Oñati Socio-Legal Series (ISSN: 2079-5971)
Oñati International Institute for the Sociology of Law
Avenida Universidad, 8 Apdo. 28
20560 Oñati, Gipuzkoa, Spain
Tel. (+34) 943 783064 / opo@iisj.net / https://opo.iisj.net
(cc) BY-NC-ND

Ciberdelincuencia y crisis de la regulación sociojurídica en el Marruecos digital: desincronización normativa y producción de incertidumbre jurídica

(Cybercrime and the crisis of socio-legal regulation in digital Morocco: Normative asynchrony and the production of legal uncertainty)

OÑATI SOCIO-LEGAL SERIES FORTHCOMING
DOI LINK: HTTPS://DOI.ORG/10.35295/OSLS.IISL.2817
RECEIVED 26 JUNE 2026, ACCEPTED 13 OCTOBER 2026, FIRST-ONLINE PUBLISHED 16 NOVEMBER 2026

ISMAIL RAZZOUK[1]

Resumen

Este estudio analiza la ciberdelincuencia en Marruecos desde una perspectiva sociojurídica, como un terreno en el que se hace visible la capacidad del derecho y de las instituciones para adaptarse al cambio digital. Sostiene que la respuesta jurídico-institucional a la ciberdelincuencia refleja una desincronización normativa entre el ritmo de la transformación digital y el de la adaptación jurídica e institucional, que se expresa en formas concretas de incertidumbre jurídica. El diseño es cualitativo e interpretativo: combina el análisis de textos normativos y estadísticas oficiales (2020-2025) con treinta entrevistas semiestructuradas con profesionales de la justicia y la regulación digital. Las dificultades más señaladas se concentran en la prueba digital, el acceso a datos en poder de plataformas extranjeras y la calificación jurídica de nuevas conductas, y se corresponden con desfases observables en la cronología normativa y en la cooperación con las plataformas. El artículo propone un indicador analítico de desincronización en cuatro dimensiones —temporal, normativa, institucional y plataformal— aplicable a otros contextos.

Palabras clave

Ciberdelincuencia, desincronización normativa, incertidumbre jurídica, prueba digital, plataformas digitales, Marruecos.

El autor agradece a los dos evaluadores anónimos sus valiosos comentarios y sugerencias, que contribuyeron a mejorar la versión final de este artículo, así como al equipo editorial de *Oñati Socio-Legal Series* por su acompañamiento durante el proceso de publicación.

[1] Ismail Razzouk, Doctor en Ciencias Jurídicas y Políticas por la Universidad Mohamed V de Rabat. Facultad de Ciencias Jurídicas, Económicas y Sociales –Souissi, Rabat(Marruecos). Correo electrónico: razzoukismail600@gmail.com ORCID: https://orcid.org/0009-0007-3830-3751

This is an open access work licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International license. (c) The Author(s)

Abstract

This study examines cybercrime in Morocco from a socio-legal perspective, as a field in which the capacity of law and institutions to adapt to digital change becomes visible. It argues that the legal and institutional response to cybercrime reflects a normative asynchrony between the pace of digital transformation and the pace of legal and institutional adaptation, which takes the form of concrete legal uncertainty. The design is qualitative and interpretive: it combines the analysis of legal texts and official statistics (2020–2025) with thirty semi-structured interviews with judges, prosecutors, judicial police officers, lawyers and digital evidence specialists. The difficulties most often reported concern digital evidence, access to data held by foreign platforms and the legal qualification of new conduct; they are consistent with observable time lags in the legislative chronology and in cooperation with platforms. The article proposes a four-dimensional analytical indicator of asynchrony (temporal, normative, institutional and platform-related) applicable to other contexts.

Key words

Cybercrime, normative asynchrony, legal uncertainty, digital evidence, digital platforms, Morocco.

Table of contents

1. Introducción 4
2. Revisión de la literatura y laguna de investigación 5
3. La desincronización normativa como marco sociojurídico 7
    3.1. Transformación digital, plataformas y tecnonormatividad 8
    3.2. Desincronización normativa, técnica legislativa e incertidumbre jurídica 9
    3.3. Marco interpretativo del estudio 10
4. Metodología 11
5. Resultados 13
    5.1. Contexto: expansión del espacio digital y evolución de los asuntos registrados 14
    5.2. Dimensión temporal: cronología normativa y percepción profesional del desfase 17
    5.3. Dimensiones normativa e institucional: incertidumbre jurídica y capacidad de respuesta 19
    5.4. Dimensión plataformal y transnacional: la cooperación con las plataformas 21
    5.5. Síntesis de los resultados 22
6. Discusión de los resultados 22
    6.1. Dónde se localiza la desincronización 22
    6.2. Del retraso legislativo a la incertidumbre interpretativa 22
    6.3. Implicaciones para el estudio sociojurídico de la regulación 23
7. Conclusión 23
Referencias 24
    Fuentes de datos e informes oficiales 27
    Fuentes normativas 28

1. Introducción

Durante las últimas décadas, el mundo ha experimentado una transformación digital acelerada que ha reconfigurado las distintas dimensiones de la vida social, económica, política y jurídica. La amplia difusión de Internet, los teléfonos inteligentes, las plataformas digitales, la inteligencia artificial y los macrodatos ha dado lugar a nuevos espacios de interacción social, producción económica y circulación de información, convirtiendo la digitalización en uno de los principales motores estructurales de las transformaciones contemporáneas (Castells 2010, van Dijck *et al.* 2018).

Paralelamente a estas transformaciones han surgido nuevas formas de riesgo y de conductas desviadas vinculadas al espacio digital. Entre ellas destaca la ciberdelincuencia, que se ha convertido en uno de los principales desafíos para los sistemas jurídicos e institucionales en todo el mundo (Yar 2013, Wall 2024).

Marruecos no es ajeno a esta tendencia global. En los últimos años ha conocido una dinámica digital acelerada, reflejada en el aumento constante de los indicadores de acceso a Internet y en la expansión del uso de plataformas digitales y servicios electrónicos. En 2025, el número de suscripciones a Internet superó los 41 millones; los usuarios de Internet alcanzaron aproximadamente los 35,3 millones y los usuarios de redes sociales se situaron en torno a los 21,3 millones (Agencia Nacional de Reglamentación de las Telecomunicaciones 2025, DataReportal 2025).

Al mismo tiempo, los datos oficiales revelan un aumento notable de los asuntos relacionados con la ciberdelincuencia, tanto por el número de casos registrados como por la diversidad de las conductas delictivas cometidas mediante medios digitales. Los informes nacionales indican igualmente que los atentados contra la vida privada y los datos personales, el fraude electrónico y la extorsión digital ocupan un lugar cada vez más relevante en el mapa de la criminalidad digital en Marruecos (Observatorio Nacional de la Criminalidad 2025, Dirección General de la Seguridad Nacional 2025).

A pesar del creciente interés académico y profesional por la ciberdelincuencia, la mayoría de los estudios se ha centrado bien en las dimensiones técnicas del fenómeno, bien en sus aspectos penales y jurídicos. La relación entre transformación digital y ciberdelincuencia desde una perspectiva sociojurídica sigue estando relativamente poco explorada, especialmente en el contexto marroquí. Asimismo, la literatura disponible rara vez aborda la ciberdelincuencia como un indicador de la capacidad del sistema jurídico para regular un entorno en rápida transformación.

A partir de esta laguna, el presente artículo propone una aproximación sociojurídica que adopta **la desincronización normativa** como clave interpretativa para comprender la relación entre transformación digital y ciberdelincuencia. Por desincronización normativa se entiende la brecha que aparece cuando la velocidad de las transformaciones tecnológicas supera la capacidad del derecho y de las instituciones reguladoras para adaptarse y responder, produciendo incertidumbre jurídica y dificultades de regulación en el entorno digital (Ost 1999, Rosa 2013), en diálogo con la literatura sobre el llamado *pacing problem* (Bennett Moses 2007, Marchant *et al.* 2011). En este marco, la ciberdelincuencia no se concibe como una consecuencia directa de la tecnología en sí misma, sino como un terreno en el que se hace visible el desequilibrio entre el tiempo de la tecnología y el tiempo del derecho.

La problemática central del estudio se formula en los siguientes términos: ¿en qué medida la respuesta jurídico-institucional a la ciberdelincuencia en Marruecos revela una desincronización normativa entre la rapidez de la transformación digital y la lentitud de la adaptación jurídica e institucional, y cómo se traduce esa desincronización en incertidumbre jurídica en la práctica profesional?

El estudio parte de la hipótesis de que la evolución de la ciberdelincuencia en Marruecos, y sobre todo la respuesta jurídico-institucional que suscita, refleja una brecha entre el ritmo acelerado de la transformación digital y el ritmo más lento de la adaptación jurídica e institucional; esa brecha se expresa en formas concretas de incertidumbre jurídica en la práctica profesional. La hipótesis no afirma una relación causal entre desincronización y volumen de delitos: se refiere a la capacidad del sistema jurídico para calificar, probar y perseguir las conductas digitales.

La contribución del artículo es doble. En el plano teórico, propone un marco interpretativo que articula transformación digital, desincronización normativa e incertidumbre jurídica para analizar la respuesta a la ciberdelincuencia. En el plano metodológico, operacionaliza la desincronización mediante un indicador analítico de cuatro dimensiones —temporal, normativa, institucional y plataformal— que combina fuentes normativas, estadísticas y testimonios profesionales, y que puede aplicarse a otros sistemas jurídicos.

2. Revisión de la literatura y laguna de investigación

La ciberdelincuencia ha recibido una atención creciente en la literatura jurídica y sociológica durante las últimas décadas, especialmente a medida que se ha expandido el uso de Internet y de las plataformas digitales y que una parte cada vez mayor de las relaciones sociales y económicas se ha trasladado al espacio digital. Los primeros trabajos se centraron principalmente en las dimensiones técnicas y penales del fenómeno, analizando las modalidades de los delitos informáticos, los medios empleados para cometerlos, los mecanismos de lucha, las dificultades de la prueba digital y la cooperación judicial transfronteriza (Barrio Andrés 2011, Yar 2013, Cabezudo Rodríguez 2016, Martínez Galindo 2022, Wall 2024).

Estas aproximaciones rara vez tratan la ciberdelincuencia como indicador de las transformaciones de la regulación. En este artículo se la considera tal en un sentido preciso: no por su volumen, que depende también de las prácticas de denuncia y registro (Kitsuse y Cicourel 1963, Brenner 2004), sino por los puntos de fricción que su tratamiento produce en el sistema jurídico. Son tres: la calificación (si las categorías existentes captan las nuevas conductas), la prueba (si los hechos pueden acreditarse con evidencia electrónica válida) y la cooperación (si las autoridades pueden acceder a datos en poder de actores transnacionales). Es, así, un indicador de la capacidad reguladora del sistema de justicia, no de las transformaciones sociales en su conjunto.

Paralelamente, la literatura sobre transformación digital y sociedad digital ha mostrado que la digitalización no consiste únicamente en introducir tecnología en la vida social, sino que constituye una transformación estructural que reconfigura las relaciones sociales y los modos de organización. La sociedad contemporánea depende cada vez más de las redes digitales y de los flujos de información, mientras que las plataformas se han convertido en espacios centrales para la interacción social, económica y política

(Castells 2010, van Dijck *et al.* 2018, Cohen 2019). Sin embargo, estos trabajos rara vez han situado la ciberdelincuencia en el centro del análisis y suelen abordarla de manera implícita como uno de los efectos o riesgos de la transformación digital.

También se ha desarrollado una literatura sobre gobernanza y regulación digital que subraya la dificultad de regular tecnologías, plataformas e inteligencia artificial en entornos caracterizados por la rapidez de la innovación y la multiplicidad de actores. En este marco, el principal desafío no reside en la tecnología misma, sino en la capacidad de los sistemas jurídicos y reguladores para acompañar la innovación sin menoscabar derechos y libertades (Taeihagh 2021). A su vez, los estudios sobre corregulación muestran que la regulación del espacio digital ya no puede descansar únicamente en la intervención estatal, sino que requiere cooperación entre instituciones públicas, plataformas, sector privado y sociedad civil (Di Porto y Zuppetta 2021). En el ámbito hispanohablante, la reflexión sobre los derechos fundamentales ante la era digital ha subrayado igualmente que la transformación tecnológica afecta a categorías jurídicas tradicionales y exige revisar los instrumentos de protección y regulación (Benlloch Domènech y Sarrión Esteve 2022).

Esta problemática se ha profundizado con la literatura sobre plataformas y algoritmos. Las plataformas ya no son consideradas simples intermediarios técnicos neutrales, sino actores que desempeñan funciones reguladoras mediante condiciones de uso, mecanismos de moderación de contenidos y algoritmos que controlan la visibilidad, el acceso y la interacción (van Dijck *et al.* 2018). Estudios recientes sostienen que los artefactos digitales ejercen funciones normativas dentro y fuera del derecho, lo que obliga a repensar la relación entre tecnología y regulación (Judge *et al.* 2025, Loddo 2025).

Vincular ambas literaturas es una exigencia del objeto. Las plataformas son, a la vez, el entorno en que se cometen muchas de las conductas registradas, custodios de los datos necesarios para identificar a los autores y probar los hechos, y reguladores privados que deciden la entrega de esos datos según sus políticas y el derecho extranjero aplicable. Esta dependencia explica los instrumentos de cooperación directa con los proveedores de servicios, como el Segundo Protocolo Adicional al Convenio de Budapest (2022) o el Reglamento (UE) 2023/1543, que confían a actores privados funciones cuasijudiciales (Rojszczak 2022, Sachoulidou 2024). Estudiar la ciberdelincuencia sin las plataformas ignora dónde surge la fricción probatoria; estudiar las plataformas sin la justicia penal ignora uno de sus efectos más relevantes.

En el contexto marroquí, la ciberdelincuencia se ha abordado sobre todo desde el derecho penal y la ciberseguridad: desde la primera aproximación de conjunto de El Azzouzi (2010) y el análisis de sus retos por Missaoui (2016) hasta trabajos recientes sobre la Ley n.º 07-03, que completa el Código Penal en lo relativo a las infracciones relativas a los sistemas de tratamiento automatizado de datos (Marddi 2024), la prueba digital (Abou El Jaouad 2023), la protección penal de las víctimas (Hamouti y Elbouzidi 2025), la ciberseguridad (Maleh y Maleh 2022) o los comportamientos de los jóvenes frente al delito digital (El Hamzaoui y Bensalah 2019). Estos estudios aportan un conocimiento jurídico y técnico valioso, pero no examinan la relación temporal entre el cambio tecnológico y la adaptación del derecho ni emplean categorías sociojurídicas de la regulación.

La revisión permite identificar tres lagunas. Primera: los estudios sobre ciberdelincuencia han analizado tipos penales, técnicas de investigación y prueba, pero no la redistribución de la capacidad reguladora hacia plataformas y expertos técnicos ni el tiempo que necesita el sistema de justicia para adaptar sus categorías y procedimientos. Segunda: la literatura sobre gobernanza de plataformas ha estudiado la moderación de contenidos y las reglas privadas, pero rara vez sus efectos sobre la investigación y la prueba de los delitos. Tercera: la literatura sobre el *pacing problem* (Bennett Moses 2007, Marchant *et al.* 2011) y sobre la desincronización entre derecho y tecnología (Rosa 2013, Ortega Esquembre 2023) se ha centrado en sistemas europeos y norteamericanos y en tecnologías emergentes; no hemos identificado estudios que la apliquen a la respuesta penal a la ciberdelincuencia en sistemas jurídicos magrebíes, marcados por la dependencia de plataformas extranjeras y por una tradición penal de legalidad estricta.

En la propia literatura sociojurídica publicada en *Oñati Socio-Legal Series*, varios trabajos recientes han mostrado la pertinencia de analizar las transformaciones digitales como problemas de regulación y de adaptación institucional. Algunos estudios analizan la desinformación digital como fenómeno asociado a la transformación estructural de los medios de comunicación y a las estrategias de aprendizaje regulador del sistema jurídico (Loschiavo Leme de Barros y Fucci Amato 2024); otros subrayan la ampliación de la brecha entre derecho y tecnología en el metaverso (Bengoetxea y Cruz Balbuena 2024); también se analiza la normalización de la prueba electrónica en los procedimientos judiciales (Ontanu 2022); y otros trabajos muestran cómo nuevas formas de ciberdelincuencia generadas por inteligencia artificial producen vacíos legales y exigencias de responsabilidad (Jamaludin *et al.* 2026).

A partir de estas lagunas, el artículo propone una lectura sociojurídica de la respuesta a la ciberdelincuencia en Marruecos en la que la desincronización normativa funciona como clave interpretativa central.

3. La desincronización normativa como marco sociojurídico

El marco combina tres conceptos de contexto y una categoría analítica central, la desincronización normativa, en línea con los trabajos que han abordado el desajuste entre innovación tecnológica y regulación jurídica (Ortega Esquembre 2023). La Tabla 1 indica qué aporta cada concepto al análisis de la ciberdelincuencia, con qué dimensión del indicador de desincronización (apartado 4) se relaciona y dónde se observa en los resultados.

TABLA 1

Concepto	**Qué aporta al análisis de la ciberdelincuencia**	**Dimensión del indicador**	**Dónde se observa (apartado 5)**
Sociedad red (Castells 2010)	Desterritorialización de las conductas y carácter transnacional de autores, víctimas y datos.	Plataformal o transnacional.	Carácter transfronterizo (Tabla 11); problemas de competencia (Tabla 10).
Sociedad de plataformas (van Dijck *et al.* 2018)	Custodia privada de la prueba y producción privada de reglas.	Plataformal o transnacional.	Cooperación con las plataformas (Tabla 12); datos de Meta.
Tecnonormatividad (Lessig 2006, Lehaire 2022, Loddo 2025)	Parte de la regulación de la conducta opera mediante el diseño técnico, fuera de la norma jurídica.	Normativa e institucional.	Pluralidad de fuentes reguladoras (Tabla 10); acceso a datos (Tabla 11).
Desincronización normativa (Ost 1999, Bennett Moses 2007, Rosa 2013)	Desajuste entre el ritmo del cambio técnico y el de la adaptación jurídico-institucional.	Las cuatro.	Cronología normativa (Tabla 8); Tablas 9 a 12.

Tabla 1. Conceptos del marco y su función en el análisis.
(Fuente: elaboración propia.)

3.1. Transformación digital, plataformas y tecnonormatividad

La literatura sobre la sociedad red sostiene que las transformaciones tecnológicas de finales del siglo XX dieron lugar a una nueva forma de organización social basada en redes y flujos de información, más que en instituciones y fronteras tradicionales. En esta sociedad red, las relaciones sociales ya no dependen únicamente de la proximidad geográfica o de las pertenencias tradicionales, sino que se forman mediante espacios digitales interconectados que permiten una circulación de información e interacciones a una escala inédita (Castells 2010).

Para el análisis de la ciberdelincuencia, lo relevante de esta perspectiva es la desterritorialización de las conductas: autores, víctimas y datos pueden situarse en jurisdicciones distintas, lo que genera fricciones de competencia y de cooperación.

Si la sociedad red explica el cambio general de la estructura de las relaciones sociales, el concepto de sociedad de plataformas permite comprender cómo las plataformas

digitales se han convertido en actores centrales de la organización de la vida social. No se limitan a ofrecer espacios de interacción, sino que determinan las condiciones de acceso, participación, visibilidad y comunicación mediante algoritmos y reglas técnicas propias (van Dijck *et al.* 2018).

En este sentido, las plataformas desempeñan funciones reguladoras tradicionalmente asociadas a las instituciones estatales o a las normas jurídicas: controlan los flujos de información, gestionan contenidos, establecen estándares de conducta aceptable e imponen sanciones a los usuarios. Una parte creciente de la regulación del espacio digital se ejerce así mediante mecanismos técnicos y organizativos diseñados por las propias plataformas, redistribuyendo el poder regulador entre el Estado y los actores digitales. Para la ciberdelincuencia, ello significa que una parte decisiva de la prueba queda bajo custodia privada.

Estas transformaciones se profundizan con el concepto de tecnonormatividad. La teoría del código mostró que la conducta en el ciberespacio no está regulada únicamente por normas jurídicas, sino también por la propia arquitectura técnica, es decir, por el «código». El diseño técnico puede permitir, impedir u orientar una conducta del mismo modo que lo hace el derecho (Lessig 1999).

Por «tecnonormatividad» se entiende la normatividad producida por artefactos técnicos que orientan la conducta sin pasar por la norma jurídica (Lehaire 2022, Loddo 2025), distinta de la normatividad propiamente jurídica (Hildebrandt 2015). La regulación de la conducta digital no es un proceso exclusivamente jurídico —nunca lo fue: el derecho siempre ha coexistido con las normas sociales, el mercado y la arquitectura (Lessig 2006)—, pero en el entorno digital aumenta el peso relativo de la regulación mediante el diseño, que ejercen a gran escala actores privados transnacionales y que opera *ex ante* y de forma automatizada (Yeung 2017, Brownsword 2019). Para la ciberdelincuencia, ello significa que la prevención, la detección y la conservación de la prueba dependen en parte de decisiones de diseño y de políticas privadas ajenas al legislador.

3.2. Desincronización normativa, técnica legislativa e incertidumbre jurídica

En el análisis de la aceleración social, se muestra que las sociedades contemporáneas experimentan un aumento continuo del ritmo del cambio tecnológico y social, mientras que las instituciones se adaptan más lentamente (Rosa 2013). Por su parte, la teoría del tiempo jurídico sostiene que el derecho posee una temporalidad propia, distinta de la temporalidad técnica, pues necesita etapas de legislación, interpretación, aplicación y construcción jurisprudencial (Ost 1999). Esta lectura ha sido retomada en la literatura reciente sobre inteligencia artificial para mostrar que los procesos jurídicos tienden a llegar tarde frente a innovaciones tecnológicas de rápida evolución (Ortega Esquembre 2023). Es el fenómeno que la literatura anglosajona denomina *pacing problem* (Bennett Moses 2007, Marchant *et al.* 2011).

Esta diferencia de ritmos se refuerza en la literatura sociojurídica reciente sobre tecnología y derecho. Algunos trabajos señalan, a propósito del metaverso, la ampliación de la brecha entre los sistemas jurídicos y los avances tecnológicos, así como la necesidad de adaptar normas e instituciones a entornos digitales emergentes (Bengoetxea y Cruz Balbuena 2024). Otros estudios muestran que la incorporación de la prueba electrónica exige transformar objetos técnicos en categorías procesales jurídicamente operativas

(Ontanu 2022). Desde esta perspectiva, la desincronización normativa no expresa solo un retraso legislativo, sino una tensión estructural entre normatividad jurídica, normatividad técnica y capacidad institucional de traducción.

La desincronización normativa aparece cuando las transformaciones tecnológicas avanzan más rápidamente que la capacidad del derecho y de las instituciones para acompañarlas. Se amplía entonces la distancia entre los nuevos hechos digitales y los marcos jurídicos disponibles, generando incertidumbre jurídica, dificultades de calificación, ambigüedad de responsabilidades, pluralidad de fuentes normativas y mayor complejidad de los mecanismos de regulación.

Cabe objetar que la desincronización es, en el fondo, un problema de técnica legislativa. La objeción es en parte correcta: la principal estrategia para que las normas resistan el cambio tecnológico es la redacción tecnológicamente neutra y abierta (Koops 2006, Bennett Moses 2007). En derecho penal, sin embargo, esa estrategia choca con el mandato de determinación o taxatividad (Ossandón Widow 2009, Navarro Frías 2010), que el derecho marroquí recoge en el principio de legalidad (art. 3 del Código Penal; art. 23 de la Constitución de 2011). El legislador penal se enfrenta así a un equilibrio difícil: la precisión garantiza la certeza, pero expone la norma a la obsolescencia técnica; la amplitud le da adaptabilidad, pero traslada la incertidumbre a la fase de interpretación judicial.

El derecho marroquí ilustra ambos lados del equilibrio. La Ley 07-03 (2003) empleó una fórmula relativamente neutra, la de los «sistemas de tratamiento automatizado de datos», que ha envejecido bien. En cambio, la difusión de imágenes privadas y el «montaje» de palabras o imágenes requirieron una intervención específica quince años después (Ley n.º 103-13, relativa a la lucha contra la violencia contra las mujeres, de 2018, arts. 447-1 a 447-3), y la aplicación de la noción de «montaje» a contenidos sintéticos generados por inteligencia artificial plantea dudas de calificación que una fórmula más amplia solo resolvería a costa de la determinación (sobre esta tensión en un delito propio de la era digital, véase Ossandón Widow 2014). Otras fuentes de desincronización quedan fuera del alcance de la técnica legislativa, como el acceso a datos en poder de plataformas extranjeras o la construcción de capacidades institucionales. La técnica legislativa puede, por tanto, mitigar la desincronización, pero no eliminarla: la desplaza del legislador al intérprete o la hace depender de factores ajenos al legislador nacional.

Los términos del artículo designan niveles distintos de análisis. La «brecha entre tecnología y derecho» es la categoría con la que los profesionales describen su experiencia y solo se usa para referir sus percepciones. La «desincronización normativa» es la categoría analítica, observable en cuatro dimensiones. La «incertidumbre jurídica» es su expresión en la práctica: dificultades para calificar, probar, atribuir responsabilidades y determinar la competencia. La «crisis de la regulación sociojurídica» designa un diagnóstico de conjunto —la reducción persistente de la capacidad del sistema para producir certeza práctica y eficacia— y se reserva para la discusión y las conclusiones.

3.3. Marco interpretativo del estudio

A partir de los conceptos anteriores, el artículo propone el siguiente marco interpretativo:

FIGURA 1

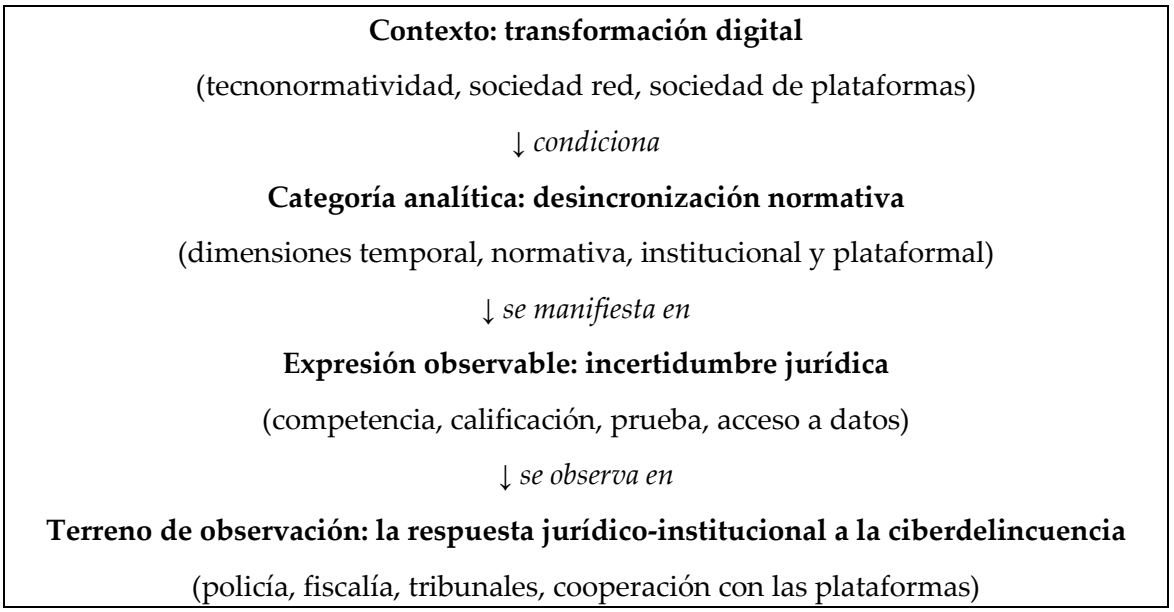


Figura 1. Marco interpretativo del estudio.
(Nota: la figura no representa una secuencia causal; indica el nivel de análisis de cada concepto. Fuente: elaboración propia.)

La ciberdelincuencia no aparece en la figura como efecto final de una cadena: su tratamiento jurídico-institucional es el terreno en el que se observan la desincronización y la incertidumbre. La «crisis de la regulación sociojurídica» no forma parte del marco; es el diagnóstico que se discute, con las debidas cautelas, en los apartados 6 y 7.

El marco propuesto no pretende explicar causalmente el aumento de la ciberdelincuencia. Su función es más limitada: ofrecer categorías para observar dónde y cómo la respuesta jurídico-institucional a la ciberdelincuencia pierde sincronía con el cambio tecnológico, y ordenar la lectura de los datos del apartado 5.

4. Metodología

El estudio adopta un enfoque sociojurídico cualitativo de carácter interpretativo. Busca comprender la relación entre transformación digital y ciberdelincuencia en Marruecos mediante el concepto de desincronización normativa. No pretende medir una relación causal cuantitativa entre digitalización y criminalidad, sino interpretar cómo la transformación digital reconfigura las condiciones de la regulación jurídica e institucional en la sociedad digital.

El análisis distingue tres niveles de inferencia: la asociación empírica (la evolución paralela de los indicadores digitales y de los asuntos registrados entre 2021 y 2025, descrita sin inferir causalidad); la interpretación sociojurídica (cómo viven y explican los profesionales las dificultades de la respuesta reguladora y qué muestran los documentos normativos e institucionales); y la causalidad, que no se afirma porque el diseño no permite establecerla. Las conclusiones del artículo se sitúan en el segundo nivel.

La investigación se basó en un diseño de fuentes múltiples que combina, por un lado, el análisis documental y estadístico y, por otro, entrevistas semiestructuradas. Los documentos examinados incluyen informes e indicadores oficiales de instituciones

nacionales e internacionales, entre ellas la Agencia Nacional de Reglamentación de las Telecomunicaciones (Agence Nationale de Réglementation des Télécommunications, ANRT), la Dirección General de la Seguridad Nacional (Direction Générale de la Sûreté Nationale, DGSN), la Presidencia del Ministerio Público (Présidence du Ministère Public) y el Observatorio Nacional de la Criminalidad (Observatoire National de la Criminalité), así como informes sobre el uso de Internet y de plataformas digitales. Estos datos se utilizaron como indicadores contextuales para comprender la expansión del espacio digital y la evolución de la ciberdelincuencia, no como base para contrastar hipótesis cuantitativas. Se analizaron además los textos normativos pertinentes (leyes, convenios y anteproyectos), para reconstruir la cronología de la respuesta normativa (Tabla 8), y los informes de transparencia de Meta sobre las solicitudes gubernamentales de datos.

Además, se realizaron treinta entrevistas semiestructuradas con profesionales implicados en la gestión de delitos cibernéticos o de sus efectos jurídicos e institucionales. Su selección fue intencional, atendiendo a la relación directa de los participantes con el objeto de estudio y a su experiencia práctica en ciberdelincuencia, prueba digital y cooperación con plataformas. Las entrevistas se realizaron entre el 10 de enero y el 6 de marzo de 2026, tuvieron una duración media de 50 minutos y se desarrollaron en árabe.

Las entrevistas se organizaron en torno a varios ejes: representaciones de la transformación digital, evolución de la ciberdelincuencia, dificultades de calificación jurídica, desafíos de la prueba digital, cooperación con plataformas y percepción de la brecha entre la velocidad de la tecnología y la capacidad del derecho y de las instituciones para acompañarla. Este material permitió comprender cualitativamente cómo los profesionales perciben la desincronización normativa y la incertidumbre jurídica en su práctica cotidiana.

El guion incluía una pregunta directa sobre la percepción de la brecha entre tecnología y derecho. Como esta formulación puede inducir la respuesta, sus resultados, así como las manifestaciones de la desincronización recogidas en la Tabla 9, se presentan solo como percepciones de los participantes y no se utilizan como apoyo de la hipótesis. Las dificultades concretas de calificación, prueba y cooperación con plataformas se recogieron en ejes distintos del guion, referidos a la práctica profesional de los entrevistados.

Los datos se analizaron mediante análisis temático. Se leyeron las entrevistas y los documentos, se identificaron los temas recurrentes y se organizaron en torno a la transformación digital, la desincronización normativa, la incertidumbre jurídica y la crisis de la regulación sociojurídica. El estudio aplicó además triangulación metodológica, combinando datos documentales, estadísticos y testimonios profesionales para reforzar la fiabilidad de los resultados y vincular los indicadores cuantitativos con los contextos profesionales e institucionales que permiten interpretarlos.

Para ordenar la lectura empírica de los resultados, el estudio utiliza un indicador analítico de desincronización normativa, concebido como una herramienta interpretativa y no como un índice estadístico cerrado. Este indicador permite observar la distancia entre la velocidad de transformación del espacio digital y la capacidad del derecho y de las instituciones para responder a los nuevos riesgos de la

ciberdelincuencia. Se articula en cuatro dimensiones: temporal, referida al desfase entre la aparición de nuevas prácticas delictivas digitales y los tiempos de producción normativa o respuesta judicial; normativa, relativa al grado de claridad, suficiencia y adaptabilidad de las reglas jurídicas; institucional, vinculada a la capacidad técnica y organizativa de los actores judiciales y policiales; y plataformal o transnacional, relacionada con la cooperación de las plataformas digitales y la dependencia de datos conservados por actores privados extranjeros.

La Tabla 2 indica qué fuentes sustentan cada dimensión del indicador.

TABLA 2

Dimensión	**Qué se observa**	**Fuentes documentales y estadísticas**	**Entrevistas**
Temporal	Desfase entre la aparición de prácticas delictivas digitales y la respuesta normativa.	Cronología normativa 2003-2025 (Tabla 8); informes de la Presidencia del Ministerio Público.	Tabla 9.
Normativa	Claridad, suficiencia y adaptabilidad de las reglas jurídicas.	Leyes 07-03, 103-13 y 03-23.	Tabla 10.
Institucional	Capacidad técnica y organizativa de los actores policiales y judiciales.	Balances de la DGSN; Ley 03-23.	Tabla 11.
Plataformal o transnacional	Cooperación de las plataformas y dependencia de datos conservados en el extranjero.	Informes de transparencia de Meta; Ecofin Agency (2025); estado del Segundo Protocolo Adicional al Convenio de Budapest.	Tablas 11 y 12.

Tabla 2. Fuentes que sustentan cada dimensión del indicador de desincronización. (Fuente: elaboración propia.)

La investigación respetó los principios éticos aplicables a los estudios sociales y jurídicos: confidencialidad de la identidad de los participantes, exclusión de datos personales que pudieran permitir su identificación y uso exclusivo de la información con fines científicos. Los resultados están condicionados por el carácter intencional de la muestra y por el periodo temporal analizado. Por tanto, son resultados interpretativos que no pretenden una generalización estadística, pero ofrecen una base sociojurídica para comprender la respuesta jurídico-institucional a la ciberdelincuencia en Marruecos.

5. Resultados

Los resultados se presentan en cinco pasos: el contexto (expansión del espacio digital y evolución de los asuntos registrados), las dimensiones del indicador de

desincronización, agrupadas en tres apartados —temporal, normativa e institucional, y plataformal— y una síntesis de lo que los datos permiten afirmar y lo que no.

5.1. Contexto: expansión del espacio digital y evolución de los asuntos registrados

Los indicadores del sector de las telecomunicaciones y de las tecnologías de la información muestran que Marruecos experimentó entre 2021 y 2025 una expansión digital significativa que afectó tanto a la infraestructura como a los patrones de uso de Internet y de las plataformas (Tabla 3).

TABLA 3

Indicador	**2021**	**2025**	**Evolución**
Total de suscripciones a Internet	32,846 millones.	41,460 millones.	+8,614 millones.
Crecimiento total de las suscripciones	—	—	+26,2 %.
Internet móvil	30,621 millones.	38,520 millones.	+7,899 millones.
Fibra óptica FTTH	384.000.	Más de 1,4 millones.	Más de +1,016 millones.
Crecimiento total de la fibra óptica	—	—	+264,6 %.
Tasa de penetración de Internet	90,45 %.	112,59 %.	+22,14 puntos.
Suscripciones ADSL	1,598 millones.	1,440 millones.	-158.000.

Tabla 3. Evolución de los indicadores de transformación digital en Marruecos, 2021-2025. (Fuente: elaboración propia a partir de datos de la Agencia Nacional de Reglamentación de las Telecomunicaciones (ANRT 2025).)

La mayoría de los profesionales entrevistados confirmó que la ciberdelincuencia ya no constituye un fenómeno técnico aislado, sino una realidad vinculada a la vida diaria y al uso intensivo del espacio digital.

Paralelamente a la expansión del espacio digital, los balances de la DGSN (Dirección General de la Seguridad Nacional 2021, 2022, 2023, 2024, 2025) registran un aumento claro de los asuntos policiales relacionados con la ciberdelincuencia. El número de casos pasó de 5.275 en 2021 a 13.643 en 2025, con una aceleración especialmente marcada durante 2024 y 2025.

TABLA 4

Año	Número de casos	Diferencia respecto al año anterior	Tasa de crecimiento
2021	5.275	—	—
2022	5.623	+348	+6,60 %
2023	5.969	+346	+6,15 %
2024	8.333	+2.364	+39,60 %
2025	13.643	+5.310	+63,72 %

Tabla 4. Evolución de los asuntos de ciberdelincuencia tratados por los servicios policiales (DGSN), 2021-2025.
(Fuente: elaboración propia a partir de los balances anuales de la DGSN (2021-2025). Unidad: asuntos tratados por los servicios policiales.)

Las cifras de este apartado proceden de dos series distintas que no deben compararse ni sumarse: los balances de la DGSN recogen los asuntos tratados por la policía bajo una rúbrica amplia de criminalidad vinculada a las nuevas tecnologías, mientras que los informes de la Presidencia del Ministerio Público recogen los asuntos registrados y las personas procesadas por la fiscalía, desglosados por calificación jurídica. Ambas son indicadores de actividad institucional, no medidas de la prevalencia (Kitsuse y Cicourel 1963), y reflejan también la capacidad de denuncia y registro. Así, el fuerte aumento de 2024 y 2025 coincide con la puesta en marcha, en junio de 2024, de la plataforma de denuncia en línea E-Blagh de la DGSN, que había recibido 25.876 denuncias en diciembre de 2025 (Dirección General de la Seguridad Nacional 2025).

Los informes de la Presidencia del Ministerio Público ofrecen una serie distinta, referida a la fase de persecución penal (Tabla 5). Los asuntos de delitos informáticos registrados por las fiscalías pasaron de 559 en 2020 a 3.057 en 2022 y a 2.632 en 2023, y 8.658 personas fueron procesadas en el conjunto del periodo (Presidencia del Ministerio Público 2020, 2021, 2022, 2023).

TABLA 5

Año	Asuntos registrados	Personas procesadas
2020	559	772
2021	842	1.110
2022	3.057	3.617
2023	2.632	3.159

Tabla 5. Asuntos de delitos informáticos registrados y personas procesadas por la fiscalía, 2020-2023.
(Fuente: elaboración propia a partir de los informes anuales de la Presidencia del Ministerio Público (2020-2023). Unidad: asuntos registrados y personas procesadas por las fiscalías. Serie no comparable con la Tabla 4.)

Sin ser comparable con la serie policial, esta serie muestra que la ciberdelincuencia se ha incorporado al trabajo ordinario de las fiscalías: la subida de 2022 marca una aceleración

de la respuesta penal, y los niveles de 2023, su estabilización como categoría de la política penal.

Los datos de 2024 se presentan con un desglose distinto y se comentan aparte. El informe anual de la Presidencia del Ministerio Público registra 1.980 asuntos relativos a atentados contra la vida privada por medios electrónicos, con 2.313 personas procesadas, además de 470 asuntos de delitos comunes cometidos mediante medios informáticos, con 556 personas procesadas. Dentro de esta última categoría destacan 250 asuntos de extorsión sexual; el informe también menciona 17 asuntos vinculados al uso de criptomonedas en prácticas de fraude o extorsión (Presidencia del Ministerio Público 2024).

La ciberdelincuencia ya no se limita a ataques contra sistemas informáticos, sino que afecta a la privacidad, la reputación, la confianza digital y las transacciones económicas cotidianas.

Los datos del Boletín Estadístico n.º 03/2025 del Observatorio Nacional de la Criminalidad muestran que, en 2023, los delitos contra la vida privada de las personas representaron la mayor parte de los delitos informáticos.

TABLA 6

Tipo de delito informático	**Porcentaje**
Delitos contra la vida privada de las personas	71,2 %
Delitos comunes cometidos mediante medios electrónicos modernos	19,8 %
Delitos contra sistemas automatizados de tratamiento de datos	7,9 %
Delitos de contenido cometidos mediante medios modernos	1,1 %

Tabla 6. Distribución de los delitos cibernéticos en Marruecos según su naturaleza, 2023. (Fuente: elaboración propia a partir del Boletín Estadístico n.º 03/2025 del Observatorio Nacional de la Criminalidad.)

Estos datos coinciden con las entrevistas, en las que los participantes identificaron como delitos más frecuentes en su práctica profesional el fraude electrónico, la extorsión digital, los atentados contra los datos personales y la suplantación de identidad digital.

TABLA 7

Tipo de delito	Entrevistados que lo mencionan
Fraude electrónico	28
Extorsión digital	25
Atentados contra los datos personales	21
Suplantación de identidad digital	19
Intrusión en sistemas informáticos	14

Tabla 7. Delitos cibernéticos más presentes en la práctica profesional según las entrevistas (n = 30).
(Fuente: elaboración propia a partir de las entrevistas semiestructuradas. Respuesta múltiple; n = 30.)

Estos datos se sitúan en el nivel de la asociación empírica: describen la evolución paralela del espacio digital y de los asuntos registrados, pero no permiten inferir sus causas. Los apartados siguientes examinan cómo responde a ellos el sistema jurídico-institucional.

5.2. Dimensión temporal: cronología normativa y percepción profesional del desfase

La dimensión temporal de la desincronización puede observarse, en primer lugar, en la cronología de la respuesta normativa marroquí a las prácticas digitales (Tabla 8).

TABLA 8

Año	Instrumento	Contenido pertinente
2003	Ley 07-03 (Dahir 1-03-197, de 11-11-2003).	Tipifica los atentados contra los sistemas de tratamiento automatizado de datos (arts. 607-3 a 607-11 del Código Penal).
2007	Ley 53-05 (Dahir 1-07-129, de 30-11-2007).	Intercambio electrónico de datos jurídicos y firma electrónica.
2009	Ley 09-08 (Dahir 1-09-15, de 18-2-2009).	Protección de los datos personales; crea la Comisión Nacional de Control de la Protección de Datos de Carácter Personal (CNDP).
2017	Comunicado de la Oficina de Cambios (Office des Changes) (20-11-2017).	Declara las operaciones con monedas virtuales infracción a la normativa de cambios.
2018	Ley 103-13 (Dahir 1-18-19, de 22-2-2018; en vigor el 12-9-2018).	Introduce los arts. 447-1 a 447-3 del Código Penal: captación y difusión de palabras o imágenes privadas y montajes sin consentimiento.

Año	Instrumento	Contenido pertinente
2018	Adhesión al Convenio de Budapest (depósito el 29-6-2018; en vigor el 1-10-2018).	Marco de cooperación penal internacional.
2020	Ley 05-20 (Dahir 1-20-69, de 25-7-2020).	Ciberseguridad de los organismos del Estado y de las infraestructuras críticas.
2020	Ley 43-20(Dahir 1-20-100, de 31-12-2020).	Servicios de confianza para las transacciones electrónicas.
2022	Firma del Segundo Protocolo Adicional al Convenio de Budapest (12-5-2022).	Cooperación directa con los proveedores de servicios; sin ratificación constatada.
2024	Plataforma E-Blagh de la DGSN (junio).	Denuncia en línea de contenidos ilícitos.
2025	Anteproyecto de ley 42-25 sobre criptoactivos.	Primer marco legal para los criptoactivos.
2025	Ley 03-23 (Dahir 1-25-55, de 13-8-2025; BO n.º 7437, de 8-9-2025; en vigor el 8-12-2025).	Reforma procesal penal: registro y aprehensión de datos digitales, técnicas especiales de investigación.
2025	Firma de la Convención de las Naciones Unidas contra la Ciberdelincuencia (Hanói, 25-10-2025).	Cooperación internacional.

Tabla 8. Hitos normativos y convencionales relativos a la ciberdelincuencia en Marruecos, 2003-2025.
(Fuente: elaboración propia a partir de los textos normativos citados (véase «Fuentes normativas»)).

La cronología muestra que la adaptación normativa existe, pero llega mediante intervenciones sucesivas y específicas, a menudo años después de que las prácticas se extiendan. El caso más claro son los criptoactivos: la primera respuesta (2017) fue una prohibición administrativa y el primer marco legal no llegó a la fase de anteproyecto hasta 2025, cuando la fiscalía ya registraba asuntos de fraude y extorsión con criptomonedas (17 en 2024). La cooperación directa con las plataformas muestra un desfase similar (apartado 5.4).

Esta cronología concuerda con la percepción de los profesionales: 27 de los 30 entrevistados describieron una brecha clara entre la velocidad de las transformaciones digitales y la capacidad del derecho y de las instituciones para acompañarlas, y los 3 restantes una brecha parcial. Como se indicó en el apartado 4, este resultado procede de

una pregunta directa y se presenta solo como percepción. La rapidez con la que surgen nuevos delitos, el retraso legislativo, la lentitud de la adaptación institucional y la dificultad para seguir la evolución de las plataformas fueron los rasgos más citados de esta desincronización (Tabla 9).

TABLA 9

Manifestación	**Entrevistados que la mencionan**
Rapidez de aparición de nuevos delitos.	27
Retraso de la adaptación legislativa.	25
Lentitud de la adaptación institucional.	23
Dificultad para acompañar a las plataformas digitales.	21

Tabla 9. Manifestaciones de la desincronización normativa en la lucha contra la ciberdelincuencia según los entrevistados (n = 30).
(Fuente: elaboración propia a partir de las entrevistas semiestructuradas. Respuesta múltiple.)

La aparición de nuevos delitos es la manifestación más frecuente, seguida de las dificultades de adaptación legislativa e institucional y de la incapacidad de seguir la evolución de las plataformas. Estas categorías expresan cómo viven el desfase los profesionales; su valor como evidencia depende de su concordancia con la cronología normativa de la Tabla 8.

5.3. Dimensiones normativa e institucional: incertidumbre jurídica y capacidad de respuesta

La desincronización normativa se traduce en la práctica profesional en diversas formas de incertidumbre jurídica y en desafíos concretos para la investigación y persecución de la ciberdelincuencia. Las Tablas 10 y 11 sintetizan las principales dificultades señaladas por los profesionales entrevistados.

TABLA 10

Manifestación	**Entrevistados que la mencionan**	**% de n**
Dificultades de calificación jurídica.	18	60 %
Ambigüedad de algunas normas.	14	47 %
Pluralidad de fuentes reguladoras.	12	40 %
Problemas de competencia.	10	33 %

Tabla 10. Manifestaciones de la incertidumbre jurídica señaladas por los entrevistados (n = 30).
(Fuente: elaboración propia a partir de las entrevistas semiestructuradas. Respuesta múltiple; porcentajes sobre n = 30.)

TABLA 11

Desafío	**Entrevistados que lo mencionan**	**% de n**
Dificultades de prueba digital.	26	87 %
Acceso a datos digitales.	22	73 %
Carácter transfronterizo.	19	63 %
Limitación de la experiencia técnica.	17	57 %

Tabla 11. Desafíos profesionales señalados por los entrevistados (n = 30).
(Fuente: elaboración propia a partir de las entrevistas semiestructuradas (n = 30). Respuesta múltiple. El retraso legislativo se trata en la Tabla 9 como manifestación de la dimensión temporal.)

Los datos muestran que los desafíos profesionales van más allá de los problemas puramente técnicos y están estrechamente vinculados con la incertidumbre jurídica del entorno digital. Las dificultades de prueba digital ocupan el primer lugar (26 de 30 entrevistados), seguidas de las dificultades para obtener datos digitales (22). Esto refleja que la investigación y el enjuiciamiento dependen de datos que a menudo están en poder de plataformas o actores técnicos situados fuera del alcance directo de las autoridades. La frecuencia con que se menciona el carácter transfronterizo (19) indica que los desafíos también se relacionan con los límites de los marcos jurídicos e institucionales existentes.

Por otro lado, las manifestaciones de incertidumbre jurídica incluyen dificultades persistentes de calificación jurídica (18 menciones), ambigüedad de ciertas normas (14), pluralidad de fuentes reguladoras (12) y problemas de competencia (10). Los profesionales no afrontan únicamente problemas de aplicación de las normas existentes, sino un entorno regulador cambiante en el que se superponen normas jurídicas, reglas técnicas y condiciones de las plataformas, haciendo más complejas la atribución de responsabilidades y la calificación de los hechos. Estas dificultades ilustran el desplazamiento descrito en el apartado 3.2: cuando la norma penal no puede anticipar la técnica sin perder determinación, la incertidumbre pasa a la fase de interpretación, como ocurre con la aplicación del «montaje» del art. 447-2 del Código Penal a contenidos sintéticos generados por inteligencia artificial.

La incertidumbre jurídica no constituye, por tanto, un problema meramente teórico o legislativo, sino que afecta directamente a la práctica profesional cotidiana. En la dimensión institucional, la limitación de la experiencia técnica (17 de 30) contrasta con los medios especializados de que se han dotado las autoridades, como los servicios de prueba digital de la DGSN o las disposiciones sobre registro y aprehensión de datos digitales de la Ley n.º 03-23, que modifica y completa la Ley n.º 22-01 relativa al procedimiento penal, en vigor desde diciembre de 2025, cuya eficacia depende de capacidades que se construyen a su propio ritmo. Estos resultados son coherentes con la hipótesis.

5.4. Dimensión plataformal y transnacional: la cooperación con las plataformas

La mayoría de los profesionales evaluó como débil la cooperación con las plataformas digitales (16 participantes); once la consideraron media y solo tres la calificaron de buena. Existe así una brecha entre el papel creciente de las plataformas en la gestión del espacio digital y la capacidad de las instituciones jurídicas y judiciales para acceder efectivamente a los datos y a la información que aquellas poseen.

TABLA 12

Nivel de cooperación	**Entrevistados (n = 30)**
Débil	16
Medio	11
Bueno	3

Tabla 12. Evaluación profesional del nivel de cooperación con las plataformas digitales. (Fuente: elaboración propia a partir de las entrevistas semiestructuradas.)

Este resultado es coherente con lo planteado en el apartado 3.1 sobre la tecnonormatividad. Las plataformas no actúan únicamente como intermediarios técnicos, sino como actores con capacidad real para regular el acceso a la información y fijar las condiciones de cooperación. Según los entrevistados, su escasa colaboración se asocia a una mayor incertidumbre jurídica y a una menor eficacia de la respuesta frente a la ciberdelincuencia.

Esta constatación se refuerza al contrastarla con los informes de transparencia publicados por las grandes plataformas digitales sobre las solicitudes gubernamentales de acceso a datos de usuarios. En el caso de Marruecos, el Centro de Transparencia de Meta indica que, entre julio y diciembre de 2024, la plataforma recibió 612 solicitudes gubernamentales relativas a 665 usuarios o cuentas, y que produjo algún tipo de información en el 31,05 % de dichas solicitudes (Meta 2024). Estos datos muestran que la respuesta de la plataforma no es automática ni plena, sino que queda sometida a la valoración de la empresa sobre la legalidad, suficiencia y conformidad de la solicitud con sus propios criterios internos.

Desde una perspectiva comparada africana, Marruecos aparece además como una excepción regional por el volumen de solicitudes dirigidas a Meta. Según los datos publicados sobre el año 2024, el país habría formulado 1.188 solicitudes, una cifra muy superior a la registrada por otros Estados africanos (Ecofin Agency 2025).

Este desfase se refleja también en los instrumentos de cooperación directa con los proveedores de servicios. Marruecos se adhirió al Convenio de Budapest en 2018 y firmó el 12 de mayo de 2022 su Segundo Protocolo Adicional, relativo a la cooperación reforzada y la revelación de pruebas electrónicas, sin que conste su ratificación. Este tipo de instrumentos confía a los proveedores privados la valoración de las solicitudes (Rojszczak 2022, Sachoulidou 2024), lo que subraya que una parte decisiva de la prueba queda bajo el control de actores privados transnacionales.

5.5. Síntesis de los resultados

Los resultados son coherentes con la hipótesis en un sentido acotado. No muestran que la desincronización cause el aumento de la ciberdelincuencia, sino que la respuesta jurídico-institucional a esta presenta desfases identificables en las cuatro dimensiones del indicador. Los más marcados se sitúan en la dimensión plataformal (acceso a datos y cooperación con plataformas extranjeras) y en la institucional (prueba digital y experiencia técnica). La dimensión normativa se expresa sobre todo como dificultad de calificación, es decir, como incertidumbre desplazada a la fase de interpretación.

6. Discusión de los resultados

La discusión se organiza en torno a tres puntos: dónde se localiza la desincronización, cómo se desplaza la incertidumbre del legislador al intérprete y qué implicaciones tiene el caso marroquí para el estudio sociojurídico de la regulación.

6.1. Dónde se localiza la desincronización

Los resultados sitúan la desincronización sobre todo en las dimensiones plataformal e institucional. Las dificultades más citadas —prueba digital (26 de 30) y acceso a datos (22)— y la valoración mayoritariamente débil de la cooperación con las plataformas (16) remiten a un mismo hecho: una parte decisiva de la prueba está bajo custodia de actores privados transnacionales. Ello concuerda con la tesis de la sociedad de plataformas (van Dijck *et al.* 2018) y con la teoría del código, según la cual la arquitectura técnica regula la conducta junto al derecho (Lessig 2006).

La dimensión temporal ofrece un cuadro distinto: la adaptación normativa existe, pero llega por intervenciones sucesivas y específicas. Ello coincide con la tesis de la aceleración social (Rosa 2013) y con la concepción del tiempo jurídico como temporalidad propia (Ost 1999). El caso marroquí sugiere, sin embargo, que el desfase no es solo de velocidad: afecta a la capacidad de convertir innovaciones técnicas en categorías, pruebas y competencias jurídicamente estabilizadas, como se ha observado a propósito de la prueba electrónica y de la digitalización de los procedimientos (Contini y Reiling 2022, Ontanu 2022).

6.2. Del retraso legislativo a la incertidumbre interpretativa

La incertidumbre jurídica no procede solo de la ausencia de normas: las dificultades de calificación (18 de 30), la ambigüedad de algunas normas (14) y la pluralidad de fuentes reguladoras (12) aparecen en un sistema que ha legislado de forma reiterada sobre el entorno digital. Ello concuerda con el argumento del apartado 3.2: en derecho penal, la redacción tecnológicamente neutra está limitada por el mandato de determinación (Ossandón Widow 2009, Navarro Frías 2010), de modo que una parte del desfase se traslada del legislador al intérprete.

Esta lectura permite precisar la literatura sobre el *pacing problem* (Bennett Moses 2007, Marchant *et al.* 2011). Más que una carrera entre la tecnología y el derecho que el legislador podría ganar acelerando su producción normativa, el caso marroquí muestra una redistribución de la incertidumbre: hacia los jueces, que deben calificar conductas nuevas con categorías previas; hacia los peritos, que deben convertir datos técnicos en

prueba; y hacia las plataformas, que deciden sobre la entrega de datos. La eficacia del derecho depende así de su capacidad para producir una certeza práctica en la calificación, la prueba y la atribución de responsabilidades (Cabezudo Rodríguez 2016, Grimmelikhuijsen y Meijer 2022).

6.3. Implicaciones para el estudio sociojurídico de la regulación

Los resultados permiten, por último, precisar en qué sentido cabe hablar de una crisis de la regulación sociojurídica. El término no designa aquí un colapso normativo, sino una reducción persistente de la capacidad del sistema para producir certeza práctica y eficacia en un ámbito concreto. En ese sentido acotado, la respuesta a la ciberdelincuencia pone de manifiesto los límites de un modelo de regulación centrado en la producción legislativa nacional frente a un entorno transnacional y técnicamente mediado.

Este planteamiento parte de la literatura clásica que ha mostrado la transformación de la criminalidad en la era de la información (Yar 2013, Wall 2024), y la complementa al situar en el centro la dimensión sociojurídica. El artículo no se ocupa de las características técnicas o penales de la ciberdelincuencia, sino de las condiciones en que el sistema jurídico puede calificarla, probarla y perseguirla.

Esta lectura invita a repensar las políticas de lucha contra la ciberdelincuencia. No deberían limitarse a endurecer sanciones o actualizar normas, sino incluir el desarrollo de capacidades institucionales, la creación de mecanismos de cooperación con plataformas, el refuerzo de la cultura digital y una gobernanza capaz de reducir la brecha entre el tiempo de la tecnología y el tiempo del derecho.

7. Conclusión

El estudio ha analizado la relación entre transformación digital y ciberdelincuencia en Marruecos mediante una aproximación sociojurídica centrada en la desincronización normativa. Partió de la hipótesis de que la evolución de la ciberdelincuencia, y sobre todo la respuesta jurídico-institucional que suscita, refleja una brecha entre el ritmo de la transformación digital y el de la adaptación jurídica e institucional, que se expresa en formas concretas de incertidumbre jurídica.

Junto a la expansión del espacio digital, los datos estadísticos y de campo muestran un aumento notable y una diversificación de los casos de ciberdelincuencia, especialmente fraude digital, extorsión, atentados contra datos personales y vida privada.

La principal contribución del estudio no consiste en demostrar una relación entre digitalización y ciberdelincuencia, sino en mostrar dónde y cómo la respuesta jurídico-institucional pierde sincronía con el cambio tecnológico. El desafío principal no es la ausencia de normas o instituciones especializadas, sino la brecha entre el ritmo acelerado de la transformación digital y el ritmo más lento de la estructura jurídica e institucional. El concepto de desincronización normativa permite interpretar esta brecha como fuente de incertidumbre jurídica, visible en dificultades de calificación, complejidad de la prueba digital, cooperación limitada con plataformas y pluralidad de fuentes reguladoras.

Estos resultados invitan a estudiar la ciberdelincuencia no solo como fenómeno delictivo, sino como un terreno en el que se observan los límites de los modelos de regulación centrados en la producción legislativa nacional. No permiten afirmar que esos límites causen el aumento de los delitos, pero sí muestran que condicionan la capacidad del sistema para calificarlos, probarlos y perseguirlos.

La contribución teórica del artículo reside en proponer un marco interpretativo que articula transformación digital, desincronización normativa e incertidumbre jurídica, y un indicador de desincronización en cuatro dimensiones aplicable a otros sistemas jurídicos. El estudio amplía además el debate sociojurídico sobre digitalización al desplazar la atención desde los actos delictivos en sí mismos hacia las condiciones jurídicas e institucionales de su tratamiento.

A pesar de la relevancia de los resultados, el estudio está condicionado por la naturaleza cualitativa de la aproximación, los límites de la muestra y el periodo temporal de los datos. La muestra incluye solo a profesionales de la justicia y la regulación, no a víctimas ni a representantes de las plataformas; las estadísticas utilizadas son productos de la actividad institucional y no miden directamente la prevalencia; y el diseño no permite establecer relaciones causales. Futuras investigaciones podrían comparar experiencias nacionales, estudiar los efectos de la inteligencia artificial y de las plataformas algorítmicas sobre la regulación jurídica o analizar nuevas formas de interacción entre derecho y tecnología en entornos digitales emergentes.

En definitiva, el principal desafío que plantea la ciberdelincuencia en Marruecos no se limita a desarrollar mecanismos de lucha o actualizar textos legales, sino que consiste en construir nuevas formas de gobernanza y regulación capaces de reducir la brecha entre el tiempo de la tecnología y el tiempo del derecho en una sociedad sometida a transformaciones digitales aceleradas.

Referencias

Abou El Jaouad, A., 2023. La preuve numérique à l'épreuve de la cybercriminalité en droit marocain. *Revue Droit et Société* [en línea], *3*(11), 7–18. Disponible en: https://doi.org/10.5281/zenodo.10054215

Barrio Andrés, M., 2011. La ciberdelincuencia en el Derecho español. *Revista de las Cortes Generales* [en línea], (83), 273–305. Disponible en: https://doi.org/10.33426/rcg/2011/83/473

Bengoetxea, J., y Cruz Balbuena, R. L., 2024. Institutions of law in the metaverse. *Oñati Socio-Legal Series* [en línea], *14*(6), 1531–1554. Disponible en: https://doi.org/10.35295/osls.iisl.1852

Benlloch Domènech, C., y Sarrión Esteve, J., 2022. Los derechos fundamentales ante las aporías de la era digital. Cuestiones Constitucionales. *Revista Mexicana de Derecho Constitucional* [en línea], *1*(46), 3–28. Disponible en: https://doi.org/10.22201/iij.24484881e.2022.46.17046

Bennett Moses, L., 2007. Recurring dilemmas: The law's race to keep up with technological change. *University of Illinois Journal of Law, Technology & Policy*, *2007*(2), 239–285.

Brenner, S. W., 2004. Cybercrime metrics: Old wine, new bottles? *Virginia Journal of Law & Technology*, *9*(13).

Brownsword, R., 2019. *Law, technology and society: Reimagining the regulatory environment* [en línea]. Londres : Routledge. Disponible en: https://doi.org/10.4324/9781351128186

Cabezudo Rodríguez, N., 2016. Ciberdelincuencia e investigación criminal: Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. *Boletín del Ministerio de Justicia*, *70*(2186), 7–60.

Castells, M., 2010. *The rise of the network society* [en línea]. 2.ª ed. Hoboken : Wiley-Blackwell. Disponible en: https://doi.org/10.1002/9781444319514

Cohen, J. E., 2019. *Between truth and power: The legal constructions of informational capitalism* [en línea]. Nueva York : Oxford University Press. Disponible en: https://doi.org/10.1093/oso/9780190246693.001.0001

Contini, F., y Reiling, D., 2022. Double normalization: When procedural law is made digital. *Oñati Socio-Legal Series* [en línea], *12*(3), 654–688. Disponible en: https://doi.org/10.35295/osls.iisl/0000-0000-0000-1305

Di Porto, F., y Zuppetta, M., 2021. Co-regulating algorithmic disclosure for digital platforms. *Policy and Society* [en línea], *40*(2), 272–293. Disponible en: https://doi.org/10.1080/14494035.2020.1809052

El Azzouzi, A., 2010. *La cybercriminalité au Maroc* [en línea]. Edición del autor. Disponible en: https://cybercrime-fr.org/wp-content/uploads/2020/04/10.pdf

El Hamzaoui, M., y Bensalah, F., 2019. Cybercrime in Morocco: A study of the behaviors of Moroccan young people face to the digital crime. *International Journal of Advanced Computer Science and Applications* [en línea], *10*(4). Disponible en: https://doi.org/10.14569/IJACSA.2019.0100457

Grimmelikhuijsen, S., y Meijer, A., 2022. Legitimacy of algorithmic decision-making: Six threats and the role of institutional mechanisms. *Perspectives on Public Management and Governance* [en línea], *5*(3), 232–247. Disponible en: https://doi.org/10.1093/ppmgov/gvac008

Hamouti, N., y Elbouzidi, A., 2025. Victims of cybercrime: What criminal protection under Moroccan law? *International Journal of Social Science and Human Research* [en línea], *8*(7), 5094–5102. Disponible en: https://doi.org/10.47191/ijsshr/v8-i7-20

Hildebrandt, M., 2015. *Smart technologies and the end(s) of law: Novel entanglements of law and technology* [en línea]. Cheltenham : Edward Elgar. Disponible en: https://doi.org/10.4337/9781849808774

Jamaludin, A., *et al*., 2026. Propagation of AI-generated child sexual abuse material as a cybercrime commodity in Indonesia. *Oñati Socio-Legal Series* [en línea], *16*(3), 1189–1206. Disponible en: https://doi.org/10.35295/osls.iisl.2579

Judge, B., Nitzberg, M., y Russell, S., 2025. When code isn't law: Rethinking regulation for artificial intelligence. *Policy and Society* [en línea], *44*(1), 85–97. Disponible en: https://doi.org/10.1093/polsoc/puae020

Kitsuse, J. I., y Cicourel, A. V., 1963. A note on the uses of official statistics. *Social Problems* [en línea], *11*(2), 131–139. Disponible en: https://doi.org/10.2307/799220

Koops, B. J., 2006. Should ICT regulation be technology-neutral? *En :* B. J. Koops *et al.*, eds., *Starting points for ICT regulation: Deconstructing prevalent policy one-liners*. La Haya : T.M.C. Asser Press, 77–108.

Lehaire, B., 2022. *L'innovation hors-la-loi: Les origines de la techno-normativité.* Bruselas : Bruylant.

Lessig, L., 1999. *Code and other laws of cyberspace*. Nueva York : Basic Books.

Lessig, L., 2006. *Code: Version 2.0.* Nueva York : Basic Books.

Loddo, O. G., 2025. Regulatory digital artefacts: Digital regulation with and without rules. *International Journal of Law and Information Technology* [en línea], *33*, eaaf016. Disponible en: https://doi.org/10.1093/ijlit/eaaf016

Loschiavo Leme de Barros, M. A., y Fucci Amato, L., 2024. Regulation of digital misinformation: A socio-legal study on medical fake news in the Brazilian case. *Oñati Socio-Legal Series* [en línea], *14*(3), 719–738. Disponible en: https://doi.org/10.35295/osls.iisl.1804

Maleh, Y., y Maleh, Y., 2022. *Cybersecurity in Morocco* [en línea]. Cham : Springer. Disponible en: https://doi.org/10.1007/978-3-031-18475-8

Marchant, G. E., Allenby, B. R., y Herkert, J. R., eds., 2011. *The growing gap between emerging technologies and legal-ethical oversight: The pacing problem* [en línea]. Dordrecht: Springer. Disponible en: https://doi.org/10.1007/978-94-007-1356-7

Marddi, A., 2024. Lutte contre la cybercriminalité au Maroc: analyse de la contribution de la loi 07-03 sur les infractions relatives aux systèmes de traitement automatisé des données. *Revue Droit et Société* [en línea], *5*(13). Disponible en: https://doi.org/10.5281/zenodo.11323096

Martínez Galindo, G., 2022. Problemática jurídica de la prueba digital y sus implicaciones en los principios penales. *Revista Electrónica de Ciencia Penal y Criminología* [en línea], (24-23), 1–38. Disponible en: http://criminet.ugr.es/recpc/24/recpc24-23.pdf

Missaoui, M. K., 2016. *La cybercriminalité au Maroc, enjeux, évolution et défis*. Tesis doctoral, Universidad Mohammed V de Rabat.

Navarro Frías, I., 2010. *Mandato de determinación y tipicidad penal*. Granada : Comares.

Ontanu, E. A., 2022. Normalising the use of electronic evidence: Bringing technology use into a familiar normative path in civil procedure. *Oñati Socio-Legal Series* [en línea], *12*(3), 582–613. Disponible en: https://doi.org/10.35295/osls.iisl/0000-0000-0000-1304

Ortega Esquembre, C., 2023. Sobre los diferentes ritmos del derecho y la Inteligencia Artificial: La desincronización como patología social. *Daimon Revista Internacional de Filosofía* [en línea], (90), 147–161. Disponible en: https://doi.org/10.6018/daimon.551741

Ossandón Widow, M. M., 2009. *La formulación de tipos penales: Valoración crítica de los instrumentos de técnica legislativa.* Santiago: Editorial Jurídica de Chile.

Ossandón Widow, M. M., 2014. La técnica de las definiciones en la ley penal: Análisis de la definición de «material pornográfico en cuya elaboración hubieren sido utilizados menores de dieciocho años». *Política Criminal* [en línea], *9*(18), 279–337. Disponible en: https://doi.org/10.4067/S0718-33992014000200001

Ost, F., 1999. *Le temps du droit.* París : Odile Jacob.

Rojszczak, M., 2022. e-Evidence cooperation in criminal matters from an EU perspective. *The Modern Law Review* [en línea], *85*(4), 997–1028. Disponible en: https://doi.org/10.1111/1468-2230.12749

Rosa, H., 2013. *Social acceleration: A new theory of modernity*. Nueva York: Columbia University Press.

Sachoulidou, A., 2024. Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation. *New Journal of European Criminal Law* [en línea], *15*(3), 256–274. Disponible en: https://doi.org/10.1177/20322844241258649

Taeihagh, A., 2021. Governance of artificial intelligence. *Policy and Society* [en línea], *40*(2), 137–157. Disponible en: https://doi.org/10.1080/14494035.2021.1928377

van Dijck, J., Poell, T., y de Waal, M., 2018. *The platform society: Public values in a connective world*. Nueva York: Oxford University Press.

Wall, D. S., 2024. *Cybercrime: The transformation of crime in the information age*. 2.ª ed. Cambridge : Polity.

Yar, M., 2013. *Cybercrime and society*. 2.ª ed. Londres : Sage.

Yeung, K., 2017. 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society* [en línea], *20*(1), 118–136. Disponible en: https://doi.org/10.1080/1369118X.2016.1186713

Fuentes de datos e informes oficiales

Agence Nationale de Réglementation des Télécommunications [Agencia Nacional de Reglamentación de las Telecomunicaciones], 2025. *Observatoire de l'internet : Tableau de bord du parc internet au Maroc 2021–2025.* ANRT.

DataReportal, 2025. *Digital 2025: Morocco*. Kepios.

Direction Générale de la Sûreté Nationale [Dirección General de la Seguridad Nacional], 2021. *Bilan annuel des activités de la Direction Générale de la Sûreté Nationale au titre de l'année 2021.* DGSN.

Direction Générale de la Sûreté Nationale [Dirección General de la Seguridad Nacional], 2022. *Bilan annuel des activités de la Direction Générale de la Sûreté Nationale au titre de l'année 2022*. DGSN.

Direction Générale de la Sûreté Nationale [Dirección General de la Seguridad Nacional], 2023. *Bilan annuel des activités de la Direction Générale de la Sûreté Nationale au titre de l'année 2023*. DGSN.

Direction Générale de la Sûreté Nationale [Dirección General de la Seguridad Nacional], 2024. *Bilan annuel des activités de la Direction Générale de la Sûreté Nationale au titre de l'année 2024*. DGSN.

Direction Générale de la Sûreté Nationale [Dirección General de la Seguridad Nacional], 2025. *Bilan annuel des activités de la Direction Générale de la Sûreté Nationale au titre de l'année 2025*. DGSN.

Ecofin Agency, 2025. *Africa made the fewest data requests to Meta in 2024, raising questions on regulation* [en línea]. 9 de septiembre. Disponible en: https://www.ecofinagency.com/news/0909-48522-africa-made-the-fewest-data-requests-to-meta-in-2024-raising-questions-on-regulation

Meta, 2024. *Government requests for user data: Morocco, July–December 2024* [en línea]. Transparency Center. Disponible en: https://transparency.meta.com/reports/government-data-requests/country/MA/

Observatoire National de la Criminalité [Observatorio Nacional de la Criminalidad], 2025. *Bulletin statistique n° 03/2025: Indicateurs statistiques de la criminalité au Maroc.* Ministerio de Justicia.

Présidence du Ministère Public [Presidencia del Ministerio Público], 2020. *Rapport annuel sur la mise en œuvre de la politique pénale et l'amélioration de la performance du Ministère Public.* Presidencia del Ministerio Público.

Présidence du Ministère Public [Presidencia del Ministerio Público], 2021. *Rapport annuel sur la mise en œuvre de la politique pénale et l'amélioration de la performance du Ministère Public.* Presidencia del Ministerio Público.

Présidence du Ministère Public [Presidencia del Ministerio Público], 2022. *Rapport annuel sur la mise en œuvre de la politique pénale et l'amélioration de la performance du Ministère Public*. Presidencia del Ministerio Público.

Présidence du Ministère Public [Presidencia del Ministerio Público], 2023. *Rapport annuel sur la mise en œuvre de la politique pénale et l'amélioration de la performance du Ministère Public.* Presidencia del Ministerio Público.

Présidence du Ministère Public [Presidencia del Ministerio Público], 2024. *Rapport annuel sur la mise en œuvre de la politique pénale et l'amélioration de la performance du Ministère Public.* Presidencia del Ministerio Público.

Fuentes normativas

Avant-projet de loi n.º 42-25 relative aux crypto-actifs [Anteproyecto de ley n.º 42-25 relativo a los criptoactivos]. 5 de agosto de 2025.

Consejo de Europa, 2001. *Convenio sobre la Ciberdelincuencia (STE n.º 185)*. Adhesión de Marruecos : 29 de junio de 2018 ; entrada en vigor: 1 de octubre de 2018.

Consejo de Europa, 2022. *Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la cooperación reforzada y la revelación de pruebas electrónicas (STCE n.º 224)*. Firmado por Marruecos el 12 de mayo de 2022.

Constitución del Reino de Marruecos, 2011. *Dahir n.º 1-11-91*, de 29 de julio de 2011.

Dahir n.º 1-03-197, de 11 de noviembre de 2003, por el que se promulga la Ley n.º 07-03 que completa el Código Penal en lo relativo a las infracciones relativas a los sistemas de tratamiento automatizado de datos [portant promulgation de la loi n.º 07-03 complétant le Code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données].

Dahir n.º 1-07-129, de 30 de noviembre de 2007, por el que se promulga la Ley n.º 53-05 relativa al intercambio electrónico de datos jurídicos [portant promulgation de la loi n.º 53-05 relative à l'échange électronique de données juridiques]. *Boletín Oficial* (edición en lengua francesa), n.º 5584.

Dahir n.º 1-09-15, de 18 de febrero de 2009, por el que se promulga la Ley n.º 09-08 relativa a la protección de las personas físicas respecto del tratamiento de datos de carácter personal [portant promulgation de la loi n.º 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel]. *Boletín Oficial* (edición en lengua francesa), n.º 5714, 5 de marzo de 2009.

Dahir n.º 1-18-19, de 22 de febrero de 2018, por el que se promulga la Ley n.º 103-13 relativa a la lucha contra la violencia contra las mujeres [portant promulgation de la loi n.º 103-13 relative à la lutte contre les violences faites aux femmes]. *Boletín Oficial* (edición en lengua francesa), 5 de julio de 2018.

Dahir n.º 1-20-100, de 31 de diciembre de 2020, por el que se promulga la Ley n.º 43-20 relativa a los servicios de confianza para las transacciones electrónicas [portant promulgation de la loi n.º 43-20 relative aux services de confiance pour les transactions électroniques].

Dahir n.º 1-20-69, de 25 de julio de 2020, por el que se promulga la Ley n.º 05-20 relativa a la ciberseguridad [portant promulgation de la loi n.º 05-20 relative à la cybersécurité]. *Boletín Oficial* (edición en lengua francesa), n.º 6906, 6 de agosto de 2020.

Loi n.º 03-23 modifiant et complétant la loi n.º 22-01 relative à la procédure pénale. [Ley n.º 03-23 que modifica y completa la Ley n.º 22-01 relativa al procedimiento penal, promulgada por el Dahir n.º 1-25-55 de 19 de safar de 1447 (13 de agosto de 2025)]. *Boletín Oficial* [edición en lengua francesa], n.º 7437, 8 de septiembre de 2025.

Naciones Unidas, 2024. *Convención de las Naciones Unidas contra la Ciberdelincuencia.* Firmada por Marruecos el 25 de octubre de 2025.

Office des Changes [Oficina de Cambios], 2017. *Communiqué relatif aux monnaies virtuelles* [Comunicado relativo a las monedas virtuales]. 20 de noviembre.

Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales.