



Universidad
de Alcalá



PRESENTE Y FUTURO DEL EMPLEO DE LAS NUEVAS TECNOLOGÍAS EN LOS DOCUMENTOS DE IDENTIDAD

**PRESENT AND FUTURE OF THE USE OF NEW
TECHNOLOGIES IN IDENTITY DOCUMENTS**

AUTOR

JOSÉ MANUEL SAIZ ALIAGA

Dirigido por:

D. Enrique Sanz Delgado. Tutor de la Universidad de Alcalá de Henares

D. Antonio Jesús Llamas Guerra. Tutor Servicio de Criminalística Guardia Civil

**MÁSTER UNIVERSITARIO EN
CIENCIAS POLICIALES**

(Trabajo fin de Máster – 12 ETCS)

2020-2021

iuicp

INSTITUTO UNIVERSITARIO DE INVESTIGACIÓN EN CIENCIAS POLICIALES

AGRADECIMIENTOS

Me quiero acordar en este momento, en el cuál quiero dar las gracias a todos los profesores que han impartido sus clases con gran dedicación y profesionalidad haciéndolas amenas y comprensibles.

Gracias a los Tutores por su paciencia, comprensión y especialmente por su gran profesionalidad, exquisita docencia en el tema elegido y por la ayuda que me han prestado en la orientación y confección de este TFM.

Gracias en general, a la Dirección del Máster y a las personas que me han dado la oportunidad de realizarlo y haber confiado en la realización del mismo.

Les quiero dedicar este TFM con cariño especial a mis padres, familia y amigos, por animarme y saber que siempre están ahí, en los buenos y malos momentos dando ánimos.

A todos los mencionados mi más afectuoso y respetuoso agradecimiento.

ÍNDICE

RESUMEN- PALABRAS CLAVE	1
INTRODUCCION	2
OBJETIVOS	4
1.-DOCUMENTOS DE IDENTIDAD	5
2. EL PASAPORTE COMO MODELO REFERENCIAL DE LOS DOCUMENTOS DE IDENTIDAD	8
2.1.-Marco regulador de los pasaportes.	8
2.2.- Fortalezas y debilidades de los documentos de identidad.	21
2.3.-Tipologías de fraudes.	29
3.-PROTECCIÓN JURÍDICA DE LOS PASAPORTES Y OTROS DOCUMENTOS DE IDENTIDAD	40
4.-FUTURO DE LOS DOCUMENTOS DE IDENTIDAD. BIOMETRIA Y LAS BILLETERAS DIGITALES	49
5.-CONCLUSIONES	68
6.-BIBLIOGRAFIA, WEBGRAFIA Y LEGISLACIÓN CONSULTADA	70

ABREVIATURAS

CE:	Constitución Española
CC:	Código Civil
CP:	Código Penal
TC:	Tribunal Constitucional
STC:	Sentencia Tribunal constitucional
TS:	Tribunal Supremo
STS:	Sentencia del Tribunal Supremo
AP:	Audiencia Provincial
LEC:	Ley de Enjuiciamiento Civil
LEcrim:	Ley de Enjuiciamiento Criminal
LOFCS:	Ley Orgánica de Fuerzas y Cuerpos de Seguridad
LOPSC:	Ley Orgánica de Protección de la Seguridad Ciudadana
LOPDCP:	Ley Orgánica de Protección de Datos de carácter Personal
LOPTP:	Ley Orgánica de Protección a Testigos y Peritos en causas criminales
BOE:	Boletín Oficial del Estado
DOUE:	Diario Oficial Unión Europea
ICAO:	Organización Internacional de Aviación Civil
ENFSI:	Red Europea de Laboratorios de Ciencias Forenses
RAE:	Real Academia de la Lengua Española
Art.	Artículo
ONU:	Organización de Naciones Unidas
AGE:	Administración General del Estado

RESUMEN

A lo largo de los siglos el ser humano se ha visto en la necesidad de ser identificado en sus desplazamientos de un lugar a otro. Esta identificación ha ido evolucionando notablemente con el transcurso de los siglos, de manera particular en las últimas décadas, donde se ha producido una transformación significativa de los documentos de identidad empleados para tales fines.

Esas modificaciones técnicas se han ido realizando principalmente con la finalidad de erradicar su reproducción, lo cual ha resultado materialmente imposible, si bien se ha conseguido al menos reducir o limitar notablemente esos intentos de obtener una identidad supuesta bajo el amparo de un documento falso u otro original sometido a algún tipo de alteración. De ahí la constante necesidad de perfeccionar ese tipo de documentos que acreditan la identidad de una persona o en su caso, buscar e incorporar medios alternativos que autentifiquen a la persona que lo porten como la billetera digital.

PALABRAS CLAVE: Documento de identidad, medida de seguridad, biometría, sistemas de impresión, contrastes de seguridad, billetera digital.

ABSTRACT

Throughout the centuries, human beings have found it necessary to be identified in their movements from one place to another. This identification has evolved notably over the centuries, particularly in recent decades, where there has been a significant transformation of the identity documents used for such purposes.

These technical modifications have been carried out mainly with the purpose of eradicating their reproduction, which has been materially impossible, although it has been possible to reduce or significantly limit these attempts to obtain a supposed identity under the protection of a false document or another original subject to some type of alteration. Hence the constant need to perfect this type of documents that prove the identity of a person or, where appropriate, seek and incorporate alternative means that authenticate the person who carries it like the digital wallet.

KEY WORDS: Identity document, security measure, biometrics, printing systems, security contrasts, digital wallet.

INTRODUCCION

En sus orígenes, las personas eran libres para moverse por el mundo y no existían trabas u obstáculos que imposibilitaran el movimiento de un territorio a otra, sin embargo, con el transcurso del tiempo asociado al desarrollo de las sociedades, se comienza a demandar documentos que sean capaces de acreditar la identidad de las personas que se desplazaban y de las mercancías que se transportaban.

Estos documentos fueron los antecesores del pasaporte que puede considerarse como el documento de identidad referencial a nivel mundial. Sin embargo, son numerosos los tipos de documentos que se engloban bajo la tipología de “identidad” pudiendo definirlo, entre otras formas, como aquel documento oficial emitido por la Administración que sirve para identificar a las personas por su nombre, nacimiento, nacionalidad y domicilio¹. En nuestro país el documento básico por excelencia para acreditar la identidad de una persona sería el Documento Nacional de Identidad, el cual puede ser utilizado no sólo dentro de nuestro país sino también en los desplazamientos realizados dentro de la Unión Europea.

Por lo tanto, dado que el pasaporte puede considerarse el documento de identidad por antonomasia y que nos habilita en mayor o menor medida para nuestros desplazamientos por cualquier parte del mundo tomaremos este como referencia para analizar si cumple perfectamente y con suficientes garantías la función para la cual fue creado haciendo una revisión de su situación actual y su previsible evolución, conscientes que alguno de los desarrollos tecnológicos que se produzcan en los próximos años van a incidir de una u otra forma no solo en el diseño y características técnicas de dicho documento sino en la forma en la que las personas van a poder acreditar su identidad en el futuro próximo y que puede afectar en mayor o medida a la supervivencia en sí de dicho documento tal y como lo conocemos actualmente, debido principalmente a la evolución de los sistemas de identificación basados en la integración de rasgos biométricos de la persona como serían el iris, la huella dactilar, la voz, etc., alguno de los cuales ya se encuentran plenamente operativos para facilitar el acceso tanto a recintos o espacios públicos- recintos aeroportuarios- como privados- controles de identificación y acceso a las instalaciones de empresas.

¹ <https://dpej.rae.es/lema/documento-de-identidad>

Como se ha indicado en el apartado anterior, mientras se producen de forma paulatina alguno de esos cambios debemos prestar atención a cómo evolucionan los documentos de identidad disponibles en la actualidad, y muy particularmente los pasaportes, dada la importancia y necesidad cada vez más creciente que tiene el ser humano de desplazarse, por distintas motivaciones, de un punto a otro del mundo.

Asociado a lo indicado debemos de señalar que las Autoridades deben proveer un documento de identidad a cada uno de sus conciudadanos que garantice fehacientemente ésta, dotándole de un conjunto de medidas de seguridad que minimicen o eviten los intentos de su manipulación y posterior uso por parte de bandas organizadas dedicadas al tráfico de estupefacientes, migración irregular y en definitiva cualquier tipo de actividad delictiva que permita a los usuarios transferirse de un país a otro.

Al margen de lo anterior, es decir, el hecho de mejorar la seguridad de ese tipo de documentos, se debería legislar para endurecer las penas vinculadas con las distintas actuaciones que se recogen dentro del delito de falsedad documental asociada a los documentos de identidad, conscientes de la importancia que dichas infracciones son favorecedoras de otras que se pueden expandir en el plano internacional al facilitarse el movimiento de personas bajo el amparo de documentos de identidad falsos o falsificados,

En definitiva, el presente trabajo, independientemente de presentar el estado en el que se encuentran los documentos de identidad, focalizado en el pasaporte, descubrirá hacia donde se encamina la evolución de éstos en las próximas décadas manteniendo la seguridad y eficacia demostrada hasta el momento actual para garantizar el fin para el que fueron creados.

OBJETIVOS

Dada la importancia que tiene la acreditación de la identidad de cualquier persona para la ejecución de multitud de servicios y actividades que efectúa en su actividad cotidiana, la cual se realiza fundamentalmente a través de la exhibición y verificación de un documento de identidad, por medio del presente Trabajo Fin de Máster (T.F.M.), cuyo contenido se centra en el pasaporte como modelo referencial, se persiguen los siguientes objetivos:

- Determinar el marco normativo regulador de dicho documento a nivel internacional.
- Informar sobre la protección legal que existe a nivel nacional frente a la falsificación documental.
- Informar sobre las fortalezas y debilidades que presentan los documentos de identidad actualmente frente los intentos de manipulación y/o alteración del contenido de los mismos.
- Señalar cuál es el presente y futuro de las nuevas tecnologías aplicadas a los documentos de identidad, como medio para erradicar o disminuir las falsificaciones de éstos y consecuentemente mejorar su seguridad.

1. DOCUMENTOS DE IDENTIDAD.

Antes de entrar en detalles sobre algunos de los tipos de documentos de identidad que existen debemos partir de lo que entendemos como documento, para lo cual podemos utilizar alguna de las definiciones o conceptos empleados por los expertos forenses en el análisis de éstos una de las cuales lo asocian con el soporte material, sustrato papel o polímero plástico, que incorpora datos, hechos o narraciones y que sirve para fijar, perpetuar o demostrar, a través de la grafía o de la impresión, identidades, autorizaciones, certificaciones, derechos, negocios o declaraciones de voluntad que en su ausencia serían de difícil acreditación.

Una subsiguiente clasificación podría venir determinada en función de la autoría de emisión del documento en cuestión del que estemos hablando, así pueden distinguirse tres clases o grupos de documentos²:

- a) **Documentos públicos**, es decir, los autorizados por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias y con los requisitos exigidos por la Ley en cada caso.
- b) **Documentos oficiales**, esto es, los expedidos y firmados por funcionarios o empleados públicos, en el ejercicio de sus funciones públicas y conforme a su legislación específica. La diferencia con los públicos estriba en que éstos no tienen atribuida la facultad de dar fe pública.
- c) **Documentos privados**, es decir, todos aquellos en los que no hay intervención de funcionarios como tales, ni en funciones de fedatario ni en otra distinta.

² <https://guiasjuridicas.wolterskluwer.es/Content/Documento>

En base a lo anterior, para que un documento pueda ser calificado de público se necesitan los siguientes requisitos³:

- • Que sea autorizado por funcionario, es decir, por persona que reúna la calificación jurídica de tal.
- • Que dicho funcionario tenga atribuida la facultad de dar fe pública.
- • Y que además actúe (el mencionado funcionario) en el ámbito de sus competencias y con cumplimiento de los requisitos exigidos por la Ley en cada caso.

Ese documento que cumple con las indicaciones manifestadas va a permitir la identificación personal e inequívoca de los ciudadanos en todos los escenarios o ámbitos de relación dentro de la sociedad. Dentro de este tipo de documentos a su vez nos encontraríamos con los denominados “de identidad”, cuya definición la podremos hallar en numerosas fuentes como la R.A.E.⁴ y en la que encajaría perfectamente el pasaporte, así como, entre otros, los siguientes: Documento Nacional de Identidad (D.N.I); Número de Identificación Fiscal (N.I.F.); Número de Seguridad Social; Número de Identidad de Extranjero (N.I.E.); Permiso de Residencia de la U.E.

Dado que abarcar el estudio y evolución del conjunto de dichos documentos sería demasiado extenso, tomaremos como referencia uno de ellos, en concreto, el pasaporte, al ser éste un documento de identidad cuyo valor trasciende más allá de las fronteras de un país al tiempo que permite analizar en mejor medida la situación actual y futura de aquéllos al permitir integrar un conjunto más amplio de medidas de seguridad que cualquier otro tipo de documento de similares características, por lo que nuestro trabajo empleará como patrón referencial dentro de los documentos de identidad el aludido pasaporte, el cual aparece definido como “un documento

³ <https://guiasjuridicas.wolterskluwer.es/Content/Documento>

⁴ Según la R.A.E. son documentos de identidad “aquellos documentos oficiales emitidos por la Administración que sirven para identificar a las personas por su nombre, nacimiento, nacionalidad y domicilio.

público, personal, individual e intransferible”⁵ en el Real Decreto 896/2003. Lo expide la AGE, que permite acreditar fuera del territorio nacional la identidad y nacionalidad de los ciudadanos españoles.

Por otro lado, dentro del ámbito de la documentoscopia se define como documento de identidad aquel que tiene un valor potencial y que está protegido contra la falsificación por medidas de seguridad adecuadas. Estas medidas deben de ser inusuales y diversas para evitar en lo posible su reproducción o imitación, el empleo por parte de impostores o su transferibilidad ilegal.

Dentro de ellos podemos clasificarlos en tres niveles, según su finalidad y los recursos que la autoridad o entidad de expedición dispone para su confección⁶.

- Documentos de nivel bajo o Tarjetas de afiliación, de transporte, entradas de cine, etc.
- Documentos de nivel medio o Certificados de nacimiento, defunción, matrimonio, divorcio, educativos. o Sellos oficiales, etiquetas. o Distintivos de identidad, billetes de avión, documentación de vehículos, entre otros.
- Documentos de nivel alto o pasaportes, cartas de identidad, visados, papel moneda, etc (dependiendo de la autoridad de expedición).

Como observamos, de lo indicado anteriormente podemos extraer que tanto los pasaportes como las cartas de identidad poseen, a efectos de su protección, un nivel de seguridad más elevado, y por lo tanto se le implementan un conjunto amplio de medidas de seguridad para evitar o minimizar los ataques y garantizar de esta forma la finalidad para la que fueron creados, es decir, para identificar a su portador.

⁵ Artículo 1 Real Decreto 896/2003, de 11 de julio por el que se regula la expedición del pasaporte ordinario y se determinan sus características.

⁶<https://www.studocu.com/es/document/universidad-pontificia-comillas/policia-cientifica/tema-4-documentoscopia-intro/4742900>

2. EL PASAPORTE COMO MODELO REFERENCIAL DE LOS DOCUMENTOS DE IDENTIDAD.

Una vez que hemos explicado en el apartado anterior algunos conceptos vinculados con los documentos de identidad y el carácter que estos tienen vamos a proceder a realizar un análisis de la situación actual del pasaporte, documento de identidad por excelencia. Para ello expondremos cual es el marco regulador del mismo, donde podremos observar que, a pesar de que existe una normativa internacional y europea donde se establece un conjunto de características técnicas que deben tener ese tipo de documentos, nos encontraremos que no existe un formato estándar común a todos los países y que como consecuencia de ello las bandas o grupos organizados podrán actuar más fácilmente sobre aquel tipo de pasaportes cuya vulnerabilidad sea mayor.

En consonancia con lo anterior, realizando una visión desde un prisma más amplio, destacaremos brevemente cuales son las fortalezas y debilidades que presentan estos documentos.

Finalmente, se hará una breve reseña del marco legal español donde se recogen las actuaciones relacionadas con la falsedad documental, los distintos tipos, sujetos activos, penalidad, etc. que nos permitirá formarnos una idea generalizada sobre si los delitos vinculados con la manipulación o alteración documental están o no severamente castigados.

2.1. Marco regulador de los pasaportes.

Uno de los problemas a los que se enfrentan las Fuerzas y Cuerpos de Seguridad a la hora de llevar a cabo un control de identificación de personas en un punto fronterizo o en cualquier otro lugar viene determinado porque no existe una homogeneidad de los documentos de identidad que son sometidos a su examen, por lo que resultará imposible tener memorizado el diseño y características que poseen éstos, y de esa forma, con conocimientos técnicos y el auxilio de alguna herramienta o instrumento proceder a llevar a efecto un chequeo de forma correcta en ciertos supuestos.

A pesar de lo anterior, existe cierta normativa internacional que regula las características técnicas mínimas que deben incorporar algún documento de identidad, en concreto, los pasaportes. Dicha normativa a la que nos referimos es la denominada ICAO 9303, y en el plano europeo, el Reglamento (CE) n.º 2252/2004 y el n.º 444/2009 del Parlamento Europeo y del Consejo. A continuación pasamos a exponer parte de la información técnica extraída de la misma.

2.1.1. Normativa ICAO 9303

La Organización de Aviación Civil Internacional (OACI-ICAO) es un organismo especializado de la ONU que comenzó en el año 1968 con la creación de un grupo de expertos con la misión de elaborar unas recomendaciones para un modelo de libreta o tarjeta de lectura mecánica para acelerar el trámite documental y de identificación en los controles de los puestos fronterizos. Este grupo propuso como técnica el reconocimiento óptico de caracteres o también conocido como “*Optical Character Recognition (OCR)*”⁷ para la lectura más ágil de los documentos. La publicación de estas recomendaciones fue plasmada en un documento llamado “Doc. 9303” y su primera edición se publicó en el año 1980 con el título “*Pasaporte susceptible de lectura mecánica*”.

⁷ Este sistema es un software específico introducido en un ordenador que digitaliza los textos y los identifica automáticamente a partir de unos símbolos o caracteres de un alfabeto para después transformarlos en datos, permite el reconocimiento óptico de una imagen introducida normalmente con un formato de imagen, ya sea escaneada o en fotografía. El programa rastrea los píxeles de la imagen para encontrar coincidencias con los caracteres introducidos previamente y aceptarlos tras un análisis comparativo.

Convenio sobre Aviación Civil Internacional firmado en Chicago (EE.UU.), 7 de diciembre de 1944, entra en vigor el 4 de Abril de 1947 ICAO.

España el 5 de marzo de 1947, ratifica y se adhiere a dicho convenio ICAO.

Países que se puede viajar con pasaporte pero sin visado: Tailandia, Filipinas, Japón, Argentina, México, Vietnam, Malasia, Indonesia o Nueva Zelanda.

Países que a parte del pasaporte, hace falta el visado para viajar: Canadá, EE.UU, China, Rusia, Australia, Cuba, India, Birmania, Camboya y Laos.

Países de la Unión Europea se puede viajar simplemente con el Documento Nacional de Identidad.

En el año 1998 comienza la andadura para un sistema de identificación biométrica con un porcentaje mayor de efectividad. Este sistema adquirió mucha importancia en seguridad y tuvo un detonante con los atentados terroristas del 11 de septiembre del año 2001 en los Estados Unidos de América. Los Estados tomaron conciencia de la importancia de los documentos de viaje y de las medidas de seguridad incluidas en ellos para la identificación de su titular.

Los 188 Estados miembros de la OACI en el año 2005 (Actualmente 193 Estados) aprobaron el inicio de la expedición uniforme con las recomendaciones del Doc. 9303 con una moratoria hasta el año 2010 y con el requisito de caducidad de los documentos que carecen de lectura mecánica en el año 2015.

Estructura del Documento ICAO 9303.

El Doc. 9303 ha sufrido diversas modificaciones. Desde el presente año está vigente la octava edición y consta de trece partes, en las cuales se describe un aspecto específico del Documento de Viaje de Lectura Mecánica (MRTD), destacando especialmente en lo que a medidas y características técnicas a tener en consideración las obrantes en las partes 3 a 7 y la 9, esta última específica de aspectos biométricos.

El Doc. 9303 integra diversos documentos en los cuales se agrupan especificaciones de carácter general (aplicables a todos los MRTD) así como específicas sobre el formato de esos documentos.

Se establecen tres tipos de formatos: DV1, DV2 y DV3.

- DV1 para documentos como el Documento Nacional de Identidad de España.
- DV2 empleado para cartas de identidad como la de Francia o Rumanía, y para el Visado en formato Schengen.
- Y el DV3, empleado para los pasaportes.

Características técnicas comunes en los MRTD.

Para una lectura correcta con los medios adecuados los MRTD y que no solo disponga de un elemento de seguridad como es la propia codificación de la zona de lectura, se necesitan tres

elementos de seguridad verificables por la máquina para minimizar los riesgos. Estos elementos de seguridad verificables por máquina son los siguientes:

- a) Elemento estructura: Es una estructura medible en un elemento de seguridad que contiene algún tipo de información en o sobre la página de datos (p. ej. Imágenes retroreflectantes empotradas en un laminado de seguridad).
- b) Elemento sustancia: Material que no está presente en la inspección ocular del documento (p. ej. Tintas con reacción específicas e inusuales a longitudes de ondas específicas de luz).
- c) Elemento datos: Información oculta que generalmente se incorpora a los datos de personalización, especialmente el retrato (p. ej. Datos codificados en el MRTD en medios magnéticos tales como los hilos de seguridad especiales).

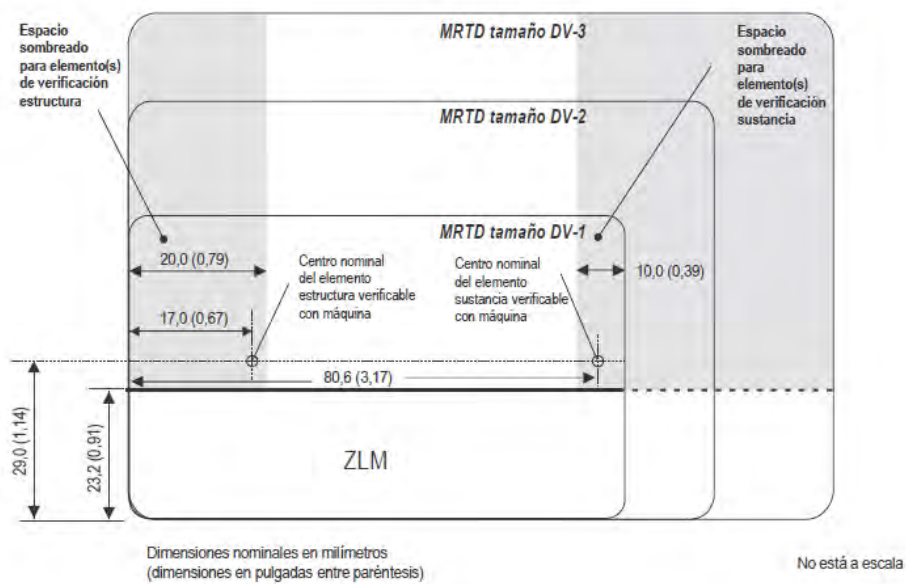


Figura 1. Diagrama con los tamaños de MRTD con la colocación recomendada de los elementos para la verificación del documento con ayuda de la máquina.

En la figura siguiente de un pasaporte utopía, podemos observar una zona de inspección visual (ZIV) que comprende los datos obligatorios y opcionales diseñados para una inspección visual, la página del pasaporte que tradicionalmente llamamos página biográfica.

Para que estos caracteres tengan un lugar específico y uniforme de impresión, el Doc. 9303 establece una zona de lectura efectiva en los tres tipos de modelo, con unas dimensiones fijas de 17 x 118 mm, siendo estas las del modelo mayor (DV3) para permitir el uso de un único lector para todos los tamaños MRTD. Como hemos mencionado anteriormente, para aumentar la seguridad de la zona, se permite la introducción de elementos que no interfieran con la lectura precisa de los caracteres OCR en la banda B900, según la definición de la ISO 1831.

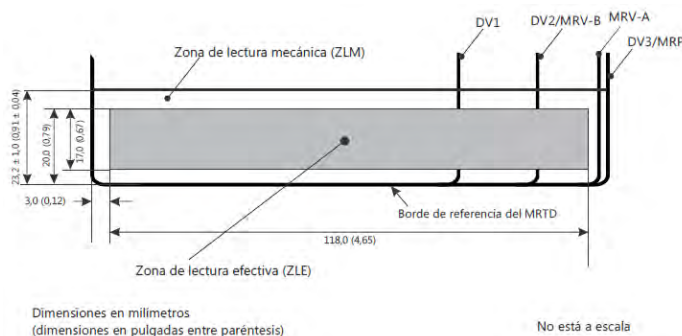


Figura 4. Diagrama esquemático de la zona de lectura efectiva.

Características técnicas en los documentos.

Formato DV1. Los formatos con tamaño DV1, como es el caso del Documento Nacional de Identidad en España, cambia la configuración de la zona de inspección ocular y la zona de lectura mecánica. En este tamaño los caracteres OCR-B se sitúan en el reverso del documento y la fotografía con los datos biográficos en el anverso.

Formato DV2. Utilizado como carta de identidad (p. ej. Estados como Francia o Rumanía) y el Visado con formato Schengen tienen similitudes con la página biográfica de pasaportes (DV3). La zona de inspección visual mantiene la mayoría de las características como son la disposición de la zona de lectura mecánica, fotografía del titular y datos de filiación. Un atributo de la visa es su formato adhesivo, el cual es pegado en una página del pasaporte. Normalmente son utilizadas como autorización para la entrada al país que permite el cruce de la frontera.

Características técnicas de los eMRTD (documentos de viaje electrónicos).

La parte número nueve del Doc. 9303 denomina los eMRTD como documentos de viaje de lectura mecánica con capacidad biométrica y de interfuncionamiento mundial. Los documentos en los tres formatos vistos anteriormente, para el uso de este símbolo tienen que contener un circuito integrado sin contacto, con capacidad de almacenamiento de datos con una capacidad mínima (32 kB), con una codificación con estructura lógica de datos, con una imagen facial del titular del documento y con todos los datos protegidos con una firma digital. El símbolo del eMRTD se situará preferentemente en el anverso de los formatos tarjeta (DV1) y tarjeta-visa (DV2) y en la portada del librito del pasaporte y en la página biográfica.



Figura 8. Imagen del logotipo representativo de un documento de identidad electrónico.

Para la lectura de estos datos biométricos, será necesaria previamente la lectura de los datos OCR-B de la ZLM para aumentar la seguridad del CI sin contacto, así se evitan lecturas del chip fraudulentas. La combinación de este elemento de seguridad electrónico cambiando con los elementos de seguridad descritos anteriormente genera una calidad mayor para la correcta identificación del titular del documento.

2.1.2. Normativa Europea.

El día 23 de junio de 1981 los representantes de los Estados miembros de la Unión Europea se reúnen en el Seno del Consejo y aprueban el empleo de un modelo estandarizado de pasaporte, en lo que refiere a las dimensiones, forma, contenido y ámbito de aplicación. Estas medidas se aprueban como símbolo de unión entre los ciudadanos de los Estados miembros. También pretenden facilitar las comunicaciones que se realicen entre los países de la UE (*Pasaporte único para los ciudadanos europeos*, s. f.).

Entre las decisiones tomadas durante la reunión que tuvo lugar el 23 de junio de 1981 se acuerda que el número de páginas será treinta y dos, salvo que el solicitante justifique que debe hacer uso del documento de manera habitual, solo en ese caso podrá contar con más páginas. En la carátula, encontraremos el número de serie correspondiente y, en el idioma oficial del país de la UE, las siguientes palabras: “Comunidad Europea”. También aparecerá el nombre del país para el que se expida y “Pasaporte”. A continuación, se hallará una página con una plastificación específica y otra página sin plastificar. En ellas se detallará los datos relativos a la persona, como son el nombre y apellidos, sexo, nacionalidad, lugar y fecha de nacimiento, fecha de expedición y expiración, autoridad y firma del solicitante. En una de estas dos páginas se plasmará una foto del titular. En la siguiente hoja, los países decidirán si añaden datos como el lugar de residencia, la altura, color de ojos o información relativa a la prórroga del documento.

Por otro lado, en lo que refiere al alcance, esta regulación solo se aplicará a los países miembros de la UE.

Unos años después de la unificación del pasaporte en la UE, y con el avance de las nuevas tecnologías, ha sido necesario la creación de nuevos reglamentos que regulen la incorporación de mecanismos de seguridad y la tecnología biométrica empleada en los pasaportes.

Los mecanismos de seguridad mínimos con los que debe contar el pasaporte se establecen por Resolución en la reunión que tuvo lugar en el seno del Consejo, el día 17 de octubre del 2000. Durante dicha reunión se destacó la importancia de desarrollar las medidas de seguridad en base a la nueva tecnología biométrica. Esto queda recogido en el Reglamento (CE) n.º 2252/2004 del Consejo, de 13 de diciembre de 2004⁸ y posteriormente en el Reglamento (CE) n.º 444/2009 del Parlamento Europeo y del Consejo, de 6 de mayo de 2009 donde se incorporan algunas matizaciones al reglamento anterior.

De acuerdo con los Reglamentos n.º 2252/2004 y n.º 444/2009 y atendiendo a las especificaciones de la Organización de Aviación Civil Internacional (OACI) sobre el uso fraudulento, se establece que tanto los pasaportes como los documentos de viaje deben cumplir

⁸ El Reglamento n.º 2252/2004 estará en vigor una vez transcurran veinte días desde su publicación en el DOUE.

las normas mínimas de seguridad establecidas en el anexo.

En lo que refiere a las medidas de seguridad de los materiales, encontramos que el papel empleado deberá cumplir los siguientes requisitos: “No tendrá blanqueante óptico; llevará marcas de agua bitono; contendrá reactivos de seguridad contra las manipulaciones de borrado químico; contendrá fibrillas coloreadas (visibles y fluorescentes a la luz ultravioleta, o invisibles y fluorescentes, al menos en dos colores); se recomienda que contenga planchetes fluorescentes a la luz ultravioleta (obligatorios para las etiquetas adhesivas); se recomienda que contenga hilos de seguridad”⁹.

Asimismo, se establece que en los casos en los que la página que contiene los datos personales se adhiera una etiqueta de plástico, no tendrá que llevar marca de agua. Se puede prescindir de esta medida de seguridad también en la portada, la guarda de la portada, la contraportada y la guarda de contraportada, y solo deberán tener reactivos de seguridad las páginas que contengan datos del titular. Adicionalmente, se protegerá el hilo de costura, a fin de evitar su suplantación¹⁰.

Si los datos del titular deben introducirse en una tarjeta cuyo soporte es sintético, es imposible aplicarle las mismas medidas de seguridad que al resto de hojas de papel. Este tipo de material contará con medidas de seguridad propias siempre y cuando sean acordes a las técnicas de impresión que se mencionan a continuación.

El pasaporte contará con una página de datos personales de lectura mecánica. La cumplimentación de dichos datos se hará conforme a lo dispuesto en las especificaciones de la parte primera del documento 9303 de la OACI. Los datos, junto con una fotografía del titular, se cumplimentarán en la segunda página del documento, es decir, la primera hoja tras la portada. Esta página será diferente a las demás.

⁹ Anexo del Reglamento CE2252/2004 del Consejo, de 13 de diciembre de 2004 sobre normas para las medidas de seguridad y datos biométricos en los pasaportes europeos. Introducción. Punto 1. Materiales.

¹⁰ Anexo del Reglamento CE2252/2004 del Consejo, de 13 de diciembre de 2004 sobre normas para las medidas de seguridad y datos biométricos en los pasaportes europeos. Punto 2. Página de datos personales.

Las técnicas de impresión que se podrán implementar son:

a) “Fondos impresos”: guilliches bicolores o estructuras equivalentes; impresión en iris, fluorescente cuando sea posible; sobreimpresión fluorescente a la luz ultravioleta; motivos eficaces contra la falsificación, haciendo hincapié en la página de datos personales y pudiendo introducir microimpresiones; utilización obligatoria de tintas reactivas en las páginas de papel del documento y en las etiquetas adhesivas; el uso de tintas reactivas será optativo si el papel del documento está bien protegido de las modificaciones.

b) Menciones fijas: con microimpresión incorporada.

c) Numeración; en cada página interior se imprimirá o perforará el número de identificación del documento, preferiblemente empleando alguna tipología especial y con tinta fluorescente a la luz UV. Asimismo, tanto las tarjetas encartadas y las etiquetas adhesivas, como el resto de las páginas del documento deberán contener el número de identificación del pasaporte (se aconseja que el número se vea por ambas caras de la tarjeta).

Para todo lo mencionado anteriormente, será obligatorio el empleo de impresiones calcográficas con imagen latente, microtextos, tintas ópticamente variables y dispositivos difractantes con imágenes ópticamente variables (DOVID). Para los soportes sintéticos también se aplicará DOVID o equivalente”¹¹.

A fin de proteger los datos personales de posibles copias o falsificaciones, se empleará un OVD (Dispositivo ópticamente variable) o un dispositivo similar a los empleados en los visados, que garantice la seguridad y autenticidad de estos. Contará con estructuras difractivas de efecto variable que cambiarán de color según desplazemos el documento sobre su eje vertical u horizontal. Estas estructuras abarcarán la mayor superficie posible, integrándose de forma que una capa quede superpuesta por otra y se empleará la técnica hot-stamping o estampado en caliente. Del mismo modo, se procurará que las capas sean lo más finas posibles y en el caso de que el papel lo permita, se aplicará un revestimiento de seguridad. En las páginas no plastificadas o etiquetas adhesivas, se integrará el OVD de forma metalizada o parcialmente

¹¹ Anexo del Reglamento CE2252/2004 del Consejo, de 13 de diciembre de 2004 sobre normas para las medidas de seguridad y datos biométricos en los pasaportes europeos. Punto 3. Técnicas de impresión.

desmetalizada (con sobreimpresión calcográfica). Tanto las tarjetas de material sintético que empleen grabado por láser, como el texto que contenga los datos personales se añadirán con un OVD. El OVD que se emplee deberá ser al menos un DOVID metalizado o transparente a registro. Esto mismo se aplicará a la página en la que se introducen los datos personales cuando su soporte sea sintético en el exterior y de papel en el interior.

En lo que refiere a las técnicas de expedición del pasaporte, se podrán emplear: impresión láser; procedimiento termotransfer; impresión por chorro de tinta; procedimiento fotográfico; grabado por láser que penetre efectivamente en las capas de la tarjeta que llevan las medidas de seguridad”¹².

Todos los documentos serán unipersonales. Asimismo, los documentos deberán contar un soporte de almacenamiento suficientemente amplio y resistente a las posibles vulnerabilidades. Se añadirán dos impresiones dactilares. Los datos contarán con todas las medidas de seguridad correspondiente, garantizándose en todo momento la integridad, autenticidad y confidencialidad.

Para una correcta implementación de la regulación europea en los documentos, se podrá realizar las especificaciones técnicas que sean necesarias, siempre y cuando sean relativas a los mecanismos de seguridad y los medios de almacenaje de los datos biométricos y su seguridad. Todo ello se empleará a fin de evitar usos fraudulentos. Asimismo, se podrán realizar especificaciones relativas a la calidad y a la regulación existente sobre la imagen del rostro y estampaciones dactilares. Esta regulación podría ser de carácter privado, lo que implicaría que no se publicaría en ningún boletín o página oficial. En este supuesto, el acceso se verá restringido solo al personal designado por los países miembros de la UE. Cada país establecerá un órgano encargado de imprimir los documentos¹³.

¹² Anexo del Reglamento (CE) n.º 2252/2004 del Consejo, de 13 de diciembre de 2004 sobre normas para las medidas de seguridad y datos biométricos en los pasaportes europeos. Introducción. Punto 5. Técnicas de expedición.

¹³ El nombre del órgano encargado de imprimir los documentos será facilitado a la CE y demás países. Estos decidirán si quieren emplear el mismo órgano de impresión y en el caso de realizar alguna modificación deberán dar cuenta a la CE (Reglamento (CE) n.º 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes europeos art.3.2).

2.2. Fortalezas y debilidades de los documentos de identidad actuales.

Llevar a cabo un examen sobre las fortalezas y debilidades que presentan los documentos de identidad, y muy particularmente el pasaporte como referencia, en el presente trabajo resulta una tarea un tanto ardua dado que como bien conocemos las distintas tipologías de salvoconductos que acreditan la identidad de una persona no están sometidos en una parte muy importante de los supuestos a normas regulatorias comunes que amparen las medidas de seguridad a implementar en ese tipo de documentos. Por lo tanto, esta situación es aprovechada por los grupos criminales que se dedican a la obtención y distribución de ese tipo de documentos para conseguir sus objetivos.

De una forma generalizada podemos señalar que los documentos de identidad actuales, desde un punto de vista de la seguridad de éstos, en cuanto a acreditar fehacientemente la identidad de una persona y estar protegidos frente a los intentos de manipulación o alteración, se encuentran afectados por una serie de fortalezas y debilidades.

Dentro de las **fortalezas** que presentan frente a los intentos de vulnerabilidad o manipulación podemos señalar las siguientes:

- Dificultad de acceso a determinadas materias primas y elementos empleados en su confección.*
- Existencia de base de datos de consulta de datos sobre especímenes y documentos falsificados.*
- Formación y medios disponibles para los ciudadanos y las Fuerzas y Cuerpos de Seguridad para detección de posibles alteraciones.*
- Dificultad de vulnerabilidad o reproducibilidad de determinadas medidas de seguridad.*

Dificultad de acceso a determinadas materias primas y elementos empleados en su confección.

Este punto podría ser considerado en su doble faceta, tanto fortaleza al tiempo que debilidad. Por un lado, con el ánimo de preservar el acceso público a determinados materiales y tecnologías empleadas en la elaboración este tipo de documentos como norma general, una

parte considerable, por no decir la totalidad de materias primas específicas asociadas con la fabricación de documentos de identidad están restringidas, en cuanto a su elaboración y sobre todo a su distribución a determinadas empresas u organismos que se dedican a tales fines.

Así, partiendo del sustrato o soporte empleado mayoritariamente en la confección de esas autorizaciones nos encontramos que tanto lo que se denomina como “papel de seguridad” como los sustratos poliméricos (particularmente el policarbonato), que se vienen utilizando con una mayor frecuencia en la obtención de buena parte de los documentos de identidad como serían las cédulas de identidad o las licencias de conducción no se encuentran accesibles a la ciudadanía.

Dentro del conjunto de materias y tecnologías empleadas en la elaboración de ese tipo de credenciales nos encontramos con las distintas tecnologías de impresión. Sobre este particular conviene señalar que a nivel general, la mayor parte de los equipos que generan los principales sistemas de impresión empleados en el campo de la seguridad documental están en mayor o menor medida al alcance de los falsificadores. Al día de la fecha existen contadas tecnologías que “sobreviven” a su posible reproducción con las mismas características que las propias como sería la calcografía o intaglio, dentro de los sistemas tradicionales de impresión, y el láser de quemado o “laser engraving”, este último englobado en las tecnologías digitales. El primero de ello se ha mantenido invulnerable debido al estricto control que existe en cuanto a la fabricación y distribución de los equipos impresores de esas tecnologías, al margen del alto coste que tendrían para las bandas organizadas disponer de ellos. Por lo que se refiere al laser de quemado, a pesar de su utilización desde la década en los noventa en la personalización de tarjetas, se ha detectado un número insignificante de reproducciones de documentos de identidad que emplearan este sistema de impresión, a pesar de su amplia difusión en otros sectores industriales.

En el mismo sentido conviene referirse a los diferentes tipos de tintas u otro tipo de medidas que como contrastes de seguridad y/o signos de autenticidad quedarían definidas como aquellas que en mayor o menor grado tratan de proteger ese tipo de documentos frente a intentos de manipulación y/o alteración. Al igual que en los casos precedentes comentados respecto al tipo de sustrato o soporte empleado como a las diferentes tecnologías de impresión, lo que

conocemos como “medidas de seguridad” que se introducen en los documentos son accesibles en una buena parte, no ya como productos originales en sí sino también a través de imitaciones de éstas, obteniéndose de su empleo un alto grado de calidad en los productos elaborados con su utilización.

-Existencia de base de datos de consulta de datos sobre especímenes y documentos falsificados.

Una herramienta fundamental para que puedan desempeñar adecuadamente su labor los expertos forenses en documentos es la existencia de bases de datos que contengan información sobre las características técnicas de los distintos documentos de identidad, al menos los más representativos como cédulas de identidad y pasaportes, y que permiten servir de referencia para que tanto esos expertos forenses como las Fuerzas y Cuerpos de Seguridad, así como cualquier ciudadano (en el caso de las bases de datos abiertas) puedan chequear adecuadamente los documentos y las distintas medidas integradas en ellos previo conocimiento de sus principales características. Este tipo de bases de datos abarcan desde las que se sitúan en un ámbito público o abierto como PRADO (Ifado), EDISON, etc., a otras de carácter totalmente privado donde mediante una suscripción se puede tener acceso a la información en las mismas como sería el caso de KEESING DOCUMENT CHECKER.

Igualmente, hoy día están proliferando ciertas aplicaciones descargables desde cualquier teléfono (APLICACIÓN) donde se puede verificar algunas medidas de seguridad como el MRZ o la información obrante en el chip que pueda disponer el documento en sí. El uso de estas aplicaciones permite de una manera sencilla contrastar parte de la información gráfica obrante en un documento y de esta forma poner de manifiesto la posible existencia de alguna manipulación.

-Formación y medios disponibles para los ciudadanos y las Fuerzas y Cuerpos de Seguridad.

A nivel general, las nuevas tecnologías de la información han facilitado considerablemente el acceso a todo tipo de información. Sobre el caso particular que estamos tratando, a través de internet podemos hallar en ocasiones tutoriales que describen como están confeccionados alguno de los documentos de identidad a los que estamos haciendo referencia más allá de esas bases de datos que anteriormente comentamos y que igualmente posibilitan a cualquier ciudadano conocer de primera mano las características técnicas principales del documento que

portamos en nuestra cartera. En el mismo sentido, y con un mayor grado de alcance se encontrarían las Fuerzas y Cuerpos de Seguridad garantes de evitar la proliferación de documentos de identidad falsos o falsificados y que luchan contra aquellas organizaciones que se dedican a producir y traficar con éstos. En nuestro caso, resulta especialmente destacable los esfuerzos que en ese sentido de formación y disposición de herramientas y medios adecuados para combatir contra esa tipología delictiva que se estaría realizando en la parte de la Unión Europea, y dentro de ésta algunos organismos integrados en su estructura como FRONTEX, en el que se encuentra, entre otros el Centro de Excelencia para la lucha contra el fraude documental (CED), oficina esta que apoya a los Estados miembros y aborda las amenazas a la seguridad de la UE relacionadas con el fraude de documentos. La tarea principal del Centro es brindar apoyo en operaciones conjuntas de diferentes países, pero también contribuir y colaborar con una serie de unidades de Frontex en distintas misiones y actuaciones, incluido el análisis de riesgos, la capacitación, así como la investigación y la innovación.

-Dificultad de vulnerabilidad o reproducibilidad determinadas medidas de seguridad.-

Aunque no hay nada que garantice la imposibilidad de imitación o simulación de una determinada medida de seguridad, conforme avanza el tiempo desde que se pone en circulación un determinado documento de identidad nos encontramos que alguna de éstas presentan una mejor “resistencia” frente a los intentos de reproducción de las mismas. Con anterioridad se había comentado de algunos sistemas de impresión como la calcografía o el propio láser de quemado que hasta el momento actual su presencia garantizaría por sí misma la autenticidad de un documento con un alto grado de acierto en nuestra evaluación

Al margen de los sistemas de impresión señalados algunos tipos de tinta se mantienen con cierta fortaleza o resistencia frente a los intentos de imitación o simulación con el transcurso de los años siempre que se conozca como chequear éstas. Nos estamos refiriendo a algunas como las T.I.R/no T.I.R y más recientemente otras como las Spark, presentes, entre otros, en el papel moneda euro de la serie Europa.

Dentro del amplio espectro de contrates de seguridad y signos de autenticidad otras que han demostrado fehacientemente el escaso éxito alcanzado en su alteración o simulación sería la propia zona de lectura mecánica (MRZ), compuesta por un conjunto alfanumérico de caracteres

OCR y los diferentes tipos de chips asociados a determinados documentos, cuya información almacenada permite un adecuado contraste con la visible sobre el propio documento en sí en página biográfica.

En el lado contrario, nos encontraríamos con un grupo de factores que debilitarían esa presunta integridad de la que deben gozar los documentos de seguridad, y particularmente los de identidad. Dentro de éstas podemos enumerar, entre otras, las siguientes:

-Documentos robados en blanco.

-Breeder documents.

-El acceso a materias primas y material empleado en la confección de dichos documentos.

-La inexistencia de formatos de documentos de identidad universales.

-La falta de colaboración y/o inexistencia de bases de datos de documentos interconectadas entre las Fuerzas y Cuerpos de Seguridad.

-El fácil acceso a documentos falsos o falsificados a través de las redes sociales.

-Documentos robados en blanco. Una de las principales preocupaciones de las Fuerzas y Cuerpos de seguridad cuando tienen que hacer frente a la lucha contra la falsificación de documentos sería el supuesto indicado, es decir, aquellas situaciones en las que se produce lo que se denomina “documentos robados en blanco”, o lo que es lo mismo sustratos o soportes auténticos de los diversos tipos de documentos de identidad existentes que han sido sustraídos de los centros oficiales donde se custodian y son posteriormente empleadas previa personalización de éstos. Aunque en la mayoría de los supuestos existe un control ciertamente exhaustivo sobre este tipo de soportes dada la peligrosidad que entraña su disponibilidad por bandas organizadas, existen otras ocasiones en la que esos soportes pueden estar al alcance de esas bandas actuando quienes actúan de forma directa para su obtención o mediante el soborno de los funcionarios que los custodian



Figura 9. Imagen de documentos en blanco remitidos por una agencia de mensajería.

La peligrosidad que conlleva la falta de control de ese tipo de documentos discurriendo por los circuitos ilegales viene determinado porque si esas organizaciones se preocupan por conocer los sistemas de impresión y restantes medidas de seguridad que portan esos y obtienen productos similares para su reproducción podrán obtener falsificaciones de muy alta calidad y por lo tanto, difícilmente detectables tanto por la ciudadanía en general, como por un conjunto importante de las Fuerzas y Cuerpos de Seguridad dado que el soporte o sustrato en sí, junto con las medidas de seguridad que llevan incorporadas durante su fase de fabricación proporcionarán una garantía elevada de sortear numerosos controles.

-Breeder documents. Se definen con tal concepto aquel conjunto de documentos como sería un certificado de nacimiento o ciudadanía, libro de familia, factura de servicios públicos, etc. requeridos por un Estado para emitir un pasaporte o cualquier otro documento de identidad.



Figura 10. Ejemplos de distintos formatos de “breeder documents”.

Como bien se ha descrito en su definición se trata de una serie de documentos auxiliares cuya aportación resulta necesaria para la expedición de ciertos documentos de identidad. Ante las graves dificultades que en buena parte de las ocasiones las bandas organizadas encuentran para reproducir o falsificar ese tipo de credenciales, se recurre a medios alternativos para conseguir éstos, en este caso documentos de identidad auténticos obtenidos bajo el amparo de esas justificaciones documentales como certificados de nacimiento, matrimonio, etc. Sobre los que existe mayor dificultad para su control por parte de las Fuerzas y Cuerpos de Seguridad, especialmente, por:

-La ausencia de formatos estándar en la confección de ese tipo de documentos, lo que unido a la carencia o escasez de medidas de seguridad implementadas en torno a éstos los hacen fácilmente vulnerables en cuanto a su reproducción total o parcial.

-La escasez o dificultad de medios disponibles para compartir inteligencia sobre ese tipo de documentos, tanto en la forma de confeccionar éstos como en la difusión de alertas sobre aquellas falsificaciones más detectadas a nivel mundial, a lo que habría que añadir la voluntariedad y predisposición tanto de las autoridades gubernativas como policiales de muchos países para intercambiar información sobre este asunto.

Todo lo indicado, convierte a este tipo de documentos en un elemento muy vulnerable como vía o medio para obtener un documento de identidad auténtico.

Otros. Aquí podríamos hacer mención entre otros a la existencia, a fecha de hoy, de determinados documentos de identidad que no han evolucionado acorde a como lo han realizado otro tipo de documentos de identidad de semejante tipología. Bajo este supuesto, a título de ejemplo, podríamos incluir la carta de identidad italiana, un documento que identifica a cualquier ciudadano nativo de ese país, realizado en soporte papel y dotado con un conjunto escaso y fácilmente imitable de medidas de seguridad, lo que le convierten en objetivo prioritario de los falsificadores para su reproducción dado el acceso hoy día a numerosas materias primas y tecnologías que facilitan ésta.

- *El acceso a materias primas y material empleado en la confección de dichos documentos.* Al igual que anteriormente habíamos comentado las dificultades que existen para acceder a determinadas medidas de seguridad o medios que permitan reproducir específicas tecnologías de impresión como sería la calcografía, nos encontramos con la existencia no sólo de un mercado negro sino de uno totalmente “lícito”, donde a priori se pueden adquirir sin moverse uno desde su domicilio con distintos tipos de tintas, papeles u otro tipo de elementos necesarios para conseguir elaborar un documento de identidad con un grado más que aceptable de la mayor parte de las medidas de seguridad que podemos encontrar en uno auténtico de similares características. De esta forma, al igual que suele ocurrir con otro tipo de actividades delictivas, se abre el camino para que aquellas personas que lo deseen puedan acceder a este tipo de

materiales sin sujeción a ningún control y realizar prácticas, con la finalidad que se desee.

-La inexistencia de formatos de documentos de identidad universales. Uno de los problemas que afectan a las Fuerzas y Cuerpos de Seguridad, en conexión con el que se trata acto seguido, viene determinado por el hecho de no emplearse un modelo estandarizado en los diferentes tipos de documentos de identidad que amparan a los ciudadanos de distintos países. Aunque como se indica en el presente trabajo existen algunas normativas internacionales donde se recogen unos estándares mínimos a los que deben sujetarse esos documentos de identidad (nos estamos refiriendo al caso específico del pasaporte), cada país tiene plena libertad para, en el supuesto de aceptar la adopción de estas normas, diseñar su propio documento de identidad e incorporarle aquellas medidas que considere oportunas. Esta situación al final genera la existencia de un amplio abanico de documentos de la misma tipología a los que deben enfrentarse las Fuerzas y Cuerpos de Seguridad para chequear éstos sin que sea posible, cuando hablamos de puntos fronterizos con movimiento masivo de ciudadanos de muchas nacionalidades, conocer las características técnicas específicas de éstos y por lo tanto, con la posibilidad de cometer más errores en la verificación de los mismos.

-La falta de colaboración y/o inexistencia de bases de datos de documentos interconectadas. Se trata de un problema que aunque ha ido mejorando con el transcurso del tiempo queda aún mucho camino por recorrer no solo en la cooperación y colaboración entre países, cuestión clave para luchar adecuadamente contra aquellas organizaciones que se dedican al tráfico de éstos, sino también mediante la utilización de nuevas tecnologías que permitan establecer bases de datos interconectadas entre las Fuerzas y Cuerpos de Seguridad a nivel internacional. Esta situación es aprovechada actualmente, junto con otras comentadas, por los falsificadores para llevar a cabo sus actuaciones con total impunidad.

-El fácil acceso a documentos falsos o falsificados a través de las redes sociales. Al igual que ocurre con otro tipo de actividades delictivas el uso tanto de internet como de las redes sociales ha favorecido el tráfico de documentos falsos o falsificados y con ellos la posibilidad de obtener, por una determinada cantidad de efectivo no muy significativa, un documento de identidad a su nombre. En la propia “deep web” y “dark net” se pueden encontrar sin mucha dificultad ofertantes de este tipo de productos. Asimismo, se ha observado en los últimos años una

tendencia creciente a adquirir éstos mediante las redes sociales, con lo que resulta extremadamente fácil la obtención de un documento de tales características con los peligros que puede conllevar en función del uso que haga de dicho medio.



Figura 11. Imagen de noticia publicada sobre operación policial de incautación de documentos de identidad vendidos a través de las redes.

2.3. Tipología de fraudes.

Como hemos dicho con anterioridad a los documentos de identidad y al pasaporte en particular se le trata de dotar de un conjunto de medidas de seguridad que impidan o al menos dificulten la acción de los falsificadores en su intento de manipular o alterar los mismos.

Las mejoras tecnológicas producidas en los últimos años y el desarrollo de nuevas medidas de seguridad han ido generando unos productos, en este caso, el pasaporte cuyo grado de dificultad para reproducir íntegramente el mismo (documento falso) es elevado por no decir imposible de conseguirlo. Ante esta situación, las organizaciones criminales que se dedican profesionalmente a este tipo de actividades tratan de buscar las vulnerabilidades que en mayor o menor medida puedan presentar esos documentos de identidad con el fin de obtener al menos un “producto” falsificado de cierta calidad que permita sortear los controles fronterizos de las Fuerzas y Cuerpos de Seguridad.

A continuación se exponen las distintas tipologías de fraude documental más habituales que podremos encontrarnos, alguna de las cuales podemos considerar obsoletas o escasamente empleadas en el momento actual:

- Sustitución fotográfica (convencional e integrada).*
- Alteración de datos en página biográfica u otras.*

- Sustitución de página biográfica u otras.*

- Falsificación de sellos.*

- Visas (alteración o falsificación).*

- Documentos robados en blanco.*

- Otras situaciones vinculadas al fraude documental. Los fraudes de identidad.*

Pasamos a exponer brevemente algunas de las características que presentan cada una de las tipologías enumeradas, así como las tendencias o uso actuales y pasados que se hacen de las mismas en función de la casuística a la que se enfrenta un laboratorio forense dedicado al examen forense de documentos.

-Sustitución fotográfica. Fotografía convencional e integrada.

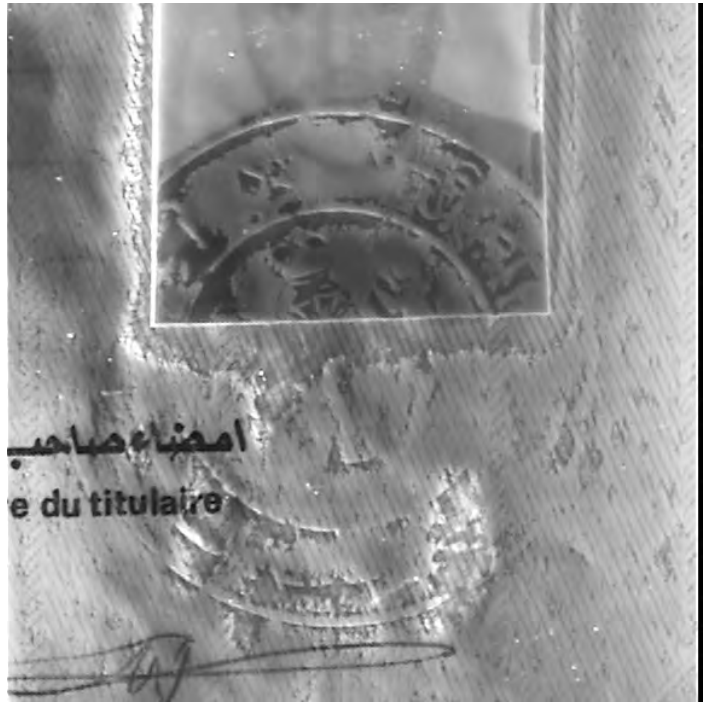
Supone una de las zonas más sensibles de un documento de identidad y por lo tanto objeto preferente de los falsificadores conscientes de realizar el mínimo número de manipulaciones posibles en los documentos auténticos obtenidos por distintas vías. En tal sentido, tratan de mantener inalterable los datos personales que obran en la página biográfica y su actuación se centra en modificar o sustituir la fotografía por la de la persona que va adquirir esa identidad de forma fraudulenta.



Figura 12. Fotografía adherida a la carta de identidad italiana mediante remaches.

Salvo contadas excepciones, como podría ser el caso de la carta de identidad italiana, por referirnos a algún documento que nos resulta más familiar por su cercanía, donde la fotografía aparece integrada sobre el documento en sí y adherida a éste mediante unos remaches, la mayoría de documentos de identidad, es decir, pasaportes, cédulas o incluso permisos de conducir llevan actualmente integradas las fotografías mediante distintos tipos de tecnologías de impresión.

Figura 13. Imagen del área de un pasaporte donde figura adherida la fotografía del titular. Enmarcando en color rojo se señala la presencia de algunos signos que evidenciarían un levantamiento del laminado que protege la misma.



El problema que presenta para los falsificadores actualmente viene determinado por dos circunstancias básicamente:

-En primer lugar, la posibilidad de acceder a las distintas tecnologías de impresión empleadas para imprimir o estampar la fotografía en el soporte correspondiente. En este sentido el mayor grado de dificultad se plantea cuando tratan de reproducir una fotografía realizada en el documento original con láser de quemado. En este caso, al no poder disponer en la mayor parte de las ocasiones con dicha tecnología la sustituyen mediante la estampación a través de una impresora láser (tónor).

Por otro lado, con el ánimo de dificultar y/o impedir dicha alteración los falsificadores

cuentan con otras barreras u obstáculos a los que enfrentarse. Nos referimos a la impresión de una segunda imagen del titular del documento (imagen fantasma o secundaria) ejecutada con otra tecnología de impresión diferente a la fotografía principal; y la existencia de una imagen fotográfica almacenada dentro del chip integrado dentro del pasaporte (una lectura automatizada del contenido de este dispositivo permite poner de relieve si ha habido o no alteración documental en este aspecto al visualizarse la imagen almacenada en el chip, y de esta forma contrastarse con la existente en la página biográfica del pasaporte).



Figura 14. Imagen secundaria realizada con láser de quemado que aparece en la página biográfica de un pasaporte de Holanda.

Uno de los métodos más utilizados para sustituir una imagen fotográfica en los documentos de identidad es lo que se denomina “sobreimpresión”. En algún caso es posible detectar esta falsificación, ampliando los bordes de las fotos y evidenciar la existencia de restos de la tecnología de impresión empleada en el documento original.

El método de sobreimpresión se utiliza para todas las fotos integradas, independientemente del sustrato (papel / polímero). En algún momento no afecta a las características de seguridad. Por tanto, podría resultar muy engañoso su examen.

-Alteración de datos. En página biográfica u otras.

Como hemos comentado con anterioridad, actualmente los falsificadores tratan de manipular los documentos aludidos lo menos posible, conedores que los distintos dispositivos y equipos de lo que disponen las Fuerzas y Cuerpos de Seguridad en los controles fronterizos detectarán mayoritariamente, por no decir la totalidad, de aquellas alteraciones o manipulaciones que se produzcan sobre éstos.

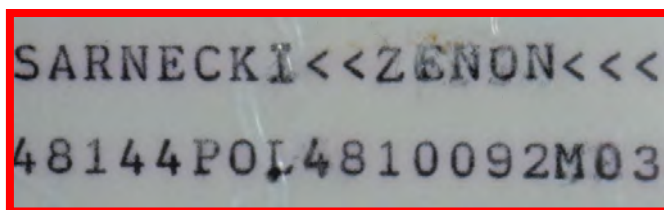
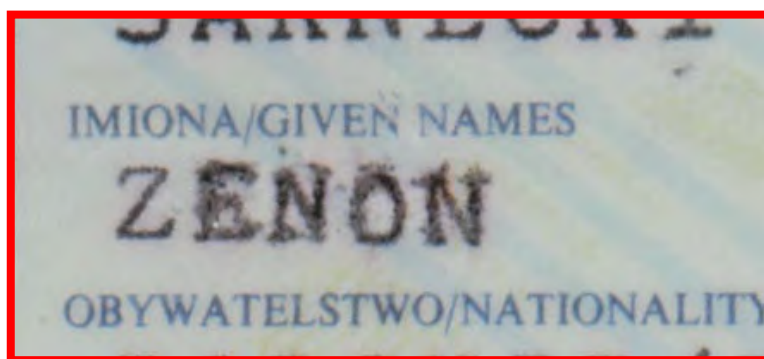


Figura 15. Imagen de detalle de datos manipulados en la página biográfica de un pasaporte y en la zona de lectura mecánica.

En los últimos años son escasas las ocasiones en las que se detectan alteraciones parciales de datos, bien sea de los disponibles en la página biográfica o en cualquier otra parte del pasaporte en sí. Los pocos supuestos podrían encontrarse en las estampaciones de los sellos de entrada y salida por distintos puestos fronterizos, donde se manipulan escasamente las fechas consignadas en los mismos.

-Sustitución de página. Biográfica u otras.

Esta alteración o modificación fraudulenta constituye, junto con la sustitución fotográfica, las principales manipulaciones detectadas en los últimos años sobre los pasaportes, sin contabilizar aquellos supuestos en los que se ha realizado una reproducción íntegra del pasaporte en sí (documento falso, como bien sabemos).



Figura 16. Imagen de detalle del levantamiento fraudulento realizado en la página biográfica de un pasaporte.

A pesar de las dificultades que puede entrañar la eliminación de la página biográfica (suele ser la única hoja del documento analizado sobre la que se realiza esta operación) para no dejar ninguna “huella” o indicio de manipulación, las bandas o grupos organizados dedicados a estas actividades delincuenciales optan por sustituir la totalidad de la página biográfica creando una adaptada al perfil del impostor que va a utilizar dicho documento.



Figura 17. Contraste entre una marca de agua simulada (imagen enmarcada en color rojo) y una multicolor de un pasaporte auténtico (imagen con contorno verde).

Aunque en buena parte de las ocasiones se logra un resultado muy óptimo difícilmente detectable a simple vista, especialmente para aquellas personas o especialistas que no conozcan las características técnicas de un espécimen del mismo tipo al analizado, sí que se evidencia simplemente con el auxilio de medios ópticos de aumento esta suplantación de página, no ya sólo porque en algunos supuestos el papel empleado en la sustitución no es de seguridad, y por lo tanto, presenta ciertas fluorescencias ante su examen bajo iluminación ultravioleta, sino que ante el análisis con esos medios de aumento se pone de manifiesto el uso de otras tecnologías de impresión para los motivos de fondo que las utilizadas en los documentos auténticos (offset), utilizando en la mayor parte de las ocasiones una impresora de inyección de tinta.

En otras ocasiones, conscientes de la dificultad que tienen la mayor parte de los falsificadores de acceder a determinadas tecnologías de impresión a pesar del tiempo ya transcurrido desde su uso en los documentos de seguridad como sería el láser de quemado, se inserta como página biográfica de un pasaporte una realizada con un material distinto al papel, en concreto, uno polimérico (policarbonato). En este tipo de sustrato la cumplimentación tanto de los datos personales como la fotografía del titular del documento suele realizarse mediante láser de quemado. Pues bien, y como constancia que no existe documento de identidad inalterable o imposible de manipular, en los últimos años se están detectando en algunos documentos falsos el empleo de ese tipo de sustrato, inaccesible a priori para el público en general. No solo se han detectado el uso de este tipo de sustratos sino que también se observó el empleo de la tecnología de impresión comentada (láser de quemado) para la personalización. Tan solo la experiencia de los expertos forenses y un examen concienzudo por parte de los mismos consigue poner de relieve las falsificaciones comentadas.

-Falsificación de sellos. Sellos falsificados o falsos.

Al igual que se comentó con anterioridad con la alteración o manipulación de datos, la falsificación o manipulación de sellos (nos referimos a aquellas estampaciones realizadas en los controles fronterizos de aduanas que acreditan la entrada y salida por un determinado punto y la fecha en la que se produjo dicho tránsito) no suele encontrarse en las primeras posiciones en cuanto a la casuística observada en la alteración de pasaportes detectados por las Fuerzas y Cuerpos de Seguridad. En ocasiones, por determinadas circunstancias interesa al usuario del

documento falso o falsificado que consten los sellos de entrada y/o salida por determinados puntos fronterizos y es en estos supuestos cuando se realiza algunas de las manipulaciones necesarias para ello recurriéndose a la creación de sellos “ad hoc”, dado que no existe una uniformidad en este tipo de estampaciones a nivel mundial, o bien realizan la impresión mecánica de la estampación de uno cuya imagen ha sido previamente escaneada.



Figura 18. Estampaciones de sellos húmedos en el interior de las páginas de un pasaporte. La izquierda corresponde a una estampación con datos manipulados y la derecha a una reproducción mecánica de un sello auténtico.

-Visas. Alteración o utilización de visas falsas.

Esta autorización, a través de la cual se permite al ciudadano de un determinado país acceder a otro en unas determinadas condiciones, hace que sea una parte muy “sensible” de los pasaportes, y por lo tanto donde se debe prestar mayor atención a los intentos de manipulación o alteración de la misma. Con el transcurso del tiempo estas autorizaciones han ido mejorando notablemente las características técnicas tanto del diseño como la implementación de distintas medidas de seguridad con el fin de dificultar esos intentos de alteración, no obstante esto no ha desmotivado a los falsificadores a la hora de reproducir las mismas, si bien de un examen detallado de la misma con los equipos y herramientas adecuadas se permite desvelar la existencia o no de manipulaciones o reproducciones íntegras de dichas estampaciones (normalmente se encuentran adheridas a una de las páginas del pasaporte por el adhesivo disponible en su reverso).



Figura 19. Numeración manipulada de una visa.

-Documentos robados en blanco.

Constituyen un serio peligro para las Fuerzas y Cuerpos de Seguridad dado que estamos hablando de documentos auténticos que presentan las características técnicas, en su fase de elaboración y preimpresión, de cualquier otro documento genuino. Esta modalidad defraudatoria no suele producirse con mucha frecuencia, cuando nos referimos a un documento de identidad (pasaporte, cédulas de identidad o permiso de conducir) ya que suele existir, al menos en el ámbito europeo, un control muy estricto sobre la fabricación y distribución de este tipo de soportes. En este supuesto, el riesgo añadido viene determinado cuando la cumplimentación de los datos del futuro titular del documento (personalización) se realizan empleando la misma tecnología de impresión que la de uno auténtico.



Figura 20. Imagen de documentos robados en blanco intervenidos en una operación policial.

-Documentos de camuflaje.

Afirma provenir de países u organizaciones que ya no existen o tienen un nuevo nombre, p. Ej. Samoa Oriental, Nuevas Hébridas (ahora Vanuatu), Rhodesia (ahora Zimbabwe), Honduras Británica (ahora Belice) o Alto Volta (ahora Burkina Faso).



Figura 21. Imágenes de documentos de camuflaje.

-Documentos de fantasía.

Llevar los nombres de estados imaginarios o de una organización. El emisor no es un estado reconocido por el derecho internacional ni una institución autorizada; p.ej. Pasaporte de Hutt River, pasaporte de Texas, Republik Maluku SELATAN Surat Pas, pasaporte de la Autoridad de Servicio Mundial, etc.



Figura 22. Imágenes de documentos de fantasía.

Pseudocumentos.

Comprende una variedad de documentos que no tienen base legal; normalmente no se basan en ningún documento legítimo.



Figura 22. Imagen de pseudocumento.

Un pseudo- documento tiene la apariencia de un documento oficial, pero no es emitido por una autoridad o institución estatal existente legalmente reconocida o por una organización reconocida bajo el derecho internacional, y como tal no tiene validez legal.

Aunque podríamos considerar fuera de lo que serían las tipologías de los fraudes documentales que podremos encontrar hoy día, debemos tener presente que en ocasiones se sustituye la manipulación o alteración de un documento de identidad como sería un pasaporte por lo que conocemos como “fraude de identidad” y que básicamente podemos considerar que se tratan de impostores que se hacen pasar por otras personas suplantando su identidad bajo el amparo de documentos obtenidos fraudulentamente, como ahora veremos, o bien adaptado sus rasgos físicos, en la medida de lo posible, a los que obran en la página biográfica del pasaporte o documento de identidad del que estemos hablando.

Como se ha comentado dentro de esta modalidad nos encontramos con los documentos de identidad obtenidos fraudulentamente. Aquí no solo tiene cabida la posibilidad de obtener los documentos mediante engaño o soborno con aquellos empleados o funcionarios encargados de su expedición sino también lo que se conocen en el argot internacional como “breeder documents”, y que en definitiva se tratarían de un conjunto de documentos de muy diversa tipología y formato que son requeridos para su presentación y obtención del documento de identidad correspondiente.

3. PROTECCIÓN JURÍDICA DE LOS PASAPORTES Y OTROS DOCUMENTOS DE IDENTIDAD.

Si queremos abordar cual es la protección legal que existe para los documentos de identidad sobre los que versa el presente trabajo deberíamos de considerar en primer lugar que engloba el concepto “documento” dentro de nuestro sistema legislativo penal, y en concreto, en nuestro Código Penal. Sobre este particular, nos encontramos que a tenor de lo que se establece en el artículo 26 del mismo se extrae la definición del término “documento”, a partir del cual podremos saber que se tratan de archivos que pueden ser objeto de un delito de falsedad documental.

Según lo indicado en ese punto, se define como documento “todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica”.

Una vez dicho lo anterior, y enlazada con su definición habría que plantearse cuales son los documentos que tras ser alterados pueden encajar en un delito de falsedad documental. En este sentido, entrarían dentro de esa tipología delictiva los siguientes:

- Los **documentos públicos**, especificados en el artículo 1216 del Código Civil: *"Son documentos públicos los autorizados por un Notario o empleado público competente, con las solemnidades requeridas por la ley."*
- Los **documentos oficiales**. Son aquellos expedidos y firmados por funcionarios en el ejercicio de sus funciones.
- Los **documentos mercantiles**. Se definen como tal aquellos que encierran cualquier acto o derecho de naturaleza mercantil.
- Los **documentos privados**. Según la doctrina hacen referencia a aquellos que no constituyen un documento oficial, mercantil o público.

Cada uno de los diferentes tipos de documentos enumerados aparecen recogidos dentro del vigente código penal español, aprobado mediante Ley Orgánica 10/1995, de 23 de noviembre¹⁴.

¹⁴ Título XVIII “De las Falsedades”, en su capítulo II sección 1 la denominada literalmente “De la falsificación de

En este se distinguen las siguientes secciones:

- Sección 1ª: de la falsificación de **documentos públicos, oficiales y mercantiles** y de los despachos transmitidos por servicios de telecomunicación.
- En la sección 2ª: de la falsificación de **documentos privados**.
- Sección 3ª: de la falsificación de **certificados**.

Si nos atenemos a la definición que sobre el pasaporte español establecida en el Real Decreto 896/2003, de 11 de julio¹⁵, por el que se regula la expedición del mismo y se determinan sus características y en la propia web del Ministerio del Interior ¹⁶observamos que tiene la consideración por una parte de documento público y oficial por otro hace que cualquier tipo de actuación delictiva en la que esté inmerso este tipo de documentos, así como la protección legal que se brinda al mismo se encuentra recogida específicamente en la Sección 1 del título anterior indicado denominada “De la falsificación de documentos públicos, oficiales y mercantiles y de los despachos transmitidos por servicios de telecomunicación (arts. 390 a 394)”, y más concretamente en su totalidad a excepción del artículo 394 que hace referencia a los servicios de telecomunicaciones, cuyo texto íntegro es el que acto seguido se reproduce.

documentos públicos, oficiales y mercantiles y de los despachos transmitidos por servicios de telecomunicación”.

¹⁵ Art.1 R.D. 896/2003, de 1 de julio dice literalmente“...El pasaporte ordinario español es un documento público, personal, individual e intransferible, expedido por los órganos de la Administración General del Estado que en este Real Decreto se señalan, que acredita, fuera de España, la identidad y nacionalidad de los ciudadanos españoles salvo prueba en contrario, y, dentro del territorio nacional, las mismas circunstancias de aquellos españoles no residentes.....”.

¹⁶ “...El pasaporte ordinario español es un documento público, personal, individual e intransferible, expedido por los órganos de la Administración General del Estado que en este Real Decreto se señalan, que acredita, fuera de España, la identidad y nacionalidad de los ciudadanos españoles salvo prueba en contrario, y, dentro del territorio nacional, las mismas circunstancias de aquellos españoles no residentes.....” y más adelante figura que “...Los documentos oficiales son los públicos, ya que los ejemplos dados para su identificación no se diferencian ni por su contenido, ni por su forma o solemnidades de los públicos. Podrían ser los que cursan entre sí los organismos públicos, o que de ellos parten con destino a los particulares...”

Artículo 390

1. Será castigado con las penas de prisión de tres a seis años, multa de seis a veinticuatro meses e inhabilitación especial por tiempo de dos a seis años, la autoridad o funcionario público que, en el ejercicio de sus funciones, cometa falsedad:

- 1.º Alterando un documento en alguno de sus elementos o requisitos de carácter esencial.
- 2.º Simulando un documento en todo o en parte, de manera que induzca a error sobre su autenticidad.
- 3.º Suponiendo en un acto la intervención de personas que no la han tenido, o atribuyendo a las que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieran hecho.
- 4.º Faltando a la verdad en la narración de los hechos.

2. Será castigado con las mismas penas a las señaladas en el apartado anterior el responsable de cualquier confesión religiosa que incurra en alguna de las conductas descritas en los números anteriores, respecto de actos y documentos que puedan producir efecto en el estado de las personas o en el orden civil.

Artículo 391

La autoridad o funcionario público que por imprudencia grave incurriere en alguna de las falsedades previstas en el artículo anterior o diere lugar a que otro las cometa, será castigado con la pena de multa de seis a doce meses y suspensión de empleo o cargo público por tiempo de seis meses a un año.

Artículo 392

1. El particular que cometiere en documento público, oficial o mercantil, alguna de las falsedades descritas en los tres primeros números del apartado 1 del artículo 390, será castigado con las penas de prisión de seis meses a tres años y multa de seis a doce meses.

2. Las mismas penas se impondrán al que, sin haber intervenido en la falsificación, traficare de cualquier modo con un documento de identidad falso. Se impondrá la pena de prisión de seis meses a un año y multa de tres a seis meses al que hiciere uso, a sabiendas, de un documento de identidad falso.

Esta disposición es aplicable aun cuando el documento de identidad falso aparezca como perteneciente a otro Estado de la Unión Europea o a un tercer Estado o haya sido falsificado o adquirido en otro Estado de la Unión Europea o en un tercer Estado si es utilizado o se trafica con él en España.

Artículo 393

El que, a sabiendas de su falsedad, presentare en juicio o, para perjudicar a otro, hiciere uso de un documento falso de los comprendidos en los artículos precedentes, será castigado con la pena inferior en grado a la señalada a los falsificadores.

Asimismo, y por las razones que se esgrimen en el presente trabajo también debería tomarse en consideración los referentes a los certificados, al considerar, desde nuestro punto de vista que en muchas ocasiones la obtención de pasaporte auténticos se consiguen mediante la obtención y presentación de documentos fraudulentos secundarios requeridos para la expedición de los aludidos pasaportes, y por lo tanto, asociados con la expedición fraudulenta de los mismos. En este caso, existe una Sección específica relativa a certificados que abarca los artículos 397 a 399, ambos inclusive y cuyo texto redacción literal es la siguiente:

Artículo 397

El facultativo que librare certificado falso será castigado con la pena de multa de tres a doce meses.

Artículo 398

La autoridad o funcionario público que librare certificación falsa con escasa trascendencia en el tráfico jurídico será castigado con la pena de suspensión de seis meses a dos años.

Este precepto no será aplicable a los certificados relativos a la Seguridad Social y a la Hacienda Pública.

Artículo 399

1. El particular que falsificare una certificación de las designadas en los artículos anteriores será castigado con la pena de multa de tres a seis meses.
2. La misma pena se impondrá al que hiciere uso, a sabiendas, de la certificación, así como al que, sin haber intervenido en su falsificación, traficare con ella de cualquier modo.

3. Esta disposición es aplicable aun cuando el certificado aparezca como perteneciente a otro Estado de la Unión Europea o a un tercer Estado o haya sido falsificado o adquirido en otro Estado de la Unión Europea o en un tercer Estado si es utilizado en España.

Finalmente, en el Capítulo III se encuentra recogido los artículos 400 y 400 bis., que de forma indirecta hacen referencia a un conjunto de acciones preparatorias o no para la comisión de alguno de los delitos enumerados con anterioridad, y que tienen una especial incidencia a la hora de poder condenar posteriormente a personas u organizaciones delictivas dedicadas a estas actividades. El contenido literal de dicho artículo es el siguiente:

Artículo 400

La fabricación, recepción, obtención o tenencia de útiles, materiales, instrumentos, sustancias, datos y programas informáticos, aparatos, elementos de seguridad, u otros medios específicamente destinados a la comisión de los delitos descritos en los Capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 400 bis

En los supuestos descritos en los artículos 392, 393, 394, 396 y 399 de este Código también se entenderá por uso de documento, despacho, certificación o documento de identidad falsos el uso de los correspondientes documentos, despachos, certificaciones o documentos de identidad auténticos realizado por quien no esté legitimado para ello.

La nueva y actual regulación obedece a la necesidad de atender a la problemática derivada de la extensión y práctica generalizada relativa a la falsificación de documentos de identidad, tanto para los documentos españoles como para conductas realizadas en relación con documentos de identidad pertenecientes a otro Estado de la Unión Europea o de un tercer Estado si el objetivo es utilizarlos en España, tal y como se indicaba en la Exposición de motivos de la LO 5/2010, de 22 de Junio¹⁷.

¹⁷ Literalmente se dice “También se han abordado reformas en ámbitos como el de la falsificación de certificados, a la que se ha de añadir, en todas sus modalidades, la de documentos de identidad que se ha transformado en una práctica intolerablemente extendida. Por razones fácilmente comprensibles, la intervención penal se extiende al tráfico de documentos de identidad falsos, así como a las mismas conductas realizadas en relación con documentos de identidad pertenecientes a otro Estado de la Unión Europea o de un tercer Estado si el objetivo es utilizarlos en España”.

Por razones fácilmente comprensibles, la intervención penal se extiende al tráfico de documentos de identidad falsos, así como a las mismas conductas realizadas en relación con documentos de identidad pertenecientes a otro Estado de la Unión Europea o de un tercer Estado si el objetivo es utilizarlos en España.

La tutela penal se extiende a su vez al tráfico con esos instrumentos falsos y a su uso y tenencia en condiciones que permitan inferir su destino al tráfico, aunque no se haya intervenido en la falsificación, de modo que se mantiene la consideración de que el delito de falsificación no es un delito de propia mano en cuanto que se considera también autor a aquél que no ha realizado materialmente la falsificación pero que ha encargado su confección para su ulterior utilización en beneficio propio, aportando elementos necesarios para que dicha falsificación sea realizada. Es por ello que se busca dar una justa respuesta a conductas similares en las que se ataca del mismo bien jurídico mediante la utilización de documentos auténticos por personas no legitimadas para ello, al no existir una correlación entre el portador del documento y el titular reseñado en el mismo, produciéndose una quiebra de la confianza y seguridad jurídica ínsita a la documentación de identidad expedida por las autoridades oficiales competentes.

La conducta delictiva del art. 400 bis en relación con el art. 392.2 in fine tiene un previo antecedente en el art. 310 párrafo segundo del Texto Refundido del Código Penal de 1973, en el cual se castigaba a “los que hicieren uso de un documento verdadero [...] expedido a favor de otra persona”, refiriendo tales documentos a documentos de identidad o cédulas de carácter personal (art. 308 del mismo texto legal). La incorporación al Código Penal vigente obedece sin duda a la generalizada utilización con fines fraudulentos de documentación de identidad como fenómeno asociado a la inmigración, buscando los sujetos activos del delito su exhibición como medio para conseguir otros fines relacionados con la residencia, la sanidad y la contratación laboral, pero también portando tales documentos de identidad ajenos para evitar retenciones policiales relacionadas con los expedientes de expulsión del territorio nacional, extendiéndose su tutela no sólo a los documentos de otros países de la Unión Europea, que facilitarían el tránsito de su portador por cualquiera de ellos, sino también a los de otros países siempre y cuando se utilicen en España.

Ciñéndonos a los artículos que afectan específicamente a las acciones realizadas con los documentos objeto de estudio se centran principalmente en los artículos 390 a 393, ambos inclusivo, quedando excluido el 394 al hablarnos de las actuaciones llevadas a efecto en el despacho de un servicio de telecomunicaciones o similar.

Pasando a realizar un examen más en profundidad del articulado referenciado podemos encontrar los siguientes elementos intervinientes o afectados por éstos.

Sujeto activo.

Observamos que pueden ser:

La autoridad o funcionario: La autoridad o funcionario público que por imprudencia grave incurriere en alguna de las falsedades previstas en el artículo anterior o diere lugar a que otro las cometa, será castigado con la pena de multa de seis a doce meses y suspensión de empleo o cargo público por tiempo de seis meses a un año (art 391).

El particular: Art. 392. 1. El particular que cometiere en documento público, oficial o mercantil, alguna de las falsedades descritas en los tres primeros números del apartado 1 del artículo 390, será castigado con las penas de prisión de seis meses a tres años y multa de seis a doce meses. 2. Las mismas penas se impondrán al que, sin haber intervenido en la falsificación, traficare de cualquier modo con un documento de identidad falso. Se impondrá la pena de prisión de seis meses a un año y multa de tres a seis meses al que hiciere uso, a sabiendas, de un documento de identidad falso. (art. 392).

Bien jurídico protegido.

El bien jurídico protegido a través de la tipificación del delito de falsedad documental es la veracidad de la que gozan determinados objetos en el tráfico jurídico como medios de prueba. En otras palabras, se podría decir que lo que el bien afectado por este hecho ilícito es la confianza en la autenticidad del documento y en la información veraz de su contenido probatorio.

Elementos objetivos.

Se necesitará la presencia de los siguientes elementos para corroborar que se está ante un delito de falsedad documental:

1. Alteración de la verdad (*mutatio veritatis*) a través de algunas de las formas que enumera el artículo 390 del Código Penal.

2. Dicha mutación ha de recaer sobre alguno de los elementos esenciales del documento.
3. Ese cambio en los datos ha de ser lo suficientemente importante como para afectar a las consecuencias jurídicas que provocaría ese documento.

Elemento subjetivo.

Desde el punto de vista subjetivo, los elementos esenciales que han de concurrir para afirmar la presencia de este delito son la conciencia y la voluntad del autor para alterar el documento en cuestión.

Una vez indicado lo anterior sometemos a un breve análisis las conductas en las que pueden incurrir cualquiera de los sujetos anteriormente indicados.

El artículo 390 establece una serie de acciones u omisiones en las que el sujeto activo es la autoridad o funcionario público que, en el ejercicio de sus funciones, cometa una serie de falsedades en concreto:

La *alteración del documento o algún elemento* (apartado 1.1.). La acción puede llevarse a cabo de cualquier manera y recaer sobre elementos esenciales (fecha, lugar, comparecientes, plazos, prestaciones de las partes, firma).

La *simulación total o parcial del documento* (apartado 1.2). Precisa de un acto creativo de la totalidad o de la parte simulada, y como la falsificación de moneda, debe hacerse con un alto grado de similitud, tal como para inducir a error acerca de su autenticidad. Tampoco se exige perjuicio, ni dolo especial, ni producción de determinados efectos jurídicos del documento. No es posible la complicidad porque es un delito de propia mano, aunque puede haber cooperación necesaria si el autor precisa de otro funcionario para acceder al documento al que quiere introducir una parte simulada. Es posible la tentativa si es sorprendido a media tarea de la falsificación, que es de carácter material.

La *suposición de intervención de personas* (apartado 1.3). Este delito es de falsificación ideológica porque la falsedad ni siquiera roza el papel, sino que altera la realidad del contenido mediante dos modos: haciendo comparecer a quien no ha estado presente en el acto de otorgamiento del documento, o atribuyendo a los presentes inexactas manifestaciones, cambiando lo que dijeron o haciéndoles decir lo que callaron.

Falsear la verdad de los hechos (apartado 1.4). Es tanto como atribuir a los intervinientes declaraciones que no han sido verdaderas o modificando las dichas, porque en realidad, los hechos

de un documento no son otra cosa que el resultado de la narración de los intervinientes.

La conducta descrita por el art. 392.2 in fine en relación con el art 400 bis excluye la modalidad imprudente en su comisión, la cual ha de considerarse atípica, ya que la conducta es esencialmente dolosa “a sabiendas”, bastando el uso consciente del documento auténtico ajeno para cubrir las exigencias del elemento subjetivo del tipo de injusto y sin que sea preciso, a diferencia de lo que ocurre con el tipo penal del art. 393 CP que concurra un específico ánimo de perjudicar.

Así lo pone de manifiesto la Sentencia N° 129/2014, de 2 de Abril de 2014 de la Audiencia Provincial de Madrid, Sección 3ª, en que la acusada finalmente condenada presentó un documento de identidad que no era suyo, ni le había sido facilitado por su titular quien, por el contrario, había denunciado su previa sustracción.

La Sentencia de la Sala Segunda del Tribunal Supremo STS 5574/2014, de 30 de Diciembre, se pronunció sobre la posibilidad de apreciar la continuidad delictiva en el tipo penal. En ella se indicaba que la utilización de un documento de identidad belga expedido a nombre de otra persona, haciéndolo en una pluralidad de ocasiones para registrarse en distintos hoteles radicados en diferentes calles de una misma localidad, y en algunos casos incluso en establecimientos situados en distintas provincias, determinaba que se estuviera ante un delito continuado, siendo procedente la aplicación del art. 74 CP¹⁸ excluyendo la posibilidad de acudir a una supuesta unidad natural de acción, ya que los hechos aisladamente considerados serían constitutivos de infracciones penales por sí mismas. Impone la pena privativa de libertad en su extensión máxima de un año justificando dicha pena en atención al carácter reiterado y contumaz de la utilización del pasaporte belga expedido a nombre de otra persona, también por la proximidad temporal con la que los hechos fueron ejecutados y por el hecho de que los actos cometidos se extendieran a establecimientos hoteleros situados en distintas provincias del territorio nacional.

Resulta aplicable, por lo tanto, al delito del art. 400 bis la distinción jurisprudencial asentada

¹⁸ Art.74.1. Código Penal. “...No obstante lo dispuesto en el artículo anterior, el que, en ejecución de un plan preconcebido o aprovechando idéntica ocasión, realice una pluralidad de acciones u omisiones que ofendan a uno o varios sujetos e infrinjan el mismo precepto penal o preceptos de igual o semejante naturaleza, será castigado como autor de un delito o falta continuados”.

sobre los conceptos de unidad de acción en sentido natural, unidad natural de acción, unidad típica de acción y unidad jurídica de acción o delito continuado (STS 487/2014, de 9 de junio , STS 5534/2014, de 29 de Diciembre). Y así, en el caso anteriormente expuesto, es posible apreciar una pluralidad de acciones homogéneas, una repetición de varias realizaciones típicas individuales que acaban siendo abrazadas en una unidad jurídica, como un delito continuado.

4. FUTURO DE LOS DOCUMENTOS DE SEGURIDAD. BIOMETRIA Y BILLETERA DIGITAL.

Como bien sabemos ha ido está produciendo, a nivel general, un fuerte desarrollo tecnológico durante las últimas décadas, si bien el acceso a los nuevos productos y servicios derivados del mismo no alcanza por igual a todas las personas ni a todos los sectores, uno de los cuales sería el de los sistemas de identificación y autenticación de personas, tanto presencial como digital, y la desprotección que se produce en el tráfico y el uso de nuestros datos personales en internet.

El mecanismo de identificación y autenticación presencial más confiable que se utiliza hoy en día en la inmensa mayoría de los lugares donde necesitan saber quiénes somos consiste en solicitarnos un documento oficial de identidad con una fotografía y hacer una comparación visual. En muchas ocasiones el verificador no cuenta con tecnología que le permita comprobar que el documento de identidad no sea falso, y solamente en lugares muy puntuales se lleva a cabo una verificación biométrica para asegurar que efectivamente somos el dueño o el propietario de ese documento de identidad.

En otro orden nos encontramos con la identificación y autenticación digitales. De la información técnica extraída de distintas webs especializadas ¹⁹ podemos observar cómo de forma progresiva, aunque en ocasiones algo lenta, algunos países van ofreciendo a sus ciudadanos una tarjeta o ID electrónico que les permite acceder a servicios electrónicos de manera autenticada. Sin embargo, incluso en los países más avanzados, estos servicios están generalmente limitados a aquellos que ofrecen la administración pública, no pudiendo usarse estos ID electrónicos para acceder a servicios ofrecidos por entidades privadas. Dentro del ámbito de la identificación y

¹⁹ <https://esemanal.mx/2019/07/El-futuro-de-los-documentos-de-identidad-digitales-primero-en-moviles-luego-en-wearables/>

<https://www.wellsfargo.com/es/mobile/payments/digital-wallet-basics/>

<https://nanova.org/que-es-una-billetera-digital>

autenticación digital debemos destacar una realidad cada vez más patente en nuestra actividad diaria, en concreto, lo que se denomina “cartera o billetera digital”.

Una cartera o billetera digital es una manera de llevar la información de su tarjeta de crédito o de débito en una forma digital segura en su dispositivo móvil (smartphone [teléfono inteligente], smartwatch [reloj inteligente], tableta)²⁰. En lugar de usar su tarjeta de plástico física para hacer compras, la billetera digital le permite pagar en tiendas, en apps o por Internet. Las credenciales se pueden pasar a la terminal de un comerciante de forma inalámbrica a través de la comunicación de campo cercano (NFC por sus siglas en inglés). Es importante señalar que normalmente hay dos tipos de sistemas POS de monedero digital en uso hoy en día: sin contacto y magnético.

Los terminales sin contacto le permitirán realizar transacciones a través de NFC, Bluetooth, WI-FI o alguna otra forma de transmisión inalámbrica. La tecnología de comunicaciones de campo cercano, o NFC, es uno de los tipos de tecnología de billetera móvil de más rápido crecimiento en el mercado. En comparación, la mayoría de las demás formas de transacciones con carteras móviles requieren que se sostenga el teléfono en el punto de venta directamente para completar las transacciones.

Cada vez más, las billeteras digitales se están usando no solo para transacciones financieras básicas, sino también para autenticar las credenciales del titular permitiendo disponer de una “copia” digital de determinados documentos de identidad como pasaportes o licencias de conducción²¹. Además, la interfaz del usuario de la identidad digital conecta y protege el intercambio de datos entre los usuarios y los oficiales, ya que cifra toda la información personal y permite la verificación en tiempo real. La comprobación de la identidad se puede llevar a cabo donde sea, incluso en áreas sin señal de red o con señal limitada.

Para disponer de una billetera o cartera digital sólo necesita descargar una aplicación móvil de billetera digital para comenzar a operar, alguna de las cuales se encuentran disponibles en plataformas de descarga de aplicaciones como Google Play o a la Apple Store.

²⁰ <https://www.wellsfargo.com/es/mobile/payments/digital-wallet-basics/>

²¹ <https://esemanal.mx/2019/07/EI-futuro-de-los-documentos-de-identidad-digitales-primero-en-moviles-luego-en-wearables/>

Una billetera digital tiene un componente de software y de información. Los sistemas de pago electrónico seguros y justos son un tema importante. El software proporciona seguridad y encriptación para la información personal y para la transacción real.

La disponibilidad de documentación diversa, tanto financiera (como tarjetas de crédito o débito) como de identidad, no supone un reemplazo del documento real en si, sino un compañero digital que le aporta más valor; puede contener información de uso por tiempo limitado, el impedimento de acceso a los usuarios no autorizados, datos cifrados y todo al alcance de la mano.

Con el transcurso del tiempo el uso de este medio alternativo de medio de pago y de acreditación de identidad se está haciendo más extensivo, si bien para el usuario actual su empleo viene acompañado de una serie de ventajas e inconvenientes.

Dentro de las ventajas²² podemos enumerar:

Seguridad.-En las transacciones comerciales los consumidores tienen la tranquilidad y seguridad que su información está encriptada o protegida por un código de software privado; a su vez, los comerciantes se benefician al recibir una combinación de protección contra el fraude, un recibo de pago más rápido, menores costos de transacción y menores pérdidas por robo. Además, los usuarios pueden recuperar los datos perdidos mediante copias de seguridad. Los monederos digitales incorporan diversos protocolos de seguridad para garantizar que sólo el propietario legítimo tenga acceso a la información que contienen. Dependiendo del proveedor de la billetera, esta seguridad podría incluir contraseñas, tecnología de escaneo de huellas dactilares o faciales, etc.

Comodidad para utilización en múltiples servicios. Desde compras a través del comercio electrónico hasta poder realizar trámites administrativos mediante la acreditación de los datos de su identidad recogidos en diferentes documentos personales como pasaportes, cédulas de identidad o licencias de conducción.

Dentro de las desventajas o inconvenientes²³ señalar:

²² <https://nanova.org/que-es-una-billetera-digital/>

²³ <https://nanova.org/que-es-una-billetera-digital/>

Problemas tecnológicos. Uno de los principales problemas que rodean la adopción de la billetera digital se deriva de las restricciones tecnológicas, no de los protocolos, sino de los dispositivos con los que funcionan. Básicamente, incluso la mejor billetera digital del mundo es inútil si la batería de tu teléfono se agota.

Inseguridad en su uso. Otro obstáculo importante para la adopción de la billetera digital es el hecho de que la mayoría de las personas todavía prefieren usar plástico y dinero en efectivo ya que no consideran que las carteras de los móviles sean seguras.

Lenta difusión de las nuevas tecnologías. La falta de tecnología en materia de identidad tiene grandes consecuencias negativas. En el día a día, son frecuentes la indocumentación de personas, la falsificación de documentos de identidad, la usurpación de identidad o la pérdida de documentos de identidad. En poblaciones vulnerables expuestas a catástrofes naturales o forzadas a la migración, la situación es mucho más crítica, pues se cuentan en millones las personas que cada año no solo se quedan sin hogar sino que no disponen los documentos que les permitirían probar quiénes son, de dónde vienen o qué formación y experiencia profesional tienen.

Adicionalmente, el hecho de que los sistemas de identificación y autenticación electrónica de individuos sean casi inexistentes genera una serie de consecuencias como la limitación de la digitalización de muchos servicios y la generación de monopolios de entidades intermediarias que ofrecen confianza entre las dos partes interactuantes.

En los últimos años se han venido desarrollando un conjunto de estándares, protocolos y tecnologías que buscan ofrecer un nuevo concepto de identidad al alcance de todos, barata, segura y escalable, que pueda solucionar los problemas actuales presentes en la identificación y autenticación de personas dándole además al individuo un control total sobre su persona digital. Este nuevo modelo de identidad se conoce como *identidad digital auto-soberana* e incorpora dos elementos tecnológicos innovadores: las billeteras digitales, ya comentadas, y los registros descentralizados de información.

Conviene señalar, para evitar confusiones que se puedan producir, que en la identidad digital auto-soberana son las administraciones públicas quienes tienen la soberanía última de la identificación de los ciudadanos. Por tanto, lo que la identidad auto-soberana propone es una soberanía para el individuo no en la emisión de la identidad sino en su administración y

presentación a terceros.

En primer lugar, este modelo habilita que los individuos tengan soberanía en la administración y manejo de sus activos y credenciales digitales -como por ejemplo un pasaporte digital, un título académico, un título de propiedad, o divisas como dólares o euros - usando billeteras digitales personales y portables como por ejemplo un aplicativo móvil.

En segundo lugar, elimina la necesidad de que la entidad tercera a la que se le presente un activo digital tenga que acudir directamente al emisor para comprobar su veracidad o validez, pues puede hacerlo contra un registro público y descentralizado.

Se puede definir la identidad digital como un conjunto finito de atributos que permite a una persona, animal, cosa o proceso ser identificado como único y probar su identidad frente a terceros electrónicamente.

Nuestra persona digital se compone de varias identidades digitales, estando a su vez cada una de estas identidades representada por uno o varios identificadores y atributos que son únicos en un contexto específico. La verificación de la identidad digital presenta algunos desafíos como, por ejemplo, el hecho de que ya no sea posible comparar visualmente las características físicas de un individuo con las de un documento oficial de identidad para verificar quién es. Sin embargo, al mismo tiempo ofrece enormes ventajas pues nos permite tener acceso a todo tipo de servicios digitales globales.

A medida que surgen nuevas tecnologías, los reguladores adquieren una mayor comprensión del mundo digital, los gobiernos y las entidades privadas encuentran mejores formas de interactuar electrónicamente, y los usuarios se sienten más seguros con el uso de internet para todo tipo de transacciones. Sin embargo, las soluciones actuales aún presentan diversos problemas que pueden clasificarse en tres categorías: regulación, tecnología, y seguridad

Regulación y estándares. A medida que las sociedades crecen digitalmente, las nuevas formas de conectarse e interactuar entre individuos y organizaciones requieren de una evolución constante de los requisitos de la identidad digital.

En primer lugar, es esencial identificar los diferentes contextos de las interacciones electrónicas para que los estándares y las regulaciones puedan adaptarse y apoyarlos si fuese necesario.

Uno de los problemas a los que se enfrentan hoy en día la identificación, la autenticación y la autorización electrónica es que la regulación sobre transacciones electrónicas, cuando existe, se centra en un uso limitado de la identidad digital para la interacción entre individuos y servicios proporcionados por la administración pública.

Es en Europa donde podemos encontrar la normativa más avanzada para la identificación electrónica y la protección de datos²⁴.

Tecnología. Utilizada hoy en día para la identificación electrónica de las personas dista mucho de ser ideal.

Seguridad. En general las personas no pueden administrar sus identidades digitales, ya que no tienen el control de sus autenticadores, de sus datos o de sus credenciales digitales pues se almacena en las bases de datos de terceros y son estos quienes nos proporcionan acceso a ella. Básicamente, nuestra interacción electrónica está en manos de proveedores de servicios que nos dan acceso a aquellos datos e información que ellos controlan, así como de proveedores de identidad de terceros que administran nuestros autenticadores y los usan en nuestro nombre.



Figura 23. Imagen de aplicaciones descargables

En resumen, la digitalización de los documentos de identidad está alcanzando nuevos niveles impulsado por la desmaterialización de las licencias de conducir y de los documentos de salud

²⁴ Reglamento eIDAS y Reglamento General de Protección de Datos-GDPR.

principalmente, situación ésta que se está ya produciendo en algunos países como Estados Unidos, Australia, México, etc., donde se están realizando distintas pruebas piloto o se encuentran en una fase de implementación.

La licencia de conducir digital es más que una imagen de su documento, es una versión altamente segura de su licencia de conducir o documento de identidad físico almacenado en su teléfono inteligente al estar protegido por capas adicionales de seguridad, como un PIN o la huella dactilar.

La comodidad, la seguridad, la privacidad y la concentración en el usuario son las características que distinguen a la licencia de conducir digital y que la hacen tan atractiva y fácil de usar.

Estas características se pueden expandir y personalizar rápidamente para incluir un grupo de credenciales más amplio y constituir lo que podríamos llamar como la “billetera de la identidad digital del usuario”. Esta cartera de identidad digital, algún día puede crecer e incluir documentos como pasaportes y tarjetas de salud. De tal manera, se permitirá a los usuarios futuros almacenar todos los documentos de identidad digitales en un punto seguro de su teléfono inteligente.

Además, el software permite compartir solo la información relevante para determinada transacción específica, lo que protege su información personal.

A medida que los desarrollos tecnológicos avancen, los usos posibles de los documentos digitales son ilimitados. Las carteras de identidad digital y su verificación en las transacciones comerciales son solo algunas de las áreas potenciales en las que se puede implementar. En este sentido conviene destacar los esfuerzos realizados dentro del ámbito europeo donde sus ciudadanos podrán en los próximos años tener acceso a un “monedero digital”, es decir, una plataforma creada por la Unión Europea desde donde podremos identificarnos, registrarnos, alquilar un coche o pagar impuestos desde el móvil. Ya se conocen los planes de esta nueva 'Identidad Digital Europea', un ambicioso proyecto para evitar tener que pasar por el registro de las grandes compañías tecnológicas y de paso unificar los accesos electrónicos a nivel europeo bajo una misma gran plataforma.

Esta 'Identidad Digital' será reconocida por todos los países europeos, servirá para identificarnos desde el móvil y las grandes compañías tecnológicas estarán obligadas a aceptar su uso, según explica la Comisión Europea. También está pensada para los trámites administrativos como por ejemplo, al presentar la declaración de la renta o al matricularse en una universidad europea donde se exija identificación oficial”.

La 'Identidad Digital Europea' estará disponible para todos los ciudadanos y empresas y prometen que se garantizará el control por el usuario de sus datos, pudiendo elegir qué aspectos de la identidad se comparten con terceros. En la práctica, lo que ahora ofrecen empresas como Google o Amazon, en los próximos años también se podrá hacer a través de esta plataforma europea.

Mientras que se produce todo el desarrollo tecnológico indicado y se implementa a nivel mundial, al tiempo que se resuelve la problemática anteriormente comentada, el futuro de los documentos de identidad en al menos la próxima década se centra en mejorar la seguridad de dichos documentos para dificultar en mayor medida los intentos de manipulación o alteración, conscientes de la importancia y riesgos que conlleva la detección de aquellos supuestos en los que se produce una suplantación de la identidad, especialmente en situaciones relacionadas con la actuación de los integrantes de bandas organizadas y organizaciones terroristas.

Ciertamente no es muy previsible determinar cuál será el futuro de los documentos de seguridad. En los últimos años estamos asistiendo a un cambio cualitativo muy importante en todo aquello relacionado con los aspectos biométricos de la persona, su desarrollo tecnológico en diferentes herramientas y su implementación en distintos usos y actividades de la vida cotidiana de los ciudadanos.

Hasta que llegue ese momento en el que posiblemente tal vez no sea necesario portar ningún tipo de documento que nos permita acreditar nuestra identidad gracias a la existencia de esos dispositivos que almacenen información biométrica del conjunto población amparados o respaldados con base de datos gubernamentales interconectadas con éstos, debemos conformarnos con presenciar como alguna de estas tecnologías están implementadas en ciertas empresas para permitir el control de accesos a través del reconocimiento por huellas dactilares, el iris o por medición de determinadas facciones de la cara de una persona, medios estos que igualmente observamos de forma cada vez más generalizadas en otros recintos de acceso más

masivos como los controles de accesos a los recintos aeroportuarios.

No obstante, hasta que dicha situación llegue a generalizarse en todos los países y sitios por más remotos que éstos sean queda mucho camino por recorrer y todavía deberá de transcurrir alguna que otra década para ver implementado tales medios de forma globalizadas. Mientras tanto, desde la información adquirida por los laboratorios forenses de Documentoscopia a través de su permanente contacto con las empresas cuya actividad se desarrolla en torno a los documentos de seguridad, se observa como asistimos a un continuo desarrollo tecnológico dentro de las distintas partes que configuran un documento de seguridad, y particularmente, uno de identidad como sería el soporte o sustrato y las medidas de seguridad adheridas o incorporadas al mismo.

Sobre el primer aspecto, es decir, el soporte, hemos podido comprobar como en los últimos años se ha ido produciendo una proliferación de documentos en soporte polimérico que hay ido sustituyendo a los tradicionales confeccionados en papel. Toda la variabilidad de materiales empleados para su confección viene en definitiva a tratarse de un sustrato obtenido artificialmente a partir de la reacción química de componentes derivados del petróleo. Su nombre viene determinado porque a partir de una molécula de pequeña masa molecular que unida a otros monómeros de manera covalente forman macromoléculas llamadas polímeros. De los 109 átomos existentes, los que se agrupan para la obtención de polímeros son el hidrógeno (H), el carbono (C), el oxígeno (O), el cloro (Cl) y el nitrógeno (N).

A pesar del conjunto amplio de materiales que conforman los polímeros, solamente algunos de estos son lo que vienen tradicionalmente empleándose en la industria de los documentos de seguridad, en concreto, el cloruro de polivinilo o PVC, el polipropileno, el poliéster, el ABS y el policarbonato. A continuación presentamos algunas de las características que poseen estos materiales en su utilización para la producción de parte o totalidad del sustrato o soporte de un documento de seguridad.

Polivinilo o PVC

- 85% de las tarjetas comerciales.
 - Tarjetas bancarias.
- + Bajo coste.
- + Fácilmente imprimible.
- + Admite sublimación de tinta.
- + Admite grabado láser.
- + Admite chip proximidad y contacto.
- Baja resistencia a flexión, calor y UV.
- Mediana resistencia al delaminado.
- Deformación: 65-70°



Figura 24. Tarjeta bancaria realizada en PVC.

Polipropileno

- + Muy resistente mecánicamente:
 - Billetes de banco.
 - Ensamblaje página biográfica.
- No admite grabado láser.
- Deformación: 65-70°.



Figura 25. Pestaña de sujeción de hojas de pasaporte realizada en polipropileno.

Poliéster.

- + Resistente mecánicamente/abrazión.
- + Fácil de producir.
- + Muy útil como laminado.
- No admite grabado láser sin PVC.
- Deformación 65-70°.



Figura 26. Plastificado del Documento Nacional de Identidad de España realizada en poliéster.

ABS

Acrilonitrilo-Butadieno-Estireno

- + Versatilidad: inyección molde.
 - Tarjetas SIM.
 - Tarjetas pago teléfono con chip.
- + Buena resistencia térmica.
 - Tacógrafos.
- Poca durabilidad.
- Muy caro.
- Deformación 85-90°.



Figura 27. Tarjetas telefónicas fabricadas en ABS.

Policarbonato

- + Resistencia mecánica y térmica.
- + Permite grabado láser.
 - Documentos de seguridad.
- Difícil de procesar y alto coste.
- Baja resistencia rotura.
- Sensible éter/acetona.
- Deformación 150°.

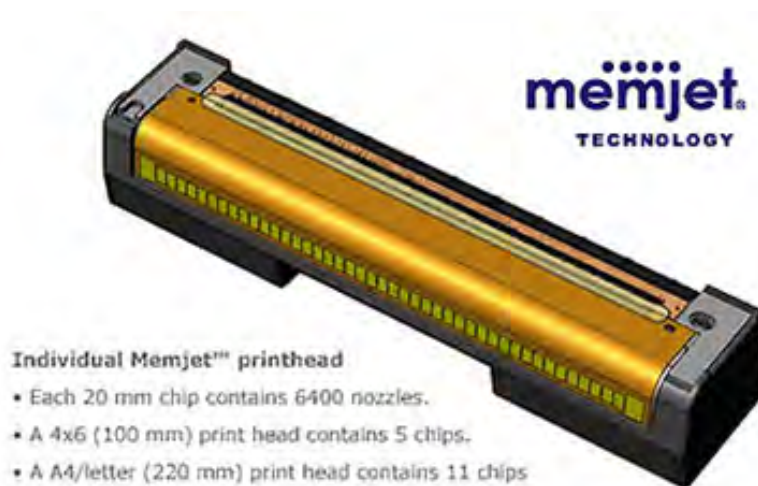


Figura 28. Sustrato del Documento Nacional de Identidad de España 2.0 realizado en policarbonato.

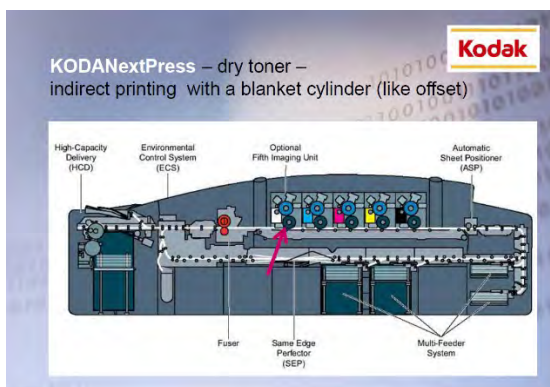
Para la obtención final de los sustratos antes mencionados cabe señalarse que en su origen éstos están conformados por un conjunto de láminas de distintos tamaños y ligeras variaciones en su composición que mediante técnicas de fusión, aplicando presión y calor durante un determinado tiempo convenido, se logra el enlace molecular entre polímeros del mismo origen. La temperatura es controlada para que el polímero alcance su fase elástica (rubber state) -y sin llegar a estado líquido-, para favorecer su enlace. Durante una de las fases que integran ese proceso de fabricación de este tipo de sustratos (preimpresión e impresión, ensamblado, laminado, troquelado y personalización), en concreto, durante su laminado se aprovecha para introducir relieves táctiles o estructuras lenticulares que interactuarán con el grabado láser en la fase de personalización.

Al margen de lo comentado sobre este tipo de soporte que constituye el presente y futuro en los próximos años en lo que se refiere al sustrato tipo a emplear en los documentos de seguridad, también coexisten investigaciones en las que se trata de desarrollar materiales híbridos entre el papel y el sustrato polimérico que confieran a ese material finalmente obtenido las cualidades más propicias para poder ser empleadas por las empresas que se dedican a la fabricación de este tipo de productos, así encontramos ya comercializados desde hace años materiales como el Neobond, Teslín, etc.

Adentrándonos en el campo de las medidas de seguridad que se implementan en los documentos objeto de estudio, y centrando la atención sobre los sistemas de impresión hemos de señalar que dentro de este terreno los avances que se pueden producir en los próximos años están más enfocados hacia aquellos que se engloban como sistemas digitales, y particularmente, las tecnologías láser (tanto lo que conocemos como impresoras láser-aquellas que emplean como fungible impresor el tóner- así como lo que se denomina como laser engraving o laser de quemado) y las de inyección de tinta. Dentro de estas últimas los avances experimentados van en el camino de lograr, como no podría ser de otra forma, hacia una mayor calidad de impresión y menor tiempo, asociados a un menor coste. En este sentido, nos encontramos como un ejemplo de lo indicado con las impresoras MEMJET. En este caso las investigaciones discurren por el nuevo desarrollo de cabezas impresoras en línea y panorámica. Se trata de impresoras con un cabezal fijo que cubre toda la superficie del papel. En estos dispositivos es el papel el único que avanza bajo el flujo de tinta. Del formato en línea (donde el papel avanza en vertical) tenemos las máquinas Lomond Evojet Office y la Brother HLS7000DN; del formato panorámico (donde el papel avanza apaisado).



Por igual término discurre la evolución de las impresoras láser, es decir, por la mejora en la calidad de imagen. Sobre este particular, y dadas las mejoras experimentadas por algunas de éstas, con una calidad que se aproxima en buena medida a las impresiones realizadas mediante un sistema planográfico como el offset, englobadas dentro de lo que se denomina como “offset digital”, aunque como bien sabemos su funcionamiento se fundamenta en un proceso electrostático como sería el caso de la HP INDIGO, Nexpress, Xeikon, etc.



HP Indigo



Figura 30. Ejemplos de impresora de offset digital (kodak nexpress y HP Indigo).

Respecto a lo que sería propiamente calificado como medida de seguridad una parte importante de los avances que deben de producirse en los próximos años será en todo el campo de las tintas de seguridad dada la eficacia y solvencia que han demostrado la mayor parte de ellas para salvaguardar o dificultar los intentos de manipulación de los documentos de identidad, principalmente aquellas áreas o zonas del mismo que presentaba los datos del titular. En este terreno discurre los avances realizados por la empresa SICPA, como líder mundial en la producción de este tipo de productos, con la incorporación en los últimos años de algunas variedades como las tintas bifluorescentes ²⁵ o las spark ²⁶.

²⁵ Tintas bifluorescentes. Emiten colores diferentes cuando se excitan en longitudes de onda diferentes.

²⁶ Tintas Spark. Capaces de visualizar dos colores simultáneamente con el reflejo de la luz incidente sobre la parte del documento donde se asienten.

Under UV light

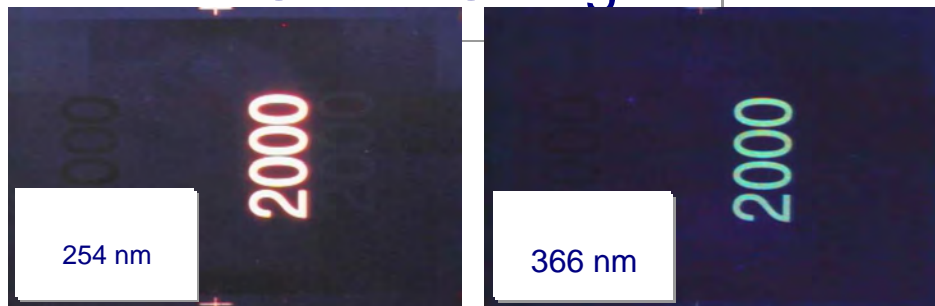


Figura 31. Tintas bitonales empleadas en papel moneda.



Figura 32. Tintas spark incorporadas en los billetes de la serie Europa del euro.

Por último, y al igual que lo expuesto con anterioridad, nos encontramos con una serie de dispositivos que si bien se han incorporado recientemente o al menos en los últimos años, la tendencia es que continúe su evolución y desarrollo implementando nuevas versiones o mejoras sobre los mismos. En este sentido, cobra especial fuerza todo lo referente al desarrollo de medidas asociadas o vinculadas con aspectos biométricos de la persona.

Antes de entrar a exponer alguno de esos dispositivos o medidas a las que nos hemos referido convendría aclarar a qué hacemos referencia cuando hablamos sobre biometría o rasgos biométricos. Pues bien, a nivel general, el término biometría se define como una tecnología de identificación basada en el reconocimiento de una característica física e intransferible de las personas o un proceso en los sistemas de identificación biométrica.

-Como característica:

- Una característica biológica (anatómica y fisiológica) y de comportamiento medible que se puede utilizar para el reconocimiento automático.

-Como proceso:

- Métodos automatizados de reconocimiento de un individuo basados en características biológicas (anatómicas y fisiológicas) y conductuales mensurables.

Dentro de los sistemas de identificación biométricos nos encontramos aquellos que se fundamentan en características físicas como el reconocimiento facial, las huellas dactilares, el iris, la retina, el ADN, etc. Y otros que se articulan en torno a características de comportamiento personales como la firma, la voz, los patrones de movimientos, etc.

El uso de estos sistemas de identificación biométricos como elementos auxiliares o complementarios implementados en los documentos de seguridad van asociados a una normativa existente tanto a nivel europeo, en el caso de nuestro país, como a otra de carácter mundial desarrollada por la Organización de Aviación Civil Internacional (OACI). En concreto, en esta última se establece según resolución N001, adoptada el 28 de junio de 2002 en Berlín que respalda el uso del reconocimiento facial como el biométrico interoperable globalmente para máquinas asistidas para confirmar la identidad de personas a través de equipos verificadores de documentos que lleven a cabo la lectura de las zonas mecánicas del documento. Así mismo da libertad a los países para que puedan elegir cómo elemento biométrico adicional para esos fines de confirmación a tecnologías biométricas basadas en el iris o las huellas dactilares.

Para emplear dichas tecnologías biométricas deben disponerse de unos dispositivos de almacenamiento de esta información. Como norma general en la norma ICAO (OACI) 9303 se establece que sea en un microchip de proximidad (comunicaciones a menos de 10 cm del lector), también llamado microchip RFID sin contacto, es el medio de almacenamiento de identificadores biométricos. El microchip tiene una antena que permite la comunicación con los lectores. Normalmente, el microchip no es visible como está incorporado en la página de biodatos (policarbonato), en la contraportada o en las páginas centrales de un pasaporte. Para

garantizar la invulnerabilidad de estos dispositivos por la información sensible que contienen se utilizan distintos tipos de métodos de autenticación o protección que constituyen al fin y al cabo sistemas de encriptación de esa información. Los métodos de autenticación implican el intercambio y validación de certificados y ello hace factible que puedan ser leídos en cualquier país de mundo, facilitando la interoperabilidad. Un lector sin la firma digital del país puede abrir el microchip pero no garantiza la autenticidad de los datos.

Por lo tanto, siendo este el medio elegido por los distintos organismos internacionales que establecen normas de seguridad para los documentos de viaje, y dado el potencial que ofrecen hasta el momento actual ese tipo de dispositivos se prevé que en los próximos años se producirá un mayor desarrollo en dichos dispositivos.



Figura 33. Chip de proximidad incorporado en un pasaporte. Detalle del circuito.

Sin embargo, también queremos exponer brevemente la existencia de otras serie de dispositivos que, aunque no fueron elegidos o seleccionados por la OACI, al no estar garantizada su interoperabilidad entre países, sí que proporcionan igualmente seguridad y son empleados como medios auxiliares o complementarios para contrastar la información obrante en la página biográfica de un pasaporte o en la zona donde figuren los datos del titular cuando hablamos de otro tipo de documentos de identidad como cédulas o permisos de conducir. Estos dispositivos constituyen el presente y futuro de almacenamiento de información disponible en los documentos de seguridad y sobre los cuales se producirá un importante desarrollo y mejora.



Figura 34. Pasaporte electrónico de Portugal y lectura del mismo en un verificador de documentos.

Banda magnética

Una banda magnética es un dispositivo de almacenamiento formado por pequeñas partículas magnéticas. Las partículas magnéticas se aplican directamente a la tarjeta o se convierten en una franja que se aplica al documento. Los datos de una banda magnética se codifican con una cantidad específica de energía magnética. Tiene un bajo nivel de seguridad y, según el tipo, se puede desmagnetizar fácilmente (borrado de datos).



Figura 35. Tarjetas bancarias y lector de banda magnética de éstas.

Códigos de barras

Un código de barras es una representación óptica de datos legible por máquina. Originalmente, los códigos de barras representaban datos en los anchos (líneas) y el espaciado de líneas paralelas, y pueden denominarse códigos de barras lineales o 1D (unidimensionales).

También vienen en otros patrones como: cuadrados, puntos, hexágonos y otros patrones geométricos dentro de las imágenes, denominados 2D (bidimensionales) o códigos de barras de respuesta rápida (Qrcode).



Figura 36. Distintos tipos de códigos (1D, 2D y QR).

Banda de memoria óptica

Los datos se almacenan y recuperan de forma similar a un CD. Puede almacenar hasta 4 Mb de información y los datos no se pueden modificar (Write Once Read Many - WORM).



Figura 37. Imagen general y de detalle de un documento de identidad con banda de memoria óptica.

Chip de contacto

Un chip de contacto es un circuito integrado miniaturizado que integra dispositivos semiconductores. El chip se activa a través del módulo de contacto visible en la superficie del sustrato. Algunos documentos como la carta de identidad de Lituania posee ambos chips, tanto el de contacto como el de proximidad.



Figura 38. Carta de identidad de Lituania que presenta chip de contacto.

5. CONCLUSIONES

Como se ha indicado a lo largo del presente trabajo el rápido desarrollo experimentado por nuestras sociedades durante estas últimas décadas asociado todo ello a ese fenómeno comúnmente conocido como “globalización”, y que afecta principalmente al plano económico y social, ha generado, entre otras consecuencias, un aumento importante del flujo de personas que por diversas circunstancias se trasladan de un punto a otro del globo terráqueo con distintas motivaciones, gracias en otros al desarrollo de las comunicaciones, al abaratamiento de costes de estos últimos y a la mejora de la capacidad adquisitiva de los ciudadanos.

Ante tal incremento significativo de movimientos de flujos humanos a lo largo y ancho del mundo se requiere extremar aún más las medidas necesarias para garantizar la seguridad sobre los documentos de identidad que amparan a esos ciudadanos frente a los intentos de manipulación y/o alteración de esos y evitar así que, bajo el amparo de ese movimiento continuo e incesante de personas, la delincuencia nacional e internacional pueda circular y desplazarse libremente con documentos de identidad falsos o falsificados que oculten la verdadera identidad de quienes lo portan.

Durante el trabajo se ha expuesto la situación actual y futura del documento de identidad de referencia, es decir, el pasaporte desde distintos puntos de vista (técnico, legal...), al objeto de determinar si cumple o no con los fines para el que fue creado, es decir, acreditar fehacientemente la identidad de una persona y evitar situaciones como las descritas en el párrafo anterior. En relación a este asunto del presente trabajo podemos extraer las siguientes conclusiones:

PRIMERA.- A pesar de las medidas adoptadas en distintos órdenes, principalmente el legal, no se ha conseguido erradicar los intentos de manipulación y/o falsificación de los documentos de identidad a nivel general, y del pasaporte en particular. Las innovaciones y cambios periódicos que se producen en el diseño de dichos documentos logran una disminución a corto plazo en el número de falsificaciones, si bien la casuística sobre este asunto se incrementa conforme transcurre el tiempo y los falsificadores consiguen adquirir los medios necesarios para afrontar en mejor medida los intentos de falsificación de esos documentos.

SEGUNDA.-Teniendo presente que la falsificación de documentos constituye en sí una acción punible dentro de las realizadas por las personas u organizaciones criminales, se considera que la penalidad establecida para ese tipo delictivo es ciertamente insuficiente para hacer desistir de esas acciones a las personas integradas en bandas organizadas criminales.

TERCERA.-Aunque existe una normativa internacional, no solo europea sino mundial como es el documento ICAO 9303 al que están suscritos un conjunto importante de países, se observa una cierta deficiencia en exigir una mayor homogeneización en el formato de pasaporte, en concreto, a la hora de requerir un diseño similar y el uso de medidas de seguridad comunes más restrictivas, lo cual facilitaría notablemente la labor de las Fuerzas y Cuerpos de Seguridad, entre otras, a la hora de proceder a la verificación de su autenticidad.

CUARTA.-El futuro de los documentos de identidad discurrirá en los próximos años por una mejora de los ya existentes implementando innovaciones en las distintas partes que conforman el mismo. Respecto a la posible sustitución de dichos documentos “físicos” por otros “digitales” existen una serie de obstáculos o inconvenientes, principalmente desde el punto de vista técnico, que imposibilitará a corto y medio plazo hacer extensivo el uso generalizado de estos.

QUINTA.- Independientemente de las consideraciones realizadas en alguno de las conclusiones anteriores la mayor parte de los documentos de identidad actuales gozan de suficiente número de contrastes de seguridad que dificultan en gran medida la realización de falsificaciones de gran calidad y facilitan, en caso de manipulación y/o alteración, su rápida detección por los cuerpos policiales; por lo que la sociedad en general y el ciudadano en particular pueden tener confianza en el uso de las aplicaciones digitales que se van implementando progresivamente en el presente y futuro de los documentos de identidad.

6.BIBLIOGRAFIA.

- ÁLVAREZ SAAVEDRA, F.J., *Historia del pasaporte español*. Fundación Policía Española. Madrid, 2017.
- BERMEJO GARCÍA, R., *El método. Manual de verificación operativa de documentos*. Editorial Netpol Seguridad S.L. Madrid, 2016.
- DE LA UZ JIMÉNEZ, J., *Manual de Grafística*. Editorial Tirant Lo Blanch. Valencia, 2013.
- HERRÁEZ MARTÍN, José L., MÉNDEZ FUENTES, Miguel A., y SÁEZ MARTÍNEZ, Julio: 2005. *Manual de Fundamentos Teóricos de Grafística*. Departamento de Grafística del Servicio de Criminalística de la Guardia Civil. Madrid, 2005.
- MACIAS TÚNEZ, V., *Manual práctico de Grafística y Documentoscopia*, Editorial Graphicae. Madrid, 2017.
- MARTÍN RAMOS, R., *Documentoscopia: método para el peritaje científico de documentos*. Editorial La Ley. Madrid, 2010.
- SÁEZ MARTÍNEZ, J., (2019). *Ciencias forenses II: Grafística. Fundamentos*. Centro Universitario de la Guardia Civil (CUGC). Madrid, 2019.
- SANCHEZ GOZALO, R., *Guía práctica de detección de documentos falsos*. Sindicato Unificado de Policía SUP. Madrid, 2004.

WEBGRAFIA

https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1080&id_menu=5

5. *Cómo es el pasaporte español*. (s. f.). Cuerpo Nacional de Policía.

https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1090&id_menu=5

5. *Marco Legal del Pasaporte*. (s. f.). Cuerpo Nacional de Policía.

<https://dpej.rae.es/lema/documento-de-identidad>.

https://ec.europa.eu/home-affairs/orphan-pages/glossary/breeder-documents_en.

<https://esemanal.mx/2019/07/El-futuro-de-los-documentos-de-identidad-digitales-primero-en-moviles-luego-en-wearables/>.

https://www.europarl.europa.eu/doceo/document/E-8-2014-007417_ES.html. *Pasaporte único para los ciudadanos europeos*. (s. f.). © Unión Europea, 2014 - Fuente: Parlamento Europeo.

<https://guiasjuridicas.wolterskluwer.es/Content/Documento>.

<https://nanova.org/que-es-una-billetera-digital/>.

<https://www.studocu.com/es/document/universidad-pontificia-comillas/policia-cientifica/tema-4-documentoscopia-intro/4742900>.

<https://www.wellsfargo.com/es/mobile/payments/digital-wallet-basics/>.

LEGISLACIÓN CONSULTADA.

-*Ley Orgánica 10/1995*, de 23 de noviembre de 1995, del Código Penal; publicación BOE nº 281, de 24 de noviembre de 1995.

-*Ley Orgánica 4/2015*, de 30 de marzo, de protección de la seguridad ciudadana; publicación BOE nº 77 de 31 de marzo de 2015; Capítulo II. Documentación e identificación personal. (DNI, Pasaporte, etc.).

-*Real Decreto 896/2003* de 11 de julio, por el que se regula la expedición del pasaporte ordinario y se determinan sus características. BOE nº 166 de 12 de julio; modificado por R.D. 411/2014 de 6 de junio BOE nº 154, de 25 de junio de 2014.

-*Reglamento (UE) nº 2252/2004* del Consejo de la Unión Europea de 13 de diciembre de 2004; sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros; publicado DOUE (Diario Oficial Unión Europea) nº 385, de 29 de diciembre de 2004.

-*Reglamento (UE) nº 444/2009* del Parlamento Europeo y del Consejo de la Unión Europea de 6 de mayo de 2009, por el que se modifica el Reglamento (CE) nº 2252/2004 del Consejo sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros; publicado DOUE nº 142, de 6 de junio de 2009.

-*Reglamento (UE) nº 910/2014* del parlamento y del consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE. Publicado DOUE nº 257, de 28 de agosto de 2014.

-*Reglamento (UE) nº 679/2016* del parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Publicado DOUE nº 119, de 4 de mayo de 2016.

-*Reglamento (UE) 1953/2016* del Parlamento Europeo y del Consejo. de 26 de octubre de 2016, relativo al establecimiento de un documento de viaje europeo para el retorno de los nacionales de terceros países en situación irregular y por el que se deroga la Recomendación del Consejo de 30 de noviembre de 1994. Publicado DOUE nº 311, de 17 de noviembre de 2016.

-Reglamento (UE) 1191/2016 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, por el que se facilita la libre circulación de los ciudadanos simplificando los requisitos de presentación de determinados documentos públicos en la Unión Europea y por el que se modifica el Reglamento (UE) nº 1024/2012.

-*Documento 9303, sobre documentos de viaje de lectura mecánica*. Organización Internacional de Aviación Civil (ICAO). Octava edición. Quebec (Canadá), 2021.

-*UNE-EN ISO/IEC 7810:1997*. Características físicas de las tarjetas de identificación. Asociación Española de Normalización. Madrid, 1997