El peso de la historia: desafíos de la policía en la gobernanza del cibercrimen en España

The Weight of History: Challenges for Police in the Governance of Cybercrime in Spain

CRISTINA DEL-REAL

Leiden University, Países Bajos

RESUMEN: El cibercrimen presenta diversos desafíos para la policía, incluyendo la complejidad y globalidad de las acciones criminales, la dificultad de rastrear el ciberespacio y la constante evolución de estas actividades delictivas. A través del marco conceptual de institucionalismo histórico y discursivo, este artículo explora los retos de la policía en la gobernanza del cibercrimen en España. El artículo destaca la importancia de situar la policía en el contexto del sistema de gobernanza de la ciberseguridad para comprender sus desafíos y adaptaciones. A través del análisis de 36 documentos clave, se argumenta que los orígenes y la evolución de las políticas de ciberseguridad se fundamentaron en narrativas centradas en la protección de la información y el incremento de la confianza de la sociedad en las tecnologías digitales, ambas narrativas alejadas del discurso centrado en la ciberdelincuencia. El estudio de caso en España enriquece la literatura sobre gobernanza de la ciberseguridad al explorar cómo la evolución histórica y las narrativas impactan en la posición de los actores involucrados en el sistema de gobernanza.

PALABRAS CLAVE: Gobernanza de la ciberseguridad; Institucionalismo discursivo; Institucionalismo histórico; Narrativas de ciberseguridad.

ABSTRACT: Cybercrime presents a myriad of challenges for law enforcement agencies, including the complexity and global nature of criminal activities, the difficulties in tracing activities within cyberspace, and the perpetual evolution of these unlawful practices. This article employs the conceptual framework of historical and discursive institutionalism to investigate the hurdles faced by the police in governing cybercrime in Spain. The study emphasizes the importance of situating law enforcement within the cybersecurity governance system to comprehend their challenges and adaptations. By analyzing 36 key documents, it argues that cybersecurity policies' origins and evolution were rooted in narratives focused on information protection and enhancing society's trust in digital technologies, narratives distinct from the discourse centered on cybercrime. The Spanish case study enriches the literature on cybersecurity governance by examining how historical evolution and narratives impact the roles of actors involved in the governance system.

KEYWORDS: Cybersecurity governance; Discursive institutionalism; Historical institutionalism; Cybersecurity narratives.

Revista de Estudios en Seguridad Internacional, Vol. 9, No. 2, (2023), pp. 77-99. http://www.seguridadinternacional.es/resi/index.php/revista

ISSN: 2444-6157. DOI: http://dx.doi.org.10.18847/1.18.5

INTRODUCCIÓN

El ciberespacio es una compleja red global que conecta las tecnologías digitales. En los últimos 30 años, ha evolucionado hasta convertirse en una de las columnas vertebrales de nuestra sociedad. Ciudadanos, empresas e instituciones utilizan el ciberespacio para sus actividades cotidianas, ofrecer productos o servicios, y gestionar las infraestructuras de un país (p.ej., aeropuertos, gestión de aguas, redes eléctricas, entre otras). Esta hiperconectividad en las sociedades avanzadas trae consigo importantes ventajas, como una mayor eficiencia y accesibilidad a los recursos, así como la democratización del acceso a servicios e información. Sin embargo, también implica crecientes riesgos, ya que las tecnologías de redes digitales a menudo presentan vulnerabilidades que pueden ser aprovechadas por actores maliciosos o provocar errores humanos o del sistema con graves consecuencias económicas, sociales, políticas e incluso psicológicas y físicas. A medida que aumenta nuestra dependencia del ciberespacio, este problema se vuelve más urgente y complejo.

Las políticas de ciberseguridad buscan ofrecer soluciones a los crecientes riesgos y amenazas presentes en el ciberespacio. Este campo es relativamente nuevo y ha ido consolidándose en la Unión Europea en los últimos años, hasta alcanzar su estatus como área política independiente en 2013 con la primera Estrategia de Ciberseguridad (Carrapico & Farrand, 2020; European Commission, 2013). En España, las políticas de ciberseguridad han seguido un proceso paralelo al de las políticas europeas, impulsadas en gran medida por estas últimas. Como resultado de esta consolidación, han surgido y evolucionado nuevas instituciones y estrategias para enfrentar las amenazas y riesgos del ciberespacio. Una de las instituciones que ha tenido que adaptarse a estas nuevas amenazas es la policía.

La policía ha tenido que adaptarse a la nueva amenaza del cibercrimen[1]. De forma general, un *cibercrimen* es aquel crimen facilitado o llevado a cabo por dispositivos digitales, como puede ser un ordenador (Gordon & Ford, 2006). Dentro de esta amplia definición, la literatura criminológica distingue entre i) delitos tradicionales que utilizan el ciberespacio como medio para su comisión, y ii) nuevas formas delictivas en las que las tecnologías digitales son tanto el medio como el objetivo del delito (Gordon & Ford, 2006; Leukfeldt & Holt, 2020; McGuire, 2020; Wall, 2007). La clasificación más utilizada en Criminología diferencia entre: delitos tradicionales i), que son conocidos como "delitos facilitados por el ciberespacio" (en inglés, *cyber-enabled crimes*), y las nuevas formas delictivas ii), definidas como "delitos dependientes del ciberespacio" (en inglés, *cyber-dependent crimes*)[2] (McGuire & Dowling, 2013a, 2013b, 2013c). Como ejemplos de delitos facilitados por el ciberespacio se encontrarían el fraude en línea, el

[1] Los conceptos que entran dentro de la definición de "acciones maliciosas en el ciberespacio" son objeto de amplio debate. Cada disciplina ofrece una visión y vocabulario propios. La criminología define el cibercrimen de forma amplia, como el producto del comportamiento delictivo en el ciberespacio. Sin embargo, las ciencias de la computación diferencian entre cibercrimen (p.ej., fraude online a través de phishing) de un ciberataque por malware (que no definen estrictamente como cibercrimen). Desde las ciencias jurídicas, el concepto de cibercrimen no es tan relevante como el hecho de que la acción sea punible en el Código Penal. Finalmente, los estudios desde las relaciones internacionales están más interesados en comprender estas acciones maliciosas en el contexto de conflictos entre Estados y actores no estatales con intereses geopolíticos, por lo que se decantan por denominarlas "ciber-operaciones" y prefieren ignorar el componente delictivo. La policía, en tanto que su actuación está determinada por las leyes (penales), comprende el cibercrimen desde un punto de vista jurídico y criminológico.

[2] Traducción propia de los originales en inglés.

stalking o el ciberacoso, mientras que el *hacking* malicioso[3], el ataque por denegación de servicios[4] o la infección de dispositivos por *malware*[5], entre otros, serían delitos dependientes del ciberespacio.

El cibercrimen presenta numerosas características que dificultan la respuesta de la policía. En primer lugar, su comisión a menudo involucra múltiples jurisdicciones, ya que los cibercriminales pueden operar desde cualquier parte del mundo y sus acciones afectan a víctimas en diferentes países. Esta falta de fronteras físicas y la globalización de las acciones cibercriminales dificultan la actuación de las organizaciones policiales, cuyas competencias están limitadas por las fronteras físicas establecidas por ley, lo que requiere un mayor esfuerzo de coordinación y cooperación internacional. En segundo lugar, gran parte del cibercrimen es complejo y el ciberespacio es difícil de rastrear. Obtener evidencia sobre la autoría de un cibercrimen es complicado. Además, el cibercrimen está cada vez más profesionalizado, y un reducido número de criminales suele ser responsable de la mayoría de los delitos, en línea con la "ley de la concentración delictiva" identificada en investigaciones sobre *website defacement*[6] (Moneva et al., 2022) y cibercrimen relacionado con Bitcoin (Buil-Gil & Saldaña-Taboada, 2022). Los cibercriminales y grupos cada vez adoptan modelos similares a los de empresas tecnológicas, reinvirtiendo el dinero obtenido de actividades ilícitas en su propio negocio y mejorando constantemente su preparación y equipamiento. Esto desafía a las policías, cuya adopción de innovaciones suele ser más lenta (Weisburd & Braga, 2019). Por último, el cibercrimen está en constante evolución, lo que requiere que las organizaciones policiales se adapten y actualicen continuamente sus estrategias para combatirlo de manera efectiva.

Este artículo amplía el enfoque de análisis de la policía para situarla en el contexto del sistema de gobernanza de la ciberseguridad. Se argumenta que, además de los desafíos organizativos (ver sección de "Antecedentes"), la policía en España enfrenta un *reto histórico y narrativo*. A través del institucionalismo histórico y discursivo, se sostiene que las políticas de ciberseguridad en España, que a menudo excluyen a la policía, y la relación de esta última con los actores centrales, pueden entenderse mediante el contexto histórico y discursivo en el que han surgido y evolucionado dichas políticas. Basándose en estudios previos realizados en el contexto de la Unión Europea (ver Carrapico & Farrand, 2020), este trabajo propone que la actual posición de la policía en la gobernanza de la ciberseguridad está asociada al desarrollo y formalización de las políticas de ciberseguridad en España, las cuales son el resultado de dependencias de enfoques ideacionales basados en narrativas alejadas de la policía. El artículo sostiene que la policía en España ha "perdido" la batalla narrativa del cibercrimen y la seguridad pública a favor de las narrativas centradas en la protección de la información y la confianza de la sociedad en las tecnologías digitales.

Este artículo contribuye al campo de la gobernanza de la ciberseguridad al ampliar el enfoque de análisis sobre las percepciones, estrategias y adaptaciones organizativas de

[3] Intrusión ilícita en los sistemas de otra persona u organización.

[4] Ciberataque (generalmente causado por una sobrecarga del sistema) que provoca que un sistema o recurso sea inaccesible a sus usuarios legítimos.

[5] Infección producida por un programa informático malicioso que causa daños en el sistema infectado.

[6] El concepto de "*website defacement*" hace referencia a una práctica en el ámbito de la ciberseguridad que consiste en efectuar alteraciones, modificaciones o cambios en el contenido de un sitio web sin contar con la debida autorización del propietario legítimo.

policía al cibercrimen y situarla en un contexto más amplio de desarrollo de políticas de seguridad (ver para un enfoque similar Jiménez y Torrente, 2017). El estudio de caso en España tiene como objetivo enriquecer la literatura al explorar los desafíos que enfrenta la policía en la gobernanza del cibercrimen, evidenciando cómo la evolución histórica y las narrativas relacionadas con el desarrollo de políticas nacionales impactan en la posición de los diferentes actores dentro del sistema de gobernanza y sus cambios institucionales.

ANTECEDENTES: ESTUDIOS SOBRE LOS RETOS DE LA POLICÍA EN LA LUCHA CONTRA EL CIBERCRIMEN

Los retos a los que se ha enfrentado la policía para adaptar su organización al cibercrimen han sido objeto de numerosos estudios durante los últimos quince años. La revisión de ellos permite identificar cuatro grandes motivos: i) tardía y desigual percepción policial del problema del cibercrimen, ii) estrategias y herramientas policiales inadecuadas, iii) confusión jurídica y jurisdiccional, y iv) elevada cifra negra del cibercrimen.

Percepción policial tardía y desigual del problema del cibercrimen

Uno de los desafíos planteados inicialmente por Senjo (2004) y Wall (2007) radica en la discrepancia entre la percepción de la policía sobre los cibercrímenes y la verdadera magnitud de la delincuencia en el ciberespacio, un fenómeno al que se ha denominado "percepción subestimada" del problema (Wall, 2007). Esta discrepancia ha sido corroborada por diversos estudios (Bossler & Holt, 2012; Holt & Bossler, 2012) realizados con policías tanto estadounidenses como británicos, en los cuales se constató que los agentes encuestados no consideraban que la lucha contra el cibercrimen fuera una de sus responsabilidades principales. En cambio, opinaban que la prevención del cibercrimen era una tarea exclusiva de los ciudadanos y las empresas (Bossler & Holt, 2012).

Estudios más recientes, sin embargo, indican que esta percepción subestimada del cibercrimen puede considerarse más bien como una percepción tardía, ya que actualmente las fuerzas policiales parecen haber adquirido una conciencia más realista respecto al problema del cibercrimen (Holt et al., 2018; Lee et al., 2019). Especialmente en lo que se refiere a aquellos delitos que hemos definido como "facilitados por el ciberespacio" (Holt et al., 2018; Lee et al., 2019), se observa una mayor toma de conciencia. Esta tardanza en la identificación del cibercrimen como una problemática relevante por parte de las fuerzas policiales ha tenido como consecuencia que los recursos destinados para enfrentarlo, como la creación de unidades especializadas en cibercrimen o la adquisición de herramientas informáticas avanzadas, se hayan asignado principalmente en años recientes.

Estrategias y herramientas policiales inadecuadas

Gran parte de las estrategias y herramientas que las fuerzas policiales emplean en la actualidad tienen sus raíces en la Policía Metropolitana de Londres, fundada en 1829 (Lab, 2016). Estas instituciones enfatizan en el patrullaje como un método para prevenir y detectar delitos mediante la disuasión (Weisburd & Braga, 2019). A pesar de los avances tecnológicos y las innovaciones en las estrategias policiales en años recientes,

como la prevención comunitaria, la resolución de problemas o la predicción del delito (Weisburd & Braga, 2019), la mayoría de las fuerzas policiales continúan basando sus operaciones en el patrullaje para la disuasión y detección del delito, sin haber adaptado completamente sus estrategias y herramientas para abordar eficazmente el cibercrimen.

La primera ola de estudios que examinaban la preparación de las fuerzas policiales para combatir el cibercrimen (p.ej., Burns et al., 2004; Hinduja, 2004; McQuade, 2006; Senjo, 2004) se une a investigaciones más recientes que continúan concluyendo que las policías aún no están preparadas (Burruss et al., 2019; Harkin et al., 2018; Leukfeldt et al., 2013). En un estudio realizado en los Países Bajos por Leukfeldt et al. (2013), se encontró que las policías holandesas no estaban adecuadamente preparadas para enfrentar el cibercrimen, particularmente en los casos de hacking y fraude en línea, debido a la falta de comprensión de la mayoría de los agentes. Como resultado, la responsabilidad se centraba en las unidades especializadas en cibercrimen de cada policía, pero estas se veían abrumadas por el alto y creciente volumen de delitos cibernéticos, lo que las obligaba a priorizar casos más graves (Leukfeldt et al., 2013: 12).

En otro estudio más reciente realizado por Harkin et al. (2018) en dos organizaciones policiales de Australia, los autores concluyeron que el 71% de los policías consideraba insuficiente su conocimiento y preparación para combatir el cibercrimen. Según los policías entrevistados, a pesar de recibir formación técnico-teórica sobre el tema, esta no era suficiente para enfrentar eficazmente el cibercrimen debido a su naturaleza cambiante y compleja (Harkin et al., 2018: 526). En otro estudio con 1467 policías de Inglaterra y Gales, los profesores Burruss et al. (2019) encontraron que el 80,9% no confiaba en la efectividad de la respuesta policial actual ante el cibercrimen.

En este contexto, la formación y capacitación en cibercrimen se ha considerado una vía para mejorar la preparación de las fuerzas policiales frente a estos casos. Sin embargo, las investigaciones realizadas hasta la fecha indican que esta medida no es suficiente. Por ejemplo, en un estudio llevado a cabo con 16 agentes de policía en Australia, se encontró que consideraban que la policía carecía del conocimiento necesario para abordar casos de cibercrimen (Hadlington et al., 2021). Otro estudio de caso con tres unidades de cibercrimen en Australia concluyó que el entrenamiento mejoraría la preparación de los agentes ante el cibercrimen (Harkin & Whelan, 2022). Aun así, solo un número limitado de agentes tenía un conocimiento avanzado sobre cómo funcionan las redes informáticas. Esta falta de entrenamiento afectaba a diferentes escalas dentro de la policía). Otro estudio realizado con 442 agentes de policía en Australia reveló que, aunque la mitad de los participantes había recibido entrenamiento sobre cibercrimen, la mayoría seguía sintiendo que carecían de los conocimientos necesarios para enfrentar casos de esta índole (Wilson et al., 2022). Finalmente, un estudio en España con 129 expertos en ciberseguridad obtuvo que mientras la Policía Nacional y la Guardia Civil eran percibidas como más legítimas (con un mayor capital simbólico) que otras organizaciones públicas o privadas en el ámbito de la ciberseguridad, estas no cuentan con los recursos económicos y de personal necesarios para hacer frente a las demandas del cibercrimen (Del-Real & Díaz-Fernández, 2022).

Estas investigaciones sugieren que las policías se beneficiarían de destinar mayores recursos económicos, de personal, entrenamiento en las competencias requeridas para la gestión de casos de cibercrimen, como el manejo de escenas de crimen digitales, la preservación de evidencia digital o los procedimientos para recibir o remitir denuncias de víctimas de cibercrimen. Asimismo, se observó que diferentes categorías de policías

en Australia presentaban distintos niveles de déficit en su formación. Aquellos que habían completado entrenamientos específicos sobre cibercrimen se mostraban más confiados en su capacidad para responder ante incidentes de esta naturaleza.

Esta falta de preparación ha llevado a las fuerzas policiales a depender de actores externos para complementar su trabajo (Burruss et al., 2019; Harkin et al., 2018; Nhan & Huey, 2008). En este sentido, los estudios han encontrado que la conciencia sobre los déficits en las capacidades propias entre agentes de policía correlaciona con niveles más altos de apoyo a las asociaciones público-privadas para regular el ciberespacio (Button, 2020; Paek et al., 2020).

Confusión jurídica, jurisdiccional y terminológica

El cibercrimen, al no tener limitaciones geográficas y estar en constante evolución, ha planteado desafíos a las regulaciones penales y procesales en términos de qué conductas se consideran delito y qué tribunal sería competente para conocer del caso (Brenner, 2006; Cross, 2019; Holt, 2018). El principio *nullum crimen sine lege* establece que para que la policía pueda investigar una conducta como delito, esta debe estar definida como tal en una ley penal. Sin embargo, surge un problema debido a que las leyes suelen tener un alcance limitado a fronteras territoriales específicas (Wall, 2007). Los cibercrímenes, en cambio, no se ajustan a las tradicionales fórmulas utilizadas por el Derecho penal y procesal para asignar competencia en la investigación y enjuiciamiento de delitos, ya que ocurren a escala global o en un marco geográfico que trasciende las fronteras estatales. Es decir, tanto su comisión como las potenciales víctimas pueden estar físicamente ubicadas en diferentes países, lo que afecta a diferentes jurisdicciones. La dificultad para perseguir estos delitos radica en la falta de homogeneidad en la calificación jurídica de las conductas entre los distintos sistemas jurídicos de los países.

Relacionado con este problema, existe un problema conceptual del cibercrimen que puede trasladarse a confusiones en la regulación y la práctica policial (Del-Real, 2022). En este sentido, el estudio de Hadlington et al. (2021) encontró que la ambigüedad terminológica era uno de los grandes problemas de las unidades policiales especializadas en cibercrimen. Más adelante, y basándose en 13 entrevistas semiestructuradas a especialistas de cibercrimen de ocho países distintos, un estudio también confirmó que existe una confusión generalizada sobre el uso de definiciones y taxonomías para el cibercrimen (De Paoli et al., 2021). Las diferentes policías y jurisdicciones utilizan diversas definiciones, dificultando la coherencia en las denuncias, la recogida de datos y la investigación estadística (De Paoli et al., 2021).

Falta de denuncias y elevada cifra negra

La efectividad de las medidas de prevención del crimen depende en gran medida del conocimiento que tengamos sobre el fenómeno que queremos prevenir. Una de las fuentes más confiables de información es a través de las estadísticas oficiales. Sin embargo, para obtener estadísticas precisas, es necesario que las víctimas denuncien los delitos ante la policía, lo que daría lugar a investigaciones que permitan abrir procedimientos penales para esclarecer las causas y características del delito, aumentando así el conocimiento policial. No obstante, un problema que afecta a las estadísticas oficiales es la existencia de la "cifra negra" del crimen (Coleman & Moynihan, 1996), que representa la gran cantidad de delitos que no se denuncian. Esta

cifra negra es aún más pronunciada en el caso del cibercrimen, lo que dificulta aún más la obtención de datos precisos y representativos.

Investigaciones empíricas han mostrado que solo una pequeña proporción de los cibercrímenes cometidos se denuncian a las autoridades. Un estudio realizado por Domenie et al. (2013) en los Países Bajos, con una muestra de 9.163 usuarios de Internet, reveló que solo el 13,4% de las víctimas de cibercrimen había denunciado el delito a la policía. Dentro de los tipos de delitos, solo el 4,1% de las víctimas de hacking había presentado denuncia, mientras que el delito más denunciado fue el stalking, con un 30,4% de denuncias.

Los estudios cualitativos han arrojado resultados similares, mostrando que las víctimas de cibercrímenes suelen ser reticentes a denunciar, e incluso cuando están dispuestas a hacerlo, muchas veces no saben dónde hacerlo (p.ej., Bidgoli, 2015; Burgard & Schlembach, 2013). Un estudio más reciente realizado por Van de Weijer et al. (2019) con una amplia muestra de 97.186 víctimas de delitos también reveló tasas bajas de denuncias en cibercrímenes en comparación con delitos tradicionales. Por ejemplo, mientras que los delitos como el robo de coches o el intento de allanamiento de morada se denunciaban en más del 70% de los casos, la denuncia por cibercrímenes estaba por debajo del 30%. Específicamente, el robo de identidad se denunció en un 26,3% de los casos, el ciberfraude en un 24% y el hacking en un 7,1%. Esta baja tasa de denuncias representa un desafío significativo para la policía y otros actores involucrados en la ciberseguridad, ya que dificulta el diseño de medidas de prevención coherentes con las evidencias científicas en relación a este tipo de delitos.

Los estudios mencionados anteriormente se han enfocado en comprender los desafíos que enfrentan las fuerzas policiales en la lucha contra el cibercrimen. Se han identificado retos en la percepción policial del cibercrimen como problema, la adaptación insuficiente de capacitaciones y herramientas a las necesidades de esta lucha, el marco jurídico, jurisdiccional y terminológico que limita las actuaciones policiales y dificulta la cooperación entre distintos departamentos y organizaciones policiales, y las bajas cifras de ciberdelincuencia denunciadas. No obstante, estos estudios se han centrado principalmente en los desafíos organizativos de la policía. En este artículo, se propone ampliar el campo de estudio hacia los desafíos que enfrenta la policía en relación con la evolución del sistema de gobernanza de la ciberseguridad en España, para lo cual se utilizará el enfoque analítico del institucionalismo histórico y discursivo.

El institucionalismo histórico y discursivo para entender el rol de la policía en la lucha contra el cibercrimen

Este estudio adopta el marco analítico propuesto por Carrapico y Farrand (2020) que combina el institucionalismo histórico y el institucionalismo discursivo. Por un lado, el institucionalismo histórico representa una corriente en la ciencia política que se enfoca en el análisis de las instituciones políticas y sociales teniendo en cuenta su desarrollo y evolución a lo largo del tiempo (Skocpol, 1979). Este enfoque tiene como objetivo comprender cómo las instituciones han sido configuradas por eventos y decisiones pasadas, y cómo dichas estructuras institucionales influyen en el comportamiento político y social en la actualidad. El institucionalismo histórico pone énfasis en la

trayectoria histórica y la dependencia del camino[7] en la configuración de las instituciones. Se argumenta que el pasado ejerce una influencia significativa en el desarrollo y funcionamiento de las instituciones actuales, así como en las preferencias de los individuos que las forman (Peters, 2019). Este enfoque reconoce que los momentos críticos (*"critical junctures"*) y eventos clave pueden generar cambios significativos en las instituciones y sus resultados, alterando el curso de su evolución. Para Carrapico y Farrand (2020: 1113), los procesos graduales son tan importantes como estos momentos críticos: "los momentos críticos sirven como ventanas de oportunidad para reformas más profundas que producen dependencias del camino, que enmarcan los micro-cambios cotidianos que siguen teniendo lugar y que la igualdad contribuye a cambiar las trayectorias institucionales, aunque de forma menos perceptible"[8]. El institucionalismo histórico, aplicado al caso de la policía, ha sido utilizado para comprender reformas policiales (Lau, 2004; Medeiros Passos, 2015), y las percepciones de legitimidad y equidad policial entre países postcomunistas y democracias establecidas (Baćak & Apel, 2021).

El institucionalismo histórico ha sido criticado porque ignora el rol de las ideas, los discursos y las narrativas en el cambio institucional (Schmidt, 2011, 2008). Al no tener en cuenta el rol de las ideas y los discursos, el institucionalismo histórico dibuja una visión materialista y determinista de las instituciones (Carrapico and Farrand, 2020). En su lugar, el institucionalismo discursivo representa una corriente teórica dentro de la ciencia política y la sociología enfocada en el papel del discurso y las ideas en la formación, el cambio y la reproducción de las instituciones políticas y sociales. El institucionalismo discursivo es el "más nuevo" de los cuatro neoinstitucionalismos en ciencia política (junto con el institucionalismo de elección racional, el institucionalismo sociológico, y el ya comentado arriba institucionalismo histórico) (Schmidt, 2008). Esta corriente enfatiza cómo las representaciones simbólicas, las narrativas y los discursos influyen en la configuración de las instituciones, y cómo los actores sociales construyen significados y comprenden el mundo político a través de la comunicación. Desde el institucionalismo discursivo se reconoce que los discursos y las narrativas tienen un poder significativo al contribuir a la construcción de la realidad social y política. Las palabras y las ideas no solo reflejan la realidad, sino que también la moldean y le otorgan significado. En este sentido, las instituciones y las políticas no son únicamente estructuras físicas o procedimientos formales, sino también construcciones simbólicas que se mantienen y transforman a través de las prácticas discursivas. Los estudios desde esta perspectiva analizan cómo ciertas narrativas y discursos dominantes pueden influir en la toma de decisiones, la formulación de políticas y la acción política, y cómo el lenguaje y las representaciones simbólicas pueden legitimar o cuestionar determinadas instituciones y prácticas políticas.

De acuerdo con Schmidt (2008), para comprender cómo las ideas y los discursos generan dependencia del camino, es fundamental explorar su papel en la formulación de políticas. Según esta autora, las ideas pueden organizarse en un sistema de tres niveles, estructurados de manera similar a una muñeca Matryoshka: la primera muñeca representa las "filosofía" –ideologías o concepciones del mundo– que encapsulan a una segunda muñeca, compuesta por los "programas" –la traducción de las filosofías en

[7] Este concepto es más conocido en su versión en inglés, *path dependency*.
[8] Traducción propia del original en inglés.

principios y directrices estratégicas–, que a su vez contiene en su centro las "políticas" – la aplicación práctica de las filosofías y programas.

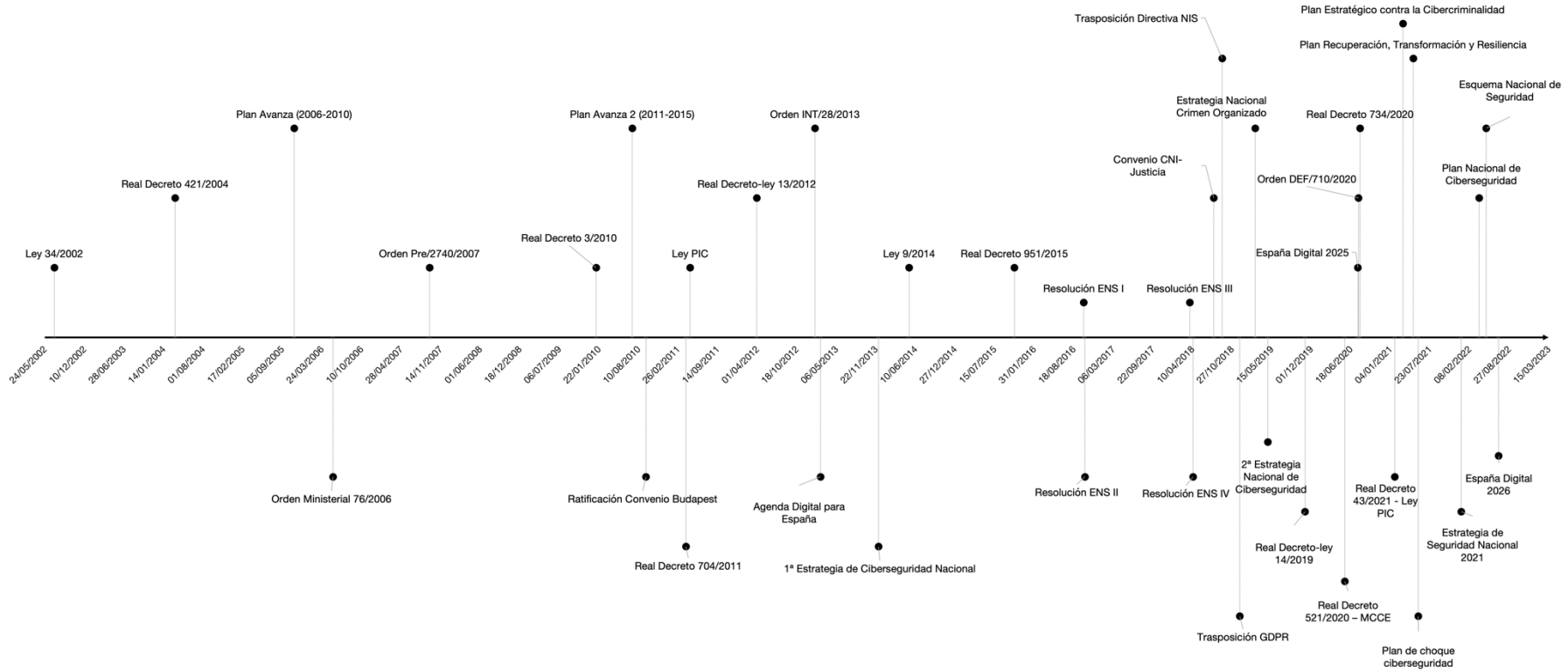
En este artículo se sostiene que las políticas de ciberseguridad en España se establecieron inicialmente alejadas de la narrativa de seguridad pública y, en consecuencia, de las policías, debido a la percepción inicial de que la ciberseguridad era principalmente una responsabilidad individual, ya sea de los ciudadanos o de las empresas (Broeders, 2021), o bien una característica secundaria en comparación con el objetivo principal de desarrollo económico y crecimiento digital del mercado (Carrapico & Farrand, 2020). Para respaldar esta afirmación, se ha llevado a cabo un análisis de 36 documentos clave que abarcan la evolución de la ciberseguridad en España, incluyendo leyes, regulaciones y planes estratégicos (la lista completa se puede consultar en el Anexo 1).[9] Estos documentos se han utilizado como fuente de datos para explorar la evolución de las narrativas, políticas y marcos de gobernanza del cibercrimen (ver ejemplos similares de uso de documentos como fuente de información para investigaciones sobre gobernanza del cibercrimen y la ciberseguridad en Bossong & Wagner, 2017; Cruz Lobato, 2017; Dupont, 2017; Kuerbis & Badiei, 2017).

Evolución de las políticas de ciberseguridad y el rol de la policía en la lucha contra el cibercrimen en España

Esta sección se enfoca en la evolución y consolidación de las políticas de ciberseguridad de España, combinando los enfoques del institucionalismo histórico y el institucionalismo discursivo. Para alcanzar este objetivo, se tratará de identificar los fundamentos ideacionales subyacentes a las políticas. Además, se analizará el desarrollo discursivo a lo largo del tiempo, señalando los momentos cruciales que han moldeado los enfoques adoptados. La trayectoria de las políticas de ciberseguridad en España se ha dividido en cuatro fases principales: la fase de origen, que abarca desde comienzos del siglo XX a 2012, la fase de consolidación, que se extiende de 2013 a 2017, la fase de ruptura ideológica (2017-2020), y la fase de adaptación, a partir de la pandemia de Covid-19 de 2020 (en la Figura 1 se puede consultar la evolución de las políticas de ciberseguridad y cibercrimen). El objetivo es demostrar que los retos de la policía en España, en términos de su acceso a la información, su rol dentro del sistema de lucha contra el cibercrimen, y sus relaciones con otros actores, no puede ser comprendido únicamente desde sus retos organizativos. Por el contrario, para comprender plenamente los retos presentes y futuros de la policía en España en la gobernanza del cibercrimen es necesario situarlas dentro de un contexto histórico, ideacional y discursivo más amplio.

[9] Aunque este estudio se basa en leyes, regulaciones y documentos de políticas, es necesario precisar que no es un estudio jurídico. Por tanto, el análisis que se realiza sobre los documentos no tiene un enfoque jurídico.

Figura 1. Evolución de las políticas de ciberseguridad (y cibercrimen) más relevantes en España (2000-2023)



Fuente: elaboración propia.

Origen: protección de la información y construcción de confianza en las nuevas tecnologías

El artículo 11.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, en sus apartados f) y g) establece que las Fuerzas y Cuerpos de Seguridad del Estado tienen "como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana" mediante la prevención de la comisión de delitos (apartado f) y la investigación de los delitos "para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del Juez o Tribunal competente y elaborar los informes técnicos y periciales procedentes" (apartado g). De acuerdo con este artículo, a las Fuerzas y Cuerpos de Seguridad del Estado les corresponde la responsabilidad de prevenir e investigar los ciberdelitos.

Y es aquí donde radica el primer reto de las policías en su relación con las políticas de ciberseguridad: el origen de estas políticas que luego determinarían todas las políticas de gobernanza de la ciberseguridad y el cibercrimen posteriores se encuentra alejado de la concepción del cibercrimen como el fenómeno social central. En su lugar, se identifican dos narrativas fundacionales que justificaron las primeras políticas en España: en primer lugar, una narrativa con un enfoque tecnológico, que se centra principalmente en la protección de la información; en segundo lugar, la narrativa de la necesidad de generar confianza en las nuevas tecnologías. Estas narrativas fundacionales influyeron en las políticas iniciales relacionadas con la ciberseguridad y sientan las bases para el abordaje de los desafíos de la policía.

El origen del sistema de gobernanza de ciberseguridad se encuentra en tres documentos de principios del siglo XX. Por un lado, la Ley 11/2002, de 6 de mayo, que regula el Centro Nacional de Inteligencia (CNI), le encomendó funciones relacionadas con la seguridad de la información en su artículo 4.e). Esto llevó a la creación en 2004 del Centro Criptológico Nacional (CCN) (Ministerio de Defensa, 2004), cuyo ámbito de actuación incluye la protección de los sistemas de tecnologías de la información de la Administración que procesan, almacenan o transmiten información en formato electrónico, y que están sujetos a normativas de protección, incluyendo los medios de cifrado; así como la seguridad de los sistemas de tecnologías de la información que manejan información clasificada (Artículo 2.1 del Real Decreto 421/2004, de 12 de marzo, que regula el Centro Criptológico Nacional).

En los inicios de la era de la digitalización, se observa que la concepción de la ciberseguridad era más limitada y, en cierta forma, basada principalmente en aspectos técnicos en comparación con la actualidad. Concretamente, el Real Decreto 421/2004 define la "seguridad de los sistemas de información" basada en la tradicional tríada CIA (confidencialidad, integridad y disponibilidad). Por tanto, la creación del CCN, que tenía como objetivo proteger los sistemas de tecnologías de la información, inicialmente se basó en una narrativa centrada en la protección de la información, sin enfatizar en gran medida el aspecto delictivo de algunos incidentes. Su creación otorgó al servicio de inteligencia el respaldo legal y la legitimidad para asumir funciones de prevención y respuesta ante ciberincidentes.

Debido a que la ciberseguridad incluye la protección frente a daños causados tanto por errores humanos o del sistema, como por acciones maliciosas, es lógico que la narrativa inicial se centrara en el objetivo (i.e., protección de la información) y no tanto en la motivación maliciosa de la conducta – ya que solo abarcaría la mitad teórica del problema. En su lugar, se buscó una solución que pudiera integrar ambas perspectivas:

la protección ante riesgos fortuitos (p.ej., accidentes, errores, etc., lo que en inglés se conceptualiza como "*safety*") y ante actos maliciosos intencionados (p.ej., cibercrimen). A esto se une que este discurso se centró en la *información*, competencia del servicio de inteligencia (Díaz Fernández, 2005), por lo que se erigió como el organismo más adecuado para cumplir estas funciones. Esta regulación fundacional dio lugar a que se desarrollaran luego más competencias atribuidas al CCN, como la evaluación y certificación de la seguridad de las tecnologías de la información (Ministerio de la Presidencia, 2007), la respuesta a incidentes de seguridad de la información mediante el CCN-CERT (Centro Criptológico Nacional–*Computer Emergency Response Team*), y la prestación de servicios de respuesta a incidentes de seguridad a las administraciones públicas (Ministerio de Presidencia, 2010).

No obstante, de forma paralela se identifica en las políticas originarias un discurso basado en la necesidad de proteger las tecnologías de la información y las comunicaciones (TIC) para conseguir que la población confiara en estas (y, por tanto, las adoptara). Esta fue la filosofía del Plan Avanza (2006-2010) (Ministerio de Industria, Turismo y Comercio, 2005). Su objetivo principal era incrementar la digitalización en España para lograr un crecimiento económico. El Plan incluía un apartado de "e-Confianza" que justificaba desde la necesidad de incrementar la confianza en las TIC para incrementar la adopción de las TIC en la ciudadanía mediante actuaciones que abordaran su seguridad.

Como parte de este Plan, se tomó la decisión de establecer en 2006 el Instituto Nacional de Tecnologías de la Comunicación (INTECO) con tres áreas de trabajo: en primer lugar, la promoción de la concienciación sobre la seguridad de la información y el uso seguro de las redes; en segundo lugar, la mejora de la calidad del software, brindando asistencia a las empresas para desarrollar programas con altos estándares de calidad y seguridad; y finalmente, el enfoque en la accesibilidad web, con el objetivo de garantizar que los sitios web creados fueran accesibles para toda la ciudadanía, independientemente de sus discapacidades o limitaciones temporales o permanentes (Del-Real, 2022). La decisión de asignar al INTECO la responsabilidad de promover un comportamiento seguro, como un organismo independiente de otros organismos de seguridad, se tomó con el propósito de fomentar este comportamiento sin disuadir a los ciudadanos y empresas de adoptar las Tecnologías de la Información y Comunicación (TIC). De haber encomendado esta misión a la policía, es probable que los ciudadanos hubieran percibido las TIC como una innovación "peligrosa" y, por ende, su aceptación pública podría haberse visto afectada.

Ello no implica que las FCSE no tomaran medidas durante estos años para adaptarse a la ciberdelincuencia. En 1996 se creó el Grupo de Delitos Informáticos en la Guardia Civil, que en 2003 pasaría a denominarse Grupo de Delitos Telemáticos y que depende de la Unidad Central Operativa. También en 2003 se creó el Grupo de Ciberterrorismo, dependiente del Servicio de Información. Por su parte, la Policía Nacional creó en 2002 la Brigada de Investigación Tecnológica, cuyo origen se encuentra en el Grupo de Delitos Informáticos de la Brigada de Delincuencia Económica y Financiera creado en 1995. El análisis de documentos de entonces revela, no obstante, que dos detalles en las narrativas utilizadas por entonces que pueden aportar reflexiones sobre cómo se ha ido construyendo el discurso sobre el rol de la policía en la lucha contra la ciberdelincuencia. Por un lado, se observa un énfasis en la función de *investigación* de este tipo de delitos por encima de otras funciones. Por otro, el discurso se centra más en los tipos de delincuencia facilitados por el ciberespacio, principalmente los relacionados

con la pornografía infantil, fraudes y la propiedad intelectual e industrial, en la delincuencia dependiente del ciberespacio (Rivero, 2009).

Las políticas aprobadas durante los primeros años de la década de 2010 –quizás impulsadas por el Programa de Estocolmo (European Council, 2010)– continúan el proceso de desarrollo de la ciberseguridad como área política a través de nuevas ideas, normativas e instrumentos que se basaban en los existentes. El análisis de estos documentos desvela una clara dependencia histórica (del camino) justificada por este doble discurso de necesidad de proteger la información y aumentar la confianza pública, donde el discurso centrado en el rol de la policía queda diluido. A esta la estructura incipiente, donde se habían establecido las bases de la gobernanza, llegó la ratificación del Convenio sobre la Ciberdelincuencia (Jefatura de Estado, 2010), aprobado en Budapest nueve años antes. La estructura básica del sistema de gobernanza ya se había establecido: por un lado, nuevas unidades policiales especializadas en investigación de la ciberdelincuencia; por otro, dos nuevos organismos con competencias específicas en la seguridad de la información.

Consolidación: gobernanza pública y privada

La consolidación del modelo de gobernanza de ciberseguridad y cibercrimen en España comenzó en 2013 con la publicación de la primera Estrategia de Ciberseguridad Nacional (Departamento de Seguridad Nacional, 2013). Esta estrategia supuso el instrumento oficial por el cual apareció la ciberseguridad como área política en España. La Estrategia definía diferentes riesgos y amenazas a la ciberseguridad nacional, y urgía a la necesidad de desarrollar acciones de prevención, defensa, detección, respuesta y recuperación frente a ciberamenazas. En esta Estrategia se identifican elementos del discurso adoptado por la Agenda Digital para Europa (European Commission, 2010), en el cual el cibercrimen no es la única amenaza a la actividad económica de la Unión (en el caso de la Estrategia, a la seguridad nacional), sino que también puede ser causado por actores con intereses geopolíticos, o bien por fallos humanos y del sistema (Carrapico & Farrand, 2020). Por tanto, España decidió seguir el ejemplo europeo y apostar por un enfoque basado en la ciberseguridad más que en el cibercrimen.

La Estrategia de Ciberseguridad Nacional incorporaba el reforzamiento de organismos existentes como el CCN-CERT, a los que instaba a mejorar sus Sistemas de Detección y Alerta Temprana (lo que le permite monitorear las redes de las administraciones públicas), el CERT las Fuerzas Armadas (del Mando Conjunto de Ciberdefensa), y el CERT de "seguridad e industria", que terminaría siendo el de INTECO. Paralelamente, en 2013 INTECO se desprende de los ejes de calidad del software y accesibilidad web para centrarse en la ciberseguridad, por lo que es renombrado como Instituto Nacional de Ciberseguridad (INCIBE) (Hernández Moreno, 2018).

En este documento es evidente el marco ideológico subyacente de estos organismos públicos como los actores bisagras de la colaboración público-privada y la implicación de los ciudadanos como la vía para mejorar la ciberseguridad. Este documento supone entonces una continuidad histórica e ideacional en las políticas de ciberseguridad de España, ya que trabaja con estructuras institucionales existentes a las que expande sus actuaciones. Esta tendencia se observa en diversas políticas posteriores (Ministerio de Hacienda y Administraciones Públicas, 2016a, 2016b; Ministerio de Hacienda y Función Pública, 2018a, 2018b). Y, aunque el documento incluye una línea de acción

enfocada a mejorar las capacidades de investigación y persecución del ciberterrorismo y la ciberdelincuencia, no menciona específicamente a las FCSE.

Ruptura ideológica: nueva concepción de la ciberseguridad

El inicio de la fase de ruptura ideológica se dio con la promulgación de la Estrategia de Seguridad Nacional de 2017, que representó "un punto de inflexión en el pensamiento estratégico nacional, otorgando un espacio propio y diferencial a la ciberseguridad" (Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad, 2019). Paralelamente a lo ocurrido en las políticas de la Unión Europea (Carrapico & Farrand, 2020), en España también se produjo un cambio ideológico al entender la ciberseguridad no solo como la protección del patrimonio tecnológico, sino como un ámbito en el que operan actividades económicas, políticas, sociales y diplomáticas con la capacidad de desestabilizar a los Estados. Esta perspectiva queda claramente plasmada en la Estrategia Nacional de Ciberseguridad de 2019, donde se concibe el ciberespacio como un medio de comunicación estratégica capaz de ser utilizado para influir en la opinión pública.

Otro elemento de ruptura ideacional en la nueva Estrategia es la concepción del ciberespacio como una dimensión "fundamental para la estabilidad, la preservación de la defensa de los valores y principios constitucionales y democráticos, así como los derechos fundamentales de los ciudadanos en el ciberespacio" (Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad, 2019: 43441). Aunque este nuevo énfasis en los derechos fundamentales y los principios democráticos marca una ruptura ideológica a nivel discursivo, las soluciones propuestas, en realidad, refuerzan el sistema de gobernanza existente. Esto incluye el fortalecimiento de las competencias del CCN mediante el impulso de las capacidades de ciber-inteligencia (que también puede observarse en Jefatura del Estado, 2019), la estructura de las Fuerzas Armadas para incorporar unidades especializadas en la ciberdefensa (que posteriormente sería el Mando Conjunto del Ciberespacio, MCCE) (Ministerio de Defensa, 2020a, 2020b), y las competencias del INCIBE como el organismo adecuado para fomentar la concienciación en ciberseguridad en el sector privado y la industria de ciberseguridad, con la aspiración de alcanzar autonomía tecnológica[10].

Relacionado con lo anterior, en esta Estrategia se evidencia un cambio ideológico en el enfoque de la seguridad de los sistemas de información hacia la prevención y respuesta ante ciberamenazas. A pesar de este giro hacia una perspectiva más centrada en la seguridad nacional y pública, la función de las FCSE se limita únicamente a la Línea de Acción 3, "Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio". En este punto, se observa nuevamente la continuidad ideológica del discurso enfocado en la actividad policial centrada en la investigación de ciberdelitos, pero excluyendo la prevención, detección y (parte de la) respuesta.

[10] No obstante, esto no ha sido impedimento para que, por ejemplo, el Cuerpo Nacional de Policía desarrolle su propio proyecto de formación, concienciación y desarrollo de capacidades de ciberseguridad denominado "proyecto C1b3rWall" (https://c1b3rwall.policia.es/), entre otros proyectos (Del-Real, 2022).

Adaptación a la pandemia de Covid-19: continuidad y ruptura de las tendencias existentes

En esta última etapa, se argumenta que la pandemia de Covid-19 ha sido un momento crítico que ha continuado y acelerado tendencias preexistentes, fortaleciendo la dependencia de las ideas previas, pero también ha producido algunos cambios en el discurso. Antes de la declaración del Estado de Alarma, solo el 7,3% de los trabajadores españoles realizaba teletrabajo a diario, mientras que un 5,3% lo hacía varias veces a la semana y un 4,6%, varias veces al mes. Durante la pandemia, esta cifra aumentó significativamente hasta el 31,7% (Observatorio Nacional de Tecnología y Sociedad, 2022). Este incremento del teletrabajo vino acompañado de un aumento del cibercrimen, dado que se incrementó el tiempo de uso de las tecnologías digitales y se trasladaron nuestras actividades cotidianas al ciberespacio (Buil-Gil et al., 2021). También se observaron campañas de desinformación relacionadas con la existencia del virus (Loomba et al., 2021). No solo los ciudadanos y las empresas experimentaron un aumento de ciber-victimizaciones, sino que incluso en 2021, el Ministerio de Trabajo fue víctima de un ciberataque, lo que supuso otro momento crítico para las políticas de ciberseguridad (Jiménez, 2021).

A partir de 2020, el Gobierno de España promulgó numerosas leyes, normativas y planes estratégicos (como se puede observar en la Figura 1) debido en parte a las necesidades de ciberseguridad surgidas a raíz de la rápida digitalización de la sociedad provocada por la pandemia de Covid-19. Algunas de estas nuevas normativas continuaron siendo herederas de instrumentos preexistentes, como el Real Decreto 43/2021, de 26 de enero, que desarrolló el Real Decreto-ley 12/2018, de 7 de septiembre, sobre seguridad de las redes y sistemas de información (Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática, 2021). Este Real Decreto consolidó el modelo dual de respuesta a ciberincidentes, en el cual el CCN-CERT se encargaba de los ciberincidentes que afectaban a las administraciones públicas y apoyaba al ESPDEF-CERT en caso de que el ciberincidente afectara al Ministerio de Defensa o a las operaciones de las Fuerzas Armadas, mientras que el INCIBE-CERT se ocupaba de los ciberincidentes que afectaban a empresas privadas y particulares, coordinados mediante la Oficina de Coordinación de Ciberseguridad con las Unidades de la Policía Judicial.

Sin embargo, otros instrumentos surgieron expresamente como respuesta a la pandemia, como el programa España Digital 2025 (Ministerio de Asuntos Económicos y Transformación Digital, 2020) y su revisión posterior (Gobierno de España, 2022), el Plan de Recuperación, Transformación y Resiliencia (Ministerio de Hacienda y Función Pública, 2021), el Plan de Choque de Ciberseguridad (Ministerio de Asuntos Económicos y Transformación Digital, 2021), la Estrategia de Seguridad Nacional 2021 (Presidencia del Gobierno, 2021), la revisión del Esquema Nacional de Seguridad (Ministerio de Asuntos Económicos y Transformación Digital, 2022), el Plan Estratégico contra la Cibercriminalidad (2021) y el Plan Nacional de Ciberseguridad (2022)[11].

Como se mencionaba al inicio de este sub-apartado, se identifican tanto continuidades como evoluciones en las políticas de ciberseguridad a partir de 2020. En primer lugar, persiste la narrativa de aumentar la confianza ciudadana en el uso de las

[11] A estos dos últimos la autora no ha tenido acceso porque son documentos clasificados.

tecnologías, se consolida aún más el papel del CCN con el futuro Centro de Operaciones de Ciberseguridad de la Administración General del Estado, se refuerza la idea de lograr un ecosistema empresarial de ciberseguridad y de aumentar la formación y capacitación en ciberseguridad de ciudadanos y empresas a través de INCIBE, y se reitera la importancia de que la ciberseguridad sea un esfuerzo conjunto entre actores públicos y privados. No obstante, apenas se observan esfuerzos por integrar a las FCSE en este modelo más allá de fomentar la cooperación de los organismos principales con estas en su misión de investigar ciberdelitos.

Sin embargo, el discurso sobre la ciberseguridad experimenta durante estos años un giro humanista, que encuentra su origen en la ruptura discursiva de la fase anterior, al centrarse en los derechos fundamentales de los ciudadanos. Este discurso, ya presente en el programa España Digital 2025, se consolida, especialmente en su revisión España Digital 2026:

> (…) el acceso general y asequible de personas y empresas a las nuevas herramientas digitales, su preparación para su uso y aprovechamiento, la formación en capacidades que les permitan conducirse en los entornos digitales y discernir la calidad de los múltiples contenidos que se alojan en ellos, la pérdida de la privacidad o el riesgo al que se exponen la protección de los derechos individuales y colectivos de las personas en el entorno online.
>
> **Junto a avances y soluciones técnicas revolucionarias, la digitalización genera también nuevas problemáticas y conflictos, pudiendo llegar a erosionar incluso derechos fundamentales**. No podemos permitir que la disrupción tecnológica origine nuevas brechas ni que suponga retrocesos en nuestro estado de derecho.
>
> **Por ello, este proceso de transformación digital debe ser humanista e inclusivo, poniendo a la persona en el centro**, para no dejar a nadie atrás y para garantizar los principios, valores y derechos que representan a la sociedad que hemos construido. (Gobierno de España, 2022: 21)

Esta nueva concepción de la ciberseguridad, que parece estar afianzándose en las políticas más recientes, se basa en la "seguridad de la vida digital" y plantea la necesidad de avanzar en la integración del modelo de gobernanza de la ciberseguridad. Esta situación podría representar una oportunidad propicia para llevar a cabo acciones dirigidas a lograr un modelo de gobernanza más integrado y coordinado con las actuaciones de las FCSE.

CONCLUSIONES

A través del marco conceptual del institucionalismo histórico y discursivo, este estudio ha identificado elementos clave en las políticas de ciberseguridad que han generado dependencias del camino. El artículo ofrece una nueva perspectiva, argumentando que la posición actual de la policía en la gobernanza de la ciberseguridad en España está influenciada por el desarrollo histórico y discursivo de estas políticas. La investigación se basa en documentos normativos y políticos. No obstante, es importante destacar las limitaciones de este estudio. En primer lugar, al basarse en documentos oficiales, no ha sido posible captar el proceso de toma de decisiones, por lo que no se pueden extraer conclusiones sobre el porqué de los discursos y decisiones políticas. De hecho, como se argumenta arriba, la ciberseguridad es más amplia que la cibercriminalidad. Este artículo no trata de criticar las decisiones adoptadas por España, sino ofrecer una perspectiva más amplia para comprender los retos actuales de la policía en la lucha contra el cibercrimen. En segundo lugar, se trata de un estudio de tipo argumentativo,

pero no proporciona evidencias reproducibles para respaldar sus argumentos. Por lo tanto, futuras investigaciones en España deberían utilizar este estudio, así como otros relacionados, para recopilar datos primarios (por ejemplo, mediante encuestas a las fuerzas policiales o entrevistas en profundidad) sobre los desafíos que enfrenta la policía en España y la importancia relativa de cada uno de los factores mencionados en este artículo.

La investigación ha demostrado que la policía se enfrenta a muchas dificultades organizativas para adaptarse a la lucha contra el cibercrimen. A ellas se suman desafíos históricos y narrativos que han centrado la atención de las políticas en la seguridad de la información y la confianza de la sociedad en las tecnologías, relegando al segundo plano la lucha contra el cibercrimen. En consonancia con estas narrativas, se han creado organismos independientes de las FCSE que, en los últimos 15 años, han asumido cada vez más competencias en prevención, monitoreo, detección y respuesta ante ciber incidentes maliciosos. No obstante, este artículo identifica momentos críticos que han generado ligeros cambios narrativos –aunque aún no se han materializado en acciones concretas– y que se traducen en una concepción de la ciberseguridad que se aleja de la mera protección de la información, sistemas y redes, para adoptar una visión más humanista, centrada en el ciudadano y sus derechos como eje central de las políticas. Este último cambio ideológico podría brindar oportunidades para justificar futuras actuaciones encaminadas hacia una mayor integración de las funciones de ciberseguridad, como la creación de un cuerpo policial especializado en el ciberespacio. Como sostiene este artículo, la consecución de esta integración dependerá, en cierta medida, del peso de la historia.

NOTA SOBRE LA AUTORA:

Cristina Del-Real es Assistant Professor de gobernanza de ciber crisis en el Institute of Security and Global Affairs de la Universidad de Leiden (La Haya, Países Bajos) e investigadora asociada al The Hague Program on International Cyber Security. Imparte docencia en el MSc Crisis and Security Management y el Executive Master Cyber Security de la Universidad de Leiden sobre gestión de ciber incidentes y crisis. Su investigación aborda políticas y prácticas de ciberseguridad en organizaciones públicas y privadas. Correo electrónico: c.del.real@fgga.leidenuniv.nl

REFERENCIAS

Baćak, Valerio & Apel, Robert (2020), "Police Fairness and Legitimacy across the Post-Communist Divide in Europe", *Law & Society Review*, Vol. 55, No. 3, pp. 473–95. https://doi.org/10.1111/lasr.12570.

Bidgoli, Morvareed (2015), *A Mixed Methods Approach to Understanding Undergraduate Students' Victimization, Perceptions, and Reporting of Cybercrimes*, Trabajo de Fin de Máster. Universidad de California Irvine. http://search.proquest.com/docview/1711749029?accountid=14509.

Bossler, Adam M. & Holt, Thomas J. (2012), "'Patrol Officers' Perceived Role in Responding to Cybercrime", *Policing: An International Journal of Police Strategies & Management*, Vol. 35, No. 1, pp. 165–81. https://doi.org/10.1108/13639511211215504.

Bossong, Raphael & Wagner, Ben (2017), "A Typology of Cybersecurity and Public-Private Partnerships in the Context of the EU", *Crime, Law and Social Change*, Vol. 67, No. 3, pp. 265–88. https://doi.org/10.1007/s10611-016-9653-3.

Brenner, Susan W. (2006), "Cybercrime Jurisdiction", *Crime, Law and Social Change*, Vol. 46, No. 4–5, pp. 189–206. https://doi.org/10.1007/s10611-007-9063-7.

Broeders, Dennis (2021), "Private Active Cyber Defense and (International) Cyber Security—Pushing the Line?", *Journal of Cybersecurity*, Vol. 7, No. 1, tyab010. https://doi.org/10.1093/cybsec/tyab010.

Buil-Gil, David; Miró-Llinares, Fernando; Moneva, Asier; Kemp, Steven & Díaz-Castaño, Nacho (2021), "Cybercrime and Shifts in Opportunities during COVID-19: A Preliminary Analysis in the UK", *European Societies*, Vol. 23, No. sup1, pp. S47–59. https://doi.org/10.1080/14616696.2020.1804973.

Buil-Gil, David & Saldaña-Taboada, Patricia (2022), "Offending Concentration on the Internet: An Exploratory Analysis of Bitcoin-Related Cybercrime", *Deviant Behavior*, Vol. 43, No. 12, pp. 1453–70. https://doi.org/10.1080/01639625.2021.1988760.

Burgard, Anna & Schlembach, Christopher (2013), "Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet", *International Journal of Cyber Criminology*, Vol. 7, No. 2, pp. 112–24.

Burns, Ronald G.; Whitworth, Keith H. & Thompson, Carol Y. (2004), "Assessing Law Enforcement Preparedness to Address Internet Fraud", *Journal of Criminal Justice*, Vol. 32, No 5, pp. 477–93. https://doi.org/10.1016/j.jcrimjus.2004.06.008.

Burruss, George; Howell, Christian Jordan; Bossler, Adam & Holt, Thomas J. (2019), "Self-Perceptions of English and Welsh Constables and Sergeants Preparedness for Online Crime: A Latent Class Analysis", *Policing: An International Journal*, Vol. 43, No. 1, pp. 105–19. https://doi.org/10.1108/PIJPSM-08-2019-0142.

Button, Mark (2020), "The "New" Private Security Industry, the Private Policing of Cyberspace and the Regulatory Questions", *Journal of Contemporary Criminal Justice*, Vol. 36, No. 1, pp. 39–55. https://doi.org/10.1177/1043986219890194.

Carrapico, Helena & Farrand, Benjamin (2020), "Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy", *Journal of European Integration*, Vol. 42, No. 8, pp. 1111–26. https://doi.org/10.1080/07036337.2020.1853122.

Coleman, Clive & Moynihan, Jenny (1996), *Understanding Crime Data: Haunted by the Dark Figure*, Crime and Justice. Buckingham; Philadelphia: Open University Press.

Cross, Charlotte (2019), "Cybercrime and the Policing of Politics in Tanzania", en Dwyer, Maggie & Molony, Thomas (Eds.), *Social Media and Politics in Africa: Democracy, Censorship and Security*, Zed Books.

Cruz Lobato, Luísa (2017), "La Política Brasileña de Ciberseguridad Como Estrategia de Liderazgo Regional [The Brazilian Cybersecurity Policy as a Strategy of Regional Leadership]", *URVIO - Revista Latinoamericana de Estudios de Seguridad*, No. 20 (June), 16. https://doi.org/10.17141/urvio.20.2017.2576.

De Paoli, Stefano; Johnstone, Jason; Coull, Natalie; Ferguson, Ian; Sinclair, Georgina; Tomkins, Patrick; Brown, Maureen & Martin, Rebecca (2021), "A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the

Perspective of Police Cybercrime Specialists", *Policing: A Journal of Policy and Practice*, Vol. 15, No. 2, pp. 1429–45. https://doi.org/10.1093/police/paaa027.

Del-Real, Cristina (2022), "Panorama institucional de la gobernanza de la ciberseguridad en España", *Revista de Estudios Jurídicos y Criminológicos*, No. 6, pp. 15-51. https://doi.org/10.25267/REJUCRIM.2022.i6.03.

Del-Real, Cristina & Díaz-Fernández, Antonio M. (2022), "Understanding the Plural Landscape of Cybersecurity Governance in Spain: A Matter of Capital Exchange", *International Cybersecurity Law Review*, Vol. 3, No. 2, pp. 313–43. https://doi.org/10.1365/s43439-022-00069-4.

Departamento de Seguridad Nacional (2013), "Estrategia de Ciberseguridad Nacional", https://www.dsn.gob.es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional.

Díaz Fernández, Antonio M. (2005), *Los Servicios de Inteligencia Españoles: Desde la Guerra Civil Hasta El 11-M: Historia de Una Transición*, Madrid: Alianza Editorial.

Domenie, Miranda M. L.; Leukfeldt, Rutger; Wilsem, Johan van; Jansen, Jurjen & Stol, Wouter (2013), *Victimisation in a Digitised Society: A Survey among Members of the Public Concerning e-Fraud, Hacking and Other High Volume Crimes*, Safety & Security Studies, The Hague: Eleven International Publishing.

Dupont, Benoît (2017), "Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime", *Crime, Law and Social Change*, Vol. 67, No. 1, pp. 97–116. https://doi.org/10.1007/s10611-016-9649-z.

European Commission (2010), "A Digital Agenda for Europe", EUR-Lex.

— (2013), "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Brussels: European Commission.

European Council (2010), *The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens*. *Official Journal of the European Union*. Vol. 2010/C 115/01.

Gobierno de España (2022), "España Digital 2026".

Gordon, Sarah & Ford, Richard (2006), "On the Definition and Classification of Cybercrime", *Journal in Computer Virology*, Vol. 2, No. 1, pp. 13–20. https://doi.org/10.1007/s11416-006-0015-z.

Hadlington, Lee; Lumsden, Karen; Black, Alexandra & Ferra, Fenia (2021), "A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime", *Policing: A Journal of Policy and Practice*, Vol. 15, No. 1, pp. 34–43. https://doi.org/10.1093/police/pay090.

Harkin, Diarmaid & Whelan, Chad (2022), "Perceptions of Police Training Needs in Cyber-Crime", *International Journal of Police Science & Management*, Vol. 24, No. 1, pp. 66–76. https://doi.org/10.1177/14613557211036565.

Harkin, Diarmaid; Whelan, Chad & Chang, Lennon (2018), "The Challenges Facing Specialist Police Cyber-Crime Units: An Empirical Analysis", *Police Practice and Research*, Vol. 19, No. 6, pp. 519–36. https://doi.org/10.1080/15614263.2018.1507889.

Hernández Moreno, Alberto (2018), "De INTECO a INCIBE: Un proceso de transformación para el fortalecimiento de la ciberseguridad de los ciudadanos y empresas en España", *Economía Industrial*, No. 410, pp. 71–80.

Hinduja, Sameer (2004), "Perceptions of Local and State Law Enforcement Concerning the Role of Computer Crime Investigative Teams", *Policing: An International Journal of Police Strategies & Management*, Vol. 27, No. 3, pp. 341–57. https://doi.org/10.1108/13639510410553103.

Holt, Thomas J. (2018), "Regulating Cybercrime through Law Enforcement and Industry Mechanisms", *The ANNALS of the American Academy of Political and Social Science*, Vol. 679, No. 1, pp. 140–57. https://doi.org/10.1177/0002716218783679.

Holt, Thomas J. & Bossler, Adam M. (2012), "Police Perceptions of Computer Crimes in Two Southeastern Cities: An Examination from the Viewpoint of Patrol Officers", *American Journal of Criminal Justice*, Vol. 37, No. 3, pp. 396–412. https://doi.org/10.1007/s12103-011-9131-5.

Holt, Thomas J.; Burruss, George W. & Bossler, Adam M. (2018), "An Examination of English and Welsh Constables' Perceptions of the Seriousness and Frequency of Online Incidents", *Policing and Society*, Vol. 29, No. 8, pp. 906–21. https://doi.org/10.1080/10439463.2018.1450409.

Jaime Jiménez, Oscar y Torrente, Diego (2017), "Los desafíos de la policía como actor político en España", *Revista Española de Ciencia Política*, No. 45, pp. 147–72.

Jefatura de Estado (2010), *Instrumento de Ratificación Del Convenio Sobre La Ciberdelincuencia, Hecho En Budapest El 23 de Noviembre de 2001*. *Boletín Oficial Del Estado*. Vol. 226.

Jefatura del Estado (2019), *Real Decreto-Ley 14/2019, de 31 de Octubre, por el que se adoptan medidas urgentes por razones de Seguridad Pública en materia de Administración Digital, Contratación del Sector Público y Telecomunicaciones*. *Boletín Oficial Del Estado*. Vol. 266.

Jiménez, Marimar (2021), "El Ministerio de Trabajo Sufre Un Ciberataque, Tres Meses Después de Ser 'hackeado' El SEPE", *El País*, 6 de septiembre.

Kuerbis, Brenden & Badiei, Farzaneh (2017), "Mapping the Cybersecurity Institutional Landscape", *Digital Policy, Regulation and Governance*, Vol. 19, No. 6, pp. 466–92. https://doi.org/10.1108/DPRG-05-2017-0024.

Lab, Steven P. (2016), *Crime Prevention: Approaches, Practices, and Evaluations*, Ninth Edition. New York; London: Routledge Taylor & Francis Group.

Lau, Raymond W.K. (2004), "History as Obstacle to Change: A Neo-Institutionalist Analysis of Police Reform in Hong Kong", *International Journal of the Sociology of Law*, Vol. 32, No. 1, pp. 1–15. https://doi.org/10.1016/j.ijsl.2004.03.001.

Lee, Jin R.; Holt, Thomas J.; Burruss, George W. & Bossler, Adam M. (2019), "Examining English and Welsh Detectives' Views of Online Crime", *International Criminal Justice Review*, Vol. 31, No. 1, pp. 20-39. https://doi.org/10.1177/1057567719846224.

Leukfeldt, E. Rutger & Holt, Thomas J. (2020), *The Human Factor of Cybercrime*, Abingdon, Oxon; New York, NY: Routledge.

Leukfeldt, E. Rutger; Veenstra, Sander & Stol, Wouter (2013), "High Volume Cyber Crime and the Organization of the Police: The Results of Two Empirical Studies in the Netherlands", *International Journal of Cyber Criminology*, Vol. 7, No. 1, pp. 1–17.

Loomba, Sahil; De Figueiredo, Alexandre; Piatek, Simon J.; De Graaf, Kristen & Larson, Heidi J. (2021), "Measuring the Impact of COVID-19 Vaccine Misinformation on Vaccination Intent in the UK and USA", *Nature Human Behaviour*, Vol. 5, No. 3, pp. 337–48. https://doi.org/10.1038/s41562-021-01056-1.

McGuire, Mike (2020), "It Ain't What It Is, It's the Way That They Do It? Why We Still Don't Understand Cybercrime", en Leukfeldt, Rutger & Holt, Thomas J. (Eds.), *The Human Factor of Cybercrime*, 1st ed., Routledge Studies in Crime and Society, Oxon: Routledge, pp. 3–28.

McGuire, Mike & Dowling, Samantha (2013a), "Chapter 1: Cyber-Dependent Crimes", Research report 75. *Cyber Crime: A Review of the Evidence*. Home Office.

— (2013b), "Chapter 2: Cyber-Enabled Crimes -Fraud and Theft", *Research report 75. Cyber Crime: A Review of the Evidence*. Home Office.

— (2013c), "Chapter 3: Cyber-Enabled Crimes - Sexual Offending against Children", *Research report 75. Cyber Crime: A Review of the Evidence*. Home Office.

McQuade, Samuel C. (2006), *Understanding and Managing Cybercrime*, Boston: Pearson/Allyn and Bacon.

Medeiros Passos, Anaís (2015), "Continuity in Mexico's Security Police and Historical Institutionalism", Science Po.

Ministerio de Asuntos Económicos y Transformación Digital (2020), "España Digital 2025", Gobierno de España.

— (2021), "El Gobierno aprueba el 'Plan de Choque de Ciberseguridad' en el marco de un nuevo paquete de medidas ante las ciberamenazas", *Gobierno de España*, 25 May 2021.

— (2022), *Real Decreto 311/2022, de 3 de Mayo, por el que se regula el Esquema Nacional de Seguridad*. *Boletín Oficial Del Estado*. Vol. 106.

Ministerio de Defensa (2004), *Real Decreto 421/2004, de 12 de Marzo, por el que se regula el Centro Criptológico Nacional*. *Boletín Oficial Del Estado*. Vol. 68.

— (2020a), *Real Decreto 521/2020, de 19 de Mayo, por el que se establece la organización básica de las Fuerzas Armadas*. *Boletín Oficial Del Estado*. Vol. 143.

— (2020b), *Orden DEF/710/2020, de 27 de Julio, por la que se desarrolla la organización básica del Estado Mayor de La Defensa*. *Boletín Oficial del Estado*. Vol. 204.

Ministerio de Hacienda y Función Pública (2021), "Plan de Recuperación, Transformación y Resiliencia".

Ministerio de Hacienda y Administraciones Públicas (2016a), *Resolución de 7 de Octubre de 2016, de La Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad*. *Boletín Oficial Del Estado*. Vol. 265.

— (2016b), *Resolución de 13 de Octubre de 2016, de La Secretaría de Estado de Administraciones Públicas, por la que se aprueba la instrucción técnica de seguridad*

de conformidad con el Esquema Nacional de Seguridad. *Boletín Oficial del Estado*. Vol. 265.

Ministerio de Hacienda y Función Pública (2018a), *Resolución de 27 de Marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información*. *Boletín Oficial Del Estado*. Vol. 81.

— (2018b), *Resolución de 13 de Abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad*. *Boletín Oficial Del Estado*. Vol. 95.

Ministerio de Industria, Turismo y Comercio (2005), "Plan Avanza: Plan 2006-2010 para el desarrollo de la Sociedad de la Información y de Convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas", Gobierno de España.

Ministerio de la Presidencia (2007), *Orden PRE/2740/2007, de 19 de Septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Boletín Oficial Del Estado*. Vol. 230.

Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad (2019), *Orden PCI/487/2019, de 26 de Abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, Aprobada por el Consejo de Seguridad Nacional*. *Boletín Oficial Del Estado*. Vol. 103.

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática (2021), *Real Decreto 43/2021, de 26 de Enero, por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de Septiembre, de Seguridad de las Redes y Sistemas de Información*. *Boletín Oficial Del Estado*. Vol. 24.

Ministerio de Presidencia (2010), *Real Decreto 3/2010, de 8 de Enero, por el que se regula el Esquema Nacional de Seguridad en el Ámbito de la Administración Electrónica. Boletín Oficial del Estado*. Vol. 25.

Moneva, Asier; Leukfeldt, E. Rutger; Weijer, Steve G.A. (van de) & Miró-Llinares, Fernando (2022), "Repeat Victimization by Website Defacement: An Empirical Test of Premises from an Environmental Criminology Perspective", *Computers in Human Behavior*, Vol. 126 (January), 106984. https://doi.org/10.1016/j.chb.2021.106984.

Nhan, Johnny & Huey, Laura (2008), "Policing through Nodes, Clusters and Bandwidth: The Role of Network Relations in the Prevention of and Response to Cyber-Crimes", en Leman-Langlois, Stéphane (Ed.), *Technocrime: Technology, Crime and Social Control*, Portland: OR: Willan Publishing, pp. 66–87.

Observatorio Nacional de Tecnología y Sociedad (2022), "El Teletrabajo en España: Antes, Durante y Después de la Pandemia", Madrid, España: Ministerio de Asuntos Económicos y Transformación Digital.

Paek, Seung Yeop; Nalla, Mahesh K. & Lee, Julak (2020), "Determinants of Police Officers' Support for the Public-Private Partnerships (PPPs) in Policing Cyberspace", *Policing: An International Journal*, Vol. 43, No. 5, pp. 877-892.

Peters, B. Guy (2019), *Institutional Theory in Political Science: The New Institutionalism*, Fourth edition, Northampton, MA: Edward Elgar Pub.

Presidencia del Gobierno (2021), *Real Decreto 1150/2021, de 28 de Diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021*. *Boletín Oficial Del Estado*. Vol. 314.

Rivero, Jesús (2009), "Actualmente La Brigada de Investigación Tecnológica está en la vanguardia internacional en la lucha contra la ciberdelincuencia", *Revista A+*.

Schmidt, Vivien A. (2008), "Discursive Institutionalism: The Explanatory Power of Ideas and Discourse", *Annual Review of Political Science*, Vol. 11, No. 1, pp. 303–26. https://doi.org/10.1146/annurev.polisci.11.060606.135342.

— (2011), "Reconciling Ideas and Institutions through Discursive Institutionalism", en Beland, Daniel & Cox, Robert H. (Eds.), *Ideas and Politics in Social Science Research*, Oxford: Oxford University Press, pp. 76–95.

Senjo, Scott R (2004), "An Analysis of Computer-Related Crime: Comparing Police Officer Perceptions with Empirical Data", *Security Journal*, Vol. 17, No. 2, pp. 55–71. https://doi.org/10.1057/palgrave.sj.8340168.

Skocpol, Theda (1979), *States and Social Revolutions: A Comparative Analysis of France, Russia and China*. 1st ed., Cambridge University Press. https://doi.org/10.1017/CBO9780511815805.

Wall, David S. (2007), "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace", *Police Practice and Research*, Vol. 8, No. 2, pp. 183–205. https://doi.org/10.1080/15614260701377729.

Weijer, Steve G.A. van de; Leukfeldt, Rutger & Bernasco, Wim (2019), "Determinants of Reporting Cybercrime: A Comparison between Identity Theft, Consumer Fraud, and Hacking", *European Journal of Criminology*, Vol. 16, No. 4, pp. 486–508. https://doi.org/10.1177/1477370818773610.

Weisburd, David & Braga, Anthony Allan (2019), *Police Innovation: Contrasting Perspectives*, Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press.

Wilson, Michael; Cross, Cassandra; Holt, Thomas & Powell, Anastasia (2022), "Police Preparedness to Respond to Cybercrime in Australia: An Analysis of Individual and Organizational Capabilities", *Journal of Criminology*, Vol. 55, No. 4, pp. 468–94. https://doi.org/10.1177/26338076221123080.