

Cibercriminología y Tecnocriminología:

El lugar donde sí hay trabajo

Prof. Dr. Abel González García
Universidad a Distancia de Madrid (UDIMA)
II Congreso de Criminología de la Comunidad de Madrid,
Universidad Complutense, 14 de noviembre de 2024

1. Introducción: Nuevos horizontes para la Criminología aplicada

En el contexto actual de acelerada transformación tecnológica, las disciplinas criminológicas enfrentan el desafío de redefinir sus ámbitos de estudio, intervención y aplicabilidad profesional. La consolidación de una sociedad digital, interconectada y basada en la automatización de procesos sociales, productivos y comunicacionales, ha generado nuevas formas de conflicto, vulnerabilidad, victimización y criminalidad que exceden los marcos tradicionales de análisis. En este escenario, emergen con fuerza dos campos complementarios: la cibercriminología y la tecnocriminología, cuya relevancia práctica y teórica está en plena expansión.

La presente contribución se inscribe en el marco del II Congreso de Criminología de la Comunidad de Madrid, celebrado en la Universidad Complutense el 14 de noviembre de 2024. En ella se propone una reflexión técnico-profesional orientada a explorar el posicionamiento estratégico de la Criminología frente al fenómeno digital y su impacto en los nuevos perfiles de intervención. Lejos de constituir una amenaza para la disciplina, la digitalización de la vida social representa una oportunidad para reforzar su utilidad aplicada, su presencia institucional y su potencial de empleabilidad.

La tesis central que articula este trabajo puede sintetizarse así: la Criminología, si asume con rigor los retos que plantean el ciberespacio y las tecnologías emergentes, dispone de un amplio campo de trabajo en expansión. No se trata solo de comprender nuevas tipologías delictivas, sino de intervenir proactivamente en los sistemas de seguridad, evaluación de riesgos, prevención situacional, formación digital ciudadana y auditoría ética de sistemas automatizados. Desde esta perspectiva, la pregunta “¿hay trabajo para la Criminología?” encuentra una respuesta afirmativa en la medida en que se despliega una criminología tecnológicamente competente y socialmente comprometida.

La noción de “horizonte profesional” remite no solo a salidas laborales tradicionales, sino también a nuevas funciones de asesoramiento, análisis, evaluación e innovación en escenarios como la ciberseguridad, la inteligencia artificial, la gestión de datos personales, los sistemas de justicia digital, la protección de menores online o la prevención de la radicalización digital. La Criminología aplicada tiene la capacidad para articularse con equipos multidisciplinares en estos contextos, aportando una mirada experta sobre la conducta humana en entornos virtuales y la gobernanza ética de tecnologías disruptivas.

El campo de la cibercriminología se ha venido consolidando en las últimas dos décadas como un ámbito autónomo de estudio y aplicación. Su objeto de análisis se focaliza en la

conducta delictiva y desviada en entornos digitales, considerando las dimensiones técnicas, psicológicas, sociales y jurídicas involucradas. A diferencia de un enfoque exclusivamente jurídico o informático, la cibercriminología aporta una comprensión holística del comportamiento en red, prestando atención a variables como el anonimato, la identidad digital, la socialización virtual, la oportunidad situacional y la cultura de la transgresión tecnológica.

Por su parte, la tecnocriminología representa una ampliación conceptual que no se limita a los delitos informáticos, sino que examina críticamente el impacto criminógeno de las tecnologías emergentes en distintos planos de la vida social: desde la aplicación de algoritmos en decisiones judiciales hasta el uso de drones en el control fronterizo, pasando por los riesgos éticos de la inteligencia artificial en entornos laborales, policiales o penitenciarios. La tecnocriminología se vincula así con una perspectiva de evaluación crítica de la tecnología como factor de riesgo, control o desigualdad.

Ambos campos comparten una preocupación por el análisis del nuevo entorno sociotécnico bajo una perspectiva criminológica aplicada. Esto implica no solo describir los fenómenos, sino intervenir sobre ellos mediante diseño de políticas públicas, asesoramiento institucional, generación de evidencia empírica, diseño de programas preventivos y desarrollo de marcos regulatorios adaptados al nuevo ecosistema digital.

En este sentido, la formación del criminólogo del siglo XXI debe contemplar competencias vinculadas al análisis de riesgos tecnológicos, la comprensión de estructuras delictivas digitales, la ética algorítmica, el análisis forense digital, el conocimiento de sistemas de inteligencia artificial y la capacidad de diálogo con profesionales del derecho, la informática, la ingeniería y las ciencias sociales. Esta transversalidad metodológica y epistémica no debilita la identidad criminológica, sino que la potencia como disciplina estratégica en la gobernanza de sociedades digitalizadas.

La consolidación del campo también exige una mayor presencia institucional de la Criminología en espacios de toma de decisiones públicas y privadas sobre seguridad tecnológica. Los colegios profesionales, las universidades, las agencias gubernamentales y los actores del sector privado deben articular mecanismos de reconocimiento y empleabilidad de perfiles criminológicos en estas áreas. La cooperación interinstitucional y la certificación de competencias específicas son claves para esta expansión.

Algunos ejemplos de nichos de intervención profesional para la Criminología digital incluyen:

- Análisis y prevención del ciberacoso y la violencia digital.
- Diseño de sistemas de alerta temprana para radicalización en redes.
- Evaluación de impacto ético de sistemas predictivos en justicia penal.
- Participación en equipos de auditoría algorítmica en servicios públicos.
- Formación en alfabetización digital crítica para colectivos vulnerables.
- Colaboración con departamentos de ciberseguridad en el análisis del factor humano.
- Investigación empírica sobre victimización online y ciberviolencia de género.
- Diseño de entornos virtuales más seguros desde la perspectiva situacional.

La cibercriminología y la tecnocriminología no son opciones periféricas ni modas pasajeras, sino ámbitos centrales para una criminología contemporánea que asuma los retos de la era digital con rigor técnico, ética profesional y compromiso social. La urgencia de repensar la Criminología en clave tecnológica no es solo un asunto académico, sino una cuestión estratégica de presencia, influencia y utilidad disciplinar.

Desde este punto de partida, el documento desarrollará los cinco apartados siguientes abordando con profundidad las dimensiones clave de estos campos: la caracterización teórica y aplicada de la cibercriminología; el impacto de la inteligencia artificial desde una óptica tecnocriminológica; la clasificación de los crímenes vinculados a la IA; los dilemas éticos y legales de la automatización en el ámbito penal y familiar; y las oportunidades formativas y laborales que se abren para los criminólogos especializados en estos nuevos horizontes de intervención.

2. Cibercriminología: El factor humano en la ciberseguridad

La cibercriminología es una disciplina emergente que estudia la delincuencia, la desviación y el control social en el ciberespacio. Se trata de un campo de conocimiento interdisciplinar que combina elementos de la Criminología tradicional con aportes de la informática, la psicología, la sociología de internet y la teoría de los sistemas. Su objetivo principal es comprender las formas específicas en que se manifiesta el comportamiento delictivo y desviado en entornos digitales, así como las estrategias de prevención, intervención y reacción que pueden adoptarse desde una perspectiva criminológica aplicada.

Uno de los ejes centrales de la cibercriminología es el análisis del **factor humano** en los sistemas de seguridad digital. Lejos de centrarse exclusivamente en la dimensión tecnológica, esta disciplina pone el foco en los individuos y grupos sociales que interactúan con la tecnología: usuarios, víctimas, ciberdelincuentes, desarrolladores, profesionales de seguridad y operadores institucionales. En este sentido, la cibercriminología critica la visión tecnocéntrica que considera al usuario como el "eslabón débil" de la ciberseguridad, y propone en cambio una comprensión más matizada del comportamiento humano en el ciberespacio.

El comportamiento en red se ve influido por factores culturales, cognitivos, emocionales y estructurales. La identidad digital, la sensación de anonimato, la inmediatez de la interacción, la ausencia de vigilancia física directa y la posibilidad de amplificación de la conducta generan un entorno propicio para la aparición de conductas desviadas o delictivas que pueden no manifestarse en contextos presenciales. Estas dinámicas requieren un enfoque criminológico que no solo identifique patrones técnicos, sino que entienda las motivaciones, oportunidades y racionalizaciones que operan en los sujetos.

En este marco, es fundamental comprender que el ciberdelincuente no responde a un perfil único. Lejos del estereotipo del "hacker solitario", los actores que cometen delitos en línea pueden incluir desde adolescentes experimentando con técnicas de intrusión hasta redes criminales altamente organizadas que operan a nivel transnacional. Estas redes muestran grados de profesionalización, especialización de tareas, lógicas de mercado, mecanismos de reputación y estructuras cooperativas que desafían los esquemas clásicos de delincuencia organizada.

La cibercriminología aporta herramientas analíticas para clasificar y entender estas formas de organización delictiva. Entre ellas se incluyen:

- **Hacktivismo:** ciberataques con motivación ideológica o política.
- **Cibercrimen económico:** fraudes, phishing, ransomware, clonación de tarjetas.
- **Ciberdelincuencia sexual:** grooming, sextorsión, distribución de material de abuso sexual infantil.
- **Ciberacoso y violencia digital:** hostigamiento sistemático, doxing, difusión no consentida de imágenes.
- **Crimen organizado digital:** mercados ilegales en la dark web, tráfico de datos personales, servicios criminales como "crime-as-a-service".

Cada una de estas tipologías presenta desafíos analíticos y operativos distintos, y exige el desarrollo de perfiles criminológicos específicos, basados en investigación empírica y en metodologías adaptadas al medio digital. La observación de foros, la etnografía virtual, el análisis de patrones de comportamiento y la cooperación internacional en inteligencia son herramientas cada vez más necesarias para la labor criminológica aplicada.

Uno de los grandes aportes de la cibercriminología radica en su capacidad para identificar las oportunidades situacionales del delito en el entorno digital. Desde una perspectiva de prevención situacional, se reconoce que muchos ciberataques no requieren sofisticación técnica, sino el aprovechamiento de vulnerabilidades humanas como el desconocimiento, la negligencia o la confianza excesiva. Las campañas de phishing, por ejemplo, explotan la ingeniería social para inducir a las víctimas a realizar acciones que comprometen la seguridad.

En este contexto, el criminólogo digital puede desempeñar un papel clave en el diseño de entornos digitales más seguros. Esto implica colaborar con ingenieros de software, desarrolladores de plataformas y equipos de seguridad para identificar puntos críticos de interacción, evaluar la experiencia del usuario desde una perspectiva de riesgo y proponer intervenciones conductuales (nudges) que promuevan prácticas seguras.

Asimismo, la formación en ciberseguridad no debe limitarse a lo técnico. La cibercriminología propone una educación crítica para usuarios, centrada en el desarrollo de competencias digitales, la conciencia sobre los riesgos, la comprensión de los modos de manipulación y la responsabilidad ética en el uso de tecnologías. Estas campañas pueden tener especial relevancia en colectivos vulnerables como menores, personas mayores o usuarios con bajo nivel de alfabetización digital.

A nivel profesional, la cibercriminología abre múltiples campos de actuación para los criminólogos/as:

- Evaluación de riesgos digitales en organizaciones públicas y privadas.
- Diseño de programas de formación en ciberconducta ética.
- Participación en equipos de respuesta a incidentes (CSIRT).
- Elaboración de perfiles de ciberdelincuentes para investigaciones.
- Apoyo en litigios relacionados con ciberdelitos.
- Asesoramiento en políticas públicas de ciberseguridad.
- Intervención en proyectos de ciberprevención en escuelas y comunidades.

El ámbito de la **ciberinteligencia** es especialmente relevante. En este campo, el criminólogo puede aplicar sus conocimientos sobre análisis del comportamiento, patrones de victimización y estructura de redes para contribuir al análisis OSINT (Open Source Intelligence), la monitorización de amenazas emergentes y la elaboración de informes de riesgo. Esta labor, tradicionalmente centrada en perfiles técnicos, se enriquece con una mirada social y conductual sobre el entorno digital.

Cabe destacar, además, la importancia de la cooperación internacional en cibercriminología. Dado que internet no conoce fronteras, la persecución de delitos digitales exige mecanismos de colaboración entre agencias, armonización normativa, plataformas de intercambio de inteligencia y formación conjunta. El criminólogo digital debe comprender los marcos normativos europeos e internacionales, así como las competencias y limitaciones de instituciones como Europol, Interpol, ENISA o el Consejo de Europa (Convenio de Budapest).

Desde una perspectiva ética, la cibercriminología también debe reflexionar sobre los límites de la vigilancia, el uso legítimo de herramientas de monitorización, la protección de datos personales y la preservación de derechos fundamentales en entornos digitales. La tensión entre seguridad y privacidad, cada vez más presente en el discurso público, requiere profesionales capaces de equilibrar ambos valores con criterio técnico y sensibilidad democrática.

En síntesis, el enfoque cibercriminológico sitúa al ser humano en el centro del análisis de la criminalidad digital. No se trata solo de proteger sistemas, sino de comprender a las personas: sus motivaciones, errores, hábitos, miedos, expectativas y reacciones frente a la tecnología. En este sentido, la cibercriminología no sustituye a la Criminología clásica, sino que la amplía y la actualiza frente a los desafíos de la sociedad digital. Su consolidación como disciplina aplicada exige inversión en formación, investigación empírica, generación de evidencia y reconocimiento institucional de los nuevos perfiles profesionales que demanda la seguridad en red.

3. Tecnocriminología: El impacto de la Inteligencia Artificial en el control social

La tecnocriminología se ha consolidado como un campo emergente que analiza críticamente la interacción entre tecnología avanzada y sistemas de control social desde una perspectiva criminológica. Uno de los desarrollos más disruptivos en este ámbito es la inteligencia artificial (IA), cuyo despliegue en contextos policiales, judiciales, penitenciarios y sociales plantea tanto oportunidades como amenazas. La tecnocriminología, lejos de adoptar una postura tecnofóbica o tecnófila, se sitúa como disciplina evaluadora, capaz de identificar usos legítimos, zonas grises y riesgos estructurales derivados de la automatización de decisiones en el sistema de justicia.

La IA, en términos generales, hace referencia a sistemas informáticos diseñados para simular procesos cognitivos humanos: aprendizaje, razonamiento, toma de decisiones, reconocimiento de patrones y predicción de comportamientos. Estos sistemas se nutren de grandes volúmenes de datos (big data), que procesan mediante algoritmos para ofrecer resultados, sugerencias o respuestas autónomas o semiautónomas. Su aplicación al control social —entendido como el conjunto de mecanismos formales e informales de

regulación de conductas— está transformando el modo en que se detecta, analiza, previene y sanciona la criminalidad.

Uno de los ámbitos más visibles de aplicación de la IA es la **predicción delictiva**. En Estados Unidos, sistemas como **PredPol** han sido utilizados por departamentos de policía para anticipar zonas con mayor probabilidad de comisión de delitos, basándose en patrones históricos de criminalidad. Aunque la herramienta prometía eficiencia en la asignación de recursos, ha sido ampliamente criticada por reproducir sesgos raciales y socioeconómicos, debido a que los datos alimentados ya estaban contaminados por prácticas policiales discriminatorias.

En el ámbito judicial, destaca el sistema **COMPAS** (Correctional Offender Management Profiling for Alternative Sanctions), utilizado en varios estados norteamericanos para predecir la probabilidad de reincidencia de los acusados y orientar decisiones judiciales sobre libertad condicional o condena. Investigaciones independientes han demostrado que COMPAS presenta sesgos significativos, siendo más proclive a calificar como de "alto riesgo" a personas afroamericanas, aun cuando sus antecedentes fueran similares o inferiores a los de personas blancas. Este caso es paradigmático de los peligros de utilizar IA sin una evaluación crítica de los datos, los algoritmos y sus implicaciones sociales.

En Europa, los usos de IA han sido más comedidos y regulados. No obstante, existen ejemplos relevantes. En **Países Bajos**, se desarrolló el sistema **SyRI** (Systeem Risico Indicatie), destinado a detectar fraude en subsidios sociales. Su implementación fue suspendida tras una sentencia judicial que consideró que vulneraba derechos fundamentales al no ser transparente ni permitir la defensa efectiva del ciudadano. En **España**, algunos proyectos piloto han explorado el uso de IA para análisis forense digital o para estimación de riesgo de reincidencia en instituciones penitenciarias, aunque su extensión práctica aún es limitada. No obstante, existen iniciativas como el sistema de vigilancia con cámaras dotadas de reconocimiento facial y detección de anomalías de comportamiento en infraestructuras críticas, o el uso de IA para clasificar incidentes en centros penitenciarios.

El uso de **IA en el ámbito penitenciario** introduce también nuevas formas de control. Algoritmos pueden ser usados para clasificar internos según su peligrosidad, establecer prioridades en la asignación de beneficios penitenciarios o vigilar interacciones sospechosas mediante análisis de video. Estas aplicaciones, si bien pueden aumentar la eficiencia del sistema, plantean interrogantes éticos sobre la autonomía de los profesionales, la posibilidad de errores automatizados, la cosificación de los internos y la opacidad del sistema.

Otro campo en crecimiento es el **uso de IA para el monitoreo y análisis de redes sociales** como estrategia preventiva frente a radicalización, amenazas terroristas o difusión de discursos de odio. Aunque estas herramientas pueden detectar patrones de riesgo antes de que se materialicen conductas, el riesgo de vigilancia masiva y criminalización de expresiones no delictivas está presente. En este sentido, el Reglamento Europeo de Inteligencia Artificial (AI Act), actualmente en fase de implementación, intenta establecer límites claros a los usos de alto riesgo, protegiendo derechos fundamentales y promoviendo la transparencia algorítmica.

Desde la tecnocriminología, se enfatiza la necesidad de evaluar el **impacto criminógeno de la tecnología**. La IA no es solo una herramienta neutra, sino un actor que puede reforzar desigualdades estructurales, invisibilizar sesgos históricos o consolidar lógicas de exclusión. El uso de IA en decisiones de libertad, vigilancia o clasificación penitenciaria tiene consecuencias reales sobre la vida de las personas, y su opacidad técnica puede erosionar garantías procesales, dificultar la defensa jurídica y fomentar la deshumanización del sistema.

Es por ello que se reclama la incorporación de **auditorías algorítmicas independientes**, mecanismos de control ético, protocolos de explicabilidad (que permitan entender cómo y por qué se llega a una decisión), y espacios deliberativos donde participen no solo expertos técnicos, sino también profesionales del Derecho, de la Criminología, de la Filosofía y de las Ciencias Sociales. La gobernanza algorítmica no puede quedar en manos exclusivas de ingenieros o empresas tecnológicas.

En el ámbito académico y profesional, la tecnocriminología puede contribuir:

- A la **evaluación de impacto ético y social** de tecnologías aplicadas al control social.
- Al diseño de protocolos de uso legítimo de IA en instituciones públicas.
- A la elaboración de guías de buenas prácticas en vigilancia digital.
- A la formación de cuerpos policiales y judiciales en sesgos algorítmicos.
- Al asesoramiento a organismos reguladores en materia de IA y derechos fundamentales.
- A la denuncia de usos ilegítimos o abusivos de IA desde una perspectiva de justicia social.

Ejemplos institucionales concretos incluyen el papel del criminólogo en los **comités de ética de innovación tecnológica** en ayuntamientos (como los promovidos por el Ayuntamiento de Barcelona), en grupos de investigación en proyectos europeos (como el Horizon Europe) donde se estudian implicaciones éticas de IA en seguridad, o en tareas de formación de operadores jurídicos en el Consejo General del Poder Judicial en España.

Asimismo, iniciativas como el **European AI Observatory** o el **Centre for Artificial Intelligence and Digital Ethics** incluyen cada vez más profesionales con perfil criminológico en sus equipos, dada la necesidad de incorporar análisis sociales y de impacto humano a tecnologías emergentes.

Desde un enfoque tecnocriminológico, se advierte que el uso de tecnologías predictivas o clasificatorias en sistemas de justicia puede cristalizar lógicas de "punicción preventiva" (punish before the fact), erosionando principios del derecho penal clásico como la presunción de inocencia, el principio de legalidad o la proporcionalidad de la sanción. La tecnocriminología, en este sentido, no solo diagnostica, sino que propone alternativas: sistemas de IA explicables, modelos híbridos de decisión, supervisión humana obligatoria, participación ciudadana en procesos regulatorios y modelos de justicia restaurativa digitalmente asistida.

En definitiva, el impacto de la IA en el control social no puede entenderse únicamente como una cuestión técnica, sino como un fenómeno sociopolítico que requiere respuestas interdisciplinarias. La tecnocriminología, como disciplina crítica, tiene la capacidad de

interpelar a los sistemas de poder digital, identificar riesgos criminógenos y proponer marcos normativos y operativos que garanticen una gobernanza democrática de la tecnología. Su consolidación como campo profesional depende de la articulación entre investigación, formación, incidencia pública y cooperación institucional. La inteligencia artificial no es el futuro de la Criminología: es su presente, y exige profesionales preparados para comprender, cuestionar y orientar su desarrollo hacia fines legítimos, justos y socialmente responsables.

4. La profesionalización en Criminología Digital: Perfiles, competencias y empleabilidad

En los últimos años, el ecosistema profesional de la Criminología ha experimentado una transformación significativa impulsada por los entornos digitales, la tecnología aplicada a la seguridad y el auge de nuevos riesgos sociales. Esta evolución ha propiciado la aparición de una rama emergente: la **Criminología Digital**, un espacio interdisciplinar en el que confluyen conocimientos criminológicos, habilidades técnicas y competencias analíticas vinculadas al ciberespacio. Este apartado examina los perfiles emergentes, las competencias clave y los escenarios laborales donde se consolida esta especialización, subrayando la importancia de la formación técnica aplicada y el papel estratégico de los criminólogos en un entorno digitalizado.

La Criminología Digital no se limita al estudio de los delitos cometidos a través de internet. Implica una comprensión amplia del impacto que las tecnologías de la información tienen sobre los fenómenos delictivos, las estrategias de prevención, los procesos de victimización y las nuevas formas de control social. Esto exige una **actualización radical del perfil profesional del criminólogo**, que debe incorporar nuevas herramientas, lenguajes y marcos teóricos.

Entre los **perfiles profesionales emergentes** destacan:

- **Analista de inteligencia digital:** especializado en el uso de técnicas de OSINT (Open Source Intelligence), SOCMINT (Social Media Intelligence) y análisis de metadatos para la prevención y detección de amenazas.
- **Criminólogo experto en ciberseguridad:** colabora en el diseño de estrategias de seguridad de la información en empresas, instituciones o infraestructuras críticas, evaluando riesgos humanos y sociales.
- **Consultor de prevención de ciberdelitos:** diseña campañas, protocolos y formaciones adaptadas a colectivos vulnerables, empresas o cuerpos policiales.
- **Investigador forense digital:** contribuye a la identificación y análisis de evidencias electrónicas, colaborando con peritos informáticos y expertos judiciales.
- **Especialista en ética tecnológica y derechos digitales:** analiza el impacto de la tecnología sobre los derechos fundamentales y participa en comités éticos, organismos reguladores y procesos legislativos.

Cada uno de estos perfiles exige una combinación de **competencias técnicas, sociales y éticas**. A nivel técnico, se requiere familiaridad con entornos digitales, herramientas de rastreo y análisis, nociones de ciberseguridad y comprensión básica de arquitecturas informáticas. A nivel social, es clave el conocimiento de teorías criminológicas aplicadas, comprensión de dinámicas de victimización digital, mediación social en entornos online

y análisis de riesgo. Y a nivel ético, se exige una sólida formación en derechos fundamentales, privacidad, protección de datos y responsabilidad profesional.

En el plano institucional, **la demanda de criminólogos digitales ha crecido** en diversas áreas:

- **Fuerzas y Cuerpos de Seguridad:** en unidades de cibercrimen, análisis estratégico, prevención de radicalización online o cooperación internacional.
- **Empresas del sector tecnológico y de seguridad privada:** como analistas de fraude, diseñadores de sistemas de cumplimiento normativo (compliance) o responsables de formación y cultura de ciberseguridad.
- **Administraciones públicas:** en unidades de cibervigilancia, centros de respuesta ante incidentes (CERT/CSIRT), observatorios de cibercriminalidad o servicios sociales adaptados a la era digital.
- **ONGs y organismos de derechos humanos:** en defensa de víctimas de violencia digital, protección de datos de colectivos vulnerables o denuncia de prácticas tecnológicas abusivas.
- **Academia y centros de investigación:** en proyectos multidisciplinares sobre justicia algorítmica, cibervictimización, tecnologías policiales o delitos emergentes.

Un ejemplo paradigmático es el programa **Hack_Right**, desarrollado por el Ministerio de Justicia de Países Bajos, que ofrece a jóvenes hackers primerizos una vía de reorientación profesional en ciberseguridad. Este tipo de programas requiere expertos que comprendan tanto la dimensión tecnológica como la social y criminológica del fenómeno. Otro caso es el **Centro Criptológico Nacional** en España, que incorpora analistas con perfil mixto (tecnológico-social) para la gestión de incidentes en organismos públicos.

En términos de **empleabilidad**, los estudios recientes indican que los profesionales con formación en cibercriminología tienen tasas de inserción laboral superiores a la media del sector social. Según el informe de Cybersecurity Ventures (2023), se estima una demanda global de más de 3 millones de profesionales en ciberseguridad no cubierta, lo que representa una oportunidad estratégica para los criminólogos especializados. La clave está en la **hibridación de perfiles**: aquellos criminólogos que complementan su formación con conocimientos técnicos en seguridad digital, análisis de datos o derecho tecnológico tienen mayor proyección profesional.

El desarrollo de estos perfiles requiere una **formación académica adaptada**. Universidades y centros de formación deben integrar asignaturas de cibercriminología, ética digital, análisis de datos aplicados, técnicas de investigación digital o inteligencia abierta. Asimismo, se hace necesario el fortalecimiento de las **certificaciones profesionales**, como las relacionadas con OSINT, análisis forense digital o cumplimiento normativo en entornos digitales (ISO 27001, GDPR, ENS, etc.).

El reto no es solo formar profesionales competentes, sino **construir un ecosistema laboral que reconozca y valore la especificidad del saber criminológico**. Esto implica impulsar la colegiación, la certificación profesional, la presencia institucional en foros tecnológicos y la visibilidad mediática del papel del criminólogo digital. Iniciativas como las del Colegio Profesional de la Criminología de la Comunidad de Madrid, que

promueven certificaciones en ciberinteligencia, representan pasos clave hacia esta consolidación.

En definitiva, la Criminología Digital y la Tecnocriminología no son solo campos de estudio, sino **espacios de profesionalización real**. El factor humano sigue siendo clave en la prevención del delito, la gestión del riesgo y la defensa de los derechos en el entorno digital. Formar criminólogos preparados para actuar en estos escenarios es una prioridad estratégica si queremos responder a los desafíos de la sociedad tecnológica desde una perspectiva ética, crítica y eficaz.

5. Propuestas académicas y estratégicas para una Criminología útil en la era digital

El avance de la Criminología en entornos digitales exige no solo adaptaciones teóricas, sino también transformaciones profundas en los marcos institucionales, académicos y estratégicos que estructuran su desarrollo. En este apartado se exponen propuestas concretas orientadas a consolidar una **Criminología Digital** eficaz, reconocida y socialmente útil, atendiendo a tres ejes clave: formación académica, articulación institucional y estrategia profesional.

1. Formación académica orientada a la realidad digital

El currículo formativo de la Criminología debe evolucionar para incorporar asignaturas, competencias y metodologías propias de la era digital. Esto incluye la inclusión sistemática de:

- **Cibercriminología** como asignatura troncal o itinerario especializado, que analice fenómenos como el hacking, la cibervictimización, el grooming, el ciberacoso o el fraude online desde una perspectiva criminológica.
- **Tecnocriminología y ética algorítmica**, con contenidos sobre inteligencia artificial, decisiones automatizadas, sesgos algorítmicos, sistemas predictivos, vigilancia digital y gobernanza de la tecnología.
- **Metodologías digitales de investigación**, incluyendo análisis de redes sociales, minería de datos, estudios de cibercultura y metodologías mixtas aplicadas al entorno online.
- **Técnicas de inteligencia abierta (OSINT)** y análisis de fuentes digitales para la prevención del delito, en coordinación con materias sobre análisis del riesgo, prevención situacional y análisis del comportamiento.
- **Formación en competencias digitales y jurídicas**, como privacidad, ciberseguridad, regulación tecnológica (GDPR, ENS, AI Act), protección de datos o derecho penal informático.

Además, se propone el desarrollo de **laboratorios de Criminología Digital** en universidades, que integren simulaciones de ciberincidentes, ejercicios de análisis de casos reales, laboratorios de OSINT y escenarios de predicción y respuesta ante ciberdelitos.

2. Articulación institucional: redes, colegios y alianzas

La consolidación de la Criminología Digital requiere una **articulación efectiva entre academia, profesión e instituciones públicas y privadas**. Algunas propuestas clave son:

- **Creación de redes nacionales de Criminología Digital**, que permitan compartir buenas prácticas, investigaciones, materiales formativos y estrategias de intervención en cibercriminalidad.
- **Impulso desde los Colegios Profesionales** para establecer itinerarios de certificación, formación continua y acreditación de perfiles profesionales en ciberinteligencia, cibervictimología, análisis de riesgos digitales o mediación tecnológica.
- **Alianzas con centros tecnológicos y de ciberseguridad**, como INCIBE, CCN-CERT o universidades tecnológicas, para fomentar proyectos de investigación aplicada, transferencia de conocimiento y formación especializada conjunta.
- **Participación en consorcios europeos** (Horizon Europe, Digital Europe, Erasmus+) que permitan a los criminólogos contribuir en proyectos de justicia digital, ciberseguridad o derechos digitales desde una perspectiva social.

Estas acciones no solo legitiman el papel del criminólogo en nuevos entornos, sino que permiten construir estructuras de oportunidad profesional y académica sostenibles.

3. Estrategia profesional: visibilidad, innovación y evaluación

Para que la Criminología Digital tenga un impacto real, es necesario consolidar una **estrategia profesional proactiva** que articule visibilidad pública, innovación aplicada y mecanismos de evaluación:

- **Campañas de comunicación pública**, con presencia activa en medios, redes sociales y espacios de divulgación, que muestren el valor añadido de los criminólogos en entornos digitales.
- **Innovación en servicios criminológicos**, desarrollando consultorías, programas de prevención adaptados al entorno online, sistemas de evaluación de riesgos digitales, asesoría institucional o desarrollo de materiales educativos sobre ciberseguridad y derechos digitales.
- **Evaluación del impacto**: establecer mecanismos para evaluar la eficacia y calidad de las intervenciones criminológicas digitales, generando evidencia sobre su aportación real en contextos de seguridad, justicia y educación.

Ejemplos concretos incluyen la creación de **observatorios de cibercriminalidad y vulnerabilidades digitales**, dirigidos por equipos criminológicos, que alimenten políticas públicas basadas en evidencia. También la implantación de programas piloto de **prevención del discurso de odio** en centros educativos o la colaboración con cuerpos policiales para analizar patrones de victimización online.

4. Reivindicación del rol institucional del criminólogo digital

El acceso a posiciones clave en la administración pública, en organismos reguladores, en comités éticos o en empresas tecnológicas sigue siendo limitado para los criminólogos. Se proponen acciones para revertir esta situación:

- Incluir la titulación en Criminología en **ofertas públicas y perfiles de acceso** a cuerpos técnicos en áreas de ciberseguridad, análisis delictivo o inteligencia estratégica.
- Reconocer al criminólogo como experto en **intervención social digital**, tanto en entornos de violencia de género digital, como en delitos de odio o mediación online.
- Fomentar la figura del criminólogo como **asesor en proyectos de desarrollo tecnológico** con impacto social (IA, metaverso, smart cities).

La Criminología Digital no puede quedar relegada a un rol meramente académico o de análisis. Su dimensión aplicada debe ser reivindicada desde una visión transformadora, profesional y basada en evidencia.

En conclusión, para que la Criminología sea útil en la era digital, debe repensarse estratégicamente: actualizar su currículo, articularse institucionalmente, innovar en sus servicios y ganar visibilidad e impacto. Solo así podrá responder a los retos contemporáneos y convertirse en un actor relevante en la gobernanza social de la tecnología. El momento es ahora. Y el lugar, está donde están los datos, los algoritmos y las personas: en lo digital.

6. Conclusiones: ¿Dónde está el trabajo? Visión estratégica y horizonte profesional

A modo de cierre, es necesario sintetizar los principales hallazgos y reflexiones que han emergido a lo largo de esta conferencia. A partir del diagnóstico actual del ecosistema criminológico y de las transformaciones digitales que impactan en el delito, la prevención y el control social, se extraen cinco ideas clave que orientan el desarrollo de la Criminología en las próximas décadas:

1. La digitalización del delito exige una criminología adaptada al nuevo entorno

La transición de las conductas delictivas hacia el ciberespacio no es un fenómeno accesorio, sino estructural. Desde el fraude digital al ciberacoso, pasando por el ransomware, la trata de personas mediante criptomonedas o la manipulación electoral con bots, los delitos se redefinen tecnológicamente. Esto requiere una respuesta criminológica fundamentada, capaz de analizar no solo los hechos delictivos, sino también los vectores tecnológicos que los posibilitan. La Criminología del siglo XXI debe ser digital por diseño, no por adaptación reactiva.

2. La tecnocriminología permite evaluar el impacto ético, social y criminógeno de la tecnología

Las decisiones automatizadas, el uso de IA en sistemas de justicia y vigilancia, la consolidación de ciudades inteligentes o el control algorítmico del comportamiento social no pueden quedar fuera del análisis criminológico. La tecnocriminología propone herramientas para evaluar el riesgo de deshumanización del sistema penal, los sesgos sistémicos de los algoritmos y la erosión de derechos fundamentales. Esta dimensión crítica es clave para mantener una justicia tecnológicamente asistida pero socialmente legítima.

3. El mercado laboral ya demanda criminólogos digitales: el problema no es de empleabilidad, sino de adecuación

El déficit global de expertos en ciberseguridad, análisis de riesgos, inteligencia digital y ética tecnológica es una oportunidad para los criminólogos. Sin embargo, la empleabilidad efectiva depende de la adecuación del perfil: es necesario combinar competencias sociales y jurídicas con habilidades técnicas. La formación universitaria debe anticipar esta demanda y ofrecer itinerarios formativos coherentes con los nuevos nichos profesionales.

4. La visibilidad institucional del criminólogo digital es una cuestión política y estratégica

El reconocimiento del criminólogo como profesional clave en la gobernanza de la seguridad digital no se logrará únicamente desde la academia. Requiere acción política, incidencia institucional, alianzas estratégicas y campañas de comunicación que evidencien el valor añadido del saber criminológico. La certificación profesional, la creación de figuras laborales específicas y la inclusión en órganos decisores son pasos ineludibles.

5. La Criminología Digital y la Tecnocriminología no son el futuro: son el presente

La velocidad del cambio tecnológico obliga a actuar ahora. No se trata de prepararse para un escenario lejano, sino de consolidar ya estructuras formativas, redes profesionales y modelos de intervención. Como bien ha sintetizado un informe del European Union Agency for Cybersecurity (ENISA, 2023), “la ciberseguridad será tanto técnica como social: lo contrario será inseguridad”.

En conclusión, **sí hay trabajo para la Criminología**. Pero está donde están los nuevos riesgos, las nuevas preguntas y las nuevas tecnologías. El reto es triple: saber verlo, saber prepararse y saber ocuparlo. La Criminología Digital y la Tecnocriminología ofrecen esa posibilidad: una ciencia social aplicada, conectada con la realidad, comprometida con los derechos y capaz de generar soluciones. El lugar donde sí hay trabajo es donde la Criminología se convierte en acción informada y estrategia profesional. Ese lugar es, hoy más que nunca, el entorno digital.

Referencias

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (2022). *Cybercrime en jongeren: Van spel naar straf?* Den Haag: AIVD.

Clough, J. (2015). *Principles of Cybercrime* (2nd ed.). Cambridge University Press.

Council of Europe. (2023). *Budapest Convention on Cybercrime*. Retrieved from <https://www.coe.int/en/web/cybercrime>

ENISA. (2023). *Threat Landscape Report*. European Union Agency for Cybersecurity. Retrieved from <https://www.enisa.europa.eu/>

Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: Europol.

Floridi, L. (2021). *The Ethics of Artificial Intelligence*. Oxford University Press.

González García, A. (2025). *Geopolítica del ciberespacio: Ciberinteligencia y cibercriminología en la sociedad digital*. Tirant lo Blanch.

Harari, Y. N. (2024). *Nexus: Tecnología y poder en el siglo XXI*. Debate.

Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Polity Press.

Moody, G. D., Siponen, M., & Pahlila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), 285–311.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

Weulen Kranenbarg, M., & Holt, T. J. (Eds.). (2022). *Cybercrime and Digital Deviance*. Springer.

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.