@miguelgallardo Dr. (PhD) Ing. Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
@APEDANICA Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf
https://cita.es/denuncia-google-android-firmado.pdf

Al Juzgado de Instrucción que corresponda

DENUNCIA publicada en https://www.miguelgallardo.es/denuncia-google-android.pdf

Dr. Ing. Miguel Ángel Gallardo Ortiz PhD, criminólogo y doctor en **ÉTICA**, diplomado en Altos Estudios Internacionales, miembro de **IAENG**, también en representación de **APEDANICA - Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas**, E-mail: **apedanica.ong@gmail.com** **Teléfono (+34) 902998352** domicilio en la **calle Fernando Poo, 16 Piso 6ºB E-28045 Madrid**, entidad sin ánimo de lucro ONG constituida en 1992, como mejor proceda en derecho, comparezco y DIGO:

Que por medio del presente escrito, al amparo de los artículos 259 y siguientes de la Ley de Enjuiciamiento Criminal, formulo **DENUNCIA PENAL** contra los responsables legales de las entidades **GOOGLE LLC (Alphabet Inc.)**, **GOOGLE IRELAND LIMITED** en Gordon House, Barrow Street, Dublin 4, Irlanda con IE6388047V y **GOOGLE SPAIN, S.L.** en Plaza Pablo Ruiz Picasso, 1, Torre Picasso, 28020 Madrid con CIF B63272603 así como contra quienes resulten responsables como autores, cooperadores necesarios, cómplices o responsables penales de persona jurídica, por la presunta comisión continuada de **delitos de descubrimiento y revelación de secretos** (arts. 197.1, 197.2, 197.3 y 197.5 del Código Penal), **acceso ilícito a sistemas de información** (art. 197 bis CP), **daños informáticos** (art. 264 CP), **publicidad engañosa** (art. 282 CP) y **responsabilidad penal de la persona jurídica** (arts. 31 bis y 197 quinquies CP) y otros delitos perseguibles de oficio en concurso, por acceso y recopilación masiva, sistemática y sin consentimiento válido de datos y **METADATOS** personales sensibles que merecen especial protección, y secretos de hasta **37 millones de usuarios españoles** de dispositivos Android, solicitando medida cautelar urgente, por todos estos **HECHOS:**

Primero.- Google, a través del sistema operativo Android, Google Play Services y aplicaciones preinstaladas (Play Store, Maps, Gmail, Chrome, YouTube, Photos y otras), recopila de forma sistemática y desde, al menos, el año 2022, datos personales sensibles, y secretos, incluyendo:

- Uso detallado de aplicaciones que posibilitan espionaje masivo y “AD HOC”.
- Contactos y comunicaciones con datos y metadatos ilícitamente obtenidos.
- Actividad física (sensores del dispositivo) que monitorizan y trazan al usuario de Android.
- Ubicación geográfica precisa y conexiones inalámbricas, permitiendo inferir domicilios, rutinas diarias y lugares habituales, así como el seguimiento en tiempo real de usuarios.
- Datos que revelan o permiten inferir categorías especiales: ideología, religión, creencias, salud, origen racial o étnico, vida sexual. Prácticamente, puede espiarse todo Android.

Segundo.- Esta recopilación se activa por defecto en la configuración inicial, sin opciones claras, para rechazar el seguimiento. Muchos datos recopilados no son necesarios en absoluto para el funcionamiento del dispositivo y no pueden desactivarse completamente. El artículo del Prof.

Doug Leith (Trinity College Dublin, febrero 2025: "Cookies, Identifiers and Other Data That Google Silently Stores on Android Handsets") publicado en **https://www.scss.tcd.ie/doug.leith/pubs/cookies_identifiers_and_other_data.pdf** documenta que Google almacena cookies publicitarias, identificadores persistentes y datos de seguimiento sin consentimiento explícito, incluso sin abrir apps de Google. Ese artículo evidencia los hechos y las intenciones técnicas, o "dolo tecnológico" de Google, y ha sido citado, al menos, por ABDALLAH, Ammar; AHMAD, Ala'eddin; SAID, Belal. Balancing privacy and usability: A design science research approach for cookie consent mechanisms. *Journal of Open Innovation: Technology, Market, and Complexity*, 2025, vol. 11, no 2, p. 100520 disponible en **https://www.sciencedirect.com/science/article/pii/S2199853125000551** que a su vez, a la fecha de hoy, ha sido citado al menos en otros dos artículos publicados en revistas referenciadas por Citation Index. Con toda seguridad, esas publicaciones, y la que desarrollen y precisen, más y mejor, todas las responsabilidades penales y los beneficios ilícitamente obtenidos por Google, van a tener consecuencias judiciales en varios países. APEDANICA está atenta a las nuevas publicaciones que puedan facilitar el trabajo de quienes tienen obligación de proteger, a todos los usuarios de Android, del espionaje masivo de Google.

Otros medios y análisis independientes han detectado y evidenciado el espionaje masivo en Android, reforzando su relevancia técnica y posibles consecuencias regulatorias/judiciales:

- **Trinity College Dublin (noticia oficial, 2025)**: Resalta que las apps de Google descargan cookies de tracking incluso sin abrirse, y que las reglas de cookies en apps móviles están poco reguladas comparado con la tecnología y el derecho en web. https://www.tcd.ie/e3/news/google-apps-silently-store-cookies-and-identifiers-on-android-phones-study-finds/
- **The Register (marzo 2025)**: Describe las prácticas como "spyware" sin consentimiento, destacando identificadores PII (información personalmente identificable) y ausencia de opt-out. Enfatiza violación de GDPR/UK GDPR. https://www.theregister.com/2025/03/04/google_android/
- **Malwarebytes (marzo 2025)**: Detalla al menos cinco tipos de identificadores sin consentimiento, ironizando sobre cookies como DSID que supuestamente "respetan" configuraciones de privacidad pero se instalan sin aviso. https://www.malwarebytes.com/blog/news/2025/03/android-devices-track-you-before-you-even-sign-in
- **ITC.ua (marzo 2025)**: Cubre el uso de NID cookies, tokens A/B y registro invisible en servicios Google, violando e-Privacy y GDPR. https://itc.ua/en/news/google-secretly-collects-information-from-android-devices-even-before-apps-are-launched/

Tercero.- Lo denunciado afecta potencialmente a toda la población española usuaria de Android (cuota >76%), constituyendo un espionaje digital masivo con ánimo de lucro publicitario y para entrenamiento de IA (incluyendo Gemini), vulnerando gravemente la intimidad (historial y rutinas revelan secretos íntimos, STS 489/2019). Los petabytes (unidad masiva de almacenamiento digital que equivale a 1024 terabytes TB o un millón de gigabytes GB) de datos extraídos y constituyen una "remesa ilícita" que circula, sin control alguno, hacia los servidores de Google.

Cuarto.- Google niega todas las acusaciones calificándolas de "incorrectas", pero no desmiente la recopilación, configurando dolo intencional en un modelo de negocio abusivo reincidente. Ver

TechXplore (19 diciembre 2025): "Google denies the claims and opposes the data request." Enlace: https://techxplore.com/news/2025-12-spanish-consumer-group-sue-google.html
Free Malaysia Today (20 diciembre 2025): "Google rejected claims that Android is a mass surveillance tool, urging courts to dismiss the AUC's intrusion request." (Rechaza que sea "herramienta de vigilancia masiva", pero no desmiente la recopilación subyacente). Enlace: https://www.freemalaysiatoday.com/category/business/2025/12/20/spanish-consumer-group-seeks-to-sue-google-in-data-row
The Economic Times (2025): "Google denies the claims, calling them misleading and intrusive." https://economictimes.indiatimes.com/tech/technology/spanish-consumer-group-seeks-to-sue-google-in-data-row/articleshow/126087670.cms

Quinto.- APEDANICA está proponiendo a sus miembros, y en general, a todos los usuarios del sistema Android en móviles smartphones, investigar a quien les espía mediante lo que denominamos como "**CRIPTOENTREGAS**" o **entregas controladas** AD HOC. En aras de la eficacia probatoria solicitamos que funcionarios de Policía Judicial, y también el Letrado de la Administración de Justicia, supervisen y den fe pública judicial de posibles resultados.

Ponemos en conocimiento del Juzgado el novedoso y trascendental medio de prueba "AD HOC" para que se practiquen urgentemente las DILIGENCIAS JUDICIALES DE COMPROBACIÓN, Y OTRAS DE INVESTIGACIÓN con el máximo valor probatorio en sede judicial, y para evitar acusaciones de "inducción al delito", también pedimos que las realice la Policía Judicial mediante su protocolo de "**entrega controlada**" o "**entrega vigilada**" *AD HOC* que proponemos por los arts. 263 bis, 299, 588 y 544 de la LECrim. Yo mismo me hago plenamente responsable de todo lo publicado en **https://cita.es/entregas-controladas.pdf**

Sexto.- Para mayor precisión probatoria, estamos utilizando Gemini, la Inteligencia Artificial IA de Google, para evidenciar lo que nadie mejor que Google conoce. No tenemos noticia de que nunca antes ningún juez haya conocido ningún caso de uso de una Inteligencia Artificial IA para evidenciar los delitos de su propietario, pero en este caso, Gemini reconoce hechos con relevancia penal y ofrece detalles que son indicios racionales de criminalidad. En este sentido, https://gemini.google.com/app/fe84f567c8774901 ilustra el conocimiento consciente de Google, por su IA Gemini de la gravedad de los hechos publicados mencionados en el hecho segundo sobre los que afirma textualmente lo siguiente:

Este es un análisis técnico-jurídico de los hechos expuestos en las investigaciones del Prof. Doug Leith (2025) y las publicaciones complementarias, bajo el prisma del Código Penal (CP) español.

El escenario descrito —la recolección masiva de identificadores persistentes (IMEI, Android ID, Advertising ID) y cookies (DSID, NID) sin consentimiento y de forma oculta— podría incardinarse en varios tipos delictivos, especialmente tras las últimas reformas en materia de delitos informáticos.

---

1. Descubrimiento y Revelación de Secretos (Delitos contra la Intimidad)

Este es el bloque de mayor gravedad. El Artículo 197 bis 1 es fundamental en este análisis.

- El Tipo: Castiga a quien, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización o se mantenga contra la voluntad de su titular en el conjunto o parte de un sistema de información.
- Relevancia en el caso: Si Google utiliza procesos "silenciosos" para extraer datos de un terminal (el cual es un sistema de información propiedad del usuario) sin que el usuario haya otorgado un consentimiento informado y previo, se está produciendo un acceso no autorizado a datos alojados en el dispositivo.
- Agravante (Art. 197.2): Se castiga la interceptación de datos de transmisión y el acceso a datos reservados de carácter personal que se hallen en ficheros o soportes informáticos. El uso de identificadores como el IMEI vinculados a cookies de seguimiento constituye,
  de facto, la creación de un perfil de usuario sin su permiso.

2. Daños Informáticos (Art. 264 y 264 ter)

Aunque no haya un "borrado" de archivos, el Código Penal español castiga la alteración del funcionamiento de sistemas.

- Art. 264 ter: Se refiere a la facilitación de programas o "cookies" maliciosas (entendidas técnicamente como herramientas de intrusión) diseñadas para cometer los accesos del 197 bis.
- Dolo Tecnológico: El hecho de que las cookies se descarguen *antes* de abrir cualquier app y sin que el usuario pueda evitarlas (ausencia de *opt-out*) sugiere un diseño deliberado para eludir los controles de privacidad del sistema operativo, lo que podría interpretarse como una "interfererencia grave" en la autodeterminación informativa del dispositivo.

3. Estafa de Infracciones de Propiedad Industrial y Mercado (Art. 278-282)

Dada la mención a los "beneficios ilícitamente obtenidos", entra en juego la protección de los consumidores y la competencia.

- Art. 282 bis: Delito de publicidad engañosa. Si Google promociona Android como un sistema que respeta la privacidad mientras técnicamente implementa un "espionaje masivo" mediante identificadores ocultos, podría haber una responsabilidad penal por perjudicar de forma masiva a los consumidores mediante alegaciones falsas sobre las características de seguridad del producto.
- Beneficio económico: El uso de estos datos para alimentar el ecosistema publicitario sin pagar el "precio" del consentimiento real constituye un beneficio patrimonial ilícito derivado de una conducta engañosa.

4. Responsabilidad Penal de las Personas Jurídicas (Art. 31 bis)

En España, Google (como entidad legal) puede ser imputada penalmente por los delitos cometidos en su nombre o por su cuenta, y en su beneficio directo o indirecto, por sus representantes legales o directivos.

- Falta de Medidas de Prevención: La existencia de estas prácticas "silenciosas" por diseño (Privacy by Design inverso) indicaría una ausencia de modelos de organización y gestión (Compliance) adecuados para evitar la comisión de delitos contra la intimidad de los usuarios a escala global.

Resumen de Gravedad Penal

Delito	Precepto CP	Gravedad Potencial	Conducta Clave
Intromisión Informática	Art. 197 bis	Muy Alta	Acceso a identificadores (IMEI/NID) sin permiso explícito.
Interceptación de Datos	Art. 197.2	Alta	Captura de cookies publicitarias de forma oculta.
Delitos contra Consumidores	Art. 282	Media-Alta	Engaño masivo sobre las opciones de privacidad de Android.
Daños Informáticos	Art. 264 ter	Media	Implementación de software de rastreo no autorizado.

Observación sobre el "Dolo Tecnológico"

El estudio del Prof. Leith es crucial porque demuestra que no se trata de un "error de código", sino de una arquitectura de sistema. En el derecho penal español, esto facilita la prueba del dolo (intencionalidad), ya que la persistencia de los identificadores y la imposibilidad de desactivarlos demuestran una voluntad consciente de vulnerar la esfera privada del usuario para obtener un lucro económico.

¿Desea que profundice en cómo se articularía una denuncia penal específica ante la Fiscalía de Criminalidad Informática en España basándome en estos hallazgos?

NOTA IMPORTANTE: La anterior conversación de la IA Gemini de Google está públicamente accesible completa e íntegra en el enlace https://gemini.google.com/share/a7a33d8c4407 y en

ese relevante enlace pueden hacerse más preguntas a la IA Gemini de Google sobre los hechos como si fuera un empleado de Google interrogado por un juez o un fiscal o un policía.

Séptimo.- APEDANICA está buscando algún precedente judicial de confesión o autoinculpación de una empresa tecnológica por medio de algo tan sofisticado como su propia Inteligencia Artificial IA como es el singular y gravísimo caso de los delitos imputables a Alphabet por Google y su Android mediante su propia IA Gemini. Es un audaz medio de prueba, o al menos, es la mejor fuente de muy relevantes indicios racionales, completamente novedoso y de máxima trascendencia criminológica y criminalística doctrinal y jurisprudencialmente, por lo que insistiremos en que por el Juzgador se tome pleno conocimiento de lo anterior comprobando lo que está publicado de la misma IA, en, repito, **https://gemini.google.com/share/a7a33d8c4407**

Octavo.- Pudiera parecer, creemos que erróneamente, que la competencia para investigar los hechos denunciados no corresponde a la Jurisdicción Penal, sino a la civil y a la administrativa. APEDANICA mantiene el criterio de que los hechos denunciados tienen relevancia penal, y además, tiene la más crítica opinión amparada por el artículo 20 de la Constitución Española hacia los máximos responsables de la Agencia Española de Protección de Datos AEPD, y en especial, denuncia el descarado conflicto de intereses de varios funcionarios, alguno incluso con empresa mercantil ostentando el cargo de Administrador Único, de manera incompatible e ilegal, y especialmente señalamos a su actual presidente ejecutivo, Lorenzo Cotino Hueso, por sus antecedentes publicados por La Razón el 23.04.2025 con el titular "***La sombra de las irregularidades tras el jefe de la Agencia Española de Protección de Datos. Si ya fue polémico su nombramiento, ahora se coloca bajo la lupa un proyecto que dirigió Lorenzo Cotino con Google por exceso de presupuesto***" (cita textual) que por su relevancia y trascendencia publicamos íntegro en **https://cita.es/lorenzo-cotino-google.pdf**

En nuestra opinión, es gravísimo que la máxima autoridad administrativa haya mantenido ese tipo de relaciones con Google, lo que le inhabilita para investigar los hechos denunciados al estar gravemente contaminado por un conflicto de intereses notorio, y obvio. Esas relaciones deberían ser investigadas por la Oficina de Conflictos de Intereses, pero según parece, no es competente porque la AEPD es un organismo autónomo y solamente su presidente puede sancionar las incompatibilidades, incluyendo las de funcionarios de la AEPD que administran y poseen empresas mercantiles, o realizan actividades remuneradas más incompatibles aún.

Considerando lo anterior, además de la Policía Judicial, dado el alcance masivo (hasta 37 millones de usuarios españoles afectados) y la elevada complejidad tecnológica de los hechos denunciados —que involucran la recopilación silenciosa y persistente de datos sensibles en dispositivos Android, incluso sin interacción del usuario, mediante cookies publicitarias,

identificadores persistentes y flujos de datos no consentidos, tal como documenta el informe pericial del Prof. Doug Leith ("Cookies, Identifiers and Other Data That Google Silently Stores on Android Handsets", de febrero 2025— con el debido respeto y como mejor proceda en Derecho, proponemos que se requiera informe pericial AD HOC al **Centro Criptológico Nacional CCN del Centro Nacional de Inteligencia CNI.**

El CCN-CNI es el organismo nacional experto en ciberseguridad, responsable de analizar riesgos, amenazas y vulnerabilidades en sistemas como Android, con un historial consolidado de publicaciones específicas sobre la seguridad de dispositivos móviles Google. Entre sus contribuciones relevantes destacan:

- Las Guías CCN-STIC 453 (series E, F, G, etc.) dedicadas a la seguridad de dispositivos móviles Android (versiones 7.x, 8, 9 y posteriores), que incluyen evaluaciones detalladas de mecanismos de configuración segura, riesgos asociados a la recopilación de datos, localización, servicios de Google Play y flujos de información hacia servidores externos (ej. Guía CCN-STIC 453E: https://www.ccn.cni.es/es/actualidad-ccn/314-dos-nuevas-guias-de-seguridad-sobre-dispositivos-moviles-android-y-su-cuenta-de-usuarios-de-google).
- La Guía CCN-STIC 456 sobre cuentas de usuario, servicios y aplicaciones de Google en Android, con análisis de privacidad en copias de seguridad, single sign-on y almacenamiento remoto de datos sensibles (misma referencia anterior).
- Informes anuales sobre amenazas en dispositivos móviles, que identifican Android como objetivo principal de ciberamenazas, incluyendo spyware, explotación de vulnerabilidades en componentes de bajo nivel y riesgos de exposición masiva de datos (ej. Informe Anual 2023: Dispositivos y Comunicaciones Móviles, disponible en secciones públicas de https://www.ccn.cni.es que es el web oficial al que nos remitimos, y también al subdominio https://www.ccn-cert.cni.es).

Los hechos denunciados pueden afectar a todo tipo de funcionarios públicos, por ejemplo, a diplomáticos en destinos conflictivos, pero también a miembros de los Cuerpos y Fuerzas de la Seguridad del Estado, Fiscales y por supuesto, magistrados-jueces (véase la Ley 11/2002 y el RD 421/2017). Es precisamente el CCN-CNI el organismo público que debe garantizar especialmente la seguridad de todas las comunicaciones, y de los datos sensibles, reservados o secretos, de los que son responsables los funcionarios públicos, pero también de todos los españoles y residentes en España, así como en el extranjero, funcionarios o no. El informe AD HOC del CCN-CNI resultaría de gran utilidad para esclarecer la gravedad técnica de las prácticas denunciadas (flujos de datos ilícitos, "remesa ilícita" de petabytes sensibles y posible dolo tecnológico), complementando las periciales propuestas y reforzando los indicios de encaje en los arts. 197 y ss. CP, más allá de meras infracciones administrativas. Ofrecemos

colaboración de APEDANICA para facilitar el análisis pericial de dispositivos testigo, así como para proyectar y ejecutar "**CRIPTOENTREGAS**" o **entrega controlada** AD HOC, pero creemos que la responsabilidad tecnológica última debería ser, al menos en España, del CCN-CNI.

FUNDAMENTOS JURÍDICOS:

Los hechos denunciados son constitutivos de delitos perseguibles de oficio, contra la intimidad y la protección de datos personales secretos, tipificados en el Capítulo I del Título X del Libro II del Código Penal (arts. 197 a 201 CP), en concurrencia ideal o medial con otras figuras delictivas, así como con responsabilidad penal de la persona jurídica (arts. 31 bis y 197 quinquies CP), por:

1. **Delito de descubrimiento y revelación de secretos (art. 197 CP)**:
   El apoderamiento ilegítimo de datos personales reservados (apartado 1), su utilización o modificación en perjuicio de tercero (apartado 2), y su difusión o cesión a terceros (apartado 3), sin consentimiento del afectado. La jurisprudencia del Tribunal Supremo (entre otras, STS 489/2019) ha interpretado que el mero acceso no autorizado a datos sensibles —como ubicación precisa, rutinas diarias, actividad física o datos que permiten inferir ideología, salud o vida sexual— vulnera la intimidad y causa perjuicio, al revelar aspectos del núcleo duro de la privacidad. Google ha hecho negocio de todo ello porque, en el presente caso, la recopilación sistemática y por defecto de tales datos sensibles (categorías especiales del art. 9 RGPD) activa el **agravante del apartado 5** (penas en su mitad superior cuando los datos revisten carácter especialmente protegido), y concurre ánimo de lucro (publicidad dirigida y entrenamiento de IA, incluyendo Gemini). La escala masiva (hasta 37 millones de usuarios en España) y la difusión implícita a servidores externos, sin control alguno, configuran una gravedad excepcional creciente.
2. **Acceso ilícito a sistemas de información (art. 197 bis CP)**:
   El acceso no autorizado a sistemas informáticos vulnerando medidas de seguridad (sandboxing de Android y ajustes de privacidad). Este tipo, introducido por LO 1/2015, protege la seguridad de los sistemas como barrera a la intimidad, consumándose con el mero acceso ilegítimo, incluso sin apoderamiento posterior (Circular 1/2015 de la Fiscalía General del Estado). Google ha accedido así a todos los sistemas Android.
3. **Daños informáticos (art. 264 CP)**:
   El consumo innecesario de recursos del dispositivo (sensores, batería, ancho de banda) para envíos silencios de datos, causando perjuicio patrimonial indirecto al usuario.
4. **Publicidad engañosa (art. 282 bis CP)**:
   Posible encaje subsidiario por inducción a error sobre el alcance real de la privacidad en Android (ajustes premarcados que simulan control, pero permiten tracking persistente).
5. **Responsabilidad penal de la persona jurídica (arts. 31 bis y 197 quinquies CP)**:
   Las entidades GOOGLE LLC (Alphabet Inc.), GOOGLE IRELAND LIMITED y GOOGLE

> SPAIN, S.L. podrían responder penalmente por deficiencias graves en modelos de cumplimiento (compliance), pese a multas previas acumuladas por prácticas similares (más de 5.000 millones de euros en sanciones GDPR europeas, incluyendo condenas específicas por tracking no consentido). El art. 31 bis CP exige programas efectivos de prevención; la reincidencia y el diseño deliberado del modelo de negocio (priorizando recopilación sobre privacidad) evidencian ausencia o ineficacia de tales medidas.

APEDANICA, además, tiene la fundada sospecha de que numerosas estafas son publicitadas utilizando datos espiados a los estafados por los medios aquí denunciados, de manera que existiría conexión con otros delitos que puedan estar siendo enjuiciados por estafas tipo pirámides Ponzi y criptoestafas, o falsas inversiones en activos fraudulentos, más sofisticadas, usualmente relacionadas con criptomonedas en las que Google tiene una doble responsabilidad, porque utiliza datos obtenidos delictivamente para vender publicidad a estafadores, y por otro, **dificultan el conocimiento público de advertencias de organismos reguladores, como la Comisión Nacional del Mercado de Valores CNMV, sobre "chiringuitos estafadores". Instamos a los representantes del Ministerio Público en casos de estafas masivas, mediante lo que se denomina como "publicidad inteligente", que usen alguno de los datos ilegalmente obtenidos por Google, para que se coordinen pronto y eficazmente.**

Aunque las vulneraciones más ordinarias del RGPD y LOPDGDD suelen resolverse por vía administrativa (AEPD) o civil, la doctrina y jurisprudencia reservan la vía penal para casos de especial gravedad: escala masiva, datos sensibles, perjuicio grave y directo a la intimidad, y dolo o intencionalidad técnica manifiesta (configuración por defecto no desactivable, negación pública sin desmentir hechos técnicos). Así lo avala la doctrina (entre otros, comentarios al CP de Tirant lo Blanch y análisis en Anuario de Derecho Penal y Ciencias Penales), que considera la tutela penal subsidiaria pero necesaria cuando la administrativa resulte insuficiente para proteger el bien jurídico (intimidad y autodeterminación informativa, art. 18.4 CE).

Invocamos los principios procesales **iura novit curia** (el juez conoce el Derecho y puede recalificar los hechos) y **da mihi factum, dabo tibi ius** (proporcionados los hechos, el tribunal aplicará el Derecho), solicitando la incoación de Diligencias Previas para investigar indicios robustos (informe pericial Doug Leith, febrero 2025; fuentes técnicas citadas; admisiones implícitas en respuestas de Gemini). Existe **periculum in mora** por reiteración diaria de la conducta y riesgo de destrucción o modificación de evidencias (logs, código fuente).

Por ello, entendemos que los hechos denunciados trascienden la mera infracción administrativa y revisten carácter de delito, justificando la intervención penal urgente, con medidas cautelares.

Por lo expuesto, AL JUZGADO SUPLICO: Que tenga por presentado este escrito, admita la denuncia, acuerde la incoación de Diligencias Previas y, previas las diligencias de comprobación oportunas, practique urgentemente las siguientes actuaciones de investigación, con el alcance y precisión que estime conveniente:

1. Requerimiento a las entidades GOOGLE SPAIN, S.L., GOOGLE IRELAND LIMITED y GOOGLE LLC (Alphabet Inc.) para que, en plazo perentorio y bajo apercibimiento de desobediencia del art. 556 CP o requerimiento coercitivo, aporten logs detallados, código fuente histórico y actual de los módulos de recopilación de datos en Android (incluyendo Google Play Services y aplicaciones preinstaladas), toda su documentación interna de evaluación de impacto (DPIA) relativa a tratamientos de datos en dispositivos Android en España, preservación inmediata de evidencias digitales relevantes y explicación técnica completa de los flujos de datos desde dispositivos españoles a servidores externos.
2. Informe policial urgente (art. 544 LECrim) a cargo de los peritos de la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional, o del Grupo de Delitos Telemáticos de la Guardia Civil, que incluya la reproducción de las situaciones y procedimientos del citado artículo del Prof. Doug Leith en dispositivos testigo, para el análisis exhaustivo de los flujos de datos, el registro de tráfico de red y la verificación de identificadores persistentes y cookies publicitarias instaladas sin consentimiento.
3. Informe pericial AD HOC al **Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI)**, dada su competencia funcional en análisis de vulnerabilidades y riesgos en sistemas como Android, para evaluar la gravedad técnica de las prácticas de Google aquí denunciadas y su impacto en la seguridad de comunicaciones y datos sensibles de funcionarios públicos, personas jurídicas y ciudadanos particulares.
4. Diligencias de comprobación e investigación tecnológica avanzada mediante protocolo de "**entrega controlada**" o "**entrega vigilada**" **AD HOC** (arts. 263 bis, 299, 588 y ss. LECrim) en la inteligencia artificial **Gemini** (gemini.google.com y aplicación móvil), supervisada por la Policía Judicial con fe pública y cadena de custodia estricta (capturas con timestamp y hash), para interrogar a Gemini sobre los hechos denunciados, seguir la "remesa ilícita" de petabytes de datos sensibles, y obtener posibles admisiones o autodelaciones relevantes penalmente (calificación como descubrimiento y revelación de secretos, dolo tecnológico, responsabilidad corporativa), generando informes periciales detallados y evitando cualquier posible inducción al delito, o sus pretextos.
5. **Medidas cautelares urgentes (arts. 13 y 544 LECrim):**
    - Orden de cese inmediato y provisional de la recopilación no consentida de datos sensibles en dispositivos Android en territorio español (desactivación remota de módulos de tracking y bloqueo de envíos a servidores externos), por concurrir **fumus boni iuris** (indicios robustos del informe Leith y fuentes técnicas),

periculum in mora (reiteración diaria y riesgo de destrucción de evidencias) y proporcionalidad (medida reversible y limitada al ámbito español).

- Prohibición temporal de modificación o actualización de Gemini que pudiera alterar respuestas relevantes para la investigación.

6. Comisión rogatoria internacional, si fuere necesario, para la práctica de diligencias en Irlanda o Estados Unidos, y coordinación con el Centro Criptológico Nacional CCN del Centro Nacional de Inteligencia CNI, INCIBE, Agencia Española de Protección de Datos (AEPD), Comisión Nacional de los Mercados y la Competencia (CNMC), el European Data Protection Board (EDPB) y autoridades europeas más competentes en aplicación del Digital Markets Act (DMA) y Digital Services Act (DSA), dado el carácter de Google como "gatekeeper" en toda la Unión Europea.

Ofrecemos la colaboración plena de APEDANICA, con responsabilidad individual o colectiva del representante, para la ejecución de periciales, ampliaciones, análisis de dispositivos testigo y proyección o ejecución de "**CRIPTOENTREGAS**" o **entregas controladas** AD HOC.

OTROSÍ 1 DIGO: Que, para la práctica de las diligencias propuestas, en especial las de entrega vigilada en Gemini y las periciales técnicas, se designe Policía Judicial especializada (BIT o Guardia Civil), con facultad para utilizar dispositivos testigo y herramientas de captura forense, acordándose si procediere el secreto de las actuaciones (art. 302 LECrim) durante el tiempo estrictamente necesario, más aún porque los hechos denunciados tienen trascendencia internacional y el conocimiento de las actuaciones de las fiscalías y de los juzgados de cada país por los demás es fundamental. Una cosa es la privacidad y el secreto de los datos y asuntos personales y otra la imprescindible transparencia sobre hechos con relevancia penal y sobre los medios tecnológicos utilizados para delinquir de los que todos debemos protegernos.

OTROSI 2 DIGO: Que se acuerde la acumulación de estas Diligencias Previas a cualquier otro procedimiento penal relacionado con los mismos hechos que pudiera estar tramitándose en otros Juzgados de Instrucción, conforme al art. 17.3 LECrim. En caso de que se tenga conocimiento de procedimientos civiles o administrativos relacionados con los hechos aquí denunciados (hay parciales y confusas noticias sobre alguna solicitud de práctica judicial de diligencias preliminares en la jurisdicción civil parece ser que pidiendo la identificación de los usuarios de productos Google y Android en España, estimados en 37 millones, para concretar quiénes son los afectados y determinar la cuantía de la indemnización por hechos que aquí entendemos que tienen naturaleza penal), que se oficie a los juzgados y a las autoridades competentes para que aporten todos los indicios racionales de criminalidad a este Juzgado.

OTROSI 3 DIGO: Que se tenga a APEDANICA por personada como perjudicada (disponemos de varios teléfonos móviles con Android de Google que usamos intensamente y representamos

a nuestros socios que pueden ser personas físicas o jurídicas) **como acusación particular**, o subsidiariamente, como acusación popular (art. 19 y 101 LECrim por art. 125 de la Constitución Española), con depósito provisional si fuere requerido, de mínima cuantía, y se nos notifiquen todas las resoluciones, motivadas y con pie de recurso AD HOC. Tenemos máximo interés por toda la complejidad tecnológica pericialmente relevante sobre los hechos denunciados, pero absolutamente ningún interés por ningún dato personal de nadie que no esté publicado con el expreso consentimiento del afectado (el presidente de APEDANICA autoriza expresamente la publicación de este escrito), por lo que **agradeceremos que se nos proporcione toda la información judicial posible, preferentemente bien anonimizada por el Juzgado**.

A los efectos de acreditar la representación de APEDANICA se adjunta documentación sobre nuestro registro oficial, situación fiscal, nuestros estatutos de fecha 9.12.1992 y la resolución por la que se inscribió en el Registro de Asociaciones del Ministerio del Interior con el número 116.377, todo ello publicado en **https://cita.es/apedanica-acreditada.pdf**

Por último, en este mismo PDF firmado digitalmente, se adjunta a continuación el informe elaborado por la Inteligencia Artificial IA Gemini 3 de Google en conversación recuperable y reproducible mediante el enlace **https://gemini.google.com/app/fe84f567c8774901**

Nótese en el informe ANEXO que es la misma Inteligencia Artificial IA Gemini 3 de Google la que va proponiendo ampliaciones de su propio informe, preguntando al usuario. He respondido a todo que “sí” salvo en único caso en el que he pedido una traducción al inglés para facilitar la solicitud de la comisión rogatoria que ya se ofrecía en castellano. Este denunciante está francamente sorprendido por lo mucho y bien que colabora la Inteligencia Artificial IA Gemini 3 de Google para hacer más eficaz la denuncia, incluyendo propuestas de citaciones e interrogatorios a los responsables de Google, y recomienda la máxima atención tanto a los juristas como a los expertos en tecnología de Inteligencia Artificial en todas las Ciencias de la Computación analizar el anexo porque nunca antes se ha visto algo así, que sepamos. En opinión del denunciante, el anexo plantea una situación completamente nueva para la Filosofía del Derecho y la Ética de la Inteligencia Artificial, digna, por lo menos, de varias tesis doctorales, pero antes, de la instrucción para garantizar la tutela judicial efectiva, inteligente y pronta.

Es de hacer Justicia que, en mi propio nombre y derecho, y también en representación de la asociación APEDANICA que presido desde 1992, pido en Madrid, en la fecha de la firma digital.

ANEXO: CITA TEXTUAL DE GEMINI 3 DISPONIBLE EN EL ENLACE

https://gemini.google.com/app/fe84f567c8774901

Este informe técnico-jurídico ha sido diseñado como un instrumento de refuerzo para la denuncia penal interpuesta por APEDANICA, disponible en https://www.miguelgallardo.es/denuncia-google-android.pdf. Su propósito es dotar al Juez de Instrucción de los argumentos técnicos y normativos necesarios para apreciar la concurrencia de indicios racionales de criminalidad y la urgencia de las diligencias propuestas.

INFORME TÉCNICO-JURÍDICO AD HOC DE REFUERZO (VERSIÓN INTEGRAL 2025)

ANEXO DOCUMENTAL A LA DENUNCIA PENAL CONTRA GOOGLE LLC / ALPHABET INC. POR ESPIONAJE MASIVO Y SISTEMÁTICO.

I. PREÁMBULO: EL "DOLO TECNOLÓGICO" COMO BASE DE LA ACCIÓN PENAL

La presente ampliación se fundamenta en el hallazgo de una arquitectura de vigilancia deliberada. A diferencia de errores puntuales de seguridad, las investigaciones del Prof. Doug Leith (Trinity College Dublin, febrero 2025) demuestran que Google ha implementado un sistema de "almacenamiento silencioso" de identificadores y cookies que operan al margen del consentimiento del usuario.

Este informe sostiene que estamos ante un caso de "Dolo Tecnológico": la voluntad consciente de diseñar un sistema operativo (Android) que elude los controles de privacidad declarados para maximizar la extracción de datos con fines lucrativos.

II. FUNDAMENTOS TÉCNICOS: EVIDENCIAS DE LA INTRUSIÓN

1. El "Silent Tracking" (Rastreo Silencioso)

Según el estudio de Leith (2025), Google Android almacena y transmite datos incluso antes de que el usuario abra cualquier aplicación de Google o inicie sesión.

- Identificadores Persistentes: Se capturan el IMEI, el número de serie del hardware y el Android ID. Al ser vinculados con cookies como DSID y NID, Google crea un "gemelo digital" del usuario que es imposible de anonimizar.

- Inoperancia del Opt-Out: Los mecanismos de "exclusión" (opt-out) publicitarios son meramente cosméticos para ciertos identificadores de bajo nivel que Google sigue utilizando para el perfilado.

2. El papel de la IA Gemini y el procesamiento masivo

La denuncia en https://www.miguelgallardo.es/denuncia-google-android.pdf subraya que estos datos alimentan los modelos de IA de Google (Gemini). Esto agrava el tipo penal, pues la información no solo se almacena, sino que se procesa algorítmicamente para inferir datos de salud, ideología y comportamiento íntimo sin base legal.

III. FUNDAMENTOS JURÍDICOS: SUBSUNCIÓN EN EL CÓDIGO PENAL ESPAÑOL

1. Delito de Descubrimiento y Revelación de Secretos (Art. 197.1 y 197.2 CP)

El Tribunal Supremo (STS 384/2013) establece que la protección de la intimidad no se limita a "secretos" en sentido estricto, sino a cualquier dato reservado.

- Hecho Típico: La interceptación de cookies (DSID, NID) y tokens de autorización sin consentimiento constituye un apoderamiento de datos reservados en soporte informático.
- Gravedad: Al afectar a millones de usuarios, el perjuicio es masivo, lo que obligaría a la aplicación de las penas en su mitad superior.

2. Acceso Ilícito a Sistemas de Información (Art. 197 bis CP)

Google utiliza su control sobre el kernel de Android para acceder a áreas del dispositivo (sandboxing) que el usuario cree protegidas.

- Conducta: Acceso no autorizado a identificadores de hardware (IMEI/Serial) mediante procesos ocultos que eluden las medidas de seguridad del propio sistema operativo promocionado como "seguro".

3. Publicidad Engañosa y Estafa de Mercado (Art. 282 bis CP)

Google promociona Android como un sistema que respeta la privacidad ("Privacy by Design"). Sin embargo, las evidencias técnicas demuestran lo contrario.

- Relevancia: Existe un engaño a los consumidores sobre las cualidades fundamentales del producto (su seguridad y privacidad), afectando a la competencia y al patrimonio de los usuarios (extracción de datos como activo económico).

IV. ANÁLISIS DE LAS DILIGENCIAS PROPUESTAS EN LA DENUNCIA

El informe del Prof. Leith y las publicaciones de *The Register* y *Malwarebytes* validan la necesidad imperiosa de las diligencias solicitadas en la denuncia de APEDANICA:

1. Pericial Informática de la Guardia Civil (BIT) o CNP: Para verificar que los terminales Android en España realizan las conexiones "silenciosas" descritas en el informe Leith 2025.
2. Requerimiento a Google Spain SL: Para que aporte los protocolos de cumplimiento (Compliance) que justifiquen la legalidad de la instalación de cookies DSID y NID antes de la interacción del usuario.
3. Informe del Centro Criptológico Nacional (CCN): Sobre el riesgo para la seguridad nacional que supone la recopilación masiva de metadatos de ciudadanos españoles por una entidad extranjera.
4. Interrogatorio de Gemini (IA): Como herramienta de "autodelación". Tal como indica la denuncia, la propia IA de Google, al ser consultada bajo parámetros técnicos, reconoce que estas prácticas podrían vulnerar el Art. 197 del CP.

V. CONCLUSIÓN PARA EL ÓRGANO JUDICIAL

La denuncia publicada en https://www.miguelgallardo.es/denuncia-google-android.pdf no es una mera queja administrativa; es la exposición de una vulneración estructural de los derechos fundamentales protegidos por el Código Penal.

La independencia judicial es el último baluarte ante el "espionaje masivo" documentado por el Trinity College Dublin. La admisión a trámite es necesaria no solo para castigar el hecho, sino para cesar de inmediato la comisión del delito que se produce en cada segundo que un terminal Android permanece encendido en territorio español.

¿Desea que redacte una estructura de interrogatorio pericial específico para que el juez pueda dirigirlo a los técnicos de Google basándose en estos hallazgos?

Esta estructura de interrogatorio está diseñada para que el Juez de Instrucción pueda interpelar tanto a los peritos judiciales (BIT/Guardia Civil) como a los representantes técnicos de Google Spain SL / Google Ireland Ltd. en calidad de investigados.

El objetivo es cercar técnicamente la defensa de la compañía, obligándoles a admitir la existencia de procesos que escapan al control del usuario y que se encuadran en el Art. 197 y 197 bis del Código Penal.

ESTRUCTURA DE INTERROGATORIO PERICIAL JUDICIAL (AD HOC)

Asunto: Investigación penal por espionaje masivo y acceso no autorizado en Android.

Referencia Técnica: Informe Prof. Doug Leith (2025) y Denuncia APEDANICA (https://www.miguelgallardo.es/denuncia-google-android.pdf).

BLOQUE I: Operaciones "Silenciosas" y Acceso sin Interacción (Art. 197 bis CP)

Justificación: Demostrar que el acceso al sistema de información del usuario se produce sin su consentimiento ni conocimiento.

1. ¿Puede confirmar si los servicios "Google Play Services" y el proceso "com.google.android.gms" inician transferencias de datos a servidores de Google inmediatamente después de un restablecimiento de fábrica, incluso antes de que el usuario inicie sesión o abra una aplicación?
2. En caso afirmativo, ¿qué base técnica justifica que el dispositivo "despierte" procesos de red para enviar identificadores de hardware (IMEI/Serial) sin que el usuario haya aceptado aún los Términos de Servicio en esa sesión?
3. Según el informe de la Universidad de Dublín (2025), se instalan cookies de rastreo como DSID y NID de forma silenciosa. ¿Puede explicar la finalidad técnica de instalar una cookie publicitaria (DSID) en un sistema operativo antes de que el usuario haya interactuado con ninguna función publicitaria?

BLOQUE II: Identificadores Persistentes y Perfilado (Art. 197.2 CP)

Justificación: Demostrar que los datos recogidos son "datos reservados" que permiten la identificación unívoca del individuo.

4. ¿Existe alguna forma técnica para que un usuario de Android desvincule totalmente su "Android ID" y su "Advertising ID" de su identidad real, sin que Google pueda volver a asociarlos mediante la dirección IP o el IMEI?
5. ¿Es cierto que, aunque el usuario desactive el "Personalized Ads", Google continúa recopilando el "AdAttest Token" y otros identificadores de bajo nivel que permiten el seguimiento "cross-device"?
6. ¿Cómo garantiza Google que los metadatos de las aplicaciones preinstaladas (que registran cada vez que se abre o cierra una app) no se utilizan para inferir hábitos de vida, salud o religión del usuario sin su permiso explícito?

BLOQUE III: Inexistencia de Consentimiento Válido (Dolo Tecnológico)

Justificación: Desmontar la defensa del "consentimiento por aceptación de términos" (Art. 6 y 7 RGPD en relación al CP).

7. ¿Existe algún mecanismo en la interfaz de usuario de Android que permita al ciudadano español desactivar la descarga y almacenamiento de las cookies NID y DSID sin deshabilitar las funciones básicas de telefonía del terminal?
8. Si la respuesta es negativa, ¿no estaríamos ante un diseño que impone la vigilancia como condición para el uso de un bien de consumo básico?
9. ¿Por qué el "opt-out" de privacidad en Android no detiene la comunicación de procesos internos hacia el dominio android.clients.google.com, el cual el Prof. Leith identifica como un vector de extracción de metadatos?

BLOQUE IV: Destino de los Datos e Inteligencia Artificial (IA Gemini)

Justificación: Vincular el lucro cesante y el beneficio ilícito (Art. 197.4 CP).

10. ¿Se utilizan los datos "silenciosos" recopilados por Google Play Services para el entrenamiento, refinamiento o validación de los modelos de lenguaje de Gemini (IA)?
11. ¿Qué valor económico estima Google que genera la extracción masiva de metadatos de los 37 millones de usuarios en España para la optimización de sus sistemas publicitarios y de IA? (Esta pregunta busca cuantificar el beneficio delictivo).
12. ¿Puede asegurar bajo juramento que los datos obtenidos mediante el proceso "Droidguard" no son utilizados para el perfilado comercial de los usuarios fuera de las finalidades estrictamente de seguridad?

BLOQUE V: Responsabilidad de la Persona Jurídica (Art. 31 bis CP)

Justificación: Evidenciar la falta de control y el diseño deliberado.

13. ¿Dispone Google de una evaluación de impacto específica para el mercado español que analice la legalidad penal (no solo administrativa) de la recopilación de datos sin "opt-out" real en Android?
14. ¿Qué directivo o comité de ingeniería tomó la decisión técnica de que las cookies de tracking se descarguen automáticamente sin aviso previo al usuario en las versiones de Android de 2024 y 2025?

Sugerencia de Próximo Paso para el Letrado/Denunciante:

Este interrogatorio debería ir acompañado de una Solicitud de Comisión Rogatoria Internacional a las sedes de Google en Dublín y Mountain View, exigiendo la entrega del código fuente de los módulos de comunicación de *Google Play Services* que gestionan las cookies mencionadas en el informe Leith.

¿Desea que prepare el texto de la solicitud de medidas cautelares para exigir el cese inmediato de la descarga de cookies DSID/NID en territorio español hasta que se resuelva el juicio?

A continuación, presento la propuesta de solicitud de medidas cautelares redactada con el rigor técnico y jurídico necesario para ser presentada ante el Juzgado de Instrucción.

Este escrito se fundamenta en la necesidad de detener la lesión continuada del derecho fundamental a la intimidad (Art. 18 CE) y evitar que el daño sea irreversible durante el tiempo que dure la instrucción.

SOLICITUD DE MEDIDAS CAUTELARES URGENTES (Art. 13 LECrim)

AL JUZGADO DE INSTRUCCIÓN QUE CONOZCA DE LA DENUNCIA DE APEDANICA

OBJETO: Interrupción inmediata de la recopilación no consentida de identificadores persistentes y cookies de seguimiento en dispositivos Android dentro del territorio nacional.

I. FUNDAMENTOS JURÍDICOS DE LA MEDIDA

La adopción de medidas cautelares en el proceso penal español se rige por dos principios que concurren plenamente en este caso:

1. Fumus Boni Iuris (Apariencia de Buen Derecho): Las evidencias técnicas aportadas por el Prof. Doug Leith (2025) y las publicaciones de revistas indexadas (Citation Index) constituyen un principio de prueba robusto sobre la comisión de delitos previstos en los Arts. 197 y 197 bis del Código Penal.
2. Periculum in Mora (Peligro por la Mora Procesal): Cada segundo que transcurre, el sistema operativo Android en España (con una cuota de mercado superior al 76%) continúa extrayendo datos de 37 millones de usuarios. Una vez que esos datos son integrados en los modelos de IA de Google (Gemini), el daño a la privacidad es irreparable, pues no existe tecnología de "des-aprendizaje" que garantice la eliminación total de la huella digital del usuario.

II. PETICIÓN CONCRETA DE MEDIDAS

Se interesa del Juzgado que, con carácter urgente, acuerde:

- A) Cese inmediato de la descarga silenciosa: Ordenar a Google Ireland Ltd. y Google Spain SL la modificación técnica de los servicios *Google Play Services* en territorio español para que cesen de almacenar las cookies DSID y NID, así como los tokens de seguimiento de bajo nivel, en tanto el usuario no haya otorgado un consentimiento expreso, positivo y granular tras ser informado de la finalidad comercial de dichos datos.
- B) Bloqueo de transmisión de identificadores de hardware: Prohibir la transmisión del IMEI y el número de serie del hardware vinculados a cuentas de usuario para fines publicitarios o de

entrenamiento de IA, limitando su uso estrictamente a funciones de seguridad y autenticación técnica esencial.

- C) Implementación de un "Kill Switch" de Privacidad: Obligar a Google a desplegar una actualización de seguridad que incluya un interruptor único y accesible que permita al usuario español detener toda comunicación de procesos de fondo hacia los dominios de recolección de metadatos (ej. `android.clients.google.com`).

III. JUSTIFICACIÓN DE LA PROPORCIONALIDAD

La medida es proporcionada puesto que:

- No impide el funcionamiento básico del teléfono (llamadas, mensajes, apps de terceros).
- Solo afecta a los procesos de "rastreo silencioso" que el Prof. Leith ha identificado como no esenciales para la operatividad del sistema.
- Protege el orden público y la seguridad nacional, evitando que el perfilado masivo de la población española sea utilizado por una corporación extranjera para manipular mercados o tendencias de opinión mediante IA.

IV. DILIGENCIA DE COMPROBACIÓN (LA "PRUEBA DEL ALGODÓN")

Para que el Juez pueda verificar la necesidad de esta medida, se propone la siguiente Diligencia de Prueba Anticipada:

> "Que se proceda a la entrega de un dispositivo Android nuevo, sellado, a los peritos de la Unidad de Delitos Informáticos para que, en presencia judicial, se encienda el terminal sin introducir cuenta de Google y se monitorice el tráfico de red mediante un 'Man-in-the-Middle' (MITM). Si el dispositivo intenta contactar con servidores de Google y descargar cookies de rastreo sin intervención humana, quedará acreditado el hecho delictivo de acceso no autorizado y la urgencia de la medida cautelar."

Refuerzo adicional para el Juez: El riesgo de la IA

Es vital subrayar al instructor que estos datos alimentan a Gemini. Si el Juez no detiene la entrada de datos hoy, cualquier sentencia condenatoria futura será inútil, pues Google ya habrá obtenido el beneficio (el entrenamiento de su IA con datos ilícitos) y los ciudadanos habrán perdido su intimidad para siempre.

¿Desea que redacte el oficio formal dirigido a la Agencia Española de Protección de Datos (AEPD) para que, en auxilio judicial, emita un informe urgente sobre la imposibilidad de 'opt-out' en estas cookies específicas?

Esta es la propuesta formal y técnica de Oficio de Requerimiento que el Juzgado de Instrucción debería dirigir a la Presidencia de la Agencia Española de Protección de Datos (AEPD).

El objetivo es que el Juez utilice a la AEPD como auxilio judicial técnico para validar los hechos denunciados, obligando a la Agencia a pronunciarse sobre la inviabilidad técnica del "opt-out" en Android, lo cual es la clave del dolo penal.

PROPUESTA DE MANDAMIENTO JUDICIAL DE REQUERIMIENTO TÉCNICO A LA AEPD

AL JUZGADO DE INSTRUCCIÓN Nº [Insertar Número] DE [Ciudad]

DILIGENCIAS PREVIAS: [Insertar número] / PROCEDIMIENTO: DELITOS CONTRA LA INTIMIDAD

A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)

En virtud de lo dispuesto en los artículos 18.4 de la Constitución Española, 11 y 13 de la Ley de Enjuiciamiento Criminal, y en el marco de la cooperación institucional, se requiere a la Agencia Española de Protección de Datos para que, a través de su División de Evaluación y Estudios Tecnológicos, emita un INFORME PERICIAL URGENTE sobre los siguientes extremos técnicos relacionados con el sistema operativo Android y los servicios de Google:

1. Sobre la Persistencia y Opacidad de Identificadores

- Identificación de Cookies Silenciosas: Analice la existencia y el comportamiento de las cookies DSID y NID en dispositivos Android. Especifique si dichas cookies se descargan y almacenan en el terminal de forma previa a cualquier interacción del usuario con servicios publicitarios.
- Vinculación unívoca: Determine si la combinación del IMEI, el Android ID y estas cookies permite a Google identificar de forma única al usuario, incluso si este ha reseteado su ID publicitario o utiliza el dispositivo sin haber iniciado sesión en una cuenta personal.

2. Sobre la Imposibilidad Técnica de "Opt-Out" (Derecho de Oposición)

- Inexistencia de controles: Informe si existe en la interfaz estándar de Android (versiones 14 y 15) un mecanismo que permita al usuario bloquear o eliminar de forma permanente la generación de las cookies DSID/NID sin comprometer la funcionalidad básica del dispositivo.
- Eficacia de los ajustes de privacidad: Evalúe si la opción "Eliminar ID de publicidad" detiene efectivamente la transmisión de metadatos de uso hacia los servidores de Google (`android.clients.google.com`) o si, por el contrario, el rastreo continúa mediante identificadores de bajo nivel (como el *AdAttest Token*).

3. Sobre el Cumplimiento del Principio de "Privacidad por Defecto"

- Configuración de fábrica: Dictamine si el diseño actual de los *Google Play Services* cumple con el principio de Privacidad desde el Diseño y por Defecto (Art. 25 RGPD), o si la arquitectura del sistema operativo está configurada para la extracción máxima de datos de forma predeterminada.
- Análisis de Flujo hacia la IA: Informe sobre si el tratamiento de estos datos "silenciosos" es compatible con las finalidades declaradas por Google o si, técnicamente, estos datos son aptos para el entrenamiento de modelos de inteligencia artificial (Gemini) sin una base legal específica.

FUNDAMENTACIÓN DE LA URGENCIA PARA LA AEPD

Se hace saber a la AEPD que el presente requerimiento se enmarca en una investigación penal por Descubrimiento y Revelación de Secretos (Art. 197 CP). El informe solicitado es esencial para determinar la concurrencia de dolo tecnológico, entendido como la implementación deliberada de barreras técnicas que impiden al ciudadano español ejercer su derecho a la intimidad y a la autodeterminación informativa.

PLAZO DE ENTREGA: Se concede un plazo máximo de diez (10) días hábiles debido a la naturaleza continuada del presunto ilícito y el riesgo de afectación masiva a derechos fundamentales de millones de usuarios en territorio español.

Por qué este oficio es estratégico para la denuncia:

1. Fuerza a la AEPD a tomar partido: Históricamente, la AEPD ha sido lenta en actuar contra las Big Tech. Un requerimiento judicial la obliga a actuar como perito del Estado.
2. Prueba pericial preconstituida: Si la AEPD confirma que no hay "opt-out" real para las cookies DSID/NID, el Juez tendrá la prueba técnica definitiva del acceso no autorizado (Art. 197 bis CP).
3. Evidencia el engaño: Si Google dice que Android es privado y la AEPD demuestra lo contrario, el delito de publicidad engañosa queda automáticamente acreditado.

¿Le gustaría que redactara ahora la solicitud de citación judicial para el Director de Ingeniería de Privacidad de Google, a fin de que comparezca como investigado y responda sobre estas contradicciones técnicas?

Esta es la propuesta formal de Solicitud de Citación en Calidad de Investigado para el máximo responsable técnico de Google en Europa/España.

Este escrito busca que el Juez de Instrucción no se conforme con una respuesta por escrito del departamento legal de Google, sino que exija la presencia física (o por videoconferencia judicial) del responsable de la arquitectura de privacidad para que responda bajo apercibimiento penal sobre las contradicciones técnicas detectadas.

SOLICITUD DE CITACIÓN JUDICIAL EN CALIDAD DE INVESTIGADO

AL JUZGADO DE INSTRUCCIÓN Nº [Número] DE [Ciudad]

DILIGENCIAS PREVIAS: [Número] / DELITOS CONTRA LA INTIMIDAD

A LA ATENCIÓN DEL MAGISTRADO-JUEZ:

La representación procesal de la parte denunciante, en el ejercicio de las facultades que le otorga la Ley de Enjuiciamiento Criminal (LECrim), comparece y, como diligencia de investigación esencial para el esclarecimiento de los hechos, SOLICITA:

I. DESIGNACIÓN DEL INVESTIGADO

Se proceda a la citación, para que preste declaración en calidad de INVESTIGADO (con asistencia letrada), al Director de Ingeniería de Privacidad (Privacy Engineering Director) de Google Ireland Limited (en su condición de Responsable del Tratamiento para el EEE) y, subsidiariamente, al responsable técnico de Google Spain SL.

Se requiere que la entidad Google identifique con nombre y apellidos al directivo con competencia directa sobre el diseño de la arquitectura de "Google Play Services" y la integración de metadatos en el modelo de IA Gemini.

II. OBJETO DE LA COMPARECENCIA (CONTRADICCIONES TÉCNICAS)

El investigado deberá responder sobre los siguientes extremos que evidencian el "Dolo Tecnológico" y la posible comisión de los delitos tipificados en los Arts. 197 y 197 bis del Código Penal:

Punto de Contradicción	Realidad Declarada por Google	Evidencia Técnica (Leith 2025 / Denuncia)
Consentimiento	El usuario "elige" qué datos comparte.	Cookies DSID/NID se instalan antes de que el usuario pueda elegir o abrir ninguna app.
Identificadores	Los ID de publicidad son "reseteables".	El IMEI y el Android ID permanecen vinculados de forma persistente y secreta en los servidores.

Opt-Out	"Eliminar ID de publicidad" detiene el rastreo.	El tráfico hacia android.clients.google.com persiste con tokens de seguridad (AdAttest) usados para perfilado.
Finalidad IA	Mejora de la experiencia del usuario.	Extracción masiva de metadatos para alimentar el entrenamiento de Gemini sin consentimiento específico.

III. MOTIVACIÓN DE LA CONDICIÓN DE INVESTIGADO

La citación debe realizarse bajo la condición de investigado y no como testigo, por cuanto:

1. Responsabilidad Corporativa (Art. 31 bis CP): Los hechos denunciados no son fruto de un error técnico fortuito, sino de un diseño de sistema deliberado que beneficia económicamente a la persona jurídica.
2. Derecho de Defensa: Dada la gravedad de las penas asociadas al Art. 197 CP, el responsable técnico debe comparecer con todas las garantías procesales, pudiendo negarse a declarar sobre aspectos que pudieran autoincriminar a la compañía, pero quedando bajo el control del Instructor.

IV. REQUERIMIENTO PREVIO DE EXHIBICIÓN DOCUMENTAL

Se solicita que, con al menos cinco días de antelación a la declaración, el investigado aporte al Juzgado:

- A) El Registro de Actividades de Tratamiento (RAT) específico para los datos capturados por los servicios de fondo de Android en territorio español.
- B) La Evaluación de Impacto (EIPD) que justifique legalmente por qué las cookies publicitarias se descargan "en frío" (nada más encender el dispositivo por primera vez).

V. CONCLUSIÓN Y PETITORIO

La declaración del Director de Ingeniería es la única vía para romper la opacidad de los algoritmos de Google. El contraste entre sus declaraciones y los hallazgos del informe del Prof. Leith (Trinity College Dublin) permitirá a este Juzgado constatar si Google ha engañado de forma masiva a los usuarios españoles, accediendo a sus terminales de forma ilícita.

POR TODO LO EXPUESTO, SOLICITO AL JUZGADO: Que tenga por presentado este escrito, lo una a las actuaciones y acuerde la citación del representante técnico de Google en los términos solicitados.

Estrategia para el denunciante:

Al pedir que declare como investigado, se le pone en una posición de debilidad. Si miente ante el Juez y el peritaje posterior (de la Guardia Civil o la AEPD) demuestra que los datos sí se envían silenciosamente, la posición procesal de Google en España se volvería insostenible.

¿Desea que redacte ahora una solicitud de "Exhorto o Comisión Rogatoria" para requerir formalmente a Google la entrega del código fuente de los módulos responsables de la comunicación de estas cookies?

Esta es la propuesta formal de Comisión Rogatoria Internacional y Exhorto dirigida a las autoridades judiciales de Irlanda (donde Google tiene su sede europea) y, subsidiariamente, a los Estados Unidos (sede de Alphabet Inc.).

Este documento es una de las herramientas más potentes del Juez de Instrucción, ya que obliga a Google a entregar evidencias que no están en suelo español, bajo los tratados de auxilio judicial mutuo en materia penal.

PROPUESTA DE COMISIÓN ROGATORIA INTERNACIONAL Y EXHORTO JUDICIAL

AL JUZGADO DE INSTRUCCIÓN Nº [Número] DE [Ciudad]

DILIGENCIAS PREVIAS: [Número] / DELITOS CONTRA LA INTIMIDAD

A LA ATENCIÓN DE LA AUTORIDAD JUDICIAL COMPETENTE DE IRLANDA (DUBLÍN) / ESTADOS UNIDOS (CALIFORNIA):

El Juzgado de Instrucción de [Ciudad], España, en el ejercicio de sus competencias y en virtud de los Convenios de Asistencia Judicial Mutua en Materia Penal (Convenio de la Unión Europea de 2000 y Tratados Bilaterales con EE. UU.), interesa la práctica de la siguiente DILIGENCIA DE PRUEBA dirigida a las entidades GOOGLE IRELAND LIMITED y GOOGLE LLC:

I. OBJETO DEL REQUERIMIENTO: CÓDIGO FUENTE Y LOGS DE SISTEMA

Se requiere de forma imperativa la entrega y exhibición ante este Juzgado (o ante la autoridad judicial requerida para su remisión) de la siguiente documentación técnica y digital:

1. Segmentos de Código Fuente (Source Code):
    - Módulos de comunicación de la librería com.google.android.gms (Google Play Services) responsables de la generación, almacenamiento y transmisión de las cookies DSID y NID en dispositivos Android (versiones 14 y 15).
    - Lógica algorítmica que determina la transmisión de identificadores de hardware (IMEI, Número de Serie, Android ID) antes de que el usuario proceda al inicio de sesión (Log-in) o acepte los términos de servicio tras un "factory reset".
2. Protocolos de Telemetría:

   - Especificaciones técnicas de los paquetes de datos enviados al dominio android.clients.google.com. Se requiere conocer qué datos exactos se encapsulan bajo el token "AdAttest" y si dichos datos son disociados de la identidad real del usuario de forma irreversible.
3. Documentación de Integración con IA (Gemini):
   - Esquema de flujo de datos (Data Flow Diagrams) que detalle el camino de los metadatos recolectados "silenciosamente" desde los dispositivos Android hacia los servidores de entrenamiento de los modelos de Inteligencia Artificial Gemini.

II. JUSTIFICACIÓN DE LA NECESIDAD Y PROPORCIONALIDAD

Esta medida es indispensable para la averiguación del delito de Descubrimiento y Revelación de Secretos (Art. 197 CP español) por los siguientes motivos:

- Imposibilidad de obtención alternativa: La prueba se halla bajo el control exclusivo de la entidad denunciada en sus sedes centrales.
- Evidencia del Dolo: Solo el análisis del código fuente permitirá determinar si la captura de datos sin consentimiento es un "comportamiento deliberado de diseño" (Dolo Tecnológico) o una contingencia técnica.
- Verificación de Hallazgos Internacionales: Es necesario contrastar judicialmente las investigaciones del Trinity College Dublin (2025) que denuncian el espionaje masivo.

III. GARANTÍA DE CONFIDENCIALIDAD (SECRETOS COMERCIALES)

Este Juzgado reconoce que el código fuente constituye un activo crítico. Por ello, se ofrece la posibilidad de que la exhibición se realice mediante "In-Camera Review" (revisión en sede judicial restringida) por parte de peritos oficiales de la unidad de delitos informáticos (Guardia Civil/BIT), bajo estricto deber de secreto, con el único fin de informar al Juez sobre la existencia de los procesos de rastreo denunciados.

IV. APERCIBIMIENTO

El incumplimiento o la falta de colaboración en la entrega de estos elementos será interpretado como una obstrucción a la justicia y podría derivar en la imputación de responsabilidades penales adicionales a los directivos de las filiales locales, así como en la adopción de medidas cautelares más gravosas (bloqueo de servicios).

Impacto Estratégico de esta Diligencia:

1. El "Miedo" de Google: El código fuente es su secreto mejor guardado. Pedirlo judicialmente pone a la compañía en la posición de tener que elegir entre la transparencia judicial o admitir que su sistema es opaco.
2. Conexión con la Denuncia: Este exhorto es la ejecución directa de la petición de peritaje independiente solicitada en https://www.miguelgallardo.es/denuncia-google-android.pdf.

3. Cooperación Internacional: Al citar el informe del Prof. Leith (Irlanda), el Juez español facilita que el juez irlandés colabore, pues el origen de la prueba técnica es de su propia jurisdicción.

¿Desea que redacte una "Nota de Prensa Jurídica" o un resumen ejecutivo para medios de comunicación, con el fin de que la opinión pública conozca la contundencia de estas medidas y presione socialmente en defensa de la privacidad de los usuarios de Android?

No, traduce lo anterior al inglés jurídico para facilitar al máximo el trabajo del Juzgado de Instrucción español para dirigirse a las autoridades irlandesas

Esta es la traducción técnica y jurídica al inglés del documento de Comisión Rogatoria Internacional (Letter Rogatory).

Este formato sigue los estándares internacionales de Auxilio Judicial Mutuo (MLA) para que el Juzgado de Instrucción español pueda remitirlo directamente a las autoridades de Irlanda (Central Authority for Mutual Assistance) con el fin de obtener las pruebas en la sede de Google en Dublín.

FORMAL REQUEST FOR MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS (LETTER ROGATORY)

FROM: Investigating Court No. [Number], [City], Spain.

TO: The Competent Judicial Authority of Ireland (The Central Authority, Department of Justice).

CASE REFERENCE: Preliminary Proceedings [Number] – Crimes Against Privacy (Art. 197 Spanish Penal Code).

I. INTRODUCTION AND SUMMARY OF THE INVESTIGATION

The Investigating Court of [City], Spain, is currently conducting a criminal investigation against GOOGLE IRELAND LIMITED and its parent company, ALPHABET INC., for the alleged commission of Discovery and Revelation of Secrets and Illicit Access to Information Systems (Articles 197 and 197 bis of the Spanish Penal Code).

The investigation stems from technical evidence—supported by the study of Prof. Doug Leith (Trinity College Dublin, February 2025)—indicating that the Android Operating System, through "Google Play Services," performs mass, silent, and unauthorized collection of user metadata, persistent identifiers (IMEI, Serial Number, Android ID), and tracking cookies (DSID, NID) without valid user consent.

II. PURPOSE OF THE REQUEST: DISCOVERY OF EVIDENCE

To determine the existence of "Technological Intent" (Dolo Tecnológico) and the scope of the unauthorized data extraction, this Court hereby requests the following evidence from the offices of Google Ireland Ltd. in Dublin:

1. Disclosure of Source Code (Technical Modules)

- Source Code Segments: Access to the specific modules within the com.google.android.gms (Google Play Services) library responsible for the automated generation, storage, and transmission of DSID and NID cookies.
- Trigger Logic: Documentation of the algorithmic logic that initiates data transfers to Google servers immediately upon factory reset, prior to any user interaction, log-in, or acceptance of terms of service.

2. Telemetry and Data Flow Documentation

- Metadata Encapsulation: Technical specifications of data packets transmitted to the domain android.clients.google.com, specifically detailing the information contained within the "AdAttest" security tokens and whether such data is irreversibly de-identified.
- AI Integration (Gemini): Detailed Data Flow Diagrams illustrating the path of "silently collected" metadata from Android devices to the training environments of Google's Artificial Intelligence models (Gemini).

3. Internal Compliance and Impact Assessments

- DPIAs: Copies of the Data Protection Impact Assessments regarding the collection of hardware identifiers in the European Economic Area (EEA) for the years 2024-2025.

III. NECESSITY AND PROPORTIONALITY

This request is essential for the criminal proceedings in Spain because:

- Exclusive Control: The evidence is held exclusively by the investigated party at its European headquarters in Dublin.
- Mass Impact: The alleged criminal activity affects over 37 million users in Spain, constituting a significant breach of fundamental rights to privacy (Art. 18 Spanish Constitution and Art. 8 ECHR).
- Avoidance of Irreparable Harm: The continuous integration of this data into AI models makes the damage to citizens' privacy irreversible.

IV. CONFIDENTIALITY AND RECIPROCITY

This Court guarantees that any trade secrets or proprietary source code disclosed will be handled with the utmost confidentiality. Access will be restricted to court-appointed forensic experts under a strict duty of secrecy. The Spanish Judiciary offers full reciprocity to the Irish Authorities in similar matters.

V. FORMAL PETITION

We respectfully request the Competent Authority of Ireland to:

1. Serve this request upon Google Ireland Limited.
2. Compel the production of the requested technical documentation and source code.
3. Facilitate the taking of testimony from the Director of Privacy Engineering at Google Ireland Ltd. via judicial videoconference.

Instrucciones para el Juzgado (Nota Técnica):

- Tratado Aplicable: Se recomienda citar el *Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union* (2000).
- Urgencia: Debe marcarse como "URGENT - DATA SUBJECT TO POTENTIAL DESTRUCTION" para evitar que Google alegue ciclos de rotación de logs o borrado de versiones de código.

¿Desea que prepare el "Index of Exhibits" (Índice de Pruebas) en inglés para adjuntar el informe del Prof. Leith y la denuncia de APEDANICA de forma que la autoridad irlandesa identifique rápidamente la base del cargo?

Este es el Index of Exhibits (Índice de Pruebas) redactado en inglés jurídico profesional. Su función es servir de guía rápida para que el Juez irlandés o el Fiscal encargado de cumplimentar la Comisión Rogatoria comprenda inmediatamente la conexión entre la evidencia técnica y el tipo penal imputado en España.

ANNEX I: INDEX OF EXHIBITS AND SUPPORTING EVIDENCE

ATTACHED TO THE LETTER ROGATORY FROM INVESTIGATING COURT NO. [NUMBER], SPAIN

This Index categorizes the evidence supporting the criminal allegations of Technological Intent (Dolo) and Mass Unauthorized Data Access.

EXHIBIT NO. 1: THE PRIMARY TECHNICAL PERITAGE

- Title: *"Cookies, Identifiers and Other Data That Google Silently Stores on Android Handsets"* (February 13, 2025).
- Author: Prof. Doug Leith, School of Computer Science and Statistics, Trinity College Dublin.
- Key Findings: Documentation of "cold" data exfiltration (IMEI, Android ID) and silent cookie storage (DSID/NID) without user interaction or log-in.

- Legal Relevance: Provides the technical basis for Article 197 bis (Unauthorized Access) and Article 197.2 (Misuse of Reserved Personal Data) of the Spanish Penal Code.

EXHIBIT NO. 2: THE CRIMINAL COMPLAINT (INITIATING DOCUMENT)

- Title: *Criminal Complaint against Google for Mass Spying on Android and Gemini AI.*
- Source: APEDANICA (Association for the Prevention and Study of Delicts, Negligence and Abuse in Computer Science and Communications).
- Reference URL: https://www.miguelgallardo.es/denuncia-google-android.pdf
- Legal Relevance: Establishes the jurisdictional grounds and the specific criminal charges under Spanish Law, representing the interests of approximately 37 million affected users.

EXHIBIT NO. 3: CORROBORATIVE CYBERSECURITY REPORTS

- Content: Compilation of reports from *The Register*, *Malwarebytes*, and *ITC.ua* (March 2025).
- Key Findings: Independent verification of the "spyware-like" behavior of Google Play Services and the absence of a genuine "opt-out" mechanism.
- Legal Relevance: Corroborates the systemic nature of the alleged crime, proving it is not an isolated technical glitch but a deliberate corporate design.

EXHIBIT NO. 4: TECHNICAL NOTE ON PROFIT MOTIVE AND AI (GEMINI)

- Content: Analysis of the integration between Android metadata collection and the training of Google's Artificial Intelligence (Gemini).
- Legal Relevance: Directly addresses Article 197.4 of the Spanish Penal Code (Crimes committed for profit). It links the unauthorized data extraction to Google's multi-billion dollar AI and advertising revenue streams.

TECHNICAL SUMMARY FOR THE REQUESTED AUTHORITY

The combination of these exhibits demonstrates a "Prima Facie" case for criminal investigation. The evidence suggests that:

1. Intentionality: The data collection is hardcoded into the system kernel (Google Play Services).
2. Secrecy: The collection occurs in the background, eluding standard user-facing privacy toggles.
3. Harm: The persistent nature of identifiers (IMEI/Serial) creates a permanent, non-consensual digital profile of the victims.

Sugerencia de Siguiente Paso:

Con este documento en inglés y la Comisión Rogatoria, el Juzgado de Instrucción tiene todo lo necesario para proceder. Para cerrar el círculo de presión legal, ¿le gustaría que redactara una "Petición de Auxilio a la Europol (Cybercrime Centre - EC3)"? Dado que el delito afecta a varios países de la UE y la prueba

está en Irlanda, la intervención de Europol podría acelerar enormemente la obtención de la prueba técnica y la coordinación entre jueces.

Esta es la propuesta formal de Solicitud de Cooperación y Auxilio Técnico dirigida al Centro Europeo de Ciberdelincuencia (EC3) de Europol.

Dada la dimensión transfronteriza del presunto delito (la matriz está en EE. UU., la sede europea en Irlanda y los millones de víctimas en España), la intervención de Europol es clave para coordinar la obtención de pruebas digitales y analizar la complejidad del "dolo tecnológico" denunciado en https://www.miguelgallardo.es/denuncia-google-android.pdf.

SOLICITUD DE COOPERACIÓN TÉCNICA Y COORDINACIÓN TRANSFRONTERIZA A EUROPOL (EC3)

AL JUZGADO DE INSTRUCCIÓN Nº [Número] DE [Ciudad]

DILIGENCIAS PREVIAS: [Número] / DELITOS INFORMÁTICOS TRANSNACIONALES

A LA ATENCIÓN DEL CENTRO EUROPEO DE CIBERDELINCUENCIA (EC3) – EUROPOL (LA HAYA):

El Juzgado de Instrucción Nº [Número] de [Ciudad], España, en el marco de una investigación penal por delitos de Descubrimiento y Revelación de Secretos (Art. 197 CP) y Acceso Ilícito a Sistemas de Información (Art. 197 bis CP) cometidos de forma masiva y sistemática a través del ecosistema Android y servicios de Google, solicita formalmente el auxilio técnico y operativo de Europol (EC3) basándose en los siguientes puntos:

I. NATURALEZA TRANSFRONTERIZA DEL ILÍCITO (UBICUIDAD)

Los hechos investigados presentan una complejidad que excede la capacidad de las unidades nacionales debido a:

1. Víctimas: Aproximadamente 37 millones de usuarios en territorio español y cientos de millones en la Unión Europea.
2. Sujeto Investigado: Una corporación multinacional con sede principal de datos en Irlanda (Google Ireland Ltd.) y desarrollo de software en EE. UU. (Alphabet Inc.).
3. Infraestructura: El presunto espionaje se ejecuta mediante el control del sistema operativo Android, cuya telemetría es enviada a servidores ubicados en múltiples jurisdicciones de la UE.

II. SOLICITUD DE APOYO OPERATIVO AL EC3

Se interesa la intervención de los expertos de Europol para las siguientes tareas:

- A) Análisis Forense de Alto Nivel: Realización de un informe técnico independiente que valide los hallazgos del Prof. Doug Leith (Trinity College Dublin, 2025) sobre la captura silenciosa de

identificadores persistentes (IMEI, Android ID) y la inyección de cookies de seguimiento (DSID, NID) sin consentimiento del usuario.
- B) Coordinación con las Autoridades Irlandesas: Facilitar, a través de los canales de Europol, la ejecución de la Comisión Rogatoria Internacional remitida a Irlanda, asegurando que la evidencia digital (logs y código fuente) no sea alterada o destruida.
- C) Trazabilidad de Datos hacia la IA (Gemini): Analizar si el flujo de metadatos extraídos de los ciudadanos europeos está siendo utilizado de forma ilícita para el entrenamiento de modelos de Inteligencia Artificial, lo que constituiría un beneficio económico derivado de una actividad delictiva a escala continental.

III. JUSTIFICACIÓN SEGÚN EL MANDATO DE EUROPOL

Esta solicitud se ampara en la misión del EC3 de combatir los ciberdelitos que causan un perjuicio grave a los ciudadanos de la Unión y que requieren un análisis técnico especializado de gran escala. El "espionaje masivo" denunciado por APEDANICA representa una amenaza a la soberanía digital europea y a la intimidad de millones de personas, lo que justifica una respuesta coordinada a nivel de la Unión.

IV. PETICIÓN DE "OPERATIONAL SUPPORT"

Se solicita que Europol designe un equipo de enlace para colaborar estrechamente con la Unidad de Delitos Informáticos de la Guardia Civil / Policía Nacional de España en la práctica de los peritajes judiciales acordados en esta causa.

Por qué esta petición a Europol es determinante:

1. Evita el "bloqueo" de Google en Irlanda: Google tiene una gran influencia en Irlanda. La presencia de Europol (una agencia de la UE) en la investigación garantiza que las autoridades irlandesas actúen con la diligencia debida.
2. Experiencia Técnica Superior: El EC3 dispone de laboratorios de análisis de tráfico de red y de ingeniería inversa de aplicaciones móviles que pueden certificar el "dolo tecnológico" de forma que no pueda ser rebatido por los abogados de Google.
3. Efecto Multiplicador: Si Europol interviene, el caso deja de ser un "problema español" para convertirse en un caso europeo, lo que aumenta exponencialmente la relevancia penal y la presión sobre Google.

Con este último documento, el "Pack Judicial de Refuerzo" está completo. Contiene:

1. Informe Técnico-Jurídico AD HOC.
2. Estructura de Interrogatorio Pericial.
3. Solicitud de Medidas Cautelares.
4. Requerimiento técnico a la AEPD.
5. Citación de Investigados.

6. Comisión Rogatoria Internacional (Bilingüe).
7. Petición de auxilio a Europol.

¿Desea que realice un último documento de "Instrucciones de Uso para el Abogado/Denunciante" para explicar cómo presentar estratégicamente estos escritos ante el Juzgado de Instrucción?

Para que esta ofensiva legal sea efectiva y no se pierda en la burocracia judicial, el abogado o denunciante debe actuar con precisión quirúrgica. No se trata de presentar todos los folios a la vez, sino de crear una narrativa de urgencia y dolo tecnológico que obligue al Juez a actuar.

Aquí tienes la guía estratégica para implementar el pack de documentos reforzando la denuncia de https://www.miguelgallardo.es/denuncia-google-android.pdf.

GUÍA ESTRATÉGICA DE ACTUACIÓN PROCESAL (INSTRUCCIONES DE USO)

Fase 1: La Presentación y la "Activación" del Juez

No envíes los documentos como simples anexos. Deben presentarse mediante Escritos de Impulso Procesal separados para generar hitos en el sumario.

1. Presentación del Informe Técnico-Jurídico AD HOC: Úsalo como "Escrito de Ratificación y Ampliación". Su función es elevar el tono de la denuncia original de una "queja por privacidad" a un "delito de espionaje masivo con dolo de diseño".
2. La "Prueba de Visibilidad": Solicita que el Juez vea el diagrama de flujo de datos. Un Juez de Instrucción suele ser ajeno a la tecnología; visualizar cómo el IMEI vuela a servidores de Google antes de tocar el teléfono es el "momento de la verdad".

Fase 2: El Ataque Cautelar (El "Golpe" de Efecto)

La clave aquí es el Art. 13 de la LECrim (obligación de los jueces de detener los efectos del delito).

- Estrategia: Presenta la Solicitud de Medidas Cautelares 48 horas después de la denuncia.
- Argumento de cierre: "Si el Juzgado no detiene hoy la descarga de cookies DSID/NID, la sentencia condenatoria de dentro de 5 años será papel mojado, pues los datos ya habrán sido 'digeridos' por la IA Gemini".
- La Diligencia de la "Caja Precintada": Insiste en la prueba del terminal Android nuevo. Es una prueba barata, rápida y demoledora que acredita la flagrancia.

Fase 3: El Cerco Institucional (AEPD y Europol)

Google intentará alegar que esto es un tema administrativo de la AEPD para sacar al Juez penal de la ecuación. Anticipate:

- Uso del Oficio a la AEPD: Presentalo como un requerimiento de Auxilio Judicial. No pides que la AEPD sancione, pides que la AEPD informe al Juez sobre la "imposibilidad técnica de oposición". Si la AEPD dice que no hay botón de "no rastrear", el delito del Art. 197 bis está probado.
- El Factor Europol: Úsalo si el Juez duda de su competencia. Al presentar la solicitud de Europol, le estás diciendo al Juez: "Usted no está solo, tiene a los mejores expertos en ciberdelincuencia de Europa a su disposición".

Fase 4: El Interrogatorio y la Trampa del Código Fuente

Cuando el Juez cite a los responsables de Google (Investigados):

- El Interrogatorio: Úsalo como guion. No permitas que el técnico de Google hable de "experiencia de usuario". Fuerza al Juez a preguntar por nombres específicos de dominios (`android.clients.google.com`) y cookies (`NID`). La especificidad técnica anula la oratoria corporativa.
- La Comisión Rogatoria (Inglés): Tenla lista para cuando el investigado diga: *"Esa información está en servidores de Irlanda y yo no tengo acceso"*. En ese momento, entrega el documento bilingüe al Juez: *"Señoría, aquí tiene el exhorto redactado para pedirlo a Dublín hoy mismo"*.

Cronograma Recomendado de Escritos

Tiempo	Acción	Objetivo
Día 1	Denuncia + Informe AD HOC	Apertura de Diligencias Previas.
Día 3	Medidas Cautelares + Prueba "Caja Precintada"	Detener el flujo de datos y asegurar la prueba.
Día 10	Solicitud Oficio AEPD y Europol	Blindar la instrucción con peritos del Estado.

Día 20	Citación Investigados + Comisión Rogatoria	Identificar responsables y exigir el código fuente.

Recomendación Final: El "Dolo Tecnológico"

Repite este término en cada escrito. El abogado debe convencer al Juez de que el espionaje no es un "efecto secundario" de Android, sino su propósito principal oculto. La referencia al artículo del Prof. Doug Leith (2025) es tu mayor activo: es una fuente académica de prestigio (Trinity College) que el Juez no puede ignorar.

¿Hay alguna sección específica o algún escenario de contraataque por parte de los abogados de Google que te gustaría que analizara para preparar la respuesta? Sería un placer ayudarte a anticipar sus movimientos.

FIN DE LA CITA TEXTUAL de la Inteligencia Artificial Gemini 3 en el enlace https://gemini.google.com/app/fe84f567c8774901 en parte compartido en https://gemini.google.com/share/a7a33d8c4407

Recomendamos los Grupos de WhatsAPP de APEDANICA
Google en los Juzgados ❓ 😱
https://chat.whatsapp.com/IrD2Gh637Xs3IV3Vzp7RQJ
Ética en Protección de Datos denunciando corrupción encubridora. Intimidad y derecho a informar ⚖️ ⚠️
https://chat.whatsapp.com/JTBhDuGjSoA0KEg8zyxbyW
Querellas y denuncias penales con PRONÓSTICOS Y APUESTAS JUDICIALES SOBRE ACUSACIONES CRIMINALES ⚖️ 🎰 🏆
https://chat.whatsapp.com/E4VYpuFCxbBEhwvOkmwZtt
Derecho e Inteligencias Artificiales éticas vigilando procedimientos administrativos y judiciales ⚖️ 💻
https://chat.whatsapp.com/DWse5XL8e4a63ZcWpN5O5K

Esta denuncia penal está publicada en

https://cita.es/denuncia-google-android-firmado.pdf

Al Juzgado de Instrucción que corresponda

DENUNCIA publicada en https://www.miguelgallardo.es/denuncia-google-android.pdf

Más información:

@miguelgallardo Dr. (PhD) Ing. Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
@APEDANICA Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf