Comentario Seguridad y autenticidad en las comunicaciones digitales: la respuesta regulatoria frente al fraude de identidad en la Circular 1/2026

Resumen

El presente comentario analiza el fenómeno del fraude de identidad en las comunicaciones digitales a la luz de la **Circular 1/2026, de 18 de marzo, de la Comisión Nacional de los Mercados y la Competencia**, centrando la atención en los mecanismos jurídicos y técnicos introducidos para combatir la suplantación de identidad en llamadas y mensajes electrónicos. Se estudia el funcionamiento del Registro de Alias como instrumento clave para garantizar la autenticidad de los remitentes, así como los sistemas de verificación, control y bloqueo de comunicaciones fraudulentas.

A lo largo del análisis se examina el impacto práctico de estas medidas en la seguridad de los usuarios, en la operativa de los operadores y en la configuración del mercado de las comunicaciones electrónicas, destacando su contribución a reducir la eficacia de técnicas como el *spoofing* y el *smishing*. Asimismo, se incorporan referencias legislativas y jurisprudenciales recientes que avalan la legitimidad de este tipo de intervenciones regulatorias.

Desde una perspectiva crítica constructiva, se identifican los principales retos del modelo, entre ellos la necesidad de una implementación homogénea, la coordinación internacional y el equilibrio entre seguridad y proporcionalidad. En conjunto, la Circular 1/2026 se configura como un avance relevante hacia un entorno digital más seguro, cuya eficacia dependerá de su aplicación práctica y de su capacidad de adaptación a la evolución del fraude tecnológico.

1. Contexto actual del fraude de identidad en comunicaciones digitales

El fraude de identidad en comunicaciones digitales se ha consolidado en los últimos años como una de las principales amenazas en el ámbito de las telecomunicaciones, afectando tanto a usuarios particulares como a empresas e instituciones públicas. La creciente digitalización de los servicios y la generalización del uso de canales como llamadas telefónicas, mensajes SMS y sistemas de mensajería con identificadores alfanuméricos han generado un entorno propicio para la proliferación de prácticas de suplantación de identidad.

Este fenómeno se manifiesta especialmente a través de técnicas como el *spoofing*, mediante las cuales el emisor de una comunicación falsifica el identificador de origen para aparentar que el mensaje o la llamada procede de una entidad legítima, como una entidad bancaria, una Administración pública o una empresa reconocida. Esta capacidad de manipulación del identificador constituye el núcleo del problema, ya que erosiona la confianza del usuario en los sistemas de comunicación.

El impacto de estas prácticas es significativo. Desde el punto de vista económico, el fraude de identidad genera pérdidas directas para los usuarios, derivadas de la obtención ilícita de datos personales o financieros. Desde una perspectiva institucional, afecta a la credibilidad de las entidades suplantadas, que ven comprometida su reputación y la confianza de sus clientes o ciudadanos.

El incremento de estos fraudes ha sido reconocido en el ámbito normativo y regulatorio. La **Ley 11/2022, General de Telecomunicaciones**, establece entre sus objetivos la protección de los usuarios frente a prácticas fraudulentas y la garantía de la seguridad en las comunicaciones electrónicas. Este marco normativo habilita la adopción de medidas específicas para prevenir y combatir la suplantación de identidad.

Asimismo, la evolución tecnológica ha facilitado la ejecución de estos fraudes a gran escala. La automatización de envíos masivos de mensajes y la utilización de infraestructuras internacionales dificultan la identificación de los responsables y la aplicación de medidas de control tradicionales. Este carácter transnacional del fenómeno añade un elemento de complejidad a su regulación.

La jurisprudencia ha comenzado a abordar las implicaciones jurídicas de este tipo de conductas. El **Tribunal Supremo**, en la **STS de 20 de mayo de 2021 (rec. 3387/2019)**, analizó supuestos de fraude vinculados a comunicaciones electrónicas, destacando la necesidad de reforzar los mecanismos de protección de los usuarios frente a prácticas engañosas que aprovechan la apariencia de legitimidad de los canales digitales.

En el ámbito europeo, el fenómeno del fraude de identidad se vincula con la protección de datos personales y la seguridad de las redes y sistemas de información. El **Reglamento (UE) 2016/679 (RGPD)** establece obligaciones estrictas en materia de tratamiento de datos y seguridad, mientras que la normativa sobre servicios digitales refuerza la responsabilidad de los prestadores en la prevención de abusos.

En este contexto, la intervención regulatoria se presenta como una necesidad ineludible. La complejidad técnica del fraude y su impacto creciente exigen la adopción de medidas específicas que permitan reforzar la autenticidad de las comunicaciones y limitar la capacidad de los operadores fraudulentos para manipular los identificadores.

Desde una perspectiva crítica constructiva, puede afirmarse que el contexto actual evidencia una clara asimetría entre la capacidad tecnológica de los defraudadores y los mecanismos de control disponibles. La respuesta normativa debe orientarse a reducir esta brecha, introduciendo sistemas de verificación más robustos y reforzando la coordinación entre operadores y autoridades.

En conclusión, el fraude de identidad en comunicaciones digitales constituye un problema estructural del ecosistema de las telecomunicaciones modernas, caracterizado por su creciente sofisticación y su impacto transversal. Este contexto justifica plenamente la adopción de instrumentos regulatorios específicos, como los previstos en la **Circular 1/2026**, orientados a reforzar la seguridad y la confianza en las comunicaciones electrónicas.

2. Naturaleza jurídica de la Circular 1/2026 y su encaje en el marco regulatorio de telecomunicaciones

La **Circular 1/2026, de 18 de marzo, de la Comisión Nacional de los Mercados y la Competencia (CNMC)** se configura como una disposición de carácter normativo dictada en el ejercicio de las potestades regulatorias atribuidas a dicho organismo en el ámbito de las

comunicaciones electrónicas. Su finalidad es establecer un marco técnico y jurídico para la gestión del Registro de Alias, como instrumento destinado a prevenir el fraude de identidad en comunicaciones digitales.

Desde el punto de vista jurídico, las circulares de la CNMC tienen naturaleza reglamentaria en el ámbito de sus competencias específicas, tal y como se desprende de la **Ley 3/2013, de creación de la CNMC**, que reconoce su capacidad para dictar disposiciones de carácter general en materias reguladas. Esta potestad normativa se ejerce dentro de los límites establecidos por la legislación sectorial, especialmente por la **Ley 11/2022, General de Telecomunicaciones**, que constituye el marco básico del sector.

La Circular 1/2026 se inserta, por tanto, en el desarrollo de las obligaciones de los operadores en materia de seguridad, integridad y autenticidad de las comunicaciones electrónicas. En particular, la Ley General de Telecomunicaciones establece la necesidad de garantizar la protección de los usuarios frente a prácticas fraudulentas, habilitando a las autoridades regulatorias para imponer medidas técnicas y organizativas que refuercen dicha protección.

El encaje de la Circular en el sistema normativo debe analizarse también desde la perspectiva del Derecho de la Unión Europea. La regulación de las comunicaciones electrónicas se encuentra fuertemente armonizada a nivel europeo, especialmente a través del **Código Europeo de las Comunicaciones Electrónicas (Directiva (UE) 2018/1972)**, que impone a los Estados miembros la obligación de garantizar la seguridad de las redes y la protección de los usuarios frente a abusos. La Circular 1/2026 puede interpretarse como una medida de desarrollo de estos principios en el ámbito nacional.

La jurisprudencia ha reconocido la legitimidad de este tipo de intervenciones regulatorias. El **Tribunal Supremo**, en la **STS de 15 de marzo de 2021 (rec. 3936/2018)**, confirmó la validez de las actuaciones normativas de los organismos reguladores independientes, siempre que se ajusten a sus competencias y respeten los principios de legalidad, proporcionalidad y seguridad jurídica. Esta doctrina resulta plenamente aplicable a la Circular 1/2026.

Asimismo, el **Tribunal Constitucional**, en la **STC 79/2017, de 22 de junio**, ha señalado que la atribución de potestades normativas a autoridades independientes es compatible con el marco constitucional, siempre que dichas potestades se ejerzan dentro de los límites legales y con sujeción a los principios de control y responsabilidad. Esta doctrina refuerza la validez del papel de la CNMC en la regulación del sector.

Desde una perspectiva funcional, la Circular 1/2026 no se limita a establecer principios generales, sino que introduce obligaciones concretas para los operadores en relación con la gestión del Registro de Alias. Estas obligaciones tienen un carácter técnico y operativo, lo que justifica su regulación mediante una disposición específica del regulador sectorial, capaz de adaptarse a la evolución tecnológica.

No obstante, desde una valoración crítica constructiva, puede señalarse que este tipo de instrumentos normativos plantea retos en términos de coordinación con otras normas del ordenamiento, especialmente en materia de protección de datos y servicios digitales. La coexistencia de múltiples marcos regulatorios exige una interpretación sistemática que evite conflictos y garantice la coherencia del sistema.

En particular, la interacción con el **Reglamento (UE) 2016/679 (RGPD)** resulta especialmente relevante, ya que la gestión del Registro de Alias implica el tratamiento de datos personales y la adopción de medidas de seguridad. La Circular debe aplicarse, por tanto, en consonancia con las obligaciones derivadas de la normativa de protección de datos.

En conclusión, la **Circular 1/2026** se configura como un instrumento normativo legítimo y necesario dentro del marco regulatorio de las telecomunicaciones, orientado a reforzar la seguridad de las comunicaciones digitales. Su encaje jurídico es coherente con la legislación nacional y europea, si bien su eficacia dependerá de su correcta integración con otros marcos normativos y de su aplicación proporcionada por los operadores del sector.

3. El fenómeno del spoofing y otras técnicas de suplantación de identidad

El fraude de identidad en comunicaciones digitales encuentra su manifestación más característica en el denominado *spoofing*, técnica mediante la cual el emisor de una comunicación altera o falsifica el identificador de origen —número telefónico o alias alfanumérico— con el objetivo de aparentar que la comunicación procede de una fuente legítima. Este fenómeno constituye el núcleo operativo de gran parte de los fraudes actuales, al aprovechar la confianza del usuario en la identidad del remitente.

Desde un punto de vista técnico, el *spoofing* se apoya en las propias características de las redes de telecomunicaciones, especialmente en protocolos que, en su diseño original, no incorporaban mecanismos robustos de autenticación del origen. Esto ha permitido que operadores fraudulentos manipulen el identificador de llamada o de mensaje sin necesidad de controlar realmente la línea o el sistema suplantado.

El *spoofing* puede adoptar diversas formas. En el ámbito de las comunicaciones de voz, se materializa mediante la falsificación del número de teléfono que aparece en el terminal del receptor, lo que permite simular llamadas procedentes de entidades reconocidas. En el caso de los mensajes SMS, la suplantación puede extenderse al uso de alias alfanuméricos, que permiten identificar al remitente con el nombre de una empresa o institución, incrementando así el grado de credibilidad del mensaje.

Este fenómeno se ve reforzado por técnicas complementarias, como el *smishing* (fraude a través de SMS) o el *vishing* (fraude mediante llamadas de voz), que combinan la suplantación de identidad con estrategias de ingeniería social destinadas a obtener información sensible del usuario. Estas prácticas explotan no solo vulnerabilidades técnicas, sino también factores psicológicos, como la confianza en marcas reconocidas o la urgencia generada por determinados mensajes.

Desde el punto de vista jurídico, estas conductas pueden encuadrarse en distintos tipos delictivos, como la estafa o el acceso ilícito a datos personales, conforme al **Código Penal español**, particularmente en sus artículos relativos a los delitos contra el patrimonio y contra la intimidad. No obstante, la respuesta penal, aunque necesaria, resulta insuficiente para abordar un fenómeno de carácter masivo y preventivo, lo que justifica la intervención regulatoria.

La **Ley 11/2022, General de Telecomunicaciones**, establece la obligación de los operadores de garantizar la integridad y seguridad de las comunicaciones, lo que incluye la adopción de medidas para prevenir la manipulación de los identificadores. En este sentido, el fenómeno del *spoofing* pone de manifiesto la necesidad de reforzar los mecanismos técnicos de autenticación en las redes.

La jurisprudencia ha comenzado a abordar las implicaciones de estas prácticas. El **Tribunal Supremo**, en la **STS de 20 de mayo de 2021 (rec. 3387/2019)**, analizó supuestos de fraude mediante comunicaciones electrónicas, destacando la relevancia de la apariencia de legitimidad generada por el uso de identificadores falsificados como elemento determinante para inducir a error al usuario.

Asimismo, en el ámbito europeo, el fenómeno del *spoofing* se vincula con la seguridad de las redes y la protección de los usuarios, en línea con el **Código Europeo de las Comunicaciones Electrónicas (Directiva (UE) 2018/1972)**, que impone a los operadores la adopción de medidas para garantizar la autenticidad de las comunicaciones.

Desde una perspectiva funcional, el problema del *spoofing* no radica únicamente en la existencia de la técnica, sino en su facilidad de ejecución y en la dificultad de detección por parte del usuario final. La suplantación de un identificador legítimo elimina uno de los principales elementos de verificación de la autenticidad de la comunicación, lo que incrementa significativamente el riesgo de fraude.

Desde una valoración crítica constructiva, puede afirmarse que el fenómeno del *spoofing* pone de relieve una debilidad estructural en los sistemas de comunicación tradicionales, basada en la falta de mecanismos robustos de autenticación del origen. La respuesta regulatoria, como la introducida por la **Circular 1/2026**, debe orientarse a corregir esta deficiencia mediante sistemas de verificación y registro que permitan identificar de forma fiable a los emisores.

En conclusión, el *spoofing* y las técnicas asociadas de suplantación de identidad constituyen el principal vector del fraude en comunicaciones digitales. Su complejidad técnica y su impacto creciente justifican la adopción de medidas regulatorias específicas, orientadas a reforzar la autenticidad de las comunicaciones y a proteger a los usuarios frente a prácticas engañosas cada vez más sofisticadas.

4. El Registro de Alias como instrumento de prevención del fraude

La **Circular 1/2026, de 18 de marzo**, introduce el Registro de Alias como uno de los instrumentos clave para combatir el fraude de identidad en comunicaciones digitales, especialmente en el ámbito de los mensajes SMS y servicios de mensajería donde el identificador del remitente puede adoptar forma alfanumérica. Este registro responde a la necesidad de reforzar la autenticidad del origen de las comunicaciones, limitando la capacidad de los operadores fraudulentos para suplantar identidades legítimas.

Desde una perspectiva funcional, el Registro de Alias se configura como un sistema centralizado en el que se inscriben los identificadores alfanuméricos utilizados por entidades legítimas en sus comunicaciones con usuarios. A través de este mecanismo, se establece una

correspondencia verificable entre el alias y el titular autorizado para su uso, lo que permite a los operadores validar la autenticidad del remitente antes de permitir la transmisión del mensaje.

El objetivo principal de este instrumento es evitar que terceros no autorizados puedan utilizar alias que identifiquen a entidades reconocidas, como bancos, administraciones públicas o empresas de servicios. De este modo, se introduce un sistema de control previo que actúa directamente sobre uno de los principales vectores del fraude: la falsificación del identificador del remitente.

Desde el punto de vista jurídico, el Registro de Alias se inserta en el marco de las obligaciones de los operadores en materia de seguridad de las comunicaciones, previstas en la **Ley 11/2022, General de Telecomunicaciones**, que exige garantizar la integridad y autenticidad de las comunicaciones electrónicas. La Circular desarrolla estas obligaciones mediante la introducción de un mecanismo técnico específico.

El funcionamiento del registro implica que los operadores deben consultar la base de datos antes de cursar determinados mensajes, verificando que el alias utilizado corresponde a un titular legítimo. En caso contrario, la comunicación puede ser bloqueada o sometida a controles adicionales. Este sistema introduce una capa de seguridad adicional en el proceso de transmisión de mensajes.

La jurisprudencia ha avalado la adopción de medidas preventivas de este tipo en sectores regulados. El **Tribunal Supremo**, en la **STS de 15 de marzo de 2021 (rec. 3936/2018)**, reconoció que los organismos reguladores pueden imponer obligaciones técnicas a los operadores para proteger a los usuarios frente a riesgos sistémicos, siempre que dichas medidas sean proporcionadas y estén justificadas por el interés general.

Asimismo, el Registro de Alias debe operar en coordinación con la normativa de protección de datos, especialmente con el **Reglamento (UE) 2016/679 (RGPD)**, ya que implica el tratamiento de información asociada a identificadores que pueden estar vinculados a personas físicas o jurídicas. Esto exige garantizar la seguridad de los datos y limitar su uso a los fines previstos.

Desde una perspectiva técnica, el registro contribuye a mejorar la trazabilidad de las comunicaciones, permitiendo identificar de forma más precisa el origen de los mensajes y facilitando la detección de patrones de fraude. Además, refuerza la capacidad de los operadores para aplicar medidas de bloqueo de comunicaciones sospechosas.

No obstante, desde una valoración crítica constructiva, puede señalarse que la eficacia del Registro de Alias depende de su correcta implementación y de la cobertura efectiva de los alias utilizados en el mercado. La existencia de alias no registrados o la utilización de infraestructuras internacionales puede limitar el alcance del sistema.

Asimismo, el registro introduce nuevas obligaciones para los operadores, lo que puede generar costes adicionales y requerir adaptaciones técnicas. Es necesario, por tanto, que la regulación garantice un equilibrio adecuado entre la protección de los usuarios y la viabilidad operativa de los operadores.

En conclusión, el Registro de Alias se configura como un instrumento innovador y necesario para prevenir el fraude de identidad en comunicaciones digitales, al reforzar la autenticidad del remitente y limitar las posibilidades de suplantación. Su integración en el sistema regulatorio representa un avance significativo, aunque su eficacia dependerá de su correcta aplicación y de su adaptación a la evolución de las técnicas de fraude.

5. Sujetos obligados y responsabilidades en la prevención del fraude

La eficacia del sistema diseñado por la **Circular 1/2026, de 18 de marzo**, y en particular del Registro de Alias, depende en gran medida de la correcta actuación de los distintos sujetos obligados que intervienen en el ecosistema de las comunicaciones electrónicas. La norma configura un modelo de responsabilidades compartidas, en el que operadores, prestadores de servicios y, en menor medida, usuarios, participan en la prevención del fraude de identidad digital.

En primer lugar, los **operadores de telecomunicaciones** constituyen los principales sujetos obligados. Sobre ellos recae la responsabilidad de implementar las medidas técnicas necesarias para garantizar la autenticidad de las comunicaciones, incluyendo la verificación de los alias registrados y el bloqueo de aquellos que no cumplan con los requisitos establecidos. Esta obligación se fundamenta en la **Ley 11/2022, General de Telecomunicaciones**, que impone a los operadores el deber de garantizar la seguridad e integridad de las redes y servicios.

El papel de los operadores no se limita a una función pasiva de transmisión de comunicaciones, sino que implica una actuación activa en la prevención del fraude. Deben adaptar sus sistemas para integrar el Registro de Alias, establecer mecanismos de validación en tiempo real y aplicar medidas de control ante posibles irregularidades. Esta transformación refuerza su papel como garantes de la seguridad del sistema.

La jurisprudencia ha avalado esta ampliación de responsabilidades. El **Tribunal Supremo**, en la **STS de 15 de marzo de 2021 (rec. 3936/2018)**, señaló que los operadores en sectores regulados pueden ser objeto de obligaciones específicas cuando su actividad incide directamente en la protección de los usuarios, siempre que dichas obligaciones sean proporcionadas y estén justificadas por el interés general.

En segundo lugar, intervienen los **prestadores de servicios de mensajería y entidades emisoras de comunicaciones**, como bancos, empresas o Administraciones públicas. Estos sujetos son responsables de registrar correctamente sus alias en el sistema y de utilizarlos conforme a las condiciones establecidas. Su actuación resulta clave para garantizar la fiabilidad del registro y evitar usos indebidos.

El incumplimiento de estas obligaciones puede generar riesgos no solo para los usuarios, sino también para la reputación de las entidades emisoras. La correcta gestión de los alias se convierte, por tanto, en un elemento esencial de su política de seguridad y de protección de sus clientes.

En tercer lugar, deben considerarse los **agentes intermediarios**, que pueden intervenir en la gestión de campañas de comunicación o en la prestación de servicios técnicos asociados. Estos agentes también pueden asumir obligaciones específicas en función de su grado de participación en el proceso de emisión de comunicaciones.

Desde el punto de vista jurídico, el sistema de responsabilidades se complementa con el régimen sancionador previsto en la normativa de telecomunicaciones. La **Ley 11/2022** establece un conjunto de infracciones y sanciones aplicables a los operadores que incumplan sus obligaciones, lo que refuerza el carácter vinculante de las medidas introducidas por la Circular.

El **Tribunal Constitucional**, en la **STC 79/2017, de 22 de junio**, ha reconocido la legitimidad de imponer obligaciones específicas a operadores económicos en sectores regulados, siempre que estas se orienten a la protección de intereses generales y respeten los principios de proporcionalidad y seguridad jurídica. Esta doctrina resulta aplicable al régimen de responsabilidades establecido por la Circular 1/2026.

Desde una perspectiva crítica constructiva, puede señalarse que el sistema de responsabilidades presenta un equilibrio adecuado entre los distintos actores, aunque plantea desafíos en términos de implementación. La carga técnica y organizativa recae principalmente sobre los operadores, lo que puede generar dificultades en su adaptación, especialmente en entornos tecnológicos complejos.

Asimismo, la coordinación entre los distintos sujetos resulta esencial para el correcto funcionamiento del sistema. La falta de alineación entre operadores, prestadores de servicios y Administración puede generar lagunas que sean aprovechadas por los operadores fraudulentos.

En conclusión, la **Circular 1/2026** configura un sistema de responsabilidades compartidas en la prevención del fraude de identidad en comunicaciones digitales, en el que los operadores desempeñan un papel central, complementado por la actuación de los prestadores de servicios y otros agentes. La eficacia del sistema dependerá de la correcta asunción de estas responsabilidades y de la coordinación entre los distintos actores implicados.

6. Mecanismos de control, verificación y bloqueo de comunicaciones fraudulentas

La **Circular 1/2026, de 18 de marzo**, articula un conjunto de mecanismos técnicos y jurídicos orientados a reforzar el control de las comunicaciones electrónicas y a prevenir la suplantación de identidad mediante la verificación del origen y el eventual bloqueo de aquellas comunicaciones que no cumplan los requisitos establecidos. Estos mecanismos constituyen el núcleo operativo de la respuesta regulatoria frente al fraude digital.

En primer lugar, el sistema se apoya en un **mecanismo de verificación previa del identificador**, especialmente en lo relativo a los alias alfanuméricos. Los operadores deben contrastar, en tiempo real o mediante procesos automatizados, que el identificador utilizado en una comunicación se encuentra inscrito en el Registro de Alias y que su uso corresponde

efectivamente al titular autorizado. Esta verificación introduce un filtro técnico que impide, en origen, la utilización de identificadores falsificados.

Este tipo de control se enmarca en las obligaciones generales de seguridad establecidas en la **Ley 11/2022, General de Telecomunicaciones**, que exige a los operadores adoptar medidas adecuadas para garantizar la integridad de las comunicaciones y proteger a los usuarios frente a riesgos de fraude.

En segundo lugar, la Circular prevé **mecanismos de bloqueo de comunicaciones** cuando no se pueda verificar la legitimidad del identificador o cuando existan indicios de fraude. Este bloqueo puede operar de forma automática, en función de parámetros previamente definidos, o mediante actuaciones específicas de los operadores o de la autoridad reguladora.

La adopción de medidas de bloqueo plantea cuestiones relevantes desde el punto de vista jurídico, en particular en relación con el principio de proporcionalidad. La jurisprudencia ha señalado que este tipo de medidas restrictivas deben estar justificadas y ser necesarias para la protección de un interés general. En este sentido, el **Tribunal Supremo**, en la **STS de 15 de marzo de 2021 (rec. 3936/2018)**, ha reconocido la legitimidad de imponer restricciones técnicas en sectores regulados cuando se dirigen a prevenir riesgos relevantes para los usuarios.

En tercer lugar, el sistema incorpora **mecanismos de monitorización y detección de patrones de fraude**, que permiten identificar comportamientos anómalos en el tráfico de comunicaciones. La utilización de herramientas de análisis de datos facilita la detección temprana de campañas fraudulentas y permite adoptar medidas preventivas antes de que se produzcan daños significativos.

Estos sistemas de control continuo se complementan con la posibilidad de realizar **actuaciones de supervisión e inspección** por parte de la Administración, lo que refuerza el carácter dinámico del sistema de control. La intervención administrativa permite adaptar las medidas a la evolución de las técnicas de fraude.

El **Tribunal Constitucional**, en la **STC 55/2018, de 24 de mayo**, ha señalado que la utilización de medios tecnológicos en la actuación administrativa puede reforzar la eficacia del control público, siempre que se respeten las garantías jurídicas de los ciudadanos. Esta doctrina resulta plenamente aplicable a los sistemas de verificación y bloqueo previstos en la Circular.

Desde una perspectiva técnica, estos mecanismos permiten actuar sobre el principal vector del fraude, que es la falsificación del identificador de origen. Al dificultar la suplantación de identidad, se reduce significativamente la eficacia de las técnicas de *spoofing* y de ingeniería social asociadas.

No obstante, desde una valoración crítica constructiva, pueden identificarse ciertos retos. En primer lugar, la eficacia de los mecanismos de verificación depende de la calidad y actualización del Registro de Alias. Un registro incompleto o desactualizado puede generar tanto falsos positivos como falsos negativos.

En segundo lugar, el bloqueo de comunicaciones debe aplicarse con cautela para evitar interferencias indebidas en las comunicaciones legítimas. La existencia de errores en la

verificación puede afectar a la continuidad de servicios esenciales o a la comunicación de entidades legítimas.

Asimismo, la naturaleza global de las comunicaciones electrónicas puede limitar la eficacia de estos mecanismos cuando las comunicaciones fraudulentas se originan fuera del ámbito jurisdiccional nacional. Esto exige una coordinación internacional y la adopción de estándares comunes.

En conclusión, los mecanismos de control, verificación y bloqueo previstos en la **Circular 1/2026** constituyen una respuesta técnica y jurídica adecuada frente al fraude de identidad en comunicaciones digitales. Su eficacia dependerá de su correcta implementación, de la calidad de los sistemas de verificación y de la capacidad de adaptación del sistema a la evolución constante de las técnicas de fraude.

7. Impacto práctico en la seguridad de las comunicaciones digitales

La implementación de las medidas previstas en la **Circular 1/2026, de 18 de marzo**, y en particular del Registro de Alias y de los mecanismos de verificación y bloqueo, tiene un impacto directo en la seguridad de las comunicaciones digitales, tanto desde la perspectiva de los usuarios como desde la de los operadores y las entidades emisoras de mensajes.

En primer lugar, desde el punto de vista del usuario final, la principal consecuencia es el **refuerzo de la confianza en la autenticidad de las comunicaciones**. La posibilidad de verificar que un alias corresponde efectivamente a una entidad legítima reduce significativamente el riesgo de ser víctima de fraudes basados en suplantación de identidad. Esto resulta especialmente relevante en sectores sensibles, como el financiero o el administrativo, donde la apariencia de legitimidad del remitente es determinante.

Este refuerzo de la confianza se alinea con los objetivos de protección del usuario establecidos en la **Ley 11/2022, General de Telecomunicaciones**, que reconoce el derecho de los usuarios a recibir comunicaciones seguras y fiables. La aplicación práctica de la Circular contribuye a materializar este derecho mediante la introducción de garantías técnicas adicionales.

En segundo lugar, el impacto se manifiesta en la **reducción de la eficacia de las técnicas de fraude**, especialmente del *spoofing* y del *smishing*. Al dificultar la utilización de identificadores falsificados, el sistema limita la capacidad de los operadores fraudulentos para engañar a los usuarios. Esto no elimina completamente el fraude, pero sí reduce uno de sus principales vectores.

El **Tribunal Supremo**, en la **STS de 20 de mayo de 2021 (rec. 3387/2019)**, puso de relieve que la apariencia de legitimidad en las comunicaciones electrónicas constituye un elemento esencial en la configuración del engaño en los fraudes digitales. La eliminación o reducción de esta apariencia mediante mecanismos de control tiene, por tanto, un efecto directo en la prevención del fraude.

Desde la perspectiva de los operadores, la aplicación de la Circular implica una **transformación de sus sistemas técnicos y operativos**. La integración del Registro de Alias y de los mecanismos de verificación requiere inversiones tecnológicas y ajustes en los procesos de gestión del tráfico de comunicaciones. Este impacto organizativo es significativo, aunque necesario para garantizar la seguridad del sistema.

Asimismo, las entidades emisoras de comunicaciones —como bancos, empresas o Administraciones públicas— se ven obligadas a **adaptar sus prácticas de comunicación**, registrando sus alias y asegurando su uso correcto. Este proceso contribuye a profesionalizar y estructurar el uso de identificadores en las comunicaciones digitales.

No obstante, desde una perspectiva crítica constructiva, el impacto práctico del sistema presenta ciertas limitaciones. En primer lugar, la eficacia de las medidas depende de su **aplicación uniforme por todos los operadores**. La existencia de diferencias en la implementación puede generar brechas que sean aprovechadas por los operadores fraudulentos.

En segundo lugar, el sistema no elimina completamente el riesgo de fraude, ya que los defraudadores pueden adaptar sus estrategias, utilizando otros canales o técnicas distintas a la suplantación de alias. Esto pone de manifiesto la necesidad de complementar las medidas regulatorias con acciones de concienciación y formación de los usuarios.

El **Tribunal Constitucional**, en la **STC 55/2018, de 24 de mayo**, ha señalado que la eficacia de las políticas públicas en entornos digitales depende no solo de las medidas técnicas, sino también de la implicación de los distintos actores, incluidos los propios usuarios. Esta doctrina refuerza la idea de que la seguridad de las comunicaciones es una responsabilidad compartida.

Otro aspecto relevante es la posible **incidencia en la continuidad de las comunicaciones legítimas**, especialmente en casos en los que la verificación no se realice correctamente. La existencia de falsos positivos en los sistemas de bloqueo puede afectar a la prestación de servicios, lo que exige un diseño cuidadoso de los mecanismos de control.

En conclusión, la **Circular 1/2026** tiene un impacto positivo en la seguridad de las comunicaciones digitales, al reforzar la autenticidad de los identificadores y reducir la eficacia de las técnicas de fraude. No obstante, su efectividad dependerá de su correcta implementación, de la coordinación entre operadores y de su complementariedad con otras medidas de protección y concienciación.

8. Valoración crítica constructiva de la regulación del fraude de identidad digital

La **Circular 1/2026, de 18 de marzo**, representa un avance significativo en la respuesta regulatoria frente al fraude de identidad en comunicaciones digitales, al introducir instrumentos específicos como el Registro de Alias y mecanismos de verificación y bloqueo que inciden directamente sobre el principal vector del fraude: la suplantación del identificador de origen. Desde una perspectiva global, la norma se alinea con las tendencias regulatorias europeas orientadas a reforzar la seguridad de las comunicaciones electrónicas.

Uno de los principales aciertos de la regulación es su **enfoque preventivo**, que actúa en origen sobre la autenticidad de las comunicaciones. A diferencia de los modelos tradicionales basados exclusivamente en la sanción posterior del fraude, la Circular introduce mecanismos que dificultan la ejecución de las conductas fraudulentas, reduciendo su eficacia antes de que produzcan efectos.

Asimismo, la creación del Registro de Alias constituye una **innovación relevante**, al establecer un sistema estructurado de identificación de remitentes en el ámbito de los mensajes alfanuméricos. Este instrumento permite reforzar la trazabilidad y facilita la aplicación de medidas de control por parte de los operadores, contribuyendo a mejorar la seguridad del sistema.

La legitimidad de este tipo de intervenciones ha sido avalada por la jurisprudencia. El **Tribunal Supremo**, en la **STS de 15 de marzo de 2021 (rec. 3936/2018)**, reconoció la capacidad de los organismos reguladores para imponer obligaciones técnicas a los operadores cuando resulten necesarias para la protección de los usuarios y la integridad del sistema. Esta doctrina refuerza la validez del modelo adoptado.

No obstante, desde una perspectiva crítica constructiva, la regulación presenta ciertos límites que deben ser considerados. En primer lugar, la eficacia del sistema depende en gran medida de su **implementación técnica por los operadores**. La existencia de diferencias en los niveles de desarrollo tecnológico o en la aplicación de los mecanismos de verificación puede generar desigualdades y reducir la efectividad del sistema.

En segundo lugar, la **naturaleza global de las comunicaciones electrónicas** plantea un desafío estructural. Las medidas adoptadas a nivel nacional pueden verse limitadas cuando las comunicaciones fraudulentas se originan en otros países o a través de infraestructuras no sujetas al control directo de la CNMC. Esto exige avanzar hacia una mayor coordinación internacional y la adopción de estándares comunes.

Otro aspecto a considerar es la **complejidad técnica y operativa del sistema**, que puede suponer una carga significativa para los operadores y para las entidades emisoras de comunicaciones. La necesidad de registrar alias, adaptar sistemas y gestionar procesos de verificación requiere recursos técnicos y organizativos que no todos los agentes pueden asumir con la misma facilidad.

El **Tribunal Constitucional**, en la **STC 79/2017, de 22 de junio**, ha señalado que las obligaciones impuestas a los operadores económicos deben respetar el principio de proporcionalidad, evitando cargas excesivas que puedan afectar a la libre competencia o a la actividad económica. Esta doctrina invita a valorar cuidadosamente el equilibrio entre seguridad y eficiencia.

Asimismo, el sistema debe integrarse de forma coherente con otros marcos normativos, especialmente en materia de protección de datos. La gestión del Registro de Alias implica el tratamiento de información sensible, lo que exige su compatibilidad con el **Reglamento (UE) 2016/679 (RGPD)** y la adopción de medidas adecuadas de seguridad.

Desde una perspectiva estratégica, la Circular 1/2026 puede interpretarse como un primer paso hacia un modelo más robusto de autenticación de las comunicaciones, pero no como una

solución definitiva. La evolución constante de las técnicas de fraude obliga a mantener una actitud dinámica y a adaptar continuamente los instrumentos regulatorios.

En conclusión, la regulación introducida por la **Circular 1/2026** constituye una respuesta adecuada y necesaria frente al fraude de identidad en comunicaciones digitales, al reforzar los mecanismos de prevención y control. Sin embargo, su eficacia dependerá de su correcta implementación, de la coordinación entre los distintos actores y de su capacidad para evolucionar en un entorno tecnológico en constante cambio.