

## **El alcance del secreto profesional del abogado frente al uso de inteligencia artificial en el proceso penal argentino**

por Marcela Marta Rosa D' Alessandre

Sumario: 1. Introducción. - 2. Marco conceptual de la inteligencia artificial. - 3. El secreto profesional del abogado en el derecho argentino. 3.1. Constitución Nacional. 3.2. Código Penal. 3.3. Código Procesal Penal. Declaración testimonial del abogado. 3.4. Regulación del ejercicio profesional de la abogacía (Leyes 23.187 y 5.177). 3.5. Ley 25.326 de Protección de Datos Personales. 3.6. Concepción amplia del secreto profesional. Actividad cognitiva defensiva. - 4. Análisis del caso *United States v. Bradley Heppner*. 4.1. Hechos relevantes. 4.2. Fundamentos del tribunal. A) Inexistencia de relación abogado-cliente. B) Ausencia de expectativa razonable de confidencialidad. C) Rechazo de la *work product doctrine*. 4.3. Críticas al fallo. A) Concepto rígido de "tercero". B) Deficiente diferenciación entre herramienta tecnológica y divulgación. C) Alcance restrictivo de la *work product doctrine*. 4.4. Valoración. - 5. Análisis comparado: derecho argentino y estadounidense. 5.1. Naturaleza jurídica de la protección: privilegio vs. garantía constitucional. 5.2. Alcance del secreto profesional en ambos sistemas. 5.3. Tratamiento de la inteligencia artificial en ambos países. 5.4. Proyección del caso Heppner en el derecho argentino. - 6. Consecuencias probatorias y reglas de admisibilidad. 6.1. Prueba generada mediante inteligencia artificial. 6.2. Criterios de admisibilidad y fiabilidad. 6.3. Relación con la doctrina de la prueba ilícita. 6.4. Impacto sobre el derecho de defensa e igualdad de armas. - 7. Propuestas normativas. 7.1. Estándares internacionales aplicables. 7.2. Estándares argentinos aplicables. 7.3. Protección de la actividad cognitiva defensiva. 7.4. Pautas mínimas de uso profesional. 7.5. Criterios funcionales para determinar la prevalencia del secreto profesional en contenidos generados por inteligencia artificial. 7.6. Proyección probatoria de los criterios funcionales: inadmisibilidad de la prueba obtenida con vulneración del secreto profesional. 7.7. Integración con el sistema jurídico vigente. - 8. Conclusiones. - 9. Bibliografía.

### Índice de abreviaturas

CN: Constitución Nacional Argentina. CP: Código Penal de la Nación Argentina.

CPPN: Código Procesal Penal de la Nación (Ley 23.984 actualizada hasta las Leyes 27.372, 27384, 27.401).

CPPF: Código Procesal Penal Federal.

CSJN: Corte Suprema de Justicia de la Nación.

CCC: Cámara Criminal y Correccional.

SDNY: Southern District of New York.

IA: Inteligencia Artificial.

IAGen: Inteligencia Artificial Generativa.

LLM: Large Language Model.

FBI: Federal Bureau of Investigation.

OCDE: Organización para la Cooperación y el Desarrollo Económicos.

UNESCO: Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

UE: Unión Europea.

AI Act: Reglamento de Inteligencia Artificial de la Unión Europea.

CPACF: Colegio Público de la Abogacía de la Capital Federal.

CADH: Convención Americana sobre Derechos Humanos.

PIDCP: Pacto Internacional de Derechos Civiles y Políticos.

DUDH: Declaración Universal de Derechos Humanos.

## 1. Introducción

La era digital ha planteado uno de los desafíos más significativos para el derecho, un sistema inherentemente lento que contrasta con la velocidad de los cambios tecnológicos. En ese contexto, la inteligencia artificial (IA) representa una transformación radical del paradigma tecnológico, jurídico y social. Su impacto trasciende el plano técnico, incidiendo directamente en los modos de producción, circulación y validación de conocimiento, incluido el jurídico.

Dentro de este escenario, la inteligencia artificial generativa (IAGen) emerge como una de las tecnologías más disruptivas. Así, herramientas de IA, como GPT 4 de Open AI, Bing Chat de Microsoft, Bard de Google, entre otras, están destinadas a convertirse en asistentes jurídicos productivos(1). Sin embargo, su utilización también ha introducido una tensión inédita entre la innovación tecnológica y las garantías fundamentales del proceso penal.

En particular, el uso de IAGen por parte de imputados y abogados para analizar casos, estructurar estrategias defensivas o generar documentos plantea interrogantes en torno al alcance del secreto profesional y la inviolabilidad del derecho de defensa en juicio(2).

En este marco, el fallo dictado en el caso *United States v. Bradley Heppner* (SDNY, 2026) constituye un antecedente inédito, en tanto aborda por primera vez y de manera directa la naturaleza jurídica de las interacciones entre un imputado y una herramienta de IAGen. La decisión judicial citada, al negar la aplicación del privilegio abogado-cliente y de la *work product doctrine* (doctrina del producto del trabajo) respecto de los contenidos generados mediante IAGen, se fundamenta en dos premisas centrales: por un lado, la inexistencia de una relación profesional entre el usuario y el sistema; por otro, la ausencia de una expectativa razonable de confidencialidad, dada la intervención de un tercero tecnológico.

No obstante, la traslación de tales criterios al derecho argentino no puede realizarse de manera automática ni acrítica. Ello obedece a diferencias estructurales entre ambos sistemas jurídicos. Mientras que en el derecho estadounidense el privilegio abogado-cliente se configura primordialmente como una regla probatoria, en el ordenamiento argentino el secreto profesional se encuentra íntimamente vinculado con la garantía constitucional de defensa en juicio consagrada en el artículo 18 de la CN.

Esta diferencia no es meramente terminológica: en Argentina, la confidencialidad de la relación abogado-cliente no sólo protege la comunicación entre los mismos, sino que resguarda el proceso de construcción de la defensa.

Desde esta perspectiva, el problema central que motiva la presente investigación puede formularse en los siguientes términos: ¿los contenidos generados mediante IA por un imputado o su defensa técnica deben ser considerados ajenos al ámbito de protección del secreto profesional, o bien pueden integrar la esfera de la actividad cognitiva defensiva? La relevancia de esta cuestión se potencia si se advierte que la IAGen interviene activamente en la elaboración de determinados contenidos. A diferencia de las herramientas tradicionales -como libros, bases de datos jurídicas o software de procesamiento de texto-, los sistemas de IAGen no solo procesan información, sino que también pueden almacenarla y eventualmente reutilizarla, lo que introduce un riesgo concreto de pérdida de confidencialidad. En este sentido, la IAGen no es un mero instrumento pasivo, sino un agente dinámico en la generación de contenidos jurídicos, que se nutre de la información suministrada por el usuario.

Ahora bien, la incorporación de una herramienta como la IAGen no puede conducir, sin más, a la desprotección de la actividad defensiva. De lo contrario, se configuraría una restricción al derecho de defensa en juicio, en tanto se limitaría el acceso a herramientas tecnológicas que hoy son relevantes para el ejercicio de la profesión jurídica. En efecto, exigir al imputado o a su abogado que renuncien al uso de IAGen para preservar la confidencialidad implicaría imponer una carga irrazonable que, incluso, podría afectar la igualdad de armas en el proceso penal.

En este contexto, la hipótesis que guía el presente trabajo sostiene que los contenidos generados mediante IAGen no deben ser excluidos de manera automática del ámbito de protección del secreto profesional. Por el contrario, cuando tales contenidos se integran al proceso de elaboración de la defensa técnica, pueden ser considerados como manifestaciones de la actividad cognitiva defensiva, y, por ende, merecedores de tutela constitucional.

No obstante, esta protección no es absoluta, sino que se encuentra condicionada por el grado de exposición de la información y por la existencia de mecanismos que garanticen su confidencialidad.

A fin de desarrollar esta hipótesis, el trabajo se estructura en tres ejes principales. En primer lugar, se delimita el marco conceptual de la IAGen en el ámbito jurídico, analizando sus características técnicas y su impacto en la práctica profesional. En segundo lugar, se examina el régimen del secreto profesional en el derecho argentino, con especial énfasis en su vinculación con la garantía de defensa en juicio y su proyección sobre la actividad cognitiva del abogado y del imputado. Finalmente, se aborda el análisis del caso Heppner y su posible recepción en el ordenamiento local, proponiendo criterios interpretativos que permitan armonizar la innovación tecnológica con la preservación de las garantías fundamentales.

En definitiva, el presente estudio no se limita a describir un fenómeno emergente, sino que busca contribuir a la construcción jurídica capaz de responder a los desafíos que plantea la IAGen. Ello exige abandonar enfoques meramente formalistas y adoptar una perspectiva que, sin desconocer los riesgos tecnológicos, preserve el núcleo esencial del derecho de defensa como pilar del Estado de Derecho.

## 2. Marco conceptual de la inteligencia artificial

La IA, en su concepción contemporánea, puede definirse como el conjunto de sistemas informáticos capaces de realizar tareas que, tradicionalmente, requerían inteligencia humana, tales como el procesamiento del lenguaje natural, el reconocimiento de patrones y la toma de decisiones basada en datos.

Por su parte, la IAGen puede definirse como el conjunto de tecnologías capaces de crear contenido nuevo -texto, imágenes, videos, sonidos o código- en lugar de limitarse a clasificar o analizar datos preexistentes. Dentro de ese universo, los modelos de lenguaje de gran escala (Large Language Models o LLM) constituyen una de sus expresiones más relevantes, pues son sistemas entrenados con grandes volúmenes de palabras y datos que permiten generar respuestas complejas a partir de una instrucción o prompt. A su vez, muchos de estos sistemas operan bajo un esquema, en el que el resultado es visible, pero no siempre lo es el proceso interno que condujo a dicha respuesta.

En el plano jurídico, esta caracterización técnica no es un dato menor. La guía elaborada por el CPACF destaca que la IAGen ha irrumpido en el mundo legal como una herramienta de gran potencial, apta para asistir en la investigación jurídica, automatizar tareas y generar borradores de textos. No obstante, enfatiza que se trata exclusiva y únicamente de un instrumento: no reemplaza el análisis jurídico, no toma decisiones y no exime al abogado de responsabilidad profesional. La decisión final -remarca el documento- debe continuar siendo humana(3).

Desde una perspectiva técnica, estos sistemas operan mediante el entrenamiento sobre grandes volúmenes de datos, lo que les permite predecir secuencias lingüísticas con alto grado de coherencia. Sin embargo, su funcionamiento implica necesariamente el procesamiento de la información ingresada por los usuarios, lo que plantea interrogantes en materia de privacidad y confidencialidad.

En el ámbito jurídico, la IAGen ha comenzado a desempeñar un rol cada vez más activo. No sólo se utiliza para la búsqueda de jurisprudencia o doctrina, sino también para la redacción de escritos, la elaboración de estrategias procesales y el análisis de riesgos legales. Esta evolución ha llevado a que este tipo de tecnología sea una herramienta relevante en la práctica profesional.

No obstante, la implementación de la IAGen en la práctica legal, si bien promete mayor eficacia, enfrenta importantes riesgos y desafíos éticos y legales(4).

En esta línea, uno de los aportes más significativos reside en su carácter instrumental: no sustituye el juicio humano, pero sí amplía la base empírica sobre la cual ese juicio puede realizarse. Así, puede contribuir a la búsqueda, sistematización, reconstrucción y organización de información relevante para el caso, e incluso a la conformación de hipótesis de trabajo. Sin embargo, esa utilidad técnica no elimina los riesgos jurídicos, pues el empleo de tecnologías opacas, no verificables o insuficientemente aceptadas puede comprometer la legitimidad del proceso y afectar garantías procesales fundamentales(5).

Entre los principales riesgos se destacan aquellos vinculados con la confidencialidad y privacidad de los datos, en tanto la información ingresada a estos sistemas puede ser utilizada -al menos potencialmente- en procesos de entrenamiento o mejora de modelos. Precisamente por ello, la guía del CPACF incluye entre los pilares del uso responsable de la IAGen la protección de datos personales y el deber de confidencialidad. Allí se advierte que “cuidar la privacidad es sagrado” y que debe evitarse subir expedientes o información sensible a herramientas que no ofrezcan garantías suficientes. Asimismo, el documento enfatiza que el abogado debe respetar estrictamente el secreto profesional y oponerse ante jueces u otras autoridades a cualquier requerimiento que lo exponga a vulnerarlo, salvo autorización del cliente o supuesto de propia defensa(6).

Este cambio de paradigma resulta central para el análisis del secreto profesional. Mientras que las herramientas tradicionales no implicaban la intervención de terceros en el proceso de elaboración de la defensa, la IAGen introduce un elemento externo que podría acceder a la información ingresada por el usuario. En este sentido, la cuestión no radica únicamente en la capacidad técnica del sistema, sino en si es o no jurídicamente hablando un tercero.

En síntesis, el marco conceptual de la IAG en el derecho exige reconocer su doble naturaleza: por un lado, como herramienta que potencia la capacidad cognitiva del abogado; por otro, como posible fuente de riesgo para la confidencialidad de la información. Esta tensión constituye el punto de partida para el análisis del secreto profesional en el contexto tecnológico contemporáneo.

## 3. El secreto profesional del abogado en el derecho argentino

Conforme las recomendaciones sobre ética profesional efectuadas por la XIV Conferencia de la Federación Interamericana de Abogados(7):

“El secreto profesional está constituido por las manifestaciones que hace el cliente, quién puede ser persona natural o jurídica, al abogado, no sólo bajo promesa expresa de silencio, sino por la simple exposición de un caso en solicitud de asesoramiento profesional”.

Asimismo, se ha señalado que el secreto profesional “constituye una guarda de este secreto, un deber y un derecho: frente al cliente es un deber que subsiste íntegramente aún después de terminado el patrocinio jurídico; es un derecho del abogado frente a las autoridades administrativas o judiciales que solicitan declaraciones de cualquier naturaleza del abogado respecto al secreto profesional”.

La protección que brinda el secreto profesional no se limita a las manifestaciones verbales del cliente, sino que se extiende, además, a “los documentos, planos, dibujos, fotografías y objetos que hubiera confiado el cliente al abogado para el estudio y defensa de su caso”.

En este sentido, el secreto profesional del abogado constituye uno de los pilares fundamentales del sistema jurídico argentino, en tanto garantiza la confianza necesaria para el ejercicio efectivo del derecho de defensa. Su fundamento se asienta en una pluralidad de fuentes normativas, que incluyen disposiciones constitucionales, legales y deontológicas, configurando un régimen de tutela amplio e integral.

### 3.1. Constitución Nacional

En primer lugar, el artículo 18 de la CN consagra -entre otras garantías- el derecho de defensa en juicio que ha sido protegido por la jurisprudencia de la CSJN(8). Dentro de este marco, la confidencialidad de la relación abogado-cliente se erige como un elemento esencial, en tanto permite al imputado comunicarse libremente con su defensor sin temor a que dicha información sea utilizada en su contra.

Sobre el particular, Clariá Olmedo enseña que “por vía indirecta se arrancarían la confesión del imputado suprimiéndose la garantía de defensa material que lo faculta a no declarar o, si se quiere, a mentir si se pudiera obligar al defensor a declarar sobre las confidencias recibidas de sus patrocinados”(9).

En el ámbito de la abogacía el secreto profesional no se agota con una mera obligación ética ni en una regla de reserva, sino que encuentra una justificación adicional de jerarquía superior en la garantía de defensa en juicio. En efecto, mientras que en otras profesiones el deber de confidencialidad protege primordialmente la intimidad y la confianza de la persona, en el caso del abogado se proyecta, además, sobre la necesidad de asegurar un ámbito libre, reservado y seguro para la preparación de la defensa técnica. De allí que su tutela no sólo responda únicamente al interés individual del cliente, sino también a la preservación de principios constitucionales básicos del Estado de Derecho.

Este criterio ha sido sostenido por el Comité de Derechos Humanos encargado de interpretar el Pacto Internacional sobre Derechos Civiles y Políticos donde dejó sentado que: “el derecho a comunicarse con el defensor exige que se garantice al acusado el pronto acceso a su abogado. Los abogados deben poder reunirse con sus clientes en privado y comunicarse con los acusados en condiciones que garanticen plenamente el carácter confidencial de sus comunicaciones. Además, los abogados deben poder asesorar y representar a las personas acusadas de un delito de conformidad con la ética profesional establecida, sin ninguna restricción, influencia, presión o injerencia indebida de ninguna parte”(10).

Asimismo, el artículo 18 de la CN consagra la inviolabilidad de la correspondencia y de los papeles privados, estableciendo una garantía de resguardo frente a injerencias indebidas por parte del Estado o de terceros. Esta previsión no sólo protege el contenido de las comunicaciones, sino también los soportes materiales e inmateriales en los que se exterioriza la actividad intelectual de las personas.

Por último, la garantía se ve reforzada por lo dispuesto en el artículo 19 de la CN, que consagra el principio de reserva y la inviolabilidad de la esfera privada. En este sentido, la confidencialidad de las comunicaciones entre abogado y cliente se inscribe dentro del ámbito de protección de la intimidad, así como también en la inviolabilidad de la correspondencia. Por consiguiente, cualquier medida que directa o indirectamente comprometa el secreto profesional del abogado debe ser analizada con criterio restrictivo, por cuanto se encuentra en juego no sólo un deber deontológico, sino una garantía constitucional de máxima jerarquía.

### 3.2. Código Penal

En segundo lugar, el artículo 156 del CP tipifica el delito de violación de secretos, sancionando a quien, teniendo conocimiento de un secreto por razón de su estado, oficio, empleo, profesión o arte, lo revelase sin justa causa.

La norma citada refuerza el carácter obligatorio del secreto profesional y su función como garantía institucional, en tanto constituye una obligación jurídicamente exigible cuyo incumplimiento acarrea consecuencias penales.

La figura resulta aplicable a todas las profesiones, incluyendo expresamente a la abogacía. El bien jurídico protegido es la intimidad, entendida como el ámbito de reserva que tiene la vida de una persona, sus acciones, sus asuntos, sus sentimientos, sus creencias, relaciones y demás aspectos que el individuo decide sustraer del conocimiento de terceros. Se trata de un derecho de carácter personalísimo, irrenunciable, inalienable e imprescriptible(11).

En ese sentido, la doctrina ha definido el derecho de la intimidad como “el derecho que garantiza a su titular el desenvolvimiento de su vida y de su conducta dentro de un ámbito privado, sin injerencias ni intromisiones que pueden provenir de la autoridad o de terceros, y en tanto dicha conducta no ofenda el orden público y a la moral pública, ni perjudique a otras personas”(12).

Por su parte, la CSJN ha conceptualizado este derecho como “aquel que protege jurídicamente un ámbito de autonomía individual constituida por sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o datos que teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial para la intimidad”(13).

Asimismo, el Máximo Tribunal sostuvo que: “el derecho a la privacidad comprende no sólo a la esfera doméstica, al círculo familiar y de amistad, sino otros aspectos de la personalidad espiritual o física de las personas tales como la integridad corporal o la imagen y nadie puede inmiscuirse en la vida privada de una persona, ni violar áreas de su actividad no destinadas a ser difundidas, sin su consentimiento o el de sus familiares autorizados para ello y, salvo que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución de un crimen (de la doctrina del caso “Ponzetti de Balbín”)(14). Pues bien, este derecho es razonable recordar que en forma genérica encuentra su amparo en los artículos 19, 18, 43 y 75 inciso 22 de la Constitución Nacional”(15).

El derecho a la intimidad y privacidad también ha sido motivo de protección por los tratados internacionales con jerarquía constitucional (artículo 75 inciso 22 CN), tales como la Convención Americana sobre Derechos Humanos (artículo 11), el Pacto Internacional de Derechos Civiles y Políticos (artículo 17), la Declaración Universal de Derechos Humanos (artículo 12) y la Declaración Americana de los Derechos y Deberes del Hombre (artículo 5).

El verbo típico de la figura en estudio es “revelar”, lo cual implica dar a conocer a una o más personas una información que debía permanecer reservada, es decir, ponerla en conocimiento de quienes no se encontraban autorizados a acceder a ella(16).

En este marco, la relevancia penal del secreto profesional radica precisamente en la prohibición de divulgar aquella información conocida debido al ejercicio profesional. Se trata de evitar que quien ha accedido legítimamente a datos sensibles los exteriorice en violación del ámbito de reserva que justifica su conocimiento.

El ejercicio de la abogacía exige necesariamente que el profesional conozca situaciones y hechos que las personas consideran que deben quedar resguardadas en un ámbito de reserva y que son reveladas a fin de lograr precisamente una mejor tutela de aquellos intereses. La adecuada preparación de la defensa requiere el conocimiento pleno de los hechos, lo cual solo es posible si el cliente cuenta con la garantía de que la información proporcionada permanecerá confidencial.

El secreto del abogado reviste, por ello, carácter inviolable, no solo en interés del cliente, sino en el interés de toda la sociedad y en el resguardo de un correcto funcionamiento del sistema de justicia(17). Se funda en una relación de confianza indispensable para el ejercicio efectivo del derecho de defensa. Como advierte Pérez Cepeda, la lealtad para con la reserva es “la base fundamental y primaria de la figura delictiva”(18).

La información confiada al abogado puede referirse a la libertad, el honor, el patrimonio, la vida familiar o la estrategia de defensa del cliente. Por ello, la incriminación de su divulgación no responde sólo a un reproche ético, sino a la necesidad de resguardar jurídicamente la intimidad y la confianza sobre las que se construye la relación profesional(19).

En igual sentido, se ha dicho que “el secreto profesional del abogado pertenece a la categoría de los derechos humanos fundamentales, por ser esencial para el derecho de defensa y formar parte de la protección de la intimidad personal”(20).

Por otra parte, el tipo penal previsto en el artículo en análisis exige una conducta dolosa, es decir, el conocimiento por parte del sujeto activo del carácter secreto de la información y la voluntad de revelarla, lo que supone un obrar consciente y voluntario.

La mera revelación del secreto no resulta, por sí sola, suficiente para la configuración del tipo penal, en tanto la norma requiere que de dicha conducta pueda generarse un perjuicio, ya sea a la persona que confió la información al profesional o incluso para un tercero(21). El perjuicio puede ser tanto de naturaleza material como moral.

No obstante, no resulta necesario que el daño se produzca efectivamente, sino que basta la potencialidad de causarlo, en la medida en que el tipo penal se satisface con la puesta en peligro del bien jurídico protegido.

En cuanto al sujeto activo del delito, la obligación de guardar el secreto profesional recae sobre todos aquellos sujetos que, debido a su estado, oficio, profesión o empleo, hayan tomado conocimiento de hechos o circunstancias que, por su propia naturaleza, están destinados a permanecer reservados.

Ahora bien, el artículo 156 del CP no sanciona cualquier revelación de secretos, sino únicamente aquella realizada “sin justa causa”, lo que introduce un elemento normativo del tipo que opera como límite a la punibilidad. En efecto, la doctrina admite como justas causas de revelación: a) el consentimiento del titular del secreto; b) la defensa del interés propio o de terceros (artículo 34 incisos 6º y 7º CP); c) el ejercicio de un derecho (34 inciso 4º CP); y d) la obligación de denunciar ciertos hechos -ejemplo, los médicos tienen la obligación de denunciar nacimientos, defunciones, delitos perseguibles de oficio, etcétera(22).

En ese sentido, la conducta deviene atípica o exculpatoria cuando media el consentimiento del titular del secreto(23), en tanto desaparece la afectación al bien jurídico protegido, esto es, la intimidad de la persona que confió la información.

Tampoco resultará punible cuando la revelación se realice en ejercicio legítimo de un derecho, como puede ser la necesidad del profesional de defenderse frente a una imputación o de resguardar sus propios intereses jurídicos(24), supuesto en el cual el ordenamiento no puede imponer una obligación de reserva absoluta.

De igual modo, la doctrina admite que la revelación puede encontrarse justificada en situaciones de conflicto de intereses o estado de necesidad(25), cuando la preservación del secreto implique un riesgo grave para bienes jurídicos superiores, como la vida, la integridad física o la seguridad pública.

Asimismo, la revelación del secreto no será punible cuando se efectúe en cumplimiento de un deber legal impuesto por el ordenamiento jurídico, como ocurre en aquellos supuestos en los que la ley obliga a denunciar determinados hechos o a informar a la autoridad competente. En tales casos, la conducta no solo es lícita, sino exigida por el derecho(26).

El secreto profesional presenta una doble dimensión: constituye un deber frente al cliente y, simultáneamente, un derecho frente a terceros -incluidos los órganos jurisdiccionales-, en cuanto faculta al abogado a negarse a declarar sobre hechos amparados por dicho deber de reserva.

### 3.3. Código Procesal Penal.

Una última cuestión relevante es la situación del profesional que, hallándose en posesión de un secreto, es citado a prestar declaración testimonial y eventualmente “relevado” del deber de confidencialidad por el juez.

En tal sentido, corresponde señalar que el deber de comparecer se encuentra impuesto por el ordenamiento jurídico. En efecto, el artículo 243 del CP sanciona a quien, habiendo sido legalmente citado como testigo, se abstuviera de concurrir o de prestar declaración. Asimismo, el artículo 275 del citado cuerpo legal reprime al testigo que afirmare una falsedad o negare o callare la verdad en todo o en parte.

Al respecto, la doctrina contemporánea sostiene que se verifica un conflicto entre la obligación de guardar secreto que tiene el profesional y la obligación que tiene el mismo de atestiguar con veracidad(27).

Carrera por su parte, considera que es indudable que el juez no puede imponer la violación del secreto profesional(28); no hay mejor ni más juez que la propia conciencia del profesional convocado como testigo al juicio para pronunciarse sobre la naturaleza del hecho y la existencia de justa causa cuando la justicia exige su revelación(29). Es el profesional quien debe evaluar si existe o no justa causa para revelar algún secreto que le haya sido confiado debido a su profesión. Frente a ello, podrá optar el testigo por prestar declaración y manifestarse con verdad de todo cuanto supiere y le fuere preguntado, o bien, negarse a declarar amparándose en el deber de abstención que consagran los artículos 244 del CPPN y 160 del CPPF, para no cometer el delito previsto por el artículo 156 del CP(30). Esta solución se vincula, además, con la especial protección que el ordenamiento procesal penal reconoce a la relación entre imputado y defensor. En ese sentido, el artículo 197 del CPPN establece que, en la primera oportunidad -inclusive durante la prevención policial y, en todo caso, antes de la declaración indagatoria-, el juez debe invitar al imputado a elegir defensor. La misma norma dispone que el defensor podrá entrevistarse con su asistido inmediatamente antes de los actos previstos en los artículos 184, penúltimo párrafo, y 294 del CPPN, bajo pena de nulidad.

Por su parte, el artículo 65 inciso d) del CPPF, también otorga el derecho al imputado a ser asistido desde el primer acto del procedimiento por el defensor de su elección o por uno propuesto por una persona de confianza, o en su defecto, por un defensor público. De ello se desprende que la entrevista previa entre imputado y defensor son una garantía esencial del derecho de defensa. Su eficacia presupone necesariamente un ámbito de reserva, confianza y confidencialidad, sin el cual la defensa técnica perdería contenido real.

Asimismo, el artículo 237 del CPPN dispone que no podrán secuestrarse las cartas o documentos que se envíen o entreguen a los defensores para el desempeño de su cargo. Esta previsión confirma que la confidencialidad profesional no sólo protege las manifestaciones verbales efectuadas por el asistido a su abogado, sino también las comunicaciones, documentos y antecedentes entregados en función del ejercicio de la defensa. En igual sentido, el artículo 149 del CPPF protege las comunicaciones y notas que se crucen el imputado y sus defensores.

Los artículos citados impiden que el proceso penal utilice compulsivamente contra el imputado aquello que fue confiado al defensor para posibilitar una defensa eficaz. En consecuencia, refuerzan la conclusión de que el secreto profesional del abogado defensor se encuentra íntimamente ligado al derecho de defensa en juicio. Si el imputado tiene derecho a entrevistarse reservadamente con su defensor antes de actos procesales relevantes, y si los documentos remitidos o entregados al abogado para el desempeño de su cargo se encuentran excluidos de una orden de secuestro, entonces resulta coherente afirmar que el abogado no puede ser compelido a declarar sobre aquello que conoció precisamente en razón de esa relación profesional.

La doctrina también sostiene que el único que puede relevar al profesional que guarda el secreto de su obligación de mantenerlo, es la persona que se lo confió, no el juez(31). Sin perjuicio de lo señalado, frente a la circunstancia de que el juez releve al profesional del deber de confidencialidad, será el testigo quién decidirá

revelarlo o callarlo, pues sólo él puede determinar bajo qué circunstancias violará o no las reglas de ética que rigen su profesión. Es decir, que el relevamiento judicial no implica la imposición de una obligación de declarar sobre los hechos amparados por el secreto, sino únicamente la eliminación del obstáculo jurídico que impedía hacerlo. Dicho de otro modo, el relevamiento judicial autoriza la revelación, pero no la impone.

Por consiguiente, el profesional conserva la facultad de abstenerse de declarar en todos aquellos casos en los que, conforme a su leal saber y entender, considere que el secreto debe ser preservado. La decisión final queda, en este punto, sujeta a la valoración del propio testigo respecto de la existencia de una justa causa que legitime la revelación.

Parma ha señalado que la justa causa no genera necesariamente un deber jurídico de revelar, sino que su función consiste en excluir la tipicidad penal de la conducta. Por ello, aun mediando relevamiento judicial, el profesional podrá optar por no declarar si entiende que la confidencialidad debe prevalecer(32). Bajo estas condiciones, la eventual negativa a declarar no configura delito, siempre que el testigo actúe de buena fe y en la convicción de que el secreto debe ser mantenido. En tal supuesto, la ausencia de dolo excluye la responsabilidad penal(33). De este modo, la situación del abogado citado como testigo no difiere sustancialmente de la analizada en relación con el deber general de confidencialidad: el secreto profesional continúa operando como regla, y su revelación como excepción fundada en la existencia de una causa jurídicamente válida.

A ello debe agregarse que, tratándose del abogado defensor, la confidencialidad adquiere una dimensión constitucional y procesal específica, pues constituye una condición de posibilidad del derecho de defensa en juicio, de la entrevista reservada con el imputado y de la inviolabilidad de las comunicaciones y documentos entregados para el desempeño del cargo.

#### 3.4. Regulación del Ejercicio Profesional de la Abogacía (Leyes 23.187 y 5.177)

Por su parte, la Ley 23.187 -que regula el ejercicio de la abogacía en la Capital Federal-establece expresamente el deber de guardar secreto profesional, incluso después de finalizada la relación con el cliente. Este deber no sólo protege al cliente, sino que resguarda la integridad del sistema de administración de justicia.

En términos normativos concretos, la Ley 23.187 impone al abogado el deber de “observar con fidelidad el secreto profesional, salvo autorización fehaciente del interesado” (artículo 6, inciso f), mientras que el Código de Ética del Colegio Público admite su revelación únicamente cuando exista autorización del cliente o se trate de la propia defensa del profesional (artículo 11, inciso h)(34). Este esquema confirma que la regla es la reserva y que sus excepciones son de interpretación estricta(35).

En la Provincia de Buenos Aires, la Ley 5.177/54 (texto ordenado por el Decreto 2885/01 con las modificaciones introducidas por la Ley 13419), que regula el ejercicio de la abogacía, en su artículo 59, inciso 6) dispone que el abogado debe “guardar secreto profesional respecto de los hechos que ha conocido con motivo del asunto que se le hubiere encomendado o consultado, con las salvedades establecidas por la Ley”.

Por lo expuesto, al igual que lo sostuvo D´Albora(36) es inconcebible la declaración del abogado en el cumplimiento de su ministerio; si se desconociese este límite se coloca a dichos profesionales frente a la alternativa de violar el secreto o desobedecer la orden judicial.

#### 3.5. Ley 25.326 de Protección de Datos Personales

Desde la perspectiva de la protección de datos personales, la Ley 25.326 introduce un marco normativo que, aun cuando no regula específicamente el uso de IAGen en el ejercicio de la abogacía, resulta plenamente aplicable a los tratamientos de información que los profesionales realicen en ese contexto.

La ley establece principios rectores que imponen que los datos personales sean tratados de manera leal, lícita y adecuada a la finalidad para la cual fueron recolectados, así como también que se adopten las medidas necesarias para garantizar su seguridad y confidencialidad. En particular, adquiere especial relevancia el deber de seguridad de los datos previsto en el artículo 9(37), que obliga a los responsables o usuarios del archivo de datos a adoptar las medidas técnicas y organizativas necesarias para evitar su adulteración, pérdida, consulta o tratamiento no autorizado.

A su vez, el artículo 10 exige el deber de confidencialidad, donde el responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de estos. Incluso, tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. Respecto a la revelación del secreto, lo contempla en los casos de resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública(38). En este marco, la actividad del abogado se encuentra directamente alcanzada por estas disposiciones, en tanto el ejercicio profesional implica, de manera habitual, el tratamiento de datos personales -muchas veces de carácter sensible- vinculados a la vida privada, patrimonial y jurídica de sus clientes.

La utilización de herramientas basadas en IAGen introduce, en este contexto, un factor de riesgo adicional. Ello así, en tanto el procesamiento automatizado de información puede implicar: la transferencia de datos a servidores de terceros, el almacenamiento en infraestructuras ajenas al control directo del profesional, y la

eventual reutilización de la información con fines distintos a aquellos para los cuales fue originalmente proporcionada.

En consecuencia, el uso de estas tecnologías exige extremar los recaudos de confidencialidad, ya que una gestión inadecuada de los datos podría no solo vulnerar las disposiciones de la Ley 25.326, sino también comprometer el secreto profesional del abogado, afectando directamente la relación de confianza con el cliente.

Asimismo, debe considerarse que, tratándose de datos sensibles -en los términos del artículo 2 de la ley(39)-, el estándar de protección se intensifica, requiriéndose un tratamiento aún más restrictivo, en tanto se trata de información que puede dar lugar a discriminación o afectar gravemente la esfera íntima del titular.

De este modo, la interacción entre la normativa de protección de datos personales y el deber de secreto profesional pone de manifiesto que el abogado no solo debe abstenerse de revelar información confidencial, sino también garantizar que los sistemas y herramientas que utilice no generen filtraciones, accesos indebidos o tratamientos incompatibles con la finalidad para la cual los datos fueron confiados.

En definitiva, aun en ausencia de una regulación específica sobre IAGen aplicada al ejercicio profesional, la Ley 25.326 proporciona un marco normativo para exigir al abogado un estándar elevado de diligencia en el tratamiento de la información, reforzando -desde una perspectiva tecnológica- la vigencia del deber de confidencialidad que rige su actuación.

### 3.6. Concepción amplia del secreto profesional. Actividad cognitiva defensiva

A través del juego armónico de los artículos 18, 19 y 75 inciso 22 de la CN, citados precedentemente, se garantiza el derecho de defensa del ciudadano, se tutelan libertades, garantías individuales y derechos constitucionales. El derecho a obtener la tutela efectiva de jueces y tribunales es un derecho fundamental y para hacerlo efectivo la Constitución reconoce y protege el derecho de defensa del ciudadano, así como la prohibición de obligarlo a declarar contra sí mismo, garantizando que los abogados puedan cumplir con su labor.

En ese sentido, la inviolabilidad de la correspondencia y de los papeles privados (artículo 18 CN), no se limita a resguardar documentos en sentido material, sino que delimita un verdadero ámbito de reserva a injerencias externas. Se trata de preservar todos aquellos espacios en los que el individuo -y, en particular, el abogado en el ejercicio de la defensa- desarrolla su actividad intelectual, estratégica y comunicacional.

Desde esta perspectiva, los papeles de trabajo del abogado -entendidos como borradores, notas, esquemas argumentales, líneas de estrategia y registros de análisis jurídico- constituyen una manifestación directa de dicha esfera protegida.

En ese orden, el artículo 237 del CPCCN consagra una regla de resguardo especial al impedir el secuestro de la correspondencia o documentos dirigidos o entregados a los defensores para el desempeño de su cargo, al igual que el artículo 149 del CPPF respecto a las comunicaciones y notas. Tales previsiones garantizan la intangibilidad del espacio de preparación de la defensa.

Por ello, la protección alcanza no sólo a las comunicaciones entre abogado y defendido-incluidas las realizadas por medios telefónicos y correo electrónico-, sino también a todos aquellos instrumentos que permitan construir la estrategia defensiva.

Su eventual revelación no implicaría simplemente el acceso a información, sino la exposición anticipada de la estrategia de la defensa, con la consiguiente afectación sustancial del derecho de defensa en juicio. En otros términos, vulnerar estos papeles de trabajo equivale a desarticular el proceso de construcción de la defensa(40).

Lo expuesto permite concluir que lo relevante no es el soporte o canal de la interacción, sino su función dentro del proceso defensivo. Las citadas comunicaciones son consideradas inviolables no por su forma, sino porque en ellas se desarrolla -entre otras cosas- la estrategia, el análisis jurídico y la construcción del caso. La inviolabilidad de las comunicaciones, en ese sentido, actúa como presupuesto indispensable del secreto profesional, en tanto garantiza un intercambio libre, confidencial y exento de interferencias, sin el cual el derecho de defensa quedaría vacío de contenido(41).

De este modo, la tutela constitucional de la correspondencia, de los papeles privados y de la defensa en juicio, se complementan con el secreto profesional del abogado. Se trata de asegurar la igualdad de armas y la efectividad de la defensa en juicio. Cualquier intromisión en ese ámbito -sea mediante la exigencia de declaraciones, la interceptación de comunicaciones o el acceso a documentos de trabajo- importa, en los hechos, una vía indirecta de vulneración del derecho a no autoincriminarse(42) y del principio de defensa material(43).

En este contexto, la interacción del abogado o del imputado con sistemas de IAGen presenta una analogía con los papeles de trabajo y los medios de comunicación entre abogado y cliente precedentemente desarrollados, en tanto también constituye un espacio de elaboración cognitiva en el que se ensayan hipótesis, se organizan argumentos y se proyectan líneas defensivas. En consecuencia, así como las comunicaciones telefónicas y correos electrónicos(44) han sido reconocidas como parte del ámbito protegido del secreto profesional, cabe sostener que determinadas interacciones con herramientas de IAGen -bajo condiciones adecuadas de confidencialidad y

control- pueden integrar la esfera de la actividad cognitiva defensiva, sin que su sola mediación tecnológica implique la pérdida automática de dicha protección.

Por consiguiente, si se admite que la actividad cognitiva del abogado y del imputado forma parte del ámbito protegido -como ocurre con las comunicaciones entre ellos vinculadas a la defensa-, entonces los contenidos generados mediante IAGen podrían quedar comprendidos dentro de esta esfera, siempre que no se haya producido una pérdida efectiva de confidencialidad.

No obstante, esta conclusión no está exenta de tensiones. Al respecto, la guía práctica del CPACF refuerza este razonamiento al advertir que el abogado debe evitar cargar datos sensibles en herramientas sin garantías y que la IAGen no exime de responsabilidad(45). También recuerda que el profesional debe validar todo el contenido generado, detectar posibles sesgos o alucinaciones y ejercer siempre supervisión humana suficiente. Por eso, más que una incompatibilidad absoluta entre IAGen y secreto profesional, lo que emerge es un deber reforzado de diligencia en la selección de la herramienta, en el modo de uso y en el control posterior del resultado.

La utilización de estos sistemas implica en muchos casos, la transferencia de información a servidores externos, lo que podría ser interpretado como una divulgación a terceros. En tal caso, cabría preguntarse si se mantiene la protección del secreto profesional o si, por el contrario, se configura una renuncia implícita a la confidencialidad.

La respuesta a este interrogante requiere adoptar un enfoque funcional. No toda intervención de un tercero implica necesariamente la pérdida del secreto. Así ocurre, por ejemplo, con los auxiliares del abogado, quienes pueden acceder a la información sin que ello afecte la confidencialidad, en la medida en que actúan bajo su control.

En ese orden, el análisis de las políticas de privacidad y condiciones de uso de diversas plataformas de IA permite advertir la existencia de límites concretos en el tratamiento de los datos ingresados, en tanto su utilización se encuentra generalmente circunscripta a la prestación y mejora del servicio.

Asimismo, en determinados supuestos -especialmente en entornos configurables o empresariales- se prevén restricciones en la reutilización de dicha información para el entrenamiento de modelos, así como mecanismos técnicos y organizativos orientados a la protección de los datos personales y/o sensibles, tales como cifrado, control de acceso y medidas de seguridad. Estas características refuerzan la posibilidad de considerar a tales sistemas, bajo ciertas condiciones, como herramientas que deben estar supervisadas por el profesional.

A título ilustrativo, plataformas como ChatGPT u otras herramientas de IAGen cuentan con sus propias políticas de privacidad, cuya aceptación implica el sometimiento a determinados términos y condiciones, lo que conlleva el riesgo de que la información compartida pueda ser recopilada y utilizada con diferentes fines(46).

Por otro lado, desarrollos específicos del ámbito jurídico, como el sistema “Sherlock Legal” implementado por el portal ELDial.com, han sido diseñados sobre modelos de IA con información controlada y provista por la propia empresa, lo que incrementa el nivel de seguridad respecto de las fuentes utilizadas y de los datos procesados(47).

En definitiva, el secreto profesional en el derecho argentino debe ser interpretado de manera dinámica, de modo de adaptarse a los cambios tecnológicos. Ello implica reconocer que la IAGen no puede ser considerada, sin más, como un tercero que excluye la protección, sino que su impacto debe ser evaluado en función de las circunstancias concretas de cada caso y teniendo en cuenta que es una herramienta de utilidad para el operador judicial.

#### **4. Análisis del caso United Satetes v. Bradley Hepper**

El caso United States v. Bradley Heppner (SDNY, 2026)(48) reviste singular trascendencia porque constituye uno de los primeros precedentes judiciales en abordar de manera directa la relación entre IAGen y los institutos clásicos de confidencialidad jurídica. Su relevancia no se agota en el resultado al que arriba el tribunal, sino que se proyecta sobre el razonamiento empleado para negar tutela a las interacciones mantenidas por el imputado con una plataforma de IAGen. En ese sentido, el fallo permite advertir cómo las categorías tradicionales del privilegio abogado-cliente y de la work product doctrine comienzan a ser tensionadas por nuevas formas de producción, circulación y tratamiento de la información jurídica.

Lejos de consagrar una adaptación flexible de esas garantías al entorno digital, la decisión adopta una lectura estricta de sus presupuestos clásicos. El tribunal parte de la premisa de que la novedad tecnológica no altera por sí sola las reglas que gobiernan la confidencialidad. Así, aunque reconoce que la IAGen representa una nueva frontera en el diálogo entre derecho y tecnología, concluye que su utilización no justifica crear una categoría autónoma de protección ni flexibilizar los requisitos tradicionales del privilegio. En palabras del propio juez Rakoff, el uso de IAGen “no significa que quede sustraído a los principios jurídicos de larga data” que rigen el privilegio abogado-cliente y el producto del trabajo.

##### **4.1. Hechos relevantes.**

Según surge del memorándum, Bradley Heppner fue acusado de fraude de valores, fraude electrónico, conspiración y falsedad en registros societarios, en el contexto de maniobras vinculadas a empresas controladas por él. Tras su arresto, el FBI ejecutó una orden de allanamiento en su domicilio y secuestró documentación y

dispositivos electrónicos. Entre los materiales incautados se encontraban documentos que reflejaban comunicaciones entre Heppner y la plataforma de IA “Claude”, operada por Anthropic. Dichos intercambios habían tenido lugar en 2025, luego de que el imputado recibiera una citación del gran jurado y cuando ya estaba claro que era objeto de una investigación federal.

La defensa sostuvo que esos documentos formaban parte de la preparación de la estrategia defensiva. Afirmó que Heppner había introducido en Claude información obtenida de sus abogados, había utilizado la herramienta con el propósito de analizar su situación y de preparar argumentos para su defensa, y posteriormente había compartido con su letrado el contenido producido. Con base en ello, invocó dos fuentes de protección: por un lado, el attorney-client privilege; por el otro, la work product doctrine. El tribunal rechazó ambos planteos.

Este marco fáctico resulta central, porque el caso no versa sobre una utilización tangencial o recreativa de IA, sino sobre un uso directamente conectado con un proceso penal en curso y con la elaboración de posibles líneas de defensa. Precisamente por ello el fallo adquiere un valor paradigmático: obliga a preguntarse si la utilización de una herramienta tecnológica en la preparación de la defensa debe o no recibir el mismo nivel de tutela que otras formas modernas de asistencia instrumental.

#### 4.2. Fundamentos del tribunal

La decisión se articula sobre tres ejes principales: la inexistencia de una relación abogado-cliente entre el imputado y la plataforma, la ausencia de una expectativa razonable de confidencialidad, y la improcedencia de la work product doctrine respecto del material generado. Seguidamente, se analizarán cada uno de ellos.

##### A) Inexistencia de relación abogado-cliente.

El tribunal destaca que el privilegio abogado-cliente protege únicamente comunicaciones confidenciales entre cliente y abogado, efectuadas con el propósito de obtener o brindar asesoramiento jurídico. Añade además que se trata de una excepción a la regla general de producción de prueba relevante y, por ello, debe interpretarse restrictivamente. Sobre esa base, entiende que los documentos cuestionados no satisfacen al menos dos de los requisitos básicos del privilegio.

El primer obstáculo es ontológico y profesional: Claude no es un abogado. El tribunal afirma de modo terminante que entre Heppner y la IA no existió ni podía existir una relación abogado-cliente, y que las discusiones sobre cuestiones legales mantenidas con un sistema no habilitado para ejercer el derecho no se encuentran cubiertas por el privilegio. Señala incluso que, dado que Anthropic niega expresamente que Claude proporcione asesoramiento legal, resultaría impropio asimilar sus respuestas a consejo jurídico profesional. El juez destaca que, cuando el Gobierno le preguntó a Claude si podía dar asesoramiento legal, la propia herramienta respondió que no era abogada y que no podía brindar asesoramiento o recomendaciones legales formales.

Este punto es decisivo en las argumentaciones del fallo. Para el tribunal, no basta con que la comunicación verse sobre asuntos jurídicos ni con que posteriormente sea remitida al abogado defensor; es indispensable que la interacción privilegiada se produzca con un profesional del derecho o, en su caso, con un agente suyo actuando dentro de una relación de confianza jurídicamente protegida. Como la plataforma Claude no reúne ninguna de esas condiciones, el privilegio no nace.

##### B) Ausencia de expectativa razonable de confidencialidad

El segundo fundamento reside en la falta de confidencialidad. El tribunal subraya que, aun dejando de lado la inexistencia de una relación abogado-cliente, los intercambios con Claude tampoco fueron confidenciales. Y ello no sólo porque interviniera un tercero - Anthropic-, sino porque la propia política de privacidad de la plataforma advertía que los datos ingresados por el usuario podían ser recolectados, utilizados para entrenar el sistema y divulgados a proveedores externos, autoridades gubernamentales regulatorias o terceros en determinados supuestos. El memorándum remarca que esa política claramente ponía al usuario en conocimiento de que no podía reclamar privacidad sobre tales datos frente a demandas o litigios.

A partir de ello, el tribunal concluye que Heppner no podía albergar una expectativa razonable de confidencialidad respecto de sus comunicaciones con Claude. Ergo: cuando una persona revela voluntariamente información a una entidad externa sometida a condiciones contractuales que prevén tratamiento y eventual divulgación de los datos, se quiebra uno de los presupuestos esenciales del privilegio. El fallo refuerza esta idea citando jurisprudencia reciente en materia de plataformas digitales de acceso público, en la que se sostuvo que los usuarios no tienen intereses sustanciales de privacidad cuando revelan voluntariamente sus comunicaciones a una plataforma que las almacena en el curso ordinario de sus negocios.

El razonamiento del juez es especialmente severo al señalar que los documentos no se transforman “alquímicamente” en privilegiados por el solo hecho de haber sido luego compartidos con un abogado. Si el intercambio no fue confidencial en su origen, su posterior remisión al defensor no sana ese defecto inicial ni altera su naturaleza probatoria.

##### C) Rechazo de la work product doctrine

El tribunal también descarta la aplicabilidad de la work product doctrine. Recuerda que esta doctrina protege materiales preparados por o para un abogado, o por su agente, en anticipación a un litigio o juicio, y que su finalidad consiste en preservar los procesos mentales del abogado, otorgándole un ámbito de privacidad para desarrollar teoría del caso, estrategia y análisis probatorio.

Sin embargo, entiende que los documentos generados por Heppner mediante el uso de Claude no reúnen esos recaudos. Aunque pudieran haber sido elaborados en un contexto de investigación penal y, por tanto, con un litigio razonablemente previsible, no fueron preparados por el abogado ni a pedido suyo, ni tampoco reflejaban la estrategia del defensor al momento de su creación. Por el contrario, fueron producidos por el propio imputado por iniciativa propia, sin dirección de su letrado. El fallo enfatiza que el propio abogado de Heppner reconoció que no había instruido al cliente a realizar búsquedas en Claude. Esa admisión debilita de modo definitivo el argumento de que la IA hubiera actuado como una extensión operativa del trabajo del defensor.

En esta parte, la sentencia delimita con precisión el núcleo de la doctrina: lo protegido no es cualquier documento subjetivamente vinculado a la defensa, sino aquellos materiales que expresan, resguardan o facilitan el trabajo intelectual del abogado. De allí que el juez rechace la idea de ampliar la protección a documentos creados autónomamente por el acusado sólo porque más tarde fueron remitidos a su defensor.

#### 4.3. Críticas al fallo

Aunque la decisión presenta una estructura lógica consistente dentro del marco doctrinal norteamericano tradicional, su fundamentación exhibe límites importantes si se la examina desde una perspectiva funcional y garantista, especialmente en el contexto actual de digitalización incluso de los expedientes judiciales.

El primer punto discutible del fallo radica en su fuerte formalismo. El tribunal centra el análisis en la identidad del interlocutor -si es o no abogado- y no en la función que la herramienta cumple dentro del proceso de preparación de la defensa. Desde luego, es correcto afirmar que una IA o la IAGen no es abogada ni puede equipararse sin más a un profesional habilitado. Pero de ello no se sigue necesariamente que todo contenido generado con su auxilio quede automáticamente excluido de cualquier tutela reforzada. El problema no reside únicamente en quién emite la respuesta, sino en para qué se utiliza la herramienta y en qué condiciones se integra al trabajo defensivo. En la actualidad, abogados y clientes emplean softwares de búsqueda, análisis documental, revisión de contratos, organización probatoria y síntesis de información. Si el criterio decisivo fuera exclusivamente la ausencia de una persona humana investida de título profesional en el otro extremo de la interacción, podría llegarse a una contracción excesiva del ámbito de protección, incompatible con las condiciones reales en que hoy se desarrolla buena parte del trabajo jurídico.

##### A) Concepto rígido de “tercero”

También resulta discutible la noción de “tercero” que maneja la sentencia en estudio. El tribunal trata a la plataforma como un tercero externo en un sentido muy próximo al de la divulgación a otra persona o entidad ajena a la relación de la defensa. Sin embargo, la IAGen no se comporta exactamente como un tercero humano dotado de voluntad, interés autónomo o capacidad propia de explotar el contenido recibido. Es, antes bien, una infraestructura tecnológica operada por un proveedor, cuyo grado de exterioridad dependerá de variables técnicas y contractuales concretas: arquitectura del sistema, condiciones de retención, uso para entrenamiento, cifrado, posibilidad de entornos cerrados o empresariales, control de acceso, entre otras.

En el caso Heppner, ese análisis estricto prácticamente no aparece: el tribunal se apoya en la política de privacidad de Claude y en la posibilidad de divulgación para concluir que la confidencialidad se perdió. Esa conclusión puede ser correcta para esa plataforma concreta y bajo esas condiciones específicas, pero no necesariamente permite generalizar un criterio absoluto respecto de toda herramienta similar. El verdadero problema jurídico quizá no sea la IA en sí misma, sino la forma específica en que se instrumenta su uso y el régimen de datos que lo acompaña.

##### B) Deficiente diferenciación entre herramienta tecnológica y divulgación.

El fallo parece asumir que ingresar información en un sistema de IA equivale, sin más, a revelarla a un tercero. Ese paralelismo, aunque comprensible, simplifica una realidad tecnológica más compleja. Muchas herramientas digitales funcionan a través de servidores remotos, almacenamiento en nube, procesamiento automatizado y servicios externalizados. Si toda mediación técnica implicara automáticamente destrucción de la confidencialidad, buena parte de la práctica jurídica contemporánea quedaría estructuralmente desprotegida.

Por supuesto, no toda herramienta merece el mismo tratamiento. Pero justamente por eso el análisis debería ser más exhaustivo. Sería posible distinguir, por ejemplo, entre plataformas abiertas de consumo masivo cuyas condiciones prevén utilización amplia de datos (ChatGPT), y entornos cerrados o profesionales diseñados específicamente para preservar reserva, limitar retención y excluir reutilización (ELDial.com). El fallo no ensaya esa diferenciación, sino que adopta una solución categórica fundada en los hechos del caso.

##### C) Alcance restrictivo de la work product doctrine

La negativa a aplicar la work product doctrine también admite críticas. El tribunal acierta al recordar que la doctrina protege prioritariamente los procesos mentales del abogado y no toda producción privada del cliente.

Pero podría discutirse si, en ciertos supuestos, una herramienta utilizada como apoyo técnico en la elaboración de borradores, hipótesis o matrices argumentales por parte del imputado, para ser trabajadas luego con el defensor no debería ser vista funcionalmente como parte del proceso de preparación del caso.

En Heppner, el obstáculo fue claro: el imputado actuó por su cuenta, sin instrucciones del abogado, y el contenido no reflejaba estrategia letrada ya definida. Bajo esos hechos, la negativa resulta defendible. No obstante, el propio razonamiento del tribunal deja abierta una pregunta relevante para futuros casos: ¿qué ocurriría si la plataforma hubiera sido utilizada por indicación concreta del abogado, dentro de un entorno técnicamente seguro y como instrumento de apoyo en la preparación del caso? El fallo no resuelve esa hipótesis; sólo decide que, en las circunstancias examinadas, esos presupuestos no se verificaron.

#### 4.4. Valoración.

El precedente Heppner constituye un punto de partida relevante. Su principal mérito consiste en haber visibilizado con claridad que la utilización de IAGen dentro del ámbito de la defensa no puede analizarse al margen de las categorías clásicas del privilegio y de la teoría del producto del trabajo. En ese aspecto, el fallo: recuerda que la novedad tecnológica no suspende los requisitos jurídicos tradicionales ni habilita, por sí sola, una expansión automática de la confidencialidad.

Sin embargo, su alcance también es limitado. La sentencia resuelve un caso concreto marcado por circunstancias particularmente desfavorables para la defensa: uso autónomo de la herramienta por parte del imputado, ausencia de directivas del abogado, plataforma pública de terceros y condiciones de privacidad incompatibles con una expectativa de reserva. Por ello, el valor del precedente debe ser analizado con cautela. Más que establecer una regla general sobre toda interacción entre abogados, clientes e IAGen, el fallo demuestra que no cualquier uso de esta tecnología puede aspirar a quedar protegido. Desde una perspectiva más amplia, la decisión invita a formular la siguiente conclusión: la tutela de la confidencialidad en entornos de IAGen no dependerá únicamente del contenido de la comunicación, sino también del diseño institucional y técnico del canal utilizado. Allí se abre el verdadero desafío contemporáneo. La pregunta ya no es sólo si la IA puede o no intervenir en la preparación de la defensa, sino en qué condiciones normativas, contractuales y tecnológicas esa intervención podría compatibilizarse con el secreto profesional y con las garantías del debido proceso.

En definitiva, Heppner no clausura el debate; apenas lo inaugura. Su enseñanza central es negativa pero valiosa: la IA no crea una zona inmune al escrutinio judicial ni reemplaza los requisitos clásicos del privilegio. Al mismo tiempo, deja planteada la necesidad de construir criterios más específicos para distinguir entre usos incompatibles con la confidencialidad y usos técnicamente controlados que, integren la labor defensiva, que podrían merecer una protección diferenciada en el futuro.

### 5. Análisis comparado: derecho argentino y estadounidense

#### 5.1. Naturaleza jurídica de la protección: privilegio vs. garantía constitucional

El contraste entre el derecho estadounidense y el argentino revela una diferencia estructural que condiciona todo el análisis posterior. En el sistema norteamericano, el attorney-client privilege se configura primordialmente como una regla de exclusión probatoria<sup>(49)</sup>. Su función es impedir que determinadas comunicaciones ingresen al proceso como prueba, en tanto ello podría desalentar la franqueza del cliente. En consecuencia, su interpretación es restrictiva, al tratarse de una excepción al principio de amplitud probatoria, y su aplicación depende del cumplimiento estricto de requisitos formales: relación abogado-cliente, confidencialidad y finalidad jurídica de la comunicación.

Por el contrario, en el derecho argentino el secreto profesional no se agota en una dimensión probatoria, sino que se encuentra directamente anclado en la garantía constitucional de defensa en juicio (artículo 18 CN), así como en la inviolabilidad de la correspondencia y de los papeles privados y el derecho a la intimidad (artículo 19 CN). Esto implica que su función excede la mera exclusión de prueba: constituye una condición fundamental del debido proceso.

La diferencia no es meramente técnica, sino ontológica. Mientras que en el modelo estadounidense la protección opera como un límite a la actividad probatoria del Estado, en el sistema argentino configura un ámbito necesario para la construcción de la defensa. De allí que su vulneración no genere únicamente un problema de admisibilidad, sino una afectación directa de garantías constitucionales.

#### 5.2. Alcance del secreto profesional en ambos sistemas

En línea con lo anterior, el alcance de la protección también difiere sustancialmente. En el derecho estadounidense, el privilegio se circunscribe a comunicaciones específicas entre abogado y cliente, bajo condiciones estrictas de confidencialidad. Quedan fuera de su ámbito tanto las interacciones con terceros como los materiales que no cumplan con los requisitos formales exigidos.

El derecho argentino, en cambio, adopta una concepción amplia y funcional del secreto profesional. No sólo protege las comunicaciones, sino también el proceso de elaboración de la defensa. Esto incluye los papeles de trabajo, las estrategias, los borradores y, en general, toda actividad cognitiva orientada a la construcción del caso.

Desde esta perspectiva, la confidencialidad no se limita al intercambio comunicacional, sino que abarca el espacio intelectual en el que se desarrolla la defensa técnica. En consecuencia, el eje de protección se desplaza desde la forma hacia la función: lo relevante no es el canal o soporte utilizado, sino su integración en la actividad defensiva(50).

### 5.3. Tratamiento de la inteligencia artificial en ambos países

Las diferencias estructurales señaladas se proyectan directamente en el modo en que cada sistema aborda la utilización de la IA.

En el precedente *United States v. Bradley Heppner*, el tribunal estadounidense adopta un enfoque formalista. La IA es considerada un tercero ajeno a la relación abogado-cliente, lo que excluye automáticamente la aplicación del privilegio. Asimismo, la existencia de políticas de privacidad que permiten el tratamiento de datos impide reconocer una expectativa razonable de confidencialidad. Bajo este esquema, la intervención tecnológica opera como un factor de ruptura de la protección.

En el derecho argentino, en cambio, la cuestión debe abordarse desde un enfoque más funcional. La IA no puede ser considerada, sin más, como un tercero en sentido jurídico relevante. Su tratamiento dependerá de las condiciones concretas de uso, del grado de control ejercido por el profesional y de la existencia o no de una pérdida efectiva de confidencialidad.

Así, cuando la IA se integra al proceso de elaboración de la defensa -como herramienta de análisis, organización o generación de hipótesis-, puede ser asimilada a otros instrumentos técnicos tradicionalmente utilizados en la práctica jurídica. En este marco, su utilización no implica necesariamente una renuncia al secreto profesional, sino que activa un deber reforzado de diligencia en la protección de la información.

Asimismo, esta interpretación se ve reforzada por el derecho a la no autoincriminación consagrado en el artículo 18 de la Constitución Nacional y en los tratados internacionales con jerarquía constitucional (artículo 75 inciso 22)(51). Desde esta óptica, los materiales generados por el imputado en el marco de la preparación de su defensa -incluidos aquellos producidos mediante IAGen- pueden ser concebidos como una extensión de su actividad intelectual, lo que justifica su protección frente a eventuales medidas de secuestro o incorporación probatoria(52).

En otro orden, la garantía de la inviolabilidad de los Estudios Jurídicos, así como de los documentos confiados al abogado para su asesoramiento prevista por el artículo 7 de la Ley 23.187 refuerzan la protección del derecho argentino.

En consecuencia, los documentos generados por IAGen por parte del cliente podrían considerarse amparados por formar parte de la defensa(53).

### 5.4. Proyección del caso Heppner en el derecho argentino

La recepción del criterio adoptado en el caso *United States v. Bradley Heppner* en el derecho argentino no puede realizarse de manera automática. Las diferencias en la naturaleza y alcance de la protección imponen una lectura crítica del precedente.

Si se trasladara sin matices el razonamiento del tribunal estadounidense, se correría el riesgo de restringir de manera indebida el ámbito del secreto profesional, afectando directamente la garantía de defensa en juicio. En particular, la equiparación entre uso de IAGen y divulgación a terceros resultaría problemática en un sistema que protege no sólo la comunicación, sino también la actividad cognitiva defensiva.

No obstante, el caso ofrece elementos valiosos como advertencia. En particular, pone de relieve que la protección no es absoluta y que puede perderse cuando se verifica una exposición relevante de la información, ya sea por el uso de plataformas sin garantías adecuadas o por la ausencia de control sobre el tratamiento de los datos.

En este sentido, el precedente Heppner, enseña que no todo uso de IAGen en el ámbito de la defensa será protegido. La clave, en el derecho argentino, residirá en determinar si la utilización de la herramienta se realizó bajo condiciones que preserven la confidencialidad y la integridad del proceso defensivo.

En definitiva, la proyección del caso en el ámbito local no conduce a la exclusión automática de la protección, sino a la necesidad de desarrollar criterios propios que permitan compatibilizar el uso de tecnologías emergentes con las exigencias del Estado de Derecho.

## 6. Consecuencias probatorias y reglas de admisibilidad

### 6.1. Prueba generada mediante inteligencia artificial

La irrupción de la IAGen introduce una categoría probatoria novedosa cuya calificación jurídica no puede resolverse mediante esquemas tradicionales rígidos. En efecto, los contenidos generados mediante IA no constituyen prueba en sentido clásico, sino que deben ser analizados en función de su origen, finalidad y grado de integración en la actividad procesal.

En el ámbito penal argentino, corresponde distinguir entre dos supuestos. Por un lado, aquellos contenidos generados con fines externos al proceso -por ejemplo, documentos producidos por terceros o información obtenida mediante IA como fuente autónoma-, que pueden ser considerados prueba documental o indiciaria, sujeta a las reglas generales de su incorporación.

Por otro lado, los contenidos generados en el marco de la preparación de la defensa técnica -esto es, como parte de la actividad cognitiva del imputado o su abogado- no constituyen prueba en sentido estricto, sino manifestaciones del proceso de elaboración defensiva. En este último supuesto, su eventual incorporación al proceso debe ser examinada con criterio restrictivo, en tanto su divulgación puede implicar la exposición de la estrategia de defensa.

En consecuencia, la prueba generada mediante IAGen no admite una calificación uniforme: su naturaleza dependerá de su función concreta dentro del proceso.

## 6.2. Criterios de admisibilidad y fiabilidad

La admisibilidad de los contenidos generados mediante IAGen exige la aplicación de estándares reforzados de control, tanto en términos de legalidad como de fiabilidad.

En primer lugar, desde el punto de vista de la admisibilidad formal, deberá verificarse que la obtención del contenido no haya implicado la vulneración de garantías constitucionales, en particular el secreto profesional y el derecho de defensa en juicio. En este sentido, no todo contenido técnicamente accesible resulta jurídicamente admisible. En segundo lugar, desde la perspectiva de la fiabilidad, la prueba generada mediante IAGen presenta desafíos específicos derivados de su funcionamiento. Los sistemas de IAGen operan sobre modelos probabilísticos y, en muchos casos, se dificulta la trazabilidad del razonamiento que conduce al resultado. Ello obliga a extremar los recaudos en la valoración judicial.

Entre los criterios relevantes pueden señalarse: la identificación de la herramienta utilizada, el análisis de sus condiciones de uso, la verificación de la integridad del contenido, la posibilidad de replicación del resultado y la existencia de corroboración externa mediante otros medios probatorios.

De este modo, la IAGen no puede ser considerada una fuente de verdad autónoma, sino un instrumento cuyo resultado debe ser sometido a control crítico. La valoración judicial no puede descansar en la apariencia de objetividad tecnológica, sino en la consistencia y verificabilidad del contenido producido.

## 6.3. Relación con la doctrina de la prueba ilícita

La interacción entre IAGen y secreto profesional adquiere particular relevancia a la luz de la doctrina de la prueba ilícita.

En ese orden, en el derecho argentino, rige el principio según el cual toda prueba obtenida con violación de garantías constitucionales resulta inadmisibles, así como también aquellas que constituyen su derivación (doctrina del “fruto del árbol venenoso”). Este principio se proyecta directamente sobre los contenidos generados mediante IAGen cuando su obtención implica una afectación ilegítima de la confidencialidad.

Es así como, si la información utilizada por un sistema de IAGen proviene de comunicaciones protegidas por el secreto profesional o de la actividad cognitiva defensiva, su incorporación al proceso puede resultar inválida. La exclusión no debe limitarse al contenido obtenido de manera directa, sino que se extiende también a cualquier evidencia derivada de dicha vulneración.

A diferencia del enfoque adoptado en el caso *United States v. Bradley Heppner*, donde el análisis se centra en la ausencia de privilegio, el derecho argentino impone un examen más amplio, orientado a determinar si se ha producido una afectación del derecho de defensa.

Un supuesto particularmente complejo se presenta cuando la Fiscalía obtiene la información mediante la producción de prueba informativa dirigida directamente a la empresa proveedora del sistema de IA. En estos casos, la exclusión probatoria se torna más difícil de sostener, especialmente si la obtención se realizó con orden judicial y dentro del marco de los términos y condiciones aceptados por el usuario. Sin embargo, ello no agota el análisis.

La defensa podrá sostener la inadmisibilidad de la prueba sobre la base de la violación del derecho a la intimidad, la afectación del derecho de defensa y la aplicación de la doctrina del “fruto del árbol venenoso”<sup>(54)</sup>. En particular, deberá destacarse que el acceso a este tipo de información puede implicar una injerencia indirecta en la actividad cognitiva defensiva, en tanto permite reconstruir el razonamiento, las hipótesis o las líneas estratégicas del imputado.

Ahora bien, si las condiciones de uso de la plataforma autorizaban el tratamiento y eventual cesión de los datos -como ocurrió en el caso *United States v. Bradley Heppner*- la situación se torna más compleja, en la medida en que la Fiscalía podría sostener la inexistencia de una expectativa razonable de confidencialidad.

Este escenario pone de manifiesto uno de los principales riesgos asociados al uso de IAGen: la externalización de información estratégica hacia entornos con menor nivel de control jurídico, lo que impone un estándar reforzado de diligencia por parte del profesional en la selección y utilización de estas herramientas.

#### 6.4. Impacto sobre el derecho de defensa y la igualdad de armas

Finalmente, las reglas de admisibilidad de la prueba generada mediante IAGen deben ser interpretadas a la luz del derecho de defensa y del principio de igualdad de armas(55).

La exclusión automática de los contenidos generados mediante IAGen del ámbito de protección del secreto profesional implicaría, en la práctica, restringir el acceso a herramientas tecnológicas que hoy resultan relevantes para la elaboración de la defensa. Ello generaría una asimetría injustificada entre las partes, especialmente si el Estado cuenta con mayores recursos tecnológicos para la investigación y el análisis de información.

Desde esta perspectiva, el problema no radica en la utilización de este tipo de tecnología en sí misma, sino en las condiciones en que dicha utilización se produce. Un enfoque excesivamente restrictivo podría desalentar el uso de herramientas que potencian la capacidad defensiva, afectando indirectamente la igualdad de armas en el proceso penal. Por el contrario, un enfoque funcional -coherente con la concepción amplia del secreto profesional en el derecho argentino- permite compatibilizar el uso de IAGen con la protección de las garantías constitucionales. Ello exige reconocer que la actividad cognitiva defensiva puede desarrollarse mediante herramientas tecnológicas, sin que implique automáticamente la pérdida de confidencialidad.

En conclusión, las reglas de admisibilidad deben evitar tanto la desprotección de la defensa como la incorporación acrítica de evidencia generada mediante sistemas opacos. El desafío consiste en equilibrar innovación tecnológica y garantías procesales, preservando el núcleo esencial del derecho de defensa como condición de legitimidad del proceso penal.

### 7. Propuestas normativas

Antes de adentrarme en las propuestas normativas se hará un breve análisis de los estándares internacionales y nacionales aplicables.

#### 7.1. Estándares internacionales aplicables

En el plano internacional, la regulación de la IAGen ha comenzado a consolidarse a partir de diversos instrumentos que, aunque no se dirigen específicamente al ejercicio de la abogacía en el ámbito penal, ofrecen criterios relevantes para su utilización en contextos jurídicos.

En particular, los principios establecidos por la Organización para la Cooperación y el Desarrollo Económico en el año 2019 y actualizados en 2024, disponen que los sistemas de la IA deben ser confiables, transparentes, robustos y responsables, con especial énfasis en la protección de la privacidad y derechos humanos, así como también que se encuentra sujeta a rendición de cuentas(56). Se aclara que la Argentina se encuentra en proceso de adhesión a la citada organización.

En la misma línea, la Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial (2021)(57) introduce el principio de la dignidad humana, la supervisión humana, la responsabilidad, la protección de datos y la seguridad. Si bien no posee carácter vinculante, constituye un estándar interpretativo relevante, especialmente en ordenamientos -como el argentino- que aún carecen de una regulación integral en la materia.

Promueven directrices globales que incluyen la veracidad de contenidos automatizados, la identificación clara de contenido generado y la responsabilidad civil y penal por el uso de IAGen maliciosa(58).

Particularmente, en el punto 40 de la mentada resolución, se propuso una definición clara de explicabilidad como eje estructural definiéndolo como la necesidad de que los resultados y procesos algorítmicos, sean trazables y justificables para los usuarios afectados(59).

Por su parte, el Reglamento de Inteligencia Artificial (AI Act) del año 2024 adopta un enfoque basado en riesgos, imponiendo obligaciones reforzadas -transparencia, trazabilidad, control humano- para sistemas de alto impacto, categoría dentro de la cual pueden ubicarse las herramientas utilizadas en contextos jurídicos.

Es así como impone exigencias, como el etiquetado obligatorio de contenidos generados por IA, la documentación de los datos de entrenamiento, entre otras cosas.

Su objetivo es promover una IA segura y protegiendo los derechos fundamentales(60).

Asimismo, la Carta Ética Europea sobre el Uso de la Inteligencia Artificial en los sistemas judiciales y su entorno de 2018(61) del Consejo de Europa introdujo principios particularmente relevantes para el presente trabajo, tales como: control humano, transparencia(62), imparcialidad y justicia, calidad de datos, no discriminación, entre otros. Finalmente, en el derecho estadounidense, la aplicación del estándar de admisibilidad científica derivado de *Daubert v. Merrell Dow Pharmaceuticals*(63) evidencia que la fiabilidad, verificabilidad y aceptación científica constituyen condiciones esenciales para validar evidencia generada mediante sistemas tecnológicos.

Particularmente, en el caso en estudio, el motivo por el cual el uso de este software no había sido aceptado por la comunidad científica relevante era su falta de explicabilidad, ya que generaba información que no estaba contenida en la fuente primaria mediante un método desconocido. Esto implicaba la creación de detalles falsos en la imagen, distorsionando el significado de la escena y pudiendo inducir a error, de modo que no se podía explicar su proceso de razonamiento ni la fiabilidad de sus resultados.

En suma, si bien el derecho internacional no ofrece aún una regulación específica sobre el secreto profesional frente a la IAGen, sí establece un marco normativo claro: el uso de estas tecnologías debe integrarse dentro de un modelo garantista, basado en la protección de derechos fundamentales, el control humano y la responsabilidad profesional. Existe un consenso creciente respecto a que la trazabilidad y explicabilidad son condiciones necesarias para cualquier aplicación legítima de IAGen en el ámbito judicial<sup>(64)</sup>. Esta tendencia resulta plenamente compatible con la tesis sostenida en el presente trabajo, en cuanto exige analizar el impacto de este tipo de herramientas no desde su mera novedad tecnológica, sino desde su incidencia concreta sobre el derecho a la defensa en juicio y la confidencialidad.

## 7.2. Estándares argentinos aplicables

En el ámbito nacional, si bien no existe una regulación específica sobre IA aplicable al ejercicio de la abogacía, se han desarrollado avances relevantes en materia de lineamientos generales.

En particular, a la ya citada Guía de Uso de IA del CPACF, se suma la Disposición 2/2023 de la Jefatura de Gabinete de Ministros<sup>(65)</sup> que establece recomendaciones para una IA fiable, alineadas con los estándares internacionales. Dichas directrices enfatizan la necesidad de sistemas transparentes, explicables y centrados en el usuario.

Asimismo, el desarrollo del sistema Prometeo<sup>(66)</sup> en el ámbito del Ministerio Público Fiscal de la Ciudad de Buenos Aires demuestra la progresiva incorporación de IA en el sistema judicial, especialmente en tareas estandarizadas.

No obstante, estos avances no suplen la ausencia de una regulación específica que aborde el impacto de la IAGen sobre el secreto profesional y el derecho de defensa en el proceso penal. En consecuencia, el ordenamiento argentino presenta actualmente un vacío normativo que debe ser abordado.

## 7.3. Protección de la actividad cognitiva defensiva

Resulta imprescindible reconocer normativamente la protección de la actividad cognitiva defensiva.

Ello implica establecer que los contenidos generados mediante IAGen en el marco de la preparación de la defensa técnica se encuentran comprendidos dentro del ámbito del secreto profesional, en tanto constituyen una manifestación del proceso intelectual del abogado o del imputado.

Esta protección no se limita a las comunicaciones, sino que se extiende a los papeles de trabajo, incluyendo borradores, esquemas y desarrollos estratégicos. En consecuencia, la intervención de IAGen no debe ser equiparada automáticamente a la participación de un tercero que rompe la confidencialidad.

No obstante, dicha protección se encuentra condicionada a la inexistencia de una pérdida efectiva y jurídicamente relevante de confidencialidad, lo que exige un análisis contextual en cada caso concreto.

## 7.4. Pautas mínimas de uso profesional

El uso de IAGen en el ejercicio de la abogacía exige la adopción de estándares mínimos de conducta profesional.

En este sentido, corresponde establecer: la obligación de validar el contenido generado antes de su utilización, la adopción de medidas razonables de protección de datos, la selección de herramientas que garanticen condiciones adecuadas de confidencialidad, y la capacitación continua en materia de funcionamiento, riesgos y límites de estas tecnologías.

Asimismo, se impone la adopción de medidas preventivas, tales como la abstención de introducir datos sensibles en plataformas de acceso público o sin garantías contractuales adecuadas, la implementación de políticas internas de control sobre el uso de herramientas de IAGen, y la migración hacia entornos tecnológicos cerrados que aseguren la no reutilización de la información.

La omisión de estos deberes puede dar lugar a responsabilidad disciplinaria, civil o penal, en la medida en que implique una vulneración del secreto profesional o de derechos fundamentales.

Por otra parte, se exige la adecuación de las relaciones contractuales entre abogado y cliente, incorporando advertencias específicas sobre los riesgos asociados al uso no controlado de IAGen, en tanto dicha conducta puede derivar en una pérdida del secreto profesional y, consecuentemente, en una vulnerabilidad probatoria.

## 7.5. Criterios funcionales para determinar la prevalencia del secreto profesional en contenidos generados por inteligencia artificial

A fin de determinar si los contenidos generados mediante IAGen se encuentran alcanzados por el secreto profesional, se recomienda aplicar un test basado en las condiciones concretas de uso de la herramienta. Dicho análisis no puede agotarse en una evaluación abstracta del sistema utilizado, sino que exige ponderar el modo específico en que la tecnología es integrada en la actividad defensiva, así como los riesgos efectivos de pérdida de confidencialidad.

En particular, deberán considerarse los siguientes criterios:

A) Control funcional del profesional: Debe evaluarse si la herramienta es utilizada como un instrumento subordinado a la actividad del abogado o del imputado, sin autonomía decisoria ni intervención externa relevante. A mayor control del usuario sobre el proceso, mayor será la posibilidad de subsumir la interacción dentro de la actividad cognitiva defensiva. Por el contrario, la delegación sustancial de funciones o la intervención de terceros en el procesamiento de la información debilita la protección.

B) Régimen de tratamiento de datos y previsibilidad de uso: Resulta determinante analizar si la información ingresada puede ser almacenada, reutilizada o compartida con terceros, especialmente para fines de entrenamiento o mejora del sistema. La ausencia de previsibilidad o la existencia de cláusulas que habiliten usos amplios de los datos compromete la expectativa razonable de confidencialidad. En este sentido, el uso de plataformas abiertas o comerciales sin garantías explícitas debe ser considerado, en principio, como un entorno de riesgo elevado.

C) Existencia de garantías técnicas de confidencialidad: Debe considerarse si la herramienta incorpora mecanismos adecuados de protección, tales como cifrado, entornos cerrados, limitación de acceso o exclusión de reutilización de datos. La presencia de estas garantías permite asimilar el sistema a un ámbito controlado por el profesional. En cambio, su ausencia impone un estándar de diligencia reforzado, en tanto el riesgo de exposición no resulta meramente hipotético sino estructural.

D) Finalidad de la interacción: Es relevante determinar si el uso de la IAGen se encuentra directamente vinculado con la elaboración de la estrategia defensiva, incluyendo el análisis de hechos, la generación de hipótesis y la estructuración argumental. Cuanto más estrecha sea esa vinculación, mayor será la probabilidad de que el contenido quede comprendido dentro del ámbito protegido, en tanto expresión del proceso intelectual del defensor.

E) Grado de exposición de la información: Debe analizarse si la información ingresada incluye datos sensibles o estratégicos cuya divulgación pueda comprometer la defensa. La introducción de información altamente crítica en entornos que no garantizan confidencialidad suficiente puede implicar una pérdida jurídicamente relevante del secreto profesional, incluso cuando la finalidad de la interacción sea legítima.

Este criterio funcional no solo cumple una función interpretativa, sino que proyecta consecuencias directas en el plano de la conducta profesional.

En conclusión, la subsistencia del secreto profesional en entornos de IAGen no depende de la tecnología en sí misma, sino del grado de control, previsibilidad y resguardo efectivo de la información, debiendo evaluarse en cada caso si se ha producido -o no- una pérdida jurídicamente relevante de confidencialidad.

7.6. Proyección probatoria de los criterios funcionales: inadmisibilidad de la prueba obtenida con vulneración del secreto profesional

Los criterios funcionales desarrollados en el apartado precedente no se agotan en la determinación abstracta de la subsistencia del secreto profesional, sino que proyecta efectos directos en el plano probatorio. En efecto, la verificación de una pérdida jurídicamente relevante de confidencialidad constituye el presupuesto necesario para habilitar la incorporación de los contenidos generados mediante IA al proceso.

En consecuencia, cuando del análisis de los criterios indicados en el punto 7.5 surja que la interacción con la herramienta se mantuvo dentro de un ámbito de control funcional del profesional, con garantías suficientes de confidencialidad y en directa vinculación con la actividad cognitiva defensiva, los contenidos generados deberán ser considerados alcanzados por el secreto profesional. En tales supuestos, su incorporación al proceso resulta inadmisibile, en tanto implicaría una afectación directa del derecho de defensa en juicio.

Por el contrario, cuando se acredite que el uso de la IA implicó una exposición efectiva de la información en - entornos que permiten su acceso, almacenamiento o reutilización por terceros, y que dicha circunstancia comporta una pérdida jurídicamente relevante de confidencialidad, cesa la protección derivada del secreto profesional. En estos casos, la eventual admisibilidad de los contenidos deberá ser evaluada conforme a las reglas generales de la prueba, sin perjuicio de las restantes garantías aplicables.

No obstante, la determinación de tal pérdida no puede fundarse en presunciones abstractas ni en la mera utilización de herramientas tecnológicas, sino que exige una acreditación concreta de las condiciones de uso y de los riesgos efectivamente asumidos. Este enfoque evita soluciones automáticas que, bajo una apariencia de rigor técnico, podrían traducirse en restricciones indebidas del derecho de defensa.

Asimismo, cuando se verifique la vulneración del secreto profesional, la exclusión probatoria no se limita al contenido directamente afectado, sino que se extiende a toda evidencia derivada que guarde una relación causal adecuada con la información obtenida, conforme a la doctrina del “fruto del árbol venenoso”. Esta regla opera como un mecanismo de tutela reforzada de las garantías constitucionales, impidiendo que la ilicitud inicial sea neutralizada mediante su aprovechamiento indirecto.

En definitiva, los criterios funcionales actúan como un filtro normativo previo que condiciona la admisibilidad probatoria de los contenidos generados mediante IA, asegurando que la incorporación de nuevas tecnologías al proceso no implique una erosión encubierta del secreto profesional ni del derecho de defensa en juicio.

#### 7.7. Integración con el sistema jurídico vigente

El desarrollo de un marco normativo adecuado no requiere necesariamente la creación de un régimen completamente autónomo, sino la reinterpretación e integración de las normas existentes.

En este sentido, el artículo 156 del Código Penal puede ser interpretado de modo que contemple la revelación de secretos en entornos digitales. Asimismo, la Ley 23.187 debería incorporar deberes específicos vinculados al uso de tecnologías, especialmente en relación con la protección del secreto profesional, la confidencialidad de la información y el empleo responsable de herramientas de IAGen.

Respecto del CPPN, el artículo 237 debería readecuarse para que la exclusión de secuestro no alcance únicamente a cartas o documentos tradicionales, sino también a registros digitales, metadatos, borradores, esquemas, papeles de trabajo, prompts, respuestas generadas por IA y cualquier otro soporte físico o digital vinculado con la defensa técnica o material. Esta protección debería comprender la actividad intelectual, estratégica y cognitiva tanto del imputado, como de la defensa.

En cuanto al CPPF, el artículo 149 debería ampliar la protección actual del secreto profesional para incluir no solo comunicaciones y notas tradicionales, sino también información digital o generada mediante IA. Respecto del artículo 150 del CPPF, una eventual reforma debería actualizar el régimen de interceptación de comunicaciones para contemplar tecnologías digitales, servicios en la nube y sistemas de IA.

También deberían actualizarse las normas sobre prueba pericial, especialmente cuando la pericia involucre documentos digitales, sistemas informáticos, IA, bases de datos, modelos automatizados, dispositivos electrónicos o evidencia generada artificialmente. En tales casos, el perito debería explicar la metodología utilizada, las herramientas empleadas, la cadena de custodia, el alcance del análisis, sus limitaciones técnicas, el grado de reproducibilidad y las medidas adoptadas para no vulnerar información protegida por secreto profesional. Si el perito utilizara herramientas de IA para auxiliar su dictamen, debería identificar qué función cumplieron, qué datos fueron ingresados y cuál fue el grado de intervención humana en las conclusiones.

Finalmente, la Ley 25.326 de Protección de Datos Personales proporciona un marco relevante para el tratamiento de información en sistemas de IA, aunque requiere una actualización que contemple los procesos automatizados y las nuevas formas de tratamientos masivos de datos.

Este enfoque permite evitar una sobrerregulación que obstaculice la innovación tecnológica, al tiempo que garantiza la protección de los derechos fundamentales involucrados. En definitiva, la IAGen debe ser integrada al sistema jurídico argentino desde una perspectiva garantista, que preserve el núcleo esencial del derecho de defensa en juicio.

#### 8. Conclusión

El desarrollo de sistemas de IAGen plantea un desafío ineludible para las categorías tradicionales del derecho procesal penal, en particular en lo que respecta al alcance del secreto profesional del abogado. Sin embargo, la novedad tecnológica no justifica una exclusión automática de la tutela constitucional de la defensa en juicio, sino que exige una reinterpretación de sus presupuestos a la luz de las nuevas formas de producción y tratamiento de la información.

A diferencia del modelo estadounidense, en el que el privilegio abogado-cliente opera como una regla probatoria de interpretación restrictiva -tal como se evidencia en el precedente *United States v. Bradley Heppner*-, el derecho argentino reconoce al secreto profesional una dimensión constitucional que excede la mera confidencialidad de las comunicaciones, extendiéndose al proceso mismo de elaboración de la defensa.

Desde esta perspectiva, los contenidos generados mediante IAGen pueden integrar la esfera de la actividad cognitiva defensiva y, por ende, resultar alcanzados por el secreto profesional, siempre que su utilización no implique una pérdida efectiva y jurídicamente relevante de confidencialidad.

En consecuencia, el criterio determinante no radica en la naturaleza de la herramienta utilizada, sino en las condiciones jurídicas y técnicas bajo las cuales se produce su utilización. La IA no constituye, por definición, un tercero que excluya la protección, pero tampoco puede ser considerada automáticamente como un espacio seguro: su impacto debe ser evaluado en función del grado de control, previsibilidad y resguardo de la información.

En definitiva, el desafío contemporáneo no consiste en restringir el uso de tecnologías emergentes en el ejercicio de la defensa, sino en establecer estándares que permitan su utilización compatible con las garantías constitucionales. Solo a través de un enfoque funcional, que atienda a las condiciones concretas de uso, será posible preservar el núcleo esencial del derecho de defensa en juicio en el contexto de la transformación digital.

Por ello, los abogados del futuro necesitarán, sin dudas, una comprensión íntima y continua de cómo identificar y utilizar las soluciones de IA para satisfacer las necesidades de sus clientes sabiendo evaluar las fortalezas y debilidades relativas de determinadas soluciones, no dejándose deslumbrar por sistemas que mágicamente nos den soluciones que -arduamente- los abogados tardamos mucho en aprender -o al menos suponer- cuál es el camino más apropiado en el buen ejercicio de la profesión(67).

## 9. Índice de bibliografías

Anzisi, A. del R. (2021). Garantías de los imputados vs. averiguación de la verdad. <https://50jaiio.sadio.org.ar/pdfs/sid/SID-09.pdf>

Bacigalupo, E. (1999). Derecho Penal. Parte General (2ª ed.). Hammurabi.

Bouvet, S. E. (s.f.). El secreto profesional del abogado. Implicancias en los derechos humanos y en las garantías constitucionales. <https://ar.ijeditores.com>

Caunedo, F. M., & Gorostiaga, M. (s.f.). El secreto profesional médico. <http://www.eldial.com.ar>

Cardozo, J. E. (2023). La inteligencia artificial generativa y su impacto transformador en la prueba digital: desafíos y perspectivas en el ámbito jurídico. ELDial.

Carrara, F. (1957). Programa de Derecho Criminal. Parte General (T. 2). Temis. Colegio Público de la Abogacía de la Capital Federal. (2025). Guía para el uso de inteligencia artificial para abogados. <https://www.cpacf.org.ar>

Conti, N. J. (s.f.). El delito de violación de secreto y el profesional convocado a prestar declaración testimonial. <https://www.criticapenal.com.ar>

Couture, E. J. (2017). Los mandamientos del abogado, [trj13.pdf](#)

Creus, C., & Buompadre, J. (2007). Derecho Penal. Parte Especial (T. 1, 7ª ed.). Astrea. De Luca, J. A. (1999). El secreto de las fuentes periodísticas en el proceso penal. Buenos Aires: Ad Hoc.

De Luca, J. A., & Lacman, V. A. (2007). El secreto profesional y su relevamiento en el proceso penal. Revista de Derecho Penal y Procesal Penal, 1740-1741.

D'Albora, F. J. (1997). Código Procesal Penal de la Nación comentado (3ª ed.). Abeledo Perrot.

Finkelstein Nappi, J. L. (2017). La Corte Suprema de Justicia de la Nación frente al derecho de defensa material. Ministerio Público de la Defensa.

Fontán Balestra, C. (1998). Derecho Penal. Parte Especial (15ª ed.). Abeledo Perrot. Granero, H. R. (2023). ¿Con ChatGPT llegó el “abogado robot”? ELDial.com.

Heredia, J. R. (2022). La inviolabilidad del defensor y de su estudio jurídico. Revista Pensamiento Penal.

Islas Magallanes, O. (1962). Delito de revelación de secretos. Talleres Gráficos de la Nación.

Jara, M. L. (2024). Inteligencia artificial generativa: desafíos éticos en el ejercicio profesional de los abogados. El Derecho.

Kraut, A. J. (1988). Tratamiento psiquiátrico y secreto profesional. La Ley.

Mancuso, F. (1995). Ética de la abogacía y potestad disciplinaria. Editorial Universitaria. Núñez, R. (1989). Tratado de Derecho Penal (T. IV). Lerner.

Parma, C. (s.f.). Violación de secreto profesional. Código Penal Comentado. Asociación Pensamiento Penal.

Pérez Cepeda, A. I. (2000). Delitos de deslealtad profesional de abogados y procuradores. Aranzadi.

Pitlevnik, L. (2012). Jurisprudencia penal de la Corte Suprema de Justicia de la Nación. Hammurabi.

Riquert, M. (2006). El delito de violación de secretos. La Ley.

Rivera, J. C. (1993). Instituciones de Derecho Civil. Parte General (T. II). Abeledo Perrot.

Roxin, C. (2010). Derecho Penal. Parte General (T. I, 5ª ed.). Civitas.

Sánchez Freytes, A. (1983). Violación del secreto particular. Revista del Colegio de Abogados de Córdoba.

Tristán, R. (2012). Secreto profesional del abogado. Revista Pensamiento Penal.

Warlet, R. A. (2023). Abogacía y ética en la era de la inteligencia artificial. ELDial.

VOCES: ABOGADO - PROFESIONES LIBERALES - SECRETO PROFESIONAL - INTELIGENCIA ARTIFICIAL - INFORMÁTICA - TECNOLOGÍA - INTERNET - DEFENSA EN JUICIO - EXPEDIENTE JUDICIAL - JUECES - SENTENCIA - PROCESO ORDINARIO - EJERCICIO PROFESIONAL - ESTADO - DERECHOS Y GARANTÍAS CONSTITUCIONALES - DERECHOS HUMANOS - PODER JUDICIAL - ECONOMÍA - CONSTITUCIÓN NACIONAL - CÓDIGO DE ÉTICA - JUECES - FILOSOFÍA DEL DERECHO - SENTENCIA - ACCESO A LA JUSTICIA

1. (1) Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: Responsabilidad civil en internet: avance de las nuevas tecnologías de la información y asignaturas pendientes del sistema jurídico, por Marcelo Oscar Vuotto, ED, 261-860; ¿El control del trabajador por medio de tecnologías que posibilitan conocer su ubicación afecta su derecho a la intimidad? Nota al caso “Pavolotzki”, por Juan Ángel Confalonieri (h.), TySS, 2016-297; El uso de la tecnología y la gestión de la comunicación en la mediación actual, por Juan Fernando Gouvert, ED, 275-771; El derecho ante la inteligencia artificial y la robótica, por Verónica Elvia Melo, ED, 276-493; La protección de los datos personales en internet (una tarea ineludible), por Esteban Ruiz Martínez, ED, diario n° 14.706 del 5-9-19; La comunidad humana en la era tecnológica, por Leonardo Pucheta, ED, 282-1044; Algoritmos de inteligencia artificial con fines de control fiscal: ¿puede el derecho embridar a las nuevas tecnologías?, por José Manuel Calderón Carrero, El Derecho Tributario, marzo 2020 - Número 1, cita digital: ED-CMXIII-759; El Derecho en la nueva era tecnológica, por Julia Inés Imperiale, ED, 287-805; La inteligencia artificial en la Administración Pública y los derechos fundamentales, por Ricardo A. Muñoz (h.), Revista de Derecho Administrativo, mayo 2020 - Número 5; La inteligencia artificial en el mundo jurídico actual. (Implicancias, aplicaciones y posibilidades), por Alberto B. Bianchi, Derecho, Innovación & Desarrollo Sustentable, Número 3 - octubre 2021; El Vaticano propone ante la ONU regular el uso pacífico de la inteligencia artificial, Diario de Derecho Constitucional, El Derecho Constitucional, diciembre 2021 - Número 12; Administración de justicia e inteligencia artificial: una mirada ética sobre la relación entre eficiencia y equidad, por Estela Josefina Condrac, Derecho, Innovación & Desarrollo Sustentable, Número 6 - abril 2022; Breves consideraciones sobre el encuadre ético de la Inteligencia Artificial (IA), por Cristina Margarita Rosa Hofkamp, El Derecho Constitucional, diciembre 2022 - Número 12; Ética en tiempos de inteligencia artificial. Reflexiones en torno a los planteos éticos de las IA en tiempos laberínticos de vulnerabilidad y transhumanismo que propone la Cuarta Revolución Industrial, por Gustavo Andrade Figueroa, Derecho, Innovación & Desarrollo Sustentable, Número 14 - agosto 2023; Patrocinio letrado inteligente: ¿conviene desde la óptica de la responsabilidad civil en el derecho argentino?, por Stefanía Magdalena Elizabeth Cáceres, ED, 313. Todos los artículos citados pueden consultarse en [www.elderechodigital.com.ar](http://www.elderechodigital.com.ar).

Barrio A. M. (2023, 12 de mayo), Artículo en sección Tribuna, Diario La Ley, 10285, La Ley, Madrid, citado por Cardozo, J. E., La Inteligencia Artificial Generativa y su impacto transformador en la prueba digital: Desafíos y perspectivas en el ámbito jurídico, Citar: elDial.com - DC3665.

2. (2) Warlet, R A., (s.f.). Abogacía y ética en la era de la inteligencia artificial. Una mirada desde Entre Ríos. ELDial.com, DC35D3.
3. (3) Cfr. CPACF (2025). Guía para el uso de inteligencia artificial para abogados, del Colegio Público de la Abogacía de la Capital Federal (2025). [https://www.cpacf.org.ar/uploads/files/com/11072515\\_Gu%C3%ADaparaelusodelInteligenciaArtificialparaAbogados.pdf](https://www.cpacf.org.ar/uploads/files/com/11072515_Gu%C3%ADaparaelusodelInteligenciaArtificialparaAbogados.pdf)
4. (4) Cfr. Couture, E. J. (2017). Los mandamientos del Abogado, La imprenta YA, p. 17 citado por CARDOZO, José E., ob. cit.
5. (5) Ibid.
6. (6) Cfr. CPACF. Guía para el uso de inteligencia artificial para abogados, ob. cit.
7. (7) Heredia, J. R., (2022, mayo). La inviolabilidad del defensor y de un estudio jurídico. Revista Pensamiento Penal, 423. <https://www.pensamientopenal.com.ar/doctrina/90114-inviolabilidad-del-defensor-y-su-estudio-juridico>.
8. (8) Es así como la CSJN en los Fallos: 5:459; 192:152; 237:158; 255:91; 311:2502 ha considerado que la tutela de dicha garantía ha sido preocupación del Tribunal desde sus orígenes, en los que señaló que el ejercicio de la defensa debe ser cierto, de modo tal que quien sufre un proceso penal ha de ser provisto de un adecuado asesoramiento legal, al extremo de suplir su negligencia en la provisión de defensor asegurando, de este modo, la realidad sustancial de la defensa en juicio. Asimismo, el Superior Tribunal destacó que no basta para cumplir con las exigencias básicas del debido proceso que el acusado haya tenido patrocinio letrado de manera formal, sino que es menester además que aquel haya recibido una efectiva y sustancial asistencia de parte de su defensor (Fallos: 310:1934; 327:103; 331:2520).

9. (9) Claría Olmedo (1954). La prueba de la verdad de los procedimientos penales, Revista de derecho procesal argentino, I, p. 221.
10. (10) Bouvet, S. E. (s.f.). El secreto profesional del abogado. Implicancias en los Derechos Humanos y en las Garantías Constitucionales. Observación General 32, "El derecho a un juicio imparcial y a la igualdad ante los tribunales y cortes de justicia, párr. 34. <https://ar.ijeditores.com>.
11. (11) Cfr. Parma, C. (s.f.). Violación de Secreto Profesional, Código Penal Comentado, Asociación Pensamiento Penal, p. 19. <https://www.pensamientopenal.com.ar/cpcomentado/37763-art-156-violacion-secreto-profesional>.
12. (12) Rivera, J. C. (1993). Instituciones de Derecho civil. Parte General. (Tomo II). Buenos Aires, Abeledo Perrot. p.79.
13. (13) CSJN. (1996,13 de febrero). Dirección General Impositiva contra Colegio de Abogados de la Capital Federal. Jurisprudencia Argentina, 1996-II-29.
14. (14) CSJN. (2007, 30 de octubre). Franco, Julio César c. Diario "La Mañana" y/u otros. La Ley,14/12/2007, 6; DJ, 02/01/2008.
15. (15) Pitlevnik, L. (2012). Jurisprudencia penal de la Corte suprema de Justicia de la Nación, Hammurabi. p. 21.
16. (16) Cfr. Sánchez Freytes, Alejandro. (1983). Violación del secreto particular. Revista del Colegio de Abogados de Córdoba, 17, p. 82.
17. (17) Cfr. Islas Magallanes, O. (1962). Delito de revelación de secretos. Talleres Gráficos de la Nación. p.53.
18. (18) Pérez Cepeda, A. I. (2000). Delitos de deslealtad profesional de abogados y procuradores. Aranzadip. 49.
19. (19) Cfr. Mancuso, F. (1995). Ética de la Abogacía y Potestad disciplinaria". Universitaria de La Plata, p. 7 y ss.
20. (20) Cfr. Bouvet, S. E. (s.f). ob. cit.
21. (21) Cfr. Fontán Balestra, C. (1998). Derecho Penal: Parte especial (15° ed.); Abeledo -Perrot, p. 365.
22. (22) Cfr. Núñez, R. (1989). Tratado de Derecho Penal (T. IV), Lerner p. 126/8; Buompadre, J. (2000) Derecho Penal. Parte Especial (T.1), Mave, p. 626/9; Creus, Carlos & Buompadre, J. (2007). Derecho Penal. Parte Especial (T. 1, 7° ed.). Astrea. p. 398; Kraut, A.J., (1998). Tratamiento psiquiátrico y secreto profesional. La Ley, 1.988-C, p. 753.
23. (23) En ese sentido, ROXIN, C. (2010) sostuvo en Derecho Penal. Parte General (Tomo I, 5° ed.) Civitas ps. 765, que "A diferencia del consentimiento (expresión de la libertad de actuación del titular del BJP), que excluye ya el tipo, el consentimiento presunto (se interfiere sin permiso...) es una causa de justificación".
24. (24) Cfr. Caunedo, F. M. & Gorostiaga, M. (s.f.), señalaron en El secreto profesional médico, <http://www.eldial.com.ar/publicado>, que: entre los supuestos en los que el profesional actúa como parte en un juicio, cuando se encuentra en pleito con su cliente acerca de sus honorarios. En este caso, el deber de guardar secreto puede hallarse en colisión con bienes jurídicos del propio depositario, y el profesional puede encontrarse necesitado a efectuar alguna revelación en resguardo de sus intereses.
25. (25) Cfr. Bacigalupo, E. (1999). Derecho Penal. Parte General, (2° ed.). Hammurabi. ps. 378 dijo que existen dos formas de estado de necesidad: una en la que colisionan intereses jurídicos, y en otra, deberes jurídicos, y que el bien salvado debe ser de mayor jerarquía que el sacrificado, puesto que primero se formuló el principio de ponderación de bienes que sostiene y se limita a la ponderación a bienes jurídicos - considerados como si fueran una necesidad estática. El conflicto que caracteriza un estado de necesidad está determinado por numerosos factores y como principio más amplio se ha propuesto el de ponderación de intereses, cuya misión sería la de considerar la totalidad de las circunstancias relevantes para la situación.
26. (26) Tal como sería el caso de las Leyes Especiales que se detallan a continuación: 1. Ley 12.331 (de profilaxis, impedimento matrimonial, etc.); 2. Ley 16.668 (certificado prenupcial femenino); 3. Ley 14.586 (Registro de Estado Civil de las Personas. Bs.As.); 4. Ley 11.359 (profilaxis de la lepra); 5. Ley 11.842 (profilaxis de la peste); 6. Ley 15.465 (notificación obligatoria de enfermedades... con reserva de identidad del paciente, al sólo fin epidemiológico... se discute mental); 7. Ley 23.798 (sobre el SIDA) y Decreto 1.244 anexo I; 8. Ley 24.193 (trasplantes de órganos); 9. Ley 24.417 (protección contra la violencia familiar) y Decreto Reglamentario 235/9 (estas revelaciones se dan a instituciones o persona determinada y por un imperativo si hay revelación de secreto); 10. Ley 22.914 (internación y egreso de establecimientos de salud legal).

27. (27) Cfr. Riquert, M. (2006). El delito de violación de secretos (consideración general y su conexión con los deberes de denunciar y atestiguar. En Ferrara, J. A. (Dir.). Temas de Derecho Penal Argentino. La Ley. p. 486.
28. (28) Cfr. Carrara, F. (1957). Programa de Derecho Criminal. Parte General (T. 2), Temis, p. 442.
29. (29) Cfr. De Luca, J. A. & Lacman, V. A. (2007, septiembre). El secreto profesional y su relevamiento en el proceso penal. Revista de Derecho Penal y Procesal Penal, Lexis Nexis. p. 1.740/1.
30. (30) En igual sentido, Conti, N. J. (s.f.). El delito de violación de secreto y el profesional convocado a prestar declaración testimonial, <https://www.criticapenal.com.ar/wp-> señaló que “Es así como, el único que puede (y debe) evaluarla es el profesional interesado, pues será quien decida si la misma justifica o no revelar el secreto que le fuera confiado y arriesgarse (o no) a un proceso penal por el delito castigado por el citado art. 156 o por un delito contra el honor; máxime, cuando sean convocados a prestar declaración como testigos en un proceso penal y tengan que decidir o bien declarar, o bien, ampararse en el secreto profesional, por cuanto no es el juez quien debe (ni puede) relevar al testigo de dicho compromiso profesional y ético”
31. (31) De Luca, J.A., (1999). El secreto de las fuentes periodísticas en el proceso penal, AdHoc p. 43.
32. (32) Cfr. Parma, C. ob. cit. p. 62.
33. (33) Ibid.
34. (34) Artículo 11 inciso h): Son deberes inherentes al ejercicio de la abogacía: El abogado debe respetar rigurosamente todo secreto profesional y oponerse ante los jueces u otra autoridad al relevamiento del secreto profesional, negándose a responder las preguntas que lo expongan a violarlo. Solo queda exceptuado: a) Cuando el cliente así lo autorice; b) Si se tratare de su propia defensa.
35. (35) Bouvet, S. E. (s.f.). ob. cit.
36. (36) Cfr. D´Albora, F. J. (1997). Código Procesal Penal de la Nación. Ley 23.984 (3° ed.). Abeledo Perrot, p. 357.
37. (37) Artículo 9° (Seguridad de los datos). 1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.
38. (38) Artículo 10: 1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.  
  
2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.
39. (39) Artículo 2. (...) Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.
40. (40) Heredia, J. R. (2022, mayo). La inviolabilidad del defensor y de su estudio jurídicos. Revista Pensamiento Penal. [https://www.pensamientopenal.com.ar/system/files/este%20ete%20tetetetete\\_0.pdf](https://www.pensamientopenal.com.ar/system/files/este%20ete%20tetetetete_0.pdf), señala que “la efectividad del derecho de defensa no sólo depende del reconocimiento del derecho a recibir los servicios de un abogado, sino también de que este profesional goce de los medios y prerrogativas necesarias para el libre ejercicio de su función...”. “Entre las obligaciones de los Abogados figura el de secreto profesional (...) -lo que legitima la intervención del Decano en las diligencias de registro de los despachos profesionales-, de celo y de diligencia en la defensa que le sea encomendada (...). Asimismo, les asiste el derecho a ejercer la defensa con libertad e independencia y con pleno respeto a su función (...), lo cual implica el reconocimiento de una serie de garantías entre las que figura necesariamente la confidencialidad de las comunicaciones entre Abogado y cliente”.
41. (41) Cfr. Robles Tristán, R., (2012, 3 de julio). Secreto Profesional del Abogado”, Pensamiento Penal. <https://www.pensamientopenal.com.ar/doctrina/41469-secreto-profesional-del-abogado> dijo que: “Vale agregar que el TEDH indica escuetamente que la obstrucción al secreto profesional, trae aparejadas repercusiones lesivas sobre la administración de la justicia, interpretación que sugiere que este derecho no solo protege el negocio del letrado y la privacidad de sus clientes, sino que tiene alcances generales sobre la sociedad y el Estado. Y es que, en definitiva, el abogado es el operador jurídico de quien se espera la defensa de los derechos de las personas frente al órgano judicial, lo que justifica la importancia de su actuación como un valor caro del Estado de Derecho”.

42. (42) Cfr. Anzisi, A del R. (s.f.). Garantías de los imputados vs. Averiguación de la verdad. <https://50jaiio.sadio.org.ar/pdfs/sid/SID-09.pdf>.
43. (43) Cfr. Finkelstein Nappi, J. L. (2017) La Corte de Justicia de la Nación frente al derecho de la defensa material, Ministerio Público de la Defensa, Secretaría General de Capacitación y Jurisprudencia, p. 82 y ss. <https://repositorio.mpd.gov.ar/jspui/bitstream/123456789/3840/1/2017.7.%20La%20Corte%20Suprema%20de%20Justicia%20de%20la%20Naci%C3%B3n%20frente%20al%20derecho%20de%20defensa%20en%20juicio.pdf>
44. (44) Cfr. Corte IDH (2009, 27 de enero). Tristán Donoso v. Panamá. Excepción Preliminar, Fondo, Reparaciones y Costas. Serie C N° 193, párr. 75: el abogado Santander Tristán Donoso llegó a la Corte IDH sosteniendo que el Estado -a través de la Procuración- interceptó y divulgó una conversación telefónica que había mantenido con un cliente. La Corte sostuvo el “carácter privado” (ergo, protegido por el artículo 11 de la Convención Americana de Derechos Humanos) de la conversación, agregando además que: “... al ser realizada entre la presunta víctima y uno de sus clientes debería, incluso contar con un grado mayor de protección por el secreto profesional”.
45. (45) CPACF. Guía Práctica... ob. cit.
46. (46) Cfr. Jara, M. L., (2024, 24 de abril). Inteligencia artificial generativa: Desafíos éticos en el ejercicio profesional de los abogados. El Derecho. Cita Digital: ED-V- DXXXVII-726.
47. (47) Cfr. Granero, Horacio R. (2023, 21 de marzo). ¿Con ChatGP3 llegó el “abogado robot”? ELDial.com. DC 3195; [https://www.eldial.com/nuevo/nuevo\\_diseno/v2/doctrina\\_a.asp?base=50&id=14800](https://www.eldial.com/nuevo/nuevo_diseno/v2/doctrina_a.asp?base=50&id=14800)
48. (48) Ver [gov.uscourts.nysd.652138.22.0.pdf](http://gov.uscourts.nysd.652138.22.0.pdf)
49. (49) Granero, H. R. Confidencialidad cliente-abogado. Inviolabilidad de la actividad cognitiva defensiva frente al uso de inteligencia artificial en el Derecho argentino. ELDial.com, [https://www.eldial.com/nuevo/nuevo\\_diseno/V2/doctrina2.asp?id=16346&base=50&id\\_publicar=&fecha\\_publicar=25/02/2026&indice=comentarios&suple=Nuevas%20Tecnolog%C3%ADas%20e%20Inteligencia%20Artificial](https://www.eldial.com/nuevo/nuevo_diseno/V2/doctrina2.asp?id=16346&base=50&id_publicar=&fecha_publicar=25/02/2026&indice=comentarios&suple=Nuevas%20Tecnolog%C3%ADas%20e%20Inteligencia%20Artificial); y Roger, Alford (2018, 30 de mayo). Privilegio de abogado-cliente en la ejecución global del derecho de la competencia, Departamento de Justicia de EEUU, p. 3, <https://www.justice.gov/archives/opa/speech/file/1156721/dl>.
50. (50) Ibid.
51. (51) Convención Americana de Derechos Humanos, artículos 8.2. y 8.3; Pacto Internacional de Derechos Políticos y Económicos, artículo 14.3.G.
52. (52) Por consiguiente, en el marco de un proceso penal, la defensa del imputado podrá alegar, frente a la orden de secuestro de documentos generados a través de IA dictada por juez competente, que son una extensión de la mente del imputado o notas preparatorias. Granero, Horacio R., Confidencialidad... ob. cit.
53. (53) Ibid.
54. (54) CSJN. (1981, 10 de diciembre). Montenegro, Luciano Bernardino s/ robo, 10/12/1981, así como en los Fallos 310:1847, 317:1985.
55. (55) Lisi Trejo. (2015, enero). Problemas prácticos del proceso penal a la luz del principio de igualdad de armas como garantía constitucional del imputado, Revista 23, <https://ar.vlex.com/vid/problemas-practicos->
56. (56) Cfr. <https://oecd.ai/en/ai-principles>.
57. (57) Cfr. Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial [https://unesdoc.unesco.org/ark:/48223/pf0000381137\\_spa](https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa)
58. (58) Warlet, R. A., ob. cit.
59. (59) El artículo 40 de la Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial [https://unesdoc.unesco.org/ark:/48223/pf0000381137\\_spa](https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa) prevé: “La explicabilidad supone hacer inteligibles los resultados de los sistemas de IA y facilitar información sobre ellos. La explicabilidad de los sistemas de IA también se refiere a la inteligibilidad de la entrada, salida y funcionamiento de cada componente algorítmico y la forma en que contribuye a los resultados de los sistemas. Así pues, la explicabilidad está estrechamente relacionada con la transparencia, ya que los resultados y los subprocesos que conducen a ellos deberían aspirar a ser comprensibles y trazables, apropiados al contexto. Los actores de la IA deberían comprometerse a velar por que los algoritmos desarrollados sean explicables. En el caso de las aplicaciones de IA cuyo impacto en el usuario final no es temporal, fácilmente reversible o de bajo riesgo, debería garantizarse que se

proporcione una explicación satisfactoria con toda decisión que haya dado lugar a la acción tomada, a fin de que el resultado se considere transparente.”

60. (60) Cfr. IA Act Regulation, <https://artificialintelligenceact.eu/es/ai-act-explorer/>
61. (61) Cfr. <https://protecciondata.es/wp-content/uploads/2021/12/Carta-Etica-Europea-sobre-el-uso-de-la->
62. (62) Puntualmente, con respecto a la “transparencia”, se señaló que se trataba del acceso al proceso de diseño de las herramientas que podían llegar a tener algún tipo de consecuencia legal o que podían llegar a afectar significativamente la vida de las personas y también se resaltó que: “estas medidas se aplican a todo el diseño y la cadena operativa como el proceso de selección y la calidad y organización de los datos influyen directamente en la fase de aprendizaje.”. Esto podría darse de dos formas distintas: i) mediante la adopción de la transparencia técnica completa; o ii) por la utilización de un lenguaje claro y familiar para describir cómo se producen los resultados”.
63. (63) Cfr. Caso Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 US 579 (1993) <https://ignaciosoba->
64. (64) Cfr. Gatti, G. O. y Pongibione, P. (2025, 3 de octubre). El uso de la inteligencia artificial para la conformación del conjunto de elementos de juicio sobre cuya base se adoptará la decisión judicial.El Dial.com., <https://abogados.com.ar/el-uso-de-la-inteligencia-artificial-para-la-conformacion-del-conjunto->
65. (65) Cfr. <https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-2-2023-384656/texto>.
66. (66) Cfr. <https://mpfciudad.gob.ar/institucional/2020-03-09-21-42-38-innovacion-e-inteligencia-artificial>.
67. (67) Granero, Horacio R, ¿Con Chat...? ob. cit.