrime: forensic dcependencies and barriers to justice», *International Journal of Cyber Criminology*, enero de 2015, vol. 9, p. 55-119. DOI: 10521/Zennodo.22387.

63 Véase GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., «El nuevo protocolo del convenio de Budapest de lucha contra la cibercriminalidad», *Revista General de Derecho Procesal*, 2022, núm. 58, p. 8.

Datos y hoy en día carecen de previsiones esenciales en materia de transferencia internacional de datos, políticas de retención de datos y derecho al olvido[64].

Respecto a Estados Unidos, la anulación de la Decisión (UE) 2016/1250 de la Comisión, escudo de privacidad —*privacy shield*—, tras los pronunciamientos del TJUE en los casos Schrem I y II, ha determinado la necesidad de revisar las políticas de transferencia de datos. La propuesta de puerto seguro —*security harbour*— contenidas en la decisión de adecuación recibió un duro revés en 2013 tras las declaraciones de Edward Snowden sobre los programas de vigilancia norteamericanos y las prácticas de la National Security Agency. Estas revelaciones demostraron a la UE que los datos de los ciudadanos europeos no gozaban de una protección adecuada. Todo lo cual precipitó la invalidación del acuerdo en 2015 por la STJUE de 6 de octubre de 2015, (en adelante, Schrems I)[65] y posteriormente en el más reciente pronunciamiento de 16 de julio de 2020 (en adelante, Schrems II)[66]. Pese a las mejoras llevadas a efecto en la segunda decisión de adecuación, el STJUE sigue entendiendo que las exigencias de seguridad nacional de EE. UU. prevalecen sobre el marco legal de transferencias internacionales con la UE de manera intrusiva[67].

Estas resoluciones pusieron de manifiesto también que la existencia de una resolución de adecuación que declare un determinado nivel de exigencia no puede constituir un salvoconducto que justifique la exclusión del acceso de los titulares de los datos ante los tribunales de justicia. Ni el *Safe Harbour* ni el posterior acuerdo, *Privacy Shield,* tuvieron en cuenta, a juicio del Tribunal de Justicia europeo, las críticas y recomendaciones llevadas a cabo a lo largo del tiempo, considerando que la primacía de las exigencias sobre la seguridad nacional, el interés público y el cumplimiento de la ley estadounidenses posibilitaban injerencias en los derechos fundamentales de los ciudadanos europeos.

---

64 Concretamente con Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000; Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos; Argentina. Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003; Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003; Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004; Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo de 2008; Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010; Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010; Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011; Uruguay. Decisión 2012/484/UE, de la Comisión, de 21 de agosto de 2012; Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.

65 STJUE de 6 de octubre de 2015, Schrems I, C-362/14, EU:C: 2015:650.

66 STJUE de 16 de julio de 2020, Schrems II, C-311/18, EU:C: 2020:559.

67 Véase SOBRINO GARCÍA, I., «Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y los Estados Unidos», *Revista de Derecho Comunitario Europeo*, Centro de Estudios Políticos y Constitucionales, enero-abril de 2021, núm. 6, p. 232.

La sentencia Schrems II, de 16 de julio de 2020, pone su énfasis en aspectos formales como la falta de garantías adecuadas[68], la referencia de las cláusulas contractuales tipo presentes en la legislación interna americana que permitían la intromisión de las autoridades americanas por motivos de seguridad nacional[69] y la ausencia de vías de recurso ante un órgano con garantías suficientes que permita a los afectados el ejercicio de sus derechos[70].

Estas resoluciones, como señala De Miguel Asensio, habrán de tener un efecto relevante en el futuro de las decisiones de adecuación frente a terceros Estados, ya que la evaluación que deberá hacer la Comisión se verá condicionada al tener que examinar los ulteriores tratamientos a los que puedan verse sometidos los datos transferidos ante fines de seguridad pública bajo los mismos parámetros[71].

El hecho es que, en lo que a Marruecos se refiere, dado el elevado nivel de exigencia requerido por el TJUE, la homologación de sus sistemas de protección de datos por las autoridades de la Unión Europea no es previsible que se lleve a efecto a medio y corto plazo con un consenso que permita un acuerdo de adecuación.

Con todo, los avances que se han llevado a efecto en los últimos años son muy relevantes. Concretamente, el considerando 195 del Reglamento General de Protección de datos da especial relevancia al Convenio 108 del Consejo de Europa, de 28 de enero de 1981, y a sus protocolos adicionales, convenio en el que, como ha quedado indicado, Marruecos participó en su redacción y ratificó en enero de 2019. En definitiva, al acercarse a los parámetros europeos, Marruecos se acerca cada vez más a la obtención de una decisión de adecuación que potenciaría un procedimiento rápido de intercambio de datos personales.

En materia penal, además, la Directiva 680/2016/UE admite una cuarta posibilidad, la transferencia de datos a terceros países cuando se lleve a efecto entre autoridades competentes encargadas de la investigación de los delitos, siempre que se limite a lo que sea estrictamente necesario, proporcional y pertinente, esto es, que se considere que la transferencia a una autoridad competente del tercer país a los fines de la investigación del delito resultaría eficaz o adecuada para el logro de esta finalidad. En

68 En particular, se estimó inadecuada la supervisión llevada a efecto por el mecanismo del defensor del pueblo contemplado en la Decisión EP, pues no proporciona ninguna vía de recurso ante un órgano que ofrezca a las personas cuyos datos se transfieren a los Estados Unidos garantías sustancialmente equivalentes a las exigidas en el art. 47 de la Carta (véase parágrafo 197 de la STJUE Schrem II).

69 Véase SOBRINO GARCÍA, I., «Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y los Estados Unidos», obra cit., p. 246.

70 Véanse apartados 186 a 191 de la SJUE Schrem II.

71 Véase DE MIGUEL ASENSIO, P. A., «Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia», *La Ley Unión Europea*, 2015, núm. 31, p. 3.

tales casos se exigirán las garantías adecuadas respecto al uso de los datos cedidos (véase, artículo 39 de la directiva). En todo caso, los datos personales no se transferirán si la autoridad competente de la transferencia determina que los derechos y libertades fundamentales del interesado en cuestión prevalecen sobre el interés público en la transferencia.

8. TRANSFERENCIAS MEDIANTE GARANTÍAS APROPIADAS

En ausencia de una decisión de adecuación de la Comisión Europea y conforme al artículo 45 de la LO /2021, de 26 de mayo, el modo normal de que se lleve a efecto la transferencia internacional de datos es mediante la prestación de garantías adecuadas que permitan evaluar la calidad de los datos.

Estas garantías pueden articularse a través de los supuestos siguientes:

a) Cuando se otorguen garantías apropiadas respecto a la protección de datos personales en un instrumento jurídicamente vinculante. Tal sería el caso del Convenio entre el Reino de España y el Reino de Marruecos sobre cooperación en materia de seguridad y de lucha contra la diligencia organizada de 13 de febrero de 2019, publicado en el *Boletín Oficial del Estado* el pasado 7 de abril de 2022 y al que luego aludiremos.

b) Mediante una decisión particularizada, por parte del responsable del tratamiento, en que se evaluarán todas las circunstancias que concurren en la transferencia de datos personales y se haya concluido que existen garantías apropiadas respecto a la protección de datos personales.

Este segundo supuesto es el más complejo en la medida que implica una tramitación bastante laboriosa en la que el responsable del tratamiento informará a la autoridad de protección de datos competente acerca de las categorías de transferencias permitidas. Dicha decisión deberá documentarse, poniéndose a disposición de la autoridad de protección de datos competente, previa solicitud en la que se incluirá la siguiente información: fecha, hora de la transferencia, información sobre la autoridad competente destinataria, justificación de la transferencia y datos personales transferidos.

En todos estos supuestos, resultará decisiva la alineación de Marruecos con los modelos de tratamiento de datos a nivel internacional. Como señala KUNER, esto es decisivo porque la protección de datos es un concepto jurídico asumido a nivel internacional que va más allá de las previsiones del Reglamento General de Protección de Datos[72].

Las mayores dificultades se presentan en orden a determinar qué debe entenderse como garantías adecuadas, y, en particular, cuál es el nivel de exigencia que de aplicación conforme a lo previsto en el art. 35 de la directiva y, 45 del Reglamento General de Protección de Datos. Tal como sostiene Kuner, si bien no han faltado propuestas dirigidas a una uniformidad en las garantías exigidas[73], no existe un patrón

72 Véase KUNER, C., «The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards», *National Law School of India Review*, 2021, vol. 33, p. 89.

73 Menciona el autor últimamente citado como ejemplo *The Rule of Law Index*, publicado anualmente por el World Justice Project, el cual, en su versión de 2022, comparaba el principio de legalidad en 128 países alrededor del mundo. Véase en este sentido https://worldjusticeproject.org (consulta: octubre de 2022).

único, ni es posible exigir una trasposición literal de los preceptos[74]. En tal sentido, el Tribunal de Justicia de la Unión Europea ha declarado que la protección de datos exige no solo un marco legal suficiente, sino también la protección en la práctica. La sola trasposición legal de un marco legal no puede revelar cómo la protección de datos de carácter personal opera realmente en el terreno[75]. En todo caso, y como señala el autor últimamente citado, debe irse más allá de la legislación de protección de datos y tener en consideración otros factores tales como el marco político-constitucional, los compromisos asumidos a nivel internacional, el marco institucional en materia de protección de los derechos humanos, el marco legal civil, criminal y administrativo y la autonomía personal. Además, es importante examinar cómo estos factores realmente se conducen en la vida diaria de estos terceros países[76].

74 KUNER, C., «The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards», obra cit., p. 83.

75 Véanse apartado núm. 27 de Schrems I y apartado núm. 21 de Schrems II.

76 KUNER, C., «The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards», obra cit, pp. 83-84.

9. TRANSFERENCIA A TRAVÉS DE CONVENIO O TRATADO. EL CONVENIO DE 2019 SOBRE COOPERACIÓN EN MATERIA DE SEGURIDAD Y DE LUCHA CONTRA LA DELINCUENCIA

Como ha quedado indicado, el Convenio en materia de seguridad y de lucha contra la delincuencia, hecho en Rabat el 13 de febrero de 2019, se incorpora a nuestro ordenamiento con la finalidad de dotar de las garantías adecuadas a la transferencia de datos a nivel policial. Cuando la cooperación se formaliza a nivel judicial, ha de estarse a las previsiones contenidas en el Convenio de 2009, relativo al auxilio judicial en materia penal, hecho en Rabat el 24 de junio de 2009, si bien en este, atendido el tiempo en que fue dictado, no contempla la prestación de las garantías requeridas por el art. 44 de la Ley Orgánica 7/2021. Como veremos, sin embargo, la garantía que ofrece la remisión a través de una autoridad independiente va a simplificar en gran medida el reconocimiento de estas transferencias internacionales de datos. No es el caso de las investigaciones policiales, en que el Convenio de 2019 viene a llenar un gran vacío en materia de protección de datos.

Conforme al artículo 2 del Convenio, su ámbito se limita al intercambio de información en relación con la identificación y búsqueda de personas desaparecidas, la investigación y búsqueda de las personas que hayan cometido un delito o sean sospechosas, la identificación de cadáveres y de personas de interés policial, la búsqueda de efectos o instrumentos del delito, la financiación de actividades delictivas, el traslado de armas y las entregas controladas. De su tenor y atendidas las dificultades implícitas al traslado de datos de contenido sensible, deberían quedar excluidas las diligencias de investigación que ya se encuentren judicializadas salvo aspectos auxiliares.

El Convenio presenta y reconoce amplias garantías en orden a la transferencia internacional de datos, dedicando a este tema gran parte de su articulado. Como en otros convenios de esta índole, cuenta con un listado de acciones criminales en las que ambas partes coinciden en la aplicación del principio de reciprocidad. Contiene igualmente una cláusula de cierre para supuestos residuales, a cuyo efecto se previene en que «las partes colaborarán asimismo en la lucha contra cualquier otro delito cuya prevención, detección e investigación requiera la cooperación de las autoridades competentes de ambas partes».

Asimismo, por consenso mutuo, se admite que las partes puedan colaborar en cualquier otra área en materia de seguridad, siempre que sea compatible con el propósito de este Convenio. Cabría cuestionarse si la normativa que ampara la transferencia internacional de datos de estas otras materias que no se dirigen directamente a la investigación del delito deba ser directamente el Reglamento General de Protección de Datos y no la directiva, pues, dada su finalidad, no cabe hacer aplicación del régimen de excepción que esta última establece.

Conforme al art. 9, el intercambio de información entre las partes, de acuerdo con este Convenio, se realizará bajo las condiciones siguientes:

a) La parte requirente podrá utilizar los datos únicamente para el fin y según las condiciones determinadas por la parte requerida, tomando en consideración el plazo después de cuyo transcurso deben ser destruidos, de acuerdo con su legislación nacional.

b) A petición de la parte requerida, la parte requirente facilitará información sobre el uso de los datos que se le han ofrecido y sobre los resultados conseguidos.

c) Si resultara que se han ofrecido datos inexactos o incompletos, la parte requerida informará sin dilación a la parte requirente.

d) Cada una de las partes llevará un registro con los informes sobre los datos ofrecidos y su destrucción.

En el propio precepto, se previene que las partes asegurarán la protección de los datos ofrecidos frente al acceso, modificación, divulgación o destrucción no permitidos de acuerdo con su legislación nacional. Asimismo, se comprometen a no ceder los datos personales a que se refiere este artículo a ningún tercero distinto del órgano solicitante de la parte requirente, o, en caso de solicitarse por esta, solo podrán transmitirse a alguno de los órganos previstos en el artículo 6, previa autorización del requerido. Cualquier parte podrá aducir, en cualquier momento, el incumplimiento por la parte requirente de lo dispuesto en este artículo, como causa para la suspensión inmediata de la aplicación del Convenio y, en su caso, de la terminación automática de este.

10. RECONOCIMIENTO DE SITUACIONES PARTICULARIZADAS

El reconocimiento de unas garantías requiere una compleja tramitación que puede llevar meses, razón por la que se prevén excepciones en situaciones específicas y particularizadas. El Convenio de 2019 excluye expresamente en su artículo 5 las cuestiones relativas a la asistencia judicial en procesos penales y de extradición. Siendo así, y careciendo de los instrumentos actualmente al uso en materia de auxilio jurisdiccional de una previsión sobre las garantías que deban adoptarse en materia de protección de datos, parece claro que la transferencia internacional de datos dependerá del reconocimiento particularizado por la autoridad judicial prestadora de auxilio para cada supuesto en concreto[77].

Este reconocimiento particularizado distingue dos supuestos con un nivel de garantías distintos:

— Mediante reconocimiento particularizado por una autoridad competente para la investigación del delito. Será necesario, entonces, que la solicitud de cooperación se dirija a la protección de los intereses vitales o los derechos y libertades fundamentales de cualquier persona, de la seguridad del Estado, de los intereses legítimos del interesado y en casos individuales en orden al ejercicio de acciones legales o para la defensa frente a aquellas. En estos supuestos, tanto en situaciones individuales particularizadas como en orden al ejercicio de acciones legales, los datos personales no se transferirán si la autoridad competente de la transferencia determina que los derechos y libertades fundamentales del interesado prevalecen sobre el interés público que justifica la transferencia.

— El segundo supuesto se dará cuando se remitan a otros destinatarios que no tengan la condición de autoridad competente y resulte necesaria su intervención en virtud de una solicitud de cooperación judicial penal o policial. En estos supuestos, además de las limitaciones antes referidas, la transferencia se limitará a lo estrictamente necesario para el cumplimiento de las finalidades propias de la investigación de los delitos y siempre que no sea posible otorgar

77 El Convenio entre el Reino de España y el Reino de Marruecos relativo a la asistencia judicial en materia penal, hecho en Rabat el 24 de junio de 2009, atendido el escaso desarrollo que tenía en aquel entonces la legislación de protección de datos, no tiene referencias en la materia, pero sí aborda cuestiones como son el intercambio de comunicaciones de condena y resoluciones judiciales, previniendo en el artículo 24 que cada parte comunicará a la parte interesada las condenas penales y demás medidas de seguridad concernientes a nacionales de dicha parte y que hayan sido objeto de inscripción en el registro de antecedentes penales; las autoridades centrales procederán a dicha comunicación al menos una vez al año. Previa solicitud expresa, se remitirá una copia de la resolución dictada. La información procedente del registro de antecedentes penales, solicitada en un asunto penal, será comunicada del mismo modo que si hubiese sido solicitada por una autoridad judicial de la parte requerida; solo en el caso de que la solicitud fuese de un tribunal civil o de una autoridad administrativa estarán motivadas. En todo caso, se les dará curso ciñéndose a las disposiciones legales o reglamentarias internas de la parte requerida. Se establecen previsiones en materia de reserva de la información bancaria, así como en materia de toma de muestras genéticas.

otro nivel de garantías dentro de un plazo razonable. Se informará, además, sin dilación a la autoridad competente y al destinatario de la finalidad o finalidades específicas para las que pueden tratarse los datos personales, siempre y cuando dicho tratamiento sea necesario.

Sea cualesquiera el tipo de autoridad competente, el artículo 38 de la directiva y el artículo 46 de la Ley 5/2021, de 6 de junio, distinguen, en orden al reconocimiento de una situación específica, básicamente tres supuestos, según se trate de actuaciones de prevención o no:

— Casos individuales que se dirijan a la investigación de los delitos y de su autor, así como para el ejercicio de derecho de defensa en esas investigaciones.

— Acciones de prevención de amenazas graves e inmediatas contra la seguridad pública y la prevención de intereses vitales del interesado en los datos o de cualquier otra persona.

— De los intereses legítimos del interesado.

Para el entendimiento del precepto es esencial tener presente la distinta posición de los poderes públicos en un Estado de derecho respecto de la investigación de los delitos que ya se han cometido y las facultades en orden a prevenir un riesgo para la seguridad ciudadana.

En el primero de los casos, el principio de presunción de inocencia excluye cualquier actuación prospectiva que cree una infundada sospecha genérica sobre grupos o colectivos de población. Véase en este sentido el artículo 6 del Código Penal, que solo admite estas medidas en atención a la peligrosidad del sujeto al que se impongan, exteriorizada en la comisión de un hecho previsto como delito.

Tratándose del propio afectado, se entiende también que la directiva posibilite a los poderes públicos subrogarse en sus intereses mediante la transmisión de la información adecuada para la defensa frente a los delitos cometidos contra su persona.

Fuera de estos supuestos, la actuación propiamente a prevención de las fuerzas del orden solo está justificada por el riesgo de lesión de los intereses del propio afectado o por el riesgo que para los derechos fundamentales suponen una amenaza para la seguridad pública o una situación de un riesgo frente a la vida.

En este último caso, conforme a la STJUE de 6 de octubre de 2020, Gran Sala, La Quadrature du Net, apartado 168, matizada por las más recientes STJUE de 5 de abril de 2022, C-140/2020, y STJUE de 20 de septiembre de 2022, Space Net, solo resultaría admisible una conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse. El antiguo artículo 22 de la Ley 15/1999, de 13 de diciembre, solo admitía el acceso a los datos sensibles en estos supuestos, respecto de los que requería la

intervención de una autoridad judicial. La directiva y la Ley 7/2021, de 26 de mayo, no distinguen en este punto, quedando al criterio de las autoridades nacionales concretar la intervención judicial en función de los intereses afectados.

La ausencia de una regulación específica en Marruecos para los datos más sensibles, como puedan ser los datos de tráfico y la retención de la información que de aquellos pueda llevarse a efecto, exigirá que en cada solicitud de cooperación se llevé a efecto un compromiso individualizado en orden a la utilización de la información. En todo caso, parece claro que la entrada de una autoridad judicial independiente y los compromisos adquiridos en materia de auxilio judicial posibilitarán un examen más avanzado de estas cuestiones que permita superar los déficits que eventualmente puedan apreciarse respecto de la información más sensible.

En todos los casos, tales decisiones deberán documentarse. En la mayoría de los casos, esta garantía se documentará mediante una expresión formularia que en todo caso tendrá fuerza vinculante en orden al tratamiento de datos. Esta documentación quedará a disposición de la autoridad de protección de datos competente, con inclusión de la fecha y la hora de la transferencia, la información sobre la autoridad competente destinataria, la justificación de la transferencia y los datos personales transferidos.

El artículo 43 de la Ley 6/2021 establece que tanto en supuestos de adecuación como de otorgamiento de garantías cualquier transferencia internacional de datos deberá identificar al responsable del tratamiento competente como destinatario de los datos. Sin embargo, cuando se trate de decisiones particularizadas, la ley distingue un diverso nivel de exigencia según si los datos remitidos se dirigen a una autoridad competente o no.

Es difícil saber a qué se refiere la norma al señalar al responsable del tratamiento competente en materia de transferencia internacional de datos. En principio, no habrá problema en aquellos supuestos en que directamente se pueda inferir de una decisión de adecuación. Así, en el caso de la Decisión de Adecuación con el Reino Unido y la Unión Europea, habrá de estarse a lo expresamente indicado en el texto de la decisión, que en este supuesto se remite a las que se indican en la sección 30 de la *Data Protection Act* de 2018, las cuales incluyen a cualesquiera autoridades de diverso rango que en aquel país tengan atribuida la investigación del delito. En el caso de la Ley 6/2018, se trataría conforme al artículo 4 de toda autoridad que tenga competencias encomendadas legalmente para el tratamiento de datos personales en orden a la investigación del delito y, concretamente, además de las autoridades judiciales y el ministerio fiscal, los miembros de las fuerzas y cuerpos de seguridad, instituciones penitenciarias, Vigilancia Aduanera, el SEPBLAC y la comisión de vigilancia de actividades de financiación del terrorismo.

En lo que se refiere a Marruecos, las funciones de investigación se llevan a efecto fundamentalmente a través de la Gendarmería Real de Marruecos, un cuerpo militarizado semejante a la Guardia Civil. Las funciones de la Gendarmería Real en el ámbito de la policía judicial han sido determinadas por la Ley de Enjuiciamiento

Criminal de 1959. Realiza todas estas funciones bajo la dirección del fiscal real y el control del Tribunal de Apelación. Sus funciones consisten en la investigación criminal, la recogida de pruebas, la detención de delincuentes y la ejecución de la orden del juez. La Gendarmería Real, cuando actúa con la condición policía judicial, lo hace de acuerdo con el Tribunal, y su actuación se dirige a detectar y determinar con carácter general cualquier violación de las leyes, y cuando actúa como policía de la fuerza pública, informa al fiscal real de los crímenes y delitos de los que tiene noticia sobre los que no tienen jurisdicción.

11. TRANSFERENCIA A TERCEROS ESTADOS

Cuando los datos personales se transfieran de un Estado miembro a terceros países u organizaciones internacionales, dicha transferencia solo debe realizarse, en principio, después de que el Estado miembro del que se obtuvieron los datos haya autorizado la transferencia. Tanto el derecho marroquí como el derecho europeo son conocedores de estas exigencias que han tenido acogida, desde luego, en el acuerdo de seguridad de 2019. Se prevé, asimismo, que las partes se comprometen a no ceder los datos personales a ningún tercero distinto del órgano solicitante de la parte requirente o, en caso de solicitarse por esta, solo podrán transmitirse a través de sus respectivos departamentos de justicia, previa autorización del requerido.

Sin embargo, en determinados casos particulares, los procedimientos habituales que exigen contactar con la autoridad del tercer país en cuestión pueden ser ineficaces o inadecuados, en particular por no permitir efectuar la transferencia de forma oportuna, o porque dicha autoridad del tercer país no respete el Estado de derecho o las normas y principios internacionales en materia de derechos humanos, en cuyo caso las autoridades competentes deberán evitar la transmisión de aquella información que pueda comprometer los derechos de los titulares de los datos hasta obtener la oportuna habilitación.

12. VÍAS ALTERNATIVAS A LA CESIÓN INTERNACIONAL DE DATOS. LA FIRMA POR MARRUECOS DEL SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO DE BUDAPEST

Como hemos venido exponiendo, la ratificación del segundo protocolo adicional del Convenio de Budapest, suscrito ahora por Marruecos, va a habilitar una vía alternativa para la cesión internacional de datos. El protocolo supone un salto cualitativo respecto de los instrumentos de cooperación tradicionales, que se justifica por la necesidad de definir la acción de los Estados en un entorno virtual como es la red. La creación del Convenio de Budapest surge inicialmente como un intento de armonizar la legislación de los Estados para afrontar el fenómeno de la «ciberdelincuencia». La finalidad última es evitar la creación por los delincuentes de paraísos digitales excluidos de la acción de la justicia. Se pretende, en suma, evitar que los criminales puedan aprovecharse de la falta de consenso de los límites de la jurisdicción para procurar su impunidad.

Con todo, y pese a la voluntad de los Estados firmantes de extender la acción penal más allá de sus fronteras, el Convenio no llega a cuestionar directamente el principio de territorialidad. Establece, eso sí, diversos cauces alternativos que permiten eludir las consecuencias de un entendimiento estricto de las reglas de conflicto que impidiesen el ejercicio de la acción represiva de los Estados[78].

Concretamente se arbitran cuatro mecanismos excepcionales, que permiten violentar el acceso a los sistemas informáticos, a saber, el acceso a fuentes abiertas, el consentimiento de los interesados, la intermediación de proveedores de servicios asentados en la jurisdicción territorial y el acceso a datos informáticos libremente accesibles desde otro sistema informático. Como veremos, el segundo protocolo adicional va a ampliar enormemente las facultades conferidas a los Estados para investigar la comisión de delitos en la red, confiriendo en determinados supuestos la posibilidad de dirigirse directamente a las empresas prestadoras de servicios de internet sin necesidad de recabar el auxilio judicial internacional.

La regla general, no obstante, sigue siendo que el acceso debe quedar condicionado, no tanto por la ubicación física de los servidores como por el control de la transferencia de los datos. Según el informe explicativo del Convenio, el término «posesión o control» se refiere no solo a la posesión física de los datos en cuestión en el territorio de la parte ordenante, sino también a las situaciones en las que los datos que deben presentarse están fuera de la posesión física de la persona, pero esta puede, no

78 Algunos autores han puesto de manifiesto los riesgos de la exclusión del principio de territorialidad, poniendo la necesidad de incrementar los esfuerzos no tanto en ampliar las facultades de los Estados fuera de su propio ámbito como de restringir la interferencia de aquellos otros Estados poco propicios a la lucha contra la cibercriminalidad. ARNELL, P. y FATUROTI, B., «The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted», *International Review of Law, Computers & Technology*. DOI: 10.1080/13600869.2022.2061888.

obstante, controlar libremente la producción de los datos desde en el territorio de la parte ordenante[79].

La cuestión depende en última instancia del compromiso de los Estados de no violentar las barreras de seguridad de los programas informáticos que ostentan las grandes multinacionales del sector. De hecho, los programas informáticos cuentan con cortafuegos, algoritmos encriptados y toda clase de medidas de seguridad que suponen de suyo una primera barrera a la acción de los Estados. Lo peculiar del caso es el reconocimiento de este estatus, pese a no establecerse cuáles puedan ser las consecuencias de tal transgresión. Si ciertamente no existe una previsión sobre las consecuencias de una extralimitación en el medio virtual, como pueda ocurrir en la circunscripción territorial, parece claro que el reconocimiento de la existencia de estos ámbitos de información excluidos de la interferencia estatal es un hecho[80].

Con todo, resulta un punto polémico, en el que el Convenio de Budapest no establece sino un consenso de mínimos. Así, en el caso de Marruecos, Omar Seghrouchni, presidente de la Comisión Nacional para el Control de la Protección de Datos Personales, en su intervención en el seminario titulado «Protección de datos personales e identidad digital», se refirió a una deliberación de la Comisión, en 2020, que sentó las bases para las directrices sobre una arquitectura de identificadores que abogan por la separación de los lugares de almacenamiento de los datos de uso y los de los datos de autenticación[81].

Hasta entonces no se había abordado suficientemente el riesgo tangible que implicaría que, con base en el mismo Convenio, bajo el pretexto de proteger a los ciudadanos contra el mal uso de las tecnologías de la información y las comunicaciones, la posibilidad de que Estados con regímenes autoritarios justifiquen violaciones a derechos humanos e incluso, paradójicamente, mediante el mal uso de las tecnologías de la información y las comunicaciones, cometan delitos informáticos en contra de sus ciudadanos[82].

---

79 MILIART, J.-B., «The limits of subjective territorial jurisdiction in the context of cybercrime», *Era Fórum* 2019, núm. 19, p. 386.

80 Al comentar el artículo 19, el memorándum de la Convención (*explanatory report*) en su apartado 184 señala qué en muchos casos los datos informáticos almacenados *per se* no se consideran un objeto tangible y, por lo tanto, no pueden asegurarse en nombre de las investigaciones y los procedimientos penales de forma paralela a los objetos tangibles, salvo asegurando el soporte de datos en el que están almacenados. «El objetivo del artículo 19 de este convenio es establecer un poder equivalente en relación con los datos almacenados».

81 Véase «L'expérience marocaine en matière de protection desde donées personelles mise en exergue à Tunis». (maroc-diplomatique.net). https://maroc-diplomatique.net/lexperience-marocaine-en-matiere-de-protection/.

82 *CETS 185 - Explanatory Report to the Convention on Cybercrime.* (coe.int). https://rm.coe.int/16800cce5b.

En vista de que no se ha otorgado mayor consideración a esta posibilidad ni se ha discutido suficientemente, se estimó fundamental que la sociedad civil participase en los procesos de adopción e implementación del Convenio de aquellos Estados, con altos índices de corrupción e impunidad y bajos niveles de transparencia y rendición de cuentas, que decidan adherirse. De igual forma, es necesario que los Estados e incluso la comunidad internacional den especial seguimiento a los instrumentos jurídicos y mecanismos de cooperación que de ello deriven, incluyendo su respectiva aplicación[83].

Si dichos procesos de implementación, instrumentos jurídicos y mecanismos de cooperación no gozasen de las debidas garantías de transparencia, publicidad, objetividad, imparcialidad, legalidad y exacta aplicación de la ley penal, así como de mecanismos suficientes de supervisión independiente y de rendición de cuentas, la efectividad del Convenio para alcanzar su objetivo —proteger a los ciudadanos contra el mal uso de las tecnologías de la información y las comunicaciones— se tornaría lejana e, incluso, contraproducente[84].

El protocolo adicional al que ahora se adhiere Marruecos abre cuatro nuevas vías de acceso por los investigadores a los datos remotos a través de internet:

— La posibilidad de compartir datos entre varios países a través de equipos conjuntos de investigación. Esta posibilidad, en principio, no presenta especiales problemas y ya se venía realizando, pero siempre supeditada a los acuerdos internacionales de traspaso de datos. Se pretende ahora dar el marco legal y concretar el tipo de investigaciones que puedan llevarse a cabo por este cauce. Las legislaciones de ambos países no prevén una legislación uniforme en esta materia y ni el Convenio de auxilio y cooperación en materia de seguridad de 2019 ni el de Asistencia Judicial en materia penal de 2009 contienen tampoco previsiones al efecto. Sí ha habido reuniones periódicas de carácter informal en el ámbito propiamente policial a través de los centros de cooperación policía[85]. Bajo el mandato de la ministra española Dolores Delgado y su homólogo Mohamed Aujir, hubo una iniciativa en este sentido, pero estos intentos se han limitado a aspectos puntuales en materia de terrorismo y siempre dentro del marco policial[86].

— Las solicitudes de información de acceso al registro de dominios de internet. El acceso a la titularidad de los dominios es limitado. Dichos datos no deberían estar

83 Council of Europe, T-CY Public Hearing, June 3, 2013. https://www.coe.int/en/web/cybercrime, p. 4 .

84 Transborder Group informe de diciembre de 2012 (T-CY[2012]3), parágrafos 309 y 310.

85 BARRENECHEA, L., «Mecanismos e iniciativas de cooperación hispano-marroquí contra el terrorismo», *Revista electrónica de estudios internacionales* (REEI), 2016, núm.31, p. 28.

86 Véase en este sentido «Marruecos y España estrechan su colaboración en Justicia con propuestas de reforma de su convenio de asistencia en materia pena», publicado en *El Confidencial*: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/justicia/Paginas/2018/301018-justicia.aspx.

disponibles en relación con los contenidos alojados en un dominio, salvo orden de la autoridad competente (que debería ser una autoridad judicial independiente) y con arreglo a condiciones y garantías de protección de la intimidad. Los contenidos alojados en los sitios web bajo un determinado nivel de dominio suelen ser publicados por alguien distinto del titular del registro, pero bajo el control del usuario del servicio. Por ello, el sistema de nombres de dominio no debe convertirse en un punto de control para que los Gobiernos interfieran en la libertad de pensamiento y la actividad en línea de los usuarios. El contenido de un sitio web puede revelar una gran cantidad de información sensible y de información privada, como las creencias políticas y religiosas y las orientaciones sexuales. Con todo, el dato instrumental e inocuo de la procedencia del nombre de dominio, sin acceder a los contenidos privados, no puede poner en riesgo la intimidad del dato en sí mismo considerado. Se confiere, así, a los Estados amplios poderes para obtener la identidad de los registrantes de nombres de dominio, estableciéndose las debidas salvaguardias. El no hacerlo así crearía un efecto drástico de enfriamiento de la libertad expresión debido al miedo a las represalias y a la censura.

— La posibilidad de transmitir información por medio de la oficina de puntos de contacto en que se encontraran responsables de todos los Estados parte. Esta oficina permitirá la transferencia en tiempo real y de forma acelerada de datos, agilizando la remisión de las solicitudes sin sujeción a especiales formalidades, y solventar las eventuales deficiencias o excesos de las solicitudes. Estos puntos de contacto estarán habilitados para dirigirse directamente a los proveedores de servicio dependientes de los Estados a quienes representan, evitando traslados a través de instancias intermedias. Conforme al artículo 9, apartado cuarto, se permite la remisión de estas solicitudes no solo en formato electrónico, sino incluso oralmente, sin perjuicio de que se pueda exigir una confirmación en forma telemática. Podrán exigirse también niveles adecuados de seguridad y autenticación antes de aceptar la solicitud.

— El acceso y revelación de información en supuestos de urgencia. La convención distingue dos supuestos: el previsto en el artículo 10 del protocolo, que se limita a las emergencias que justifican esa acción rápida a través de la oficina que coordina los puntos de contacto, por medio de internet e incluso directamente entre autoridades judiciales, por otra parte, el párrafo 3 del artículo 25 del Convenio habilita la posibilidad de que las solicitudes de asistencia mutua puedan hacerse por medios de comunicación acelerados en circunstancias urgentes que no alcanzan el nivel de emergencia definido. En otras palabras, el párrafo 3 del artículo 25 tiene un alcance más amplio que el artículo 10 del protocolo, en el sentido de que abarca situaciones no contempladas en aquel precepto, como puedan ser los riesgos actuales, pero no inminentes, para la vida o la seguridad de las personas, la posible destrucción de pruebas que puedan resultar de la demora, la proximidad de la fecha del juicio u otros tipos de urgencias.

El Comité Europeo de protección de datos, siguiendo la jurisprudencia del Tribunal de Justicia de la Unión Europea —STJUE de 8 de abril de 2014, Digital Rights Ireland, EU:C:2014:238), STJUE de 21 de diciembre de 2016, Tele2, EU:C:2016:970, STJUE de

6 de octubre de 2020, Quadrature du Net, ECLI:EU:C:2020:791, STJUE de 5 de abril de 2022, An Garda Síochána, EU:C:2022:258, y STJUE de 20 de septiembre de 2022, ECLI:EU:C:2022:703—, estimó que el tipo de autoridades solicitantes que pueden emitir dicha solicitud debe limitarse a un fiscal, una autoridad judicial u otra autoridad independiente[87]. El CEPD estimó también que la participación sistemática de las autoridades judiciales de las partes requeridas es esencial para garantizar un examen del cumplimiento efectivo de las solicitudes de conformidad con el Convenio y para preservar la aplicación del principio de doble tipificación en el ámbito de la cooperación judicial. En aquel caso, dicha interpretación queda en el orden interno, pero resulta manifiesto que habrá de ser un condicionante en orden a la aplicación de sus previsiones[88]. Se pretende, en todo caso, minimizar los riesgos asociados a la divulgación acelerada de datos informáticos almacenados en caso de emergencia[89].

El protocolo contiene mecanismos de responsabilidad y supervisión pública. Estos incluyen sanciones en caso de abuso flagrante o sistémico de los poderes de emergencia por parte de alguna de las partes firmantes del protocolo. Se prevén también informes estadísticos y cualitativos sobre el volumen de divulgación acelerada que deben ser publicados anualmente.

Los proveedores de servicios también están obligados a publicar informes de transparencia. Aunque este requisito debería aplicarse a todas las solicitudes transfronterizas, es especialmente útil para las solicitudes de emergencia, dado su potencial de extralimitación, pues permite una previsión por adelantado del régimen de garantías que deba aplicarse al caso.

Por último, en cuanto a la autorización de las solicitudes verbales de emergencia, estas deberían ir seguidas inmediatamente de una solicitud por escrito para la rendición de cuentas.

Pero, como ha quedado indicado, la nota más destacada de esta normativa son las garantías contenidas en orden a la transferencia de datos de carácter personal que se contienen en el artículo 14, precepto que presentó las mayores dificultades en orden a la aprobación del protocolo. Este es el artículo más detallado de su texto y fue también

87 Sobre este particular nos remitimos a la crítica que efectuamos a la línea jurisprudencial sobre las dificultades en orden a discernir cuáles son aquellos elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario. GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., «La retención preventiva y recopilación de datos del proceso comunicativo. El difícil camino hacia la cuadratura del círculo». Artículo monográfico SEPIN. SP/DOCT/107189. Diciembre de 2020, p. 26 y ss.

88 Declaración 2/2021 sobre el nuevo proyecto de disposiciones del Segundo Protocolo adicional al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest), p. 4.

89 Véase en este sentido el Informe 3/2019 del Supervisor Europeo de Protección de datos, de 2 de abril de 2019, apartado 21, *aditional recommendations*, en el que insiste en la importancia de establecer en estos supuestos específicas salvaguardias en el caso de transferencias a terceros países.

el más difícil de negociar, atendidas las limitaciones establecidas para aquellos países, que, como Marruecos, no se encuentran incorporados a un marco jurídico integrado como es la Unión Europea. Conforme al apartado 220 del informe expositivo que se adjunta al protocolo y que se dedica a este precepto, su finalidad es establecer las salvaguardias necesarias en orden a la protección de datos que permiten a las partes cumplir con los compromisos internacionales en materia de protección de datos[90].

Para alcanzar este objetivo se tuvo que cumplir con los requisitos de diferentes Estados con marcos jurídicos bastante diferentes para la protección de datos personales, sin embargo, sus previsiones quedaban excluidas si se podían acoger otras más favorables, como pudieran ser un acuerdo de transferencia internacional de datos o un acuerdo bilateral con este exclusivo propósito, cuestiones que hemos abordado al tratar de los diversos instrumentos de transferencia internacional de datos.

La aplicación de este artículo estará sujeta a las evaluaciones previstas en el artículo 23 del protocolo y, cuando haya pruebas de un incumplimiento sistemático o material de las obligaciones de protección de datos, podrá invocarse como último recurso el apartado 15 del artículo 14, relativo a la consulta y la suspensión. El protocolo no pretende ser un instrumento de protección de datos, sino un tratado de cooperación penal, por lo que las ambiciosas pretensiones del artículo 14 se limitan a los datos personales destinados a los fines que son propios de la investigación penal. Sin embargo, es probable que contribuya a reforzar los regímenes de protección de datos entre los Estados partícipes en consonancia con el Convenio 108 sobre protección de datos del Consejo de Europa, como ya venía ocurriendo con la versión inicial del Convenio de Budapest.

Las medidas del protocolo distinguen entre los distintos tipos de datos que deben revelarse. Por ejemplo, los artículos sobre la cooperación directa con los responsables de tratamiento (artículo 6) y los proveedores de servicios (artículo 7) solo se refieren a la información de registro de nombres de dominio o a la información de los abonados, respectivamente, y no a datos más sensibles sobre el tráfico o el contenido.

90 Explanatory Report, accesible desde: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b.

13. CONSIDERACIONES FINALES

Una visión de conjunto de las iniciativas que se están realizando por las autoridades de Marruecos pone de manifiesto un extraordinario desarrollo de las cuestiones relativas a la protección de datos tan sensibles para la Unión Europea. Se constata también la existencia de iniciativas de diverso sentido, unas dirigidas a la adecuación a la normativa con la Unión Europea y otras en orden a la protección del orden jurídico interno. Dentro de este panorama resulta fundamental la posición del Centro Nacional de Protección de Datos, que está llevando a efecto una labor de concienciación de la sociedad civil en esta materia, llegando a acuerdos de gran interés con las multinacionales del sector.

La inmersión en las nuevas tecnologías resulta muy avanzada en relación con los países de su entorno. El proceso de incorporación al expediente digital se encuentra también muy adelantado y es reflejo de los avances tecnológicos que se están produciendo en todos los órdenes en el país[91]. El intercambio de información es igualmente incesante, atendidas las necesidades de colaborar frente al crimen organizado[92].

Dentro de este marco, el Convenio entre el Reino de España y el Reino de Marruecos sobre cooperación en materia de seguridad y de lucha contra la delincuencia organizada nos muestra la línea que habrá de seguirse en los próximos años ante la ausencia de una decisión de adecuación en esta materia, siendo destacable la voluntad de alcanzar acuerdos sectoriales que permitan avanzar en orden a la consecución de objetivos específicos. El nuevo canal de transmisión de información se contrapone a la falta de previsiones en los convenios de auxilio jurisdiccional penal en materia de protección de datos, los cuales requerirán una determinación de la información más particularizada respecto del origen y destino de la información más sensible.

Con todo, los intentos fallidos en orden al logro de una decisión de adecuación deben ponernos en alerta de que todavía queda mucho camino por recorrer. Las amplias facultades de empleo de información sensible con fines de seguridad nacional, la ausencia de una regulación acabada en materia de datos de tráfico o el distinto punto de vista en relación con las cuestiones de género nos dan una idea de las dificultades que deberán de lidiarse en esta materia.

Hemos apreciado también una muy distinta perspectiva respecto del tratamiento de datos en orden a la creación de bases de datos ordenadas a la investigación de los

91 SOUMAYA, A. y KWIZERA, D., «Le numérique et le paradigme juridictionnel : comprendrè l'incidence de la transformation numérique sur la performance du Système Judiciariser au Maroc», *Revue Droit & Societe*, diciembre de 2021, núm. 4, p. 50.

92 CISSÉ, A., «Exploration sur la cybercriminalité et la sécurité en Afrique: état des lieux et priorités de recherche; synthèse des rapports nationaux», Centre de Recherches pour le Développement International, IDR-CRDI, enero 2011, p. 12, accesible en: https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/47118/133493.pdf.

delitos, en que igual se constata que, frente a la regulación general de esta materia, la ordenación marroquí opta por una regulación sectorial en función de cada tipo de fichero.

Queda, además, en el aire una calculada ambigüedad en orden a la consecución de los fines que son propios: el intercambio de información recíproca sobre investigaciones en curso en las distintas formas de la delincuencia organizada, incluido el terrorismo, sus relaciones, estructura, funcionamiento y métodos. En muchos supuestos, tal intercambio de información, al margen de las vías jurisdiccionales adecuadas, puede comprometer información sensible que debería estar sometida al control judicial, o ,cuando menos, bajo el control de una autoridad administrativa independiente.

La solución a muchas de estas deficiencias en una sociedad especialmente compleja como es la marroquí —donde la población rural representa un peso específico y en que las nuevas tecnologías tienen un desarrollo muy desigual dependiendo del territorio— es dar una valoración particularizada respecto de cada tipo de actividad, estableciendo los programas o criterios de actuación sectorial en atención a los medios y recursos afectados. No se trata de obtener un reconocimiento general, sino de establecer en función de las circunstancias del caso los mecanismos de corrección necesarios que permitan dar cumplimiento a las exigencias de la Unión Europea en materia de transferencia internacional de datos.

BIBLIOGRAFÍA

AL-HUSSEINI, A. A., مدى مشروعية التسجيل الصوتي بالهاتف النقال كدليل في الاثبات الجنائي, «La legalidad de la grabación de voz en teléfonos móviles como prueba en la prueba penal», *Revista Ahl al-Bayt*, 2009, núm. 8, pp. 166-203.

ARNELL, P. y FATUROTI, B., «The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted», *International Review of Law, Computers & Technology*, 2022. DOI: 10.1080/13600869.2022.2061888.

BARRENECHEA, L., «Los otros efectos colaterales del 11 de septiembre», *Revista de Derecho Migratorio y Extranjería*, 2007, núm. 14, p. 225 y ss.

BARRENECHEA, L. «Mecanismos e iniciativas de cooperación hispano-marroquí contra el terrorismo», *Revista electrónica de estudios internacionales* (REEI), 2016, núm. 31, pp. 1-29.

BENCHEMSI, A., «Morocco: Outfoxing the Opposition», *Journal of Democracy,* 2012, 57 (enero). http://www.journalofdemocracy.org/sites/default/files/Benchemsi-23-1.pdf.

BOSSI, M., «Processing data to Third Countries or International Organizations», *Arribat – International Journal of Human Rights*, 30 de septiembre de 2021, vol. 1, cuestión 2, pp. 176-186.

BRADFORD, A., «The Brussels Effect: How European Union Rules de World» (OUP 2020),Kindle Edition, pp. 132-136.

BROWN, Cameron S. D., «Investigating and prosecuting cybercrime: forensic dependencies and barriers to justice», *International Journal of Cyber Criminology*, enero de 2015, vol. 9, núm. 1, pp. 55-119. DOI 10521/Zennodo.22387.

BYGRAVE, L., «The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects», *Computer Law & Security Review*, abril de 2021, vol. 40, Norwegian Research Center for Computers and Law, Department of Private Law, University of Oslo, Norway.

CISSÉ, A., «Exploration sur la cybercriminalité et la sécurité en Afrique: état des lieux et priorités de recherche; synthèse des rapports nationaux», Centre de Recherches pour le Développement International, IDR-CRDI, enero de 2011. https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/47118/133493.pdf.

CHENAOUI, H., «Morocco data protection law: Moving to align with EU data protection». https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection/ (consulta: julio 2022).

DE MIGUEL ASENSIO, P. A., «Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia». *La Ley Unión Europea*, 2015, núm. 31.

EL HOURRI, A., «Protection des donées pesonnelles: le Maroc vers la ratification de la "Convention 108"», *Medias 24*, publicado el 14/02/2022 y modificado el 16/02/2022, https://medias24.com/2022/02/14/protection-des-donnees-personnelles-le-maroc-ratifie-la-convention-108/ (consulta: junio de 2022).

GONZÁLEZ FUSTER, G. *The Emergence of Personal Data Protection as a Fundamental Right of the European Union*, *Law, Science, Technology and Society*. Bruselas: Springer, 2014.

GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., «La retención preventiva y recopilación de datos del proceso comunicativo. El difícil camino hacia la cuadratura del círculo». *Artículo monográfico SEPIN*. SP/DOCT/107189, diciembre de 2020.

GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., «El nuevo protocolo del Convenio de Budapest de lucha contra la cibercriminalidad». (RI §425241) *Revista General de Derecho Procesal*, 2022, núm. 58.

GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información», *La Ley Penal*, núm. 125, Sección Estudios, marzo-abril 2017.

KUNER, C., «The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards». *National Law School of India Review*, 2021, vol 37.

LLORENTE, Á., «La cooperación judicial antiterrorista entre España y Marruecos», Real Instituto El Cano, Área de Terrorismo Internacional, ARI 174/2010, 20.12.20.0, pp. 1-8.

MAKULILO, B. A., «Data Protection Regimes in Africa: too far from the European 'adequacy' standard?». *International Data Privacy* Law, 2013, vol. 3, núm. 1.

MAKULILO, B. A., *African Data Privacy Laws*, Universidad de Bremen: Springer, 2016.

MARTÍNEZ DE CAPDEVILA, C., «"El estatuto avanzado" de Marruecos en la Unión». Revista de Derecho Comunitario Europeo 2009. núm. 34, pp. 895-914.

MILIART, J.-B., «The limits of subjective territorial jurisdiction in the context of cybercrime». *Era Fórum,* 2019, núm. 19. 375-390.

RENTELN, A. D., *International Human Rights: Universalism Versus Relativism.* Quid pro books, 2013, Kindel Edition.

RUIZ TARRÍAS, S., «La sentencia del Tribunal de Justicia de la Unión Europea en el Caso Schrems II o cómo los datos personales pueden terminar viajando sin equipaje». *Revista Española de Derecho Europeo,* núm. 76, octubre-diciembre de 2020, pp. 111-162. DOI:10.37417/num_76_2020_532.

SOBRINO GARCÍA,, I. «Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y los Estados Unidos». *Revista de Derecho Comunitario Europeo, Centro de Estudios Políticos y Constitucionales*, enero-abril de 2021, núm. 6, pp. 226-256.

SOUMAYA, A. y KWIZERA, D., «Le numérique et le paradigme juridictionnel : comprendrè l'incidence de la transformation numérique sur la performance du Système Judiciariser au Maroc». *Revue Droit & Societe*, diciembre de 2021, núm. 4, pp. 36-53.

TASSINARI, F., «The Externalization of Europe's Data Protection Law in Morocco: an Imperative Means for the Management of Migration Flows», *Peace & Security – Paix et Sécurité Internationales*, 9, 2021, núm. 9.

USTARÁN, E. y GARCÍA, P. «Transferencias internacionales de datos». *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales,* coord. por Artemi Rallo Lombarte, 2019, pp. 459-490.

VILCHES DE MORAGUES, P., «Ser juez en Marruecos y España». *Seminario Fundación CIDOB,* Barcelona, España.

WALLE, E., «Le Maroc adopte une loi sur la protection des données personnelles». *Gazette du Palais,* octubre de 2009, núm. 21/22, pp. 2934-2937.

Maquetación:
Ministerio de Justicia
Secretaría General Técnica
Subdirección General de Documentación y Publicaciones