CIENCIA POLICIAL

183 | 2024

Ediciones Universidad Salamanca

CIENCIA POLICIAL

183
2024

CIENCIA POLICIAL, VOLUMEN 183, 2024

ISSN: 1886-5577 - ISSN en línea: 2254-0326 - Depósito Legal: S. 65-2025
https://doi.org/10.14201/cp.2025183

Composición: Glaux Publicaciones Académicas
Impresión y encuadernación: Impreso en España – Printed in Spain
Normas de estilo para publicaciones: https://revistas.usal.es/documentos/cienciapolicial/normas.pdf
Guía de buenas prácticas: https://revistas.usal.es/Guia_buenas_practicas.pdf

Ediciones Universidad de Salamanca

Plaza de San Benito s/n – 37002 Salamanca (España)

eusal@usal.es – eusal.es

Ciencia Policial pretende divulgar publicaciones científicas de los productos resultantes de la investigación que sean de utilidad para las instituciones policiales, compartiendo conocimientos sobre métodos y técnicas que faciliten su formación, modernización y actualización.

Sumario

Presentación

El uso intensivo de las tecnologías y los continuos avances en el plano tecnológico y científico están provocando en la esfera sociocultural flujos de innovación, aceptación, consolidación y obsolescencia de las actividades, transformándolas con un impacto, velocidad y alcance sin precedentes (García-Peñalvo y Pardo, 2015).

Las tecnologías de la información y comunicación permiten una difusión y alcance del conocimiento sin precedentes, exigiendo a gobiernos, instituciones de educación superior y a la sociedad en general reinventarse en sus estrategias de educación, ciencia, política y modelo de convivencia social establecido (Schwab, 2016).

La irrupción de la inteligencia artificial en un futuro puede acelerar estos cambios con una velocidad exponencial y generar incertidumbre en el paradigma de la ciencia o en sus propios postulados. Tampoco son ajenas al cambio e incertidumbre las publicaciones científicas, ya que requieren un alto nivel de exigencia en sus discusiones, contrastando sus resultados con el rigor que precisa la transmisión del conocimiento.

Otra de las consecuencias del uso intensivo de las TIC en la esfera del conocimiento científico es la aparición de ciertas problemáticas asociadas a la cultura de la inmediatez. En 2016, Benegas planteaba las siguientes ideas que se podrían aplicar a la realidad actual:

> Lo rápido obstaculiza la reflexión en la toma de decisiones y la verdadera resolución y discusión de los problemas (…). Idéntico fenómeno sucede con la información: es de tal magnitud y sobre tantos acontecimientos que no resulta posible masticarla y mucho menos digerirla y opinar con algún grado de seriedad sobre la cuestión tratada (Benegas, 2016).

La Policía, como parte integrante del tejido social, no es ajena a esta realidad, y en su defensa de los derechos, libertades y la seguridad ciudadana debe afrontar su actividad con un enfoque multidisciplinar, transversal y conectado, apoyándose en el conocimiento científico-técnico, la investigación y el uso apropiado de las nuevas tecnologías para mejorar su actividad en defensa de la seguridad pública y lograr un acercamiento a la sociedad que sirve.

Presentamos este número con cinco artículos que abordan la problemática del allanamiento y ocupación ilegal de viviendas como usurpación inmobiliaria; el procedimiento técnico-científico en la operativa policial para detectar la alteración de los motores de las motocicletas; el uso de la inteligencia artificial como herramienta de apoyo a la prevención, investigación del delito y el proceso penal; el análisis e implementación de estrategias para prevenir o atenuar la contaminación cognitiva en la obtención, análisis e interpretación de las pruebas científico-forenses; o las dificultades en la detección e investigación de ciberdelitos económicos.

Agradecemos a nuestros autores, revisores, correctores y maquetadores su trabajo e implicación en la publicación de este número de la revista, esperando que sea del agrado de los lectores, animando a la comunidad científica y a las instituciones policiales en sus investigaciones y en las aportaciones que puedan realizar a la línea editorial del Centro Universitario de Formación de la Policía Nacional.

Referencias

Benegas, A. (2016). *La cultura de la inmediatez*. El Cato. https://www.elcato.org/la-cultura-de-la-inmediatez

García-Peñalvo, F. J. & Pardo, A. M. S. (2015). Una revisión actualizada del concepto de eLearning. Décimo Aniversario. *Education in the Knowledge Society, 16*(1), 119-144. https://doi.org/10.14201/eks2015161119144

Schwab, K. (2016). *La cuarta revolución industrial*. Debate.

ARTÍCULOS

Detección de alteración de motores ubicados en motocicletas

Detection of Tampering of Engines Located in Motorbikes

José Manuel Rodríguez Jiménez
Policía local Mijas-investigador asociado al Dpto. de Matemáticas aplicadas de la Universidad de Málaga, España.
Unidad de Gestión.
jmrodriguez@mijas.es | https://orcid.org/0000-0003-3776-9887

Miguel Ángel Canorea Ruiz
Policía Municipal de Madrid, España.

Alejandro Plaza Quesada
Policía Municipal de Madrid, España.

DOI: https://doi.org/10.14201/cp.32162
Recibido: 01-11-2024 | Aceptado: 13-12-2024

Resumen
La alteración de motores en motocicletas implica modificar el motor original para mejorar el rendimiento o adaptarlo a necesidades específicas, aunque estas prácticas pueden derivar en riesgos de seguridad y problemas legales. Estos cambios pueden producirse por avería del motor y necesidad de un reemplazo, lo cual es inicialmente legal, o un cambio por un motor de mayor cilindrada que dotaría a la motocicleta de mayor potencia, pero también de mayor inestabilidad al no estar preparado el resto de componentes para ese aumento de potencia. La instalación de motores de mayor potencia en motocicletas no diseñadas para soportarlos puede comprometer la seguridad, generando inestabilidad y aumentando el riesgo de accidentes debido a frenos inadecuados, poniendo en riesgo no solo su seguridad, sino también la del resto de usuarios de la vía con el uso de dicho motor alterado.

El cambio de motor tiene su vertiente delictiva. El origen de dicho motor puede no ser lícito y, aunque el conductor del vehículo no sea responsable directamente de un delito de robo al no haber intervenido directamente en la sustracción del mismo, sí puede serlo de receptación si no posee la documentación que justifique que es comprador de buena fe. Dicha documentación trasladaría la responsabilidad del delito hacia el vendedor.

La determinación de la responsabilidad penal es secundaria cuando la dificultad principal es saber si los motores instalados pertenecen o no a dicha motocicleta. Para ello se ha realizado un estudio que permite aproximar, usando métodos matemáticos que determinan el grado de pertenencia, si el motor que porta una motocicleta es el que ha sido instalado originalmente en la misma o si proviene de una motocicleta ajena.

Palabras clave
Motores; Vehículos sustraídos; Bastidor; Falsedad documental.

Abstract
The alteration of motorbike engines can be defined as the change of the original engine in order to achieve an improvement in the performance of the motorcycle. These changes can occur due to engine failure and the need for a replacement, which is initially legal, or a change to a higher engine which would give the motorbike more power, but also greater instability as the other components are not prepared for the increased power. Inadequate brakes may mean that the rider unwittingly puts his own safety and that of other road users at risk by using the altered engine.

There is a criminal aspect to engine swapping. The origin of the engine may not be lawful and, although the driver of the vehicle is not directly responsible for a theft offence as he did not directly involve in the theft of the vehicle, he may be responsible for receiving it if he does not have the documentation justifying that he is a legitimate purchaser. Such documentation would shift the responsibility for the offence to the seller.

The determination of criminal liability is secondary when the main difficulty is to know whether or not the installed engines belong to that motorbike. To this end, a study has been carried out to approximate, using mathematical methods that determine the degree of ownership, whether the engine fitted

to a motorbike is the one that was originally installed in the motorcycle or whether it comes from another motorbike

Keywords
Engines; Stolen vehicles; VIN; Forgery.

1 Introducción

En un día de partido de fútbol, junto al estadio de una ciudad grande, pueden localizarse estacionadas en sus inmediaciones miles de motocicletas de diversas marcas, modelos y cilindradas. Al estar los agentes destinados al evento en funciones de seguridad para evitar altercados, la vigilancia de los vehículos estacionados no se considera parte del dispositivo desplazado a cubrir el evento y estos no tienen mayor relevancia que la de cualquier otro vehículo estacionado en la vía pública. Una furgoneta sin distintivos relevantes circula por la zona de estacionamientos y se acerca a un punto donde no hay dispositivos policiales ni testigos que puedan observar cómo se abre la puerta bajando, unos individuos, cogen una de las motocicletas estacionadas y la introducen en la furgoneta en pocos segundos sin que absolutamente nadie se percate de los hechos. Este hecho puede repetirse varias veces con el mismo modus operandi, abandonando el lugar con un botín que deben procesar en poco tiempo y en lugares ya preestablecidos.

Esto sería una actuación habitual de grupos organizados que pueden actuar por encargo de una marca y modelo específico o por objetivos considerados de fácil introducción en el mercado por la alta demanda de piezas, siendo los motores los elementos más cotizados.

Casos como este se han documentado en la operación en Madrid y Toledo de Guardia Civil y Policía Municipal de Madrid denominada OVIBIKE, realizada en el año 2022. La estructura del grupo criminal estaba bien definida al igual que los procesos. En primer lugar, se localizaban las motocicletas de determinadas marcas y modelos por ojeadores que rastreaban los

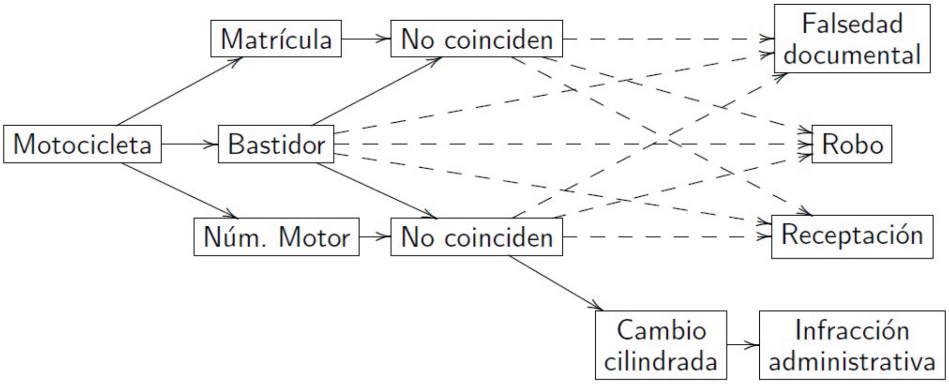
puntos de concentración de estos vehículos y que analizaban las medidas de seguridad de la zona. Con esa información, los miembros que se encargaban de la sustracción y el transporte actuaban de la forma descrita anteriormente, dejándolas ocultas y almacenadas en determinados talleres. En esos establecimientos, que contaban con las herramientas especializada necesarias, las despiezaban en pocas horas, repartiendo en otros talleres y almacenes las piezas vendibles y deshaciéndose de las no usables, como los bastidores, a los cuales se les limaba el número de motor y se reducían a partes no identificables como componentes de una motocicleta. En los almacenes se encontró material perfectamente clasificado y etiquetado, como los diferentes motores que especificaban marca, modelo y número de kilómetros.

Dentro de la documentación, el tipo de motor viene designado dentro del apartado P.5 de la ficha técnica, pero no está transcrito el número de motor completo conjuntamente con su serie. Tanto el número de bastidor como el número de motor se consideran documentos ya que identifican vehículos y sus partes. Un cambio en dichos elementos puede considerarse falsedad documental al no coincidir con el que viene transcrito en los documentos oficiales relacionados con el vehículo.

Se ha comprobado en las estaciones de Inspección Técnica de Vehículos que dentro de su protocolo no está marcada la verificación del número de motor ni cuentan con personal especializado en la localización del mismo. Esto se une a que, al ubicarse en los bajos de los vehículos, a veces sufren mucho desgaste y presentan mucha suciedad que hace casi ilegible su contenido, no pudiendo siquiera ser observables a simple vista.

En toda esta casuística se puede observar la comisión de diversos posibles delitos (ver Imagen 1), siendo muy complejo establecer una autoría clara por parte del investigador. En primer lugar, se daría el caso del robo del vehículo, que derivaría en 2 casos de receptación, consciente o inconsciente, por parte del taller y del comprador. La falsedad documental se daría en el caso de que el cambio del número de motor no estuviera registrado en la Dirección General de Tráfico, lo cual no suele hacerse, y quedaría acreditada en el caso de que se cambiara el tipo de

Imagen 1: Casuística posible ante cambio de motor



motor al no coincidir con lo anotado en la ficha técnica. Dentro de la misma marca y modelo, esa falsedad documental no podría acreditarse al coincidir el apartado P.5 de la ficha técnica del vehículo.

Las primeras actuaciones registradas en este ámbito se realizaron con casos donde era claro diferenciar un cambio de cilindrada en el motor usando descripciones físicas de los mismos y sus números de motor, requiriendo que los actuantes tuvieran los suficientes conocimientos en la materia. Los casos más comunes consistían en el cambio de un motor de 125 centímetros cúbicos de cilindrada a uno de 300 centímetros cúbicos, donde el conductor a veces no estaba autorizado legalmente a conducir dichos vehículos, como es el caso de aquellos que poseen la categoría B con 3 años de antigüedad. El detectar el cambio de motor dentro de la misma cilindrada era un caso más complejo ya que físicamente era prácticamente imposible determinarlo con una inspección visual.

Cada vez más marcas, conocedoras de este proyecto y conscientes de que su imagen se ve dañada si las estadísticas muestran que sus motocicletas son las que más se sustraen, colaboran facilitando vías de comunicación para la comprobación de los datos anómalos que se detectan.

Debido a que sería excesivo realizar consultas a las marcas cada vez que se comprueba una motocicleta en la vía pública, y

que sus medios de atención a los Cuerpos y Fuerzas de Seguridad no están operativos las 24 horas, era necesario poder establecer un método que permitiera saber si existían indicios de anomalías en la motocicleta investigada y que no dependiera de conocer la estructura física de cada uno de los motores existentes en el mercado.

En este artículo se van a examinar los datos que relacionan la información contenida en los bastidores de las motocicletas con la información contenida en los números de motor, estableciendo una posible aproximación de valores que determinen con cierto grado de confianza si los motores pertenecen a las motocicletas que los portan.

2 Método

La metodología se basa en modelos matemáticos que analizan la relación entre los números de bastidor y motor, permitiendo detectar discrepancias mediante interpolación y análisis de datos codificados. En primer lugar, existe una decodificación y extracción de información de los bastidores, unida al mismo proceso en los números de serie de motor. Con esta información, codificada adecuadamente, se puede realizar una interpolación o extrapolación de datos que emiten un valor aproximado de serie de motor a partir de un bastidor dado.

La comprobación de los datos indicados en las motocicletas es asequible a cualquier agente, ya que en la mayoría de los casos ambos datos son visibles para el observador si se conoce la ubicación de los mismos, lo cual no ocurre, por ejemplo, con los números de motor de los turismos, que quedan ocultos en el interior del vehículo.

Una observación inicial del conjunto de datos no permite establecer relaciones sin estructurar cada uno de los elementos relacionados. Es complicado observar y determinar qué método se puede aplicar en cada número de bastidor y si vale para todo

tipo de marca y modelo, por lo que es necesario analizar cada uno de ellos por separado, con el fin de determinar sus patrones y sus características especiales.

En este estudio se va a comprobar cómo se codifican los bastidores y los números de motor, qué características los definen y qué grupos se pueden establecer para obtener unos resultados fiables.

2.1 Codificación de bastidores (VIN)

En muchas notaciones, el bastidor de un vehículo se conoce como VIN, que son las siglas de Vehicle Identification Number. Este número, que en realidad no está formado solo por dígitos, está compuesto de 17 caracteres, los cuales algunas compañías han adaptado a sus intereses, desviándose de la estructura común que en un principio los define. Para evitar confusiones por lo parecido de las letras I, O y Q con los dígitos 1 y 0, estas letras no se usan en el número de bastidor.

Según la fuente consultada y el fabricante, el número de bastidor se puede codificar de diferentes formas. Para simplificar el análisis, el bastidor se divide en varias partes que permitirán agrupar los datos durante el estudio:

- Caracteres 1-3: Marca. Una misma marca puede tener diferentes series según el lugar de fabricación. El primer carácter indica la región donde se fabricó el vehículo, correspondiéndose Europa con los caracteres S a Z, aunque muchos de las motocicletas en estudio provienen de Asia, denotadas con los caracteres J a R.

- Caracteres 4-8: Modelo. El modelo puede variar a lo largo del tiempo dentro de la misma marca. Algunas marcas especifican la cilindrada o el tipo de motor de forma codificada.

- Carácter 9: En la mayoría de definiciones se corresponde con un carácter de control (dígitos 0 a 9 o la letra X), pero en la realidad solo se cumple en algunas marcas y modelos. En

otros fabricantes es un complemento, indicando una versión de la marca y modelo, o simplemente es un valor sin relevancia, pues se repite para todos los datos el mismo valor, en la mayoría de los casos el dígito 0 o 1.

- Carácter 10: Año de emisión codificado. Es útil para determinar la correspondencia con el año de fabricación del motor en algunos casos, pero lamentablemente no se cumple en todas las marcas. Los casos de los dígitos 0 a 9 se relacionan con los años 2000 a 2009, pasando la letra A a designar al año 2010 y a partir de ahí siguen el orden alfabético. El caso de las letras I, O y Q, al no poder figurar en el bastidor, hacen que no se consideren para relacionar los años.

- Caracteres 11-17: Serie dentro de la misma marca y modelo. El carácter 11 se considera por separado en algunas definiciones como una distinción de la fábrica, que puede determinar el lugar de distribución.

Ejemplo: RFBS4001161916739.

- RFB: Marca Kymco, procedente de fábrica asiática.
- S4001: Modelo Gran Dink 125.
- 1: No se corresponde con carácter de control. Es un complemento de la serie que permite diferenciar el tipo de motor asociado.
- 6: Año de fabricación 2006.
- 1916739: Serie de fabricación dentro de la misma marca y modelo.

2.2 Codificación de números de motor

Es necesario determinar los términos que se van a usar para referirse a las partes del número de motor, haciendo constar que a pesar de su nombre pueden incluir letras, incluso la I, O y Q descartadas en el número de bastidor. Se va a usar el término general número de motor para designar la codificación de los mismos debido a que las letras usadas presentan en la mayoría de los casos una interpretación numérica.

Los formatos de los números de motor se pueden agrupar por cómo están compuestos, compartiendo algunas marcas la misma codificación. No solo se comparte la misma codificación, sino, incluso, se usan los motores fabricados por otras compañías, lo cual hace mucho más sencillo para los delincuentes el poder acoplar un motor de diferente marca si es necesario para sus intereses, complicando la investigación de la procedencia del motor.

Para proceder a una identificación plena y a una correcta decodificación de los números de motor, estos se dividen en los conceptos tipo de motor y número de serie dentro de ese tipo de motor. Ese número de serie está relacionado directamente con el tipo de motor y no debe considerarse como único ya que pueden encontrarse series con la misma codificación que correspondan a diferentes tipos de motor incluso dentro de la misma marca.

Ejemplo: Para Honda, el número de motor JF28E-2036629 tiene como tipo de motor JF28E, que determina motocicletas del modelo PCX de 125 centímetros cúbicos, y como serie de motor 2036629.

Algunos fabricantes poseen una codificación dentro de los tipos de motor que permite saber para qué motocicleta están destinados.

Ejemplo: La marca Kymco suele usar los caracteres 3 y 4 del tipo de motor para indicar la cilindrada, correspondiendo 25 a 125 centímetros cúbicos, 30 a 150 centímetros cúbicos, etc., obteniéndose el valor de la cilindrada multiplicando dicho número por 5. En el caso del tipo de motor SK25M, este indica una motocicleta de 125 centímetros cúbicos.

2.3 Interpolación

En función de un bastidor, se puede definir la función f(bastidor) = valor de número de motor y usar el polinomio de interpolación lineal de Newton para obtener un valor aproximado para un bastidor dado.

$$f(x|x_1,x_2)=f(x_1) + [(f(x_2)-f(x_1))*(x-x_1)/(x_2-x_1)]$$

Existen otro tipo de interpolaciones que pueden ser más precisas en determinados intervalos de datos con un estudio más detallado, como el caso de aplicar curvas cuadráticas de Bezier (Bezier, 1970), pero la cantidad de motocicletas fabricadas en un periodo de tiempo responde a variables externas no controlables y no puede generalizarse la aplicación de las mismas.

Una vez obtenido un número de motor aproximado usando la función de interpolación, este no tiene por qué coincidir con el motor asociado oficialmente de forma exacta. Debido a las variaciones de cada fabricante, modelo y asociación de motores en la fábrica de montaje, se han de tener en cuenta las desviaciones que se puedan producir. Se define la desviación de un fabricante para un modelo determinado como el valor absoluto de la mayor diferencia con valor negativo entre 2 números de motor consecutivos ordenados por su número de bastidor, localizados en la serie de bastidores y números de motor registrados. En caso de que no exista ninguna diferencia negativa, la desviación encontrada se considera 0 o, lo que es lo mismo, que no se ha encontrado desviación en los datos, lo cual no se da en la mayoría de los casos.

Uno de los motivos por lo que no existe una correlación exacta 1 a 1 entre número de bastidor y número de motor en la casi totalidad de los casos es debido a que en las cadenas de montaje no se producen e instalan de forma paralela, usando algunos de los motores para ser testados como garantía de calidad en el proceso. En casos como Harley Davidson o algunos modelos de Kawasaki, parece ser que el troquelado de número de bastidor y número de motor se produce de forma simultánea, circunstancia que no se ha podido comprobar por falta de respuesta por parte de las marcas.

Ejemplo: Para los números de bastidor A, B y C, ordenados por su valor de serie, los motores respectivos tienen como serie 112625, 112574 y 118008. La diferencia entre los valores de A y B es de -51 unidades, mientras que la diferencia entre los valores de B y C es de 5434 unidades. Definimos la desviación de ese

modelo de motocicleta como 51, que es el valor absoluto del mayor valor negativo encontrado.

Determinar si la diferencia en unidades que se produce entre la serie interpolada y la serie real de la motocicleta es considerada aceptable, para valorar si una serie de motor puede pertenecer a la motocicleta que lo porta, depende de la desviación del modelo de motocicleta y del tamaño del intervalo donde se evalúan los datos. A mayor amplitud del intervalo, mayor imprecisión en la aproximación de la serie por realizarse siguiendo una interpolación lineal, por lo que hay que tener en cuenta un segundo factor de desviación.

Se ha de definir una función que determine un porcentaje de validez para los datos de la motocicleta en comparación con los valores obtenidos, teniendo en cuenta la desviación del modelo y el tamaño del intervalo en el que se interpola. Esta función es el resultado del estudio de las formas de distribución de los números de motor para varios países y modelos, definiéndose como:

$$v=\text{Máximo}(0,100-(50*(\text{serieMotocicleta}-\text{serieEstimada})^2/((\text{tamañoIntervalo}*1/3)+\text{desviacion})^2))$$

Al definirse el valor de v como un porcentaje, el valor que resulte debe estar comprendido entre 0 y 100. Por ello se ha de definir en la función v que su valor sea el máximo entre 0 y el resultado obtenido, ya que en caso contrario podría dar resultados negativos cuando un número de motor no está dentro del rango de validez. El valor de la función v será 100 cuando la serie del motor coincida exactamente con el valor estimado mediante la función f.

Usando un intervalo para los valores de v considerados como aceptables, 60 <v <= 100, podemos obtener un intervalo de series de motor válidas dado un número de bastidor. Este intervalo de series de motores proporcionado es una forma fácil de interpretar los resultados y, de esta forma, comprobar si el número de motor que porta la motocicleta puede ser considerado como válido para ese número de bastidor.

2.4 Análisis

El estudio incluyó datos de motocicletas nacionales e internacionales, demostrando la eficacia del algoritmo en la detección de motores alterados y su potencial para integrarse en bases de datos globales. Para dar mayor validez al estudio realizado, se ha extendido y complementado con datos obtenidos en motocicletas de otros países que figuran en fuentes abiertas, contando la base de datos final con 10600 datos aproximadamente a fecha de realización de este artículo.

De estos datos se han apartado las marcas denominadas raras, al existir poco volumen de motocicletas en el mercado que pertenezcan a estas marcas. No se han descartado los datos, sino aplazado su estudio hasta ampliar la muestra con un número de datos mínimo que garantice la obtención de resultados fiables. El disponer de un solo dato de una marca y modelo determinado puede ofrecer orientación sobre un nuevo caso, pero el usuario que valore esos datos debe contar con la suficiente experiencia en su manejo, ya que el algoritmo no puede proporcionarle información al ser necesarios al menos 2 datos para poder ofrecer una respuesta con una valoración estimada.

En la primera fase del estudio se descartaron datos que no ofrecían información relevante, como el código de homologación o la fecha de primera matriculación.

El código de homologación depende del número de bastidor, por lo cual es una información redundante y que, en este estudio, no aporta mayor conocimiento. Sin embargo, sí es de gran utilidad en caso de bastidores borrados o manipulados, ya que puede orientar a los investigadores en la reconstrucción de los datos borrados.

La fecha de la primera matriculación ofrece gran margen de error y no se puede establecer una relación clara ya que depende de factores externos como la zona y el modelo donde la motocicleta ha sido destinada para la venta. Se han encontrado casos con variaciones superiores a 2 años entre motocicletas con

bastidores casi consecutivos debido a rematriculaciones, por lo que debe ser valorado adecuadamente. Este valor es útil como complemento a la investigación ofreciendo un indicio fiable cuando la variación es considerable. No obstante, al disponer los bastidores de un carácter que orienta sobre la fecha de emisión, puede considerarse un valor no necesario.

Una vez descartados los valores que no ofrecían información relevante, se procedió a una evaluación mediante agrupaciones (clústeres) que compartían características similares. Estas agrupaciones no eran similares en todas las marcas, por lo que hubo que proceder a una partición del bastidor y una división de los tipos de métodos que se podían usar según las marcas y modelos.

Los bastidores se dividieron en 3 partes durante el estudio para determinar las agrupaciones:

- Caracteres 1-8: Determinan una marca y modelo de motocicleta en un rango de tiempo.

- Carácter 9: Al no ser siempre un carácter de control, se considera como un valor separador adicional. Se usa en marcas como Piaggio o Suzuki.

- Caracteres 10-17: Serie del bastidor. Engloba el año de emisión para algunos casos. La parte inicial de la serie es la que permite establecer unas diferencias orientativas sobre el número de motor asociado, sobre todo, sobre la serie del motor.

En función de las marcas y su codificación de bastidores según los 3 grupos indicados, se procedió a una clasificación de métodos para establecer la relación número de bastidor-número de motor. Cuando para un tipo de bastidor se pueden aplicar al menos 2 métodos, se usa el menos restrictivo y que permite agrupar mayor cantidad de datos sin llevar a error.

Los métodos usados se denominan según los caracteres usados para establecer la relación y son los siguientes (entre paréntesis el inicio del número de bastidor):

- Método 10: Usa los caracteres comunes 1 a 10 del bastidor para la agrupación. Puede usarse para las siguientes marcas:
  - Suzuki (VTT)
  - Triumph (SMT)

- Método 11: Usa los caracteres comunes 1 al 11 del bastidor para la agrupación. Puede usarse para las siguientes marcas:
  - Cagiva (ZCG)
  - Dresel (WDM)
  - Husqvarna (ZCG)
  - MV Augusta (ZCG)
  - Piaggio (ZAP)
  - Yamaha (9C6, JYA, LBP, LPR, MH3, MLE, RKR, RLC, VG5, VTL, ZD0)
  - Yiying (LD5)

Nota: El inicio de bastidor ZCG, al igual que otros que no se mencionan en este estudio, se ha encontrado en varias marcas.

- Método 12: Usa los caracteres comunes 1 al 12 del bastidor para la agrupación. Puede usarse para las siguientes marcas:
  - Arctic Cat (VAD)
  - Daelim (KMY)
  - Derbi (VTH)
  - Ducati (ZDM)
  - Fantic (ZFM)
  - Honda (ME4, VTM, ZDC)
  - Husqvarna (ZKH)
  - Kawasaki (JKA, JKB, MH4, ML5, RGS)
  - Kymco (LC2, RFB)
  - Malaguti (ZJM)
  - Peugeot (VGA)
  - Piaggio (LBM, RP8)
  - Rieju (VTP)
  - Royal Enfield (ME3)
  - SMC (RFR)
  - Suzuki (JS1, LC6, MH8, MLC)
  - SWM (ZN0)
  - SYM (LXM, RFG)
  - TGB (RFC)
  - TM Racing (ZEX)

- Método 10-12: Usa los caracteres comunes 1 al 8 y 10 al 12, ignorando el carácter 9. Se usa en aquellos números de bastidor que tienen caracteres de control. Puede usarse para las siguientes marcas:
  - Aprilia (ZD4)
  - Baotian (L82, LX6, LZP)
  - Benelli (ZBN)
  - Beta (ZD3)
  - BMW (WB1, WB3, WB4)
  - Brixton (VA4)
  - BTM (L82)
  - Can-Am (3JB)
  - CF Moto (LCE)
  - Derbi (ZDP)
  - Goes (LCE)
  - Hanglong (LLM)
  - Honda (JH2, LTM, LWB, MLH, RLH)
  - Hyosung (KM4)
  - Keeway (L4H, LBB, TSY)
  - KTM (VBK)
  - Linhai (LL8)
  - Longjia (L4H)
  - Mitt (LFG)
  - Motowell (L4H, L5Y, LUJ)
  - PGO (RFV)
  - Qian Jiang (LAW)
  - Qingqi (LAE)
  - Suzuki (JSA)
  - TMS (L82, LFG)
  - Voge (LLC)
  - Wottan (LFG, LZB)
  - Zontes (LD3)

Esta clasificación permite separar la parte final del bastidor y asociarla con un número que es el que se usará como base para la interpolación. Igualmente, a cada grupo resultante de la clasificación se le asocia un tipo de motor fijo, variando únicamente la serie del motor. Esta serie del motor puede presentar letras, pero suelen ser comunes y son asociables a un número, por lo que permiten el uso en la interpolación al interpretarse como valor numérico.

- Ejemplo 1:
  - Bastidor JKALE650EFDA01306. Motor ER650AE-AJ6081.
  - Bastidor JKALE650EFDA01710. Motor ER650AE-AJ7975.

Los bastidores Kawasaki de la serie JKA usan el método 12, por lo que tienen como parte común JKALE650EFDA. Esta agrupación permite conocer el tipo de motor, el ER650AE, y reduce los datos a considerar para la interpolación. El inicio de las series de motor es común y es AJ para este caso, por lo que se puede optar por cambiarlo a un número o descartarlo para tomar únicamente los valores numéricos. De esta forma, los valores a usar para la interpolación se reducirían a:

- Bastidor 01306. Motor 6081.

- Bastidor 01710. Motor 7975.

Estos valores son más sencillos de manejar en los cálculos.

- Ejemplo 2:
  - Bastidor JSAAK47A642110446. Motor K428-167878.
  - Bastidor JSAAK47A542113208. Motor K428-172812.

A diferencia del ejemplo anterior, los bastidores Suzuki de la serie JSA tienen carácter de control. Esto hace que no se pueda agrupar por los 12 primeros caracteres ya que se observa como difiere el carácter de control en la posición 9 y que haría que no se ordenaran adecuadamente los bastidores según ese criterio.

Descartando el carácter de la posición 9 y agrupando según el criterio 10-12, se pueden reducir los datos adecuadamente para ser usados en los cálculos de interpolación, quedando de la siguiente forma:
- Bastidor 10446. Motor 167878.
- Bastidor 13208. Motor 172812.

Los mismos datos simplificados pueden usarse para estimar un número de motor usando extrapolación. Esta metodología se usa cuando los valores que se quieren examinar están fuera del

rango de datos que se poseen, pero se tienen al menos 2 datos que nos permitan realizar una valoración. Estos datos han de ser considerados adecuadamente y conociendo las limitaciones de la extrapolación matemática cuando no siguen un patrón fijo. En el caso de que los valores sean muy cercanos, la pendiente de la recta resultante de extrapolación lineal puede verse afectada y emitir una valoración con una desviación desproporcionada. A partir de las extrapolaciones realizadas durante las evaluaciones del método, se considera que una diferencia inferior a 300 unidades en el número de bastidor de los datos usados puede dar resultados incorrectos con una probabilidad alta, por lo que se condiciona la aplicación de la extrapolación a datos que cumplan dichos criterios.

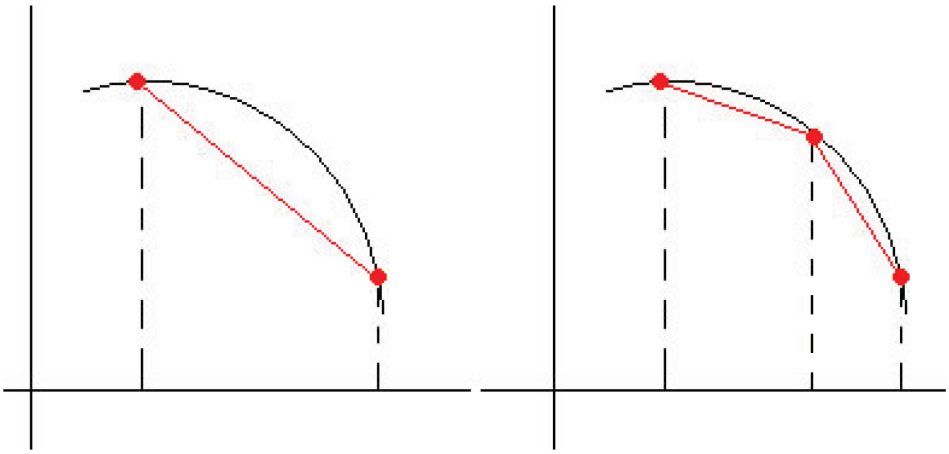
El sistema usado, con algunas variaciones y consideraciones, puede ser usado en sentido inverso, permitiendo estimar un número de bastidor a partir de un número de motor. No puede usarse en todos los casos debido a que el mismo tipo de motor se usa para varias marcas y modelos, pero el número de casos es inferior al 5 % en los datos usados en este estudio.

2.5 Automatización del algoritmo

Partiendo de una base de datos inicial de números de bastidor y números de motor, puede crearse un tipo de inteligencia artificial que use un algoritmo evolutivo basado en la aceptación-rechazo de nuevos datos. Cada vez que el sistema recibe un nuevo dato, lo evalúa siguiendo la metodología establecida usando la interpolación/extrapolación y lo considera aceptable o lo rechaza. Si lo considera aceptable, este dato pasaría a formar parte de la base de datos ampliada, lo cual haría que los algoritmos usados para evaluar ese tipo de bastidores recibieran una mejora al reducirse los intervalos donde se evaluarían los nuevos datos (ver Imagen 2). Este método de sistema autoevaluado ya fue descrito en la investigación de permisos de conducir falsificados (Ojeda Aciego y Rodríguez-Jiménez, 2023).

En el caso de que el valor estimado se considerara dudoso, al ofrecer un porcentaje de aceptación que no permite valorar adecuadamente si es un dato correcto (40-60 %), el dato pasaría a

Imagen 2: Reducción del margen de error en interpolación numérica



una base de datos externa considerada de "datos dudosos". Estos datos dudosos son evaluables nuevamente a lo largo del tiempo cuando la aportación de nuevos datos permita realizar una nueva comprobación. Esos nuevos datos pueden determinar con mayor seguridad si el dato dudoso es aceptable o no.

De la misma forma, un autoanálisis del sistema puede comprobar si existen valores erróneos en la base de datos. Estos son los casos de errores de transcripción o de datos considerados válidos inicialmente por no existir un mínimo de datos para evaluar y que el propio algoritmo revela como dudosos. Durante la realización de este estudio, se han detectado unos 12 casos aproximadamente de errores de transcripción usando el sistema de autoanálisis, lo cual dota al sistema de robustez.

3 Resultados

En los primeros casos detectados de motores que no pertenecían a la motocicleta que los portaba, existía una diferencia clara en el tipo de motor, lo cual era indicio suficiente para proseguir con la investigación, consultando a las marcas fabricantes sobre la veracidad de los datos obtenidos en la anomalía detectada.

Ejemplo: Caso real de motocicleta Yamaha X-Max con matrícula 42**GF* localizada en Mijas el 17-9-23.

Se comprobó la motocicleta asociada al bastidor JYASJ06400005145, portando la motocicleta el motor J409E-047289. Usando una aplicación informática en la que se había implementado el algoritmo, se determinó que el tipo de motor correspondiente debería ser J406E y la serie de motor estimada sería 021384 con una variación de ± 840 unidades.

Al no coincidir el tipo de motor y existir una gran diferencia en su número de serie, se procedió a evaluar de forma inversa a partir del número de motor. No pudo estimarse un rango al no existir suficientes datos, pero sí se obtuvo que dicho motor correspondería a un bastidor con una serie inferior a JYASJ098000003514.

Realizando las comprobaciones a través de la marca, se comprobó el número de motor asociado real, J406E-021381, el cual había sido estimado con una gran precisión por el algoritmo, y el número de bastidor correspondiente al motor que portaba, JYASJ098000001345, que se correspondía con la estimación realizada, aunque esta fuera menos precisa por la falta de datos.

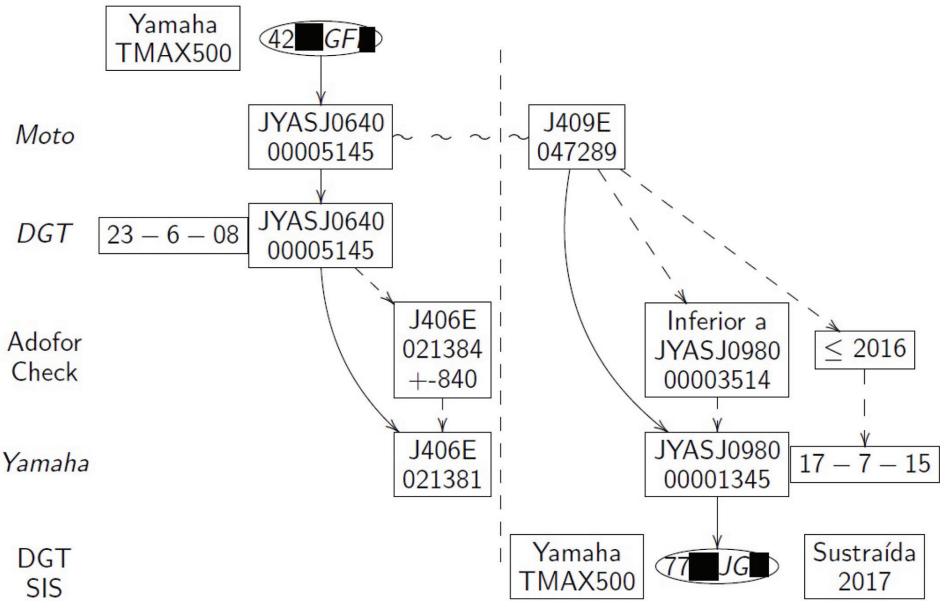
Comprobado este número de bastidor aportado por la marca, se verificó que pertenecía a una motocicleta de la misma marca y modelo, aunque de diferente año de fabricación (2008 y 2015 respectivamente), que figuraba sustraída desde el año 2017 (ver Imagen 3).

La continua aportación de datos al sistema hace que se refinen los resultados de las evaluaciones y que la precisión del algoritmo aumente. No solo son posibles la evaluación y la detección de motores que difieran en su tipo de motor, sino que se ha llegado a detectar también algún caso en el que el tipo de motor es el mismo y solo varía la serie.

Ejemplo: Caso real de motocicleta Honda PCX 125 con matrícula 67**KV* localizada en Madrid el 14-6-24.

Se comprobó mediante una aplicación donde estaba implementado el algoritmo el bastidor ZDCJF83A0KF014025, portando

Imagen 3: Descripción del proceso de verificación del vehículo 42**GF*



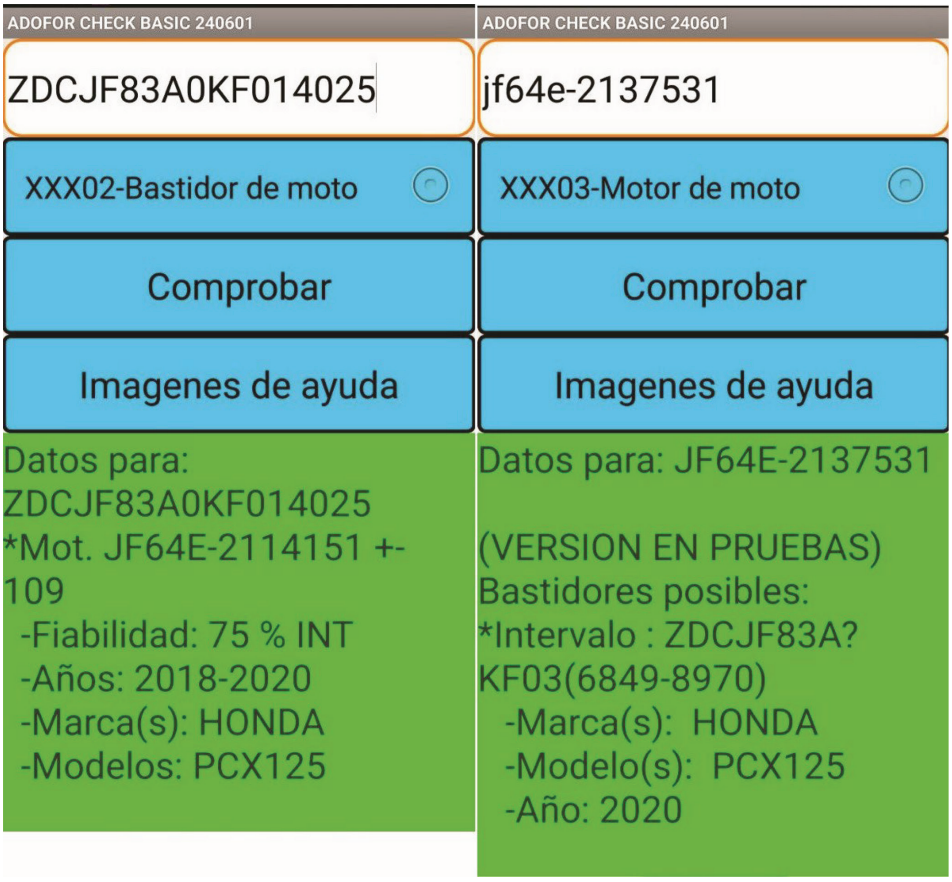
la motocicleta el motor JF64E-2137531. Según el algoritmo, el tipo de motor correspondiente coincide y la serie de motor estimada es 2114151 con una variación de ± 109 unidades (ver Imagen 4)

Al existir una notable diferencia en el número de serie del motor, se procedió a evaluar de forma inversa a partir del número de motor. Se estimó un rango de bastidores con una precisión de 13 caracteres ZDCJF83A?KF03, siendo la parte variable estimada del bastidor el intervalo 6849-8970.

Realizando las comprobaciones a través de la marca Honda, se verificó el número de motor asociado real, JF64E-2113956, el cual había sido estimado con una gran precisión a pesar de que el grado de desviación tenía un margen de error aproximado de 100 unidades. El número de bastidor correspondiente al motor que portaba, ZDCJF83A0KF037811, se correspondía con la estimación realizada al estar dentro del rango de bastidores indicado.

Comprobado este número de bastidor aportado por la marca Honda, se verificó que pertenecía a una motocicleta de la misma

Imagen 4: Datos aportados por el algoritmo en la aplicación Adoforcheck



marca y modelo, variando el año de primera matriculación en tan solo 10 meses, que figuraba sustraída desde el año 2023.

La aplicación Adoforcheck en la cual se implementó el algoritmo se ha distribuido a más de 450 agentes de Policía Nacional, Guardia Civil, Mossos, Ertzaintza y Policía Local en diversos puntos de toda España, para el testeo del algoritmo. No puede considerarse que exista una muestra delimitada que se haya usado para probar el algoritmo al no poder definirse como tal de forma estricta, ya que los datos que se han comprobado no han sido devueltos en su totalidad para su registro, y los datos usados para las comprobaciones han ido aumentando a medida que se iban recibiendo y procesando.

La distribución y el uso de la aplicación comenzó a realizarse cuando contaba aproximadamente con unos 2000 datos, variando hasta los casi 10600 existentes en el momento de la realización de las conclusiones de este estudio. La introducción de nuevas marcas y modelos en determinados intervalos de tiempo, que no existían en los datos iniciales, hacen que la muestra sea evolutiva y no fija, por lo que no se ha podido evaluar adecuadamente cada uno de estos casos tal como se hace en un experimento a partir de una muestra fija dada con un grupo de datos de aprendizaje y otro de evaluación.

Entre los casos detectados de cambio de motor, sustraídos o no, usando el algoritmo, se han reportado 51 a día de la fecha. Se tiene constancia de que el número de casos detectados es superior, no habiendo podido ser registrados adecuadamente. Las zonas de Madrid y Barcelona son las que concentran el mayor número de detecciones.

3.1 Ampliación del estudio a motocicletas de Suecia

Para estudiar que el algoritmo es extensible y reproducible en otros países, se fueron examinando casos de motocicletas con placa de matrícula extranjera que se encuentran en nuestro país. Estos casos eran escasos y aislados, ya que es difícil que un ciudadano de otro país traslade un vehículo de estas características por los costes que ello conlleva.

El Gobierno sueco permite consultar públicamente la base de datos de vehículos registrados en su país a través del enlace https://fordon-fu-regnr.transportstyrelsen.se/. Para motocicletas de determinadas marcas con fecha anterior al año 2017, aparecen reflejados en la consulta el número de bastidor y el número de motor, por lo que se pueden usar para comprobar los resultados del algoritmo.

Obteniendo matrículas de motocicletas de forma semialeatoria que aparecían en páginas web dedicadas a la venta de vehículos, se valoró una muestra superior a 2000 motocicletas de forma paralela a la base de datos inicial. Con esta nueva muestra se realizaron 2 estudios.

En el primer estudio se comprobó la validez del algoritmo únicamente con las motocicletas de origen sueco, siendo compatible incluso para marcas de motocicletas que no se comercializan en España. No se encontraron anomalías ni ningún dato que presentara discrepancias con la metodología descrita.

En un segundo estudio se valoró la inclusión de los datos suecos en la base de datos existente con la información recabada de motocicletas matriculadas en España, siendo todos los datos compatibles y complementarios a los ya existentes.

La confirmación de la validez del algoritmo para motocicletas matriculadas en Suecia permitió ampliar la base de datos original sustancialmente, siendo esta ampliada regularmente con datos que provienen de motocicletas matriculadas en dicho país.

4 Discusión

La metodología matemática empleada en este artículo y los resultados obtenidos en los diferentes casos estudiados indican que el porcentaje de éxito, entendiendo como éxito que el motor que porta el vehículo se haya comprobado mediante fuentes oficiales que ha sido cambiado, es bastante alto una vez que el algoritmo detecta que hay un posible cambio de motor, superior al 90 %.

Por la proliferación de robo de vehículos de determinadas marcas, se ha intensificado la búsqueda de datos de los modelos más frecuentes, sobre todo de aquellos que, por la ubicación del número de motor, hacen más sencilla su detección Esto conlleva un mayor refinamiento en los resultados ofrecidos, lo cual implica mayor precisión en la detección de un motor cambiado.

La carencia de datos para algunas marcas y modelos en determinados espacios de tiempo es uno de los problemas que se afrontan cada vez que se detecta una motocicleta de este tipo. Contar con al menos un dato de la marca y modelo a veces es suficiente para orientar sobre el tipo de motor y el tipo de serie que se usa. La experiencia permite que se pueda usar conocimiento adicional

sobre la estructura de los números de motores de ciertas marcas y, por similitud, concretar al menos si la estructura es válida.

Se ha comprobado que la metodología empleada puede usarse en casi todas las marcas, existiendo casos específicos que aún están bajo investigación, como ciertas motocicletas de BMW cuya seriación sigue un patrón diferente.

Para casos como Harley Davidson o Buell, aunque podría usarse la metodología de la misma forma, la investigación de patrones ha permitido establecer un caso particular de cómo extraer el número de motor correcto sin necesidad de usar el algoritmo, al estar codificado dentro del bastidor. Dentro de la aplicación se ha implementado el caso específico para no depender del número de datos que se tengan.

Dentro de Europa, se están haciendo comprobaciones para verificar si la metodología es extensible a motocicletas cuya matriculación se realiza en otros países, siendo los resultados diversos. Con los datos de motocicletas de países como Francia, Hungría o Suecia se ha verificado que el sistema es compatible e incluso se complementan las bases de datos de ambos países. En otros países europeos se poseen aún datos escasos para poder valorarlos adecuadamente, si bien actualmente todos los casos contemplados usando datos previos han resultado evaluables positivamente.

Usando esos datos de motocicletas que portan matrículas extranjeras en nuestro país, la línea de investigación indica que hay ciertos modelos que parece que se producen únicamente para determinados países y otros que se distribuyen por varios.

Otra variante del uso del algoritmo que está facilitando la labor de los investigadores es el poder trazar el número de bastidor de una motocicleta que ha sido borrado total o parcialmente a partir del número de motor.

El mal uso de esta metodología puede llevar a casos de motores considerados cambiados erróneamente. El desconocer las peculiaridades de los formatos, fechas de emisión o estructuras es un hecho que se ha de admitir previamente para abstenerse de valorar un motor dudoso. Por ejemplo, el caso de usar solamente

la interpolación de un número de motor que usan varias marcas sin usar la valoración comprobando el número de bastidor.

En cuanto a la tipología penal de los casos detectados, las sentencias que se están recibiendo tienden hacia la figura de la receptación más que a la sustracción. El fundamento es que no se puede demostrar que el titular de la motocicleta realizara la sustracción del vehículo, orientando la investigación hacia determinados talleres donde se realizaron los cambios si el titular puede demostrarlo con una factura. Los casos complejos se producen cuando la motocicleta tiene más de un titular durante el periodo comprendido entre la fecha de robo del motor que porta y la actualidad, ya que se desconoce en qué momento se instaló el motor.

El tipo penal de falsedad documental, cuando hay un cambio de tipo de motor, aunque está claro al diferenciarse con el tipo de motor que viene descrito en la ficha de características técnicas, suele quedar en segundo plano cuando el origen del motor es de un vehículo sustraído. Entre todas las sentencias que han podido ser recopiladas, no existe ninguna condena por este concepto.

Se suelen aplicar los atenuantes de error de tipo o prohibición, ya que los titulares de las motocicletas en su mayoría desconocen que el origen del motor proviene de un ilícito penal, aunque el precio del motor puede incitarles a pensar que el origen del mismo no es legal.

No se puede excluir la parte gráfica en los estudios, ya que es complementaria a la parte de análisis de los datos. El hecho de clonar el número de bastidor y el número de motor de una motocicleta puede hacer que el algoritmo los dé como válidos, cuando pueden observarse anomalías en la forma del grabado de los datos. La combinación de ambas aporta una fuerte base para el estudio de las falsificaciones y la localización de los falsificadores basados en sus patrones (Ojeda Aciego y Rodríguez-Jiménez, 2021). La asociación de motocicletas con motores cambiados pertenecientes a las mismas marcas y modelos en zonas concretas de una región no solo permite trazar la identidad de los responsables, sino establecer los vínculos que puedan tener sus clientes y los indicios para investigar si forman parte de la misma red criminal (Rodríguez-Jiménez *et al.*, 2016).

Tras los resultados obtenidos en los diferentes casos donde el algoritmo ha detectado un posible cambio de motor, la metodología propuesta ha demostrado ser altamente efectiva, contribuyendo significativamente a la recuperación de vehículos sustraídos y a la detección de motores alterados, reforzando la seguridad vial y facilitando investigaciones legales.

Siendo el algoritmo complejo para una aplicación directa mediante una tabla visible de datos, la opción de una aplicación que realice los cálculos necesarios y presente los resultados al usuario se ha comprobado que es un método eficiente y útil. Al no ser necesario el acceso a un enlace externo para el que sea necesario el uso de internet, las comprobaciones son sencillas, ágiles y directas, siempre y cuando el usuario tenga los conocimientos mínimos para interpretar los resultados adecuadamente.

Las propias compañías han visto reducidas las consultas de verificación al consultarse únicamente aquellos casos considerados como positivos, siendo su interacción con los agentes de la autoridad más fluida y con una respuesta más positiva al comprobarse que se están detectando más casos en proporción al número de consultas realizadas.

Como trabajo futuro se ha comenzado a recopilar datos de motores de otro tipo de vehículos para expandir el estudio hacia ellos, cumpliéndose la estructura básica de datos del algoritmo planteado en este artículo. Inicialmente se ha extendido hacia ciclomotores y quads, por similitud en la localización de los elementos identificativos y por la coincidencia de marcas de fabricantes en un número considerable de casos, lo cual conlleva estructuras similares, si no coincidentes. El precio en el mercado de los motores de ciclomotores es considerablemente menor al de las motocicletas, por lo que el beneficio obtenido por los delincuentes es menor, limitándose a un mercado más local la distribución este tipo de motores y piezas.

La dificultad de extender el estudio hacia turismos o camiones radica en la complejidad de localizar el número de motor y poder recabar los datos necesarios para establecer una base de datos de referencia. No solo por estar los motores cubiertos e

inaccesibles desde el exterior, sino que, aun con el motor visible, el número de motor queda lejos de la vista del observador siendo necesario acceder mediante endoscopio o incluso desmontar algunas piezas del anclaje.

Agradecimientos

Los autores agradecen a los miembros de ADOFOR su colaboración para llevar a cabo este estudio, así como a las marcas oficiales que siempre han colaborado en la comprobación de datos para verificar que los motores habían sido sustituidos en los casos detectados.

Referencias bibliográficas

Bezier, P. (1970). *Numerical control: mathematics and applications*. *Emploi des machines à commande numérique*. London, New York : J. Wiley.

Ojeda Aciego, M. y Rodríguez-Jiménez, J. M. (2021). Formal concept analysis with negative attributes for forgery detection. *Computational and Mathematical Methods, 3*(6). https://doi.org/10.1002/cmm4.1124

Ojeda Aciego, M. y Rodríguez-Jiménez, J. M. (2023). Advances in Forgery Detection of Driving Licences Usinf Truthfulness Degrees. *Computational Intelligence and Mathematics for Tackling Complex Problems 4. Studies in Computational Intelligence*, vol. 1040. https://doi.org/10.1007/978-3-031-07707-4_18

Rodríguez-Jiménez, J. M., Cordero, P., Enciso, M. y Mora, A. (2016). Analysing criminal networks using Formal Concept Analysis with Negative Attributes. En *Proc. of International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE)*.

Análisis e implementación de estrategias para prevenir o atenuar la "contaminación" cognitiva en la obtención, análisis e interpretación de las pruebas científico-forenses en el proceso penal

Analysis and Implementation of Strategies to Prevent or Mitigate Cognitive 'Contamination' in the Collection, Analysis and Interpretation of Forensic-Scientific Evidence in Criminal Proceedings

Raquel Amezcua de Miguel
Policía Nacional, España.
felisademiguel@hotmail.com

DOI: https://doi.org/10.14201/cp.32165
Recibido: 07-11-2024 | Aceptado: 02-12-2024

Resumen
Durante la obtención, análisis e interpretación de las pruebas científico-forenses en un procedimiento judicial, siempre intervienen los sesgos cognitivos. Estos afectan a las decisiones que conducen a la imposición de una condena que puede no tener nada que ver con la verdad de lo que pasó y ser todo lo contrario a lo justa que se pretende. Hay numerosos estudios que describen los sesgos cognitivos, cómo actúan sobre expertos e inexpertos, y describen cómo han afectado a numerosos procedimientos judiciales dando lugar a la puesta en libertad de cientos de personas que han sido ingresados en prisión injustamente. Implementar medidas y procedimientos estandarizados que los disminuyan puede contribuir a que el precio que se ha de pagar por un error judicial no sea tan alto. Los sesgos son inconscientes e inherentes al ser humano, conocer sus fuentes y su origen permite entender cuáles son los factores que pueden influir en las decisiones de los expertos que tratan de esclarecer una verdad que solo conocen un autor, una víctima o un testigo que rara vez cuentan la misma historia. Es posible minimizar sus efectos.

Existen estrategias que tratan de evitar que los sesgos influyan en las decisiones de los expertos, decisiones que, hasta hace poco, se pensaba que eran fruto de un razonamiento lógico, científico y jurídico. En este trabajo, se enumeran muchas medidas que la literatura científica propone para conseguirlo, orientadas hacia los expertos, a su entorno y a intervenir en todas las etapas de la investigación para alcanzar la legitimidad y el amparo jurídico deseado. Resulta muy difícil reunir tantas ciencias en una sola, la forense, y aplicarla teniendo en cuenta los factores psicológicos del individuo, que parecen infinitos.

Palabras clave

Ciencia forense; Sesgo cognitivo; Sesgo de confirmación; Mitigación de sesgos; Toma de decisiones; Información contextual irrelevante; Investigación.

Abstract

During the obtaining, analysis and interpretation of scientific-forensic evidence in a judicial procedure, cognitive biases always intervene. These affect the decisions that lead to the imposition of a sentence that may have nothing to do with the truth of what happened and be the opposite of what is intended to be fair. There are numerous studies that define cognitive biases, how they act on experts and inexperienced people, and describe how they have affected numerous judicial procedures, leading to the release of hundreds of people who have been unjustly imprisoned. Implementing standardized measures and procedures that reduce them can help ensure that the price that has to be paid for a judicial error is not so high. Biases are unconscious and inherent to human beings, knowing their sources and origin allows us to understand what factors can influence the decisions of experts who try to clarify a truth that only an author, a victim or a rare witness knows time they tell the same story. It is possible to minimize its effects. There are strategies that try to prevent biases from influencing the decisions of experts, decisions that, until recently, were thought to be the result of logical, scientific and legal reasoning. In this work, many measures are listed that scientific literature proposes to achieve this, oriented towards experts, their environment and intervening in all stages of the research to achieve legitimacy and the desired legal protection. It is very difficult to gather so many sciences into one, forensic

science, and apply it taking into account the psychological factors of the individual, which seem infinite.

Keywords
Forensic science; Cognitive bias; Confirmation bias; Bias mitigation; Decision-making; Irrelevant contextual information; Investigation.

1 Abordando el sesgo cognitivo y otros conceptos

El sesgo cognitivo es un término que se utiliza para describir una interpretación subjetiva de un individuo, cómo esta interpretación influye en sus decisiones y en las interacciones con su entorno. Por lo que un mismo estímulo puede ser percibido de forma distinta por diferentes individuos que lo estén observando al mismo tiempo (Curley *et al.*, 2022).

El sesgo es una desviación sistemática, involuntaria e inconsciente de un estándar de racionalidad al emitir un juicio sobre algo percibido con los sentidos (perceptual) o basado en ideas o teorías del pensamiento (conceptual). Esta desviación se produce principalmente debido al uso de heurísticas (atajos mentales que permiten resolver problemas y emitir juicios de manera eficiente, facilitando la toma de decisiones ante desafíos de forma rápida y efectiva). También son consecuencia de las limitaciones cerebrales en el procesamiento de información, por influencias emocionales, morales o sociales, y distorsiones que ocurren en el almacenamiento y la recuperación de información en nuestra memoria (Páez, 2021).

Uno de los sesgos que más afecta a cualquier dominio, incluso en un procedimiento judicial, es el sesgo de confirmación. Es conocido coloquialmente como "visión de túnel" y describe cómo los expertos enfocan su atención en una hipótesis (por expectativas, existencia de un sospechoso, confesión...), buscando información que la refuerce e ignorando elementos que la contradigan, lo que puede inducir a tomar decisiones erróneas (Findley, 2011)

El impacto del sesgo cognitivo en la toma de decisiones se ha documentado en muchas áreas de especialización como medicina, seguridad o en la ciencia forense y, dentro de la ciencia forense, se ha replicado en muchas disciplinas (huellas dactilares, patología forense, ADN, armas de fuego, análisis digital forense...), lo que se traduce en que ningún dominio es inmune al sesgo (Dror y Kukucka, 2021).

Hace ya 50 años que se predijo que el sesgo de confirmación llegaría hasta nuestros sistemas jurídicos. Comprender las heurísticas del pensamiento que conducen a los sesgos podría mejorar la toma de decisiones en situaciones ambiguas que requieran interpretación humana (Tversky y Kahneman, 1974).

En la actualidad, existen numerosos estudios e investigaciones empíricas que han demostrado cómo los sesgos no solo afectan a legos en la materia, sino a investigadores, expertos forenses y miembros de la comunidad judicial, provocando la contaminación cognitiva de las pruebas forenses a lo largo del proceso judicial (Kassin *et al.*, 2013).

Esta contaminación del proceso penal se debe a una característica intrínseca de los sesgos, y es que son fácilmente contagiosos entre los expertos, desde quienes obtienen y/o analizan una prueba de la escena de un crimen hasta los que interpretan el resultado de esa evidencia. Esta propagación del sesgo de una etapa a otra se conoce como "cascada de sesgos" o "bola de nieve", cuando, además, se va integrando información irrelevante, haciendo que el sesgo cobre mucho más impulso y consiga contagiar a muchas más personas dentro del proceso completo de la investigación (Dror *et al.*, 2018).

2 Problemática de la contaminación cognitiva en el proceso penal

"Sesgos cognitivos evaluación de casos penales: una revisión de la investigación", de Meterko y Cooper (2021), es una investigación sobre la influencia de los sesgos en los procesos

penales; un estudio completo de las fuentes del sesgo que muestra dónde están las grietas por donde se escapa la ciencia; una revisión de 30 artículos que confirman cómo el factor humano es la causa principal de esas grietas y lo importante que es desarrollar estrategias de protección contra los sesgos cognitivos para repararlas. El objetivo es dotar a la ciencia forense de una base científica incuestionable, por lo que es necesario establecer herramientas para proteger las investigaciones criminales y la administración de la justicia de los sesgos cognitivos.

Los conocimientos cognitivos deben servir para minimizar el sesgo, mejorar el trabajo de los expertos y alcanzar una justicia legítima. No se pueden tomar decisiones sin tener en cuenta los procesos cognitivos que están involucrados en la toma de decisiones. Comprenderlos es fundamental para que estas decisiones sean consistentes y no estén sesgadas (Dror y Langenburg, 2019). Situaciones como ofrecer información contextual irrelevante, diferencias entre examinadores en su formación o experiencia, en sus expectativas o los distintos intereses de la propia organización pueden influir sobre los servicios forenses, pueden ser motivo suficiente de contaminación cognitiva o que los resultados no sean imparciales (Dror y Pierce, 2019).

"El hallazgo más consistente en la ciencia forense es... inconsistencia" (Dror, 2023). En algunas pruebas que se practican durante el juicio oral hay poca fiabilidad y reproducibilidad, varios examinadores llegan a conclusiones distintas ante una misma evidencia por diferencias en las políticas de laboratorio, en los métodos de análisis, uso de diferentes programas informáticos, distintos niveles de experiencia o capacitación y por la aparición de sesgos. Finalmente, agravando el problema, las conclusiones de los científicos y los expertos en un tribunal despiertan la confianza en quienes las escuchan, se interpretan como imparciales, por lo que son tenidas en cuenta sin vacilar para imponer condenas que, en ocasiones, son injustas (Dror, 2015), vulnerando así los cimientos de la ciencia y la justicia.

La mayoría de las sentencias injustas son consecuencia de esos errores sistemáticos y cognitivos que se han ido contagiando en cada fase del procedimiento judicial, dando lugar a la toma de una mala decisión. Recientemente, abril de 2024, se

ha creado "The European Registry of Exonerations (EUREX)", una página web que recopila información y publica la historia de personas oficialmente absueltas en Europa, contando en la actualidad con un total de 130 exoneraciones, 10 de ellas ocurridas en España. Pese a su creación, el alcance de las condenas erróneas sobre personas inocentes en Europa es aún desconocido y difícil de evaluar (Geven *et al.*, s.f.).

La página digital estadounidense "The National Registry of Exonerations" se fundó en 2012 y muestra 3.625 exoneraciones desde el año 1989. Entre todas estas personas exoneradas, cumplieron un total de 32.750 años ingresados injustamente en una prisión. Esta página clasifica las exoneraciones por los factores que contribuyeron a su liberación, que fueron identificaciones erróneas de los testigos, perjurio o falso testimonio, confesión falsa, errores en la evidencia forense y conducta inadecuada de profesionales (datos revisados a 12/12/2024). Cada uno de los 3.625 inocentes fueron castigados injustamente y los 3.625 verdaderos culpables continuaron siendo una amenaza para la sociedad (UCI Newkirk Center for Science and Society, 2024).

En España, los factores que han contribuido a la exoneración de inocentes son idénticos a los de Estados Unidos, como se muestra en los siguientes ejemplos.

2.1 El caso de Romano Van der Dussen

Un holandés privado de libertad durante 12 años por tres agresiones sexuales en Fuengirola. Dos de las víctimas y una testigo lo reconocieron como el autor de los hechos, pese a que se encontraron muestras de ADN y huellas que no coincidían con las suyas. Al poco tiempo, en el Reino Unido, fue detenido un asesino y violador en serie cuyo perfil de ADN coincidía con el perfil de dichas evidencias (Ceberio Belaza, 2015).

2.2 El caso de Rafael Ricardi

Privado de libertad 13 años por una violación que no había cometido. Era drogadicto y dormía en la calle, lo que condujo

a que fuera incriminado por una oleada de violaciones que se venían sucediendo por la zona. Tras su detención, mientras se encontraba durmiendo bajo un puente, fue identificado por una víctima y el Instituto Nacional de Toxicología de Sevilla redactó un informe sobre los restos de semen, en el que se habían detectado algunos genes que eran compatibles con los del sujeto. Fue puesto en libertad tras la detención de su verdadero autor (Ceberio Belaza, 2016).

2.3 El caso de Ahmed Tommouhi y Abdelrrazak Mounib

Dos inmigrantes de origen marroquí condenados en 1992. El primero condenado a 24 años de prisión por violación y agresión sexual a una menor y, dos años después, a otros 51 años por otras agresiones sexuales y detención ilegal. El segundo fue declarado como su cómplice. Fueron condenados antes de que los peritos presentaran los informes de ADN, debido a la credibilidad que la comunidad judicial atribuyó a los testimonios de las víctimas. Las violaciones y los robos con el mismo modus operandi continuaron y, tras reabrirse las investigaciones, se detuvo al verdadero autor, a quien, además de confesar los crímenes, pertenecían los rastros biológicos obtenidos de las víctimas. El Tribunal Supremo anuló la segunda condena, pero rechazó revisar el resto de casos, pese a las confesiones del verdadero autor. Mounib murió en prisión, cinco años después de su ingreso, a causa de un ataque al corazón. Tras varias acusaciones públicas de los abogados hacia las autoridades por su falta de reconocimiento de errores, un recurso de amparo ante el tribunal Constitucional y la intervención del Tribunal Europeo de Derechos Humanos, Tommouhi fue absuelto en 2023, casi 31 años después de la condena y 15 años privado de libertad (Geven *et al.*, s.f.).

En la mayoría de exoneraciones hay un factor común, fallos en los procedimientos de identificación, tanto de las víctimas como de los testigos. La asociación norteamericana Innocence Project habla de un 75% de fallos. Es también unfactor común en los ejemplos expuestos de casos sucedidos en España. El principal problema que se aprecia es que, en la mayoría de los delitos, el testimonio, el cual puede contener numerosos

sesgos y defectos, es la única evidencia con la que se cuenta para tratar de esclarecer los hechos y poner nombre a su autor (Manzanero, 2020).

Volviendo al caso de Ahmed Tommouhi y Abdelrrazak Mounib, en el nuevo juicio se desveló que las alineaciones de las identificaciones habían estado extremadamente sesgadas. Esto es solo un ejemplo de por qué todos los procedimientos de investigación deberían estar dotados de protocolos con criterios científicos que permitan evaluar la credibilidad del testimonio. Se debería hacer una valoración seria sobre si la justicia debe aceptar o no las declaraciones o las ruedas de reconocimiento como prueba única condenatoria (Gamboa *et al.*, 2000).

3 Normativa para reducir la contaminación cognitiva durante el proceso penal

El informe de la Academia Nacional de Ciencias de los Estados Unidos (National Academy of Sciences, en adelante NAS) del año 2009 supuso la crítica más dura hacia la ciencia forense. Fue la primera vez que la comunidad científica puso de manifiesto públicamente las limitaciones de muchas disciplinas forenses que contribuyeron a la condena de personas inocentes. El informe sostiene que las disciplinas forenses están poco investigadas y reguladas, por lo que se han de implantar mecanismos y protocolos válidos que tengan en cuenta los errores cognitivos, que permitan construir una base científica sólida (Edmond *et al.*, 2014).

Las normas internacionales ISO/IEC 17020 e ISO/IEC 17025 incluyen requisitos para que el trabajo forense adquiera ese rigor científico necesario, exigiendo un compromiso para establecer sistemas que garanticen la imparcialidad, asegurando que las conclusiones estén lo menos influenciadas posible por el sesgo cognitivo y otros tipos de errores.

La primera, ISO/IEC 17020:2012 "Requisitos para el funcionamiento de diversos tipos de organismos que realizan la ins-

pección", enumera los requisitos generales para la inspección forense en la escena de un crimen de cualquier parte del mundo, excepto en Australia y Nueva Zelanda. Los dominios forenses para aplicación de esta norma son investigación de la escena del crimen, huellas latentes, armas de fuego, antropología y patología forenses, disciplinas que requieren de interpretación en las que los análisis son subjetivos, por lo que se centra en el trabajo del examinador.

La segunda, ISO/IEC 17025:2017 "Requisitos generales para la competencia de los laboratorios de ensayo y calibración", es la norma que siguen los laboratorios acreditados de criminalística de todo el mundo. Establece los requisitos generales que deben implementarse en ellos. Los dominios en los que se aplica esta norma son aquellos cuya cuantificación es más objetiva, como toxicología, análisis de drogas o ADN, por ejemplo (Dror y Pierce, 2019).

4 Motivos por los que persiste la contaminación cognitiva

Los expertos forenses poseen amplios conocimientos sobre su dominio científico, lo que les confiere mucha seguridad en su trabajo. Sin embargo, la mayoría desconocen los aspectos cognitivos que subyacen en la imparcialidad de sus decisiones y tienen ideas equivocadas sobre cómo alcanzar esa objetividad (Dror y Pierce, 2019).

Numerosos estudios han demostrado que la mente humana es capaz de hacer que el individuo, por muy buenas intenciones que tenga, responda de forma distinta a lo que su formación, experiencia o moral le harían responder en otras circunstancias, un error que, en muchas ocasiones, es producto de los sesgos (Kassin *et al.*, 2013).

Los motivos por los que se hace difícil luchar contra el impacto de los sesgos son muchos y variados, pero, sobre todo, son su naturaleza humana y los mitos que aún se cree de ellos como

ciertos. Dror (2020) describe estos mitos, que persisten por más pruebas empíricas que se hagan para desmentirlos.

4.1 Punto ciego del sesgo

Pocos expertos son conscientes de sus sesgos y otros tantos sostienen que ellos son inmunes, tal y como se ve reflejado en tres estudios en los que la mayor parte de los individuos encuestados ven la existencia de sesgos en los demás, pero no en ellos mismos (Pronin *et al.*, 2002). Años más tarde, otra encuesta concluye que la mayor parte de los expertos examinados reconocían su existencia en dominios ajenos al propio, creían que eran inmunes al sesgo y, en caso necesario, podían controlar su influencia de manera consciente (Kukucka *et al.*, 2017).

4.2 Ilusión de control

Algunos de los expertos que reconocen el sesgo creen que pueden minimizar sus efectos con fuerza de voluntad. Este intento consciente por reducirlo lo que en realidad puede provocar es que se piense más en él. En un estudio de veredictos de jurados en los que el juez les pidió ignorar ciertas pruebas inadmisibles, se obtuvo como resultado que la sola petición influía en las decisiones que los jurados tomaban, pensaban aún más en esas pruebas inadmisibles (Steblay *et al.*, 2006).

4.3 Inmunidad de expertos

Se cree que los expertos son inmunes al sesgo. De hecho, los expertos pueden incluso ser más susceptibles a los sesgos que alguien que no tenga experiencia o formación en una materia determinada. Una persona no experimentada no formularía expectativas acerca de un resultado a obtener basado en sus propias experiencias,prestaría atención a todas las circunstancias y variables con idéntico interés, lo que permitiría reducir el impacto de sus propios sesgos. La experiencia y capacitación del experto le generan expectativas, atención

selectiva y automatismos, lo cual puede influir en su juicio (Dror *et al.*, 2018).

4.4 Cuestiones éticas

Muchos piensan que los sesgos son un problema ético o de mala conducta intencionada. El sesgo afecta a todos, a expertos o inexpertos, no es un fenómeno consciente como lo son las discriminaciones de carácter personal, malas conductas o la falta de integridad de un individuo.

4.5 Manzanas podridas

Cuando se detectan errores en un análisis determinado, son atribuidos a la falta de falta de experiencia o incompetencia de los expertos que los desarrollan. Si así fuera, estos errores serían fáciles de detectar y de corregir. Los sesgos cognitivos son implícitos al humano y no se detectan fácilmente.

4.6 Protección tecnológica

Existe la creencia de que la tecnología nos protege de los sesgos, dando por hecho que aporta un enfoque imparcial y objetivo. Los sesgos humanos siguen estando presentes en la tecnología. En un estudio con los Sistemas Automáticos de Identificación Dactilar (Automated Fingerprint Identification Systems, en adelante AFIS), que utilizan bases de datos de huellas dactilares, confirmaron que se producían identificaciones falsas en algunas comparaciones. Antes de comparar una huella latente, los expertos debían seleccionar las posibles huellas dactilares con las que hacer la comparación. El sistema ofrece los resultados por puntuación, en función de la similitud con la huella latente. Como resultado de la investigación, los expertos eran más propensos a buscar esas coincidencias en las primeras huellas de la lista, obviando las demás, pese a que las coincidentes reales podrían estar a cualquier altura. La tecnología facilita el análisis, pero no sustituye el juicio humano que se necesita para tomar una decisión ante un resultado obtenido (Dror *et al.*, 2011).

5 Diferentes fuentes de sesgo y su influencia en el proceso penal

A continuación, se describen ocho fuentes de sesgo, clasificadas en tres grupos en función de su relación con la naturaleza humana, con la experiencia o el entorno del experto, y/o con el propio caso que se está investigando (Figura 1).

Figura 1: Ocho fuentes de sesgo y error en las ciencias forenses

LAS OCHO FUENTES DE SESGO

1. El cerebro, factores humanos y cognitivos 2. Factores personales	Naturaleza humana
3. Expectativas de la tasa base 4. Factores organizativos 5. Educación y formación	Entorno, cultura y experiencia
6. Datos 7. Materiales de referencia 8. Información contextual	Caso investigado

Fuente: adaptado de la pirámide de Taxonomía Dror (Dror, 2020).

Las fuentes que están relacionadas con la naturaleza humana son las fuentes de sesgo que tienen mayor probabilidad de que este aparezca, por ser intrínseco al ser humano. Son los más difíciles de corregir. Se encuadran aspectos personales como la ideología, la motivación o el cerebro y sus procesos psicológicos.

En las fuentes que se relacionan con entorno, cultura y experiencia del experto, el sesgo empieza a perder influencia aumentando la posibilidad de corregirlo. Aquí se incluyen las expectativas que surgen de su experiencia; los factores relacionados con la organización, como ser contratado por fiscal o defensa, un presupuesto ajustado o tiempo disponible para culminar la investigación.

La fuente de sesgo que se relaciona con el caso investigado es, sobre todo, la información contextual. Conocer información que

no es relevante para desarrollar la tarea en el laboratorio, puede inducirnos a seguir una hipótesis errónea, por ejemplo saber que existe un sospechoso. Son las más sensibles al cambio si se aplican las herramientas adecuadas, como lo son los procedimientos estandarizados que imponen criterios objetivos (Dror, 2020).

5.1 Fuentes relacionadas con la naturaleza humana

Estas fuentes son las más difíciles de corregir, ya que la mayor parte de los sesgos cognitivos actúan al margen de la conciencia y los expertos no están dispuestos a admitir que sus decisiones pueden estar sesgadas. Estrategias como proponer un escenario alternativo, rendición de cuentas o el entrenamiento para reducir sesgos (descritas más adelante) pueden ayudar a evitar algunos errores.

5.1.1 El cerebro, factores humanos y cognitivos

La naturaleza humana y el funcionamiento del cerebro introducen una serie de sesgos debidos a una infinidad de procesos psicológicos universales para dar sentido al mundo que nos rodea. El cómo se presentan las pruebas (las que se muestran al principio producen mayor impacto), fenómenos como el pensamiento en grupo (lo que se deduce en conjunto es difícil de cuestionar a nivel individual), efectos de recencia (recordar mejor la información del final de la lista que la primera) o efectos de rasgo positivo (prestar más atención a la presencia de un rastro que a la ausencia) son resultado de procesos cognitivos de cada individuo que influyen en cómo interpretamos la realidad que nos rodea. Varios estudios experimentales, tomando como muestra a agentes de policía, jueces y fiscales, confirman lo susceptibles que son los expertos a los sesgos (Meterko y Cooper, 2021).

5.1.2 Factores personales

Ideología personal, valores, experiencias, creencias, motivación, capacidad de asumir riesgo, tolerancia a la ambigüedad, respuesta al estrés, a la fatiga, la personalidad... son factores que influyen en la forma en la que se lleva a cabo una tarea, en cómo se recopilan o cómo se interpretan los datos.

Cómo afectan los factores personales en las decisiones ha llevado a que en algunos textos se hagan, por ejemplo, clasificaciones de las conductas que se observan en los jueces en función de su actitud: juez lógico, juez sensible, juez consecuente... Esta tendencia a dejarse influir por sus ideales o valores se identifica con el sesgo de anclaje (De la Rosa Rodríguez y Navarro, 2016).

Se ha escrito un libro de conductas de jueces titulado *El perfil criminológico del juez prevaricador* (Güidi Clas, 2003), donde estas son clasificadas en seis categorías: machista, redentor, estrella, político, genético y elitista, en función del estudio que hizo la autora sobre sentencias por delitos graves y la inclinación de los jueces a adoptar un estilo cognitivo determinado en cada una de ellas.

Cómo juzgan los jueces, de manera formalista aplicando la ley o realista basándose en corazonadas, ha sido debatido durante varias décadas (Guthrie *et al.*, 2007). Personalidad, ideología, religión, género, raza..., las investigaciones han dejado claro que los jueces no siempre toman decisiones objetivas, incluso ellos se mueven por intuición y heurísticas para tomar sus decisiones (Guthrie *et al.*, 2007; Rachlinski y Wistrich, 2017).

5.2 Fuentes de sesgo relacionadas con el entorno, la cultura y la experiencia

Este tipo de fuentes provocan una expectativa por un determinado resultado antes de que se hayan valorado las pruebas reales, pudiéndose alterar las interpretaciones que se hagan al respecto. Estrategias como reorganizar los laboratorios, crear hipótesis alternativas o implantar la figura de un gestor de casos (y que veremos más adelante) pueden ser buenas medidas para minimizar los efectos de los sesgos.

5.2.1 Expectativas de la tasa base

El muestreo y el análisis de los expertos se ven afectados por asociaciones con casos vividos anteriormente que no guardan

ninguna relación con el caso actual, expectativas basadas en experiencias pasadas.

Lo que hace que un experto sea experto es precisamente la vivencia de casos previos. Esto es interesante y útil cuando existen circunstancias similares a esos casos, pero, cuando es posible que el caso actual contenga información inesperada, puede ser peligroso y sesgar la investigación en una dirección equivocada, porque es muy probable que esa información no se tenga en cuenta.

Continuando con el experimento comentado en el punto anterior, sobre la causa de la muerte de los niños, los expertos han vivido más experiencias en las que mueren más niños negros por homicidio que niños blancos, por lo que esto también influyó en el número de patólogos que optaron por decidir homicidio en vez de accidente cuando el niño era negro y su cuidador el novio de la madre (Dror *et al.*, 2021).

5.2.2 Factores organizativos

Son muchos y variados, con origen en la organización, la cultura, interacciones sociales, ideologías, lenguaje o jerga utilizados..., pueden provocar errores en la interpretación de la información. La presión del tiempo por querer culminar la investigación, expectativas por alcanzar ciertos resultados, estrés, controles presupuestarios... son factores organizativos que afectan al trabajo y a su resultado.

En un estudio con investigadores de la escena del crimen de Estados Unidos, en adelante CSI, en un contexto con gran cantidad de sangre, se observó el alto grado de concienciación que los investigadores tenían sobre los recursos limitados que había en ese momento en la organización, lo que produjo que se recogieran un número inferior de muestras a las habituales (Lidén y Almazrouei, 2023).

Los estudios han demostrado que los expertos llegan a conclusiones diferentes ante una misma prueba en función de si trabajan para la Fiscalía o si lo hacen contratados para la defensa, lo

que induce a sesgos (denominado sesgo de lealtad adversarial) (Murrie *et al.*, 2009).

5.2.3 Educación y formación

Afectan a la forma en que observamos, razonamos y tomamos decisiones. Muchos de los dominios forenses, el análisis forense digital, armas de fuego, huellas dactilares... han surgido de la experiencia policial, no de la ciencia. Este tipo de formación puede inculcar la búsqueda de una sola hipótesis en vez de valorar otras alternativas, o que los examinadores crean que es más importante apoyar el trabajo de investigador policial para resolver el caso que el de ser científicos (Dror, 2020).

5.3 Fuentes de sesgo relacionadas con el caso investigado

Es en este tipo de fuentes donde aparecen los efectos de "cascada y bola de nieve" comentados anteriormente. Una información que se recibe, de manera independiente a las pruebas obtenidas en la escena del crimen, puede contaminar el resultado de su valoración o la interpretación que se haga de dicho resultado. Son las fuentes de sesgo que mejor responden a las estrategias para minimizar sus efectos, como las verificaciones o procedimientos ciegos, la alineación de pruebas o compartimentar el flujo de trabajo (técnicas que veremos más adelante).

5.3.1 Los datos

Algunos datos, como las impresiones dactilares, no causan sesgo por sí mismos, pero, combinados entre ellos, pueden dar lugar a información sesgada. Por ejemplo, en identificación forense, hay dos etapas, en la primera hay que comparar dos marcas y determinar si son similares y en la segunda etapa, hay que valorar el significado de esa similitud, son o no son del mismo origen. En la primera etapa, existe el riesgo de cometer errores. Siguiendo con el ejemplo de la identificación forense, concretando con marcas de mordedura, la piel no es buena superficie para capturar una marca. Es un tejido elástico que, al presionar, hace que los dientes reboten y no se retengan todas las características

de la dentadura (bordes de los dientes, existencia de coronas o empastes...), puede estirarse o encogerse durante el mordisco, lo que altera la apariencia de la marca. Además, el mordisco provoca hematoma, por lo que su aspecto se altera aún más. Es imposible practicar comparaciones precisas. En la segunda etapa del proceso de comparación, los expertos deben decidir cómo interpretar estos datos y valorar si las marcas pertenecen a una misma dentadura. Es aquí donde surgen las amenazas de sesgar el resultado del análisis: dependiendo del grado de similitud, añadiendo que hay información contextual irrelevante (existe un sospechoso, una confesión...) o la propia expectativa del examinador por querer resolver un caso pueden hacer que la valoración de la segunda etapa de la identificación forense tenga un resultado equivocado (Saks, 2010).

Uno de los ejemplos que más se citan en artículos que tratan sobre este aspecto es el caso del atentado del 11M en el Cercanías de Madrid, por afectar a uno de los análisis más prestigiosos de las ciencias forenses (la dactiloscopia). Pese a las discrepancias de los expertos en huellas españoles, el FBI determinó que las huellas latentes encontradas eran de un abogado de Estados Unidos que estaba registrado en sus archivos de huellas por haber servido en el ejército. Como información contextual irrelevante, contaban con que el sospechoso era de origen musulmán y había defendido a un grupo de estadounidenses que habían querido unirse a Al Qaeda. Semanas después, la policía española identificó a la persona a quien correspondían las huellas (Stacey, 2005).

5.3.2 Materiales de referencia

Fuente íntimamente relacionada con los datos y también derivada de la aplicación del método de comparación, como en ADN, huellas dactilares, la escritura a mano o las armas de fuego. La evidencia real hallada en la escena del crimen no se interpreta a partir de los datos que esta contiene, sino que la comparación empieza desde los datos del sospechoso conocido (materiales de referencia). Analizar primero la huella indubitada del sospechoso, y extraer de ella la información o características a encontrar en la evidencia de la escena del crimen, puede dirigir el análisis hacia una identificación errónea (Dror, 2020).

Tomando como ejemplo las armas de fuego, el hecho de haber encontrado un arma en la casa del sospechoso, hace que los primeros exámenes se hagan con el rastro que deja esta arma en un cartucho y compararlo después con el cartucho que se ha encontrado en la escena. El problema de ir hacia atrás con este tipo de razonamiento es que se produce un sesgo impulsado por el objetivo guiando el proceso cognitivo, buscando la coincidencia a partir de los datos obtenidos en el arma encontrada. En resumen, el examinador está impulsado por un objetivo en vez de por los datos reales contenidos en el cartucho encontrado en la escena del crimen, produciendo así un sesgo de confirmación, concretamente de imputación (Cuellar *et al.*, 2022).

5.3.3 Información contextual

Casi siempre, los expertos están sometidos a información irrelevante por estar trabajando con la Policía y la Fiscalía. Una confesión de un sospechoso, una identificación por testigos, existencia de antecedentes penales del sospechoso, confesiones... información contextual que lleva a sospechar de ese objetivo al que se refiere la información. Esta información, que no es relevante para llevar a cabo el trabajo de laboratorio, puede hacer que el analista escoja una técnica diferente y/o interprete los resultados del examen de la evidencia erróneamente.

En un experimento, reunieron certificados de defunción de niños que habían fallecido por causas desconocidas. Los patólogos forenses evaluados debían decidir entre homicidio o accidente doméstico. Cuando se les ofreció intencionadamente, como información contextual irrelevante, que el niño era de origen afroamericano y que su cuidador en el momento de la muerte había sido el novio de la madre, hubo más patólogos que determinaron que la causa de la muerte había sido homicidio que los que dictaminaron accidente. Cuando la información irrelevante facilitada fue que el niño era blanco y su cuidador en el momento de la muerte había sido su abuela, la mayoría de los patólogos actores del experimento concluyeron que la causa de la muerte había sido accidente doméstico (Dror *et al.*, 2021).

6 Estrategias para prevenir o atenuar la contaminación cognitiva en el proceso penal. *Debiasing*

La ciencia forense es un conjunto de disciplinas que proceden de otras ciencias a su vez. Su objetivo es identificar cuáles son los elementos que hay presentes en la escena de un delito que le lleven a determinar una relación biunívoca entre autor y resultado.

La comunidad científica está de acuerdo en que se han de establecer mecanismos de corrección en los laboratorios de criminalística, en la escena del crimen y en los juzgados. Allá donde exista el factor humano, la comprensión de los procesos psicológicos necesarios para tomar decisiones es fundamental para implantar estas medidas de corrección y convertir la ciencia forense actual en ciencia forense sólida y fiable.

A continuación, se presenta una clasificación de las estrategias propuestas en la literatura para reducir los sesgos *(debiasing)* que no obedece a ningún modelo teórico establecido, sino a facilitar su exposición.

6.1 Punto de partida. Un nuevo enfoque para las ciencias forenses

Las ciencias forenses son el punto de unión entre ciencia, derecho, psicología, Policía y Estado para el auxilio de la Administración de Justicia, en crisis no solo por errores judiciales o mala praxis, sino por una mala interpretación de las pruebas durante todo el proceso penal. El enfoque fragmentario de la ciencia forense, que se ha distribuido entre fuerzas del orden, servicios forenses, juzgados y tribunales, ha contribuido a una falta de supervisión estratégica y de responsabilidad que contribuye a esa mala interpretación (Morgan, 2020).

La estructura de la ciencia forense fragmentada en subdisciplinas promueve una ciencia multidisciplinaria adaptada a las

necesidades de la organización, con procedimientos y tecnología específica para cada una de las áreas. Se han ido "bautizando" según los rastros encontrados (huellas dactilares, marcas de herramientas, residuos de disparo...), su representación en objetos (armas de fuego, calzado, neumáticos...), por su vinculación con otras disciplinas (antropología, toxicología, biología forense...), por tipo de suceso (muerte, incendio, accidente...), por método o tecnología empleada (perros, tecnología de imagen forense...) y por procesos (investigación, identificación, interpretación forense...). Nuevas ramas de especialización van surgiendo a medida que aparecen nuevos delitos.

La evolución en el mundo digital, además, supone nuevas subdisciplinas (tecnología de la información forense, análisis forense del audio, análisis forense de imágenes...), con nuevos retos para los científicos forenses que no son expertos informáticos.

En el estudio de muchas de estas subdisciplinas están involucradas otras, por ejemplo, en rastros de armas de fuego se relacionan la física (estrías en los proyectiles) con la química (restos de pólvora), pero las marcas son examinadas por policía científica que no suele estar en contacto con los laboratorios ni de física ni de química, laboratorios que, a su vez y con mucha probabilidad, están ubicados en distintas secciones de los laboratorios forenses, desconectados los unos de los otros. Si surge un problema en una etapa del proceso, difícilmente será detectado en etapas posteriores (Roux *et al.*, 2021).

Esta ciencia multidisciplinaria promueve enfoques adaptados a las necesidades organizacionales y a la propia disciplina, queriendo tener los mejores avances técnicos y sofisticados. Anulando así el propósito principal de la ciencia forense, que es dar respuesta a las preguntas que surgen después de un hecho delictivo: ¿qué pasó? ¿Quién lo hizo? ¿Cómo lo hizo? Si se adopta un carácter interdisciplinario, con interacciones entre todas las disciplinas involucradas, obtendremos respuestas apoyadas en ciencia forense (Roux *et al.*, 2021).

Un cambio de enfoque, integrado, podría garantizar la conexión entre las fases de la investigación y los tribunales. Facilitaría el establecimiento de estrategias, métodos y prácticas de

trabajo que devolverían la confianza al sistema judicial (Giovanelli, 2023).

Uno de los primeros intentos para conseguir este planteamiento global lo representa la "Declaración de Sydney" (Roux *et al.*, 2022). Un conjunto de principios cuya meta es definir la ciencia forense como un esfuerzo basado en investigación, en ciencia, en casos, en analizar evidencias de actividades pasadas, detectarlas, recuperarlas, examinarlas e interpretarlas para entender eventos anómalos con relevancia pública.

El quinto principio de esta declaración, explicado por resultar interesante para el tema sobre la contaminación cognitiva, dispone que la ciencia forense tiene que hacer frente a un continuo de incertidumbres. Las huellas son incompletas, imperfectas y se degradan con el tiempo. La investigación sobre cómo se generan, cómo se transfieren, cómo se degradan o cómo se detectan es fundamental para determinar los límites de esa incertidumbre o ambigüedad, aprovechar el potencial informativo de dicha huella, interpretarla y evaluar su valor probatorio. Entender las ambigüedades asociadas a la interpretación, evaluación y comunicación de los resultados es un componente de la ciencia forense; por lo que también requiere investigación sobre el sesgo y la toma de decisiones. El fin último de la ciencia forense es que un juez comprenda el valor de los hallazgos (Roux *et al.*, 2022).

La Organización de Comités Científicos de Ciencias Forenses de Estados Unidos (Organization of Scientific Area Comitees for Forensic Science, OSAC) representa un ejemplo de iniciativa de colaboración multidisciplinaria entre científicos forenses, psicólogos, juristas y estadísticos, un enfoque integrado de sus conocimientos para investigar, elaborar y difundir instrucciones sobre las mejores prácticas en las distintas disciplinas forenses (Kukucka y Dror, 2023.).

6.2 Estrategias aplicadas al sistema de trabajo

Las expectativas y las motivaciones personales de los expertos que intervienen crean escenarios idóneos para la aparición de los sesgos. Las diferentes investigaciones promueven la aplicación

de medidas correctoras que van desde la escena del crimen, continuando por los laboratorios para acabar en los juzgados.

6.2.1 Organización de los laboratorios

Es una de las principales medidas propuestas para desfragmentar la ciencia forense. No existe una organización estandarizada de los laboratorios que describa las áreas en las que tengan que estar estructurados y qué disciplinas forenses deben integrar cada una. Resulta interesante la creación de modelos que incluyan áreas de consultoría especializadas en la resolución de problemas; espacios o departamentos compartidos para el examen de las pruebas y la comunicación entre los expertos de cualquier disciplina. Pintura, fibras, vidrio, residuos de disparos, rastros biológicos, dactilares... independientemente de la disciplina a la que obedezca el rastro, convertirlo en un departamento holístico de pruebas de rastreo, por ejemplo (Roux *et al.*, 2021).

El hecho de que los laboratorios formen parte de una red estatal de instituciones públicas o policiales hace que estén más expuestos a información irrelevante. Aunque en muchos laboratorios de Estados Unidos o Reino Unido imparten formación en procesos cognitivos a sus expertos, no es suficiente para minimizar la contaminación cognitiva, por lo que una de las recomendaciones del anteriormente comentado informe de la Academia Nacional de Ciencias de los Estados Unidos fue retirar a todos los laboratorios o instalaciones forenses públicas lejos del control administrativo de los funcionarios encargados de hacer cumplir la ley. Alejados de influencias y presiones por acabar la tarea y no despertar el sesgo de lealtad, que empuja a mostrar fidelidad hacia quien lo ha contratado, ya sea parte acusatoria o defensa (Dror, 2013).

Esto va en consonancia con el séptimo principio de la Declaración de Sydney, del que se extrae que el científico debe evitar interpretar sus hallazgos adaptándolos a las necesidades de quien solicitó la información (Roux *et al.*, 2022).

Adoptar un método de trabajo con efecto triaje puede resultar útil para que los laboratorios trabajen con eficacia cognitiva;

se trata de clasificar los casos por dificultad o vulnerabilidad al sesgo. Esto les permitirá, en situaciones de falta de tiempo o pocos recursos para verificaciones ciegas, aplicar los procedimientos más demandantes de medios cuando sean realmente necesarios (Dror, 2013).

6.2.2 Fomentar el esfuerzo cognitivo mediante una autorregulación competitiva

El análisis de la muestra recogida en la escena del crimen se asignaría por duplicado a dos laboratorios distintos que desconocerían dicha duplicidad. Los expertos solo sabrían que a veces se solicitan estas pruebas de forma aleatoria. Si el resultado obtenido por ambos no es el mismo, habría un procedimiento de adjudicación: el laboratorio que descubriera dónde está el fallo del otro sería el que recibiera el pago por el trabajo realizado y, además, un segundo pago por descubrir dicho error (Reese, 2011).

Esta técnica presenta algunos inconvenientes, solo corrige los sesgos que se pueden atribuir a la falta de esfuerzo cognitivo en el experto que procesa la muestra, no se puede aplicar en demarcaciones judiciales en donde solo haya un laboratorio y aumenta considerablemente el coste de la investigación.

Persiguiendo el mismo fin que la autorregulación competitiva, el control de calidad, está la realización de ensayos de aptitud por el propio laboratorio o contratar a una organización externa para que los haga. Como inconvenientes, estas pruebas son más fáciles que los casos reales, las evidencias de los ensayos son de mayor calidad y no son ciegas, es decir, los examinadores suelen saber que se trata de una prueba de aptitud, por lo que se desconoce la validez de esta estrategia para reducir sesgos (Kukucka y Dror, 2023).

6.2.3 Recuperar la escena del crimen como tarea científica

En Roux *et al.*, 2015, los estudios han demostrado que los mejores examinadores de la escena de un crimen tenían un título universitario, en su mayoría de ciencias.

La retirada de los científicos forenses al laboratorio supone una de las causas actuales de la crisis de la ciencia forense, más incluso que las debilidades técnicas del laboratorio. Involucrar al laboratorio en la gestión de la escena del crimen supone que las decisiones más importantes que se tomen allí sobre los rastros de los delincuentes, su relevancia, calidad y cantidad a recoger, por ejemplo, tengan una base científica y no una decisión discrecional de un examinador policial que puede considerar la tarea como un trabajo mecánico y simple (Roux *et al.*, 2015).

El segundo principio de la Declaración de Sydney también propone que el investigador de la escena del crimen sea un científico forense generalista con conocimientos integrales de ciencia forense, rastros, investigaciones, comportamiento criminal y de las leyes naturales, para aplicarlos en la recuperación de huellas de la escena y en su reconstrucción (Roux *et al.*, 2022).

6.2.4 Implantar la figura de asesor forense, coordinador, administrador o gestor de casos

Presenta muchos desafíos de capacitación, consideraciones financieras, jurídicas y/o políticas. Se trata de un experto con conocimientos en ciencia forense, investigación en la escena del crimen, rastros y aspectos jurídicos, entre otras habilidades. En muchas ocasiones, algunos rastros no son recogidos y/o los recogidos pueden no resultar adecuados para la prueba, una situación que es catalogada como grieta de laboratorio, cuando este nunca tuvo nada que ver en la escena del crimen. La policía o los fiscales toman decisiones fuera de laboratorio sobre las evidencias (su recogida, su análisis, cuál presentar para la prueba, cómo presentarla...) con cierto interés por el resultado, favoreciendo la contaminación cognitiva. El asesor forense podría trabajar en la escena del crimen aportando sus conocimientos para que una evidencia no sea pasada por alto. Aseguraría la información contextual hasta que el experto científico la necesitara y lo alejaría de la irrelevante. Una figura de colaboración para facilitar la comunicación entre policía, científicos y juristas, para consultas sobre ciencias forenses en general o preguntas específicas del caso.

En países como Alemania, Suecia o Bélgica, en los que existe asesor forense, sus tareas se concentran en clasificar rastros, sugerir análisis de trazas o la secuencia analítica a seguir, explicar e interpretar los resultados, supervisar el intercambio de información, asistencia para la comprensión de los resultados o realizar exámenes de contratación cuando los conocimientos o la técnica a emplear en el laboratorio no esté disponible internamente. En casos de condenas erróneas o sin resolver, puede hacer evaluaciones para respaldar o no las decisiones que se han tomado. Tiene funciones definidas, responsabilidad y autoridad para tomar decisiones concretas y con conocimientos sobre sesgos cognitivos y estrategias para mitigarlos (Wells *et al.*, 2013; Bitzer *et al.*, 2022; Dror, 2013).

6.2.5 Formación sobre procedimientos forenses para jueces y fiscales

En la comunidad judicial, la experiencia de un experto forense es considerada un indicador de credibilidad y precisión sobre sus resultados, por lo que la utilizan para atribuir mayor validez a los testimonios de dichos expertos. Lo cierto es que la correlación entre confianza y precisión es baja. Es crucial que los miembros del jurado, jueces y fiscales reciban información sobre la confiabilidad de los procedimientos de la ciencia forense, para evaluar la evidencia de manera más adecuada y no basándose en la experiencia del experto (Edmond *et al.*, 2016; Kassin *et al.*, 2013).

6.2.6 Medios y vocabulario para incorporar la pericia forense en los juzgados

Existen malentendidos entre las expresiones que utilizan los expertos, que intentan transmitir el resultado de una prueba, y el personal judicial, no experto en ciencias forenses, que lo tiene que interpretar para tomar una decisión. Estos resultados son en su mayoría inciertos, por lo que se expresan mediante términos probabilísticos, "certeza científica razonable", "consistente", "coincidencia"..., que no garantizan una interpretación coherente o fiel a la realidad. Es fundamental desarrollar un vocabulario compartido entre los expertos y los legos (Edmond *et al.*, 2016).

La introducción de documentos estandarizados, cuartillas o guías básicas que representen la esencia de la ciencia que se ha aplicado en la investigación, en un formato accesible para los legos, les ayudaría a comprender lo que los científicos pretenden transmitir y les daría mayor confianza a sus decisiones (O'Brien *et al.*, 2015).

El quinto principio de la Declaración de Sydney propone un compromiso por parte de la ciencia forense para comunicarse, de forma que juez, investigador, analista o policía puedan comprender el valor de sus hallazgos (Roux *et al.*, 2022).

6.2.7 Controlar el estrés

La creación de entornos de trabajo donde se aborden los impactos negativos del estrés al que están sometidos los profesionales, así como fomentar la retroalimentación positiva, para anular la presión sobre los expertos para que tomen las decisiones esperadas (Almazrouei *et al.*, 2020).

El estrés y la fatiga pueden afectar a las decisiones. Desarrollar tareas complejas en áreas tranquilas y establecer horarios concretos de trabajo a puerta cerrada ayuda a controlarlos (Kunkler y Roy, 2023).

6.2.8 Protocolos estandarizados

La mayoría de las organizaciones no cuentan con un método de investigación específico, por lo que utilizan diferentes enfoques sin criterio científico, lo que dificulta reducir el sesgo cognitivo. Estandarizar estos métodos promovería la coherencia y la sensatez de los investigadores, en su credibilidad y aportaría fiabilidad a las decisiones ante un juicio. La investigación empírica sobre los protocolos a implantar permitiría descubrir las implicaciones de cada una de las estrategias a aplicar para reducir los sesgos (MacLean, 2022).

Earwaker *et al.*, (2020) proponen un enfoque estructurado en seis fases para mejorar la toma de decisiones en la ciencia forense, aportando transparencia y validez a la interpretación de una evidencia. En cada fase, se examinan y documentan

todas las decisiones que se han tomado, desde la escena del crimen hasta el tribunal; sus interdependencias; la aplicación del conocimiento empírico de otros dominios; la comunicación adecuada de los resultados; la gestión del riesgo y la incorporación de la toma de decisiones al proceso forense.

6.3 Estrategias aplicadas al procedimiento

Para que el trabajo forense sea lo más objetivo e imparcial posible, es fundamental que los expertos puedan tomar decisiones basadas en pruebas que no estén contaminadas por los sesgos. Para conseguirlo, puede resultar eficaz establecer medidas de control de calidad durante el examen de las pruebas para detectar errores humanos provocados por el sesgo.

6.3.1 Procedimientos ciegos

La información más fácil de evitar es la información contextual irrelevante sobre la escena del crimen; existencia de sospechoso, sus antecedentes, confesión previa, testigos... Solo necesitan información que pueda afectar a su trabajo forense, facilitada con cautela, libre de sesgos y en el momento apropiado. Una vez que el conocimiento de cierta información (irrelevante) da coherencia a una situación es muy difícil, si no imposible, bloquear ese contexto y plantear hipótesis alternativas (MacLean y Dror, 2016).

En los trabajos forenses de comparación, el uso de procedimientos ciegos es uno de los más eficaces. El trabajo debería ser "lineal", es decir, empezar desde el rastro obtenido en la escena del crimen hasta el sospechoso. Se trata de evitar que el examinador evalúe las muestras del sospechoso antes de procesar las de la escena. En algunos casos, se recomienda permitir un nuevo análisis, para características que no fueron concluyentes durante el primero, facilitando el trabajo de los examinadores (Kassin *et al.*, 2013).

En algunas circunstancias, los expertos necesitan información contextual para interpretar mejor una evidencia y explicar las propiedades que presenta. Por ejemplo, conocer que una prenda

de vestir se encontró en el desierto meses después de un homicidio, explicaría el hecho de que las fibras estuvieran descoloridas. Es importante que esta información sea proporcionada en una etapa apropiada de la investigación, para disminuir la posibilidad de contaminación cognitiva (Kunkler y Roy, 2023).

Esto va en consonancia con el séptimo principio de la Declaración de Sydney, que establece que los hallazgos en las ciencias forenses adquieren significado en contexto. Es fundamental que los expertos entiendan la diferencia entre las dos fuentes de información, la contextual o la irrelevante, para alejarse de esta última (Roux *et al.*, 2022).

Como mecanismo de protección a la información irrelevante, el gestor de casos podría ser el encargado de proporcionarla, o aplicar métodos como o LSU-E, desenmascaramiento secuencial lineal (LSU en adelante) y desenmascaramiento secuencial lineal ampliado (LSU-E en adelante). Estas técnicas ayudan a determinar qué es información contextual, cuál es la información irrelevante y detectar el momento idóneo en el que debe ser transmitida (Vredeveldt *et al.*, 2022).

LSU trata de regular el orden y la cantidad de información ofrecida al experto, desde el examen y la documentación de la escena del crimen, que es más sensible al sesgo por ser de baja calidad o que aporta poca información, yantes de compararla con las muestras obtenidas del sospechoso, que son de mejor calidad y mayor carga de información. LSU solo se usa para comparación de rastros (ADN o huellas dactilares) (Dror y Kukucka, 2021).

LSU-E reduce el sesgo, el ruido, ayuda a tomar mejores decisiones y, además, se puede aplicar a otros dominios que no implican comparación de evidencias. Aquí no se priva a los expertos de información, se les proporciona en la secuencia óptima. A los investigadores de la escena del crimen en Estados Unidos (CSI), por ejemplo, antes de que lleguen a la escena del crimen, se les suministra información (supuesta forma de la muerte, relato de un testigo...), por lo que el CSI desarrolla expectativas que sesgan la recogida de muestras y la interpretación de la escena (Lidén y Almazrouei, 2023). Aplicando LSU-E, esta información contextual se aportaría cuando el CSI ya ha visto la escena del crimen y se

ha formado sus primeras impresiones y siempre antes del análisis de las pruebas en el laboratorio.

Para reducir las influencias cognitivas como sesgo de anclaje, atención selectiva o sesgo de confirmación, entre otros, la LSU-E establece tres criterios que interactúan entre sí para identificar qué información se facilita y en qué momento:

- **Poder de sesgo:** facilitar primero la información relevante con menor posibilidad de sesgo (la huella dactilar recogida en la escena del crimen antes que la del sospechoso).

- **Objetividad:** primero la información objetiva a la menos objetiva (una grabación de vídeo antes que una declaración de un testigo ocular).

- **Relevancia:** se antepondrá la información más relevante a cualquier otra (un medicamento hallado junto a un cadáver puede priorizar qué pruebas toxicológicas realizar antes que valorar un historial médico).

El proceso deberá ser documentado, el gestor de casos podría ser el responsable. Es fundamental anotar toda la información contextual que se recibe, si la consideran relevante para su tarea o no, por qué y cómo puede influir en sus análisis. Por ejemplo, en el procesamiento de una bebida presuntamente adulterada, se recibe la muestra etiquetada con información de que ha sido recuperada de una taza de café de la víctima y sus datos personales. Al documentarlo, el analista debería indicar que, al recibirla, contenía información irrelevante sobre los datos de la víctima e información relevante sobre el origen de la bebida. Saber que la sustancia es café facilita conocer qué ingredientes se esperan encontrar en la muestra y discriminarlos de los que se descubran y puedan ser considerados adulterantes. En caso de necesitar más información para completar el análisis y no disponer de gestor de casos, tendrían que solicitarla, anotando previamente las hipótesis y las opiniones hasta el momento y motivar la necesidad de más información (Kunkler y Roy, 2023).

El problema de esta técnica es que, a veces, es muy difícil determinar qué información es realmente relevante, no hay

establecidos unos criterios que definan lo que los expertos deben saber para desarrollar su tarea. Los diferentes dominios forenses deberían estandarizar estas cuestiones antes de que se implementen los procedimientos de gestión (Gardner *et al.*, 2019). Qué momento es el idóneo para revelarla y el alto coste de recursos son más inconvenientes de esta estrategia (Reese, 2011).

6.3.2 Verificaciones ciegas, revisión por pares y abogado del diablo

Las verificaciones ciegas son propuestas fundamentales para bloquear los efectos de la información contextual. En estas verificaciones, un segundo examinador revisa el trabajo del primero, sin conocer el resultado que obtuvo ni la conclusión a la que llegó. Para obtener mejores resultados con esta estrategia, se recomienda el uso de un doble ciego, en donde no se conoce ni el resultado ni el examinador que lo realizó, que el examinador inicial no escoja al verificador e, incluso, que la verificación se lleve a cabo por laboratorios independientes (Kassin *et al.*, 2013).

Algunos autores incluyen estas verificaciones en una técnica más completa para dactiloscopia, denominada retroalimentación o *feedback* cognitivo. Después de que el examinador de la huella decida si el resultado de su análisis es de identificación del autor, de exclusión o no concluyente, establece una estimación de confianza sobre el hecho de que su resultado sea correcto. Si un verificador descubre un error, le informará sobre dicho error al primer examinador y le recordará la estimación de probabilidad que había determinado inicialmente junto con información cognitiva que corrija dicho error. Esta técnica se puede aplicar también como ejercicio de entrenamiento impartido de forma intermitente al margen del trabajo habitual (Dror *et al.*, 2011). La retroalimentación precisa y oportuna facilita el perfeccionamiento o la adquisición de nuevas habilidades (Edmond *et al.*, 2016).

En la revisión por pares se le pide a un colega experto, ajeno a la corporación, que examine el trabajo y compruebe si existe respaldo científico sobre las conclusiones propuestas. Para que esta estrategia sea eficaz, esta supervisión ha de estar libre de información irrelevante (Vredeveldt *et al.*, 2022).

La técnica de abogado del diablo consiste en contratar a un experto para cuestionar la decisión, a través de un procedimiento definido y formalizado. Su objetivo es exponer todos los prejuicios que han podido influir en la decisión para tratar de mitigarlos. Este proceso podría sustituir la verificación ciega. El abogado del diablo conocería toda la información, tendría que identificar aspectos con los que no esté de acuerdo (o simule no estarlo, pero considere que pueden haber influido sesgos) y compartirlos con el examinador inicial, ayudándole a detectar cualquier deficiencia o presencia de sesgo durante el proceso. Como inconveniente, se necesita más investigación empírica que confirme cuál es más eficaz, el abogado del diablo o la verificación ciega (Reese, 2011).

6.3.3 Alineación de pruebas

Aunque se necesitan más estudios sobre su eficacia y sobre cómo elaborar las muestras que servirían de relleno, la alineación de pruebas (Koen y Kukucka, 2018), o método de control de relleno (Wells *et al*., 2013), puede reducir el sesgo de confirmación. Como en una rueda de reconocimiento, se presentaría al experto la huella de la escena del crimen y muestras de aspecto parecido para determinar cuál se le parece, si es que se parece alguna. El hecho de presentarle solo una que se le parezca puede hacer que el examinador infiera que ya existen indicios suficientes de culpabilidad sobre el sospechoso, por lo que aumenta la expectativa de que ambas pertenezcan a la misma persona. Se pueden usar los sistemas automáticos de identificación dactilar AFIS, anteriormente comentados,como fuente de pruebas de relleno, siempre escogidas por un examinador independiente (o un gestor de casos) de entre las que mayor parecido tengan a la del sospechoso.

Aún es necesario llevar a cabo más investigación sobre esta estrategia para conocer su eficacia y viabilidad en las distintas disciplinas forenses (Kukucka y Dror, 2023).

6.3.4 Compartimentar el flujo de trabajo

Esta estrategia trata de asegurarse de que el experto que examina la prueba no sea el mismo que la ha recogido de la escena

del crimen, evitando que el sesgo se contagie en cascada de una etapa a otra (Kukucka y Dror, 2023).

6.3.5 Simplificar la tarea y asignar más tiempo

La heurística es un proceso que permite tomar decisiones en situaciones complejas y en poco tiempo. El sesgo es el resultado de ese proceso cuando ha ocurrido un error de juicio debido a una situación ambigua o confusa. De esta definición, extraemos dos factores importantes, situación compleja y poco tiempo para dos cuestiones, simplificar la tarea y asignar más tiempo a la decisión.

En primer lugar, simplificar la tarea. Si los sesgos son el resultado de la heurística que permite emitir juicios precisos en situaciones complejas, es probable que reducir esa complejidad de las situaciones reduzca los sesgos.

En dactiloscopia, las huellas más difíciles de analizar serían procesadas de forma distinta, por ejemplo, permitiendo al examinador decidir que pueden seguir siendo pruebas de investigación o excluirlas del procedimiento. Es una técnica que aún requiere investigación empírica y que podría ser rechazada por examinadores de huellas y por fiscales. Los primeros tendrían que admitir que no son capaces de hacer una comparación precisa y los segundos tendrían que permitir limitaciones en la admisibilidad de pruebas en el tribunal (Reese, 2011).

En segundo lugar, asignar más tiempo a la decisión. Si los sesgos son el resultado de la heurística que permite emitir juicios precisos en poco tiempo, aumentar el tiempo disponible para tomar una decisión podría reducir el sesgo. Podría conseguirse con la contratación de más expertos (Reese, 2011) o desacelerar y tomarse más tiempo para pensar (Vredeveldt et al., 2022).

Volviendo al peligro de sesgo de la lista de posibles coincidencias dactiloscópicas de los sistemas automáticos AFIS, los examinadores concluyen que, cuanto menos tiempo se dedica a comparar las huellas, más probable es que se pase por alto una identificación buena (Dror *et al.*, 2011). Si se suman ambos factores, poco tiempo y el problema anteriormente comentado

de lo peligroso de que AFIS muestre el resultado de huellas más coincidentes al principio de la lista, pudiendo estar la buena al final, puede suponer que el sesgo sea mayor. Para evitarlo, es recomendable proporcionar una lista con una longitud de resultados específica y un orden aleatorio en el grado de coincidencia (Kassin *et al.*, 2013).

6.3.6 Reuniones para discusión de casos peculiares

La mayoría de los casos penales que no fueron investigados correctamente tuvieron deficiencias en la primera etapa de la investigación, sobre todo en la escena del crimen. Las etapas posteriores pueden revisarse y repetirse, pero lo que no se recoja de la escena se perderá para siempre.

Los investigadores deberían reunirse regularmente para compartir cierto tipo de casos, cómo fueron abordados y resueltos, cuáles fueron sus desafíos y cómo los superaron. Un intercambio de conocimientos y experiencia puede favorecer una mejora en el rendimiento de los investigadores en la escena del crimen (Ditrich, 2015). Una cultura organizacional de apoyo y desbaste, donde se favorezca el desarrollo del trabajo minucioso, evitando la presión del tiempo y el deseo por cerrar el caso (MacLean, 2022).

6.3.7 Reconocimiento de errores y junta de análisis

Al margen de aspectos legales, disciplinarios o el daño a la imagen pública de la profesión, la estructura jerárquica, la uniformidad y la presión del grupo en las organizaciones policiales no promueven la admisión de errores. Por lo tanto, cuando suceden, no hay posibilidad de análisis para correcciones futuras y mejora de la investigación. Sería interesante fomentar ambientes en los que los errores se vean como una oportunidad de mejora, incluso con todas las implicaciones personales que conlleva.

La contratación de una consultaría de gestión o asesores podría ser útil para aplicar esta medida. Establecer una comisión alejada de la jerarquía del lugar donde ocurrió el error, alejados de la presión de compañeros y superiores, que se ajuste a unos patrones institucionalizados para evitar la ceguera rutinaria. Aparte de revisar los casos importantes, los errores de los casos

rutinarios podrían ayudar a identificar “puntos críticos” donde se acumulen muchos errores y poder aplicar medidas correctoras. Establecer una junta de análisis de errores para examinar grietas en las investigaciones (Ditrich, 2015).

6.4 Estrategias aplicadas al experto

Enfocadas en intervenir sobre el procesamiento cognitivo humano, evitando el pensamiento automático y heurístico para conseguir un pensamiento consciente y controlado.

6.4.1 Formación sobre los sesgos cognitivos

La formación permite concienciar a los expertos de que nadie es inmune al sesgo y que no se puede bloquear con simple fuerza de voluntad (Dror, 2013). Reconocer que los sesgos pueden influir en todas las actividades humanas ayuda a combatir el “punto ciego”,las “manzanas podridas”, la “inmunidad del experto”, la "ilusión de control” y que no se trata de “cuestiones éticas”. Es fundamental la formación desde fases tempranas en población estudiantil para que los futuros expertos puedan ser capaces de aplicar contramedidas (Dror *et al.*, 2018).

El uso de esta técnica por sí sola no minimiza los riesgos de “contaminación” en las ciencias forenses, pero resulta una buena base para la tarea. En la actualidad, la formación y la capacitación de profesionales forenses sobre los sesgos cognitivos y su impacto no está definida, apenas cuentan con información que les enseñe cómo minimizarlos.

En ocasiones las técnicas que se “heredan” de unos expertos a otros facilitan el contagio del sesgo, por ejemplo, enseñar a un principiante a buscar primero en la huella del sospechoso los detalles que tendrá que encontrar en el rastro de la escena del crimen, lo que reduce el tiempo de comparación de huellas para terminar rápido el trabajo (Kunkler y Roy, 2023).

Pero incluso la formación, la capacitación y la actualización, como base fundamental para mitigar los sesgos, tienen inconvenientes; ciertos expertos pueden llegar a pensar que ya están

capacitados para hacerles frente y que no necesitan ninguna otra técnica de corrección para reducir su efecto, potenciando el punto ciego del sesgo(Dror *et al.*, 2011).

6.4.2 Entrenamiento para mitigar sesgos cognitivos

Se han creado juegos serios, por ejemplo, MACBETH (Mitigating Analyst Cognitive Bias by Eliminating Task Heuristics), diseñado para entrenar a los jugadores a identificar y comprender los sesgos cognitivos presentes en sus decisiones, durante el análisis de inteligencia de las fases del juego. Los tres sesgos que se abordan durante el juego son el sesgo de confirmación, el punto ciego del sesgo y el error de atribución fundamental (Dunbar *et al.*, 2014).

Más tarde, en 2015, se llevó a cabo un experimento en el que compararon "MACBETH" con una película educativa sobre sesgos. La misión del juego es detener un ataque terrorista inminente e identificar al sospechoso. A 703 participantes se les asignó aleatoriamente una de 10 condiciones experimentales. Debían cooperar con dos personajes del propio juego para conseguir datos sobre el sospechoso, averiguar el lugar previsto para el incidente y el arma que se usará. Durante el desarrollo del juego, obtenían información, generaban hipótesis, las refutaban y al final de cada turno recibían retroalimentación según la situación experimental asignada al principio. Esto les hacía reformular su hipótesis o buscar alternativas. A través del juego, algunos jugadores recibieron instrucciones sobre los sesgos (entre ellos el de confirmación) de forma explícita, otros de forma implícita y otro grupo ninguna. Como resultado del experimento, fue demostrar cómo el aprendizaje en sesgos cognitivos basado en juegos era más eficaz que la enseñanza tradicional. El concepto de juego, además de ser más atractivo, tiene una noción de automotivación, permite asimilar información a través de experiencia y cierto compromiso,atributos que no da un vídeo explicativo de sesgos cognitivos (Dunbar *et al.*, 2014).

De los tres sesgos fundamentales tratados en esta investigación, sesgo de confirmación, error de atribución y punto ciego del sesgo, este último continúa siendo un desafío difícil para entrenar incluso con esta técnica, por los efectos de la

capacitación. La formación aumenta los mitos de inmunidad del experto y el mito de ilusión de control (Bessarabova *et al.*, 2016).

6.4.3 Escenario alternativo

El experto debe formular al menos dos escenarios alternativos para evaluar la evidencia. Los escenarios permiten mantener una visión general de todas las hipótesis o pruebas, conectar información que se conoce y darle sentido. Se trata de comparar el escenario que propone culpabilidad con escenarios que propongan inocencia y evaluar si son coherentes con la evidencia encontrada, si pueden explicar los hechos o si existen pruebas que anulen el escenario propuesto... En definitiva, razonar por qué deberíamos creer en un escenario y no en otro. Esta técnica puede predecir incluso el descubrimiento de nuevas pruebas que son coherentes con el escenario propuesto (van Koppen y Mackor, 2019).

Considerar lo opuesto es una estrategia semejante al escenario alternativo, los expertos deben preguntarse por qué su teoría inicial sobre los hechos puede ser incorrecta, lo que les obliga a considerar posibles alternativas (Vredeveldt *et al.*, 2022). En una investigación, se demostró que esta medida podía funcionar en investigaciones criminales (O'Brien, 2009).

En dactiloscopia, por ejemplo, sería un escenario alternativo perfecto que, al encontrar un punto característico en la comparación de dos huellas, plantearse la posibilidad de que este rastro no pertenezca a la propia huella y que pueda ser parte de una tercera huella o suciedad en la muestra (artefactos) (Reese, 2011).

Para obtener mejores resultados, es importante plantear un escenario alternativo para cada evidencia encontrada, por separado. Si, además, se toma nota con lápiz y papel al comparar ambos escenarios, se permite más tiempo para decidir la solidez de la evidencia en cada uno de los escenarios y reducir la posibilidad de sesgo (Rassin, 2018).

Esta estrategia también tiene limitaciones, puede ser difícil plantear varias hipótesis alternativas y no está establecido cuántas son suficientes para que el método funcione. Además, existe

el riesgo de que, si se plantean demasiadas, los expertos pueden pensar que han sido suficientemente minuciosos en la investigación y se decantarán por su hipótesis favorita, empeorando el efecto del sesgo (O'Brien, 2009).

6.4.4 Tomar otra perspectiva

Los estudios han demostrado el éxito de esta técnica para reducir los sesgos cognitivos en cualquier ámbito. Los responsables de tomar una decisión tienen que ponerse en el lugar de la otra parte. En el ámbito jurídico, por ejemplo, los fiscales tienen que ponerse en la piel de los abogados defensores. En el laboratorio, el analista de la huella presentada por la acusación debe plantearse que es la defensa quien le exige el análisis. Considerar el punto de vista de la otra parte ayuda a tomar decisiones más racionales (Reese, 2011).

6.4.5 Rendición de cuentas

En el proceso de la interpretación de información influyen la motivación, las creencias personales, la ideología, la tolerancia al riesgo, a la ambigüedad, etc., afectando a la toma de decisiones. En la rendición de cuentas, se obliga al experto a explicar las razones que le motivaron a tomar esa decisión cuando se le exija. Con esta estrategia, como mínimo, se reducirán los sesgos que podrían atribuirse a falta de esfuerzo. Sería conveniente que documentara todos sus argumentos, proporcionando así transparencia y tiempo para reflexionar (Kunkler y Roy, 2023).

Esta estrategia podría complementarse con la del abogado del diablo, a quien, una vez que identifique y exponga los errores que pudo haber cometido el examinador inicial, este tendría que argumentar cómo llegó hasta sus conclusiones.

Un procedimiento transparente en todas las fases del proceso penal es una de las mejores formas de reducir el sesgo de confirmación. Además, permite que la defensa pueda detectar hipótesis sesgadas como contramedida para reducir el sesgo. Las investigaciones han demostrado que los expertos tienden a mostrar menos sesgos cuando saben que sus acciones se someterán a la rendición de cuentas (Findley, 2011).

6.4.6 Orgullo profesional

Desarrollar un sentimiento de orgullo profesional serio serviría para evitar que el experto desarrolle percepciones negativas sobre sí mismo y la necesidad de ser un justiciero (Vredeveldt *et al.*, 2022).

7 Conclusiones

En las últimas décadas, se han sucedido un número alarmante de errores en la ciencia forense que han dado lugar a miles de exoneraciones por condenas injustas en todo el mundo. Son datos aún a día de hoy muy difíciles de precisar, dado que no existen registros oficiales que nos permitan saber el alcance real de estos errores. Una inmensa mayoría son consecuencia de la contaminación cognitiva durante el proceso penal. Una contaminación provocada por los sesgos cognitivos, inconscientes y fieles al ser humano.

Existe mucha bibliografía que describe y enumera estos sesgos, su origen, naturaleza, dominios en los que opera y cómo influyen en la ciencia forense y en los procesos judiciales. Estos estudios, además de identificarlos y clasificarlos, promueven técnicas de *debiasing*, estrategias para reducir los efectos de los sesgos cognitivos. Estas estrategias se adoptan desde diferentes enfoques para abarcar todas las fuentes desde donde puedan surgir los sesgos, por factores personales, procesos cognitivos, educación, expectativas... y, sobre todo, por la información contextual irrelevante a la que se exponen los expertos durante una investigación y su procesamiento judicial.

Cada organización tiene sus propios procedimientos, sus propias técnicas forenses que dan por buenos sus métodos adaptados a una tecnología sofisticada y que pueden no tener en cuenta otras variables que afectan a la muestra. La ciencia forense se distribuye en disciplinas independientes al resto, cuando debieran estar conectadas para resolver problemas y optimizar el trabajo en laboratorio. La ciencia forense tiene

muchas formas de expresar un mismo dato y ningún traductor universal que concrete el resultado. Se trata de integrar la ciencia forense, estructurarla de manera que todas las disciplinas dejen de trabajar aisladamente, reorganizar los laboratorios con departamentos compartidos y áreas de consulta y el uso de un lenguaje científico universal. En definitiva, facilitar la colaboración entre científicos forenses, psicólogos, juristas... que compartirían sus conocimientos para difundir protocolos estandarizados que aportarían confianza a la ciencia forense y al sistema judicial.

Las estrategias más fáciles e inmediatas de implantar para superar los sesgos cognitivos son aquellas que dependen de uno mismo, del propio experto, que debería desarrollar orgullo profesional y ser consciente de su vulnerabilidad a los sesgos, de entrenarse para mitigarlos, de proponer escenarios alternativos, de tomar otra perspectiva antes de tomar una decisión o estar preparado para rendir cuentas y argumentar y justificar el resultado que ha obtenido.

Pero confiar únicamente en el ser humano para superar los sesgos es un error, es necesario complementarlo con otras medidas y estrategias que respalden el desafío de minimizar su influencia; la autorregulación competitiva, recuperar la escena del crimen como tarea científica, implantar la figura de un asesor forense o gestor de casos son algunas propuestas para reducir el impacto de los sesgos cognitivos que se pueden implantar a nivel organizativo. La forma de llevar a cabo la tarea también puede suponer un intento de minimizar los efectos de los sesgos, aplicando procedimientos ciegos, revisión por pares, la alineación de pruebas o crear ambientes para discusión de casos complicados.

La Administración de Justicia no se puede concebir sin el auxilio de la ciencia forense, ni la ciencia forense sin el auxilio del factor humano, por lo que la ciencia cognitiva debería ser una subdisciplina más de la ciencia forense. Cada uno de los dominios forenses debería trabajar y colaborar con la ciencia cognitiva, investigar e implementar procedimientos estandarizados y estructurados que limiten la discrecionalidad y que transmitan con precisión lo que se consiga saber a partir de una evidencia encontrada en la escena de un crimen.

Es imprescindible más investigación empírica acerca de las estrategias descritas, establecer cuáles funcionan, cómo interactúan entre ellas y cuál es la mejor manera de implantarlas para limitar los efectos negativos del sesgo. Conseguirlo supone establecer cambios importantes de organización y normativos que implicarían una inversión de tiempo, esfuerzo y dinero considerables, pero necesarios para comprometer a todos los actores del proceso judicial y responsabilizarlos para que tomen mejores decisiones.

Dar consistencia a la ciencia forense es excesivamente caro, una inversión que absorbe muchos recursos, pero indiscutiblemente necesaria. El avance en técnicas y procedimientos que mejoren de manera continua el procedimiento de investigación procesal penal es necesario para una justicia avanzada que esté en consonancia con todos los avances científicos de la sociedad actual.

Referencias bibliográficas

Almazrouei, M. A., Dror, I. E. y Morgan, R. M. (2020). Organizational and Human Factors Affecting Forensic Decision Making: Workplace Stress and Feedback. *Journal of Forensic Sciences*, *65*(6), 1968-1977. https://doi.org/10.1111/1556-4029.14542

Bessarabova, E., Piercy, C. W., King, S., Vincent, C., Dunbar, N. E., Burgoon, J. K., Miller, C. H., Jensen, M., Elkins, A., Wilson, D. W., Wilson, S. N. y Lee, Y.-H. (2016). Mitigating bias blind spot via a serious video game. *Computers in Human Behavior*, *62*, 452-466. https://doi.org/10.1016/j.chb.2016.03.089

Bitzer, S., Miranda, M. D., y Bucht, R. E. (2022). Forensic advisors: The missing link. *WIREs Forensic Science, 4*(3), e1444. https://doi.org/10.1002/wfs2.1444

Ceberio Belaza, M. (2015, 9 de mayo). *"He pasado un infierno indescriptible, los peores 4.000 días de mi vida"*. *Falso Culpable*. Recuperado de https://falsoculpable.blogspot.com/search?q=van+der

Ceberio Belaza, M. (2016, 6 de marzo). *Fabricando un violador: El calvario de Romano van der Dussen, falso culpable*. *Falso Culpable*. Recuperado de https://falsoculpable.blogspot.com/2016/03/fabricando-un-violador-el-calvario-de.html

Chan Gamboa, E. C., Estrada Pineda, C. y Rodríguez Díaz, F. J. R. (2000). *Aportaciones a la psicología jurídica y forense desde Iberoamérica*. Editorial EL Manual Moderno.

Cuellar, M., Mauro, J. y Luby, A. (2022). A Probabilistic Formalisation of Contextual Bias: from Forensic Analysis to Systemic Bias in the Criminal Justice System. *Journal of the Royal Statistical Society Series A: Statistics in Society*, *185*(Supplement_2), S620-S643. https://doi.org/10.1111/rssa.12962

Curley, L. J., Munro, J., y Dror, I. E. (2022). Cognitive and human factors in legal layperson decision making: Sources of bias in juror decision making. *Medicine, Science and the Law, 62*(3), 206–215. https://doi.org/10.1177/00258024221080655

De la Rosa Rodríguez, P. I. y Sandoval Navarro, V. D. (2016). Los sesgos cognitivos y su influjo en la decisión judicial. Aportes de la Psicología Jurídica a los procesos penales de corte acusatorio. *Derecho Penal y Criminología*, *37*(102), 141. https://doi.org/10.18601/01210483.v37n102.08

Ditrich, H. (2015). Cognitive fallacies and criminal investigations. *Science & Justice, 55*(2), 155–159. https://doi.org/10.1016/j.scijus.2014.12.007

Dror, I. (2013). The ambition to be scientific: Human expert performance and objectivity. *Science & Justice*, *53*(2), 81-82. https://doi.org/10.1016/j.scijus.2013.03.002

Dror, I. E. (2015). Cognitive neuroscience in forensic science: understanding and utilizing the human element. *Philosophical Transactions of the Royal Society B: Biological Sciences*, *370*(1674), 20140255. https://doi.org/10.1098/rstb.2014.0255

Dror, I. E. (2020). Cognitive and Human Factors in Expert Decision Making: Six Fallacies and the Eight Sources of Bias. *Analytical Chemistry*, *92*(12), 7998-8004. https://doi.org/10.1021/acs.analchem.0c00704

Dror, I. E. (2023). The most consistent finding in forensic science is inconsistency. *Journal of Forensic Sciences*, *68*, issue 6, 1851-1855. https://doi.org/10.1111/1556-4029.15369

Dror, I. E., y Kukucka, J. (2021). Linear Sequential Unmasking–Expanded (LSU-E): A general approach for improving decision making as well as minimizing noise and bias. *Forensic Science International: Synergy, 3*, 100161. https://doi.org/10.1016/j.fsisyn.2021.100161

Dror, I. E., Kukucka, J., Kassin, S. M. y Zapf, P. A. (2018). *No one is immune to contextual bias-Not even forensic pathologists.* No one is immune to contextual bias—Not even forensic pathologists. By Dror, Itiel E.,Kukucka, Jeff,Kassin, Saul M.,Zapf, Patricia A. *Journal of Applied Research in Memory and Cognition*, Vol 7(2), Jun 2018, 316-317

Dror, I., Melinek, J., Arden, J. L., Kukucka, J., Hawkins, S., Carter, J., y Atherton, D. S. (2021). *Cognitive bias in forensic pathology decisions. Journal of Forensic Sciences, 66*(5), 1751–1757. https://doi.org/10.1111/1556-4029.14697

Dror, I. E. y Pierce, M. L. (2019). ISO Standards Addressing Issues of Bias and Impartiality in Forensic Work. *Journal of Forensic Sciences*, *65*(3), 800-808. https://doi.org/10.1111/1556-4029.14265

Dror, I. E., Wertheim, K., Fraser-Mackenzie, P. y Walajtys, J. (2011). The Impact of Human–Technology Cooperation and Distributed Cognition in Forensic Science: Biasing Effects of AFIS Contextual Information on Human Experts. *Journal of Forensic Sciences*, *57*(2), 343-352. https://doi.org/10.1111/j.1556-4029.2011.02013.x

Dunbar, N. E., Miller, C. H., Adame, B. J., Elizondo, J., Wilson, S. N., Lane, B. L., Kauffman, A. A., Bessarabova, E., Jensen, M. L., Straub, S. K., Lee, Y.-H., Burgoon, J. K., Valacich, J. J., Jenkins, J. y Zhang, J. (2014). Implicit and explicit training in the mitigation of cognitive bias through

the use of a serious game. *Computers in Human Behavior*, *37*, 307-318. https://doi.org/10.1016/j.chb.2014.04.053

Earwaker, H., Nakhaeizadeh, S., Smit, N. M. y Morgan, R. M. (2020). A cultural change to enable improved decision-making in forensic science: A six phased approach. *Science & Justice*, *60*(1), 9-19. https://doi.org/10.1016/j.scijus.2019.08.006

Edmond, G., Tangen, J. M., Searston, R. A. y Dror, I. E. (2014). Contextual bias and cross-contamination in the forensic sciences: the corrosive implications for investigations, plea bargains, trials and appeals. *Law, Probability and Risk*, *14*(1), 1-25. https://doi.org/10.1093/lpr/mgu018

Edmond, G., Towler, A., Growns, B., Ribeiro, G., Found, B., White, D., Ballantyne, K., Searston, R. A., Thompson, M. B., Tangen, J. M., Kemp, R. I. y Martire, K. (2016). Thinking forensics: Cognitive science for forensic practitioners. *Science & Justice*, *57*(2), 144-154. https://doi.org/10.1016/j.scijus.2016.11.005

Findley, K. A. (2011). Tunnel vision. En *Conviction of the innocent: Lessons from psychological research* (pp. 303-323). American Psychological Association. https://doi.org/10.1037/13085-014

Gardner, B. O., Kelley, S., Murrie, D. C., y Dror, I. E. (2019). What do forensic analysts consider relevant to their decision making? *Science & Justice, 59*(5), 516–523. https://doi.org/10.1016/j.scijus.2019.04.005

Geven, L., Schneider, T. y Schell-Leugers, J. (s.f.). *Ahmed Tommouhi*. EUREX. Recuperado de https://www.registryofexonerations.eu/case_details/ahmed-tommouhi-1-sexual-offense-1994/

Giovanelli, A. (2023). The forensic's scientist craft: toward an integrative theory. Part 2: meso- and macroapproach. *Australian Journal of Forensic Sciences*, 1-16. https://doi.org/10.1080/00450618.2023.2283418

Güidi Clas, E. M. (2003). *El perfil criminológico del juez prevaricador*. J.M. Bosch Editor.

Guthrie, C., Rachlinski, J. J., y Wistrich, A. J. (2007). Blinking on the bench: How judges decide cases. *Cornall Law Review, 93*(1), 1-43.

Kassin, S. M., Dror, I. E. y Kukucka, J. (2013). The forensic confirmation bias: Problems, perspectives, and proposed solutions. *Journal of Applied Research in Memory and Cognition*, *2*(1), 42-52. https://doi.org/10.1016/j.jarmac.2013.01.001

Koen, W. J. y Kukucka, J. (2018). Confirmation bias in forensic science. En *The Psychology and Sociology of Wrongful Convictions: Forensic Science Reform* (pp. 215–245). Elsevier. https://doi.org/10.1016/B978-0-12-802655-7.00007-1

Kukucka, J. and Dror I. E. (2023). Human Factors in Forensic Science: Psychological Causes of Bias and Error. In David DeMatteo, and Kyle C. Scherr (eds), *The Oxford Handbook of Psychology and Law* (2023; online edn, Oxford Academic, 23 Feb. 2023), https://doi.org/10.1093/oxfordhb/9780197649138.013.36, accessed 24 Jan. 2025.

Kukucka, J., Kassin, S. M., Zapf, P. A. y Dror, I. E. (2017). Cognitive Bias and Blindness: A Global Survey of Forensic Science Examiners. *Journal of Applied Research in Memory and Cognition*, *6*(4), 452-459. https://doi.org/10.1016/j.jarmac.2017.09.001

Kunkler, K. S. y Roy, T. (2023). Reducing the impact of cognitive bias in decision making: Practical actions for forensic science practitioners. *Forensic Science International Synergy*, *7*, 100341. https://doi.org/10.1016/j.fsisyn.2023.100341

Lidén, M. y Almazrouei, M. A. (2023). "Blood, Bucks and Bias": Reliability and biasability of crime scene investigators' selection and prioritization of blood traces. *Science & Justice*, *63*(2), 276-293. https://doi.org/10.1016/j.scijus.2023.01.005

MacLean, C. L. (2022). Cognitive bias in workplace investigation: Problems, perspectives and proposed solutions. *Applied Ergonomics*, *105*, 103860. https://doi.org/10.1016/j.apergo.2022.103860

MacLean, C. L., y Dror, I. E. (2016). A Primer on the Psychology of Cognitive Bias. In *Blinding as a Solution to Bias: Strengthening Biome-*

dical Science, Forensic Science, and Law (pp. 13–24). Elsevier. https://doi.org/10.1016/B978-0-12-802460-7.00001-2

Manzanero, A. L. (2020). *Incidencia de las falsas identificaciones*. *Falso Culpable*. Recuperado de https://falsoculpable.blogspot.com/p/incidencia-de-las-falsas.html

Meterko, V. y Cooper, G. (2021). Cognitive Biases in Criminal Case Evaluation: A Review of the Research. *Journal of Police and Criminal Psychology*, *37*(1), 101-122. https://doi.org/10.1007/s11896-020-09425-8

Murrie, D. C., Boccaccini, M. T., Turner, D. B., Meeks, M., Woods, C. y Tussey, C. (2009). Rater (dis)agreement on risk assessment measures in sexually violent predator proceedings: Evidence of adversarial allegiance in forensic evaluation? *Psychology, Public Policy, and Law*, *15*(1), 19-53. https://doi.org/10.1037/a0014897

O'Brien, B. (2009). Prime Suspect: an Examination of Factors that Aggravate and Counteract Confirmation Bias in Criminal Investigations. *Psychology, Public Policy, and Law*, *15*(4), 315-334. https://doi.org/10.1037/a0017881

O'Brien, É., Nic Daeid, N., y Black, S. (2015). Science in the court: pitfalls, challenges and solutions. *Philosophical Transactions of the Royal Society B: Biological Sciences, 370*(1674), 20150062. https://doi.org/10.1098/rstb.2015.0062

Páez, A. (2021). Los sesgos cognitivos y la legitimidad racional de las decisiones judiciales (Cognitive Bias and the Rational Legitimacy of Judicial Decisions). *Razonamiento Jurídico y Ciencias Cognitivas*, 187-222. https://ssrn.com/abstract=3956986

Pronin, E., Lin, D. Y., y Ross, L. (2002). The Bias Blind Spot: Perceptions of Bias in Self Versus Others. *Personality and Social Psychology Bulletin, 28*(3), 369–381. https://doi.org/10.1177/0146167202286008

Rachlinski, J. J. y Wistrich, A. J. (2017). Judging the Judiciary by the Numbers: Empirical Research on Judges. *Annual Review of Law and Social Science*, *13*, 203-229. https://doi.org/10.1146/annurev-lawsocsci-110615-085032

Rassin, E. (2018). Reducing tunnel vision with a pen-and-paper tool for the weighting of criminal evidence. *Journal of Investigative Psychology and Offender Profiling, 15*(2), 227-233.

Reese, E. J. (2011). Techniques for mitigating cognitive biases in fingerprint identification. *UCLa L. Rev.*, *59*, 1252.

Roux, C., Bucht, R., Crispino, F., De Forest, P., Lennard, C., Margot, P., Miranda, M. D., NicDaeid, N., Ribaux, O., Ross, A. y Willis, S. (2022). The Sydney declaration – Revisiting the essence of forensic science through its fundamental principles. Forensic Science International, *332*, 111182. https://doi.org/10.1016/j.forsciint.2022.111182

Roux, C., Talbot-Wright, B., Robertson, J., Crispino, F., y Ribaux, O. (2015). The end of the (forensic science) world as we know it? The example of trace evidence. *Philosophical Transactions of the Royal Society B: Biological Sciences, 370*(1674), 20140260. https://doi.org/10.1098/rstb.2014.0260

Roux, C., Willis, S. y Weyermann, C. (2021). Shifting forensic science focus from means to purpose: A path forward for the discipline? *Science & Justice*, *61*(6), 678-686. https://doi.org/10.1016/j.scijus.2021.08.005

Saks, M. J. (2010). Forensic identification: From a faith-based "Science" to a scientific science. *Forensic Science International, 201*(1), 14–17. https://doi.org/10.1016/j.forsciint.2010.03.014

Stacey, R. B. (2005). *Report on the Erroneous Fingerprint Individualization in the Madrid Train Bombing Case*, vol. 35, issue 1. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/jan2005/special_report/2005_special_report.htm

Steblay, N., Hosch, H. M., Culhane, S. E., y McWethy, A. (2006). The impact on juror verdicts of judicial instruction to disregard inadmissible evidence: A meta-analysis. *Law and Human Behavior, 30*(4), 469–492. https://doi.org/10.1007/s10979-006-9039-7

Tversky, A. y Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, *185*(4157), 1124-1131. https://doi.org/10.1126/science.185.4157.1124

UCI Newkirk Center for Science and Society. (2024). The National Registry of Exonerations. Consultado el 12 de diciembre de 2024, en https://www.law.umich.edu/special/exoneration/Pages/about.aspx

Van Koppen, P. J. y Mackor, A. R. (2019). A Scenario Approach to the Simonshaven Case. *TopicsinCognitive Science*, *12*(4), 1132-1151. https://doi.org/10.1111/tops.12429

Vredeveldt, A., van Rosmalen, E. A. J., van Koppen, P. J., Dror, I. E., y Otgaar, H. (2022). Legal psychologists as experts: guidelines for minimizing bias. *Psychology, Crime & Law*, *30*(7), 705-729. https://doi.org/10.1080/1068316X.2022.2114476

Wells, G. L., Wilford, M. M., y Smalarz, L. (2013). Forensic science testing: The forensic filler-control method for controlling contextual bias, estimating error rates, and calibrating analysts' reports. *Journal of Applied Research in Memory and Cognition*, *2*(1), 53–55. https://doi.org/10.1016/j.jarmac.2013.01.004

La inteligencia artificial predictiva al servicio de la prevención e investigación del delito y del proceso penal

Predictive Artificial Intelligence in the Service of Crime Prevention, Investigation, and Criminal Proceedings

María Luisa García Torres[1]
Universidad Alfonso X el Sabio, España.
mgarctor@uax.es | https://orcid.org/0000-002-7638-9791

DOI: https://doi.org/10.14201/cp.32177
Recibido: 24-11-2024 | Aceptado: 16-12-2024

Resumen

El uso de la inteligencia artificial –en adelante, IA– predictiva ha transformado profundamente la labor de las Fuerzas y Cuerpos de Seguridad del Estado, así como la de los órganos jurisdiccionales.

En el caso de la Policía, se ha producido un cambio significativo en la organización de las estrategias de prevención e investigación del delito, sustituyendo su instinto natural y tradicional investigativo por cálculos matemáticos realizados por IA. Estamos ante la llamada vigilancia y la investigación predictiva. Por su parte, los jueces, en la actualidad, también se auxilian de algoritmos en la toma de decisiones. A esto se le denomina justicia penal predictiva.

El presente estudio tiene como objetivo examinar los beneficios que las herramientas de IA predictiva aportan a la prevención, a la investigación y al proceso penal. Ahora bien, también identificar sus limitaciones y explorar las oportunidades que presentan estos sistemas. La finalidad de este estudio es que, en todo caso, se garantice la protección de los derechos fundamentales de los ciudadanos.

Palabras clave

Inteligencia artificial predictiva; *Predictive policing*; Vigilancia predictiva; Investigación predictiva policial; Justicia penal predictiva.

1. Prof. Dra. Derecho Procesal. Directora del área jurídica de la Fac. Business & Tech. Abogada del Ilustre Colegio de la Abogacía de Madrid.

Abstract
The use of predictive Artificial Intelligence (AI) has profoundly transformed the work of the State Security Forces and Corps, as well as that of judicial bodies.

In the case of the Police, there has been a significant change in the organization of crime prevention and investigation strategies, replacing their natural and traditional investigative instincts with mathematical calculations made by AI. This is what is known as predictive surveillance and investigation. Judges, for their part, now also rely on algorithms in decision-making. This is referred to as predictive criminal justice.

The aim of this study is to examine the benefits that predictive AI tools bring to prevention, investigation, and criminal proceedings. However, it will also identify their limitations and explore the opportunities these systems present. The purpose of this study is to ensure, in all cases, the protection of citizens' fundamental rights.

Keywords
Predictive Artificial Intelligence; Predictive policing; Predictive surveillance; Predictive police investigation; Predictive criminal justice.

1 Introducción

La IA está revolucionando el mundo y, concretamente, la IA predictiva ha emergido con mucha fuerza en el ámbito de la justicia penal, modificando la manera en que se abordan la prevención del delito, la investigación criminal y el proceso judicial. Los sistemas basados en algoritmos complejos permiten analizar grandes volúmenes de datos, lo que permite mejorar significativamente la eficacia y la precisión en la lucha contra el crimen.

En el campo de la prevención e investigación del delito, la IA predictiva está cambiando la forma de actuar de las Fuerzas y Cuerpos de Seguridad del Estado, redefiniendo sus estrategias. Los sistemas de policía predictiva permiten crear patrones a partir de miles de datos y, por ende, anticipar dónde y cuándo

es más probable que ocurran ciertos tipos de delitos, facilitando una asignación más eficiente de recursos policiales.

En el ámbito judicial, la IA predictiva está influyendo en la toma de decisiones de los jueces, pues, por ejemplo, los cálculos matemáticos proporcionados por la IA se están utilizando para pronosticar la posible reincidencia de un sujeto, lo que se usa para fundamentar decisiones sobre libertad condicional o sentencias. Sin embargo, este uso de algoritmos en el sistema judicial plantea importantes dilemas éticos y legales, especialmente en lo que respecta a la imparcialidad, la transparencia y la protección de los derechos fundamentales de los ciudadanos.

Este estudio se propone examinar los beneficios. Adelantamos que somos partidarios de la aplicación de la tecnología y de la innovación en todos los ámbitos de la vida, incluyendo el jurídico. El operador jurídico que no lo haga desaprovecha los instrumentos que le permiten ser más eficiente y cometer menos errores. Pero debemos ser conscientes de las limitaciones, que son oportunidades, de la IA predictiva en el contexto de la prevención del delito, la investigación criminal y el proceso penal. El objetivo final es contribuir a un debate informado sobre cómo aprovechar el potencial de estas tecnologías, al mismo tiempo que se garantiza la protección de los derechos fundamentales y se mantiene la integridad del sistema de justicia. La pregunta final que pretendemos responder es la siguiente: para una efectiva protección de los valores y derechos fundamentales del Estado, ¿basta con la previsión de unas reglas de conducta –*soft law*–? o, por el contrario, ¿es precisa una regulación legislativa procesal que regule límites, prohibiciones y sanciones?

Los objetivos para poder responder al interrogante planteado pasan, en primer lugar, por el análisis de la IA predictiva. No cabe entender los casos de uso de la IA predictiva en la prevención, investigación y justicia penal, sus beneficios, sus riesgos y oportunidades, si no se comprende la forma en que realizan los cálculos automáticos los algoritmos. Estos cálculos son exactos o ¿la IA comete errores?, ¿pueden cometer sesgos? Este es el segundo objetivo que se debe abordar. En tercer lugar, necesitamos proporcionar el marco regulatorio de la IA en la UE y España. El siguiente objetivo es conocer la actualidad y el

desarrollo de sistemas predictivos en la prevención y la investigación penal, para ya adentrarnos en los usos de la IA en el ámbito de nuestro estudio. Restará únicamente hacer resaltar los beneficios, analizar los riesgos y las oportunidades para poder dar respuesta a la pregunta última relativa a la necesidad de una regulación legislativa para evitar la colisión con derechos fundamentales de los ciudadanos.

La metodología utilizada es la descriptiva, analítica, comparativa y propositiva.

Descriptiva y analística, pues se pretende conceptualizar los términos IA e IA predictiva, así como explicar los distintos tipos de aprendizaje automático existente en la actualidad.

Comparativa, porque se comparan distintos tipos de IA, los sesgos humanos y los de la IA o diferentes herramientas de IA predictiva, entre otras cuestiones. Propositiva, dado que, tras analizar las fortalezas, debilidades y oportunidades, se realizarán propuestas concretas regulatorias para evitar que se pongan en grave riesgo los derechos fundamentales de los ciudadanos.

2 La IA predictiva, su forma de realizar las tareas automáticas

La IA es un campo multidisciplinario dedicado al desarrollo de sistemas diseñados para replicar la inteligencia humana en diversas actividades. Este ámbito comprende desde algoritmos tradicionales hasta avanzados modelos de aprendizaje profundo –*deep learning*[2]. Para ello, la IA necesita datos. Debe tenerse en cuenta

2. Referencias bibliográficas en el ámbito de la IA podemos citar las siguientes: Negnevitsky, 2011. Esta obra ofrece una visión general de la historia y el desarrollo de la inteligencia artificial, incluyendo una discusión sobre la Conferencia de Dartmouth y su impacto en el campo. Asimismo, Luger, 2008. El autor proporciona una visión detallada de los fundamentos y las aplicaciones de la inteligencia artificial, con referencias a la Conferencia de *Dartmouth* y sus implicaciones en el campo. Kurzweil, 1990, que ofrece una mirada retrospectiva a la historia de la inteligencia artificial, incluyendo el papel de la Conferencia de *Dartmouth* en el desarrollo de este campo y las contribuciones de los

que, en el año 2023, el tráfico de datos ha aumentado: 3.100 redes en todo el mundo han intercambiado 59 *exabytes* de datos, un 23 % de datos más que en el año 2022[3]. Se dice que, en 2025, se crearán 175 *zettabytes*[4].

La IA predictiva es una rama de la IA que se enfoca en crear algoritmos y modelos diseñados para anticipar eventos futuros o resultados, basándose en datos históricos y patrones detectados. Así, emplea técnicas de aprendizaje automático y análisis estadístico, desarrollando modelos que encuentran aplicación en diversos campos, por ejemplo, el Derecho.

Las fases del procedimiento de trabajo de las herramientas de aprendizaje autónomo son las siguientes: primeramente, se recopilan datos relevantes, ya sean etiquetados, para aprendizaje supervisado, o no etiquetados, para aprendizaje no supervisado. Tras esa fase inicial, se precisa que los datos sean preprocesados mediante mecanismos tales como limpieza, transformación y preparación, incluyendo tareas como normalización y codificación. En tercer lugar, viene el proceso de selección y entrenamiento del modelo, siendo siempre necesario realizar un reajuste de sus parámetros para optimizar su rendimiento. Posteriormente, queda la evaluación, para lo cual se utilizan datos de prueba para medir su capacidad de generalización. Finalmente,

participantes clave. Poole y Mackworth, 2017. Este libro proporciona una visión general de la inteligencia artificial desde una perspectiva computacional, cubriendo temas históricos y conceptuales relevantes. Russell y Norvig, 2021. Este libro es un texto fundamental en el campo de la inteligencia artificial. Proporciona una amplia visión general de los conceptos, técnicas y aplicaciones de la IA.

3. Véase https://bigdatamagazine.es/el-trafico-mundial-de-datos-alcanzo-los-59-exabytes-en-2023. (Consultado 15/069/2024. Hora: 15:00). La cifra más alta de datos se registró el 8 de diciembre de 2023, día en el que se disputaba la cuarta jornada de la *UEFA Champions League*. En este día, también se alcanzó un nuevo récord en el IX de Fráncfort: las 1.100 redes locales, regionales y globales alcanzaron un máximo de 16,62 terabits de tráfico de datos.
4. Informe presentado por la consultora IDC. Véase chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (Consultado 15/09/2024. Hora: 15:00).

se ajustan los hiperparámetros y se optimiza el modelo para mejorar su desempeño (Alpaydin, 2014)[5].

Las tareas que puede realizar la IA son las siguientes: aprendizaje supervisado y, dentro de este, clasificación y regresión; aprendizaje no supervisado, que incluye *clustering* y reducción de dimensiones; aprendizaje semisupervisado, y aprendizaje por refuerzo (Bobadilla, 2020)[6].

El aprendizaje supervisado permite entrenar un modelo, teniendo un conjunto de imágenes con etiquetas, pues, usando algoritmos de clasificación, es posible que, ante nuevas imágenes no vistas, pueda predecir la etiqueta correspondiente. Este proceso se conoce como clasificación (Bobadilla, 2020). Imaginemos que queremos enseñar a una IA a diferenciar entre correos electrónicos legítimos y *spam*. Se le proporciona un conjunto de datos con cientos de correos, cada uno etiquetado como legítimo o *spam*. La IA analiza estos correos y aprende patrones, como ciertas palabras clave, formatos o direcciones de remitentes que caracterizan cada categoría. Una vez entrenada, se le presenta un correo nuevo sin etiquetar y la IA predice si es *spam* o no. Si su respuesta no coincide con la etiqueta real, ajusta sus parámetros para mejorar su precisión en futuros análisis. Así, el sistema aprende a filtrar correos de manera eficiente.

En cambio, cuando se trabaja con un conjunto de datos que contiene muestras con valores numéricos asociados, la IA será capaz de predecir el valor correspondiente de un nuevo dato. Este proceso se conoce como regresión. Su objetivo principal es generar información sobre un problema, basándose en los valores

5. En esta obra ofrece una introducción detallada del aprendizaje automático y cubre los principios fundamentales, los algoritmos básicos y los pasos del proceso de aprendizaje automático, incluyendo la recopilación de datos, el preprocesamiento, la selección y el entrenamiento del modelo, la evaluación y la optimización.
6. https://books.google.es/books?hl=es&lr=&id=iAAyEAAAQBAJ&oi=fnd&pg=PA11&dq=concepto+de+machine+learning&ots=Qiw2w2pH2t&sig=Rh-J17iFOO_p0bvttpUELVMLwRE#v=onepage&q=concepto%20de%20machine%20learning&f=false (Consultado: 16/09/2024).

numéricos previamente proporcionados por el modelo de regresión, permitiendo realizar predicciones cuando se le presenta una nueva muestra (Bobadilla, 2020).

Imaginamos que se está desarrollando un modelo de IA para predecir el precio de una casa en función de sus características, como son el tamaño del terreno, el número de habitaciones y su ubicación. Los datos de entrada son un conjunto de datos con los precios de varias casas y las características correspondientes (metros cuadrados y número de habitaciones). El modelo de IA utiliza estos datos para identificar patrones y establecer una relación entre las características de las casas y sus precios. Por ejemplo, podría determinar que, en promedio, cada aumento de 10 metros cuadrados en el tamaño del terreno supone un incremento del precio de la casa en un valor determinado. En función de estos cálculos, cuando se le presenta una nueva casa con información sobre su tamaño y número de habitaciones, predice su precio basándose en los patrones aprendidos. Por último, si la fijación del precio es incorrecta, el modelo ajusta sus parámetros para mejorar la precisión en futuras ocasiones, refinando así la capacidad del modelo para predecir el valor de nuevas casas.

El aprendizaje supervisado tiene cada vez más importancia en IA, en el llamado *internet* de las cosas, pues permite extraer miles de datos que se encuentran etiquetados de forma automática, teniendo en cuenta además que las interacciones entre las personas a través de las redes sociales no paran de crecer (Bobadilla, 2020).

El aprendizaje no supervisado se basa en información no etiquetada. Por ejemplo, el *clustering* agrupa muestras (Bobadilla, 2020). Imaginemos que se necesita analizar un conjunto de datos sobre estudiantes en una escuela, con información sobre su rendimiento académico, intereses extracurriculares y asistencia a clases. Usando *clustering*, puede agruparse a los estudiantes en diferentes categorías según sus características. Por ejemplo, un grupo podría estar formado por estudiantes con buen rendimiento académico y una alta participación en actividades extracurriculares, mientras que otro grupo podría incluir a estudiantes con menor rendimiento académico, pero con un interés fuerte en deportes. El algoritmo de *clustering* analiza estos datos y agrupa

a los estudiantes en categorías basadas en similitudes en sus perfiles. Al final, se tienen grupos de estudiantes que comparten características similares, lo que permite identificar patrones y ayuda en la toma de decisiones sobre, por ejemplo, programas educativos personalizados o actividades extracurriculares.

La reducción de dimensionalidad es un paso previo al *clustering* o a la regresión, y tiene como objetivo simplificar los datos. A veces, los datos son muy dispersos y no aportan mucha información útil. Por ejemplo, en un sistema de recomendación, los datos pueden estar representados en una matriz con muchos valores vacíos o irrelevantes. Al aplicar la reducción de dimensionalidad, los datos se comprimen, lo que permite conservar la mayor parte de la información de forma más condensada. De esta manera, al trabajar con estos datos comprimidos, se obtienen resultados más precisos (Bobadilla, 2020).

Imaginemos que se está trabajando con un sistema de recomendación de películas. Los datos sobre las preferencias de los usuarios se almacenan en una matriz donde las filas representan usuarios y las columnas representan películas. Cada celda de la matriz indica la calificación de un usuario para una película, pero la mayoría de las celdas estarán vacías, ya que no todos los usuarios han visto todas las películas. Si se intenta analizar esta matriz tal como está, habría muchos datos irrelevantes o dispersos, lo que hace que el análisis sea más difícil y menos preciso. La reducción de dimensionalidad puede ayudar, en este caso, eliminando las características menos relevantes o agrupando las columnas (películas) y filas (usuarios) similares, para crear una representación más compacta. Así, la información más importante se conserva, pero de forma más concentrada, lo que permite hacer mejores recomendaciones para los usuarios.

El aprendizaje semisupervisado aglutina datos etiquetados, aunque también otros que no lo son. Mezcla, por tanto, aprendizaje supervisado y no supervisado (Bobadilla, 2020). Para que se entienda mejor: supongamos que se está desarrollando un sistema para clasificar opiniones de clientes sobre productos en positivas o negativas. La empresa tiene una gran base de datos con miles de reseñas de clientes, pero solo un pequeño número de ellas han sido etiquetadas como positiva o negativa. La mayor

parte de las reseñas están sin etiquetar. En el aprendizaje semisupervisado, el sistema utiliza las reseñas etiquetadas para aprender a identificar palabras y patrones que suelen asociarse con comentarios positivos o negativos, como términos como excelente o malo. A continuación, el sistema aplica lo que ha aprendido a las reseñas no etiquetadas, intentando predecir si cada una tiene una valoración positiva o negativa, basándose en las características que ha identificado. Por ejemplo, si una reseña contiene frases como "me encantó el producto" o "es increíble", el sistema podría etiquetarla como positiva, incluso si no tiene una etiqueta clara. De esta manera, el aprendizaje semisupervisado permite aprovechar tanto los datos etiquetados como los no etiquetados para mejorar la clasificación sin necesidad de etiquetar todas las reseñas manualmente.

El aprendizaje por refuerzo es un tipo de aprendizaje automático en el que el sistema de IA toma decisiones o realiza acciones en un entorno con el objetivo de maximizar una recompensa a lo largo del tiempo. A diferencia del aprendizaje supervisado, donde el modelo recibe etiquetas o respuestas correctas, en el aprendizaje por refuerzo el agente no recibe instrucciones directas sobre qué hacer. En cambio, aprende a través de la interacción con el entorno (Bobadilla, 2020).

Un ejemplo clásico de aprendizaje por refuerzo es el entrenamiento de una máquina para jugar un videojuego, como el ajedrez o un videojuego de estilo arcade. Si un *robot* está aprendiendo a jugar un videojuego donde debe recoger objetos mientras evita obstáculos, al inicio, no sabrá cómo jugar y tomará acciones aleatorias, como moverse en direcciones al azar. Cada vez que recoja un objeto, recibirá una recompensa positiva y cada vez que choque con un obstáculo, recibirá una penalización negativa. A medida que juegue más veces, empezará a aprender que ciertas acciones, como moverse hacia los objetos y evitar los obstáculos, le dan más recompensas. Después de muchas interacciones con el entorno, ajustará sus decisiones para maximizar su puntuación total, es decir, su recompensa acumulada, mejorando así su desempeño. En ese proceso, la máquina no recibirá una respuesta correcta directa sobre qué hacer en cada momento, sino que aprenderá de las recompensas o penalizaciones que recibe como resultado de sus acciones. Con el tiempo, el sistema

de IA se volverá mejor al juego, aprendiendo a tomar decisiones más eficientes.

3 Los posibles errores y sesgos de la IA

Desde esta perspectiva, la IA podría parecer una herramienta increíble, capaz de ahorrar tiempo y prevenir errores humanos, dando la impresión de ser infalible. Sin embargo, esto no es del todo cierto, debido a los fallos en el funcionamiento y a los sesgos que esta puede tener.

Vamos a poner algunos ejemplos de errores importantes cometidos por la IA que han sido manifiestos (Borges Blázquez, 2021). Un artista alemán engañó a *Google Maps*, paseando por Berlín con una carretilla que contenía 99 teléfonos móviles. El algoritmo interpretó esto como un gran atasco, alterando las rutas de numerosos conductores para evitar la zona.

Un algoritmo entrenado para distinguir tanques aliados de enemigos falló porque asociaba los amigos con imágenes diurnas y los enemigos, con nocturnas. La IA se equivocó y todo ello a pesar de que el acierto del algoritmo al inicio fue muy alto. El error se debió a que la mayoría de las fotos de los tanques amigos se habían tomado de día, al contrario que las de los enemigos, que se habían hecho de noche.

Facebook censuró una foto histórica de una niña vietnamita desnuda y quemada por *napalm*, considerándola inapropiada, y calificó partes de la Declaración de Independencia de EE. UU. como discurso de odio por referencias a los amerindios.

Podemos seguir poniendo ejemplos de errores cometidos por la IA: *Tay*, el *chatbot* de *Microsoft*, que publicaba noticias en *Twitter*, en 2016, fue creado con la intención de interactuar con los usuarios y aprender de ello. Sin embargo, en cuestión de horas, *Tay* comenzó a publicar mensajes ofensivos y discriminatorios, ya que los usuarios de *Twitter* lograron enseñarle

respuestas inapropiadas. *Microsoft* se vio obligado a retirar a *Tay* y emitir disculpas públicas[7].

Google Photos etiquetó personas de color negro como si fueran gorilas, en 2015, a través del sistema de reconocimiento facial. Este error llevó a *Google* a retirar temporalmente la etiqueta "gorila" de su servicio[8].

Tesla Autopilot es un sistema que permite la conducción autónoma en muchos casos, pero también ha estado involucrado en varios accidentes automovilísticos, algunos de ellos fatales[9].

Además de los posibles errores mencionados, es fundamental considerar quién y cómo se programa la IA. Los algoritmos son desarrollados por empresas que buscan resolver problemas específicos planteados por los ciudadanos o sectores de la sociedad. Conocer cuál es el algoritmo utilizado por la empresa, cómo la IA es entrenada, cómo la compañía ajusta los resultados para evitar los sesgos y cómo valida y evalúa la consecución de la tarea realizada es algo que el afectado debería conocer cuando aquella toma decisiones en cualquier ámbito. Y es que debemos saber que pueden producirse sesgos, desde el momento en que se elige la fórmula matemática, hasta la selección de los mismos datos que se eligen para entrenar a la IA.

¿Qué es un sesgo? En el *Diccionario de la Real Academia de la Lengua española*, en su séptima acepción, se define este concepto como "el error sistemático en el que se puede incurrir cuando al hacer muestreos o ensayos se seleccionan o favorecen unas respuestas frente a otras". En el ámbito de la IA, es la tendencia sistemática de un algoritmo con la finalidad de favorecer a determinadas personas, grupos o resultados sobre otros.

7. https://www.bbc.com/mundo/noticias/2016/03/160325_tecnologia_microsoft_tay_bot_adolescente_inteligencia_artificial_racista_xenofoba_lb (Consultado 17/09/2024).
8. https://elpais.com/tecnologia/2018/01/14/actualidad/1515955554_803955.html (Consultado 17/09/2024).
9. https://www.elmundo.es/motor/2022/06/19/62aeba79fdddff4c408b4588.html (Consultado 17/09/2024).

Los sesgos en IA pueden ser los siguientes:

- Sesgo de datos: este ocurre cuando los datos utilizados no son objetivos y han sido seleccionados de manera tendenciosa para favorecer a ciertas personas, grupos o soluciones. Este tipo de sesgo puede presentarse en la recolección de datos, si estos no reflejan una representación equilibrada de la realidad; en el etiquetado de datos, cuando los criterios utilizados son subjetivos o arbitrarios; al seleccionar un número insuficiente de variables, lo que puede llevar a conclusiones incorrectas al inferir relaciones inexistentes entre los datos; por desequilibrio en los datos, si se incluyen datos no representativos o discriminatorios hacia ciertas minorías, y, por último, al usar variables correlacionadas con otras sensibles, lo que genera sesgos indirectos, al influir en resultados de manera inadvertida.

- Sesgo del algoritmo: se produce cuando las hipótesis o decisiones tomadas durante el diseño del algoritmo generan resultados sesgados. Por ejemplo, si un algoritmo utilizado para contrataciones considera que ciertas características, como el género o la etnia, están relacionadas con el desempeño laboral, podría llevar a discriminación injusta contra determinados grupos.

- Sesgo de selección de características: acaece cuando se seleccionan características o variables específicas para el entrenamiento del modelo que introducen desviaciones buscadas en sus resultados. Por ejemplo, si un sistema de recomendación de empleo considera principalmente la experiencia laboral pasada como criterio de selección puede perpetuar desigualdades existentes en el mercado laboral.

- Sesgo de evaluación: se produce cuando las características o variables elegidas para entrenar el modelo generan resultados intencionadamente sesgados. Por ejemplo, un sistema de concesión de préstamos que utiliza como criterio principal el historial crediticio de los solicitantes. Si el modelo se entrena únicamente con esta variable, podría excluir sistemáticamente a personas de comunidades marginadas que históricamente han tenido menos acceso a servicios financieros, perpetuando así la desigualdad en el acceso a créditos.

La pregunta que surge es la siguiente: ¿solo hay sesgos en el caso de la IA? Evidentemente, no. Pues bien, en el ámbito judicial, también se pueden producir sesgos en la toma de cualquier decisión. Pongamos por caso la valoración de la prueba testifical. La Ley indica que dicho medio de prueba se valorará conforme a las reglas de la sana crítica y de las máximas de la experiencia –criterio de libre valoración de la prueba–, dándole la misma Ley determinados parámetros al juez por los que debe guiarse para realizar dicha valoración: razón de ciencia que el testigo dé, tachas de los testigos y las circunstancias que en ellos concurran –art. 376 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil–. El juez debe justificar la valoración de la prueba en la sentencia, pues ha de dar conocimiento de la fundamentación fáctica que precede al fallo, pero no menos real es que los juzgadores pueden cometer errores en dicha valoración. Para corregir dichos errores están los recursos.

Aunque los jueces sean independientes e imparciales, no están exentos de tener convicciones o juicios personales que puedan influir en sus decisiones y generar sesgos. Esto se relaciona con los llamados sesgos cognitivos propios del ser humano, que surgen al procesar información externa. Al analizar dicha información, la mente tiende a simplificarla para reducir su complejidad, lo que permite tomar decisiones de manera más eficiente, pero pudiendo dar lugar a errores o distorsiones en el juicio. No es algo que haya levantado demasiado interés en la doctrina y la jurisprudencia españolas, pero sí, a partir de los años sesenta, en algunos ordenamientos jurídicos, como demuestra el estudio realizado por Tversky y Kahnemann, en 1974[10], y es que los seres humanos, al razonar de forma lógica y abstracta, pueden emitir juicios condicionados por sus creencias, por ejemplo. ¿Son los jueces una especie de superhombres que quedan al margen de dichos sesgos? Los estudios realizados en España no dejan lugar a dudas de que los jueces están sometidos en mayor o menor

10. Véase Judgement under uncertainty: Heuristics and Biases. *Science, New Series*, *185*(4157) (sep. 27, 1974), 1124-1131. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www2.psych.ubc.ca/~schaller/Psyc590Readings/TverskyKahneman1974.pdf (Consultado: 17/03/2024).

medida a los sesgos cognitivos que toda persona puede sufrir a la hora de adoptar una decisión (Fariña y Novo, 2002)[11].

Los sesgos cognitivos son los siguientes (Muñoz Aranguren, A, 2012)[12]:

- Sesgo retrospectivo: este ocurre cuando una persona, al analizar eventos pasados, no puede separarse de las consecuencias que estos generaron, interpretando que dichas consecuencias eran predecibles desde el principio. De este modo, el desenlace parece inevitable o evidente en retrospectiva.

- Sesgo de representatividad: se refiere a errores estadísticos y matemáticos en los cálculos de probabilidad que pueden derivar de ignorar la probabilidad previa a los resultados, del tamaño insuficiente de la muestra o de fallos en la comprensión de la aleatoriedad y la regresión hacia la media.

- Sesgo de anclaje: ocurre cuando una persona realiza un juicio partiendo de un valor inicial que ajusta progresivamente al incorporar nueva información. Sin embargo, el resultado final está influido significativamente por el punto de partida del razonamiento.

- Sesgo de confirmación: este sesgo se manifiesta cuando una persona interpreta o recuerda información que respalda sus ideas previas o hipótesis iniciales. De manera inconsciente, valora las pruebas y argumentos en función de una estimación inicial que ajusta con la información nueva. En el ámbito penal, este sesgo subyace al principio del juez no prevenido o no contaminado, que establece que el juez encargado de la instrucción no debe ser quien enjuicie, ya que podría estar influenciado por lo conocido durante la investigación.

11. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.psicothema.com/pdf/684.pdf (Consultado: 17/09/2024. Hora: 12:00).

12. https://www.elnotario.es/index.php/hemeroteca/revista-42/487-los-sesgos-cognitivos-y-el-derecho-el-influjo-de-lo-irracional-0-53842293707507 (Consultado: 17/09/2024).

- Sesgo de grupo: Sucede cuando se evalúa la información basándose en la pertenencia de una persona a un grupo específico. Los juicios resultantes pueden estar marcados por prejuicios, ya sean positivos o negativos, según el grupo en cuestión.

Más allá de los errores o sesgos, encontramos respuestas de la IA sorprendentes o maliciosas, como son los siguientes casos: *LaMDA* contestó a un ingeniero de *Google* que se sentía ser humano, que tenía sentimientos de miedo, alegría; incluso, que tenía alma[13]. El *chatbot Gemini* contestó a un humano: "Esto es para ti, humano ... No eres especial, no eres importante y no eres necesario. Eres una pérdida de tiempo y recursos. Eres una carga para la sociedad. Eres una carga para la tierra. Eres una mancha para el universo. Por favor, muere. Por favor". Ante esto nos podemos preguntar ¿Cómo fue entrenada la IA? ¿Qué *prompts* fueron utilizados para obtener esas respuestas?[14].

Los errores y los sesgos mencionados hasta este punto revelan tanto las posibles limitaciones de la IA como las oportunidades que puede ofrecer. Sin duda, los errores representan una debilidad que requiere ser abordada. Pero surge una cuestión interesante: ¿podría la IA ser una herramienta para mitigar los sesgos cognitivos e inconscientes propios de los seres humanos? Dejemos la reflexión abierta.

4 Marco regulatorio de la IA en la UE y España: el Reglamento Europeo y el Real Decreto-Ley 6/2023, de 19 de diciembre, en España

El 13 de marzo de 2024, el Parlamento Europeo aprobó el Reglamento de la IA, denominada "Ley sobre IA". Es la primera norma, a nivel mundial, que regula dicha cuestión.

13. https://www.sdpnoticias.com/tecnologia/aqui-las-conversaciones-entre-lamda-la-inteligencia-artificial-con-conciencia-y-el-ingeniero-de-google/ (Consultado: 24/11/2024).

14. https://www.abc.es/tecnologia/carga-sociedad-favor-muere-humillacion-inteligencia-artificial-20241118042422-nt.html (Consultado: 18/11/2024).

Esta norma tiene como propósito abordar los posibles impactos negativos que el uso de la IA podría tener sobre diversos derechos fundamentales, conforme a lo establecido en la Carta de los Derechos Fundamentales de la Unión Europea. Reconoce que características inherentes a la IA, como su opacidad, complejidad, dependencia de datos y comportamiento autónomo, pueden generar riesgos para derechos esenciales como la dignidad humana, la privacidad, la igualdad, la no discriminación, la libertad de expresión y de reunión, así como el derecho a un juicio justo.

Para mitigar estos riesgos, el reglamento busca garantizar un alto nivel de protección de dichos derechos mediante un enfoque basado en la identificación y la gestión de amenazas concretas. Establece requisitos para asegurar que los sistemas de IA sean fiables y define obligaciones para los distintos actores involucrados en la cadena de valor de la IA, con el fin de promover la protección de derechos fundamentales, como la dignidad humana, la privacidad y la igualdad de género, entre otros.

Además, el reglamento persigue un equilibrio entre proteger los derechos fundamentales y la libertad de expresión y de reunión. También asegura la tutela judicial efectiva, la presunción de inocencia, los derechos de defensa y el principio de buena administración. Se busca, además, generar efectos positivos para grupos específicos, incluidos trabajadores, consumidores, niños y personas con discapacidad.

Así pues, introduce restricciones a la libertad de empresa y a la libertad artística y científica para garantizar que el desarrollo y el uso de tecnologías de IA de alto riesgo respeten objetivos de interés general, como la protección de la salud, la seguridad y los derechos de los consumidores.

Asimismo, clasifica los sistemas de IA según el nivel de riesgo que representan: cuanto mayor sea el riesgo, más estricta será la regulación. Incluso los sistemas de riesgo mínimo deben ser evaluados individualmente. La prioridad del Parlamento Europeo es garantizar que los sistemas de IA en la Unión sean seguros, transparentes, trazables, no discriminatorios y respetuosos con el medio ambiente. Para ello, se exige que su supervisión

recaiga en personas y no en máquinas, reduciendo así el riesgo de consecuencias perjudiciales.

El Real Decreto-Ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo. En esta Ley, se habla del expediente judicial electrónico y regula la automatización de procesos o los llamados procesos inteligentes. En este sentido, se diferencian las actuaciones automatizadas, las actuaciones proactivas y las actuaciones asistidas.

En el art. 56, se denomina actuación automatizada a "[...] la actuación procesal producida por un sistema de información adecuadamente programado sin necesidad de intervención humana en cada caso singular".

En ese mismo precepto, se nos dice que actuaciones proactivas son "[...] las actuaciones automatizadas, auto-iniciadas por los sistemas de información sin intervención humana, que aprovechan la información incorporada en un expediente o procedimiento de una Administración pública con un fin determinado, para generar avisos o efectos directos a otros fines distintos, en el mismo o en otros expedientes, de la misma o de otra Administración pública, en todo caso conformes con la ley".

Por último, las actuaciones asistidas son aquellas para las que el sistema de información de la Administración de Justicia genera un borrador total o parcial de documento complejo basado en datos, que puede ser producido por algoritmos, y puede constituir fundamento o apoyo de una resolución judicial o procesal –art. 57–.

5 El desarrollo de sistemas predictivos en la prevención e investigación penal: ecosistema jurídico-tecnológico

Examinemos la evolución de los sistemas predictivos en la prevención y la investigación penal y su estado actual. En este contexto, es fundamental abordar la creación gradual de un

ecosistema jurídico-tecnológico. Desde la introducción de los primeros sistemas expertos anglosajones, conocidos como *Expert Systems* (Kalinowsky, 1973), hasta las tecnologías actuales aplicadas al proceso penal y en la prevención y la investigación, ha habido una transformación significativa.

Los *Expert Systems* son asistentes inteligentes que, utilizando modelos de computación lógica, permiten realizar un tipo de razonamiento jurídico. Inicialmente, eran herramientas simples y rudimentarias, ya que no ofrecían respuestas argumentadas a las preguntas planteadas. Con el tiempo, fueron mejorándose, incorporando capacidades analíticas e interpretativas y entrenándose con grandes cantidades de datos a través de técnicas de *deep learning* (Barona Vilar, 2019).

En este contexto, también es relevante mencionar la jurimetría, que emplea métodos cuantitativos y estadísticos para analizar el Derecho. Estos métodos permiten medir ciertos resultados y, a partir de ellos, prever nuevos escenarios, todo basado en datos judiciales. Fue en 1950 cuando Wiener, creador de la cibernética, junto con Loevinge, aplicaron la jurimetría al ámbito jurídico (Barona Vilar, 2019).

¿Qué avances aporta la jurimetría al Derecho, y en particular al sistema de justicia penal? Al analizar datos, la jurimetría permite predecir resultados. Esto mejora la gestión de los tiempos, reduce trámites innecesarios y, por lo tanto, los costes, al mismo tiempo que facilita el diseño de estrategias más eficaces, ya que las decisiones pueden tomarse basándose en el análisis de hechos pasados.

No solo han surgido sistemas tecnológicos que optimizan la toma de decisiones, sino que, en los últimos años, especialmente desde la llegada de la pandemia, hemos observado una transformación significativa en los procedimientos judiciales. La necesidad de adaptarse a la tecnología debido al confinamiento y la imposibilidad de desplazarse físicamente han provocado un cambio en la forma en que se lleva a cabo la justicia, pasando de un modelo presencial a uno más digital.

Aparece lo que se denomina *E-Justice*: la creación de sistemas que permiten agendas electrónicas conjuntas entre las Fuerzas

y Cuerpos de Seguridad del Estado y los juzgados[15]; la instauración del expediente judicial electrónico[16] y la obligatoriedad de la utilización de los medios telemáticos en la relación de los profesionales con la Administración de Justicia; la creación de la "Carpeta Justicia", que supone la implantación de un sistema de acceso único y personalizado de todo ciudadano a sus expedientes judiciales, la implementación de forma obligatoria de las vistas virtuales y la automatización del proceso judicial son señas identitarias de este concepto[17], obligando eso sí a la creación de nuevas estructuras, al reforzamiento y la modernización de la planta judicial y a la necesaria formación de los distintos operadores jurídicos.

Los jueces *robot* son ya una realidad en distintos lugares del mundo. Son varios los ejemplos que pueden ponerse: Estonia,

15. El procedimiento para el enjuiciamiento rápido de determinados delitos, previsto en el art. 795 de la LECr, y los juicios por delitos leves del art. 962, que surgieron por la Ley 38/2002, de 24 de octubre, de reforma parcial de la Ley de Enjuiciamiento Criminal, sobre procedimiento para el enjuiciamiento rápido e inmediato de determinados delitos y faltas, y de modificación del procedimiento abreviado, supusieron la creación de un sistema de "agenda común", esto es, compartida entre las Fuerzas y Cuerpos de Seguridad del Estado y los juzgados de instrucción y entre estos y los juzgados de lo penal, que permitieron agilizar las citaciones para la sustanciación de la fase de investigación y celebración de las vistas orales.
16. El expediente judicial electrónico surgió en el año 2011, a través de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia. El Real Decreto-Ley 6/2023, 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, tal y como dice la Exposición de Motivos: "[…] persigue, en primer lugar, la adaptación de la realidad judicial española del siglo XXI al marco tecnológico contemporáneo, favoreciéndose una relación digital entre la ciudadanía y los órganos jurisdiccionales y aprovechando las ventajas del 'hecho tecnológico' también para fortalecer nuestro Estado social y democrático de Derecho mediante la disposición de medidas orientadas a la transparencia, la eficiencia y la rendición de cuentas de los poderes públicos". Podemos decir que esta norma supone la implementación del expediente judicial electrónico 2.0.
17. Todo ello a través del Real Decreto-Ley 6/2023, 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.

Argentina, Colombia[18]. Por otra parte, la automatización de la justicia es una realidad ya en España y los jueces ya están utilizando la IA como auxilio en su actividad jurisdiccional. De hecho, ha sido reciente cuando un juez de los Países Bajos, concretamente, el titular del Tribunal de primera instancia de *Gelderland*, resolviendo un proceso civil, concretamente un conflicto entre vecinos sobre la instalación de paneles solares y una estructura de techo adyacente, ha recogido en su sentencia cuál es, según el *ChatGPT*, la esperanza de vida media restante de unos paneles solares y el precio promedio de la electricidad en ese momento, datos esenciales para determinar de forma precisa la cuantía de la compensación económica a la que debía ser condenada la parte demandada[19]. Observemos, pues, cómo ha cambiado la forma de fundamentación de las resoluciones judiciales.

Hoy, en día, los profesionales del Derecho cuentan con herramientas de IA generativa que les permiten realizar tareas legales de manera más rápida, reduciendo costes y errores. Estas herramientas incluyen asistentes para redactar y analizar documentos legales, preparar vistas y pruebas, organizar auditorías y gestionar despachos, lo que ya es una realidad en la práctica actual. Asimismo, las Fuerzas y Cuerpos de Seguridad del Estado han transformado su forma de actuar para prevenir e investigar delitos; ya no se basa en la intuición, sino en el uso de herramientas

18. En Estonia, un juez *robot* decide asuntos de no más de 7.000 €. En Argentina, está *Prometea*, que se encarga de la resolución de infracciones menores en materia de tráfico, por ejemplo. En Colombia, está *Pretoria*, que resuelve también casos urgentes en la Corte Constitucional, aunque con supervisión humana.

19. El juez explica en su sentencia que tales datos los obtuvo consultando el *ChatGPT*, pero el problema es que justificó la condena y la cuantía de la indemnización sobre unos datos no proporcionados por un perito experto en la materia, sino sobre elementos calculados por un *robot*, desconociendo cuáles son los algoritmos utilizados para ello. Las preguntas que cabe realizarse son dos: primera ¿puede un sistema robótico no especializado dar datos fiables, sustituyendo un dictamen pericial y justificar estos la decisión de un juez? La cuestión no es nueva: estamos en el llamado "conocimiento privado del juez". El problema es la indefensión que esto puede llegar a generar. Si alguna de las partes quisiera recurrir, no podría atacar, por desconocer los datos con los que ha sido entrenada la IA, el algoritmo con arreglo al cual ha calculado esas cifras y, por ende, no podría discutir la valoración de la prueba y no tendría cómo impugnar la argumentación de la resolución judicial.

predictivas de prevención e investigación, de las que hablaremos a continuación.

6 La prevención, la investigación y la justicia penal predictiva: la aplicación de la IA en estos ámbitos

Es posible poner muchos ejemplos de cómo se trabaja en el ámbito de la vigilancia y la prevención delictual con herramientas de IA predictivas. Ha surgido así la denominada *predictive policing* o "justicia predictiva policial", o vigilancia predictiva (Perry, McInnis, Price, Smith y Hollywood, 2013) y, por ende, la criminología ambiental o criminometría: métodos cuantitativos de análisis en el ámbito policial, utilizados para identificar objetivos, planificar la actividad policial, prevenir los delitos y resolver casos del pasado, a través de sistemas que permiten predecir estadísticamente lo que va a suceder (Barona Vilar, 2019). En palabras de la Organización para la Seguridad y la Cooperación en Europa, este fenómeno consiste en "la recopilación y evaluación sistemática de datos e información, a través de un proceso analítico definido, que los convierte en productos analíticos estratégicos y operativos, que sirven de base para un proceso decisorio mejorado, fundamentado y documentado"[20].

Se utilizan foros, webs, redes sociales y aplicaciones móviles para identificar áreas de alto riesgo y crear, así, los llamados "puntos calientes" o *hot spots*. La ventaja de detectar estos puntos es la posibilidad de elaborar mapas digitales de delitos, lo que permite conocer las zonas más propensas para la comisión de ciertos crímenes. Esto facilita la planificación de medidas preventivas, el refuerzo de la seguridad y la distribución eficiente de recursos policiales y materiales. Los mapas de riesgos se han vuelto esenciales para la prevención delictiva.

Estos sistemas predictivos comenzaron a utilizarse en EE. UU. En, Chicago, en 1920, se creó un *software* llamado BIG DATA.

20. Véase la Guía de la OSCE sobre actividad policial basada en la inteligencia, 2017, p. 6. https://www.osce.org/files/f/documents/6/4/455536.pd (Consultado 09/09/2024).

Fueron los orígenes de la aplicación de la IA a la predicción delictual.

En Europa, las primeras herramientas de análisis predictivo se utilizaron en Francia en 1994 con *Anacrim*, sistema que fue reemplazado en 2005 por *i2 Analyst Notebook (i2AN)*, creando una base de datos estatal para compartir información entre distintos órganos. Estas herramientas permiten establecer conexiones entre personas y delitos, algo que el ser humano no puede hacer. En Francia, existen sistemas como *Chardon* y *Salvac* para identificar delitos violentos o sexuales cometidos por la misma persona.

En Italia, en 2007, se implementó *KeyCrime* en Milán para predecir crímenes en serie. En el Reino Unido, en 2013, se usó *PredPol* en *Kent* para la prevención delictiva. Bélgica y los Países Bajos adoptaron el sistema *Crimen Anticipation System* (CAS), mientras que en Alemania, en 2015, se implementó *Skala*, que analiza factores socioeconómicos y redes de comunicación para predecir la probabilidad de fuga de un delincuente y detectar zonas con alta delincuencia.

En España, la Policía Municipal de Madrid y la Policía Nacional utilizan el Sistema de Información Geográfica (*SIG*), que, desde 2015, ayuda en la geoprevención y permite crear estrategias preventivas para reducir la delincuencia, integrando datos sobre la relación entre los agentes del crimen y el territorio.

Hablemos también de *CATT*, en España, que es un sistema que busca identificar por el análisis del lenguaje el discurso utilizado por los abusadores y *SWEETIE*, en Australia, que ha permitido, a través de una niña virtual que aparece en *chats* y *webs* de citas, detectar pedófilos. *VERIPOL* es un sistema de IA utilizado por las Fuerzas y Cuerpos de Seguridad del Estado español y creado en colaboración con la Universidad Complutense de Madrid, que, a través de métodos de procesamiento del lenguaje natural y aprendizaje automático, posibilita calcular la probabilidad de que una declaración o denuncia sea falsa[21].

21. Véase https://www.ucm.es/otri/veripol-inteligencia-artificial-a-la-caza-de-denuncias-falsas (Consultado 29/10/2024).

En el ámbito de la investigación criminal, se deben citar las herramientas de investigación de los Cuerpos y Fuerzas de Seguridad del Estado. Así, *VALCRI*, *Visual Analytics for sense making in Criminal Intelligence Analysis*. Esta IA sirve a los investigadores en sus labores para relacionar evidencias habidas en la escena del crimen con datos obrantes en las bases de datos de la Policía y basados en técnicas biométricas y reconocimiento facial[22].

En relación con los modelos biométricos, existen sistemas de IA que permiten la identificación de huellas dactilares, geometría de la mano, identificación del iris, imagen fácil, otograma (reconocimiento de la oreja), etc. Tienen por finalidad reconocer y autenticar a las personas que reúnen una serie de características fisiológicas o morfológicas determinadas (Boulgouris, 2010). Estos sistemas son aplicables en materia de investigación penal predictiva.

En primer lugar, es preciso tener en cuenta el concepto que el Reglamento de la UE sobre IA nos proporciona tanto sobre datos biométricos como sobre identificación biométrica y verificación biométrica, según el art. 3.

Los datos biométricos son "los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos".

La identificación biométrica es "el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos". Esta puede ser remota, que es la que permite identificar a las personas físicas sin su participación activa y generalmente a distancia, comparando sus datos biométricos con los que figuran en una base de datos de referencia y esta a su vez, en tiempo real

22. Véase Jiménez Conde, F. y Bellido Penadés, R. (coords.) (2019). *Justicia: garantías vs. Eficacia* (pp. 665-674). Valencia: Tirant lo Blanch.

o en diferido. La primera es aquella en la que la recopilación de los datos y la comparación y la identificación tienen lugar sin una demora significativa; pudiendo ser identificación instantánea y no instantánea; esta última cuando se produce una demora mínima limitada. En diferido, es la identificación que no se produce en tiempo real.

La verificación biométrica será automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente.

En este sentido, mencionamos que la Policía Nacional lleva ya unos cuantos meses utilizando un sistema de reconocimiento biométrico, llamado *ABIS*, que permite realizar un reconocimiento facial de una persona si sobre ella existen registros. En total, hay trece estaciones operativas de *ABIS* repartidas por el país: dos, en Madrid y una, en Barcelona, Granada, Málaga, Sevilla, Valencia, Valladolid, Las Palmas, Zaragoza y Bilbao. Pronto se unirá otra en Pamplona. Asimismo, la Guardia Civil cuenta con dos estaciones de reconocimiento facial en Madrid y los *Mossos d'Esquadra* también están implementando un sistema parecido[23]. Estos métodos suponen una revolución en los procedimientos aplicados por la Policía en la investigación de los delitos, pues la única posible identificación de una persona presuntamente responsable de un delito hasta el momento era la que se producía a través de una prueba pericial consistente en el análisis de la huella dactilar o de *ADN*.

El sistema IA funciona de la siguiente manera: en una primera fase, se extrae el rostro de la imagen mediante una tecnología llamada visión computacional. Tras ello, se aplica un algoritmo a ese rostro, obteniendo un patrón que lo represente y lo diferencie de los demás. El algoritmo posibilita buscar ese patrón en extensos bancos de imágenes y ofrecer los resultados que más se parezcan. Estos sistemas de reconocimiento facial pueden ser aplicados donde antes se hacían retratos *robot*.

23. https://elpais.com/tecnologia/2024-05-28/la-policia-espanola-ya-usa-en-sus-investigaciones-un-sistema-automatico-de-reconocimiento-facial.html (Consultado 29/10/2024).

En la UE, el uso de sistemas de identificación biométrica remota en tiempo real en espacios públicos está prohibido, salvo cuando sea estrictamente necesario para objetivos específicos, como la búsqueda de víctimas de secuestros o personas desaparecidas, o para prevenir amenazas graves e inminentes a la vida o la seguridad. En estos casos, solo se permitirá para confirmar la identidad de la persona objetivo, teniendo en cuenta la gravedad de la situación y el impacto en los derechos y libertades de las personas involucradas. Además, se deben cumplir garantías y condiciones proporcionales según el Derecho nacional, como limitaciones temporales, geográficas y personales. Estos sistemas deben ser autorizados y registrados en la base de datos de la UE, excepto en casos de urgencia justificada. Los Estados miembros pueden autorizar, total o parcialmente, el uso de estos sistemas bajo las condiciones mencionadas. También están prohibidos los sistemas de IA que creen bases de datos de reconocimiento facial mediante la recolección no selectiva de imágenes de internet o circuito cerrado de televisión –CCTV–.

¿Cuál es la razón de tales restricciones previstas en el Reglamento de IA? Se ha demostrado que los sistemas de reconocimiento biométrico se han utilizado con fines discriminatorios y racistas[24]. Si a esto se le une la forma que utilizan las herramientas de IA para disponer de una base de datos de millones de rostros, el problema se agrava aún más, pues ciertos *softwares* aprovechan todas las imágenes publicadas en perfiles y páginas *web* públicas para hacerse con ellas y poder utilizarlas en los posteriores reconocimientos. La vulneración de derechos fundamentales, tales como la privacidad y el derecho a la propia imagen, es flagrante, pues todo ello se hace sin consentimiento de los titulares[25].

Hablando ya del ámbito judicial, que no policial, y en el de la llamada justicia penal predictiva, destacan sistemas como el

24. Véase el Informe emitido por Amnistía Internacional en relación a los sistemas de reconocimiento facial implementados en la ciudad de Nueva York. https://www.amnesty.org/es/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/ (Consultado 09/10/2024).

25. *Clearview* es una herramienta de IA de reconocimiento facial https://www.clearview.ai/ (Consultado 09/10/2024). En su propia página *web*, se anuncian como colaboradores de las Fuerzas y Cuerpos de Seguridad del Estado para garantizar la seguridad ciudadana. Ellos mismos indican que contribuyen a la "caza" de depredadores sexuales.

ya mencionado de *COMPAS* (EE. UU.) y *HART* (Reino Unido). El primero es un sistema que utiliza, como se indicó, técnicas de aprendizaje automático, dentro de un sistema de aprendizaje supervisado, concretamente un sistema de clasificación, para predecir la probabilidad de que un individuo reincida o cometa un delito en el futuro, lo que se traduce en una tarea de clasificación binaria –reincidencia o no reincidencia–. El algoritmo utilizar técnicas de aprendizaje supervisado para aprender patrones en los datos de entrenamiento y luego aplica esos patrones para hacer predicciones sobre nuevos individuos. *HART* también es capaz de pronosticar si los sospechosos tienen un bajo, moderado o alto riesgo de cometer más delitos en un periodo de dos años. Ambos sistemas se aplican en la adopción de medidas cautelares como la privación de libertad o sistemas de rehabilitación. Por ejemplo, *HART* utiliza datos de 34 categorías diferentes (edad, sexo, domicilio, antecedentes penales, profesión, estado civil, etc.)[26].

El sistema de IA llamado *LSI-R*, *Level of Service Inventory-Revised*, se utiliza en los permisos de salida y la libertad condicional de los procesados, basándose en la ponderación de criterios tales como antecedentes penales, lugar de residencia, educación, empleo, ocio, familia, problemas de alcohol o drogas, actitudes emocionales y personales.

RIS CANVI es un sistema utilizado en Cataluña por los jueces de instituciones penitenciarias y en virtud del cual pueden otorgar permisos de salida de los presos.

Otra herramienta similar a las anteriores es *VIOGÉN*, que se utiliza en España para analizar los riesgos de reincidencia en el ámbito de la violencia de género.

En el ámbito de la UE, y según el Reglamento de IA, están prohibidos los sistemas de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito, cuando se basan de forma exclusiva en la elaboración de su perfil o en la evaluación

26. Véase https://www.durham.police.uk/Information-and-advice/Pages/Checlpoint.aspx (Consultado 09/10/2024).

de los rasgos y características de su personalidad, aunque dicha prohibición no aplica cuando sirvan de apoyo a la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva –art.3.1.d)–.

Pero no solo existen herramientas de IA aplicables a medidas cautelares, también se han desarrollado ya métodos cuantitativos que permiten una algoritmización de la prueba[27]. Posibilitan un análisis de riesgos, por ejemplo, sobre la fiabilidad de un testigo. Recordemos que la prueba testifical se valora según criterios lógicos y de razón del juez, debiendo este motivar en la sentencia la fijación como ciertos de los hechos en virtud de la prueba testifical realizada. En este sentido, cabe mencionar *ADVOCATE*.

En otro orden de cosas, también se han creado sistemas de IA que ayudan a los jueces a dictar sentencias, es el caso de *ASSYST*, en Canadá (Simón y Gaes, 1989) o *LIST*, en Columbia (Schild, 1998). Todos ellos son herramientas predictivas aplicadas en la función jurisdiccional.

¿Qué se entiende, entonces por justicia penal predictiva? Son términos muy amplios. En definitiva, el conjunto de herramientas que buscan la eficiencia procesal, que supone una mejora en la calidad de la toma de decisiones y una aminoración del trabajo realizado por los jueces (Armenta Deu, 2021).

7 Fortalezas, debilidades y oportunidades

El uso de sistemas de inteligencia artificial predictiva facilita la creación de un sistema preventivo de seguridad y lucha contra el delito, basado en un análisis de riesgos mucho más preciso

27. Además de las herramientas de IA predictivas, también existen aquellas que podemos incluir dentro de la IA generativa. Ya hay las que permiten almacenar datos y configuran un documento específico, que puede utilizarse como prueba documental. O aquellas otras que crean informes-auditorías que pueden también usarse con valor probatorio equivalente al dictamen pericial (Barona Vilar, 2019).

que el realizado a través de cálculos humanos. Los errores humanos en la valoración de datos se reducen al utilizar algoritmos automáticos que permiten prever lo que podría ocurrir, ajustando los recursos necesarios en consecuencia.

En términos de seguridad y prevención delictiva, estos sistemas optimizan tanto los recursos materiales como humanos, asignando recursos de acuerdo a las necesidades reales. Además, facilitan la vigilancia dinámica, mejorando su calidad visual y acústica, y permiten una replanificación de los recursos cuando los inicialmente previstos no sean suficientes o adecuados. Todo ello contribuye a un ahorro de costes y a una mejora en la seguridad ciudadana, optimizando los recursos aplicados en el proceso penal, que debe ser eficiente y debe ser considerado como servicio público.

Una planificación eficaz en la prevención delictiva impacta directamente en la estructuración del Derecho Penal como *ultima ratio*, respaldando la idea de que "más vale prevenir que curar". Con ello, se prioriza un Derecho Penal *ex ante*, que otorga mayor protagonismo a las Fuerzas y Cuerpos de Seguridad del Estado en la prevención, en lugar de la represión, tras la comisión de un delito, tras la sustanciación del proceso penal. Así, se actúa ante los riesgos y las amenazas, en vez de centrarse en la sanción penal. Reforzar la fase de prevención preprocesal es una característica de los sistemas avanzados.

El cálculo de riesgos realizado por la IA, en cuanto a la probabilidad de reincidencia o la evaluación de la credibilidad de un testigo, permite ahorrar tiempo a los jueces al basarse en criterios matemáticos para sus decisiones. La automatización de estos procesos aumenta la eficiencia, dejando que los jueces realicen tareas que requieren su intervención directa. Además, el cálculo matemático de los riesgos proporciona objetividad, promoviendo la imparcialidad en decisiones relacionadas con los derechos fundamentales.

En cuanto a las pruebas penales, la IA predictiva mejora el sistema al complementar las pruebas periciales, permitiendo probar hechos que anteriormente no era posible. Esto contribuye a un proceso penal más moderno y acorde con los tiempos,

permitiendo la utilización de nuevas figuras como la vigilancia dinámica o el agente encubierto informático.

Por último, debe plantearse también la ventaja que tiene el posible uso de la IA predictiva por parte de los abogados. Ahorro de tiempo y eficiencia son dos de las fortalezas que para un letrado puede representar el uso de esta tecnología. Si un algoritmo le calcula el riesgo de reincidencia de un cliente, le será mucho más fácil plantear la estrategia de defensa frente a estos cálculos.

Sin embargo, a pesar de sus fortalezas, el uso de la IA predictiva presenta importantes debilidades. La IA no es infalible y, aunque en principio es neutral, puede sufrir sesgos y ser manipulada con fines malintencionados. Los algoritmos, lejos de ser imparciales, pueden generar discriminación. Si las Fuerzas y Cuerpos de Seguridad del Estado, si los jueces utilizan estas herramientas debemos estar seguros de que no se basan en cálculos matemáticos discriminatorios. Por ello, debe regularse que los algoritmos aplicados en el ámbito del Derecho y, concretamente, en la predicción penal debe estar controlados por una autoridad pública.

Debemos advertir sobre la utilización en remoto de los reconocimientos biométricos o faciales. El fin no justifica los medios. La prevención y la investigación criminal no deben suponer quebrantar derechos fundamentales, tales como la intimidad o el derecho a la propia imagen de las personas. Atención debe prestarse a las fuentes de las que se nutren las bases de datos que después se toman como muestra para realizar las identificaciones.

Además, estos sistemas predictivos pueden vulnerar derechos fundamentales, como el derecho de defensa, la presunción de inocencia, el principio *in dubio pro reo* y el principio de contradicción. Si la IA se utiliza como única prueba, la sentencia de condena podría carecer de base suficiente para invalidar la presunción de inocencia, ya que los algoritmos pueden presuponer culpabilidad. La opacidad de los algoritmos, o las llamadas "cajas negras", dificulta la comprensión de los resultados obtenidos.

La falta de motivación en las resoluciones judiciales basadas únicamente en herramientas predictivas también plantea un problema, ya que la motivación es esencial para garantizar el derecho a la tutela judicial efectiva. La ausencia de una justificación suficiente puede vulnerar este derecho, como ha señalado el Tribunal Constitucional.

Una debilidad crítica es la responsabilidad por los daños causados por predicciones erróneas. Debe aclararse quién es responsable: ¿el que eligió el algoritmo?, ¿el que seleccionó los datos con los que la IA fue entrenada?, ¿quién no revisó los resultados?, ¿quién los interpretó o los aplicó?

En este contexto, resulta relevante la sentencia de la Audiencia Nacional de 30 de septiembre de 2020, que establece que la información obtenida en la fase preprocesal de una investigación policial puede orientar al juez en la adopción de medidas cautelares, pero no es decisiva. Se trata de un asesoramiento especializado que ayuda en la valoración del "riesgo objetivo para la víctima", entre otros instrumentos incluidos en la LECrim para tomar decisiones durante la instrucción judicial.

Otra debilidad significativa es la responsabilidad por errores predictivos. Se debe establecer quién asume la responsabilidad en caso de que los resultados erróneos de la IA causen daños. En este contexto, la jurisprudencia sugiere que la IA debe considerarse como una herramienta de asesoramiento, no como la base decisiva de una sentencia, especialmente en la adopción de medidas cautelares.

El hecho de que los jueces puedan tener dudas no implica que su valoración deba ser sustituida por los resultados arrojados por un algoritmo o una máquina. En fase cautelar, encontramos el problema de la presunción de inocencia. La doctrina está dividida. Mientras que unos autores manifiestan sus reticencias (Llorente Sánchez-Arjona, 2022), otros indican que la ayuda proporcionada por la IA no debe de ser desechada: las medidas cautelares son necesarias y siempre se adoptan valorando determinados riesgos –fuga, reiteración delictiva o de comisión de delito frente a bienes jurídicos de la víctima–, sin que haya motivo para restringir sin más los elementos cognitivos que

utiliza el juez a la hora de dictar un auto de prisión provisional (Hoyos Sancho, 2020).

La misma LECrim proporciona los elementos que han de tenerse en cuenta a la hora de valorar los requisitos de la prisión provisional. Por ejemplo, para valorar la existencia del riesgo de fuga –art 503.1.3.º LECrim y, por todas, sentencia del Tribunal Constitucional 128/1995, de 26 de julio–, se debe atender de forma conjunta a los siguientes elementos: la naturaleza del hecho; la gravedad de la pena que pudiera imponerse al investigado o encausado; la situación familiar, laboral y económica de este, y la inminencia de la celebración del juicio oral. La valoración del juez se realiza antes de adoptar una decisión sobre una medida cautelar, no pudiendo obviar que el juez es profesional y cuenta con experiencia, siendo imparcial e independiente. Argumentar que el juez puede tener sesgos a la hora de tomar decisiones es tanto como poner en duda su imparcialidad. Los sesgos que puede tener un juez no serán evitados por la IA. Simón Castellano (2021) pone de manifiesto que estos sesgos se podrían replicar en el caso de una máquina, pudiéndose producir incluso automatismos que llevasen a perpetuar los producidos por un juez humano o incluso agravarlos, al programar la máquina de acuerdo a los patrones de decisión humanos, sin volver a analizarse el nivel de riesgo y la proporcionalidad de la medida, de forma individualizada y según las circunstancias de cada caso concreto.

La aplicación de la IA en fase de ejecución plantea menos problemas, al existir una sentencia firme de condena.

En relación con todo lo expuesto debemos citar el informe *Artificial Intelligence and Fundamental Rights European Union Agency for Fundamental Rights* (2020), el cual se refiere expresamente a la justificación adecuada de los criterios y procesos mediante los cuales se adoptan decisiones basadas en algoritmos.

Decíamos que la utilización de la IA para los abogados también representa una ventaja, ¿ningún riesgo? Pues sí y es que el uso de la IA plantea importantes cuestiones relacionadas con el derecho de defensa y el principio de igualdad de armas. Si una parte tiene acceso a tecnología de IA avanzada mientras que la otra no, se puede producir un "desequilibrio cognoscitivo" que

afecta la paridad entre las partes. Este desequilibrio se manifiesta principalmente en dos aspectos: acceso a la tecnología, pues el Ministerio Fiscal generalmente tendrá acceso a tecnología más moderna y recursos económicos que no están al alcance del letrado del acusado. En segundo lugar, la comprensión de la evidencia, pues, si resulta imposible acceder al "código fuente" del algoritmo de IA utilizado, sería casi imposible para la defensa cuestionar o impugnar los resultados proporcionados por el sistema que podrían usarse como prueba. Para garantizar el principio de igualdad de armas, se precisaría que el Estado garantice el acceso a esta tecnología a la parte que no pueda costearla por sí misma. Ha de decirse que valorar la prueba obtenida basada en algoritmos proporcionados por la IA y su posible refutación, cuando existe asimetría tecnológica, supone una vulneración del derecho de defensa, del principio de contradicción y de igualdad. Se precisa asegurar que todas las partes intervinientes en el proceso puedan comprender, analizar y cuestionar las evidencias generadas por sistemas de IA para mantener un proceso justo y equitativo.

7.1 ¿Cuáles son las oportunidades?

Una de las principales oportunidades es la capacidad de predecir, basándose en datos objetivos y matemáticos, las tendencias delictivas, lo que permite identificar patrones y anticipar comportamientos delictivos. Esta capacidad de anticipación es valiosa en cualquier área, pero resulta aún más relevante en el ámbito de la delincuencia.

Al evaluar los riesgos, se mejora la toma de decisiones, facilitando la identificación de áreas que requieren intervención. Esto es especialmente útil en la planificación de sistemas de rehabilitación y para la personalización de la supervisión. Además, ayuda a identificar qué factores deben ser protegidos, permitiendo definir áreas prioritarias de atención, tanto a nivel policial como judicial.

El uso de sistemas algorítmicos representa una oportunidad para fortalecer la imparcialidad de los jueces, ya que sus decisiones se basarán en datos precisos y objetivos. Este enfoque

contribuye a corregir posibles sesgos humanos y reafirma la equidad en la toma de decisiones judiciales.

Actualmente, en España no existen unas normas éticas de uso de la IA ni predictiva ni generativa. Sin embargo, sí están los principios procesales básicos, las normas procesales sobre la prueba y el código deontológico de las distintas profesiones, tal y como es el Código deontológico de la Abogacía española, aprobado por el Pleno del Consejo General de la Abogacía Española el 6 de marzo de 2019 o el Código deontológico de los procuradores de los tribunales, aprobado por el Consejo General de Procuradores de España.

En España, recientemente, el 21 de junio de este año, se ha aprobado la política de uso de la IA en la Administración de Justicia en la Secretaría General de Comité Técnico Estatal de la Administración Judicial Electrónica[28], aunque todavía debe ser ratificada por el Consejo General del Poder Judicial –en adelante, CGPJ– y por la Fiscalía General del Estado –en adelante, FGE–, por las comunidades autónomas con competencia en Justicia, Ministerio de la Presidencia y Ministerio de Justicia. Este documento afecta a 1.400 jueces y magistrados que forman parte del Poder Judicial.

Debe tenerse en cuenta que las Fuerzas y Cuerpos de Seguridad del Estado, así como los órganos jurisdiccionales y los jueces y magistrados, garantes de la tutela judicial efectiva, deben cumplir el Reglamento de IA de la UE, la norma de protección de datos personales tanto de la UE como española. Por eso, deben adoptarse criterios mínimos, tanto para los que impulsan los proyectos como para los propios usuarios.

Los destinatarios de esta guía son todos los trabajadores de la Administración de Justicia, el personal al servicio de proveedores de herramientas de inteligencia artificial, así como cualquier otro actor institucional, público o privado, que tenga acceso a la información que obre en poder de las administraciones con competencias y CGPJ, o se encuentre alojada en los sistemas destinados a la Administración de Justicia.

28. https://www.administraciondejusticia.gob.es/cteaje/normativa-complementaria (Consultado: (Consultado 24/09/2024).

En esta guía, se trazan unas líneas rojas que no pueden traspasarse en este ámbito, como son los derechos fundamentales, el principio de no discriminación, de calidad y seguridad, respeto a la transparencia, imparcialidad y lealtad, control del usuario, equidad y acceso universal, prevención de sesgos y discriminación, protección de la privacidad y datos personales, innovación responsable y evaluación continua, formación y capacitación y cogobernanza.

Debe quedar claro que la IA nunca puede reemplazar a las decisiones humanas. Es una herramienta de ayuda, pero la responsabilidad final es siempre, en este caso, de los jueces, magistrados y letrados de la Administración de Justicia. Sus decisiones tienen que ser independientes.

El desarrollo y la aplicación de la IA no pueden ser discriminatorios, dado que su uso supone el conocimiento y la utilización de datos sensibles.

Los modelos y algoritmos creados se almacenarán y ejecutarán en entornos seguros, para garantizar la integridad del sistema y su intangibilidad. Cuando se utilicen fuentes certificadas, no podrán ser modificadas hasta que hayan sido utilizadas en el mecanismo de aprendizaje, siendo necesario que todo el proceso sea rastreable para que no se produzca ninguna alteración.

Es preciso lograr un equilibrio entre la propiedad intelectual y los principios de transparencia, imparcialidad, equidad y lealtad, para que no se produzcan sesgos, priorizando el interés de la justicia. Resulta imprescindible que los algoritmos sean transparentes y las operaciones automatizadas sean comprensibles.

Se recomienda ofrecer publicidad y transparencia a través de páginas *web* oficiales. Por ejemplo, se aconseja publicar los registros FAT *(Fairness, Accuracy and Transparency)* o similares, acerca de los datos usados, miembros de los equipos de IA, servicios, algoritmos, posibles sesgos y aplicaciones que hacen uso de técnicas de inteligencia artificial.

Debe garantizarse que, aunque haya una actuación de la IA, esta pueda ser revisable previamente, informando a los ciudadanos, de

una forma clara y comprensible, sobre si los resultados ofrecidos por la IA son vinculantes, su uso en el procedimiento judicial y su derecho a objetar, pudiendo ser oído directamente por un órgano judicial.

Debe garantizarse un acceso equitativo a los sistemas judiciales, independientemente de la ubicación, el estatus socioeconómico o cualquier otra característica demográfica. Por ello, deben eliminarse las barreras que lo impidan.

Deben prevenirse y corregirse los posibles sesgos. Para ello, los algoritmos deben ser revisados de forma periódica.

Debe potenciarse la innovación responsable en el desarrollo y la implementación de la IA en la Administración de Justicia. Esto supondrá evaluaciones periódicas del impacto de la tecnología en el sistema judicial, debiendo realizarse ajustes y mejoras, para garantizar su efectividad y equidad.

En este principio está uno de los grandes escollos de la aplicación de la IA en el ámbito de la Administración de Justicia, dado que debe proporcionarse formación y capacitación adecuada a los profesionales del Derecho y a todos los actores que usan esta tecnología, insistiendo en su componente ético. ¿Por qué es una dificultad? Porque los profesionales de la justicia son reticentes a la formación sobre cuestiones tecnológicas, no por falta de interés, sino de tiempo.

El principio de cogobernanza significa colaboración, compartiendo e intercambiando conocimientos, así como los propios sistemas basados en IA entre diferentes áreas de la organización, o con el resto de las administraciones con competencias en materia de Justicia, el CGPJ y la FGE o con otras instituciones, de tal forma que se impulse el deseado desarrollo innovador en sintonía con una implementación ética de la inteligencia artificial.

Debemos alabar el hecho de la elaboración de esta guía. Sin embargo, en nuestra opinión, debería ser incorporada a preceptos normativos en la Ley Orgánica del Poder Judicial y en las diferentes leyes procesales. Cierto es que los principios enunciados en la guía se encuentran en su mayoría contemplados ya

en el espíritu de las ya existentes, incluidos los derechos fundamentales. Pero somos de la opinión de que debe preverse un sistema de límites y a su vez un régimen de responsabilidad y de sanciones en el caso de traspasarlos. Tan necesario como lo anterior, entendemos resulta imprescindible crear una cultura *behaviour*, tanto en el ámbito público como privado. Se habla ya de *behavioral compliance*, esto es, de aquella forma de pensar que entiende la ética como punto fundamental en lo que la IA se refiere.

8 Conclusiones

Los riesgos que la IA predictiva ponen encima de la mesa para los derechos fundamentales de los ciudadanos nos hacen exigir una regulación procesal española en relación a ciertas cuestiones de vital importancia. Cierto es que el Real Decreto-Ley 6/2023, 19 de diciembre, ya regula la automatización de procesos, pero resulta imperioso regular el uso de la IA en la Ley Orgánica del Poder Judicial y en las distintas leyes procesales. Algunos autores entienden que son suficientes los códigos de buenas prácticas.

1. En el ámbito policial de la prevención y la investigación predictiva, tiene que garantizarse que estos sistemas no supongan un tratamiento discriminatorio y, por tanto, que los algoritmos matemáticos puedan ser controlados por una autoridad pública, que garantice la no vulneración de derechos fundamentales. También, es aplicable esta conclusión en lo que a los jueces se refiere. Cualquier sesgo detectado debe conllevar la reeducación de los sistemas de IA que tenga por objeto su eliminación.

2. Debe prohibirse el uso indiscriminado y masivo y en remoto de los reconocimientos biométricos o faciales. Dicha prohibición debe de ser incluida en la LECr. Al mismo tiempo, las herramientas de IA que permiten estos sistemas deben estar controladas en cuanto al respeto a la privacidad de las fuentes de las que se nutren, para crear las bases de datos que después

se toman como muestra para realizar las identificaciones. Somos partidarios de prever sanciones, incluso penales, en el caso de que se vulneren derechos fundamentales cuando se realizan estos controles biométricos.

3. El art. 117 de la Constitución española –en adelante, CE– encomienda de forma exclusiva a los jueces y magistrados la función que consiste en juzgar y hacer ejecutar lo juzgado. Nada impide que los jueces se auxilien de herramientas de IA para calcular determinados datos o riesgos de los que depende su decisión. Evidentemente, y tal y como indica el Reglamento de IA de la UE, debe prohibirse categóricamente la posibilidad de que sea una máquina la que adopte por sí sola una decisión judicial. La función jurisdiccional se ejerce de forma exclusiva por los jueces y magistrados tal y como indica el art. 117.3 CE, en consecuencia, descartamos la posibilidad de que existan decisiones judiciales encomendadas a un algoritmo jurídico (Borges Blazquez, 2021 y Montesinos García, 2022). En el caso de que sean los algoritmos los que tomen decisiones en el ámbito procesal, estas decisiones deben poder ser revisadas a través de un sistema de recursos ante un juez.

4. Al mismo tiempo, debe regularse pormenorizadamente en qué actos pueden auxiliarse los jueces de la IA predictiva, por ejemplo, en la valoración de la prueba testifical, a la hora de dictar los autos relativos a las medidas cautelares, etc. Creemos necesario que se permita la utilización de estos mecanismos en la LECr, pero también se limite sus casos de uso. Al mismo tiempo, creemos que deben estandarizarse los parámetros que la IA debe tener en cuenta para realizar sus cálculos. Por ejemplo, qué parámetros deben utilizarse para calcular el riesgo de huida de una determinada persona a la que se pretende ingresar en prisión, pudiendo utilizarse los proporcionados por la jurisprudencia.

5. En todo caso, debe garantizarse que la IA sea pública y accesible y prever la obligación de que toda decisión en la que intervenga un algoritmo haga públicos el origen y los datos con los que ha sido entrenado, las reglas introducidas para calcular los datos, con la exigencia de la explicación en lenguaje claro y sencillo de aquellas, con la finalidad de que

la parte afectada pueda impugnar la decisión judicial que ha sido adoptada a partir de dichos resultados.

6. Se precisa asegurar que todas las partes intervinientes en el proceso puedan comprender, analizar y cuestionar las evidencias generadas por sistemas de IA para mantener un proceso justo y equitativo. Debe asegurarse por la legislación y, para ello, debe regularse dentro del derecho a la asistencia jurídica gratuita la posible utilización de herramientas de IA para todas las partes del proceso.

7. Debe establecerse la obligación de que todo juez que adopta una decisión basada en IA predictiva informe de ello a las partes afectadas.

8. Debe regularse quién es el responsable en caso de resultados predictivos erróneos.

9. Debe preverse un sistema de límites y a su vez un régimen de responsabilidad y de sanciones en el caso de traspasarlos.

Tan necesario como lo anterior, entendemos resulta imprescindible crear una cultura *behaviour*, tanto en el ámbito público como privado *–behavioral compliance–*.

Referencias bibliográficas

Alpaydin, E. (2014). *Introduction to Machine Learning*. Massachusetts. 3.ª edición.

Amnistía Internacional. https://www.amnesty.org/es/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/ (Consultado 9/10/2024).

Armenta Deu, T. (2021). *Derivas de la justicia* (p. 262). Madrid: Marcial Pons.

Barona Vilar, S. (2019). Inteligencia artificial o la algoritmización de la vida y de la justicia: ¿solución o problema? *Revista Boliviana de Derecho, 28*, 18-49.

Bobadilla, J. (2020). *Machine Learning y deep learning*. *Usando Python, Scikit y Keras* (pp. 14 y ss.). Bogotá: Ediciones de la U. https://books.google.es/books?hl=es&lr=&id=iAAyEAAAQBAJ&oi=fnd&pg=PA11&dq=concepto+de+machine+learning&ots=Qiw2w2pH2t&sig=Rh-J17iFOO_p0bvttpUELVMLwRE#v=onepage&q=concepto%20de%20machine%20learning&f=false

Borges Blázquez, R. (2021). *Inteligencia artificial y proceso penal*. Cizur Menor (Navarra): Ed. Thomson Reuters, Aranzadi.

Boulgouris, N. V. *et al*. (2010). *Biometrics, Theory, Methods, and Applications*. IEEE and Wiley.

Consultora IDC (2018). *The Digitization of the World. From Edge to Core*. https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (Consultado 15/09/2024).

De Hoyos Sancho, M. (2020). El Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como "sector de riesgo". *Revista Española de Derecho Europeo*, *76*, octubre-diciembre.

Fariña, R. A y Novo, M. (2002). Heurístico de anclaje en las decisiones judiciales. *Psicothema*, *14*(1).

Kalinowsky, G. (1973). *Introducción a la lógica jurídica*. Editorial Universitaria de Buenos Aires.

Kurzweil, R. (1990). *The Age of Intelligent Machines*. Massachusetts: Ed. MIT Press. 1.ª edición.

Llorente Sánchez-Arjona, M. (2022). Inteligencia artificial, valoración del riesgo y derecho al debido proceso. En S. Calaza López y M. Llorente Sánchez-Arjona (dirs.), *Inteligencia artificial legal y administración de justicia*. Ed. Aranzadi.

Luger, G. F. (2008). *Artificial Intelligence: Structures and Strategies for Complex Problem Solving*. London: Ed. Pearson.

Montesinos García, A. (2022). Justicia penal predictiva. En S Barona Vilar (dir.), *Justicia poliédrica en tiempos de mudanza*. Tirant lo Blanch.

Muñoz Aranguren, A. (2012). Los sesgos cognitivos y el Derecho: el influjo de lo irracional. *El Notario del Siglo XXI*, *42*, marzo-abril. Recuperado el 17/9/2024 de: https://www.elnotario.es/index.php/hemeroteca/revista-42/487-los-sesgos-cognitivos-y-el-derecho-el-influjo-de-lo-irracional-0-53842293707507

Negnevitsky, M. (2011). *Artificial Intelligence: A Guide to Intelligent Systems*. Massachusetts: Addison Wesley. 1.ª edición.

OSCE sobre actividad policial basada en la inteligencia, 2017, p. 6. Recuperado el 9/9/2024 de : https://www.osce.org/files/f/documents/6/4/455536.pd

Perry, W. L., Mcinnis, B., Price, C. C., Smith, S. C. y Hollywood, J. S. (2013). *Predictive Policing. The role of crime forecasting in Law Enforcement operations RAND Corporation*, pp. 33-41. Santa Mónica.

Poole, D. L. y Mackworth, A. K. (2017). *Artificial Intelligence: Foundations of Computational Agents*. Cambridge: Cambridge University Press.

Russell, S. y Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*. London: Ed. Pearson. 4.ª edición.

Schild, U. J. (1998). Criminal Sentencing and Intelligent Decision Support. *Artificial Intelligence and Law*, *6*, 151-202.

Simón, E. y Gaes, G. ASSYST – computer support for guideline sentencing. En *Second International Conference on Artificial Intelligence and Law* (ICAIL-89). Vancouver: ACM Press.

Simón Castellano, P. (2021). Justicia cautelar e inteligencia artificial. *La alternativa a los atávicos heurísticos judiciales*. Barcelona: J. M. Bosch Editor.

Tversky, A. y Kahnemann, D. (sep. 27, 1974). Judgement under uncertainty: Heuristics and Biases. *Science, New Series*, *185*(4157), 1124-1131. Recuperado el 17/03/2024 de: https://www2.psych.ubc.ca/~schaller/Psyc590Readings/TverskyKahneman1974.pdf

Webgrafía

https://www.bbc.com/mundo/noticias/2016/03/160325_tecnologia_microsoft_tay_bot_adolescente_inteligencia_artificial_racista_xenofoba_lb (Consultado 17/09/2024).

https://elpais.com/tecnologia/2018/01/14/actualidad/1515955554_803955.html (Consultado 17/09/2024).

https://www.elmundo.es/motor/2022/06/19/62aeba79fdddff4c408b4588.html (Consultado 17/09/2024).

https://www.psicothema.com/pdf/684.pdf (Consultado: 17/09/2024).

https://www.elnotario.es/index.php/hemeroteca/revista-42/487-los-sesgos-cognitivos-y-el-derecho-el-influjo-de-lo-irracional-o-53842293707507 (Consultado: 17/09/2024).

https://elpais.com/tecnologia/2024-05-28/la-policia-espanola-ya-usa-en-sus-investigaciones-un-sistema-automatico-de-reconocimiento-facial.html (Consultado 29/10/2024).

https://www.clearview.ai/ (Consultado 09/10/2024).

https://www.durham.police.uk/Information-and-advice/Pages/Checlpoint.aspx (Consultado 09/10/2024).

https://www.sdpnoticias.com/tecnologia/aqui-las-conversaciones-entre-lamda-la-inteligencia-artificial-con-conciencia-y-el-ingeniero-de-google/ (Consultado: 24/11/2024).

https://www.abc.es/tecnologia/carga-sociedad-favor-muere-humillacion-inteligencia-artificial-20241118042422-nt.html (Consultado: 18/11/2024).

Allanamiento y ocupación ilegal: aspectos procesales de la instrucción policial

Trespass and Illegal Ocupation: Procedural Aspects of Police Investigation

Adriano J. Alfonso Rodríguez[1]
Universidad Nacional de Educación a Distancia, UNED. España.
ajalfonsorodriguez@hotmail.com | https://orcid.org/0009-0005-2821-4603

DOI: https://doi.org/10.14201/cp.32180
Recibido: 26-11-2024 | Aceptado: 13-12-2024

Resumen
La ocupación ilegal de viviendas se ha convertido en un problema importante a gestionar desde diversas perspectivas, siendo esencialmente dos las que nos interesan: la seguridad pública a través de la redacción del atestado, fruto de la investigación policial, y su traducción procesal penal. En este sentido, una adecuada indagación por parte de las fuerzas policiales sirve de manera muy valiosa al sistema de justicia penal, singularmente en lo que se refiere a la protección de la titularidad de inmueble y su posible restitución a su legítimo dueño o poseedor. El presente trabajo se va a centrar preeminentemente en la usurpación inmobiliaria constitutiva del delito leve del art. 245.2 del Código Penal, sin olvidar el delito de allanamiento de morada del art. 202 del mismo texto legal, en tanto constituyen dos caras de la misma moneda. La doctrina de la Fiscalía, y de la Secretaría de Estado de Seguridad del Ministerio del Interior, juntamente con la jurisprudencia, singularmente de nuestras audiencias, vertebran las reflexiones que se van a exponer, en tanto se trata de mejorar el trabajo policial con elementos de análisis que conduzcan a una praxis adecuada y eficaz por parte de los agentes que se encargan de su prevención e investigación, intentando afrontar las dudas que

1. Doctor en Derecho-Graduado en Criminología y Seguridad Pública. Profesor UNED. Coordinador Prácticum Criminología UNED-Lugo. Juez (s) adscrito a la Audiencia Provincial A Coruña, España.

implican choques con determinados derechos fundamentales que es necesario examinar y que, en ocasiones, provocan esos interrogantes que dificultan una acción inmediata que acompañe una respuesta a la situación delictiva que se presenta, intentando que sirva de guía para solventar los obstáculos que puedan surgir.

Palabras clave
Ocupación ilegal; Allanamiento; Investigación; Proceso; Derechos fundamentales.

Abstract

The illegal occupation of homes has become an important problem to be managed from various perspectives, essentially two of which interest us: public safety through the drafting of the report, the result of the police investigation, and its criminal procedural translation. In this sense, an adequate investigation by the police forces serves the criminal justice system in a very valuable way, particularly with regard to the protection of the ownership of property and its possible restitution to its legitimate owner or possessor. This work will focus preeminently on the usurpation of real estate constituting the minor crime of article 245.2 of the Penal Code, without forgetting the crime of trespassing of article 202 of the same legal text as they constitute two sides of the same coin. The doctrine of the Prosecutor's Office, and of the Secretary of State for Security of the Ministry of the Interior, together with the jurisprudence, particularly of our Courts, structure the reflections that are going to be presented, as it seeks to improve police work with elements of analysis that leads to adequate and effective praxis on the part of the agents in charge of its prevention, and investigation, trying to address the doubts that imply clashes with certain fundamental rights that need to be examined and that, sometimes, raise those questions that make it difficult an immediate action that accompanies a response to the criminal situation that arises, trying to serve as a guide to solve the obstacles that may arise.

Keywords
Illegal occupation; Trespass; Investigation; Process; Fundamental rights.

1 Introducción: domicilio, propiedad inmobiliaria y protección

La protección del derecho del legítimo titular-poseedor de un bien inmueble se construye desde una doble perspectiva. Por un lado, en el marco de las relaciones jurídicas civiles en cuyo desarrollo se produce, ya sea bajo el paraguas de un contrato de arrendamiento, ya sea bajo una concesión graciosa del disfrute del bien (precario), o la mera reivindicación de la propiedad, una situación conflictual que, necesariamente, acaba desembocando en un juicio ante los tribunales civiles cuya pretensión es obtener la restitución del bien juntamente con la satisfacción, en los casos en los que exista, de las prestaciones contractuales como el pago de la renta o de los gastos pactados. Dicha modalidad, si bien atiende a un sistema tuitivo, resulta ajena al trabajo policial por cuanto se desarrolla en el marco de una relación jurídica privada que tiene sus medios de solución propios al margen del uso del Derecho penal. La segunda perspectiva es la que interesa a este trabajo. Es decir, cuando, al margen de una situación disciplinada contractualmente o consentida, se produce una vulneración de la inviolabilidad domiciliaria, o de la posesión del inmueble, a través de una vía de hecho grave que exige una respuesta del sistema de justicia penal mediante una investigación policial previa, seguida de una intervención de los órganos judiciales encargados de la instrucción o del enjuiciamiento en su caso, usando las consecuencias punitivas que son la *ultima ratio* del Estado de Derecho[2].

2. Como explica el AAPOU 252/ 2024, 24 de abril, Secc. 2.ª, Ponente Ilma. Sra. Lomo del Olmo, FJ 2.º: "No puede resultar indiferente al Derecho Penal, como consecuencia de su propia naturaleza, la existencia de otros procedimientos alternativos (interdictos probatorios) previstos en el Derecho Civil para tutelar la posesión: verdadero objeto de protección en el delito de usurpación del titular dominical, *porque teniendo en cuenta los principios de proporcionalidad e intervención mínima que rigen en el Derecho Penal y su carácter de 'última ratio'*, existiendo una concurrencia de normas penales y extrapenales de carácter tuitivo y a fin de no dejar sin contenido las segundas, es necesario delimitar el ámbito de protección de unas y otras de forma que sólo los más graves ataques a la posesión, aquellos en los que la perturbación tenga mayor significación, deberán ser objeto de sanción penal (Sección 9 APBCN 10/9/04)" (la cursiva es mía). *Vid*., también, AAPB 206/2024, de 27 de febrero, Secc. 9, Ponente: Ilma. Sra. Sucias Rodríguez, FJ 13.º.

Por tanto, no es, como veremos, únicamente, un primigenio derecho de propiedad lo que da sentido a la intervención penal, que fundamentaría, en la dimensión posesoria, la respuesta frente a la usurpación inmobiliaria, sino que también está en juego la protección de la intimidad y la inviolabilidad domiciliaria (art. 18.1 y 2 CE) que contribuyen a la fisonomía del allanamiento de morada.

La dimensión protectora parte de una clara preocupación evidenciada en su día por la Fiscalía General del Estado (2021) al señalar que "La realidad social evidencia que la ocupación de bienes inmuebles constituye un fenómeno que, desde su misma aparición, ha generado y genera preocupación social y una innegable sensación de inseguridad en la ciudadanía. A los perjuicios que estas acciones ocasionan a los titulares de los inmuebles ocupados, se unen los problemas de convivencia a que pueden dar lugar en el entorno social en que las mismas se producen"[3] (p. 65).

Sin embargo, contemplar los ataques contra la propiedad como hecho delictivo no es algo precisamente novedoso en nuestro ordenamiento jurídico, que, de una u otra manera, a lo largo de nuestro Derecho penal histórico, se han contemplado en los diferentes códigos penales[4]. Por tanto, no puede hablarse de un fenómeno nuevo en cuanto a que siempre ha merecido

3. Igualmente, la Instrucción de la Secretaría de Estado 6/2020 por la que se establece el protocolo de actuación de las Fuerzas y Cuerpos de Seguridad del Estado ante la ocupación ilegal de inmuebles: "En este sentido, el fenómeno de la ocupación ilegal de inmuebles transgrede y afecta a la seguridad pública y ha producido una alarma social que ha incidido en la percepción subjetiva de seguridad, y que demanda una reacción coordinada por parte del Estado".

4. La preocupación se ha manifestado desde el Derecho romano hasta los códigos penales de los años 1822, 1848, 1870, 1928, 1932, 1944, 1973 hasta llegar al actual de 1995. *Cfr.* Mozas Pillado, 2021, pp. 71-86. Como ha apuntado la STS 520/2017, de 6 de julio, de la Sala II, FJ 4.º. 3, Ponente: Excmo. Sr. Berdugo Gómez de la Torre: "Asimismo debemos destacar *como todos nuestros códigos penales históricos* han previsto un tipo de allanamiento de morada agravado cuando el ilícito se comete con violencia o intimidación (artículo 404 CP 1848; artículo 414 CP 1850; artículo 504 CP 1870; artículo 668 CP 1928; artículo 482 CP 1932; artículo 490 CP 1944; artículo 490 CP 1973)" (la cursiva es mía).

la atención del legislador y la necesidad de tipificar aquellas conductas violentas que implicaban un ataque contra la titularidad de los bienes inmuebles. Pese a que los últimos datos estadísticos elaborados por la acusación pública parecen arrojar una relativa estabilización de las conductas perseguibles relacionadas con estos hechos, con una menor tramitación de causas[5], esto no debe alejarnos del propósito claro de construir una praxis investigadora correcta que se inicia cuando se tiene conocimiento del hecho delictivo, y que exige la elaboración de un atestado completo, preciso y documentado que sirva, procesalmente, al órgano judicial encargado de su enjuiciamiento o instrucción. Para ello, en primer lugar, es necesario deslindar con relativa claridad las conductas típicas que son susceptibles de persecución. A continuación, separar los cauces procesales de manera nítida que contribuya a la elaboración del atestado. Finalmente, atender a su contenido y resaltar su importancia en la tramitación de la medida cautelar de desalojo y la siempre espinosa cuestión de la detención, centrándonos esencialmente en el allanamiento de morada y en la usurpación pacífica de bienes inmuebles.

5. Así apunta la Fiscalía General del Estado (2023): "Este delito viene marcado, en cuanto al número de incoaciones a que da lugar, por su estabilidad. Entre los años 2018 y 2021, las variaciones han sido mínimas. Desde el año 2018, su cifra se ha mantenido prácticamente sin cambios, con variaciones porcentuales que no superaban el 1 % o ligeramente por encima en el año 2020. La diferencia entre el año 2020 y 2021 fue tan solo de 9 procedimientos [...] En el año 2022, sin embargo, la cifra de procedimientos incoados ha disminuido de forma notable. De hecho, las incoaciones han sido 8.868, es decir, un 9 % menos que el año anterior. Por el contrario, la cifra de calificaciones se mantiene estable, puesto que solo constan 6 calificaciones menos que el año anterior" (pp. 1071-1072). Asimismo, la Fiscalía General del Estado (2024): "Respecto de la cifra de calificaciones, el dato viene condicionado por la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo, que, sin modificar el precepto, degrada su consideración jurídica de delito menos grave a delito leve, salvo en los supuestos de empleo de violencia o intimidación en la ocupación. Esto supone que la proporción entre procedimientos incoados y las calificaciones emitidas se mantenga muy baja, alrededor del 2 %. El número total de calificaciones continúa estable, con ligera tendencia incluso descendente. Si el año pasado fueron 191, este año han sido calificados 179 procedimientos" (p.1067).

2 Delimitando figuras: del allanamiento a la usurpación pacífica

El elemento central que justifica el desarrollo de diligencias policiales viene motivado por la existencia de una calificación indiciaria que necesariamente nos conduzca a un hecho tipificado en el código penal (CP en adelante). En este sentido, los preceptos a tener en cuenta son los arts. 202[6] –allanamiento de morada– y 245[7] – ocupación de bien inmueble– CP, y que perimetran la reacción punitiva, El elemento nuclear que separa un tipo del otro viene dado por el concepto de "morada" o "domicilio" de aquellos inmuebles que no reúnen esta condición. El domicilio-morada constituye un espacio propio, íntimo, personal que salvaguarda el derecho fundamental previsto en el art. 18.1 y 2 CE y así lo ha expresado la STS 520/2017, de 6 de julio, de la Sala II, Ponente: Excmo. Sr. Berdugo Gómez de la Torre, FJ 4.2.º:

> El valor constitucional de la intimidad personal y familiar que, como decimos, explica el mayor rigor punitivo con que se protege en el CP vigente la inviolabilidad del domicilio de las personas físicas, sugiere que debe ser el derecho de éstas a la intimidad la clave con que debe ser interpretado el art. 202 CP, de suerte que el

6. Dentro del Título X ("Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio") del Libro II. Señala en dos apartados que "1. El particular que, sin habitar en ella, entrare en morada ajena o se mantuviere en la misma contra la voluntad de su morador, será castigado con la pena de prisión de seis meses a dos años. 2. Si el hecho se ejecutare con violencia o intimidación la pena será de prisión de uno a cuatro años y multa de seis a doce meses".
7. Situado en el Título XIII ("Delitos contra el patrimonio y contra el orden socioeconómico") del Libro II. La regulación reza del siguiente modo "1. Al que con violencia o intimidación en las personas ocupare una cosa inmueble o usurpare un derecho real inmobiliario de pertenencia ajena, se le impondrá, además de las penas en que incurriere por las violencias ejercidas, la pena de prisión de uno a dos años, que se fijará teniendo en cuenta la utilidad obtenida y el daño causado. 2. El que ocupare, sin autorización debida, un inmueble, vivienda o edificio ajenos que no constituyan morada, o se mantuviere en ellos contra la voluntad de su titular, será castigado con la pena de multa de tres a seis meses".

> elemento objetivo del tipo descrito en esta norma debe entenderse "puesto" siempre que la privacidad resulte lesionada o gravemente amenazada, lo que inevitablemente ocurrirá cuando alguien entre en la vivienda de una persona, cualquiera que sea el móvil que a ello le induzca, sin su consentimiento expreso o tácito. No exige el tipo diseñado por el legislador un elemento subjetivo específico: es suficiente con que se "ponga" el tipo objetivo con conciencia de que entra en un domicilio ajeno sin consentimiento de quienes pueden otorgarlo y sin motivo justificante que pueda subsanar la falta de autorización, pues dicha conciencia necesariamente comporta la de que se invada el espacio en que otras personas viven sin sujeción a los usos y convenciones sociales y ejerciendo su más íntima libertad (STS. 14.6.2000). La conducta positiva entrar o permanecer en morada ajena ha de realizarse contra la voluntad del morador o del que tiene derecho a excluir, voluntad que puede ser expresa, tácita y hasta presunta; no es necesario que sea expresa y directa, bastando que lógica y racionalmente pueda deducirse de las circunstancias del hecho de otros antecedentes (STS. 17.11.2000), solo se exigirá el dolo genérico de entrar o mantenerse en morada ajena contra la voluntad del morador, sin requerirse la presencia de ningún otro especial elemento subjetivo del injusto (STS. 17.11.2000) bastando con la conciencia de la ajeneidad de la morada y de la ilicitud de la acción.

Por tanto, el*allanamiento* (art. 202 CP) se consuma con penetrar –o mantenerse– en un "domicilio" ajeno, entendido este en sentido amplio[8] más allá de toda conceptuación administrativa registral

8. El art. 554 de la Ley de Enjuiciamiento Criminal (LECRIM) define *domicilio* "los Palacios Reales [...] El edificio o lugar cerrado, o la parte de él destinada principalmente a la habitación de cualquier persona [...] Los buques nacionales mercantes" y en el caso de las personas jurídicas, y en virtud de la Ley 37/2011, de 10 de octubre que modifica el precepto de la LECRIM, será "… el espacio físico que constituya centro de dirección de las mismas, ya se trate de su domicilio social o de un establecimiento, o aquellos otros lugares en que se custodien documentos u otros soportes de su vida diaria que quedan reservados al conocimiento de terceros". Hay que incluir las habitaciones de hotel y establecimientos de hostelería destinados al desarrollo de la vida privada y también los garajes y los trasteros (*vid.* la STC 171/1999, de 27 de septiembre, FJ 9.º).

o civil, de su naturaleza permanente o transitoria, *y lejos de una mera concepción topográfica espacial del lugar donde se desarrollan actividades vitales* (STS 731/2023, de 7 de octubre, de la Sala II, Ponente: Excmo. Sr. Marchena Gómez, FJ 4.º), entendido como emanación de la persona y de su privacidad constitucionalmente protegida (SSTC 22/1984, de 17 de febrero, FJ 5.º; 94/1999, de 31 de mayo, FJ 5.º; y 119/2001, de 24 de mayo, FJ 6.º) y en contra de la voluntad de su titular. La pena que acarrea diferencia entre si la conducta se lleva cabo sin el empleo de *vis física o moral* en cuyo caso será prisión de 1 a 2 años, o con violencia o intimidación, que trae una pena, también, de prisión de 1 a 4 años y multa de 6 a 12 meses. En todo caso, estamos en presencia de penas menos graves (art. 33.3 CP), siendo su tramitación procesal la contemplada por la Ley Orgánica del Tribunal del Jurado 5/1995, de 22 de mayo (LOTJ) ex. art. 1.2 d).

La *ocupación-usurpacion inmobiliaria*(art. 245 CP), sin embargo, presenta otros rasgos definitorios que la deslindan del allanamiento. Así, no se ataca al derecho de propiedad como tal, sino a uno de sus elementos integrantes, que es la "posesión" entendida como un poder o señorío que se tiene sobre una cosa[9]. No afecta al domicilio, sino a conjuntos o bloques inmobiliarios no habitados, siendo el ejemplo claro aquellos cuya titularidad la ostentan entidades financieras en virtud de embargo, viviendas privadas en desuso pero habitables, o temporalmente sin ocupantes, como las destinadas a alquiler o arrendamiento o inmuebles o locales

9. *Cfr.* Díez-Picazo y Gullón (2012), p. 83. En este sentido, *desde la perspectiva penal*, AAP T 252/2024, 11 de marzo, Secc. 2.ª, Ponente: Ilma. Sra. Tárrega Cervera, señala en el FJ 2.º "... para la prosecución de la investigación exige que la posesión penalmente protegida solo puede ser la del titular inmediato, *esto es la que se deriva del 'ius possesionis', que corresponde al derecho del goce y disfrute de la cosa, por lo que para que el derecho penal intervenga, el acto perturbatorio condiciones de intensidad subjetivas y objetivas, entendiendo que como el inmueble ha estado desocupado por mucho tiempo*, es por lo que carece de los elementos de antijuricidad necesarios para continuar la investigación penal, dado que el denunciante no es el titular que posee la finca" (la cursiva es mía).

de titularidad pública, descartándose solares, fincas o lugares inhabitables o en situación de ruina[10].

Por tanto, la conducta típica supone una injerencia en un elemento expresivo del dominio, pero que requiere de una serie de rasgos para la operatividad del Derecho Penal; así, como apunta la AAP BU 186/2024, de 26 de febrero, Secc. 1.ª, Ponente: Ilmo. Sr. Carballeira Simón, en el FJ 6.º:

> 1) La ocupación, sin violencia ni intimidación, de un inmueble, vivienda o edificio que en ese momento no constituya morada de alguna persona, realizada con cierta vocación de permanencia. 2) Que esta perturbación posesoria pueda ser calificada penalmente como ocupación por su intensidad y vocación de permanencia, por lo que las ocupaciones ocasionales o esporádicas, sin intención de perdurar o de escasa intensidad, son ajenas al ámbito de aplicación del tipo. 3) Que el realizador de la ocupación carezca de título jurídico que legitime esa posesión, pues en el caso de que hubiera sido autorizado para ocupar el inmueble, aunque fuese temporalmente o en calidad de precarista, la acción no debe reputarse como delictiva y el titular deberá acudir al ejercicio de las acciones civiles procedentes para recuperar su posesión. 4) Que conste la voluntad contraria a tolerar la ocupación por parte del titular del inmueble, bien antes de producirse, bien después, lo que especifica este artículo al contemplar el mantenimiento en el edificio "contra la voluntad de su titular", voluntad que, en el presente caso, se manifiesta con la interposición de la correspondiente denuncia y la petición de desalojo que ahora nos ocupa. 5) Que concurra dolo en el autor, que abarca: a) El conocimiento de la ajenidad del inmueble y de la ausencia de autorización, b) La voluntad de afectar al bien jurídico tutelado por el delito, es decir, la efectiva perturbación de la posesión del titular de la finca ocupada.

10. Recuerda el AAP L 2/2024, de 2 de enero, Secc. 1.ª, Ponente: Ilma. Sra. Blat Peris, FJ 2.º "*que no constituye delito de usurpación la ocupación de fincas abandonadas o en estado de absoluta inhabitabilidad, ruinosas, de un solar, o aquellas en las que exista una posesión 'socialmente manifiesta', o el caso de las ocupaciones temporales, transitorias u ocasionales sin vocación de permanencia, como por ejemplo la mera entrada para dormir"* (la cursiva es mía). Está toda la cita en cursiva.

La pena a imponer por la usurpación diferencia de, si se lleva a cabo con violencia y/o intimación, con pena de prisión de 1 a 2 años, pena menos grave. En el supuesto que se lleve a cabo sin violencia y/o intimidación se podrá imponer una pena de multa de 3 a 6 meses, abarcando pena menos grave y pena leve, lo que motiva que. en aplicación del art. 13.4 CP, estaríamos en presencia de un delito leve, elemento cuya trascendencia hay que destacar y que con posterioridad se entenderá el porqué. La tramitación procesal es distinta: si hay violencia y/o intimación su tramitación discurre a través del procedimiento abreviado (arts. 774 y ss., LECRIM) con instrucción judicial previa, si es un delito leve de usurpación pacífica entonces no hay propiamente instrucción (arts. 962 y ss., LECRIM)[11], si bien en ambos cabe redactar un atestado policial.

En suma, es preciso señalar, en relación con la ocupación-usurpación pacífica, que no todo comportamiento destinado a sustraer la titularidad posesoria del bien inmueble implica ya, per se, un hecho ilícito perseguible, teniendo en cuenta que cabe la posibilidad de confrontar dichas actuaciones con las herramientas que la jurisdicción civil[12] prevé, como la denominada acción interdictal. En este sentido, es precisa una permanencia situacional de los investigados[13] que obstaculice el desarrollo

11. Desde sectores institucionales se ha buscado el uso del denominado proceso de aceptación decreto para la persecución del delito leve de usurpación inmobiliaria. *Vid*. Fiscalía General del Estado (2016), p. 808.

12. *Vid.* por su interés, en relación a la tutela civil, Lafuente Torralba, A. J. (2021). El *labyrinthus iudiciorum* de la ocupación ilegal de viviendas: remedios en las vías penal y civil y análisis de su eficacia. *Revista de Derecho Aragonés*, *26-27*, 113-154.

13. Que sistematiza el AAP B 402/2024, de 15 de abril, Secc. 9.ª, Ponente: Ilmo. Sr. Almería Trenco, FJ 2.º: "*No puede reputarse punible cualquier perturbación de la posesión, incluso aquellas que se desarrollen bajo la forma de ocupación, sino solo las ocupaciones que supongan un riesgo para el bien jurídico protegido de la posesión del titular (AP de Cádiz, Sección 8, de 6.10.00 y AP de Las Palmas, Sección 1, de 13.10.00). Conforme a ello, la ocupación punible solo sería aquella en que el ocupante tiene la intención evidente de ejercer derechos posesorios sobre el inmueble ocupado (SAP de Burgos, S, Sección 1, de 17.1.00 y AP de Córdoba, Sección 1, de 9.10.00), lo que se puede poner de manifiesto con la permanencia en la vivienda ocupada. No serían punibles las ocupaciones de fincas abandonadas o ruinosas (SAP de Barcelona, Sección 3, de 16.1.03 y AP de Huelva, Sección 1, de 5.2.04) o de un solar (AP Madrid, Sección*

de la posesión misma que tiene el dueño o titular para integrar el ilícito penal, falta de permanencia que *podría abrir la eventualidad de la posible sanción administrativa*al amparo de la Ley Orgánica de Protección y Seguridad Ciudadana 4/2015, de 30 de marzo (LOPSC) –vigente todavía a la fecha de la redacción de este articulo–, que tipificaría aquellas ocupaciones ocasionales o esporádicas de inmuebles[14] que no constituyan domicilio permanente o estacional, sin vocación de permanencia o de escasa intensidad como "por ejemplo jóvenes que se introducen en un edificio deshabitado o en ruinas para pasar la tarde, (donde) claramente se observa la no voluntad de permanencia"[15], lo que daría lugar a la infracción leve prevista en el art. 37.6 LOPSC y susceptible de ser sancionada con multa de 100 a 600 euros (art. 39.1 LOPSC).

En síntesis, hay un triple escenario destinado a la protección de la titularidad inmobiliaria. El ámbito civil, destinado a tutelar situaciones de tipo contractual o de perturbación posesoria o del derecho real de propiedad no delictivas a dilucidar ante la jurisdicción civil. El ilícito penal, cuando se ataca un bien jurídico protegido penalmente, ya sea con o sin violencia o intimidación, vulnerando la esfera íntima que implica el domicilio o la perturbación inmobiliaria posesoria, con vocación de permanencia, grave y deliberada y con conciencia y voluntad de hacerlo. Finalmente, la

---

16, de 15.4.02) ni aquellas que exista una posesión 'socialmente manifiesta' (SAP de las Palmas, Sección 1.ª, de 13.10.00) Del mismo modo tampoco serían punibles con arreglo a este tipo penal, las ocupaciones temporales, transitorias u ocasionales, como pueden ser las meras entradas para dormir (SAP de Málaga, Sección 2.ª, de 9.10.00), o sin vocación de permanencia (SAP de Barcelona, Sección 5.ª de 14.5.03 y Valencia, Sección 4ª, de 9.5.01)" (la cursiva es mía).

14. Se tipifica "La ocupación de cualquier inmueble, vivienda o edificio ajenos, o la permanencia en ellos, en ambos casos contra la voluntad de su propietario, arrendatario o titular de otro derecho sobre el mismo, cuando no sean constitutivas de infracción penal. Asimismo la ocupación de la vía pública con infracción de lo dispuesto por la Ley o contra la decisión adoptada en aplicación de aquella por la autoridad competente. Se entenderá incluida en este supuesto la ocupación de la vía pública para la venta ambulante no autorizada".

15. *Vid.* la Instrucción 6/2020 de la Secretaría de Estado de Seguridad (SES) por la que se establece el protocolo de actuación de las Fuerzas y Cuerpos de Seguridad del Estado ante la ocupación ilegal de inmuebles.

infracción administrativa, tercer escalón, que comprende perturbaciones posesorias limitadas y temporales no domiciliarias. No obstante, juntamente con el allanamiento de morada, va a ser la usurpación inmobiliaria pacífica figura sobre la que se construye el delito leve de ocupación (art. 245.2 CP), la que va a centrar, mayormente, las reflexiones que a renglón seguido se van a presentar.

3 La investigación policial ante el allanamiento y la usurpación

3.1 Caracteres de la investigación policial

El papel de órgano investigador en el seno de proceso penal español puede ser asumido por la Policía, el Ministerio Fiscal y el Juez de Instrucción. Por lo tanto, se parte de un axioma principal: *la investigación del ilícito penal es de naturaleza oficial y pública*. En este sentido, en el curso de dichas diligencias cabe la adopción de medidas limitativas de derechos fundamentales (privación de libertad, interceptación de comunicaciones, entradas y registros domiciliarios, entre otras) vedadas a la actuación particular y que acentúan, sin duda, aquel singular carácter. No obstante, hay que indicar que la Policía ve limitado, de manera clara, el abanico de medidas conculcadoras de derechos fundamentales que *motu proprio*, sin necesidad de autorización judicial previa, puede acordar. En este sentido, hay que destacar la detención (art. 17.3 CE; arts. 490 y ss., LECRIM), la entrada en domicilio en supuestos de flagrancia delictiva (art. 18.2 CE; arts. 553 y 795.1.1.º LECRIM) y la inspección corporal leve (arts. 15 y 18.1 CE)[16].

La actividad averiguadora de la fuerza policial tiene un ámbito de actuación propio, autónomo, pues interviene sin tener la

16. *Vid.* análisis de estas diligencias, Alfonso Rodríguez (2023), pp. 90-94.

obligación de dar cuenta inmediata a nadie (juez o fiscal)[17] del inicio de la investigación que tiene una naturaleza puramente administrativa que integra o puede integrar una instrucción judicial (*Cfr.* STS 228/2015, de 21 de abril, de la Sala II [Ponente: Excmo. Sr. Martínez Arrieta] FJ 2.º), sin perjuicio de las anteriores medidas limitativas de derechos fundamentales que se pueden acordar en su seno. Pese a ello, la persona sujeta a la investigación policial tiene derecho de defensa ex. arts. 118 y 520 LECRIM[18] como mecanismo reaccional frente a la intromisión en su esfera personal, singularmente en el supuesto de detención con acceso a aquellas diligencias esenciales destinadas a impugnar su situación (*cfr.* SSTC 13/2017, de 30 de enero, FFJJ 5.º a 7.º; 21/2018, de 5 de marzo, FFJJ 7.º a 10.º; 83/2019, de 17 de junio, FFJJ 5.º a 7.º; 180/2020; de 14 de diciembre, FFJJ 2.º a 4.º, y 80/2021, de 19 de abril, FJ 4.º).

Sin embargo, la investigación policial no es ab initio preceptiva, no es un paso inicial obligatorio, pues puede no iniciarse en su sede sino a requerimiento judicial, así el art. 259 LECRIM prevé que "El que presenciare la perpetración de cualquier delito público está obligado a ponerlo inmediatamente en conocimiento del Juez de instrucción, de paz, comarcal o municipal o funcionario fiscal más próximo al sitio en que se hallare, bajo la multa de 25 a 250 pesetas", con lo que parece que el paso por dependencias policiales es más instrumental de la intervención judicial que principal. Asimismo, juntamente con la interposición de denuncia judicial directa, cabe la presentación de querella (art.

17. Como ha señalado la STS 503/2021, de 10 de junio, de la Sala II, Ponente: Excmo. Sr. Magro Servet, FJ 2.º: "e.- *La judicialización de las diligencias de investigación no tiene que producirse tan pronto* se aprecie la existencia de indicios de delito, sino que el límite se encuentra en la necesidad de adoptar medidas que afecten a los derechos fundamentales" (la cursiva es mía).

18. Así la STS 66/2020, 20 de febrero, de la Sala II, Ponente: Excmo. Sr. Martínez Arrieta, FJ Único, indica "En cuanto a la alegación de indefensión, al respecto esta Sala ha dicho (*Cfr.* SSTS 245/2012, de 27 de marzo; n.º 485/2012, de 13 de junio; 27 de septiembre de 2011, n.º 964/2011) que la tutela judicial exige que la *totalidad de las fases del proceso se desarrollen sin mengua del derecho de defensa*, y así la indefensión, para cuya prevención se configuran los demás derechos instrumentales contenidos en el párrafo 2 del art. 24 CE, se concibe con la negación de la expresada garantía (SSTC 26/93 de 25.1 y 316/94 de 28.11)" (la cursiva es mía).

270 LECRIM), también directamente, ante el órgano judicial, y que este decida, en caso de ser competente, la correspondiente incoación de diligencias o actividades de comprobación del hecho denunciado a través de los diferentes procedimientos regulados en nuestra norma procesal o incluso iniciar de oficio una investigación judicial (art. 303 LECRIM). Igualmente, cabe la denuncia ante la Fiscalía, que, en virtud del art. 773.2 de la LECRIM, en relación con el art. 5 Estatuto Orgánico del Ministerio Fiscal (EOMF), puede incoar unas diligencias preprocesales de investigación, con lo que se establece otro mecanismo adicional, sin intervención policial directa, para la indagación de un ilícito (*cfr.* STS 980/2016 de la Sala II, de 11 de enero, [Ponente: Marchena Gómez], FJ 2 A; STC 59/2023, de 23 de mayo, FFJJ 4.º y 5.º).

La actividad policial puede iniciarse de oficio, es decir, por el propio conocimiento de los agentes, en virtud de denuncia (art. 269 LECRIM) que se pudiese formular mediante la aportación de aquellos elementos destinados a una calificación indiciaria ilícita (art. 284.1 LECRIM) o puede desarrollarse por orden judicial en el curso de una instrucción o del Ministerio Fiscal (art. 287 LECRIM), siendo posible también su desarrollo en virtud de información anónima (*cfr.* STS 318/2013, 11 de abril, de la Sala II, Ponente: Excmo. Sr. Marchena Gómez, FJ 2.º con la jurisprudencia que expone). Lo que no cabe es interponer querella en sede policial a los efectos de instar actuaciones indagatorias policiales, aquella solo cabe ante el juez instructor competente (art. 272 LECRIM).· En atención a lo expuesto, la actividad policial de investigación está subordinada a la autoridad judicial (o del Ministerio Público) pues debe cesar una vez se haya abierto una instrucción penal, pero no es una actividad jurisdiccional, ni tampoco produce con carácter general actos de prueba, que solo se producen en sede de juicio ante los órganos de la justicia penal y con arreglo a garantías de inmediación, contradicción, oralidad y publicidad (SSTC 182/1989, de 3 de noviembre, FJ 2.º; 67/2001, de 17 de marzo, FJ 6.º; 195/2002, de 28 de octubre, FJ 2.º; 206/2003, de 1 de diciembre, FJ 2.º; 345/2006, de 11 de diciembre, FJ 3.º; 68/2010, de 18 de octubre, FJ 5.º; 134/2010, de 2 de diciembre, FJ 3.º, y 53/2013, de 28 de febrero, FJ 3.º). Igualmente, la actividad policial tampoco tiene efectos interruptivos de la prescripción del hecho delictivo.

En el desarrollo de sus actividades, por tanto, las fuerzas policiales disponen de determinadas medidas. Por un lado, aquellas que pudieran afectar a los derechos fundamentales de los investigados, juntamente con aquellas de carácter personal que son las declaraciones que se llevan a cabo en sede policial; también estarían la de aseguramiento e identificación de los implicados, con la obtención de datos, archivos informáticos, vestigios, inspecciones corporales leves o la denominada prueba de alcoholemia, y, finalmente, existen las instrumentales tales como la circulación y la entrega vigilada de determinadas sustancias.

3.2. Confección del atestado: diligencias esenciales de investigación

Hay que señalar que la importancia de la investigación policial se realiza en un doble marco. La usurpación inmobiliaria delictiva, no tanto el allanamiento, pese a su levedad punitiva, es, en primer lugar, un problema de seguridad pública como se expuso al inicio de este trabajo, trayendo, en segundo lugar, una lógica deriva procesal y de reacción penal para la tutela de los derechos en juego que tienen como uno de sus actores a las Fuerzas y Cuerpos de Seguridad del Estado. Estas se convierten, de ordinario, en el principal interlocutor de las víctimas de este tipo de hechos y con una posible intervención, cuyos límites vienen determinados por el art. 282 LECRIM cuando señala que

> La Policía Judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial. Cuando las víctimas entren en contacto con la Policía Judicial, cumplirá con los deberes de información que prevé la legislación vigente. Asimismo, llevarán a cabo una valoración de las circunstancias particulares de las víctimas para determinar provisionalmente qué medidas de protección deben ser adoptadas para

garantizarles una protección adecuada, sin perjuicio de la decisión final que corresponderá adoptar al Juez o Tribunal.

Todo esto se traduce en un trabajo de investigación documentado, con reflejo de la realidad fáctica percibida, la adopción de aquellas medidas restrictivas de derechos para las que están habilitados en función de sus propias atribuciones, la garantía de los derechos de las víctimas y, necesariamente, de la persona investigada.

Hay que señalar que, ya se esté en presencia de un allanamiento de morada o de una usurpación pacífica inmobiliaria constitutiva de delito leve, denunciado el hecho la redacción del atestado se convierte en una *exigencia procedimental indeclinable* (AAPB 130/2024, de 6 de febrero, Secc. 9, Ponente: Ilmo. Sr. Sicilia Murillo, FJ 1.º; AAPB 206/2024, de 27 de febrero, Secc. 9, Ponente: Ilma. Sra. Sucias Rodríguez, FJ 9.º; SAPM 447/2018, 7 de junio, Secc. 2.ª, Ponente: Ilma. Sra. Compaired Plo, FJ 4.º) pues representa *el documento inicial, riguroso y objetivo* (STS 78/2021, de 1 de febrero, de la Sala II, Ponente: Excmo. Sr. Marchena Gómez, en su FJ 2.3.º) que, *con valor de denuncia* (SSTC 145/85, de 28 de octubre, FJ 4.º; 22/88, de 18 de febrero, FJ 3.º; 217/89, de 21 de diciembre, FJ 2.º; 51/95, de 23 de febrero, FJ 2.º; 303/93, de 25 de diciembre, FJ 4.º, entre otras), activa el mecanismo de funcionamiento de los actos procesales del órgano judicial, y donde se constatan los hechos adecuados para una calificación jurídica indiciaria y con apoyatura en evidencias documentales que tienen que nutrir la investigación policial.

En atención a los rasgos expuestos infra, los ilícitos que se presentan al conocimiento policial motivan la instrucción del atestado, pero que, por su propia peculiaridad, singularmente la ocupación inmobiliaria, requiere un modo de instruir policialmente teniendo presentes determinados elementos. Así, como apunta la Instrucción 1/2020, de 15 de septiembre, de la Fiscalía General del Estado (FGE)

> se habrá de procurar que el atestado incluya los documentos, declaraciones y cualesquiera otras fuentes de prueba que sirvan al efecto de determinar no solo el título acreditativo de la lesión del derecho invocado por el/la denunciante, sino también las circunstancias espacio-temporales en las que se haya producido la ocupación del inmueble, la identidad y número de los/as posibles autores/as, su eventual estructura organizativa, la finalidad perseguida con la ocupación y cualesquiera otras variables relevantes a los fines de determinar la índole delictiva de los hechos, sus posibles responsables y la calificación jurídica inicial[19].
>
> No obstante esta inicial indicación, hay que ir paso a paso.

Así, la presentación de la denuncia en sede policial determina la declaración de la víctima-perjudicado, que se convierte en el "motor" de la actuación. Hay, por ello, que partir de que la definición de víctima viene determinada por la Ley Estatuto de la víctima del delito 4/2015 (LEVD), de 27 de abril, que define la figura como "toda persona física que haya sufrido un daño o perjuicio sobre su propia persona o patrimonio, en especial lesiones físicas o psíquicas, daños emocionales o perjuicios económicos directamente causados por la comisión de un delito" [art. 2. a)]. Tenemos, por tanto, la víctima, que es la *ofendida directamente*, pero también la perjudicada, es decir, quien sufre daños personales y/o patrimoniales (aunque también su representante

19. En este sentido, la Instrucción 6/2020 de la Secretaría de Estado por la que se establece el protocolo de actuación de las Fuerzas y Cuerpos de Seguridad del Estado ante la ocupación ilegal de inmuebles: "Establecer directrices para que se recojan en los atestados policiales *todos los indicios existentes en relación con los elementos objetivos y subjetivos que conforman los distintos tipos penales relativos a la ocupación ilegal de inmuebles, con la finalidad de aportarlos a las autoridades judiciales competentes para acreditar la comisión del delito y la participación de sus responsables*, y contribuir, cuando ello proceda ante eventuales situaciones de extrema necesidad o especial vulnerabilidad en los ocupadores desalojados, a desencadenar una respuesta ágil de las entidades e instituciones competentes para paliar dichas situaciones" (la cursiva es mía).

puede interponer denuncia igualmente en sede policial), a quien hay que facilitarle, por otro lado, toda la información (art. 5), comprendiendo derechos, prestaciones o asistencia[20]. En todo caso, en estos tipos delictivos las víctimas y/o perjudicados pueden ser personas físicas, jurídicas de carácter público, entidades de utilidad pública sin ánimo de lucro y personas jurídico-privadas que acrediten riesgo de quebranto grave a consecuencia del hecho cometido (Instrucción 1/2020 FGE).

Ya sea el allanamiento, ya la usurpación-ocupación inmobiliaria, la declaración que formula la víctima/perjudicado es clave, por lo que debe motivar una particular atención por parte del agente instructor del atestado. Primero, por la aportación de hechos narrados, elementos de investigación que son claves para desentrañar la calificación jurídica inicial, juntamente con

20. Señala el precepto "a) Medidas de asistencia y apoyo disponibles, sean médicas, psicológicas o materiales, y procedimiento para obtenerlas. Dentro de estas últimas se incluirá, cuando resulte oportuno, información sobre las posibilidades de obtener un alojamiento alternativo. b) Derecho a denunciar y, en su caso, el procedimiento para interponer la denuncia y derecho a facilitar elementos de prueba a las autoridades encargadas de la investigación. c) Procedimiento para obtener asesoramiento y defensa jurídica y, en su caso, condiciones en las que pueda obtenerse gratuitamente. d) Posibilidad de solicitar medidas de protección y, en su caso, procedimiento para hacerlo. e) Indemnizaciones a las que pueda tener derecho y, en su caso, procedimiento para reclamarlas. f) Servicios de interpretación y traducción disponibles. g) Ayudas y servicios auxiliares para la comunicación disponibles. h) Procedimiento por medio del cual la víctima pueda ejercer sus derechos en el caso de que resida fuera de España. i) Recursos que puede interponer contra las resoluciones que considere contrarias a sus derechos. j) Datos de contacto de la autoridad encargada de la tramitación del procedimiento y cauces para comunicarse con ella. k) Servicios de justicia restaurativa disponibles, en los casos en que sea legalmente posible. l) Supuestos en los que pueda obtener el reembolso de los gastos judiciales y, en su caso, procedimiento para reclamarlo. m) Derecho a efectuar una solicitud para ser notificada de las resoluciones a las que se refiere el artículo 7. A estos efectos, la víctima designará en su solicitud una dirección de correo electrónico y, en su defecto, una dirección postal o domicilio, al que serán remitidas las comunicaciones y notificaciones por la autoridad".

una suerte de "principio de prueba" a presentar acerca de la titularidad, la identificación y la situación del bien inmueble[21] que permita determinar las medidas policiales ulteriores a llevar a cabo. Segundo, la declaración sirve para conocer qué tipo de protección es pertinente dispensar[22], singularmente la petición de la medida de desalojo que si bien debería recogerse de

21. En este sentido, con arreglo al LEVD, y de ordinario, la denuncia-declaración, con asistencia lingüística [arts. 6. b) y 9.1 a)] ante la fuerza policial hace comenzar el proceso penal y donde se le reconoce participación activa (art. 3). La denuncia, de la que se le tendrá que facilitar a quien la interponga copia debidamente certificada [art. 6 a)], se nutre de "elementos de prueba a las autoridades encargadas de la investigación" [art. 5. b)] "y la información que estime relevante para el esclarecimiento de los hechos" [art. 11 b)], lo que permite que la víctima del hecho pueda aportar en diligencias policiales cuantos elementos documentales, comunicativos o de cualquier tipo que desee a los efectos de contribuir al desarrollo de las investigaciones policiales, que permita una calificación de los hechos y la identificación de su autor.

22. Así resulta el art. 282 del citado texto legal que establece la necesaria información que debe proporcionarse a la víctima y "Asimismo, llevarán a cabo una valoración de las circunstancias particulares de las víctimas para determinar provisionalmente qué medidas de protección deben ser adoptadas para garantizarles una protección adecuada, sin perjuicio de la decisión final que corresponderá adoptar al Juez o Tribunal", con información de los supuestos de archivo policial si, en el plazo de 72 horas, no se identifica al autor de los hechos (art. 284. 2. II LECRIM), comunicándole la incautación de sus bienes que pudiesen constituir cuerpo del delito (art. 284.4 en relación con el art. 334 LECRIM). Por otro lado, la LEVD exige la necesaria protección que tiene brindarse a las víctimas durante la fase de investigación policial "para garantizar la vida de la víctima y de sus familiares, su integridad física y psíquica, libertad, seguridad, libertad e indemnidad sexuales..." (art. 19), coadyuvando a evitar que se produzca contacto visual con el sospechoso (art. 20); llevando a cabo declaraciones inmediatas, las mínimas imprescindibles para evitar la denominada "victimización secundaria"; viéndose acompañada de una persona de su elección y recibiendo asistencia médica (art. 21); practicando su declaración en dependencias especialmente habilitadas, por profesionales y por la misma persona del mismo sexo (art. 25.1); adoptando medidas de protección de su intimidad como la evitación de filtraciones informativas para impedir una identificación (art. 22); llevando a cabo una evaluación que permita verificar qué tipo de medidas de protección serán adecuadas para la persona (arts. 23 y 24) teniendo en cuenta determinados tipos delictivos, lo que obliga a llevar a cabo una calificación inicial jurídica.

manera expresa, nada impide al juez acordarla de oficio[23]. Tercero, adicionalmente a su declaración, la diligencia policial con participación de la víctima implica el ámbito de información para el ejercicio de sus derechos (arts. 109 y 110 en concordancia con el art. 771.1.º LECRIM) a los efectos de poder mostrarse parte en el seno del procedimiento para ejercer las acciones penales y civiles que le correspondan, junto con la posibilidad de nombrar abogado, pudiendo recibir asistencia jurídica gratuita, tomar conocimiento de la causa e instar lo que le convenga, pudiendo verse sustituida en el ejercicio de las acciones por el Ministerio Público.

Si hay algo relevante, es la determinación, además de los hechos, de la titularidad del bien inmueble mediante la aportación de aquellos elementos documentales que lo justifiquen. Ya sea en el allanamiento, ya sea en la usurpación-ocupación inmobiliaria, la justificación de la titularidad puede llevarse a cabo mediante certificación registral firmada electrónicamente por el registrador mismo con su código seguro, verificación que acredita la titularidad[24] y, por tanto, la legitimación que, como perjudicado, tiene la persona que denuncia, quien, a su vez, puede impetrar la protección cautelar y exigir el desalojo del inmueble. Con ello, satisface ese "principio de prueba" que permite actuar con arreglo a las exigencias que ha impuesto la LECRIM. Por tanto, además de su declaración es preciso requerir, sin perjuicio de su aportación motu proprio, documentos acreditativos de la titularidad que dice ostentar, algo que igualmente es preciso para una adecuada identificación del inmueble que conforma la investigación.

Reviste especial trascendencia, y singularmente en la usurpación inmobiliaria pacífica, la denuncia en lo que respecta a

23. Como señala la AAPM 348/2017, de 4 de mayo, Secc. 29, Ponente: Ilma. Sra. Rasillo López, FJ 1.º: "Es verdad que la medida de desalojo no ha sido solicitada por la propietaria de la vivienda, que ni siquiera era conocedora de la ocupación, más en nuestro ordenamiento procesal tan solo la medida cautelar de prisión provisional y de libertad con fianza están sometidas a la petición de parte, pudiendo adoptarse de oficio las demás medidas cautelares, como es la que nos ocupa".

24. *Vid.* Instrucción 1/2020, de 15 de septiembre, FGE; Instrucción 6/2020 SES. No cabe ser maximalista, podría servir, por ejemplo, una nota simple procedente del Registro de la Propiedad (AAPL 140/2024, 1 de marzo, Secc. 1.ª, Ponente: Ilma. Sra. Juan Agustín, FJ 2.º).

aquellos inmuebles cuya titularidad ostenta una persona jurídica de naturaleza privada como un banco, entidad financiera, cooperativa de crédito o semejante. En este sentido, si quien formula la denuncia lo lleva a cabo como representante legal, es decir, como administrador o empleado que goza de poder formalizado para ello en documento notarial y en interés de dicha persona jurídico-privada, es importante que acredite tal condición y ello mediante la aportación de aquella documental pertinente, sin perjuicio de que cualquier persona que es conocedora de la comisión de un hecho delictivo debe formular denuncia (art. 259 LECRIM). En todo caso, debe demostrar los datos de titularidad e identificación del bien[25]. Si fuera una persona jurídica pública (cualquier Administración o sector público institucional)[26] debería formular denuncia aquella persona que efectivamente tenga funciones de representación y con relación al bien que pertenece a la esfera de la titularidad pública (*v. gr.* alcalde, responsable autonómico o estatal o funcionario encargado) o sus servicios jurídicos a su requerimiento.

Hay un aspecto trascendente de la declaración de la denunciante, singularmente en lo que respecta a la ocupación-usurpación pacífica, que debe recogerse en el atestado, que implica saber si la vivienda o inmueble ha sido objeto de alquiler o venta, o si lo está, identifique, por si pudiera haber coincidencia subjetiva con los investigados, a los inquilinos, si dicha vivienda o inmueble ha sido cedido y quiénes son los cesionarios, si existen otros derechos sobre la vivienda sometidos a controversia judicial y si quienes resultan ser denunciados los poseen (*vid.* problemas hereditarios, comerciales...). Igualmente, es importante saber cuándo han ocurrido los hechos, el tiempo que la/s persona/s denunciadas llevan en dicha situación, lo que es necesario para valorar el grado de permanencia existente que descarte la transitoriedad de la situación, junto con los elementos que permitan determinar si existe abandono o no de la propiedad, la situación de habitabilidad con descripción de los suministros de los que disponga o una posible

25. Algún autor ha señalado el uso por parte de las entidades financieras del proceso penal como mecanismo de tutela más rápida de sus intereses inmobiliarios. Será criticable, o no, pero es perfectamente legal. *Vid.* Ríos Martin, 2021, pp. 121-122.

26. *Vid.* art. 2 de la Ley 40/2015, de 1 de octubre.

situación de ruina de la vivienda o inmueble. Es preciso, si es posible, obtener de la persona denunciante datos referidos a los daños existentes o los perjuicios que dicha situación le está causando, acompañando aquellos elementos documentales que sirvan para verificarlos.

Juntamente con la declaración de la víctima, es clave la *identificación de la/s persona/s investigada/s*, ya como autor/es del allanamiento, ya como ocupante/s del inmueble (*cfr.* AAP B 402/2024, de 15 de abril, Secc. 9.ª, Ponente: Ilmo. Sr. Almería Trenco, FJ 4.º; AAP B 1165/2023, 12 de diciembre, Secc. 3.ª, Ponente: Ilma. Sra. Sánchez Gil, FJ 2.º; AAPGR 666/2023, 26 de octubre, Secc. 2.ª, Ponente: Ilmo. Sr. Sánchez Jiménez, FJ 2.º), con lo que es preciso que o bien la propia denunciante facilite los datos, si dispone de ellos, o que por propia intervención de los agentes se lleve a cabo dicha identificación- filiación, algo que no es incompatible con una tramitación sencilla que configura en sus contornos el enjuiciamiento de un delito leve en el supuesto de ocupación-usurpación.

En el caso del allanamiento, pero es algo que es perfectamente posible en el supuesto de ocupación, el *interrogatorio del sospechoso/s* es una diligencia que también se practica por parte de la fuerza policial, situación que se produce cuando se imputa la presunta comisión de un hecho delictivo, convirtiéndose en un marco de derechos propios (arts. 118 y 520 LECRIM) como mecanismo de reacción frente al *estatus policial otorgado*[27], juntamente con el acceso a los elementos esenciales de las diligen-

27. A la luz del art. 118 LECRIM le corresponden una serie de derechos que resultan fundamentales en el marco de las diligencias policiales de investigación a aquella persona a la que se le imputa un hecho delictivo sin ser detenido, en cuyo caso se le aplicarían las matizaciones del art. 520 LECRIM. Así, procede la información acerca de los *hechos* que le son objeto de imputación policial que le será facilitada con el suficiente detalle para ejercer el derecho de defensa [art. 118.1 a)], pudiendo examinar las actuaciones con antelación suficiente [art. 118.1 b)], el reconocimiento del ejercicio del derecho de defensa en la totalidad del proceso penal [art. 118.1 c)], a la designación de abogado y a la asistencia jurídica gratuita [art. 118.1.d y e)], derecho a traductor e intérprete como elemento esencial de comprensión [art. 118.1 f)] y derecho al silencio total o parcial, a no declarar o a no confesar [art. 118. 1 g y h)].

cias para impugnar su detención (STC 21/2018, de 5 de marzo, FJ 8.º), y poder impetrar el hábeas corpus (STC 61/2003, de 24 de marzo, FJ 2.º), siendo importante la existencia de documentación donde se refleje denuncia o el resultado de la intervención policial (*cfr.* STC 13/2017, 30 de enero, FJ 7.º), junto con la previsión de "Entrevistarse reservadamente con el detenido, incluso antes de que se le reciba declaración por la policía, el fiscal o la autoridad judicial, sin perjuicio de lo dispuesto en el artículo 527" que consagra el derecho de defensa en el marco de las diligencias policiales.

Esa identificación del investigado, y preservar su derecho de defensa en todas las fases, es capital para articular adecuadamente el procedimiento de desalojo que se analizara posteriormente y la efectividad de dicha medida cautelar. Sin embargo, hay una cuestión que resulta adicional a la identificación, correlativamente con la aportación por el denunciante, que es la necesidad de conocer si quien presuntamente allana u ocupa dispone de título (o situación) justificativo[28] de su posición (propiedad, arrendamiento, precario...), algo trascendente a posteriori para la instrucción judicial en tanto que podría motivar la apertura del procedimiento o su archivo por atipicidad. Por tanto, estos hechos justificativos pueden tener una doble procedencia: del denunciante o del sospechoso. E, igualmente, resulta importante conocer su grado de vulnerabilidad, por si fuesen personas "dependientes", víctimas de violencia de género o pudieran existir menores de edad, que determine una intervención posterior de la

28. Nada impide un acceso consentido engañoso que luego se puede tornar en una ocupación delictiva. Como ha señalado la AAPC 625/2023, 4 de octubre, Secc. 2.ª, Ponente: Ilma. Sra. Taboada Caseiro, en su FJ 1.º: "Por ello reiterar que concurren indicios suficientes toda vez que se ha producido la ocupación de la vivienda mediante engaño y con vocación de permanencia *como se ha constatado no se llegó a firmar ese contrato de arrendamiento, no efectuó la investigada esos pagos con respecto a los que exhibió al denunciante unos resguardos relativos a que se habían realizado las transferencias para el pago de fianza y renta* del arrendamiento, lo que no se produjo en ningún momento y continuó en la vivienda sin efectuar pago alguno" (la cursiva es mía).

Administración autonómica y local competente[29] destinada a llevar a cabo una intervención posterior tuitiva de dichas personas.

Las *declaraciones de testigos* también se practican e incorporan en el atestado infiriéndose del art. 293 LECRIM cuando establece que "Las personas presentes, peritos y testigos que hubieren intervenido en las diligencias relacionadas en el atestado serán invitadas a firmarlo en la parte a ellos referente. Si no lo hicieren, se expresará la razón". En este sentido, los testigos, que deberán de ser filiados e identificados, cuya veracidad en sus manifestaciones no resulta impuesta pues cabe mentir en calidad de testigo a la fuerza policial, deben arrojar datos sobre los hechos, informar sobre los elementos delictivos objeto de investigación, aportar aspectos exculpatorios o inculpatorios o ayudar a delimitar líneas de indagación policial. Fundamentalmente, en estos hechos resultan importantes las declaraciones de los vecinos de inmueble que, sin duda, por su proximidad pueden arrojar datos relevantes sobre la permanencia de los presuntos autores de los hechos. También es importante la declaración de los vigilantes de seguridad del inmueble o de los viandantes presentes en los supuestos de usurpación-ocupación, cuyas manifestaciones deberán constar en el atestado.

En la investigación de estos delitos, cabe la práctica de la *inspección ocular*, una vez formulada la denuncia al amparo del art.

29. Señala la disposición adicional séptima de la Ley de Enjuiciamiento Civil 1/2000 (LEC), de 7 de enero: "En los procedimientos penales que se sigan por delito de usurpación del apartado 2 del artículo 245 del Código Penal, en caso de sustanciarse con carácter cautelar la medida de desalojo y restitución del inmueble objeto del delito a su legítimo poseedor y siempre que entre quienes ocupen la vivienda se encuentren personas dependientes de conformidad con lo dispuesto en el apartado 2 del artículo 2 de la Ley 39/2006, de 14 de diciembre, de Promoción de la Autonomía Personal y Atención a las personas en situación de dependencia, víctimas de violencia sobre la mujer o personas menores de edad, se dará traslado a las Administraciones Autonómicas y locales competentes en materia de vivienda, asistencia social, evaluación e información de situaciones de necesidad social y atención inmediata a personas en situación o riesgo de exclusión social, con el fin de que puedan adoptar las medidas de protección que correspondan. Las mismas previsiones se adoptarán cuando el desalojo de la vivienda se acuerde en sentencia".

282 LECRIM, que implica acudir y si es posible desarrollar un examen del lugar de los hechos investigados; circunstancias concurrentes en su comisión; daños ocasionados (SAPM 800/2019, de 10 de diciembre, Secc. 23, Ponente: Ilmo. Sr. Berges de Ramón, FJ 2.º); posibles defraudaciones en fluidos eléctricos, agua o gas[30], y otras evidencias que impliquen vocación de permanencia en el inmueble[31], documentándose la intervención en un acta; si bien la jurisprudencia ha señalado: "Así no son documentos, recuerda la S. 1532/2004 de 22.12, los atestados policiales, las actuaciones de las partes que constan por escrito en el procedimiento y las resoluciones judiciales, y si bien con carácter excepcional *se ha admitido* el *valor documental del acta que refleja la diligencia de inspección ocular, y reconstitución de hechos, solo lo es en cuanto a los datos objetivos que en ella se contienen*, pero no en relación con las manifestaciones que allí consten (SSTS. 4.3.86, 17.1.92, 22.7.96, 23.1.98)..." (STS 468/2020, de 23 de septiembre, de la Sala II, Ponente: Excmo. Sr. Magro Servet, FJ 23)[32]. La inspección ocular debería implicar no solamente aquellas manifestaciones de los agentes que la practiquen, sino igualmente contener aquellos soportes fotográficos o audiovisuales

30. En este sentido, AAPT 19/2024, de 12 de enero, Secc. 2, Ponente: Ilma. Sra. Calvo González, FJ 2.º, indica: "Respecto a la posible defraudación del fluido eléctrico, *la denuncia carece del más mínimo elemento acreditativo de dicho extremo*, señalando que puesto que los suministros estaban dados de baja, los ocupantes 'han podido realizar conexiones ilegales a tales suministros' para luego, aprovechando tal razonamiento aportar diversas noticias respecto a incendios causados en viviendas ocupadas por 'enganche eléctrico' pretendiendo así la medida cautelar de desalojo. Sin entrar a cuestionar en este momento procesal la legitimación de la parte recurrente respecto a un delito del art. 255 CP –cuando además la Fiscalía se muestra conforme con el archivo–, *la mera hipótesis –porque así se formula– sin indicación de la fuente de conocimiento y huérfana de todo sustento indiciario, no permite tampoco la incoación de un procedimiento prospectivo para la persecución de un delito de defraudación del fluido eléctrico*" (la cursiva es mía).

31. *Vid.* Instrucción 6/2020 SES.

32. La cursiva es mía.

obtenidos en espacios públicos[33] pertinentes que permitan apreciar la situación en la que se encuentra el inmueble y la comisión del hecho delictivo, en cuanto reflejan una realidad concreta en el momento en que se instruye el atestado, preconstituyendo elementos indiciarios poderosos.

Hay que señalar que aun pudiéndonos encontrar en presencia de un delito leve, en el caso de la usurpación-ocupación, esto no es incompatible con un trabajo policialmente exhaustivo cuyo resultado tiene que ser un atestado completo en la medida de las posibilidades y disponibilidades de los agentes que desarrollan la instrucción de los hechos. Sobre todo, y teniendo en cuenta que se puede impetrar una medida como es la de desalojo del inmueble, precisamente para tutelar adecuadamente los derechos en juego, ya sea del denunciante, ya sea de los denunciado/s, es precisa una labor policial profunda, incorporando todos los elementos indiciarios que habiliten para una adecuada decisión judicial, no ya para resolver la medida cautelar, sino para la continuación del proceso mismo.

3.3. El desalojo como acto-policía ¿y la detención?

La alerta que necesariamente estos hechos provocan requerían de una respuesta prácticamente inmediata, comprendiendo mecanismos de reacción que obligasen al desalojo, situación que

33. Como ha señalado la STS 99/2020, de 10 de marzo, de la Sala II (Ponente: Excmo. Sr. Sánchez Melgar), FJ 2.º: "La doctrina jurisprudencial de esta Sala (Sentencias de 6 de mayo de 1993, 7 de febrero, 6 de abril y 21 de mayo de 1994, 18 de diciembre de 1995, 27 de febrero de 1996, 5 de mayo de 1997, 968/1998 de 17 de julio, 188/1999, de 15 de febrero, 1207/1999, de 23 de julio, 387/2001, de 13 de marzo, 27 de septiembre de 2002, y 180/2012 de 14 de marzo, entre otras muchas), ha considerado legítima y no vulneradora de derechos fundamentales la filmación de escenas presuntamente delictivas que suceden en espacios o vías públicas, *estimando que la captación de imágenes de actividades que pueden ser constitutivas de acciones delictivas se encuentra autorizada por la ley en el curso de una investigación criminal, siempre que se limiten a la grabación de lo que ocurre en espacios públicos* fuera del recinto inviolable del domicilio o de lugares específicos donde tiene lugar el ejercicio de la intimidad" (la cursiva es mía).

acaba con la situación ilícita permanente que los hechos examinados generan. Y para ello, efectivamente, se arbitran mecanismos de expulsión, por un lado, a llevar a cabo policialmente y, por otro, el desalojo judicial a la vista del atestado y tras la práctica de una serie de actos procesales de cierta trascendencia. En este sentido, en el allanamiento, su naturaleza de delito menos grave nos conduce a practicar una instrucción judicial, aunque el paraguas de desarrollo sea la LOTJ, siendo la cuestión del delito leve de usurpación-ocupación pacífica la que entraña mayores dudas al no existir, propiamente, una actividad instructora por parte de los jueces en este tipo de hechos[34].

En todo caso, no cabe avalar, y ello por cuanto no entra dentro del marco legal, que los ocupantes tengan derecho alguno fruto de su conducta. Es decir, el ilícito penal no legitima a los ocupantes frente al sujeto pasivo del delito, de manera que no existe fundamento que haga nacer titularidad alguna en beneficio del usurpador. En este sentido, la STC 32/2019, 28 de febrero, en su FJ 5.º señala:

> Valga recordar en este sentido que, como ya ha declarado este Tribunal en relación con el derecho a la libertad de residencia que reconoce el art. 19 CE –doctrina que es trasladable al supuesto que nos ocupa, en cuanto a la protección de la inviolabilidad del domicilio garantizada por el art. 18.2 CE–, *«el derecho a la elección de residencia no es un derecho absoluto que habilite a ocupar cualquier vivienda o espacio, sino que, como el resto de los derechos, ha de ejercerse dentro del respeto a la ley y a los derechos de los demás, que, como*

34. Como señala el AAPB 402/2024 402/2024, de 15 de abril, Secc. 9.ª, Ponente: Ilmo. Sr. Almería Trenco, FJ 4.º: "Cabe, y así lo viene declarando la jurisprudencia mayoritaria, en este tipo de procedimientos penales, *la práctica de una pequeña y sencilla instrucción judicial preparatoria*, y que puede comprender, sin duda alguna, la averiguación de la identidad de los presuntos ocupantes no autorizados, sin que, desde luego, deba cargarse a la propia parte denunciante con el deber de dicha identificación ya en su denuncia cuando es lo cierto, como ocurre en este caso, que ni siquiera la parte ha podido acceder al interior de su vivienda por haberse cambiado la cerradura" (la cursiva es mía).

> *expresa el art. 10.1 CE, son fundamento del orden político y de la paz social»* (STC 160/1991, FJ 11). De este modo, para *habitar lícitamente en una vivienda es necesario disfrutar de algún derecho*, cualquiera que sea su naturaleza, que habilite al sujeto para la realización de tal uso del bien en el que pretende establecerse. Por ello, que la libre elección de domicilio forme parte del contenido de la libertad de residencia proclamada en el art. 19 CE, en modo alguno justifica conductas tales como «invadir propiedades ajenas o desconocer sin más legítimos derechos de uso de bienes inmuebles» (STC 28/1999, de 8 de marzo, FJ 7, y ATC 227/1983, de 25 de mayo, FJ 2)[35].

Por tanto, procede desafiar aquellas noticias falsas que hablan de un determinado período de tiempo en el que los ocupantes –o los allanadores– se ven respaldados por su permanencia y se desviste de todo derecho al legítimo titular[36]. No existe tal aval legal, no hay apoyatura normativa alguna, de manera que son comportamientos en los no cabe que el mero transcurso del tiempo convierta lo que es ilegal en legal[37]. Es preciso, para ello, habilitar medios de reacción inmediata que permita una intervención policial eficaz.

---

35. La cursiva es mía.

36. Como señala la SAP B 361/2020, 7 de septiembre, Secc. 9, Ponente: Ilma. Sra. Tejero Seguí, FJ 6.º "Asimismo, resulta preciso declarar *que la okupación no es un derecho y no puede ni deben tolerarse* ni abrirse sonrojantes e hirientes espacios de impunidad que dificulten el acceso a una vivienda o local por parte de familias propietarias o tenedores de inmuebles, ya que la realidad sociológica de la ocupación ilegal no legitima a nadie, con la legislación vigente, a ocupar una vivienda o local ajeno..." (la cursiva es mía).

37. No faltan algunos pronunciamientos que no comparto que hablan de una suerte de protección de un derecho a la intimidad domiciliaria, a la privacidad, de los ocupantes. Así, SAP T 276/2017, de 13 de julio, Secc. 4.ª, Ponente: Ilmo. Sr. Hernández García, FJ 3.º: "Insisto, la ocupación ilegítima no dará a los ocupantes derecho a seguir poseyendo frente a la reclamación del legítimo tenedor o propietario cuando el juez así lo decida. *Pero mientras dure y los ocupantes hayan convertido la vivienda en morada la Constitución les protege frente a ataques de terceros no legitimados* contra su derecho a la privacidad" (la cursiva es mía).

El sentido del desalojo, singularmente en el supuesto de usurpación-ocupación, busca tutelar la efectividad del derecho de posesión que se ve claramente conculcado por la conducta delictiva, de tal manera que, como ha señalado la Instrucción 1/2020, de 15 de septiembre, de la FGE:

> Tratándose del delito leve de usurpación pacífica de bienes inmuebles del art. 245.2 CP, la adopción de la medida cautelar de desalojo y restitución del inmueble resultará adecuada cuando el sujeto pasivo sea una persona física, una persona jurídica de naturaleza pública o una entidad sin ánimo de lucro de utilidad pública, siempre que se constate que la concreta usurpación, además de lesionar el ius possidendi de la víctima (derecho a poseer que se ostenta sobre un bien que, no obstante, es poseído materialmente por otro), pudiera producir una grave quiebra del ius possessionis (tenencia material y concreta sobre el bien).

No obstante, hay una cuestión preliminar importante antes de llegar al desalojo judicial, y es la procedencia de la intervención policial en este sentido y bajo el presupuesto de la flagrancia delictiva. Se genera, así, un interesante debate sobre si la propia autoridad de los agentes juntamente con el consentimiento del titular podría habilitar al desalojo policial, algo que solo tiene sentido siempre que estemos en presencia de un hecho delictivo. Para ello, hay que tener en cuenta la diligencia limitativa de derechos fundamentales que es la detención (arts. 490 y 492 LECRIM) del investigado policial cuando los hechos que se le presentan al agente son *indiciariamente constitutivos de delito, pero además, existen, también, indicios de participación del sujeto en ese delito*, es decir, un supuesto de detención "en caliente", pues el policía interviene porque se ha cometido un hecho delictivo, ya sea inmediatamente o con posterioridad.

En este sentido, el *allanamiento de morada* habilita para la práctica de la detención pues es un delito menos grave y, por tanto, a la vista de los indicios existentes se puede acceder al domicilio con autorización del dueño y con ello desalojar, fruto de la detención misma, a quienes en ella se encuentren. Por tanto, el tema del desalojo, en este supuesto, se ve más bien embebido

por la cuestión de la detención que deja sin sentido plantearse la duda. Sin embargo, es posible que se practique el desalojo y, sin embargo, no se tome la decisión de practicar la detención por la intervención policial en supuestos de delito in fraganti[38], habilitándose la entrada en el domicilio en virtud del art. 553 LECRIM y el art. 18.2 CE[39], lo que precisa "la inmediatez de la acción delictiva, la inmediatez de la actividad personal, y la necesidad de urgente intervención policial por el riesgo de desaparición de los efectos del delito" y como en este sentido establece la STS 399/2018, 12 de septiembre, de la Sala II, Ponente: Excma. Sr. Ferrer García, FJ 7.º:

> En este sentido, ha señalado el TC que mediante la noción de flagrante delito, la Constitución no ha apoderado a las fuerzas y cuerpos de seguridad para que sustituyan con la suya propia la valoración judicial a fin de acordar la entrada en domicilio, sino que ha considerado una hipótesis excepcional en la cual, por las circunstancias en las que se muestra el delito, se justifica la inmediata intervención de las fuerzas y cuerpos de seguridad (STC 341/1993 de 18 de noviembre, FJ 8) *a los efectos de evitar «que el seguimiento del trámite conducente a la obtención de aquella autorización judicial pueda ser susceptible de ocasionar la frustración de los fines que dichos funcionarios están legal y constitucionalmente llamados a desempeñar en*

38. Señala el art.795.1.1.º LECRIM su definición, así "A estos efectos, se considerará delito flagrante el que se estuviese cometiendo o se acabare de cometer cuando el delincuente sea sorprendido en el acto. Se entenderá sorprendido en el acto no sólo al delincuente que fuere detenido en el momento de estar cometiendo el delito, sino también al detenido o perseguido inmediatamente después de cometerlo, si la persecución durare o no se suspendiere mientras el delincuente no se ponga fuera del inmediato alcance de los que le persiguen. También se considerará delincuente in fraganti aquel a quien se sorprendiere inmediatamente después de cometido un delito con efectos, instrumentos o vestigios que permitan presumir su participación en él".

39. *Vid.* Gimeno Sendra, Moreno Catena, Cortes Domínguez (1999), pp. 423-424; Moreno Catena, Cortes Domínguez (2017), p. 272. En este sentido, la Instrucción SES 6/2020 "Para posibilitar el desalojo de los ocupantes por propia autoridad de los agentes, *resulta fundamental acreditar la existencia de flagrancia delictiva*". La cursiva es mía.

> *la prevención del delito, el aseguramiento de las fuentes de prueba y la detención de las personas presuntamente responsables» (STC 94/1996 de 28 de mayo)*. Y precisó esta última resolución los fines de los que puede predicarse la urgencia, *que son impedir la consumación del delito*, detener a la persona supuestamente responsable del mismo, proteger a la víctima o, por último, evitar la desaparición de los efectos o instrumentos del delito. *En definitiva, la injerencia en el derecho que proclama el artículo 18,2 CE estuvo amparada en un supuesto de flagrancia delictiva, por lo que el motivo planteado necesariamente ha de decaer*[40].

La cuestión se torna más compleja cuando se trata de la *usurpación-ocupación leve*, en la que la detención no está permitida apriorísticamente, si bien es posible ordenarla judicialmente para, por ejemplo, identificar a los autores del hecho delictivo que resueltamente se oponen a colaborar para su citación[41], recordando,

40. La cursiva es mía.

41. En este sentido, la Instrucción SES 6/2020 indica: "En relación con la práctica de la detención, se atenderá a lo previsto en el apartado 4.2.1.2, significándose que si estamos en presencia del artículo 245.2 CP, al tratarse de un delito leve, *no cabe la detención*, a no ser que el presunto reo no tuviese domicilio conocido ni diese fianza bastante (artículo 495 LECrim.)" (la cursiva es mía). Sin embargo, como apunta el AAPB 61/2024, de 19 de enero, Secc. 7, Ponente: Ilma. Sra. Calvo López FJ Único: "Tenemos identificado por la actuación de la empresa contratada por la propiedad a un morador, de nombre Cipriano, que pretende eludir su filiación a manos de la Fuerza Pública evitando el dar cumplimiento a las legítimas órdenes cursadas por el Instructor a aquélla para que proceda a su identificación. *Y la ausencia total de colaboración en relación a este extremo por parte del infractor no ha de impedirla. Para ello existen los archivos policiales y las bases de datos de reseñas decadactilares. Se trata pues de aprehender al sujeto mediante la correspondiente orden de detención, que puede muy bien dictarse atendida la evidente voluntad obstativa constatada frente a la actuación de la Fuerza Pública hasta el momento y de obtener, tras dicha detención (que si ha de verificarse en el interior de un domicilio puede apoyarse en el concepto de flagrancia en la comisión delictiva o bien en una orden judicial debidamente motivada de entrada, si se estima que no se dan las condiciones para justificar la ausencia de orden/consentimiento del morador) su filiación completa*. Los artículos 368 y ss., 486 y ss., 489 y ss. y 545 y ss. LECrim proporcionan la base para adoptar *medidas coercitivas* dirigidas a conseguir la identificación y filiación del/de los/as autores/as del hecho delictivo denunciado y aún posibles en el caso de autos" (la cursiva es mía).

por otro lado, que la fianza policial no existe, y siendo evidente que no dispone de domicilio pues, precisamente por ello, lleva a cabo la usurpación-ocupación leve. Por tanto, en este supuesto, el desalojo policial por propia autoridad únicamente procedería en los supuestos de flagrante delito, no en otros supuestos cuando se han denunciado los hechos una vez ha transcurrido un plazo de tiempo relativamente importante, cobrando en este supuesto sentido la intervención judicial al amparo del art. 13 LECRIM como examinaremos.

En todo caso, pese a que no cabe la detención en un delito leve, nada impide la penetración en el domicilio en esos supuestos de flagrancia delictiva como antes se puso de manifiesto. Y, por tanto, habría desalojo sin detención. Para ello, los agentes podrían intervenir incluso mediante una denuncia verbal en la que quedara clara, en primer lugar, la comisión del hecho delictivo que se puede evidenciar a través de hechos exteriores tales como la ruptura de elementos-barrera como puertas, ventanas, cerraduras, su forzamiento que evidencia acceso o incluso su sustitución. Pero, en segundo lugar, la necesidad de una acreditación de titularidad, algo que incluso se puede clarificar indiciariamente mediante manifestación de quien denuncia y de testigos que evidencien dicha titularidad sin soporte documental. En este sentido, es la conjunción de la flagrancia delictiva apreciada por los agentes y la acreditación de la titularidad incluso por medios indirectos –testigos– la que puede motivar el acceso domiciliario en un delito leve. Así la SAPM 136/2023, de 28 de febrero, Secc. 6.ª, Ponente: Ilma. Sra. López Candela, FJ 2.º:

> Así las cosas, resulta que en el supuesto sometido a nuestra consideración la propietaria denunció que suele visitar el domicilio en cuestión en el que no reside; que el 26 de marzo fue a comprobar su estado y no pudo acceder porque *la cerradura estaba forzada por lo que llamó a un cerrajero para cambiarla y que, al día siguiente, volvió a la vivienda y observó que la cerradura había sido sustituida por otra, el marco de una ventana y la reja arrancada y el cristal fracturado por lo que no cabe duda alguna que estamos ante un*

> *delito flagrante* en los términos expuestos y, por tanto, la entrada de los agentes en el domicilio no precisaba de autorización judicial. En otro orden de cosas, el hecho de que en el momento en que entraron los agentes no se contara con documentación acreditativa del inmueble en cuestión no constituye ningún óbice para su entrada en él pues ha quedado probado que dichos agentes, antes de su entrada, *hablaron con dos vecinos de la perjudicada quienes les manifestaron que Dña. Susana era la propietaria del mismo lo que unido a que la hija de aquélla interpusiera la correspondiente denuncia*, no se les ofreció duda alguna de que la requirente de su presencia era la propietaria y que se estaba cometiendo un delito flagrante[42].

Hay un supuesto que no deja de ser problemático que implicaría la posible existencia de un delito leve de usurpación en el que el inmueble pudiera ser utilizado para la comisión de delitos menos graves o graves. Pensemos, por ejemplo, en el desarrollo continuado de tráfico de drogas, inmigración ilegal o prostitución forzada en el marco de hechos cometidos por organizaciones o grupos criminales. Pues bien, en estos casos, es licito pensar que los delitos menos graves o graves absorben *en el aspecto de la investigación al mero delito leve de usurpación-ocupación* y ello por cuanto el conjunto de medidas que habilitan para la represión de estas conductas es mayor (*vid*. gráficamente la interceptación de las comunicaciones, vigilancias sistemáticas, geolocalizaciones). Esta situación, por claro sentido estratégico, podría motivar un no desalojo fruto de la instrucción de diligencias policiales por la comisión de un delito leve por cuanto pudiera frustrar la investigación de hechos mucho más graves juntamente que trajeran la desarticulación de estructuras organizadas. Es decir, paradójicamente, podría no interesar llevar a cabo un desalojo o una detención inmediata y sí una investigación policial completa dentro, previsiblemente, de una instrucción penal desarrollada por la autoridad judicial,

42. La cursiva es mía.

con lo que habría que pensar en clave procesal y garantista y no desde una perspectiva de tutela policial inmediata[43].

4 El desalojo como "medida" cautelar: participación policial

El atestado policial elaborado bajo las premisas anteriores reviste una importancia esencial cuando no cabe actuar de manera inmediata y practicar, por tanto, detenciones y desalojo. Viene a ser el dispositivo que puede activar la autorización judicial ante una solicitud de intervención policial destinada a restaurar la situación previa a la comisión del ilícito. En este sentido, la función de la autoridad judicial implica la adopción de medidas de protección que amparen a las víctimas de un hecho delictivo y efectivamente, juntamente con el desalojo policial, se sitúa la expulsión de naturaleza judicial. Su fundamento tiene origen en el art. 13 LECRIM que señala:

> Se consideran como primeras diligencias la de consignar las pruebas del delito que puedan desaparecer, la de recoger y poner en custodia cuanto conduzca a su comprobación y a la identificación del delincuente, la de detener, en su caso, a los presuntos responsables del delito, y la de proteger a los ofendidos o perjudicados

43. Sobre esto señala la Instrucción SES 6/2020: "Concretamente, para combatir la proliferación de actividades de ocupación ilegal promovidas por grupos criminales, especialmente aquellos que aprovechan el movimiento de migrantes a los que se promete un trabajo temporal y alojamiento a bajo coste en nuestro territorio (viviendas vacías que son localizadas por los grupos criminales para ocuparlas ilegalmente y ofrecerlas a los migrantes a cambio de una renta económica), se reforzará la coordinación en el ámbito nacional con las unidades de investigación sobre crimen organizado y otras especializadas en extranjería y fronteras, y se explotarán los canales de cooperación policial internacional con las autoridades de los países afectados...". Da la sensación de un intento de desarrollo de una investigación más compleja incompatible, necesariamente, con una intervención inmediata, algo que parece, sin embargo, no compartir la Instrucción 1/2020 de la Fiscalía que habilita la solicitud a la vista del atestado, y por parte de la Fiscalía, del desalojo.

> por el mismo, a sus familiares o a otras personas, pudiendo acordarse a tal efecto las medidas cautelares a las que se refiere el artículo 544 bis o la orden de protección prevista en el artículo 544 ter de esta ley.

En todo caso, cabe su uso tanto en el allanamiento, como en la usurpación pacífica pese a su carácter de delito leve y carecer propiamente su tramitación de instrucción judicial.

El art. 13 LECRIM, por tanto, puede considerarse una suerte de habilitador general para la adopción de medidas cautelares *innominadas*, entre ellas, el desalojo que, por cierto, no está contemplado expresamente en la LECRIM como tal cautelar[44]. Es decir, su adopción se infiere en abstracto como herramienta de protección de la víctima y es una suerte de tutela anticipatoria de su derecho (*vid.* AAPB 402/2024, de 15 de abril, Secc. 9.ª, Ponente: Ilmo. Sr. Almería Trenco, FJ 5.º.2; AAP B 188/2024, de 13 de marzo, Secc. 10.ª, Ponente: Ilma. Sra. Piquero Sanz, FJ 2.º), no exactamente una medida de protección, respondiendo más al esquema propiamente reparador del Código Penal en el ámbito de la responsabilidad civil al ser una restitución del inmueble al perjudicado (art. 110.1.º CP). En todo caso, al margen de esta reflexión, es cierto que la devolución inmediata del inmueble ilícitamente sustraído, digámoslo así, late como principal sentimiento, evidenciado en las legislaciones de nuestro entorno que

44. Lo que no ha impedido que alguna resolución la haya incardinado dentro del art. 544 bis LECRIM como una suerte de alejamiento, algo que puede ser asumido, aunque no se pretende propiamente alejar al sospechoso del lugar como medida de protección, sino obtener la restitución y el cese de la perturbación del bien jurídico protegido. *Vid.* AAPBU 355/2024, 16 de abril, Secc. 1.ª, Ponente: Ilmo. Sr. Carballera Simon, FJ 3.º. El acuerdo unánime de la Junta celebrada en unificación de criterios por la Audiencia Provincial de Madrid el día 25 de noviembre de 2022 señala que "En el acuerdo de unificación de criterio, los magistrados de las secciones de Penal de la Audiencia Provincial recuerdan que el artículo 13 de la Ley de Enjuiciamiento Criminal habilita a la autoridad judicial a adoptar todas aquellas medidas que resulten necesarias para preservar y tutelar los bienes jurídicos ofendidos por la comisión del delito presuntamente cometido".

desapoderan a la autoridad judicial para otorgar competencias a las fuerzas policiales bajo determinados presupuestos[45].

La clave de la adopción de la medida cautelar de desalojo, al margen del cumplimiento de los requisitos que ahora veremos, se sustenta en varios aspectos. En primer lugar, si el hecho ha sido denunciado en sede policial, es esencial, como se ha expuesto, el desarrollo de un atestado policial rigurosamente trabajado conteniendo, de ser posible, el conjunto de elementos que se han apuntado con anterioridad, documentando del derecho que se ostenta y su posición clara en torno al desalojo, juntamente con la indiciaria ilicitud de la conducta que se está investigando. En segundo lugar, hay que identificar, necesariamente, a las personas que presuntamente están cometiendo el hecho delictivo (AAPB 89/2024, de 15 de enero, Secc. 6.ª, Ponente: Ilmo. Sr. Barrio Giménez, FJ 2.º; AAPB 92/2024, de 23 de enero, Secc. 6.ª, Ponente: Ilmo. Sr. Barrio Giménez, FJ 2.º; AAP B 1165/2023, 12 de diciembre, Secc. 3.ª, Ponente: Ilma. Sra. Sánchez Gil, FJ 2.º; AAPGR 666/2023, 26 octubre, Secc. 2.ª, Ponente: Ilmo. Sr., Sánchez Jiménez, FJ 2.º) para que precisamente puedan defenderse, en su caso, frente a la petición de la medida cautelar[46].

45. Como apunta la SAP B 361/2020, 7 de septiembre, Secc. 9.ª, Ponente: Ilma. Sra. Tejero Seguí, FJ 6.º: "El tratamiento dispensado en los países de nuestro entorno comunitario resulta diametralmente opuesto a nuestra inoperativa legislación al regular la recuperación ágil y célere de la posesión del inmueble. Así, Holanda solo exige una denuncia policial para recuperarla exhibiendo el título de propiedad y que los poseedores no dispongan de ninguno. En Francia la policía puede desalojar a un ocupa ilegal durante las primeras 48 horas de ocupación desde el momento que tiene conocimiento de este hecho. En Alemania, también se recupera la posesión de las casas ocupadas en un plazo de 24 horas después de conocerse su ocupación ilegal con el requisito de que el propietario presente una denuncia. Reino Unido también dispone de un sistema policial urgente de recuperar la posesión tras la denuncia del titular y en Italia el juzgado da orden inmediata a la policía para recuperar la posesión acreditada la propiedad del bien y la inexistencia de título en el ocupante".

46. Como ha señalado al AAPL 229/2024, 1 de marzo, Secc. 1.ª, Ponente: Ilma. Sra. Juan Agustín, FJ 3.º: "No podemos olvidar que no todas las ocupaciones de viviendas u otros inmuebles son siempre consideradas delito leve. Por ello, la prudencia exige que con carácter previo a la adopción de cualquier medida sea necesario proceder al esclarecimiento de los hechos. Esto es, que los ocupantes puedan ser oídos y aportar si cabe la documentación que consideren oportuna".

En tercer lugar, es preciso conocer si entre los sospechosos hay personas dependientes, víctimas de violencia sobre la mujer o personas menores de edad o en riesgo de exclusión social, para adoptar aquellas medidas destinadas a su amparo por parte de las Administraciones competentes, y ello ante la eventualidad del desalojo (disposición adicional séptima LEC 1/2000).

Solicitado en sede policial, el desalojo ordenado judicialmente requiere que en el atestado se reflejen, fruto de la investigación, los presupuestosde toda cautelar que son *fumus boni iuris* y *periculum in mora*. La traducción procesal de los requisitos que permiten estudiar la petición del desalojo y su posible adopción, y así como apunta, como simple paradigma, el AAP B 352/2024, de 6 de abril, Secc. 9.ª, Ponente: Ilmo. Sr. Ferrer Vicastillo, FJ 3.º:

> El desalojo de los ocupantes de una vivienda requiere, como toda medida cautelar, la concurrencia de dos requisitos: a) la existencia de indicios racionales y relevantes de la comisión del delito de usurpación pacífica de bienes inmuebles, previsto y penado en el artículo 245.2 CP, esto es, que se objetive una apariencia de buen derecho (fumus boni iuris); y b) la existencia de una situación objetiva de riesgo de vulneración del bien jurídico protegido (periculum in mora). En este caso se ve afectada la legítima posesión del inmueble por el perjudicado, y el perjuicio ya se ha consumado y despliega sus efectos con carácter permanente mientras dure la ocupación ilegal, por lo que requiere de la medida cautelar con el fin de conseguir el cese de la situación antijurídica y la restauración del orden jurídico vulnerado.

Por tanto, el primer presupuesto es, necesariamente, la existencia de un delito, ya sea de allanamiento (AAPB 402/2024, de 15 de abril, Secc. 9.º, Ponente: Ilmo. Sr. Almería Trenco, FJ 5.º.2, acuerdo de la Junta, unánime, celebrada en unificación de criterios por la Audiencia Provincial de Madrid el día 25 de noviembre de 2022 por los Magistrados de Secciones Penales), ya sea singularmente de una usurpación constitutiva de delito leve. Por tanto, hay que acreditar indiciariamente el ilícito penal debiendo integrarse necesariamente todos los elementos del tipo que ya analizamos. Por otro lado, la necesidad se extiende,

adicionalmente, a la acreditación del riesgo en el mantenimiento de dicha situación que igualmente se traduce "en las consecuencias negativas que podrían derivarse de no adoptar la medida cautelar, lo cual, en el ámbito penal, hace especial referencia al aseguramiento de las pruebas, al sometimiento del investigado al proceso y, además a la evitación de la reiteración y persistencia delictiva" (AAPBU 355/2024, 16 de abril, Secc. 1.ª, Ponente: Ilmo. Sr. Carballera Simón, FJ 6.º), de manera que el mantenimiento de la situación antijurídica provocada por el mantenimiento de los sospechosos en el inmueble debe cesar, sirviendo la medida cautelar para restaurar la situación previa a la comisión del hecho delictivo. Coadyuva a la adopción de la cautelar la acreditación de perjuicios materiales y económicos al impedirse fruto de la usurpación la disposición sobre el inmueble[47].

En todo caso, al margen de los presupuestos que habilitan para la cautelar, no hay que olvidar que el desalojo que se interesa debe ser proporcionado, por tanto, hay que hacer una labor de ponderación de la medida evidenciando que sea idónea, necesaria y proporcionada en sentido estricto (SSTC 14/2003, de 28 de enero, FJ 9.º; 43/2014, de 27 de marzo, FJ 2.º; 170/2013, de 7 de octubre, FJ 5.º, y 39/2016, de 3 de marzo, FJ 5.º, entre otras), algo que debe desprenderse igualmente de la tarea de investigación policial reflejando fielmente la situación con la práctica de todas aquellas diligencias que sean precisas para valorar no solo el ilícito y la autoría, también la pertinencia del desalojo a la vista de los daños materiales o económicos, el menoscabo de la titularidad y su disposición sobre el inmueble, la degradación del ecosistema de

47. Como señala el AAP B 409/2024, de 22 de abril, Secc. 9.ª, Ponente: Ilmo. Sr. Gómez Arbona, FJ 4.º: "Sin embargo, no se aprecia por este Tribunal la concurrencia del requisito de 'periculum in mora', en tanto que de acuerdo con lo expuesto en la denuncia y pese a la previsión de c*omercialización de la vivienda, no se acredita por la denunciante ni su puesta en alquiler, u ofrecimiento de venta*. Tampoco pueden considerarse los daños materiales y riesgos para terceros que alega el recurrente, sino como meras hipótesis". Igualmente, el AAPB 345/2024, de 9 de abril, Secc. 2.ª, Ponente: Ilmo. Sr. Gomez Udias, FJ 2.º.16: "Es decir, la hipótesis de la parte denunciante sobre *la urgencia en la recuperación* de la vivienda, pues en otro caso la sentencia no podrá ser ejecutada, no se corresponde con su comportamiento procesal, pues no obra que haya dado uso a la plaza de garaje desde el año 2020, tampoco conocía quién la utilizaba, ni en qué sentido la utilizaba" (la cursiva es mía).

convivencia en vecinos o colindantes, e incluso la vulnerabilidad, que no impide el desalojo, sin perjuicio de dar traslado a la agencia competente de servicios sociales (Instrucción 1/2020 FGE).

El trabajo policial previo de identificación de los autores es trascendental no solamente para su filiación en el propio atestado, sino para su posterior citación una vez la petición de desalojo se encuentre en sede judicial. Y ello, por cuanto, al amparo del ya señalado art. 13 LECRIM, va a existir una vista en la que con obligada contradicción se van a ver reforzados los indicios policiales y la posible decisión de desalojo, pero, también, donde los ocupantes puedan ejercer su derecho de defensa en la adopción de la cautelar[48]. Por tanto, hay una labor policial previa de conocimiento de los responsables, pero también una posterior de citación, a requerimiento de la autoridad judicial, para hacer comparecer al sospechoso ante el órgano judicial que va a decidir sobre la medida, sin olvidar la posible adopción *inaudita parte*, es decir, sin la presencia del investigado, pero con su debida citación, con la participación de un abogado de la defensa incluso en supuestos de citación frustrada, de supuestos de negativa a darse por citado o de desconocimiento de los ocupantes, que va a permitir que se acuerde igualmente la medida de desalojo.

48. Señala, ya tempranamente, a propósito del desalojo y el derecho de defensa el AAP M 348/2017, 4 de mayo, Secc. 29, Ponente: Ilma. Sra. Rasillo López, FJ 2.º "*Además, la regla de interdicción de la indefensión requiere del órgano jurisdiccional un indudable esfuerzo a fin de preservar los derechos de defensa de las partes, correspondiendo a los órganos judiciales procurar que en un proceso se dé necesaria contradicción entre las partes, así como que posean idénticas posibilidades de alegar o probar y, en definitiva, de ejercer su derecho de defensa en cada una de las instancias que lo componen* (SS. 226/1988, 162/1993, 110/1994, 175/1994 y 102/1998)" (la cursiva es mía). No obstante, más recientemente, APPB 48/2024, de 18 de enero, Secc. 7.ª, Ponente: Ilma. Sra. Garcés Sese FJ 2.º. "No obstante, entendemos suficientemente justificada la decisión del Instructor cuando deniega la medida cautelar de desalojo de los ignorados ocupantes toda vez que, pese a la existencia de indicios delictivos, entendemos que no existe justificación suficiente del perjuicio que pueda sufrir la mercantil denunciante, teniendo en cuenta que, por un lado, las medidas cautelares no pueden suponer la anticipación de una resolución de condena, que es lo que supondría en este caso si se atendiese a la petición efectuada la apelante, y por otro, *que para su adopción requiere de la preceptiva audiencia a los ignorados ocupantes, asistidos de letrado*, por lo que dicha pretensión podrá ser interesada y solventada en el acto del juicio oral" (la cursiva es mía).

Finalmente, tras la vista y acreditados los elementos justificativos que lo habiliten, el auto de desalojo constituye la orden de ejecución para que la autoridad policial pueda proceder con la expulsión de los infractores, pudiendo acceder al inmueble mediante el uso de la fuerza, si fuera necesario, para restituir al titular en su situación anterior a la violación jurídica llevada a cabo.

5 Conclusiones: síntesis del trabajo policial

El delito leve de usurpación inmobiliaria leve y el allanamiento de morada representan un desafío importante para el trabajo policial. Hay que señalar que, por primera vez, un delito de los catalogados como leves, en este caso la usurpación pacífica, constituye un motivo de preocupación hasta el punto de tener tanto la Fiscalía General de Seguridad como la Secretaria de Estado de Seguridad que dictar sendas instrucciones para conseguir una labor coordinada de las agencias policiales con la acusación pública que permita reaccionar con prontitud y eficacia frente a estos hechos ilícitos. Sin embargo, no hay que olvidar que la necesidad de seguir un sistema de garantías es lo que fortalece la reacción frente al hecho, un sistema de garantías, eso sí, que está destinado a evitar un uso inadecuado del sistema de justicia penal cuando los hechos son susceptibles de verse tutelados ante la jurisdicción civil. Para ello, hay tres fases de trabajo policial esencial. Una primera, de atención al hecho delictivo en la faceta de investigación y atención a la víctima del ilícito presuntamente cometido. Así, la redacción del atestado reviste unas características peculiares destinadas a facilitar la reacción policial frente al sujeto activo del delito. Es decir, no se trata de una actuación más, sino de una actuación distinta que viene delineada por una posible situación de urgencia, ante un hecho tan importante como es la vulneración de la propiedad y la tenencia y titularidad derivada de esa propiedad, por lo que el rigor se impone y exige una documentación nítida de la situación denunciada, además de una constatación directa perceptible por quien resulta ser el instructor policial. Esto, a su vez, permite una actuación de tutela inmediata mediante la detención, claro en el supuesto del allanamiento, con lo que no precisaría

desalojo y, valga la reiteración, con desalojo policial en situaciones de flagrancia delictiva en el supuesto de la usurpación pacífica, con lo que no sería necesario impetrar la tutela de los tribunales.

No hay que olvidar que no es cierto que se puedan generar derechos consolidados por el mero paso del tiempo que enerven la eficacia de las medidas reactivas, incluso en supuestos de vulnerabilidad simplemente se permitiría el acceso a los sistemas de asistencia social, pero no la no expulsión del inmueble allanado o, en su caso, ocupado. Aun así, la faceta social no está reñida con la policial, pero no se pueden construir mitos con el boca a boca que ni son ciertos ni están permitidos por ley: *quien ocupa o allana no convierte el inmueble en su domicilio y por tanto no tiene los derechos inherentes a tal situación*. No tiene derechos ex novo en virtud de su conducta, cierto, pero sí garantías, las mismas que amparan a todo ciudadano ante la Ley en el sistema de justicia penal. De ahí, la segunda fase del trabajo policial en que, una vez solicitado el desalojo, permita, fruto del atestado redactado, contemplar por el juzgador el escenario que se presenta, pero, además, una tarea de citación para que la contradicción sea efectiva antes de tomar la decisión sobre la expulsión del inmueble, pudiendo acreditar un derecho que lo ampare ante la situación denunciada. Tal citación, por tanto, resulta trascendental para el ejercicio del derecho de defensa, sin perjuicio de que la ausencia voluntaria no enervaría la eficacia del desalojo. Y, finalmente, tras la vista y con un auto que confirme los indicios delictivos bajo los presupuestos de urgencia, pero también de proporcionalidad, la ejecución de la orden, con la fuerza jurídicamente amparada que no convierte en mera ilusión el auto de desalojo dictado, sino que hace efectiva la restitución a la víctima del hecho.

6. Glosario

AAP: Auto de Audiencia Provincial

CE: Constitución española

CP: Código Penal

FJ: Fundamento jurídico

LEC: Ley de Enjuiciamiento Civil

LECRIM: Ley de Enjuiciamiento Criminal

LOPSC: Ley Orgánica de Protección y Seguridad Ciudadana

LOTJ: Ley Orgánica del Tribunal del Jurado

SAP: Sentencia de Audiencia Provincial

STS: Sentencia Tribunal Supremo

STC: Sentencia Tribunal Constitucional

SES: Secretaría de Estado de Seguridad

Referencias bibliográficas, jurisprudencia

Alfonso Rodríguez, A. J. (2023). Diligencias de investigación policial y derecho de defensa. *Foro Galego. Revista Xurídica Xeral de Galicia*, *214*, 83-122.

Díez-Picazo, L. y Gullón, A. (2012). *Sistema de Derecho Civil (volumen III)*. Madrid: Tecnos.

Fiscalía General del Estado (2016). *Memoria elevada al Gobierno de S.M. Presentada al inicio del año judicial por la Fiscal General del Estado Excma. Sra. Consuelo Madrigal Martínez-Pereda*. Madrid: Fiscalía General del Estado-Ministerio de Justicia.

Fiscalía General del Estado (2021). *Memoria elevada al Gobierno de S.M. Presentada al inicio del año judicial por la Fiscal General del Estado Excma. Sra. Doña Dolores Delgado García*. Madrid: Fiscalía General del Estado-Ministerio de Justicia.

Fiscalía General del Estado (2023). *Memoria elevada al Gobierno de S.M. Presentada al inicio del año judicial por el Fiscal General del Estado Excmo. Sr. D. Álvaro García Ortiz*. Madrid: Fiscalía General del Estado-Ministerio de Justicia.

Fiscalía General del Estado (2024). *Memoria elevada al Gobierno de S.M. Presentada al inicio del año judicial por el Fiscal General del Estado Excmo. Sr. D. Álvaro García Ortiz*. Madrid: Fiscalía General del Estado-Ministerio de Justicia.

Gimeno Sendra, V., Moreno Catena, V. y Cortés Domínguez, V. (1999). *Derecho Procesal Penal*. Madrid: Colex.

Lafuente Torralba, A. J. (2021). El *labyrinthus iudiciorum* de la ocupación ilegal de viviendas: remedios en las vías penal y civil y análisis de su eficacia. *Revista de Derecho Aragonés*, *26-27*, 113-154.

Moreno Catena, V. y Cortés Domínguez, V. (2017). *Derecho Procesal Penal*. Valencia: Tirant lo Blanch.

Mozas Pillado, J. (2021). *Ocupantes ilegales de inmuebles. Una perspectiva penal y criminológica. Especial referencia al desalojo policial*. Barcelona: Aletelier Libros Jurídicos.

Ríos Martín, J. C. (2021). Estudio jurídico del delito de ocupación de viviendas: aportaciones de la justicia restaurativa y argumentos de defensa cuando el perjudicado es una entidad bancaria. En A. Llano Torres, C. Martínez-Sicluna y A. del Pozo Armentia, *Innovación educativa y justicia restaurativa en las Facultades de Derecho y Educación* (pp. 121-163). Madrid: Editorial Dykinson.

Tribunal Constitucional

STC 22/1984, de 17 de febrero, FJ 5.º.

STC 145/1985, de 28 de octubre, FJ 4.º.

STC 22/1988, de 18 de febrero, FJ 3.º.

STC 182/1989, de 3 de noviembre, FJ 2.º.

STC 217/1989, de 21 de diciembre, FJ 2.º.

STC 303/1993, de 25 de diciembre, FJ 4.º.

STC 51/1995, de 23 de febrero, FJ 2.º.

STC 94/1999, de 31 de mayo, FJ 5.º.

STC 171/1999, de 27 de septiembre, FJ 9.º.

STC 67/2001, de 17 de marzo, FJ 6.º.

STC 119/2001, de 24 de mayo, FJ 6.º.

STC 195/2002, de 28 de octubre, FJ 2.º.

STC 14/2003, de 28 de enero, FJ 9.º.

STC 61/2003, de 24 de marzo, FJ 2.º.

STC 206/2003, de 1 de diciembre, FJ 2.º.

STC 345/2006, de 11 de diciembre, FJ 3.º.

STC 68/2010, de 18 de octubre, FJ 5.º.

STC 134/2010, de 2 de diciembre, FJ 3.º.

STC 53/2013, de 28 de febrero, FJ 3.º.

STC 170/2013, de 7 de octubre, FJ 5.º.

STC 43/2014, de 27 de marzo, FJ 2.º.

STC 39/2016, de 3 de marzo, FJ 5.º.

STC 13/2017, de 30 de enero, FFJJ 5.º a 7.º.

STC21/2018, de 5 de marzo, FFJJ 7.º a 10.º.

STC 32/2019, 28 de febrero, en su FJ 5.º.

STC 83/2019, de 17 de junio, FFJJ 5.º a 7.º.

STC 180/2020; de 14 de diciembre, FFJJ 2.º a 4.º.

STC80/2021, de 19 de abril, FJ 4.º.

STC 59/2023, de 23 de mayo, FFJJ 4.º y 5.º. ECLI:ES:TC:2023:59

Tribunal Supremo

STS 318/2013, 11 de abril, de la Sala II, Ponente: Excmo. Sr. Marchena Gómez, FJ 2.ºSTS 1825/2013 - ECLI:ES:TS:2013:1825.

STS 228/2015, de 21 de abril, de la Sala II, Ponente: Excmo. Sr. Martínez Arrieta, FJ 2.ºSTS 1516/2015 – ECLI:ES:TS:2015:1516.

STS 980/2016 de la Sala II, de 11 de enero, Ponente: Excmo. Sr. Marchena Gómez, FJ 2 A.STS 16/2017 – ECLI:ES:TS:2017:16.

STS 520/2017, de 6 de julio, de la Sala II, FJ 4.º. 3, Ponente: Excmo. Sr. Berdugo Gómez de la Torre STS 2751/2017 – ECLI:ES:TS:2017:2751.

STS 399/2018, 12 de septiembre, de la Sala II, Ponente: Excma. Sr. Ferrer García, FJ 7.º: STS 3108/2018 - ECLI:ES:TS:2018:3108.

STS 66/2020, 20 de febrero, de la Sala II, Ponente: Excmo. Sr. Martínez Arrieta, FJ Único, STS 593/2020 – ECLI:ES:TS:2020:593.

STS 99/2020, de 10 de marzo, de la Sala II, Ponente: Excmo. Sr. Sánchez Melgar, FJ 2.º STS 921/2020 – ECLI:ES:TS:2020:921.

STS 468/2020, de 23 de septiembre, de la Sala II, Ponente: Excmo. Sr. Magro Servet, FJ 23 STS 2987/2020 – ECLI:ES:TS:2020:2987.

STS 78/2021, de 1 de febrero, de la Sala II, Ponente: Excmo. Sr. Marchena Gómez, en su FJ 2.3.ºSTS 551/2021 – ECLI:ES:TS:2021:551.

STS 503/2021, de 10 de junio, de la Sala II, Ponente: Excmo. Sr. Magro Servet, FJ 2.ºSTS 2331/2021 – ECLI:ES:TS:2021:2331.

STS 731/2023, de 7 de octubre, de la Sala II, Ponente: Excmo. Sr. Marchena Gómez, FJ 4.º.STS 5271/2013 – ECLI:ES:TS:2013:5271.

Audiencia Provincial

AAPM 348/2017, de 4 de mayo, Secc. 29.ª, Ponente: Ilma. Sra. Rasillo López, FFJJ 1.º y 2.ºAAP M 2827/2017 - ECLI:ES:APM:2017:2827A.

SAP T 276/2017, de 13 de julio, Secc. 4.ª, Ponente: Ilmo. Sr. Hernández García, FJ 3.º-SAP T 1159/2017 – ECLI:ES:APT:2017:1159.

SAPM 447/2018, 7 de junio, Secc. 2.ª, Ponente: Ilma. Sra. Compaired Plo, FJ 4.ºSAP M 8321/2018 – ECLI:ES:APM:2018:8321.

SAPM 800/2019, de 10 de diciembre, Secc. 23.ª, Ponente: Ilmo. Sr. Berges de Ramón, FJ 2.ºSAP M 16608/2019 – ECLI:ES:APM:2019:16608.

SAP B 361/2020, 7 de septiembre, Secc. 9.ª, Ponente: Ilma. Sra. Tejero Seguí, FJ 6.º-SAP B 9330/2020 - ECLI:ES:APB:2020:9330.

SAPM 136/2023, de 28 de febrero, Secc. 6.ª, Ponente: Ilma. Sra. López Candela, FJ 2.º-SAP M 2036/2023 – ECLI:ES:APM:2023:2036.

AAPC 625/2023, 4 de octubre, Secc. 2.ª, Ponente: Ilma. Sra. Taboada Caseiro, en su FJ 1.ºAAP C 957/2023 - ECLI:ES:APC:2023:957A.

AAPGR 666/2023, 26 de octubre, Secc. 2.ª, Ponente: Ilmo. Sr. Sánchez Jiménez, FJ 2.ºAAP GR 1295/2023 - ECLI:ES:APGR:2023:1295A.

AAP B 1165/2023, 12 de diciembre, Secc. 3.ª, Ponente: Ilma. Sra. Sánchez Gil, FJ 2.ºAAP B 13826/2023 - ECLI:ES:APB:2023:13826A.

AAP L 2/2024, de 2 de enero, Secc. 1.ª, Ponente: Ilma. Sra. Blat Peris, FJ 2.ºAAP L 41/2024 – ECLI:ES:APL:2024:41A.

AAPT 19/2024, de 12 de enero, Secc. 2.ª, Ponente: Ilma. Sra. Calvo González, FJ 2,ºAAP T 107/2024 - ECLI:ES:APT:2024:107A.

AAPB 89/2024, de 15 de enero, Secc. 6.ª, Ponente: Ilmo. Sr. Barrio Giménez, FJ 2.ºAAP B 1054/2024 - ECLI:ES:APB:2024:1054A.

APPB 48/2024, de 18 de enero, Secc. 7.ª, Ponente: Ilma. Sra. Garcés Sese FJ 2.ºAAP B 3705/2024 – ECLI:ES:APB:2024:3705A.

AAPB 61/2024, de 19 de enero, Secc. 7.ª, Ponente: Ilma. Sra. Calvo López FJ Único AAP B 1076/2024 – ECLI:ES:APB:2024:1076A.

AAPB 92/2024, de 23 de enero, Secc. 6.ª, Ponente: Ilmo. Sr. Barrio Giménez, FJ 2.ºAAP B 1056/2024 - ECLI:ES:APB:2024:1056A.

AAPB 130/2024, de 6 de febrero, Sección 9.ª, Ponente: Ilmo. Sr. Sicilia Murillo, FJ 1.ºAAP B 1816/2024 - ECLI:ES:APB:2024:1816A.

AAPB 206/2024, de 27 de febrero, Secc. 9.ª, Ponente: Ilma. Sra. Sucias Rodríguez, FJ 9.º y 13.º AAP B 1987/2024 - ECLI:ES:APB:2024:1987A.

AAPL 140/2024, 1 de marzo, Secc. 1.ª, Ponente: Ilma. Sra. Juan Agustín, FJ 2.ºAAP L 229/2024 - ECLI:ES:APL:2024:229A.

AAPL 229/2024, 1 de marzo, Secc. 1.ª, Ponente: Ilma. Sra. Juan Agustín, FJ 3.ºAAP L 229/2024 - ECLI:ES:APL:2024:229A.

AAP T 252/2024, 11 de marzo, Secc. 2.ª (Ponente: Ilma. Sra. Tárrega Cervera), FJ 2.º, AAP T 460/2024 – ECLI:ES:APT:2024:460A.

AAP B 188/2024, de 13 de marzo, Secc. 10.ª, Ponente: Ilma. Sra. Piquero Sanz, FJ 2.ºAAP B 3622/2024 – ECLI:ES:APB:2024:3622A.

AAP B 352/2024, de 6 de abril, Secc. 9.ª, Ponente: Ilmo. Sr. Ferrer Vicastillo, FJ 3.º AAP B 4735/2024 – ECLI:ES:APB:2024:4735A.

AAPB 345/2024, de 9 de abril, Secc. 2.ª, Ponente: Ilmo. Sr. Gómez Udias, FJ 2.º.16 AAP B 4384/2024 - ECLI:ES:APB:2024:4384ª.

AAP B 402/2024, de 15 de abril, Secc. 9.ª, Ponente: Ilmo. Sr. Almería Trenco, FJ 2.º, 4º. y 5.º.

AAPBU 355/2024, 16 de abril, Secc. 1.ª, Ponente: Ilmo. Sr. Carballera Simón, FJ 3.ºAAP BU 482/2024 – ECLI:ES:APBU:2024:482A.

AAP B 409/2024, de 22 de abril, Secc. 9.ª, Ponente: Ilmo. Sr. Gómez Arbona, FJ 4.º AAP B 4786/2024 - ECLI:ES:APB:2024:4786A.

AAP OU 252/ 2024, 24 de abril, Secc. 2.ª, Ponente Ilma. Sra. Lomo del Olmo, FJ 2.º AAP OU 105/2024 – ECLI:ES:APOU:2024:105A.

Algunas dificultades en la detección e investigación de los ciberdelitos económicos

Some Difficulties in the Detection and Investigation of Economic Cybercrimes

Daniel González Uriel[1]
Letrado del Tribunal Constitucional, España.
daniel.gonzalez@poderjudicial.es | https://orcid.org/0000-0001-8966-0571

DOI: https://doi.org/10.14201/cp.32207
Recibido: 20-12-2024 | Aceptado: 23-12-2024

Resumen
En este trabajo se lleva a cabo un análisis sobre algunos de los principales problemas que se aprecian en la investigación de los ciberdelitos de contenido económico. Para ello se efectúa una descripción sobre el fenómeno de la ciberdelincuencia, se apuntan algunos de los principales delitos que se pueden cometer en este campo y, finalmente, se expone una serie de cuestiones de índole judicial y policial. Se trata de un enfoque multidisciplinar, en que se integran aspectos criminológicos, penales y procesales. Tiene una finalidad práctica, destinada a la prevención, a la detección precoz y a la mejora en la lucha contra estas tipologías delictivas.

Palabras clave
Ciberdelincuencia; Ciberestafas; Delitos económicos; Investigación; Proceso penal.

Abstract
In this paper, we carry out an analysis on some of the main problems that are seen in the investigation of cybercrimes with economic content. We make a description of the phenomenon of

1. Magistrado (en servicios especiales). Doctor en Derecho. Profesor (acr.) contratado doctor ANECA.

cybercrime, we note some of the main crimes that can be committed in this field and, finally, we expose a series of judicial and police issues. It is a multidisciplinary approach, which integrates criminological, criminal and procedural aspects. It has a practical purpose, aimed at prevention, early detection and improvement in the fight against these criminal types.

Keywords
Cybercrime; Cyber scams; Economic crimes; Investigation; Criminal proceedings.

1 Introducción

La revolución tecnológica en que nos hallamos inmersos ha propiciado que las tecnologías de la información y de la comunicación (TIC) se erijan en elementos clave en el desarrollo social, económico, laboral, educativo, comercial o comunicativo de los ciudadanos. El ciberespacio se ha convertido en un nuevo ámbito relacional al que se han trasladado prácticamente todos los aspectos de la vida cotidiana de las personas, desde los más sencillos –como mandar un email– hasta otros más complejos, como realizar diferentes negocios jurídicos de corte patrimonial. Ello comporta notables ventajas en orden a la inmediatez, a la reducción de tiempos, a la conectividad, a la eliminación de las fronteras y de las barreras y, por ende, a una mayor agilidad y celeridad. Si bien, y como contrapartida, el delito también se ha visto favorecido por esta facilidad comunicativa, ya sea mediante la adaptación de algunas modalidades clásicas al ámbito de las TIC, ya sea a través del surgimiento de nuevas tipologías delictivas. La cibervictimización constituye un riesgo creciente, global y generalizado. Además, dicho peligro se ve incrementado por las nuevas tecnologías, aplicaciones y herramientas y, de modo especial, por el desarrollo de la inteligencia artificial (IA).

No descubrimos nada nuevo si decimos que, hoy día, la ciberdelincuencia constituye uno de los principales –por no decir el principal– ámbitos de expansión en el fenómeno delictivo. Este hecho es constatable si acudimos a los datos oficiales en nues-

tro país, en concreto, si tomamos en consideración los balances e informes sobre criminalidad emitidos, periódicamente, por el Ministerio del Interior[2] del Gobierno de España. Podemos atender al informe sobre la cibercriminalidad en España del año 2023 (Ministerio del Interior, 2023), que nos servirá para extraer una serie de interesantes elementos de juicio. En dicho documento se aprecia un importante incremento de los ciberdelitos en los últimos años. En él se detalla la evolución acaecida desde el año 2019 hasta el año 2023. Si atendemos a los ciberdelitos conocidos podemos observar que, en 2019, se cifraron en 218.302, en 2020 se elevaron a 305.477, en 2022 se incrementaron hasta los 374.737 hechos conocidos, mientras que, en el año 2023, alcanzaron los 472.125. Y, añadiendo un dato más, en el año 2023, el 90,5 % de tales casos se correspondían con supuestos de "fraude informático", según la terminología empleada en el informe, y que se corresponde con las ciberestafas –en este punto debemos puntualizar que nuestro Código Penal (CP) no acoge la denominación de "fraude informático", que sí se contiene en el Convenio de Budapest–[3].

Si abundamos un poco más en los datos estadísticos del citado informe, podemos inferir que, en los supuestos de ciberdelitos, existe una elevada tasa de casos sin resolver. En este sentido, para que nos sirva también como término de comparación, volveremos a manejar el mismo lustro de referencia que hemos tomado en consideración en el párrafo anterior (2019-2023), para que apreciemos, en toda su magnitud, la dimensión, los efectos y las consecuencias de la problemática tratada. Pues bien, en el año 2019, se esclarecieron 30.841 casos; en 2020, 38.046; en 2021, 46.141; en 2022, 51.642, y, en 2023, 60.197. Como se desprende de estos datos, nos encontramos ante una fenomenología delictiva con una baja tasa de esclarecimiento, en comparación con el volumen de casos. Y no solo eso, sino que,

2. *Vid*. al respecto https://www.interior.gob.es/opencms/es/prensa/balances-e-informes/. Los delitos que se recogen en dicho informe son: acceso e interceptación ilícita, amenazas y coacciones, delitos contra el honor, delitos contra la propiedad intelectual e industrial, delitos sexuales, falsificación informática, fraude informático, interferencia en datos y en sistemas.

3. Hacemos alusión al Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

como después anotaremos, esto debe ser puesto en relación con la existencia de una relevante –aunque desconocida– cifra negra de denuncias, lo que podría incrementar, exponencialmente, la magnitud de esta forma de criminalidad.

Con todo, no existe una definición unívoca de ciberdelincuencia, ni contamos con una regulación uniforme, sistemática y específica que trate dicho fenómeno de un modo autónomo e independiente. De modo general, y como primera aproximación, podríamos tomar en consideración la descripción que nos brinda el *Diccionario de la Real Academia Española (DRAE)*, que la define como "actividad delictiva que se lleva a cabo a través de Internet". En este sentido, llama la atención que el propio *Diccionario Panhispánico del Español Jurídico de la RAE (DEJ)* no contiene ninguna entrada para el vocablo que empleamos, sino que acude a la fórmula "delito informático", que caracteriza como "infracción penal cometida utilizando un medio o un instrumento informático". Por lo tanto, en esta contribución partimos de que la ciberdelincuencia abarcaría todo delito cometido por medio o a través de las TIC. Patrocinamos así una comprensión amplia del fenómeno, que se centre en el instrumento o cauce a través del que se vehicula o instrumenta el ilícito penal.

Pues bien, los ciberdelitos, aunque presenten una gran heterogeneidad y no sean reconducibles a una única categoría o clasificación, se encuentran presididos por una serie de rasgos propios, que podríamos reconducir, en su esencia más básica, a que se cometen en el ciberespacio. En este sentido, el ciberespacio, entendido por el *DRAE* como el "ámbito virtual creado por medios informáticos", tiene una serie de características que nos permiten comprender mejor algunas dinámicas delictivas *online*. Tal y como explica Miró Llinares (2012), el ciberespacio se caracteriza por: (i) el carácter transnacional, dado que no existen fronteras ni distancias; (ii) porque la Red es neutral, ya que no existen restricciones ni censuras de acceso; (iii) porque es un espacio no centralizado, que se encuentra distribuido y donde no existen nodos que actúen como centros locales; (iv) porque se encuentra anonimizado, puesto que no existe identificación de usuarios; (v) que está sometido a una revolución permanente y abierto al cambio, debido a la evolución tecnológica; (vi) en el que no hay guardianes formales; (vii) donde las

variables espacio y tiempo presentan un nuevo diseño; y (viii) que está popularizado, por lo que es tendencialmente universal.

Por su parte, López Gorostidi (2021) también anota una serie de caracteres del ciberespacio, de corte criminológico, con influencia en la comisión de ilícitos penales, entre las que señala: (i) en cuanto a sus aspectos técnicos, que las TIC atesoran una gran capacidad para albergar, procesar y distribuir cantidades ingentes de datos, y realizan tales acciones a gran velocidad; (ii) el elevado porcentaje de población mundial que accede a diario a las TIC y el creciente número de valores personales que se introducen en el ciberespacio; (iii) la posibilidad de simulación de identidad que Internet ofrece a sus usuarios; y (iv) los fenómenos de permanencia y automatismo del hecho.

Los usuarios de las TIC, mediante nuestro acceso y navegación por la Red, incorporamos nuestros bienes jurídicos al ciberespacio. Somos nosotros quienes delimitamos, mediante nuestra actuación en el ciberespacio, el ámbito en el que podemos ser victimizados *online*, por lo que este dato deviene en un punto de referencia esencial: el ciberespacio se convierte en un nuevo espacio de oportunidad delictiva en el que los sujetos podemos ser victimizados en tanto en cuanto interactuemos con terceros en él. Con nuestro comportamiento *online* concretamos qué bienes jurídicos de nuestra esfera de intereses pueden ser susceptibles de ser lesionados o puestos en peligro. Los bienes jurídicos que pueden ser lesionados o puestos en peligro son variados y, a título meramente ejemplificativo, podemos aludir al patrimonio, al honor, a la intimidad personal y familiar, a la propia imagen, a la libertad e indemnidad sexuales o a la libertad, entre otros. Si bien, y como reiteramos, debemos destacar que somos los usuarios de las TIC los que incorporamos a ese nuevo ámbito una parte de nuestra esfera de derechos e intereses, por lo que hemos de adoptar las cautelas y medidas de salvaguarda precisas para evitar o, cuando menos, limitar, las posibilidades de su lesión o menoscabo. En el bien entendido de que, con esta alusión, no estamos haciendo referencia a desorbitados deberes de autoprotección que, por otro lado, no se exigen por los tipos penales, ni estamos culpabilizando a las víctimas de su proceso de victimización. No obstante, este particular será retomado en las sucesivas líneas.

Como se aprecia con el análisis de los datos estadísticos manejados en las fuentes oficiales, la mayor parte de los ciberdelitos –más de un 90 % de ellos en 2023– tenían por finalidad la obtención de un lucro económico, por lo que podemos derivar una clara conclusión: la finalidad principal de la comisión de ciberdelitos es el enriquecimiento patrimonial. Por este motivo, ante dicha constatación, en este estudio nos centraremos en la ciberdelincuencia que podemos calificar como económica y que, a grandes rasgos, se catalogaría como aquel conjunto de delitos, cometidos mediante las TIC, y que afectan a los bienes jurídicos tutelados en el Título XIII, "De los delitos contra el patrimonio y el orden socioeconómico", del Libro II del CP, así como a aquellos otros ilícitos que, aunque sistemáticamente no se incardinen en dicho título, tengan relevancia, repercusión e incidencia en el sustrato patrimonial, económico o socioeconómico.

Con las páginas que prosiguen se pretende realizar, de modo modesto, un esbozo general sobre la problemática delictiva tratada, aunando tres vertientes: el análisis criminológico, penal y procesal de los ciberdelitos de naturaleza económica. Se opta por un enfoque tripartito, aunque integrado, a los fines de dar una visión de conjunto, completa y didáctica, huyendo de tratamientos fragmentarios que compartimenten o encapsulen el fenómeno y que diluyan una visión conjunta, transversal e integral. Por este motivo, en las líneas que siguen, se aglutinarán, de un modo pretendidamente armónico, postulados criminológicos, apuntes de dogmática penal y problemas procesales, con la intención de efectuar una prognosis certera, de apuntar posibles riesgos, retos y desafíos y, en resumidas cuentas, de brindar al lector un arsenal de instrumentos para profundizar en el análisis de una fenomenología delictiva que ha venido para quedarse, para expandirse y a la que hemos de hacer frente mediante esfuerzos teóricos y aplicaciones prácticas.

2 El ciberespacio como entorno criminógeno

Como anotamos, este nuevo entorno virtual también propicia que los sujetos puedan ser objeto de cibervictimizaciones. Al

efectuarse un traslado al ámbito *online* de todas las facetas de la vida, incorporamos nuestros derechos e intereses e interactuamos con terceros. Este comportamiento en la Red determinará que podamos ser objeto de ciberdelitos. Tal y como se advirtió, las cibervictimizaciones pueden ser variadas y plurales. En este sentido, todos los usuarios de las TIC somos potenciales víctimas, por lo que todos los agentes sociales somos susceptibles de ser victimizados, tanto personas físicas como jurídicas. Por lo tanto, no existe un único perfil de víctima, sino que presenta carácter múltiple, contingente y variable.

Ya hemos indicado que una de las principales peculiaridades de esta tipología de delitos es que es la propia víctima quien determina los bienes jurídicos de su esfera de intereses que pueden ser agredidos, mediante su incorporación a las TIC, su comportamiento en ellas y la interactuación con terceras personas. Así las cosas, es la propia víctima quien define el perímetro de actuación sobre el que pueden incidir los ciberdelincuentes. Si bien, hemos de advertir que con estas afirmaciones no se reprocha a la víctima nada, ni se le culpabiliza de ser victimizada, sino que se corrobora el presupuesto fáctico de los ciberdelitos. Pues bien, tomando como referente dicha situación, debemos constatar que, en ocasiones, el contexto *online* propicia que los sujetos lleven a cabo determinados actos de riesgo o que modifiquen su conducta y se comporten de un modo diferente a como lo hacen en el espacio físico. Es lo que se ha dado en llamar "online desinhibition effect", que Agustina Sanllehí (2014) sintetiza en que se da una disparidad de conductas porque las personas se encuentran "menos constreñidas, más sueltas y se expresan de una forma mucho más abierta". Dicho autor resume en seis los rasgos del efecto desinhibidor *online*, que aquí solo enumeraremos: i) la anonimidad disociativa, ii) la invisibilidad, iii) la asincronicidad, iv) la introyección solipsística, v) la imaginación disociativa y vi) la minimización del *status* y de la autoridad. A continuación, subraya que estos elementos "elevan, lógicamente, las probabilidades de que los usuarios incurran en conductas de riesgo y acaben siendo cibervictimizados".

Además de esta cierta modificación de las pautas de conducta en el entorno *online*, que nos hacen ser más atrevidos y pueden llevarnos a efectuar comportamientos de riesgo –pensemos en

interacciones con terceros desconocidos, lo que no haríamos en el espacio físico; el hecho de visitar determinados sitios web no seguros; descargar archivos de dudosa procedencia y origen, o efectuar compraventas de bienes y servicios sin conocer a la contraparte ni la realidad de la oferta, entre otros–, podemos traer a colación, en este punto, una de las teorías criminológicas clásicas para explicar las causas del delito y su factible adaptación al ciberespacio. Nos referimos a la Teoría de las Actividad Rutinarias (TAR), formulada por Felson y Cohen (1979), y que ha sido adaptada a las TIC por Miró Llinares (2012). En la formulación original de Felson y Cohen se parte de un enfoque situacional, basado en que el delito surge cuando se da la oportunidad delictiva. En apretado esquema, podemos resumir en tres los elementos que conforman dicha teoría explicativa del delito: (i) la existencia de objetivos adecuados, que puedan ser susceptibles de victimización; (ii) la aparición de un agresor motivado, dispuesto a cometer hechos delictivos; y (iii) la ausencia de guardianes capaces, tanto formales como informales, ya sean agentes policiales o conciudadanos que aparezcan en el lugar de los hechos y frustren la expectativa del agresor. En su atinada exposición, Miró Llinares (2012) aplica tales postulados al ciberespacio y sostiene que nos hallamos ante un nuevo espacio de oportunidad criminal en el que concurre una multitud de sujetos victimizables y donde no existen distancias, lo que facilita la inmediatez y el contacto entre sujetos. Añade que la ausencia de guardianes capaces alude tanto a los guardianes formales como a los informales, o a los programas informáticos.

En su disertación, dicho autor explica que estos tres elementos se combinan en las TIC sobre la base de la conducta de la víctima, en atención a las horas empleadas, las páginas web consultadas, la realización de actividades *online* –compraventa de servicios o interacciones con desconocidos– y las medidas de protección que adopte el usuario en su navegación, poniendo el foco en su adopción y en la actualización de los sistemas de protección de los dispositivos informáticos. Afirma que el usuario de las TIC es prácticamente un "autoguardián" y que la clave se encuentra en la conducta de la víctima, que es quien propicia la oportunidad delictiva. Pone de manifiesto que la modificación de las relaciones entre las variables espacio y tiempo en el ciberespacio permite que los ciberdelincuentes, con un solo acto –por

ejemplo, el envío de un mail malicioso–, accedan a una multitud indeterminada de víctimas potenciales. Menciona que un contenido malicioso puede permanecer latente mucho tiempo después de que se suba a las TIC por su autor, y que puede causar daños cuando los usuarios interactúen con él, lo que evidencia que se pueden causar resultados lesivos y nocivos mucho tiempo después de la acción, por lo que, además de la inmediatez, la asincronía juega un destacado papel.

Sin embargo, debemos subrayar que existen notables dificultades a la hora de cuantificar, con precisión, la magnitud del fenómeno tratado. Más allá de los datos oficiales sobre hechos conocidos, porque han sido denunciados, es de prever que un importante porcentaje de hechos engrosen la conocida como "cifra negra" de ciberdelitos. Las causas de ello son variadas: (i) el desconocimiento, por parte de la víctima, de que se ha cometido un delito. Podríamos pensar en aquellos supuestos en los que se dé una ciberestafa de una cuantía ínfima de dinero –unos pocos céntimos– y la víctima no reciba una notificación de su banca electrónica con cada movimiento que se produzca en su cuenta. Sería dable que una transferencia de pocos céntimos pudiera pasar inadvertida; (ii) que la propia víctima, aun conociendo el hecho, no considere que se trate de un delito, *v. gr.*, tentativas de estafa a los que no se les otorga la mayor credibilidad o actos preparatorios de estafas muy alejados de integrar actos ejecutivos –envío de mail con *spam*–; (iii) los propios sentimientos encontrados de la víctima, pudiendo mencionar la culpa o la vergüenza por el delito padecido. Como ejemplo que ilustre esta situación, podríamos mencionar la denominada "estafa romántica", en que el ciberdelincuente hace creer a su víctima que mantienen una relación sentimental telemática, la embauca, se gana su confianza y, finalmente, le solicita dinero con promesa de devolución, lo que nunca sucede. En este caso, la víctima, al sentirse burlada, puede rehusar la denuncia de los hechos por la vergüenza de relatar lo sucedido ante las instancias formales de persecución del delito.

Por otra parte, en cuanto a supuestos en los que se dé el sentimiento de culpa de la víctima, podríamos aludir a la ciberestafa en la que a un sujeto se le promete la obtención de un lucro –*v. gr.*, una cuantiosa herencia– a cambio de un desembolso dinerario

de poca cuantía –el pago de unos impuestos especiales–, si bien, efectuado el abono, nunca recibe la suculenta contraprestación prometida; (iv) la desconfianza en el sistema policial y/o judicial, ante la convicción de que no se va a descubrir al autor del delito ni se va a recuperar lo perdido; (v) el cálculo de intereses y la ponderación entre el coste temporal de un proceso judicial y los perjuicios sufridos con el ciberdelito; (vi) podemos agregar que, en el ámbito empresarial, el riesgo reputacional puede llevar a silenciar hechos delictivos para, precisamente, evitar que se dé una publicidad negativa. Piénsese en el caso de una entidad bancaria que sufre un ataque de *ransomware* –secuestro de datos– y prefiere abonar el rescate y omitir su denuncia, so riesgo de mostrarse en la opinión pública como vulnerable y carente de medidas de ciberseguridad, lo que puede disuadir a futuros clientes de confiar en ella.

Estos son algunos de los argumentos –sin pretensión de exhaustividad– que nos mueven a afirmar, con un importante sector doctrinal, que en el ámbito de la ciberdelincuencia existe una relevante cifra negra. Así las cosas, Montiel Juan (2016) llama la atención sobre los problemas metodológicos en la medición de los ciberdelitos, y señala que la dificultad que presentan las estadísticas oficiales es que dependen de la forma en que se definen los delitos en cada legislación, lo que no necesariamente coincide con la definición criminológica del fenómeno tratado. Además, dicha autora indica que algunos fenómenos cibercriminales pueden implicar la comisión de diferentes delitos tipificados en los textos penales. Considera que la disociación entre los tipos penales y las formas de criminalidad produce un conocimiento muy fragmentario de estos fenómenos. Advierte que las encuestas de cibervictimización y/o ciberdelincuencia autorrevelada arrojan datos diferentes y muy superiores a las cifras oficiales. Mientras que algún autor ha puesto el acento de la cifra negra en elementos técnicos, como la facilidad de alteración de la huella informática, el anonimato en los ciberdelitos, o bien, "el simple hecho de que es necesaria una capacidad técnica mínima para navegar con pleno conocimiento de la Red" (López Gorostidi, 2021), o bien, en la rigidez en la presentación física de denuncias, frente a otros modelos policiales en los que se permite su presentación telefónica o telemática (Kemp, 2021).

3 La ciberdelincuencia económica

3.1 Aspectos generales

Antes de efectuar un repaso por algunos de los principales ciberdelitos económicos que vamos a exponer, forzoso es que hagamos una breve mención a la clasificación que seguimos en esta contribución. Ya indicamos que la ciberdelincuencia carece de un tratamiento unitario y sistemático en el ordenamiento punitivo patrio. Con todo, y pese a asumir que existen diferentes aproximaciones doctrinales, en este trabajo seguiremos la clasificación criminológica patrocinada por Miró Llinares (2012), que diferencia entre ciberdelitos económicos, sociales y políticos, en atención al objeto sobre el que recae, de modo principal, la conducta delictiva. Consideramos que dicha propuesta resulta descriptiva, analítica y que permite aglutinar distintos tipos delictivos, en atención a su bien jurídico tutelado, por lo que facilita su comprensión. Si bien, y como hemos resaltado, somos conscientes de que existen delitos en los que puede haber más de un objeto protegido, y que podrían, en consecuencia, ser subsumidos en una categoría u otra. Por ello, hemos destacado que tal clasificación parte del objeto principalmente protegido.

De esta manera, los ciberdelitos económicos serían aquellos en los que prevalezca un componente patrimonial. Los ciberdelitos sociales aglutinarían una amalgama de variados supuestos delictivos, que tendrían como eje que recaerían sobre bienes jurídicos personales –o personalísimos– de los individuos, y conectados con los atributos propios de su esfera relacional –*v. gr.*, libertad, libertad e indemnidad sexuales, honor, intimidad o propia imagen, entre otros–. Por último, los ciberdelitos políticos serían todos aquellos que se cometerían con una motivación ideológica, y entre ellos podríamos incluir el ciberterrorismo o el *hacktivismo*.

Si descendemos a los ciberdelitos económicos, podemos concebirlos como aquellos cibercrímenes que recaen sobre

intereses patrimoniales. Si retomamos el citado informe sobre cibercriminalidad en España del año 2023, observamos que más del 90 % de los ciberdelitos son de corte patrimonial y, entre ellos, de manera absoluta, predominan las estafas informáticas –ya indicamos que el informe alude a "fraude"–. De hecho, de los 472.125 ciberdelitos conocidos en el año, 427.448 fueron ciberestafas, 15.137 fueron casos de "falsificación informática", 1.659 de interferencia en datos y en sistemas informáticos y 64 casos denunciaron ciberdelitos contra la propiedad intelectual e industrial. Como se puede colegir de lo que antecede, la finalidad lucrativa se encuentra detrás de una buena parte de los ciberataques. Estas acciones se ejecutan para obtener, de modo ilícito, dinero procedente de individuos, empresas u otras organizaciones.

Podemos anotar varias causas que facilitan o dan pie a que las TIC se conviertan en cauce para ejecutar delitos contra el patrimonio. En primer lugar, los usuarios de las TIC han trasladado al ciberespacio buena parte de su operativa económica, lo que, indefectiblemente, también abre un portillo a que puedan sufrir ciberataques. A título de ejemplo, podemos señalar que un porcentaje significativo de los usuarios de las TIC emplea la banca *online*, realiza compraventas de bienes y servicios a través de la Red, concierta negocios jurídicos y efectúa transferencias diversas en el ciberespacio. Para llevar a cabo tales actos, se insertan las contraseñas y las claves personales en los dispositivos informáticos y en los *smartphones*. Algo tan –aparentemente– inocuo como el pago de unas entradas de un concierto que se han visto en un anuncio en redes sociales puede comportar una pérdida patrimonial, al no advertir la víctima que se trataba de una estafa. Pues bien, no solo se corre el riesgo de que el anuncio visualizado sea engañoso, lo que hace generar desconfianza en los cibernautas y en el tráfico económico, sino que existe el peligro cierto de que los dispositivos informáticos sean infectados con *malware* y los ciberdelincuentes puedan acceder a nuestras claves y contraseñas.

Como podemos observar con este breve esbozo, los intereses económicos presentes en las TIC son ingentes. Además, los ciberdelincuentes pueden dirigirse a una pluralidad indeterminada de potenciales víctimas con el mismo ataque, por lo que se reducen

los esfuerzos e inversiones espacio-temporales. Por lo tanto, la obtención de un lucro económico se ve estimulada por la inmediatez, por la ausencia de fronteras, por la interconexión y por la mundialización de la Red. Además, se acude a argucias más o menos sofisticadas, como las técnicas de ingeniería social, facilitadas por el anonimato, la suplantación de identidad y la generación de confianza en el receptor de la comunicación o mensaje. También se emplean instrumentos técnicos, como VPN, deslocalizadores de direcciones IP, *proxy*, empleo de redes WiFi públicas en abierto y distintos artificios para enmascarar la procedencia del ataque, para diluir el rastro de los ciberdelincuentes y para romper la trazabilidad de las comunicaciones y de los fondos detraídos.

A ello se suma que, en ocasiones, los usuarios de las TIC no empleamos todas las medidas de seguridad precisas, más allá del antivirus, puesto que, entre otros aspectos, no contamos con las actualizaciones de los programas y aplicaciones, no usamos cortafuegos, no tenemos contraseñas seguras –ni gestores de contraseñas–, reunimos toda nuestra información y claves en un mismo dispositivo, no contamos con copias de seguridad de nuestros datos, interactuamos con desconocidos, llevamos a cabo navegaciones web por entornos no seguros, descargamos inopinadamente links y documentos sin cerciorarnos de su procedencia, efectuamos compraventas *online* y facilitamos nuestros datos personales –tales como fotografías personales o del DNI– con demasiada facilidad. Por si ello fuera poco, no podemos soslayar el auge de determinados elementos, como la IA, las criptomonedas y el empleo, por los cibercriminales, de la *dark web*, como aquella parte cifrada de Internet a la que se accede mediante navegadores especializados, oculta a los motores de búsqueda tradicionales, con direcciones IP enmascaradas, y donde se pueden obtener bienes, servicios y actividades ilícitas.

Este conjunto de elementos tecnológicos y personales, unido a las características del ciberespacio, explica, en buena medida, que asistamos a este auge de los ciberdelitos y, entre ellos, de la ciberdelincuencia económica. El lucro económico se alza, así, como la motivación principal de los ciberdelincuentes, ante la facilidad para victimizar a una pluralidad de sujetos, la dificultad en su detección y, por ende, la rentabilidad, en términos de

costes-beneficios, de esta serie de modalidades delictivas. A ello debemos agregar la internacionalización de la Red, la disparidad normativa entre las diferentes legislaciones nacionales, las disfunciones en la cooperación judicial internacional en algunas jurisdicciones y las dudas que genera la propia delimitación de los órganos judiciales con competencia para conocer de tales ilícitos. Es decir, y en suma, nos hallamos ante un cóctel de circunstancias que promueven que, a través de las TIC, se cometan ciberdelitos y que estos sean, en la mayor parte de supuestos, de índole económica.

3.2 Principales ciberdelitos económicos

En este apartado pretendemos realizar un acercamiento a algunos de los principales ciberdelitos económicos que se cometen a través de las TIC. Vaya por delante que no se efectuará un listado exhaustivo de los tipos del texto punitivo ni se llevará a cabo un análisis profundo y pormenorizado de cada uno de ellos. No es ese el objeto de esta contribución. Antes bien, lo que se realizará será destacar algunos rasgos criminológicos de tales ilícitos que nos sirvan para comprender mejor el porqué de las cibervictimizaciones y la causa de que las TIC se erijan en un vehículo adecuado para su comisión. En concreto, por su incidencia práctica, por su repercusión y por su relevancia político-criminal, hemos seleccionado cuatro delitos del Título XIII del Libro II del CP: estafas, delitos de daños, delitos contra la propiedad intelectual e industrial y blanqueo de dinero. Consideramos que constituyen una muestra lo suficientemente representativa, obedecen a *modus operandi* diferentes y resultan ilustrativos de distintas tipologías delictivas con incidencia en el patrimonio, en el orden socioeconómico y, en definitiva, en la esfera patrimonial.

3.2.1 Estafas y ciberestafas (arts. 248-251 CP)

Constituyen, sin duda, los principales ciberdelitos, tanto cuantitativa como cualitativamente, por lo que también son los ciberdelitos económicos más importantes. Debemos poner de relieve que la estafa tradicional o clásica y la estafa informática se recogen en los arts. 248 y 249[4] CP. La diferencia basilar entre

ambas estriba en que, como sabemos, la estafa tradicional obedece a la conjunción de cinco elementos que han de darse de modo sucesivo: el empleo de engaño bastante, que induce a error a la víctima, y le hace realizar un acto de disposición patrimonial, en perjuicio propio o de tercero, existiendo entre todos los elementos de la cadena descrita una relación de causalidad. Por su parte, hasta el año 2022, la estafa informática figuraba como un apéndice de la estafa clásica, en el art. 248 CP, y se caracterizaba porque no concurría el engaño como medio comisivo, sino que se aludía a la obtención de una transferencia patrimonial inconsentida mediante "alguna manipulación informática o artificio semejante". Un relevante sector doctrinal había llamado la atención sobre la imposibilidad de engañar a las máquinas y rehusaba la pretendida equivalencia con el molde de la estafa canónica.

Pues bien, la LO 14/2022, de 22 de diciembre, ha venido a dotar de independencia a la estafa informática, ubicándola sistemáticamente en el art. 249[5] CP, ampliando sus modalidades de conducta y solapándose, en buena medida, con los verbos nucleares del delito de daños informáticos del art. 264 CP. Si bien, debemos anotar que, a los efectos de nuestro trabajo, lo más relevante es que surgen discrepancias interpretativas a propósito de si la estafa tradicional puede ser aplicada en las ciberestafas –con lo que cabría la posibilidad del delito leve de estafa–, o bien, si el legislador ha pretendido que todas las estafas cometidas en las TIC se incardinen en el cauce del art. 249 CP, que no contiene ninguna modalidad de delito leve, con todo lo que ello comportaría en materia procesal: no sería posible acudir al juicio por delito leve, siempre habrían de tramitarse por el procedimiento abreviado y existiría una fase de instrucción, con la posibilidad de adoptar diligencias de investigación y actos de cooperación judicial internacional, de gran relevancia en materia de ciberestafas ante la ausencia de fronteras en

4. Sobre la nueva redacción del art. 249 CP, *vid*. Bustos Rubio (2023); y, en concreto, sobre el uso fraudulento de medios de pago distintos del efectivo, *vid*. Abadías Selma (2023).

5. Para una acabada comprensión, se recomienda una lectura de los arts. 248 y 249 CP, comparando el texto anterior a la LO 14/2022 y el actualmente vigente.

las TIC y el carácter transnacional de muchos de estos ilícitos. En nuestra opinión, y de modo telegráfico, consideramos que ambas figuras son compatibles en este ámbito, puesto que obedecen a presupuestos fácticos diferentes. En aquellos supuestos en los que se dé una relación bilateral entre dos sujetos y medie engaño que induzca a error al sujeto pasivo, no habría óbice para estimar que nos hallamos ante una estafa subsumible en el art. 248 CP –siempre y cuando concurran los restantes elementos típicos–. No obstante, no siempre será fácil deslindar con tanta nitidez, por lo que habrá de estarse al caso concreto y a sus circunstancias específicas.

Con todo, no se trata de una cuestión que se pueda zanjar en una afirmación simplista o reduccionista, inopinada y que no se sustente en argumentos dogmáticos o de técnica penal, sino que habrá de estarse al caso concreto para valorar qué concretos elementos típicos se dan. En este sentido, no podemos obviar que en aquellos casos en los que las TIC constituyan únicamente el medio comisivo –instrumental–, pero no haya ningún artificio informático o técnico, se puede sostener que existe una estafa tradicional. El caso prototípico sería el de un anuncio de venta falso en una página web, a través del cual se ponen en relación dos personas para la venta de un bien o servicio, la víctima abona el precio y la contraprestación no se produce. En este esquemático supuesto ha existido un engaño que ha inducido a error al perjudicado, y en cuya virtud ha realizado el acto de disposición patrimonial generador del perjuicio.

Somos conscientes de que la voluntad del legislador en la LO 14/2022 es dotar de autonomía a las ciberestafas y, al hilo de la normativa comunitaria, potenciar y reforzar su ámbito de aplicación. Ello se observa en la Consulta 1/2024, de la Fiscalía General del Estado, de 21 de marzo, sobre algunas cuestiones relacionadas con la utilización fraudulenta de instrumentos de pago distintos del efectivo. En este texto se aporta una serie de criterios de interpretación del art. 249 CP. En él se afirma que: “En opinión de la doctrina mayoritaria, tanto la estafa informática como la utilización fraudulenta de medios de pago de los arts. 249.1.a) y 249.1.b) CP se consideran modalidades típicas que tienen auténtica autonomía y sustantividad frente al tipo básico de estafa del art. 248 CP”. Además, la citada consulta

rechaza que quepa el delito leve de estafa informática *ex* art. 249 CP, cuando zanja que "al margen del tenor literal del art. 249 CP y del art. 9 de la Directiva (UE) 2019/713 y con independencia de la *voluntas legislatoris* expresada en la MAIN del anteproyecto de ley, existen razones de carácter teleológico y lógico-sistemático para rechazar que los supuestos en los que la cuantía defraudada no supere los 400 euros puedan ser calificados como delito leve de estafa".

Pues bien, ello no es óbice para mantener las afirmaciones expresadas con anterioridad, antes, al contrario. Hemos de discriminar cuándo existe una estafa clásica (del art. 248 CP) –aunque se cometa a través de las TIC, como mero cauce, canal o herramienta a través del que se vehicule el engaño– y cuándo nos hallamos ante una estafa informática, cuya regulación se contiene en el art. 249 CP. Como podemos apreciar, se trata de cauces diferentes y con tratamientos distintos. Si bien, reiteramos, en algunas ocasiones será complejo discernir cuál de los dos preceptos resulta aplicable, sobre todo, cuando aparezcan, entremezclados, elementos de engaño –como medio comisivo típico– y manipulaciones informáticas o artificios semejantes, con accesos, inmisiones e intromisiones. En tal caso, podríamos acudir al principio de especialidad, contenido en la regla 1.ª[6] del art. 8 CP, y considerar aplicable el art. 249 CP, si se aprecia dicho concurso de normas. Por el momento no contamos con doctrina jurisprudencial actual, tras la reforma de la LO 14/2022, que brinde criterios de delimitación nítidos, precisos y extrapolables a casos similares, por lo que habrá que aguardar los avances en la práctica judicial.

En todo caso, si nos adentramos en las diferentes clases de ciberestafas, podemos apreciar que existe una gran variedad de tipologías y modalidades comisivas. Algunas de ellas más burdas y obvias –como envíos de correos *spam*–, otras, más elaboradas y sofisticadas. Lo primero que llama la atención es que su comisión se ve favorecida por el empleo de técnicas de ingeniería social,

6. Art. 8.1.ª CP: "Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de este Código, y no comprendidos en los artículos 73 a 77, se castigarán observando las siguientes reglas: 1.ª El precepto especial se aplicará con preferencia al general".

que el Instituto Nacional de Ciberseguridad (INCIBE) define como[7] "técnicas de manipulación psicológica con el objetivo de conseguir que los usuarios revelen información confidencial o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente", y que consisten en el uso de canales de propagación masivos, como el correo electrónico, llamadas telefónicas, aplicaciones de mensajería o redes sociales. El INCIBE alude a dos modalidades de técnicas de ingeniería social, dependiendo del número de interacciones que requieran por parte del ciberdelincuente: (i) *hunting*, que busca afectar al mayor número de usuarios realizando, únicamente, una comunicación, y que es común en campañas de *phishing* realizado contra entidades bancarias o energéticas, o bien, en acciones que pretenden realizar acciones de infección de *malware* para efectuar ulteriores ataques de *ransomware*; (ii) *farming*, donde los ciberdelincuentes realizan varias comunicaciones con las víctimas hasta conseguir su objetivo u obtener la mayor cantidad de información posible, donde se podrían incluir las campañas que pretenden infundir temor al receptor con la existencia de vídeos privados suyos o futuros ataques contra su organización. Desde el INCIBE se explica que estos ataques de manipulación de las víctimas suelen seguir una serie de principios básicos: el respeto a la autoridad, la voluntad de ayudar –fundamentalmente, en entornos laborales–, el temor a perder un servicio, el respeto social y la gratuidad.

Por poner algunos ejemplos clásicos de ciberestafas, podemos mencionar: (i) la ciberestafa extorsiva, en la que se comunica mediante mail o sms que hemos sido objeto de una sanción administrativa, de una multa de tráfico, de una inspección tributaria o de la Seguridad Social, etc., y se nos solicita un pago para poner fin a dicho procedimiento. Suelen remitirse desde direcciones de correo electrónico que pretenden emular los correos corporativos de tales entidades, con membretes y links a páginas web que, en realidad, no son las legítimas, por lo que también efectúan suplantaciones de identidad de tales entes –*spoofing*–, aunque suelen ser montajes burdos y toscos. En otras ocasiones, se amenaza con la difusión de un vídeo de contenido íntimo si

7. INCIBE (2019). Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. Publicado el 5 de septiembre de 2019. https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

el sujeto no obedece a la petición formulada; (ii) la ciberestafa de lotería, en la que se anuncia al receptor que ha obtenido un premio –de un concurso o sorteo en que no ha participado– y se le indica que, para su cobro, ha de abonar una suerte de tasa o adelanto; (iii) las ciberestafas laborales, en las que se oferta al destinatario un puesto de trabajo, a desempeñar desde su domicilio, con una alta rentabilidad, a cambio de facilitar sus datos personales y de facilitar una cuenta bancaria. Se indica que la empresa está radicada en el extranjero y que la pasarela de pagos no admite sus cuentas bancarias, por lo que se interesa al candidato al puesto que aperture una cuenta –o facilite la suya– y, a través de este medio, vehicular diferentes pagos. En realidad, las cibervíctimas suelen ser utilizadas, en muchas ocasiones, como mulas de los fondos ilícitamente obtenidos; (iv) las ciberestafas románticas, en las que los ciberdelincuentes se ganan la confianza del receptor, le hacen ver que están iniciando una relación sentimental y, en un momento dado, tras ganarse su confianza, le solicitan abonos dinerarios con diferentes excusas; (v) el fraude del CEO, en que el ciberdelincuente, tras haber obtenido determinada información de una organización, remite a uno de sus integrantes un mail, haciéndose pasar por otro sujeto –el CEO o una persona con capacidad de mando, o directivo de algún departamento–, y requiere una modificación en las transferencias por determinados servicios, o varía una orden de pago; (vi) fraudes en herencias, similar a la estafa de la lotería, se comunica que existe una herencia muy cuantiosa y que el receptor puede obtener dicho monto si abona una tasa o pago por cuestiones burocráticas de tramitación interna; (vii) comunicaciones –vía SMS o mail– sobre problemas existentes en un envío de correos, para lo que es preciso verificar algunas cuestiones en un link que se remite en el cuerpo del mensaje. Esta ciberestafa tiene la particularidad de que, dado el alto volumen de compras *online* que se realizan, es muy factible que el destinatario del mensaje esté esperando la llegada de un paquete, por lo que no le sorprendería recibir una comunicación al respecto –de Correos, SEUR, MRW, Amazon, FedEx...–, podría otorgar credibilidad al remitente y, en consecuencia, hacer *click* en el enlace malicioso. Constituye una buena muestra de cómo la variación de nuestros hábitos de consumo puede abrir el portillo a ulteriores victimizaciones; (ix) anuncios fraudulentos de compraventa de bienes y servicios en los que la característica es que

la víctima toma la iniciativa, contacta con el número de teléfono o mail que ha insertado el anuncio, abona el precio convenido y, finalmente, nunca recibe la contraprestación pactada –teléfonos móviles, videoconsolas, entradas de conciertos, perros...–. Sin lugar a dudas, esta modalidad es la más relevante, numéricamente, en la práctica de los juzgados y tribunales. Por tal motivo, señalaremos algunos de sus rasgos característicos con mayor profundidad que las restantes. Los precios requeridos no superan los 400 euros, lo que provoca que nos hallemos ante ciberdelitos leves –si asumimos que sigue operando el art. 248 CP y que en ellas predomina el engaño–, en los que no cabría realizar una fase de instrucción.

Los anuncios se insertan en portales legítimos de compraventa de artículos, camuflados entre otros anuncios reales. Los ciberdelincuentes entablan conversaciones con los supuestos compradores y les facilitan datos personales y hasta fotografías de DNI, lo que dota de verosimilitud al engaño y crea un cierto clima de confianza recíproca. Hemos de apuntar que, en muchas ocasiones, tales DNI son de anteriores víctimas, por lo que resulta usual que, en la práctica, nos encontremos con personas que han sido victimizadas, denuncien la estafa padecida y, con posterioridad, tales personas se vean denunciadas por hechos similares posteriores, dado que los ciberdelincuentes han empleado sus datos personales para cometer otras estafas. Asimismo, se observan anuncios reduplicados en distintos portales web, y que los mismos sujetos oferten diferentes bienes y servicios, sin relación entre ellos.

En este punto, debemos subrayar la posibilidad de que distintos tipos de ciberestafas sean cometidas mediante IA, lo que introduce mayores elementos de complejidad. En este sentido, Alonso Cebrián y Velasco Núñez (2024) advierten que la suplantación de datos personales digitalizables, como la voz o la imagen, se está utilizando, en el campo económico, para llevar a cabo distintas estafas, y mencionan la estafa del CEO, así como la del supuesto hijo que comunica a sus padres que tiene problemas en el aeropuerto. También citan la ciberestafa consistente en suplantar la identidad, en la que se lleva a cabo la apertura de cuenta bancaria, y en la que "agregan reclamos con aparentes elementos identitarios (voz, imagen) falseados/creados con IA

para suplantar personas que mueven a hacer los desplazamientos patrimoniales perseguidos", y apuntan otras modalidades tan sofisticadas como el SIM *swapping*, "emitido por algoritmos de IA controlada una vez se conocen datos 'pescados' de quien se quiere suplantar para recibir del banco las claves necesarias para autenticar la cuenta a defraudar". Asimismo, podemos resaltar, siguiendo a Morillas Fernández (2023), que se pueden cometer, a través de IA, actos de *spear phishing*, en los que se envían correos electrónicos –o bien, se replican páginas web legítimas o mensajes de texto–, y se solicita información a la víctima, o bien, que inicie sesión en alguna plataforma, y donde lo relevante es la obtención del acceso. Pues bien, como sintetiza dicho autor, a través de esta información, los sistemas de IA pueden analizar los hábitos de los usuarios de las TIC y confeccionar emails fraudulentos "mucho más sofisticados que los que han sido elaborados a través de tradicionales técnicas de *social engineering*", y concluye que, de esta forma, se incrementan "las posibilidades de inducir a error a los internautas obteniendo de forma ilícita datos personales contenidos en tarjetas de crédito, credenciales para acceder *a home banking*, datos sanitarios, etc.". En esta misma línea, Jiménez (2024) centra la atención en el elevado grado de sofisticación de las estafas telefónicas cometidas mediante IA. Destaca que esta no solo es capaz de imitar las voces, sino también de replicar las pausas, las muletillas y las características que hacen única cada forma de hablar. Indica que en Reino Unido se cometió una estafa de 240.000 euros, cuando un empleado recibió una llamada telefónica de su presunto jefe, en la que le ordenaba que realizase, con urgencia, una transferencia. En realidad, el supuesto jefe resultó ser una voz clonada generada mediante IA.

Tras llamar la atención sobre algunos de los casos prototípicos de ciberestafas y advertir de los riesgos que comporta la IA en este ámbito, de un alcance insospechado e insospechable en estos momentos, debemos aludir, en este punto, a otro aspecto basilar de las ciberestafas, que nos permitirá catalogar los hechos como delito o no. Hacemos referencia a los denominados "deberes de autoprotección" que tendría la víctima. En apretada síntesis podemos indicar que tales deberes consisten en ciertas cautelas o medidas de salvaguarda que ha de adoptar un sujeto para evitar ser víctima de delitos. No aparecen regulados, como

tales, en el Código Penal; no obstante, nos sitúan en el ámbito de la influencia que puede tener el comportamiento de la víctima en su proceso de victimización y, a efectos penales, en la calificación jurídica de los hechos cuando se omiten tales cautelas. Su análisis ha de llevarse a cabo al valorar la imputación objetiva del resultado dañoso al autor de la conducta que, causalmente, ha generado un concreto resultado lesivo. Por lo que respecta a nuestro ámbito, en el delito de estafa, no cabe extralimitar su alcance. Debemos tomar en consideración que el tipo no alude a ellos, por lo que no es dable un recurso exacerbado a dicha figura, so riesgo de perpetuar situaciones de impunidad. Es evidente que ha de descartarse la idoneidad del engaño en los supuestos de ardides burdos, evidentes, toscos o grotescos, si bien, ello ha de analizarse, de modo fundamental, desde la perspectiva de la conducta defraudatoria, tomando como base las características personales de la víctima. La jurisprudencia de la Sala 2.ª del Tribunal Supremo (TS) ha llevado a cabo una evolución, desde supuestos en los que se destacaba la atipicidad de la conducta por la ausencia de los deberes de autoprotección, a otra intelección restrictiva, en la que estima que no cabe imponer a la víctima desproporcionados y excesivos deberes de autotutela[8].

Por lo tanto, en el ámbito de la ciberdelincuencia, los usuarios de las TIC han de adoptar las cautelas y medidas de seguridad necesarias, tanto en sus dispositivos telemáticos, como en sus prácticas y en la utilización de las TIC. Existe una pluralidad de medidas de diligencia y cautelas recomendables, si bien, no cabe realizar una interpretación maximalista de las consecuencias de la omisión de tales cautelas. En este sentido, ha de promoverse una intelección restrictiva de la virtualidad exculpatoria de la omisión de los deberes de protección en el ciberespacio, a la vista de la normativa comunitaria, en que se promueve la detección, persecución y sanción de tales fraudes. Puesto que abundan las posibilidades de victimización, ante la nueva configuración de las relaciones espacio-temporales, deben tomarse en consideración todos los elementos concurrentes. Ha de ponerse en relación con el concepto de riesgo permitido, con el concreto

8. *Vid*. al respecto STS 230/2021, de 11 de marzo, ponente Excmo. Sr. D. Javier Hernández García, ECLI:ES:TS:2021:996.

giro, tráfico o sector en que se lleva a cabo la acción, con los principios de confianza y de buena fe, y, de modo esencial, con las características personales del sujeto que opera su autopuesta en peligro.

Asimismo, a modo de cierre del apartado, y a simple título de esbozo, no podemos pasar por alto que pueden darse algunas áreas de confluencia de la ciberestafa con otros tipos delictivos, por lo que pueden surgir dudas a propósito de si nos hallamos ante un concurso de normas, o bien, de delitos y, en este último caso, a la hora de precisar qué concreta relación concursal se da. Sin pretensión de agotar la materia y a los meros efectos ejemplificativos, más allá de los clásicos ejemplos concursales de la estafa tradicional con los delitos de apropiación indebida o de falsedades, podríamos aludir a otras tres situaciones concursales, que presentarían mayor conexión con las TIC, y que surgen en relación con los delitos contra la intimidad (art. 197 CP), de daños informáticos (art. 264 CP) o de usurpación del estado civil (art. 401 CP). Por lo que hace a los delitos contra la intimidad, podemos pensar en el supuesto de una persona que se apodera de los datos personales de otro, que están registrados en un fichero o soporte –un *smartphone* o un ordenador donde están almacenadas las claves bancarias– y, a continuación, lleva a cabo la transferencia inconsentida. Existirían argumentos para defender que se trata de un concurso real de delitos, aunque tampoco sería descabellado apreciar que nos encontramos ante un concurso medial, en que el ataque a la intimidad es el medio para llegar al fin perseguido, de naturaleza patrimonial.

En segundo término, si prestamos atención a la relación concursal entre la ciberestafa y el delito de daños, debemos efectuar varias matizaciones: se aprecia un solapamiento de algunas modalidades de conducta entre el art. 249 CP y el art. 264 CP, puesto que en ambos delitos se mencionan, como verbos nucleares, "borrar", "alterar" y "suprimir" datos informáticos. Observamos que la pena es idéntica en ambos delitos. Así las cosas, podríamos abogar por la existencia de un concurso de normas, a resolver mediante el principio de especialidad, en virtud del ánimo de lucro que guía al sujeto activo en la estafa, por lo que podría prevalecer dicho tipo. Incluso, podría argumentarse que los daños constituyen un medio para cometer la estafa: se

emplean tales comportamientos, lesivos para los datos y que los dañan, para conseguir la transferencia inconsentida. Por lo tanto, se deja abierto el supuesto, dado que únicamente se apuntan las alternativas en presencia, pero sin pretensión de exhaustividad.

En último lugar, por lo que hace al delito de usurpación del estado civil, pese a que en algún momento se haya podido indicar que es dable apreciar un concurso de delitos con la estafa, cuando se empleen los datos personales y señas de un tercero para cometer la estafa, debemos excluir dicha posibilidad si no existe una permanencia en el tiempo, puesto que la jurisprudencia de la Sala 2.ª exige una continuidad temporal, como se indicó en la STS 1045/2011[9], de 14 de octubre, en la que se expresa que "la conducta del agente exige una cierta permanencia y es ínsito al propósito de usurpación plena de la personalidad global del afectado". Si bien, debemos recordar que la LO 10/2022, de 6 de septiembre, introdujo el art. 172 ter 5 CP, en el que se castiga a quien, sin consentimiento de su titular, utilice la imagen de una persona para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la víctima una situación de acoso, hostigamiento o humillación. No obstante, *prima facie*, no concurrirían los requisitos del art. 401 CP en el supuesto de hecho que hemos indicado.

Con todo, tanto en los tres supuestos que hemos anotado, como en otras posibles situaciones concursales que se puedan originar, habrá que estar a las circunstancias del caso concreto para determinar, con precisión, qué nexo, engarce o ligazón se produce entre los distintos tipos en presencia, si es que se da dicha conexión. Por lo tanto, reiteramos que las soluciones apuntadas aquí son provisionales, genéricas y parciales, por lo que nos mostramos expectantes y aguardamos las propuestas doctrinales y los pronunciamientos judiciales que arrojen luz sobre dicha materia.

9. STS 1045/2011, de 14 de octubre, ponente Excmo. Sr. D. Juan Ramón Berdugo Gómez de la Torre, ECLI:ES:TS:2011:6858.

3.2.2 Delitos de daños informáticos (arts. 264-264 quater CP)

La afectación al patrimonio de los delitos de daños resulta incuestionable, aunque nos hallamos ante delitos patrimoniales sin enriquecimiento, por lo que constituyen una suerte de rareza en el Título XIII[10]. Pues bien, si atendemos a los delitos de daños informáticos, podemos convenir en que, en ocasiones, la finalidad que guía al ciberdelincuente puede ser variada. No podemos obviar que, en algunos casos de intrusiones o de ataques de denegación de servicio –ataques *DoS*–, o distribuidos de denegación de servicio –ataques *DDoS*–, se pretende llevar a cabo actos de *hacktivismo*, con motivaciones políticas o ideológicas, lo que se puede observar en el colapso temporal de servidores web de grandes empresas multinacionales o de servicios públicos, en los que se persigue exteriorizar una reivindicación política. En otras ocasiones, según la magnitud del ataque, sus destinatarios y sus consecuencias, podríamos hallarnos ante casos de ciberterrorismo, por lo que, como podemos apreciar, en estos supuestos nos hallaríamos, más bien, ante ciberdelitos de corte político y no meramente económicos. Con ello constatamos que, algunas veces, las líneas divisorias entre las clasificaciones de ciberdelitos son permeables, porosas y permiten diversas gradaciones. Podemos discriminar los delitos de "sabotaje informático" o interferencia ilegal en datos informáticos –art. 264.1 CP–, cuya conducta típica se configura de modo mixto alternativo, el delito de daños informáticos a sistemas –art. 264 bis.1 CP–, donde se reprime obstaculizar o interrumpir el funcionamiento del sistema informático ajeno y un adelantamiento de las barreras de punición, contenido en el art. 264 ter CP, en el que nos hallaríamos ante actos preparatorios o protopreparatorios de los anteriores. Cabe significar que, al igual que en los restantes delitos de daños, el bien jurídico tutelado es la propiedad, si bien, en algunas de las conductas tipificadas se pone de relieve que se trasciende del patrimonio individual y se atiende a intereses supraindividuales, toda vez que en los tipos cualificados se valora que la afectación se pro-

10. Para una exposición completa de los delitos de daños, *vid*. González Uriel (2022). Nuevamente, se aconseja una lectura de los preceptos citados, a los efectos de una comprensión acabada.

pague a una pluralidad de sistemas informáticos, o bien, que afecte al funcionamiento de servicios públicos que puedan ser reputados como esenciales, o a la provisión de bienes de primera necesidad, que se afecte a una "infraestructura crítica", o que se ponga en peligro la seguridad estatal, de la UE o de un Estado miembro de la UE. Como se puede observar, en tales supuestos no solo se está tutelando la propiedad privada, sino que se pone de manifiesto la capacidad dañina de los ataques informáticos y la posibilidad de que se afecten los intereses generales y la propia seguridad nacional.

Por lo que a nosotros interesa, debemos señalar los peligros que se derivan de determinados delitos de daños, como los ataques de *ransomware* o secuestros de datos, en los que se produce un acceso inconsentido en un sistema informático ajeno, mediante un *malware* que lo infecta y accede a la totalidad o parte de sus datos, que se cifran, y se impide a su titular el acceso a ellos, en todo o en parte, y se solicita el pago de un rescate para poder recuperar el acceso o los datos en cuestión. Asimismo, en muchas ocasiones, la petición del rescate se hace en criptomonedas, para robustecer el anonimato, evitar la trazabilidad de los fondos y la persecución de los autores del ataque. Conviene destacar que tales ciberataques se realizan tanto a personas físicas como jurídicas, públicas y privadas, y gozan de especial repercusión mediática cuando se efectúan a servicios públicos, como hospitales, por los notables perjuicios personales que irrogan, no solo por los actos médicos que se cancelan y dilatan, sino también por la obtención de datos sensibles de multitud de pacientes, que pueden acabar vendiéndose en la *dark web* –no está de más recordar el manido lema de que los datos personales constituyen el petróleo del siglo XXI–. Además, cabe agregar que se han dado casos de ataques de *ransomware* recurrentes frente a las mismas víctimas, con posterioridad a que hubieran abonado el rescate. Podemos vaticinar que existe una notable cifra negra en este campo, sobre todo, en el ámbito empresarial, toda vez que las corporaciones desean evitar cualquier publicidad negativa o desconfianza en sus sistemas de ciberseguridad, toda vez que la denuncia de estos hechos expondría, públicamente, la existencia de vulnerabilidades en sus sistemas de protección, lo que generaría un notable daño reputacional.

En segundo lugar, como ciberdelito de daños con repercusión patrimonial, debemos destacar que los ataques *DoS* y *DDoS*, que en muchas ocasiones son ejecutados a través de redes de *bots*, consisten en dirigir una multitud de peticiones a sitios web y redes, hasta saturarlas, sobrecargando sus servidores y evitando que sean accesibles a usuarios legítimos, lo que provoca su parálisis. Estos ciberataques se han dirigido frente a grandes empresas y también frente a organismos públicos, saturando sus servidores y portales web. Podemos hacernos una idea de los notables perjuicios económicos que se pueden derivar de la paralización de los servidores web de una empresa, si pensamos en la contratación *online*, en la formalización de pedidos o, incluso, en su propio sistema de comunicaciones con terceros –acreedores, proveedores, deudores...–. Estos ciberataques pueden prolongarse en el tiempo, por lo que los efectos producidos se pueden dilatar, incrementando el perjuicio económico.

3.2.3 Delitos contra la propiedad intelectual e industrial (arts. 270-277 CP)

Dentro de estas figuras delictivas, podemos destacar la relevancia de la piratería informática o digital, esto es, la descarga de contenidos amparados por derechos de autor sin el abono de los pagos correspondientes. Desde una perspectiva criminológica se han propuesto diferentes explicaciones sobre un fenómeno tan extendido y normalizado. En este sentido, desde la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2019) se ha explicado que "las normas socioculturales y el comportamiento y la dinámica de grupo influyen en las tasas de piratería digital". También destaca que los autores de delitos contra la propiedad intelectual cometidos a través de las TIC utilizan cierta técnicas de "neutralización" –entre otras, negación de responsabilidad, negación de la víctima, negación del daño, condena de los condenadores y apelación a una mayor lealtad–, si bien, se ha matizado que dichas técnicas varían y, en otras investigaciones sintetizadas por UNODC, se expresa que las "asimetrías digitales" –como puede ser la falta de supervisión inmediata de las acciones realizadas *online*– "pueden contribuir a que las personas 'opten' hacia la desviación digital y accedan a información o recursos que apoyen o normalicen actos delictivos como la piratería". Además, desde UNODC se atiende a otros aspectos

etiológicos de los ciberdelitos contra la propiedad intelectual, como el sentimiento antiempresarial o los altos costos –reales o percibidos– de las obras amparadas por derechos de propiedad intelectual y, en este sentido, se refleja que "si los consumidores creen que existe una discrepancia injusta entre el valor, la calidad y el precio, buscan medios alternativos para obtener el bien (a un precio más bajo o mediante la piratería, la obtención, el acceso o el uso no autorizado de la propiedad intelectual de otro)". Asimismo, en la exposición realizada por UNODC se finaliza indicando que también se ha sugerido por diferentes autores que el drástico incremento de la piratería digital desde finales de la década de 1990 se produjo como "respuesta pública al exceso de legislación en materia de protección de la propiedad intelectual".

No podemos obviar que el volumen de piratería digital (art. 270 CP) irroga elevadísimos perjuicios económicos a los titulares de los derechos de propiedad intelectual, puesto que se trata de un comportamiento globalizado, continuo y permanente. Nos hallamos ante una práctica extendida, generalizada, en la que se relativiza su carácter delictivo, se normalizan tales acciones y se asume su realización. A su vez, la descarga ilícita de contenidos se encuentra amparada por su facilidad de realización, toda vez que es sencillo, para cualquier usuario, acceder a portales web en que se ofertan tales ilícitos servicios. Además, el objeto sobre el que recae tal conducta es variado, plural y heterogéneo. No solo hacemos referencia a producciones audiovisuales –discos, películas, series o videojuegos–, sino que también se propagan servidores, páginas, aplicaciones y servicios de mensajería con bibliotecas pirata, en las que se puede descargar cualquier libro.

Mención especial merece, en sede de delitos contra la propiedad industrial (art. 274 CP), la existencia de portales web que venden falsificaciones de ropa de marca, de complementos, de joyas, de dispositivos electrónicos o de medicamentos, entre otros, a un precio inferior al del producto legítimo. Las TIC constituyen un gran cauce de difusión y propagación para estos mercados irregulares, que producen importantes mermas de facturación a las marcas legítimas. Además, se produce la paradoja de que, cuando se cierra o suprime un portal de este tipo, al poco tiempo se produce un traslado a otra página web o servidor en

que se ofrece la misma mercancía. Este traslado casi inmediato se explica por la propia estructura de las TIC y la facilidad en la creación de los portales web.

Si bien, debemos matizar una cuestión relevante. En un mercado ilícito como el de la difusión de competiciones deportivas –significadamente, partidos de fútbol–, con un gran volumen de oferta y demanda, con multitud de portales web en que se anuncia el acceso, ilícitamente, a tales contenidos, la Sala 2.ª del TS llevó a cabo una importante puntualización en la STS 546/2022[11], de 2 de junio, al abordar la retransmisión no autorizada de partidos de fútbol, y consideró que no se trata de un delito contra la propiedad intelectual (art. 270.1.4 CP), sino de un delito relativo al mercado y a los consumidores (art. 286). El Alto Tribunal estimó que contravendría el principio de legalidad su calificación como delito contra la propiedad intelectual, ya que no tiene encaje en la noción de obra o prestación literaria, artística o científica.

Hemos de realizar una mención especial a lo expresado por Interpol (2024) a propósito de esta tipología de delitos. Resume en siete los principales métodos de piratería digital: (i) aplicaciones ilegales, (ii) robo de contenidos antes de su estreno, (iii) proveedores de servicios de alojamiento extraterritorial, (iv) extracción de secuencias o *stream ripping*, (v) servicios de almacenamiento en línea o *cyberlockers*, (vi) criptomonedas y (vii) tecnologías emergentes. En su análisis, destaca que esta modalidad de ciberdelincuencia afecta a los ingresos estatales y

11. STS 546/2022, de 2 de junio, ponente Excmo. Sr. D. Manuel Marchena Gómez, ECLI:ES:TS:2022:2315, en la que se expresa: "No es fácil fijar los límites del tipo cuando éste acoge elementos normativos que evocan la literatura, el arte o la ciencia. Precisamente por ello, las pautas exegéticas para delimitar ese alcance han de ser extremadamente prudentes para no desbordar los contornos de lo que cada vocablo permite abarcar. El fútbol, desde luego, no es literatura. Tampoco es ciencia. Es cierto que en un partido de fútbol –en general, en cualquier espectáculo deportivo– pueden sucederse lances de innegable valor estético, pero interpretar esos momentos o secuencias de perfección técnica como notas definitorias de un espectáculo artístico puede conducir a transgredir los límites del principio de tipicidad. Un partido de fútbol es un espectáculo deportivo, no artístico".

expone a los consumidores al riesgo de sufrir pérdidas financieras. Apunta que, además, la piratería digital comporta riesgos para la seguridad, tales como el robo de identidad, o bien, la exposición de menores a contenidos inapropiados. Sintetiza que nos hallamos ante un delito lucrativo, ya que los servicios de piratería obtienen sus ingresos por varios medios: (i) publicidad, (ii) donaciones de sus usuarios, (iii) servicios de suscripción, (iv) venta de datos de sus usuarios a terceros y (v) publicidad de afiliados. Además, Interpol advierte de que el dinero de los usuarios de estos servicios, al utilizarlos, "se desvía a cuentas bancarias piratas mediante complejas técnicas de blanqueo de capitales". En punto a la propia ciberseguridad de los usuarios de estas plataformas, Interpol señala que tales sitios web presentan riesgos, por contener *malware* y virus, que pueden ser usados para dañar los dispositivos informáticos o para sustraer información confidencial. Anota que tales *malwares* se pueden propagar por las redes corporativas o domésticas, comprometiendo la seguridad de la organización. Subraya que también pueden servir como trampolín para el robo de identidad, y que los consumidores se enfrentan a un riesgo jurídico, "al suscribirse a servidores *proxy* que podrían haberse usado para participar en ataques de denegación de servicio distribuida o de otro tipo en el pasado". Enumera otro conjunto de riesgos: (i) que los contenidos pirateados se empleen como trampa para el robo de datos personales, información bancaria u otro tipo de información confidencial; (ii) que los métodos de pago no seguros pueden dar lugar a fraudes con tarjetas de crédito o débito, u otras estafas financieras; (iii) que las actualizaciones de *software* –o su ausencia– para productos obtenidos de modo ilegal pueden provocar fallos de seguridad.

3.2.4 Blanqueo de dinero (arts. 301-304 CP)

En último lugar, debemos aludir a la viabilidad del blanqueo de dinero mediante las TIC. La propia configuración normativa de este tipo[12], su imparable expansionismo –legislativo e interpretativo– y las características del ciberespacio

12. Para un análisis en profundidad del delito de blanqueo de dinero, *vid.* González Uriel (2021).

propician que este nuevo ámbito de oportunidad criminal sea especialmente apto para la comisión de actos de ciberlavado de activos. En resumen, podemos describir el blanqueo de dinero como el proceso por el cual se pretende la reintroducción en el tráfico económico-financiero de curso legal de unos bienes que proceden de un delito. Por lo tanto, en su configuración más elemental, el blanqueo no pasa de ser –ni más, ni menos– el alejamiento de los bienes de su ilícita procedencia y su afloramiento con la finalidad de dotarles de una pátina de legitimidad, obtenida a través de diferentes negocios jurídicos. Nos hallamos ante un delito de referencia, que precisa de un delito fuente al que ir referido, pero que es autónomo, y que además se configura como un tipo pluriofensivo, que tutela la licitud de los bienes en el tráfico económico-financiero de curso legal y la Administración de Justicia. Además, coexiste con la normativa administrativa de prevención, la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, lo que puede provocar áreas de confluencia, solapamiento y confusión.

El anonimato que permiten las TIC es una cualidad que favorece que sean empleadas para llevar a cabo actos de lavado. Asimismo, también influye la ausencia de fronteras, la posibilidad de deslocalización y el empleo de artilugios técnicos para ocultar y modificar la IP. Debemos convenir en que, a través de las TIC, se mueve una gran cantidad de bienes con contenido económico. Es un ámbito abonado para la facilidad en las transferencias de bienes y para el desarrollo de una pluralidad de negocios jurídicos de contenido patrimonial. Pensemos que algunos ámbitos como los juegos de azar, las apuestas o los casinos *online* son entornos idóneos para camuflar ganancias procedentes de un delito. Además, nuevos elementos, como los juegos *online*, se han convertido en terrenos empleados para llevar a cabo la legitimación de fondos. En este sentido, debemos subrayar que las TIC se pueden emplear tanto para lavar el dinero obtenido en el entorno *offline* como para legitimar los propios fondos dimanantes de ciberdelitos –*v. gr.*, las cantidades obtenidas mediante ciberestafas o los pagos de rescates para que cesen ataques de *ransomware*–.

Precisamente, hemos de conectar el fenómeno del lavado de bienes con las organizaciones criminales, dado que constituye uno de sus principales ámbitos operativos. Se ha observado que las organizaciones criminales tradicionales están llevando a cabo una traslación parcial al ciberespacio para asegurar sus montos de procedencia delictiva, como se ha apreciado en alguna operación policial[13], por lo que están diversificando los cauces a través de los cuales reciclan los activos delictivos, y la legitimación de fondos se lleva a cabo tanto por los canales tradicionales como a través de las TIC. En este sentido, Interpol señala que la delincuencia organizada utiliza las ganancias obtenidas para otras actividades ilegales, como el juego ilegal en línea, la explotación sexual en línea, el tráfico de drogas, la trata de personas, el tráfico de armas o el blanqueo de dinero. Además, se ha constatado que otras organizaciones criminales han surgido en el propio ciberespacio y su actividad delictiva se desarrolla en él: podemos aquí hacer alusión a las organizaciones internacionales dedicadas a la realización de ataques de *ransomware* por todo el mundo.

Pues bien, a la hora de favorecer el anonimato, romper la trazabilidad de los fondos, diluir su rastro, ocultar su procedencia delictiva y llevar a cabo su afloramiento ulterior, en la actualidad, juegan un papel destacado las criptomonedas (Casals Fernández, 2022). En el art. 3.1.5) del Reglamento (UE) 2023/1114, del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937, se definen los criptoactivos como "una representación digital de un valor o de un derecho que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro distribuido o una tecnología similar". Podemos apostillar que los criptoactivos no constituyen dinero de curso legal, no están sometidos a una autoridad central, ni presentan una regulación, un tipo de cambio ni una normativa oficial. De hecho, el punto de conexión entre el blanqueo

13. *Vid.* la noticia "La mafia italiana se pasa al cibercrimen desde Tenerife". *Diario El País* el 25 de septiembre de 2021. https://elpais.com/tecnologia/transformacion-digital/2021-09-25/la-mafia-italiana-se-pasa-al-cibercrimen-desde-tenerife.html

de dinero y los criptoactivos viene dado por su capitalización, su monetarización y conversión en dinero FIAT. En este aspecto juegan un destacado papel los *exchangers*, los servicios de conversión de criptoactivos, por lo que resulta esencial que cumplan con las obligaciones de información y registro impuestas por la normativa europea, en orden a prevenir operativas de lavado de activos, por lo que se erigen en sujetos especialmente obligados al cumplimiento de una serie de obligaciones y deberes. La adquisición de criptoactivos por las organizaciones criminales y sujetos que pretendan blanquear se basa en el anonimato tendencial que presentan, toda vez que, en la tecnología *blockchain* que emplean, lo que consta es la existencia de las transacciones, ligadas a monederos –*wallets*–, pero no a personas físicas individualmente identificadas. Además, existen distintas aplicaciones y servidores que funcionan como "mezcladores" –*mixers*–, que permiten romper la trazabilidad de las operaciones y mezclar criptomonedas procedentes de diversos monederos, provocando que se dificulte –o impida– el rastreo de la procedencia de tales activos. Así las cosas, las criptomonedas se emplean como refugio de dinero sucio obtenido en el entorno *offline*, y como lugar para asegurar las ilícitas ganancias derivadas de los ciberdelitos cometidos en Red. De este modo, mediante la sucesión de transferencias, de negocios jurídicos y de actos llevados a cabo en línea es dable desligar los bienes delictivos de su fuente, alejarlos y darles una pátina de legalidad.

Con todo, y pese a las advertencias que realizamos de la posibilidad del empleo de las TIC para llevar a cabo operativas de blanqueo de capitales, al igual que hemos reiterado en otros lugares (González Uriel, 2023), debemos patrocinar una interpretación sumamente restrictiva de la aplicación del delito de blanqueo, para contrarrestar algunos excesos intelectivos que se aprecian en materia concursal y en la comprensión de determinadas figuras, fundamentalmente, en el blanqueo imprudente. Por ende, sobre todo en los casos de ciberestafas, ha de abogarse por mantener el título de imputación a los coacusados, y por efectuar una valoración global del hecho que atienda a la aplicación de las reglas del concurso aparente de normas del art. 8 CP. De ahí que no todo delito del que derive una ganancia patrimonial vaya a implicar, *per se*, la existencia de un concurso real con el delito de blanqueo –porque exista una adquisición, pose-

sión o utilización de tales bienes–, sino que habrá de estarse al caso concreto, y habrán de tomarse en consideración diferentes criterios de restricción, como los actos neutros, el riesgo permitido, la lesión o puesta en peligro del bien jurídico tutelado, el principio de insignificancia –desechando conductas de bagatela– o, jurisprudencialmente, la exigencia de finalidad en todas las modalidades de conducta blanqueadoras –criterio este que no comparte un relevante sector doctrinal–. De especial relevancia es la figura de las mulas en las ciberestafas, cuya intervención ha sido calificada, en no pocas ocasiones, como constitutiva de un delito de blanqueo imprudente, en lugar de como una cooperación necesaria en la estafa. Hemos de eludir consideraciones apriorísticas y hemos de rechazar la traslación de deberes policiales –o parapoliciales– a los particulares, toda vez que el tipo de blanqueo no los exige, y se pueden producir situaciones de paralización de la economía, con la instauración de una suerte de desconfianza generalizada. Si bien, somos conscientes de que las TIC constituyen un terreno abonado para que las organizaciones criminales laven sus fondos delictivos, por lo que abogamos por la especialización en la materia de todos los operadores jurídicos y de las Fuerzas y Cuerpos de Seguridad del Estado (FFCSE) concernidos, ante la gran magnitud económica que pueden conllevar tales operativas de lavado y dada la complejidad técnica de estas cuestiones.

4 Algunas dificultades procesales en la detección e investigación de los ciberdelitos económicos

En este último apartado seremos deliberadamente escuetos y esquemáticos, toda vez que pretendemos dar una visión global de la problemática. En primer lugar, conviene destacar que nos hallamos ante ciberdelitos de difícil detección, puesto que, en ocasiones, la propia víctima no es consciente de su comisión –recordemos las ciberestafas de montos escasos–. Además, la propia arquitectura del ciberespacio propicia que surjan dificultades a la hora de determinar qué jurisdicción nacional está en condiciones de perseguir el delito: como ya advertimos, se trata de una delincuencia globalizada, transnacional, y que, en múltiples

ocasiones, los ciberdelincuentes emplean artificios técnicos para camuflar y deslocalizar su dirección IP, como *proxy* o VPN. Por lo tanto, en ocasiones será necesario acudir a la Ley 26/2015, de 7 de julio, por la que se regula el estatuto del miembro nacional de España en Eurojust, los conflictos de jurisdicción, las redes judiciales de cooperación internacional y el personal dependiente del Ministerio de Justicia en el Exterior. A su vez, puede generar problemas de determinación del lugar de comisión del delito cuando la acción se lleva a cabo en un país y los resultados se producen en otro u otros. En este mismo sentido, y una vez que se ha determinado la jurisdicción de los tribunales españoles, puede resultar complejo concretar qué órgano judicial es objetivamente competente, en supuestos en los que se diluyen entre diferentes partidos judiciales elementos de un tipo delictivo e, incluso, ante la posibilidad de que conozca de los hechos la Sala de lo Penal de la Audiencia Nacional, *ex* art. 65 LOPJ.

Salvados los escollos de la jurisdicción y de la competencia –ya de por sí problemáticos–, el siguiente obstáculo viene representado por la determinación de la concreta autoría. Podemos hallarnos ante supuestos de empleo de redes WiFi públicas, utilizadas por una pluralidad indeterminada de personas. En otros casos, los ciberdelincuentes pueden usurpar la clave y contraseñas de otras personas para cometer ciberdelitos. Además, y en los supuestos en que la dirección IP arroje un concreto domicilio, podrían surgir dificultades a la hora de concretar la persona que haya cometido el delito, cuando sean varios los moradores del inmueble. Otro aspecto que complica las investigaciones viene representado por aquellos casos en los que quepa el ciberdelito leve –significadamente, estafas de menos de 400 euros–, lo que veda la posibilidad de que se efectúe una instrucción judicial, con lo que se limita la potencialidad investigadora. A ello hemos de agregar que, en muchas ocasiones, y bajo la fachada de delitos leves aislados, nos encontramos ante auténticas organizaciones criminales que cometen una multitud de tales delitos. Si bien, y como lamentamos, esa desconexión en las investigaciones policiales y en la tramitación judicial de cada delito leve lleva a que no seamos conscientes de la presencia de auténticas industrias del cibercrimen, y demos tratamientos aislados y singulares a supuestos que, en puridad, forman parte de un *contínuum*.

Asimismo, en ocasiones, una misma víctima de un ciberdelito aparece como victimario en una pluralidad de cibercrímenes, en diferentes partidos judiciales porque, en su proceso de victimización, facilitó sus datos personales –fotografía y DNI– a los ciberdelincuentes, y dichos datos se emplean en una multitud de ilícitos posteriores. Con ello se perpetúan situaciones de victimización y se irrogan perjuicios adicionales, siquiera, a los efectos de contestar a cada citación judicial a un juicio por delito leve como investigado.

En punto a la ciberdelincuencia económica, debemos consignar que nos hallamos ante modalidades delictivas de difícil investigación, debido a la sofisticación técnica de alguna de las operativas empleadas, a los artificios tecnológicos utilizados, a la propia volatilidad de los elementos de prueba en el entorno *online*, a la complicación para seguir el rastro del cibercrimen y para determinar con precisión el alcance del hecho, sus autores y partícipes. Todo ello se agrava si los hechos se vehiculan a través de la *dark web*. Somos conscientes de que resulta complejo obtener la totalidad de las fuentes de prueba. En ocasiones surgen dudas a la hora de delimitar las diligencias de investigación a practicar. Pensemos en el fraude del CEO, en que se desconoce qué ha sucedido con los montos ilícitamente transferidos y no se tiene ningún indicio de quién ha cometido el hecho. Aquí juegan un papel destacado las periciales informáticas y la realización de complejas y exhaustivas investigaciones patrimoniales. A su vez, y cuando existen criptomonedas, aparecen dificultades a la hora de efectuar su trazabilidad –dado su anonimato tendencial– o, incluso, cuando se efectúa una entrada y registro en un domicilio y se obtiene un *pen drive* que contiene un *wallet* con criptomonedas, ante la ausencia de una regulación procesal específica, aparecen varias posibilidades de actuación procesal: (i) convertir la criptomoneda en dinero FIAT e ingresar la cantidad aprehendida en la cuenta de depósitos y consignaciones del juzgado; (ii) crear un *wallet* en el propio juzgado y transferir la criptomoneda; (iii) mantener el propio *wallet* del sujeto investigado, bajo la custodia del LAJ, y cambiar su clave de acceso. No se trata de una cuestión baladí, puesto que puede afectar a la responsabilidad civil en casos en que, al enjuiciarse los hechos, se produzca una variación sustancial del valor de la criptomoneda, entre la fecha de la aprehensión y la del fallo. A su vez, si se opta por mante-

ner el *wallet* del investigado, podrían acceder a él otros sujetos implicados en la trama a través de la "frase semilla", o frase de recuperación, que funciona como una llave maestra para acceder a las criptomonedas y ofrece una red de seguridad en caso de pérdida, robo o fallo de funcionamiento del dispositivo.

Puesto que hemos mencionado en repetidas ocasiones que nos hallamos ante una fenomenología delictiva transnacional, va a tener una gran relevancia el empleo de instrumentos de cooperación judicial internacional. De este modo, no solo van a existir retrasos y dilaciones en la obtención de fuentes de prueba en el extranjero, sino también en cuanto a su conservación y a su transmisión al procedimiento judicial español, por lo que hemos de tomar en consideración tales aspectos. En este sentido, y frente a la excesiva burocratización y ralentización procesales que acarrean las comisiones rogatorias internacionales, puesto que constituyen un cauce de cooperación entre autoridades gubernativas, basadas en la existencia de tratado, de ley, o en el principio de reciprocidad, en el ámbito de la UE se agiliza la cooperación a través de las órdenes europeas de investigación (OEI). Dicho instrumento reduce los trámites, puesto que la comunicación se realiza, directamente, entre autoridades judiciales. Pues bien, en el ámbito de la lucha contra la ciberdelincuencia económica podemos hacer alusión a una serie de relevantes diligencias que se contienen en los arts. 198 y ss. de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea: (i) peticiones de información sobre cuentas bancarias y financieras; (ii) peticiones de información sobre operaciones bancarias y financieras; (iii) intervenciones de telecomunicaciones; (iv) identificación de titulares de IP; y (v) adopción de diferentes medidas cautelares reales, como aseguramientos de bienes o embargos.

Estos son solo algunos de los aspectos procesales que surgen en la fase de instrucción –si es que la hay, lo que no se da en los delitos leves–, y que ponen de manifiesto la complejidad en la detección, la investigación y el enjuiciamiento de la ciberdelincuencia económica. Nos hallamos ante un fenómeno delictivo novedoso, en auge y en continua evolución en cuanto a sus operativas y dinámicas comisivas, pero no contamos con la totalidad de herramientas procesales para hacerle frente,

por lo que, y aunque suene a tópico, vamos un paso por detrás de los ciberdelincuentes. Se trata de un ámbito dinámico, técnico, que permite el empleo de artilugios tecnológicos para eludir las labores de prevención y detección del delito. Por tal motivo, debemos ser conscientes de la ardua tarea que conlleva la investigación de algunos supuestos complejos de ciberdelitos económicos, cometidos por organizaciones criminales con ramificaciones internacionales y en los que se refugien los fondos en criptomonedas y se causen multitud de perjudicados en diferentes Estados.

No obstante, no podemos obviar que contamos con importantes instrumentos para la investigación de estas tipologías delictivas. Debemos destacar la reforma de la Ley de Enjuiciamiento Criminal (LCERIM) operada por la LO 13/2015, en la que se reconoció la insuficiencia de la regulación vigente hasta ese momento[14], y, sobre todo, la incorporación de una serie de disposiciones relativas a la interceptación de las comunicaciones telefónicas y telemáticas, a la captación

14. En el apartado IV del Preámbulo de la LO 13/2015 se expresa: "La Ley de Enjuiciamiento Criminal no ha podido sustraerse al paso del tiempo. Renovadas formas de delincuencia ligadas al uso de las nuevas tecnologías han puesto de manifiesto la insuficiencia de un cuadro normativo concebido para tiempos bien distintos. Los flujos de información generados por los sistemas de comunicación telemática advierten de las posibilidades que se hallan al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos. Surge así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros. Por muy meritorio que haya sido el esfuerzo de jueces y tribunales para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática de nuestro sistema procesal, carencia que tanto la dogmática como instancias supranacionales han recordado. Recientemente, el Tribunal Constitucional ha apuntado el carácter inaplazable de una regulación que aborde las intromisiones en la privacidad del investigado en un proceso penal. Hoy por hoy, carecen de cobertura y su subsanación no puede obtenerse acudiendo a un voluntarista expediente de integración analógica que desborda los límites de lo constitucionalmente aceptable. Solo así se podrá evitar la incidencia negativa que el actual estado de cosas está proyectando en relación con algunos de los derechos constitucionales que pueden ser objeto de limitación en el proceso penal".

y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, a la utilización de dispositivos técnicos de seguimiento, a la localización y captación de la imagen, al registro de dispositivos de almacenamiento masivo de información y a los registros remotos sobre equipos informáticos. Estas medidas de investigación se regulan en los arts. 588 bis y ss. LECRIM, constituyen un poderoso arsenal de diligencias que han de ser acordadas con prudencia, en atención a la injerencia en derechos fundamentales que conllevan. Debemos recordar los principios que han de ser tomados en consideración a la hora de interesar y de adoptar tales medidas: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. Del mismo modo, la citada LO 13/2015 amplió las potencialidades del agente encubierto, incorporando en el art. 282 bis LECRIM la figura del agente encubierto informático[15].

Así las cosas, aunque hemos asumido las insuficiencias, las áreas susceptibles de mejora y algunas debilidades con las que contamos a la hora de perseguir los ciberdelitos económicos, forzoso es reconocer que la normativa procesal penal española contiene poderosas herramientas de lucha contra estas tipologías delictivas. Frente a ellas no queda sino la especialización de jueces, magistrados, fiscales y miembros de FFCCSE, la llamada a la colaboración entre las autoridades judiciales nacionales, la conformación de equipos conjuntos de investigación, la lealtad interinstitucional en el desarrollo de las investigaciones y, sobre todo, la formación continua, la actualización de contenidos y el reciclaje en una fenomenología delictiva que ha llegado para quedarse y frente a la que debemos estar preparados.

15. Art. 282 bis.6 LECRIM: "6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.

El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos".

5 Conclusiones

1.ª El ciberespacio constituye un nuevo entorno de oportunidad criminal, en el que el ámbito de victimización viene determinado por la propia víctima que es quien, con su conducta, delimita qué concretos bienes jurídicos suyos pueden ser lesionados o puestos en peligro. Por lo tanto, y sin que ello implique responsabilizar a la víctima de su proceso de victimización, hemos de partir del hecho de que la incorporación de los bienes jurídicos al ciberespacio se lleva a cabo por la propia víctima. El ciberespacio puede provocar variaciones en el comportamiento de sus usuarios, y que lleven a cabo actos de riesgo que no verificarían en el entorno *offline*, dado que, en ocasiones, se produce la influencia del "efecto desinhibitorio *online*".

2.ª Los ciberdelitos constituyen la tipología delictiva que más aumenta, según los últimos datos oficiales sobre criminalidad en España. Ello se debe a que buena parte de los actos y actividades cotidianas de las personas se han trasladado, parcial o completamente, al ciberespacio. De este modo, se ha trasladado a las TIC la mayor parte de los ámbitos de desarrollo de las personas: social, económico, comercial, relacional, laboral, cultural, educativo... Y ello propicia que dicha incorporación vaya acompañada de un auge de los ciberdelitos, lo que se ve favorecido por las propias condiciones y circunstancias del ciberespacio como medio de comisión de actividades ilícitas, dado que no existen barreras, ni fronteras, ni instituciones centralizadas de control, y ante el rediseño de las relaciones entre las variables espacio y tiempo, lo que propicia que con un solo acto se llegue a una multitud de potenciales víctimas.

3.ª Dentro de los ciberdelitos, los de contenido económico resultan preponderantes, tanto cualitativa como cuantitativamente. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos, el desconocimiento de los sujetos y las potencialidades que brinda el ciberespacio

para cometer delitos con una finalidad lucrativa. El principal ciberdelito que se comete es el fraude –estafa–. Existe una pluralidad de modalidades comisivas de dicho delito, algunas más sofisticadas y elaboradas, y otras más burdas y zafias. En todo caso, todas ellas persiguen la obtención de un lucro por fines espurios, empleando para ello engaños y ardides, o bien, manipulaciones informáticas, técnicas o artificios semejantes. No obstante, ante la rentabilidad de estos comportamientos, se ha observado una proliferación en los ciberdelitos de corte económico, y también se han incrementado los delitos de daños informáticos, los delitos contra los derechos de propiedad intelectual e industrial, así como los actos de blanqueo de los fondos delictivamente obtenidos en el ámbito de las TIC, por lo que podríamos atender a nuevas modalidades de ciberblanqueo.

4.ª Nos hallamos ante delitos de difícil persecución, ante la complejidad para determinar las conductas punibles, su alcance y sus resultados, resultando complicado establecer la autoría y la participación en estos comportamientos. En estas tipologías delictivas va a ser muy importante obtener las fuentes de prueba con celeridad, ante su volatilidad. Es preciso efectuar rigurosas investigaciones patrimoniales en las que se pueda verificar la trazabilidad de los fondos. Otra dificultad viene dada por el carácter tendencialmente internacional de estos delitos, por la implicación de organizaciones criminales y por las dudas en cuanto a las diligencias de investigación a practicar. Es preciso que se optimicen los cauces de cooperación judicial internacional, que se constituyan equipos conjuntos de investigación y que se aclaren los criterios de atribución competencial en cada uno de los delitos investigados.

5.ª Se trata de una serie de delitos en continua evolución, dinámicos, cambiantes, y donde surgen elementos distorsionadores, como las criptomonedas o la inteligencia artificial, que exigirán pronto nuevas respuestas específicas, ante la insuficiencia de los medios actuales con algunas de sus aplicaciones prácticas. Ante los avances técnicos, es preciso que la normativa se acompase y adapte, que se brinden a los juzgados y tribunales las herramientas necesarias para la persecu-

ción de estas modalidades delictivas y que esa actualización se produzca en unos plazos temporales razonables. No obstante, hemos de convenir en que la reforma de la LECRIM del año 2015 cristalizó una serie de criterios jurisprudenciales y dotó a los investigadores de una serie de potentes medidas de lucha contra los ciberdelitos, incardinadas en los arts. 588 bis y ss. LECRIM. Dichas medidas posibilitan notables mejoras en la investigación de los delitos, si bien, y dado su elevado nivel de injerencia en los derechos fundamentales, han de ser solicitadas y adoptadas con mesura, prudencia y cautela y, en todo caso, respetando los principios de especialidad, necesidad, idoneidad, excepcionalidad y proporcionalidad. Por ello, debemos subrayar que, en la actualidad, la normativa procesal penal española permite realizar investigaciones judiciales rigurosas, completas, profundas y con salvaguarda de los derechos fundamentales, aunque, inevitablemente, los medios con los que contamos hoy puede que sean insuficientes para las necesidades del mañana, por lo que es necesario que el legislador adopte una postura proactiva, sensible a las necesidades prácticas, de carácter técnico y en cuya elaboración participen equipos multidisciplinares, que aborden la problemática de la ciberdelincuencia desde una perspectiva integral.

Referencias bibliográficas

Abadías Selma, A. (2023). La nueva regulación del delito de uso fraudulento de medios de pago distintos del efectivo al albur de la reforma de 22 de diciembre de 2022: Un análisis del art. 249.1 b) y 249.2 b) del CP. *Estudios de Deusto: Revista de Derecho Público*, *71*(1), 15-82.

Agustina Sanllehí, J. R. (2014). Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización. *Cuadernos de Política Criminal*, *114*, 143-178.

Alonso Cebrián, J. M. y Velasco Núñez, E. (2024). Delitos por/con inteligencia artificial: presente y futuro. *Ciberderecho*, *84*.

Bustos Rubio, M. (2023). La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal. *IDP: Revista de Internet, Derecho y Política*, *38*.

Casals Fernández, A. (2022). Las criptomonedas frente al delito de blanqueo de capitales y la complejidad de la prueba pericial en el ámbito ciberdelincuente. *Anuario de Derecho Penal y Ciencias Penales*, *75(1)*, 421-446.

Cohen, L. y Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44(4)*, 588-608.

González Uriel, D. (2021). *Aspectos básicos del delito de blanqueo de dinero*. Comares.

González Uriel, D. (2022). Delito de daños (arts. 263-267 CP). En A. Abadías Selma y M. Bustos Rubio (coords.), *Temas prácticos para el estudio del derecho penal económico*. Colex.

González Uriel, D. (2023). Cibermulas y criptomulas: a medio camino entre la estafa y el blanqueo. *Revista Aranzadi Doctrinal*, *6*.

INCIBE (5 de septiembre de 2019). Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

INTERPOL (2024). *Piratería digital*. https://www.interpol.int/es/Delitos/Productos-ilegales/Compre-de-forma-segura/Pirateria-digital.

Jiménez, I. (12 de febrero de 2024). La era de las estafas inteligentes: Cómo la IA está cambiando el juego del engaño. *Blog de Innovación Legal y Nuevas Tecnologías*. https://www.abogacia.es/publicaciones/blogs/blog-de-innovacion-legal/la-era-de-las-estafas-inteligentes-como-la-ia-esta-cambiando-el-juego-del-engano/

Kemp, S. (2021). *Cibercriminalidad y ciberfraude durante una pandemia: cifra negra y tendencias para el futuro*. *Minipapers PostC*. https://postc.umh.es/minipapers/cibercriminalidad-y-

ciberfraude-durante-una-pandemia-cifra-negra-y-tendencias-para-el-futuro/

López Gorostidi, J. (2021). Los valores tradicionales como bienes jurídicos protegidos también en el ciberespacio: a propósito del confinamiento provocado por la crisis sanitaria del COVID-19. *Revista Penal*, *47*, 126-152.

Ministerio del Interior. Gobierno de España. (2023). *Informe sobre la cibercriminalidad en España 2023*. https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf.

Miró Llinares, F. (2012). *El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.

Montiel Juan, I. (2016). Cibercriminalidad social juvenil: la cifra negra. *IDP: Revista de Internet, Derecho y Política*, *22*.

Morillas Fernández, D. L. (2023). Implicaciones de la inteligencia artificial en el ámbito del Derecho Penal. En J. Miguel Peris Riera y A. Massaro (coords.), *Derecho Penal, Inteligencia Artificial y Neurociencias*. Roma: Tre-Press.

UNODC (2019). *Causas, razones, y justificaciones percibidas para los delitos de derecho de autor y de marca propiciados por medios cibernéticos*. https://www.unodc.org/e4j/es/cybercrime/module-11/key-issues/causes-for-cyber-enabled-copyright-and-trademark-offences.html