MINISTERIO PARA LA
TRANSFORMACIÓN DIGITAL Y DE
LA FUNCIÓN PÚBLICA

MEMORIA DEL ANÁLISIS DE IMPACTO NORMATIVO

PROYECTO DE ORDEN POR LA QUE SE ESTABLECEN MEDIDAS PARA COMBATIR LAS ESTAFAS DE SUPLANTACIÓN DE IDENTIDAD A TRAVES DE LLAMADAS TELEFÓNICAS Y MENSAJES DE TEXTO FRAUDULENTOS Y PARA GARANTIZAR LA IDENTIFICACIÓN DE LA NUMERACIÓN UTILIZADA PARA LA PRESTACIÓN DE SERVICIOS DE ATENCIÓN AL CLIENTE Y REALIZACIÓN DE LLAMADAS COMERCIALES PROSPECTIVAS.

23 DE JULIO DE 2024

FICHA RESUMEN EJECUTIVO

Ministerio/Órgano proponente	Ministerio para la Transformación Digital y de la Función Pública	**Fecha**	23 de julio de 2024
Título de la norma	PROYECTO DE ORDEN POR LA QUE SE ESTABLECEN MEDIDAS PARA COMBATIR LAS ESTAFAS DE SUPLANTACIÓN DE IDENTIDAD A TRAVES DE LLAMADAS TELEFÓNICAS Y MENSAJES DE TEXTO FRAUDULENTOS Y PARA GARANTIZAR LA IDENTIFICACIÓN DE LA NUMERACIÓN UTILIZADA PARA LA PRESTACIÓN DE SERVICIOS DE ATENCIÓN AL CLIENTE Y REALIZACIÓN DE LLAMADAS COMERCIALES PROSPECTIVAS.		
Tipo de Memoria	Normal ■ Abreviada ☐		
OPORTUNIDAD DE LA PROPUESTA			
Objeto de la norma	La norma adopta soluciones para evitar que progresen las comunicaciones con manipulación del identificador de llamada (CLI, por sus siglas en inglés), introduce mecanismos para evitar fraudes en el ámbito de la numeración y los códigos alfanuméricos identificativos de mensajes cortos y establece medidas para garantizar la correcta identificación de la numeración utilizada para la prestación del servicio de atención a clientes o para la realización de llamadas comerciales prospectivas.		
Objetivos que se persiguen	En los últimos años estamos asistiendo a un incremento exponencial de la cibercriminalidad y, en particular, de las estafas de suplantación de identidad que suelen comenzar con una llamada o un mensaje de texto en los que el emisor de la comunicación suplanta la identidad de una organización de confianza (entidad bancaria, administración pública, empresa de transporte, etc.) con la clara intención de defraudar, engañando al consumidor para que proporcione información personal y financiera confidencial, facilite sus claves personales o realice alguna acción como el acceso a una web, la llamada a un número telefónico, la realización de una trasferencia, o la contratación de un servicio, entre otros. La confianza de los consumidores en la fiabilidad y seguridad del contenido transmitido a través de las redes, el amplio uso que hacen las empresas y organismos de las comunicaciones electrónicas como medio para contactar con sus usuarios, así como la capacidad de estas comunicaciones para llegar a un gran número de personas a un coste		

	relativamente bajo, hacen que el uso de llamadas y mensajes de texto sea un instrumento frecuentemente utilizado en la comisión de este tipo de estafas. En consecuencia, la norma tiene por objetivo prevenir estas estafas y prácticas fraudulentas que se canalizan a través de llamadas y mensajes de texto. Asimismo, se persigue facilitar la correcta identificación de llamadas de atención al cliente y llamadas comerciales prospectivas, prohibiendo la utilización para estas llamadas de numeración móvil y atribuyendo a las mismas los rangos 800 y 900, asegurando de este modo su gratuidad en caso de devolución de la llamada.
Principales alternativas consideradas	• Se descarta la alternativa de no aprobar regulación alguna, ya que es necesario dar respuesta a la inquietud social generada ante las estafas de suplantación de identidad y facilitar la correcta Identificación de la numeración utilizada para la prestación del servicio de atención a clientes o para la realización de llamadas comerciales prospectivas. • Se considera que la aprobación de la presente orden es la opción que proporciona una mayor seguridad jurídica a los operadores involucrados en la prestación de estos servicios. Asimismo, se estima que las medidas adoptadas son las mínimas imprescindibles para atajar el uso indebido de la numeración y el tráfico irregular con fines fraudulentos, poniendo fin a la inquietud social generada.
CONTENIDO, ANÁLISIS JURÍDICO Y DESCRIPCION DE LA TRAMITACION	
Tipo de norma	Orden Ministerial
Estructura de la Norma	La Orden Ministerial consta una parte expositiva, cuatro capítulos con nueve artículos y tres disposiciones finales.
Tramitación	De acuerdo con lo establecido en el artículo 133.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el proyecto de modificación de Orden Ministerial ha sido sometido a trámite de consulta pública previa a través de la sede electrónica del Ministerio para la Transformación Digital y de la Función Pública entre los días 14 de febrero y 8 de marzo de 2024.

	De acuerdo con lo establecido en el artículo 133.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el texto será sometido, asimismo, a audiencia pública a través de la sede electrónica del Ministerio.	
Informes a recabar	Se han de recabar informes de: CNMC Ministerio de Consumo Consejo de Consumidores y Usuarios Secretaría General Técnica del Ministerio para la Transformación Digital y de la Función Pública	
ANALISIS DE IMPACTOS		
ADECUACIÓN AL ORDEN DE COMPETENCIAS	La norma se dicta al amparo de la competencia exclusiva estatal en materia de telecomunicaciones, prevista en el artículo 149.1.21. ª de la Constitución.	
IMPACTO ECONÓMICO Y PRESUPUESTARIO	Efectos sobre la economía en general.	La norma tendrá efectos positivos en la economía ya que estas estafas causan importantes daños financieros y económicos a todos los sectores de la sociedad, incluidos los consumidores, las empresas y los organismos públicos. Además, disminuyen la confianza de los consumidores en las comunicaciones electrónicas, provocando que, a raíz de la generalización de estas prácticas, desconfíen de contestar llamadas y leer mensajes de texto, perjudicando a aquellas empresas y organismos que hacen un uso legítimo de llamadas y mensajes de texto, como canal de comunicación para facilitar información u ofrecer sus servicios a los consumidores.

	En relación con la competencia	■ La norma tiene efectos positivos sobre la competencia. ☐ La norma tiene efectos negativos sobre la competencia. ☐ La norma no tiene efectos sobre la competencia.
	Desde el punto de vista de las cargas administrativas	☐ Supone una reducción de cargas administrativas. ☐ Incorpora nuevas cargas administrativas. ■ No afecta a las cargas administrativas de las empresas.
	Desde el punto de vista de los presupuestos, la norma ■ No afecta a los presupuestos de la AGE ni de otras Administraciones ☐ Afecta a los presupuestos de la AGE ☐ Afecta a los presupuestos de otras Administraciones.	☐ implica un ingreso ☐ implica un gasto
IMPACTO DE GÉNERO	La norma tiene un impacto de género:	Negativo ☐ Nulo ■ Positivo ☐

OTROS IMPACTOS CONSIDERADOS	No existen impactos por razón de género", en la "infancia y adolescencia", por razón de "oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad", en la "familia", ni "por razón de cambio climático".
OTRAS CONSIDERACIONES	

I.- OPORTUNIDAD DE LA PROPUESTA

1) Motivación.

En los últimos años estamos asistiendo a un incremento exponencial de la cibercriminalidad y, en particular, de las estafas de suplantación de identidad que suelen comenzar con una llamada o un mensaje de texto en los que el emisor de la comunicación suplanta la identidad de una organización de confianza (entidad bancaria, administración pública, empresa de transporte, etc.) con la clara intención de defraudar, engañando al consumidor para que proporcione información personal y financiera confidencial, facilite sus claves personales o realice alguna acción como el acceso a una web, la llamada a un número telefónico, la realización de una trasferencia, o la contratación de un servicio, entre otros.

La confianza de los consumidores en la fiabilidad y seguridad del contenido transmitido a través de las redes, el amplio uso que hacen las empresas y organismos de las comunicaciones electrónicas como medio para contactar con sus usuarios, así como la capacidad de estas comunicaciones para llegar a un gran número de personas a un coste relativamente bajo, hacen que el uso de llamadas y mensajes de texto sea un instrumento frecuentemente utilizado en la comisión de este tipo de estafas.

Las estafas de suplantación de identidad van en aumento en los últimos años:

Según la última Memoria de Reclamaciones del Banco de España (2022), publicada en octubre de 2023, las reclamaciones por fraude (10.361) han duplicado su volumen respecto al año anterior. La suplantación de identidad está detrás de alrededor del 47% de las reclamaciones.

De acuerdo al último Informe sobre la Cibercriminalidad en España del Ministerio del Interior (2022), los ciberdelitos (374.737) han aumentado un 22,7% respecto al año anterior, de los cuales el 90% se corresponden a fraudes informáticos.

Según el Instituto Nacional de Ciberseguridad (INCIBE) durante el año 2022 continuaron proliferando las campañas de suplantación de la identidad, mediante vía telefónica y correo electrónico, ascendiendo a un total de 33.576 incidentes.

Estas estafas causan importantes daños financieros y económicos a todos los sectores de la sociedad, incluidos los consumidores, las empresas y los organismos públicos. Además, disminuyen la confianza de los consumidores en las comunicaciones electrónicas, provocando que, a raíz de la generalización de estas prácticas, desconfíen de contestar llamadas y leer mensajes de texto, perjudicando a aquellas empresas y organismos que hacen un uso legítimo

de llamadas y mensajes de texto, como canal de comunicación para facilitar información u ofrecer sus servicios a los consumidores.

Por ello con el objetivo, recogido en el artículo 3 de la Ley 11/2022, de 28 de junio General de Telecomunicaciones, de defender los intereses de los usuarios, restaurando la confianza de los consumidores en las comunicaciones electrónicas, entre los días 14 de febrero y 8 de marzo de 2024, se han sometido a consulta pública una serie de opciones técnicas y regulatorias destinadas a prevenir y combatir este tipo de estafas y prácticas fraudulentas que se canalizan a través de llamadas y mensajes de texto.

De las respuestas a dicha consulta pública se concluye la necesidad de adoptar medidas en distintos ámbitos.

2) - Objetivos

La norma adopta soluciones para evitar que progresen las comunicaciones con manipulación del identificador de llamada (CLI, por sus siglas en inglés), introduce mecanismos para evitar fraudes en el ámbito de la numeración y los códigos alfanuméricos identificativos de mensajes cortos y establece medidas para garantizar la correcta identificación de la numeración utilizada para la prestación del servicio de atención a clientes o para la realización de llamadas comerciales prospectivas

3) Principios de buena regulación

La norma se adecua a los principios de buena regulación previstos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, particularmente:

- A los de **necesidad y eficacia**, al estar justificada por razones de interés general, en defensa de los intereses de los usuarios
- Al de **proporcionalidad**, al contener la regulación imprescindible para atender las necesidades que pretende cubrir.
- Al de **eficiencia**, ya que la iniciativa normativa evita cargas administrativas innecesarias o accesorias y racionaliza, en su aplicación, la gestión de los recursos públicos.
- Al de **seguridad jurídica**, puesto que desarrolla normativa ya aprobada, siendo su adopción predecible ante el considerable aumento de este tipo de prácticas.
- Al de **transparencia**, finalmente, toda vez que el texto del proyecto de modificación ha sido objeto de consulta y será objeto de audiencia y publicación en el "Boletín Oficial del Estado".

4) Principales alternativas consideradas

Se descarta no aprobar regulación alguna, ya que estas estafas están provocando una importante inquietud social y causan importantes daños financieros y económicos a todos los sectores de la sociedad, incluidos los consumidores, las empresas y los organismos públicos. Además, disminuyen la confianza de los consumidores en las comunicaciones electrónicas, provocando que, a raíz de la generalización de estas prácticas, desconfíen de contestar llamadas y leer mensajes de texto, perjudicando a aquellas empresas y organismos que hacen

un uso legítimo de llamadas y mensajes de texto, como canal de comunicación para facilitar información u ofrecer sus servicios

Se considera que la aprobación de la presente Orden es la opción que proporciona una mayor seguridad jurídica a los operadores involucrados en la prestación de estos servicios. Asimismo, se estima que las medidas adoptadas son las mínimas imprescindibles para atajar el uso indebido de la numeración y el tráfico irregular con fines fraudulentos, poniendo fin a la inquietud social generada.

5) Colectivos afectados:

La norma afecta a los siguientes colectivos:

- Operadores que prestan servicios de comunicaciones vocales y operadores que proporcionan servicios de comunicaciones electrónicas de almacenamiento y reenvío de mensajes, que deberán impedir que estas llamadas y mensajes fraudulentos progresen, asegurando su bloqueo.

- Empresas que prestan de servicios de atención al cliente o realizan llamadas comerciales prospectivas, que no podrán utilizar numeración móvil para la realización de estas llamadas, permitiéndoseles el acceso a los rangos de numeración 800 y 900, gratuitos para los usuarios en caso de devolución de la llamada.

- Ciudadanos, empresas y Administraciones Públicas que se verán protegidos frente a determinadas estafas que se han incrementado enormemente en los últimos años.

- **Interés público afectado:**

El interés público afectado es el correcto funcionamiento de los servicios de comunicaciones electrónicas, y la defensa de los intereses de los usuarios de estos servicios reconocida tanto en la Ley General de Telecomunicaciones como en la Directiva (UE) 2018/1972, de 11 de diciembre de 2018 por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

II: CONTENIDO, ANALISIS JURÍDICO Y DESCRIPCION DE LA TRAMITACION

1) Contenido:

El proyecto de modificación de orden ministerial de referencia se estructura en una parte expositiva, cuatro capítulos con nueve artículos y tres disposiciones finales.

Dentro del **Capítulo I, de disposiciones generales:**

- El **artículo 1** establece el **objeto de la norma** consistente en la adopción de soluciones para evitar que progresen las comunicaciones con manipulación del identificador de llamada (CLI, por sus siglas en inglés), introduce mecanismos para evitar fraudes en el ámbito de la numeración y los códigos alfanuméricos identificativos de mensajes

cortos y establece medidas para garantizar la correcta identificación de la numeración utilizada para la prestación del servicio de atención a clientes o para la realización de llamadas comerciales prospectivas.

- El **artículo 2** se refiere al **ámbito de aplicación**.

- El **artículo 3** recoge **definiciones** de términos utilizados en la norma

Dentro del **Capítulo II** destinado a **medidas para evitar que progresen las comunicaciones con manipulación del identificador de llamada**:

- El **artículo 4** obliga los operadores a b**loquear aquellas llamadas que presenten** como CLI **numeración** perteneciente al plan nacional de numeración telefónica, aprobado mediante Real Decreto 2296/2004, de 10 de diciembre, **que no haya sido atribuida, habilitada o asignada.**

- El **artículo 5** obliga a los operadores **a bloquea**r las **llamadas con origen internacional identificadas por un CLI del plan nacional de numeración.**

Dentro del **Capítulo III destinado a la adopción de medidas para evitar fraudes en el ámbito de los servicios de mensajería**:

- El **artículo 6** obliga a los operadores que proporcionan servicios de comunicaciones electrónicas de almacenamiento y reenvío de mensajes, a **bloquear los mensajes con origen internacional identificados por un CLI del plan nacional de numeración**.

- El **artículo 7** obliga a los operadores a **bloquear todos aquellos SMS/MMS que hagan uso de caracteres alfanuméricos (alias) que no consten en el Registro** gestionado al efecto por la Comisión Nacional de los Mercados y de la Competencia o **que hayan sido emitidos por proveedores de servicios de mensajería que no hayan sido habilitados en dicho registro** para el envío y transmisión de SMS/MMS utilizando como identificador el alias inscrito.

Por último, en **el capítulo IV, destinado a medidas para garantizar la correcta identificación de la numeración utilizada para la prestación de servicios de atención a clientes o para la realización de llamadas comerciales prospectivas**:

- El **artículo 8 prohíbe usar** para estas llamadas **numeración móvil**.

- El **artículo 9 permite**, con carácter general, la **utilización de numeración 800 y 900** para la realización de estas llamadas, de modo que, devolver las llamadas a estos números, resulte gratuito para los consumidores.

La **disposición final primera revisa la redacción de la Resolución de 27 de mayo de 2013, por la que se modifica la atribución de los rangos de numeración para comunicaciones móviles** para excluir la posibilidad de uso de numeración móvil para llamadas de atención a clientes

La **disposición final segunda** recoge **el título competencial** que es la competencia exclusiva del Estado en materia de telecomunicaciones reconocida en el artículo 149.1.21.ª de la Constitución.

La **disposición final tercera**, a fin de atajar cuanto antes estas estafas, protegiendo los derechos de los ciudadanos, recoge que la **entrada en vigor** de la norma se producirá a los 20 días de su publicación en el «Boletín Oficial del Estado». No obstante, para permitir que los operadores se adapten a sus medidas se establecen plazos más largos para la **aplicabilidad** de determinados artículos: el artículo 5 será aplicable a los 3 meses de su entrada en vigor, para los números llamantes del servicio de telefonía fija, y a los 6 meses para los del servicio de telefonía móvil. El artículo 6 será aplicable a los 6 meses de su entrada en vigor. El artículo 7 de la presente orden será aplicable a los 12 meses de su entrada en vigor.

2) Análisis Jurídico

La norma persigue la defensa de los intereses de los usuarios proclamada en el **artículo 3 de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones**.

Se considera que la norma debe tener rango de orden de orden ministerial ya que desarrolla preceptos contenidos en diversos Reales Decretos:

La medida prevista en el **artículo 4** (Bloqueo de llamadas que presenten como CLI numeración no atribuida, asignada o habilitada) se adopta en **desarrollo de lo previsto en el artículo 2.2.a) del Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones electrónicas**, cuya disposición final segunda permite al ahora Ministro para la Transformación Digital y de la Función Pública dicta cuantas disposiciones y medidas sean necesarias para el desarrollo y aplicación de lo establecido en dicho real decreto.

La medida contenida en el **artículo 5** (bloqueo de llamadas con origen internacional identificadas por un CLI del plan nacional de numeración) **desarrolla** lo establecido en el **artículo 81 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril,** cuya disposición final quinta autoriza al ahora Ministro para la Transformación Digital y de la Función Pública a dictar las disposiciones necesarias para el desarrollo y aplicación de este real decreto.

El **artículo 6** que obliga a bloquear los mensajes con origen internacional identificados por un CLI del plan nacional de numeración **y el artículo 7** (bloqueo de SMS/MMS que hagan uso de alias que no consten en el Registro o que hayan sido emitidos por proveedores de servicios de mensajería que no hayan sido habilitados en dicho registro) completan las obligaciones ya previstas en la Orden ITC/308/2008, de 31 de enero, por la que se dictan instrucciones sobre la utilización de recursos públicos de numeración para la prestación de servicios de mensajes cortos de texto y mensajes multimedia, y **se adoptan conforme al citado artículo 30.1 del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por Real Decreto 2296/2004 de 10 de diciembre, cuya disposición**

final primera recoge las competencias de desarrollo atribuidas al Ministro para la Transformación Digital y de la Función Pública.

El **artículo 8** (prohibición numeración móvil) **desarrolla lo previsto en el artículo 27.7 del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por Real Decreto 2296/2004, de 10 de diciembre**.

El **artículo 9,** por último, **desarrolla el artículo 61.2 del citado Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios,** aprobado por Real Decreto 424/2005, de 15 de abril.

Todo ello se completa con lo dispuesto en el **artículo 30.1 del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por Real Decreto 2296/2004, de 10 de diciembre** según el cual los operadores de redes y de servicios de comunicaciones electrónicas estarán obligados a poner en práctica las medidas necesarias para dar cumplimiento a las decisiones que adopte el Ministerio para la Transformación Digital y de la Función Pública en el ámbito de sus competencias sobre numeración. En particular, los operadores estarán obligados a realizar, en los sistemas que exploten, las modificaciones necesarias para tratar y encaminar las comunicaciones de forma eficiente cuando el Ministerio adopte decisiones que impliquen alteraciones en los planes de numeración, direccionamiento o denominación, y cuando se realicen asignaciones, atribuciones o adjudicaciones de dichos recursos públicos. El coste que ello conlleve será sufragado por cada operador.

3) Descripción de la tramitación

Este proyecto constituye una iniciativa del Ministerio para la Transformación Digital y de la Función Pública, quien ha llevado a cabo:

a) Consulta pública. De acuerdo con lo establecido en el artículo 133.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y art.26 de la Ley 50/1997, de 27 de noviembre, del Gobierno, el proyecto de orden de la ministra ha sido sometido al trámite de consulta pública mediante publicación en la Ministerio para la Transformación Digital y de la Función Pública entre los días 14 de febrero y 8 de marzo de 2024.

   En dicha consulta se recibieron 53 contribuciones cuya relación figura como Anexo 1 a la presente MAIN

   El resumen de las consultas planteadas en la consulta pública y de las principales aportaciones recibidas se contiene como Anexo 2 a la presente MAIN

b) Audiencia o información pública

   Asimismo, de conformidad con el artículo 133.2 de la Ley 39/2015, de 1 de octubre del Procedimiento Administrativo Común de las Administraciones Públicas y el artículo 26 de la Ley 50/1997, de 27 de noviembre, del Gobierno, el proyecto ha de someterse al trámite de audiencia y de información pública, al objeto de dar audiencia a los ciudadanos y

recabar cuantas aportaciones adicionales puedan hacerse, mediante publicación en la sede del Ministerio para la Transformación Digital y de la Función Pública

4. Informes

La propuesta de Orden ha de ser sometida a **informe de la CNMC.**

Asimismo, la propuesta ha de ser informada por el **Ministerio de Consumo** y por el **Consejo de Consumidores y Usuarios**

Por último, la propuesta ha de ser informada por la **Secretaría General Técnica del Ministerio para la Transformación Digital y de la Función Pública**

III.- ADECUACION AL ORDEN CONSTITUCIONAL DE DISTRIBUCIÓN DE COMPETENCIAS

El proyecto de modificación de orden de la ministra se dicta al amparo de las competencias recogidas en el artículo 149.1.21ª de la Constitución española que atribuyen al Estado competencia exclusiva en materia de telecomunicaciones.

IV.- ENTRADA EN VIGOR

La Orden entrará en vigor a los 20 días de su publicación en el Boletín Oficial del Estado, apartándose de la regla general (2 de enero o 1 de julio siguiente a su aprobación) de conformidad con el artículo 23 de la ley 50/1997, de 27 de noviembre, del Gobierno, ya que es necesario dar respuesta cuánto antes a la inquietud social generada por el creciente número de estafas que hacen uso de llamadas y mensajes.

V. ANÁLISIS DE IMPACTOS.

a) Impacto económico.

La norma proyectada tendrá efectos positivos en la economía ya que las estafas que se pretenden combatir causan importantes daños financieros y económicos a todos los sectores de la sociedad, incluidos los consumidores, las empresas y los organismos públicos. Además, disminuyen la confianza de los consumidores en las comunicaciones electrónicas, provocando que, a raíz de la generalización de estas prácticas, desconfíen de contestar llamadas y leer mensajes de texto, perjudicando a aquellas empresas y organismos que hacen un uso legítimo de llamadas y mensajes de texto, como canal de comunicación para facilitar información u ofrecer sus servicios a los consumidores.

Asimismo, se considera que la norma tiene efectos positivos sobre la competencia ya que al eliminar determinadas prácticas fraudulentas se impulsará una competencia sana entre los distintos operadores que se ajustan a los requisitos legalmente establecidos.

b) Impacto presupuestario.

La norma no tiene impacto presupuestario.

c) Impacto por razón de género.

Este impacto se analiza en virtud de lo dispuesto en el artículo 19 de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva entre mujeres y hombres, y en el artículo 26.3.f) de la Ley 50/1997, de 27 de noviembre, del Gobierno.

Este proyecto carece de impacto por razón de género al no existir una situación previa de desigualdad.

d) Impacto en la infancia y la adolescencia.

Este proyecto carece de impacto en este ámbito, más allá del beneficio general para todos los usuarios de los servicios de comunicaciones electrónicas.

e) Impacto por razón de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

El contenido del proyecto normativo no tiene impacto en este ámbito más allá del beneficio general para todos los usuarios.

f) Impacto en la familia.

El contenido del proyecto normativo no tiene impacto en la familia, más allá del beneficio general para todos los usuarios de los servicios de comunicaciones electrónicas.

g) Impacto por razón del cambio climático

De conformidad con lo establecido en el artículo 26.3.h) de la Ley 50/1997, de 27 de noviembre, del Gobierno, se estima que la norma no tiene efectos en términos de mitigación y adaptación al cambio climático.

Anexo 1

RELACIÓN DE ALEGACIONES RECIBIDAS EN FASE DE CONSULTA PÚBLICA

TOTAL ALEGACIONES RECIBIDAS: 54

1. AB HANDSHAKE CORPORATION (08/03/24)
2. ABANCA CORPORACIÓN BANCARIA, S.A. (08/03/24)
3. AEB (ASOCIACIÓN ESPAÑOLA BANCA) (08/03/24)
4. AEECF (ASOCIACIÓN ESPAÑOLA DE EMPRESAS CONTRA EL FRAUDE (07/03/24)
5. AEERC/ASOCIACIÓN CEX (ASOCIACIÓN ESPAÑOLA DE EXPERTOS EN RELACIÓN DE CLIENTES/ASOCIACIÓN DE COMPAÑÍAS DE EXPERIENCIA CON CLIENTES) (29/02/24)
6. AEFI (07/03/24)
7. ALISYS (07/03/24)
8. AOTEC (08/03/24)
9. ASOTEM (08/03/24)
10. ASSECO GROUP (08/03/24)
11. ASTEL (07/03/24)
12. AUI (07/03/24)
13. AYUNTAMIENTO DE NERJA (16/02/24)
14. CECA (08/03/24)
15. CECU (08/03/24)
16. COLT TECHNOLOGY SERVICES (08/03/24)
17. DIGI SPAIN TELECOM, S.L.U. (08/03/24)
18. DIGITALES (08/03/24)
19. ENDESA (08/03/24)
20. ENERGYA VM GESTIÓN DE ENERGIA, S.L.U. (19/03/24) (FUERA DE PLAZO)
21. EURO 6000, S.L. (08/03/24)
22. F24 SERVICIOS DE COMUNICACIÓN, S.L.U. (07/03/24)
23. FENIE ENERGIA, S.A. (08/03/24)
24. FRAUDFENSE (08/03/24)
25. FUNDACIÓN ESYS (EMPRESA, SEGURIDAD Y SOCIEDAD DIGITAL) (08/03/24)
26. GAMMA OPERADORA DE TELECOMUNICACIONES, S.A.U. (08/03/24)

27. HIYA INC. (08/03/24)

28. I3FORUM (BTSE - BUSINESS TELECOMMUNICATIONS SERVICES EUROPE, S.A.) (07/03/24)

29. IBERCAJA BANCO (07/03/24)

30. INSTITUTE IMDEA + UCL (UNIVERSITY COLLEGE LONDON) (08/03/24)

31. LLEIDANETWORKS SERVEIS TELEMATICS, S.A. (TRANSACTION NETWORK SERVICES, INC. ("TNS") Y SU SUBSIDIARIA TRANSACTION NETWORK SERVICES S.A. S.) (08/03/24)

32. MASMOVIL IBERCOM, S.A.U. (08/03/24)

33. MEF (MOBILE ECOSYSTEM FORUM) (08/03/24)

34. MINISTERIO DEL INTERIOR/UNIDAD CENTRAL CIBERDELINCUENCIA (07/03/24)

35. NUMERACLE INC (12/03/24) (FUERA DE PLAZO)

36. OCU (08/03/24)

37. ORANGE ESPAGNE, S.A.U. (08/03/24)

38. PROVENANT (09/03/24) (FUERA DE PLAZO)

39. QUOBIS NETWORKS, S.L. (08/03/24)

40. RIBBON COMUNICATIONS (08/03/24) (CONFIDENCIAL) (INGLÉS)

41. SINCH AB & SINCH SPAIN COMUNICACIONES S.L. (08/03/24)

42. SOMOS INC. (08/03/24) (INGLÉS)

43. TELEFÓNICA ESPAÑA (08/03/24)

44. TCR (THE CAMPAING REGISTRY) (08/03/24)

45. UCARAGÓN (UNIÓN DE CONSUMIDORES DE ARAGÓN) (08/03/24)

46. UNACC (UNIÓN NACIONAL DE COOPERATIVAS DE CRÉDITO) (08/03/24)

47. VODAFONE ESPAÑA, S.A.U (08/03/24) (CONFIDENCIAL)

PARTICULARES (7)

48. ALVARO SÁNCHEZ RODRÍGUEZ* (21/02/24)

49. ANA ISABEL RAMIZ PLANA (27/02/24)

50. DAVID CH** (28/02)

51. JORGE JOSÉ ARBOLEDA ROMERO (19/02/24)

52. JOSÉ CARLOS GONZÁLEZ VIEJO (14/02/24)

53. JOSÉ MARCOS GIMÉNEZ TERUEL* (16/02/24)

54. JOSÉ MARÍA NARANJO FLOX + 2 (07/03/24)

*Sin datos DNI

** Sin datos DNI, ni nombre completo

Anexo 2

Resumen de las preguntas planteadas en la consulta pública y de las aportaciones recibidas

1. Posibles medidas en el ámbito de la numeración identificativa del origen de las llamadas.

1a)

¿Qué consideración le merece la posible medida regulatoria que obligara a los operadores de comunicaciones vocales disponibles al público a bloquear las llamadas con origen internacional identificadas por un CLI del plan nacional de numeración?

OPERADORES Y ASOCIACIONES DE OPERADORES

En general se muestran a favor de la medida, y que su aplicación fuese obligatoria para todos los operadores, pero algunos muestran preocupación a que se pueda bloquear tráfico legítimo (ej. conmutación en un único punto para varios países, llamadas desviadas, …).

SUMINISTRADORES

RIBBON e HIYA están a favor de la medida, si bien esta última señala que en otros mercados se observó un descenso sólo durante 1-2 meses, antes de que se adaptaran los estafadores a la restricción (ej. manteniendo su tráfico de llamadas fuera de la red de telefonía hasta que llegara a un punto nacional, o explotando los casos de excepción dejados para el tráfico de llamadas legítimo).

Quobis y F24 que la consideran una medida demasiado restrictiva.

TCR señala que para abordar este problema debe haber una combinación establecida de firewalls a nivel TELCO, así como regulaciones y sanciones.

POLICIA NACIONAL

Consideran que deben boquearse:

- las llamadas nacionales o internacionales que tienen como CLI un número que no se ajusta al formato de numeración valido en España

- Las llamadas nacionales o internacionales que tienen como CLI un número válido pero no asignado

- las llamadas internacionales con CLI valido asignado cuando la línea móvil esté dentro de España

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC).

En términos generales se muestran a favor, para lo que algunas señalan que debe derogarse la obligación legal de cursar dicho tráfico.

AEECF

Se valora positivamente siempre que pueda haber excepciones

AEERC/CEX

Recuerdan que la industria del Contact Center español opera muchas veces desde terceros países, pero la numeración es nacional, por lo que salvo que técnicamente se pueda discriminar los "orígenes auténticos" se muestran en contra de esta medida.

OCU, CECU, AUI

Deben bloquearse.

¿Considera necesario o conveniente excluir de esta medida algún tipo de numeración nacional (p.ej. centros de atención de llamadas ubicados fuera del territorio nacional)? En caso afirmativo, identifique la numeración a excluir y explique las razones.

OPERADORES Y ASOCIACIONES DE OPERADORES

En general no se muestran proclives al establecimiento de excepciones pues podría ser una puerta de entrada al fraude. La numeración fija es para uso en España, los Call Centers en el extranjero precisan de un Punto de Terminación de Red en España. No obstante, podría haber casos legítimos que habría que estudiar Telefónica menciona los números traducidos de ámbito nacional), si bien operadores como Vodafone consideran que ninguna numeración nacional del servicio fijo debería quedar excluida de esta obligación de control (pone de ejemplo el archivo de actuaciones por parte de la AEPD al estar situados en el extranjero los que realizan estas prácticas).

SUMINISTRADORES

En términos generales se considera necesario realizar un análisis cuidadoso de los distintos escenarios.

TCR está a favor, cree que debe establecerse una whitelist.

POLICIA NACIONAL

Cualquier exclusión debe ir acompañada de medidas que aseguren que no se pueden utilizar maliciosamente los números beneficiados de la exclusión

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En términos generales se muestran a favor de crear listas blancas o listados de call centers en el extranjero a los que sí se les permitiría cursar llamadas.

AEECF

Considera conveniente tener un registro de Call Center en el extranjero.

AEERC/CEX

La elaboración de listas de exclusiones, aunque paliativa presenta problemas como la fijación de procedimientos y mecanismos que habrían de ser agiles y flexibles.

OCU, CECU, AUI

OCU cree que deben excluirse, previa solicitud, cuando esté justificado, los centros de atención al cliente situados fuera de España pero que operan en nombre de una empresa que presta servicios en España en cuyo caso el CLI debe ser nacional asociado a esa empresa y los usuarios en roaming.

CECU cree que no debe haber excepciones y que los centros de llamadas que prestan servicio en España deber tener una oficina en territorio español.

¿Considera necesario que la medida incluyese otros escenarios, por ejemplo, que el identificador de la llamada con origen internacional estuviese vacío o fuese no válido?

OPERADORES Y ASOCIACIONES DE OPERADORES

En general se muestran favorables a bloquear cualquier llamada que no tuviese una estructura válida (numeración no asignada, numeración del propio operador, campo número vacío, …), salvo MASMOVIL que es completamente contrario a la medida, y VODAFONE tiene un enfoque intermedio en el que se debería dejar como opcional y ser cada operador el que decida.

Varios operadores (DIGI y GAMMA) advierten sobre el coste de las herramientas de análisis, por lo que se debería analizar el impacto económico de su implantación.

TCR sugiere o bloquear completamente las llamadas flash o bien monetizar tipos de llamadas internacionales desde rangos que no son socios de roaming directos al operadorcobrando una tarifa especial.

SUMINISTRADORES

HIYA señala que sí, pero se tenga presente que los números no válidos y no asignados representan sólo el 0,1% de las llamadas fraudulentas.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En términos generales se muestran a favor de prohibir este tipo de tráfico.

RED6000 cree que un indicador de "no valido conforme a la normativa en vigor" podría tener efectos disuasorios.

AEECF

Aunque ya hay tecnología que permite identificar tráfico no legítimo hay obligación de mantener dicho tráfico

OCU, CECU, AUI

Si, estas llamadas también deben bloquearse.

Con la excepción de la numeración móvil que se aborda en la siguiente pregunta, - ¿existe alguna razón que aconseje una adaptación gradual de esta medida?

OPERADORES Y ASOCIACIONES DE OPERADORES

Salvo Telefónica, en general las asociaciones de operadores, así como los propios operadores son favorables a que las medidas se implanten de forma gradual y a través de grupos de trabajo.

SUMINISTRADORES

Quobis está a favor de la implantación gradual.

TCR cree que debe adoptarse gradualmente pues mejora la imagen de marca.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En términos generales se muestran a favor de implementar las medidas de manera inmediata con un mínimo periodo de aviso para crear listas blancas.

AEECF

No, debe adoptarse inmediatamente

AEERC/CEX

Consideran que la medida no debe adoptarse hasta que no exista una solución técnica adecuada y viable, que debería estudiarse en un grupo de trabajo técnico formado por personal del Ministerio, la CNMC, los operadores y el sector del call center.

OCU, CECU, AUI

OCU Y CECU creen que debe aplicarse inmediatamente. AUI cree que es aconsejable una aplicación gradual que permita crear listas blancas que deben ser validadas por el regulador.

- ¿existe alguna razón que desaconseje o impida que los operadores nacionales verifiquen que no se generan fuera de su red llamadas con una numeración que les ha sido asignada y bloqueen las llamadas que no superen esta verificación?

OPERADORES Y ASOCIACIONES DE OPERADORES

Masmóvil se muestra contrario a bloqu+ear si el número es del propio operador (pone como ejemplo desvíos de centralita PBX del cliente), y Vodafone apunta a la complejidad técnica de la medida por lo que no debe obligarse a los operadores sino ser algo opcional.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En términos generales consideran que no hay ninguna razón que desaconseje o impida la implementación de esta medida.

AEECF

No.

OCU, CECU, AUI

No

IMDEA

Señalan que su investigación acredita que solo el 5,14% de los números involucrados en fraude resultan ser válidos.

1b)

¿Qué medidas considera necesario adoptar, a nivel de cooperación entre operadores móviles, para identificar el tráfico generado por usuarios en roaming internacional, evitando que las llamadas, legítima y lícitamente originadas por estos usuarios, se vieran perjudicadas por la medida del punto 1a)?

OPERADORES Y ASOCIACIONES DE OPERADORES

En términos generales los operadores fijos consideran que si se implanta la medida debería ser sufragada por los operadores móviles, y estos últimos en términos generales son cautos por las implicaciones (coste, protección de datos, …), por lo que podría permitirse a bloquear cuando se tenga constancia que el usuario no está en roaming (ej. es del propio operador), pero no obligarse (DIGI, Vodafone). Por el contrario, MASMOVIL es abiertamente contrario a la medida.

Señalar la postura de Telefónica y DIGITALES que consideran que no es una medida necesaria a largo plazo, pues el VoLTE pone fin al *roaming* tal y como se conocía, y proponen que a corto plazo abrir los MSRN (Mobile Station Roaming Number).

SUMINISTRADORES

Ribbon indica que esta propuesta perderá eficacia a medida que se evolucione a VoLTE.

TCR recomienda el uso se listas blancas y negras, a las que pueda acceder todo el ecosistema.

OCU, CECU, AUI

OCU y CECU cree que basta con que se indique que la línea móvil llama desde el extranjero y que la posible cooperación entre operadores debe respetar la privacidad de los usuarios.

AUI considera necesario adoptar la firma digital especialmente para llamadas en roaming avisando al usuario en roaming de la necesidad de instalar una aplicación para ello. Si no se firma la llamada sería bloqueada.

POLICIA NACIONAL

Los operadores deben compartir información sobre la ubicación geográfica de las líneas móviles de sus clientes (dentro o fuera de España) para que la verificación sea válida.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

Se proponen distintas medidas: añadir marca "llamada en roaming", adoptar una base de datos común de clientes en roaming, establecer una obligación de validación a los operadores como la exigida por Traficom en Finlandia, crear un ente común o consorcio con la AP que defina un ecosistema común de intercambio de tráfico malicioso o adaptar el marco regulatorio para indicar los parámetros confidenciales que permiten cortar tráfico.

AEECF

Adaptar el marco regulatorio para indicar los parámetros confidenciales para cortar tráfico identificado como no legítimo.

IMDEA

Los proveedores de roaming y señalización deben abordar este tema.

¿existe alguna razón que desaconseje o impida que los operadores móviles nacionales verifiquen, cuando reciban una llamada de origen internacional identificada con una numeración móvil que les ha sido asignada, si el cliente al que corresponde esa numeración está en roaming y, cuando no sea así, bloqueen las llamadas?

OPERADORES Y ASOCIACIONES DE OPERADORES

DIGI señala el problema de las zonas fronterizas.

SUMINISTRADORES

Ribbon apunta al problema de si el defraudador usa un número que está en roaming.

TCR señala que en caso de roaming saliente debe realizarse una verificación de MSC en MSISDN.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En términos generales consideran que no hay ninguna razón que desaconseje o impida la implementación de esta medida, como demuestran las iniciativas de otros países europeos

AEECF

Podría valorarse una base de Datos de clientes en roaming como existe en otros países de EEE.

AEERC/CEX

Desaconseja adoptar esta medida hasta que existan soluciones técnicas adecuadas y flexibles, que deberían explorarse en un grupo de trabajo Ad hoc.

OCU, CECU, AUI

AUI señala que el acceso de consulta HLR cada vez está más restringido y bloqueado, por lo que sí puede haber problemas

IMDEA

Señalan que su investigación acredita que solo el 5,14% de los números involucrados en fraude resultan ser válidos lo que socava la eficiencia de bloquear números de teléfono no asignados

1c)

¿Qué opinión le merece la posible asignación de un rango de numeración específico para la realización e identificación de llamadas comerciales prospectivas y la consecuente prohibición de la utilización para este tipo de llamadas del resto de numeración del plan nacional?

OPERADORES Y ASOCIACIONES DE OPERADORES

No hay posición común, por una parte, se argumenta que se pondría en valor a las empresas de tele venta respetuosas con la normativa, y por otra, que el usuario no va a ser consciente de si le están llamando con un número del rango de televenta o no. En cualquier caso, se señala que sería una medida no para combatir el fraude sino para combatir las llamadas no deseadas.

Vodafone llama la atención sobre la irrelevancia de la medida si Google/Apple continúan marcando unilateralmente las llamadas como "posible SPAM telefónico".

SUMINISTRADORES

Mientras que Quobis considera que mejoraría la transparencia para el usuario final. HIYA y F24 consideran que no se ha probado una medida eficaz.

A TCR le parece adecuado, pero recuerda que las empresas deben registrarse y ser examinadas.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En términos generales valoran positivamente la propuesta, aunque se considera insuficiente por sí misma, por lo que se estima que debe adoptarse junto a las medidas de los apartados 1a y 1c.

AEECF

Se valora muy positivamente

ENDESA

Valoran de forma positiva la asignación de un rango de numeración específico para la realización e identificación de llamadas comerciales prospectiva y la consecuente prohibición de la utilización para este tipo de llamadas del resto de la numeración del Plan Nacional.

OCU, CECU, AUI

OCU y CECU la consideran una medida adecuada, INSISTIENDO cecu en la inspección y sanción

AUI cree que no podría evitarse que una persona con numeración fuera de ese rango realizara una llamada suplantando la identidad de una empresa, por lo que cree qye debe hacerse una validación de marca de la empresa firmando las llamadas con su certificado digital y una vez validada ña firma añadir el logo, solución ya implementada por TNS en otros países como EEUU.

¿En particular, considera adecuado evitar que el rango de numeración móvil sea empleado para identificar los terminales fijos de los centros de atención de llamadas por parte de las empresas de servicios de telemarketing y atención a clientes?

OPERADORES Y ASOCIACIONES DE OPERADORES

Salvo MASMOVIL que señala que se debería permitir, los operadores/asociaciones indican que ya está prohibido el uso de numeración móvil para telemarketing de acuerdo a la Resolución de la SETSI del 27 mayo 2013. En cuanto a atención a clientes, Vodafone indica que no se prohíba.

SUMINISTRADORES

Quobis considera que mejoraría la confianza.

TCR lo considera adecuado señalando que si ya existe un registro con rangos de numeración bastaría con identificar el caso de uso

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

Salvo ABANCA el resto valora positivamente la propuesta

AEECF

Se valora muy positivamente

AEERC/CEX

Rechazan ambas medidas por vulnerar la libertad de actividad empresarial, aumentar la carga regulatoria, dificultar la actividad económica, carecer de proporcionalidad y no resolver el problema.

ENDESA

Las plataformas de televenta deben utilizar la numeración asignada a la empresa en cuyo nombre contactan a los consumidores, previa autorización de esta empresa.

OCU, CECU, AUI

CECU cree que es una medida adecuada.

1d)

¿Facilitaría la persecución de algunas de estas estafas, que las plataformas de televenta vinieran obligadas a utilizar numeración asignada a la empresa en cuyo nombre contactan a los consumidores, previa autorización de esta empresa?

OPERADORES Y ASOCIACIONES DE OPERADORES

No hay posición común, desde Telefónica que señala que implicaría manipular el CLI y LleidaNET que indica que una empresa se anuncia con varias de telemarketing, hasta DIGI y Vodafone que indican que favorecería el control de la identidad del llamante.

SUMINISTRADORES

No evitaría el fraude, mejor certificar la llamada para que el usuario que recibe la misma reciba la identidad de la misma.

TCR cree que, si se implementa un registro, las estafas disminuirán considerablemente.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

Se muestran a favor. AEB considera que debe ampliarse a otro tipo de empresas como las que prestan servicios financieros.

AEECF

Se valora muy positivamente.

ENERGYA VM

Consideran adecuado que las actuaciones de telemarketing tengan una numeración específica, pero no que que la identificación de tales llamadas se asocie con las empresas en cuyo nombre contactan.

OCU, CECU, AUI

Consideran que es una medida apropiada. AUI considera que en todo caso la llamada debe firmarse con un certificado digital emitido por la empresa origen para cada teleoperador.

¿Considera que hay otras alternativas que, por ejemplo, puedan facilitar y mejorar el control de la subasignación de numeración y/o la aparición de empresas/operadores que ofrecen plataformas con el objetivo de manipular el CLI?

OPERADORES Y ASOCIACIONES DE OPERADORES

- GAMMA controlar la subasignación de numeración para que no se use fuera de España.
- MASMOVIL controlar y limitar la subasignación de numeración.
- Telefónica solicita medidas contra empresas que manipulen CLI.
- VODAFONE que la CNMC realice un mayor control de las subasignaciones a los revendedores del servicio telefónico.

SUMINISTRADORES

TCR cree que la manipulación de CLI podría ser autorizada si previamente se realiza la inscripción a través del registro (lista blanca).

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

ABANCA propone el control de mecanismos como el Call diversión. AEB proponen establecer medidas adicionales de verificación de plataformas y AEB y CECA proponen la creación de servicios de reporte y consulta por la ciudadanía y traslado al operador.

AEERC/CEX

Rechazan ambas medidas por vulnerar la libertad de actividad empresarial, aumentar la carga regulatoria, dificultar la actividad económica, carecer de proporcionalidad y no resolver el problema.

OCU, CECU, AUI

OCU propone que el CIF de la empresa vinculado a la numeración sea un dato de acceso público, crear un registro público de empresas de telemarketing, obligar a las empresas a tener un control y sobre sus canales de televenta, supervisando los números que utilizan y las prácticas que realizan, fijar la responsabilidad solidaria de la empresa titular del bien o servicio y de la empresa de telemarketing, mejorar el control por las AP´s y prohibir la contratación en la llamada comercial.

1e)

¿Qué opina del establecimiento de una lista DNO (Do Not Originate) que prohibiera el uso de las numeraciones en la lista DNO como identificador de llamadas? Por ejemplo, ciertos bancos proporcionan números para que los consumidores se comuniquen con ellos, pero nunca se comunican con un consumidor utilizando el mismo número. En consecuencia, cualquier llamada que utilizara estos números como CLI identificador de la llamada sería irregular (puesto que el CLI habría sido modificado) y con alta probabilidad, fraudulenta. Las llamadas que, a pesar de la prohibición, se generaran desde estas numeraciones podrían ser bloqueadas o anonimizadas (como "número desconocido"). ¿Qué ventajas o desventajas ve a estas alternativas?

OPERADORES Y ASOCIACIONES DE OPERADORES

En general hay tres posturas:

- Viable y de fácil implantación [ASTEL, COLT].
- Mejor establecer un rango específico para números que no originen llamadas (podría usarse además por cualquier sector) [TELEFÓNICA, MASMOVIL]
- Complejidad en la elaboración de las listas (actualización) que podría afectar a llamadas legítimas [DIGI, GAMMA]

En cuanto al bloqueo, Orange no es partidario de bloquear sino de anonimizar.

SOMOS INC (GESTOR DE LA NUMERACIÓN TIPO 800/900 en EEUU)

- Gestiona una lista DNO (inválidos, no asignados, no usados, y no originadores de llamadas) con muy buenos resultados.
- En la lista también se indica si el número es o no para llamadas de voz/SMS, y si llamadas sólo nacionales/internacionales.

SUMINISTRADORES

F24 considera que no se aborda el verdadero problema del fraude de las CLI, si bien considera que puede ser una contramedida eficaz mientras tanto para evitar estafas financieras. En cualquier caso, debería ser un registro central controlado por los operadores.

TCR cree que podría incluirse una casilla de verificación (no devolver la llamada) en el registro. Al compartir la lista negra esto se puede usar para bloquear proactivamente el uso de estos números o deshabilitarlos. Asimismo, señala que la anonimización no evitaría el fraude.

POLICIA NACIONAL

Parece una buena medida ya que los estafadores suelen usar para alterar el CLI números disponibles en fuentes abiertas, como los números de atención al cliente. Si se obliga a que estos números sean de un solo sentido se evitarían llamadas que suplantan a entidades bancarias.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

Salvo Abanca, todos se muestran favorables al establecimiento de estas listas, aunque en general prefieren el bloqueo a la anonimización

AEECF

Valora muy positivamente la medida siempre que la lista no sea accesible al público. Cree que es mejor bloqueo

AEERC/CEX

Rechazan la medida por vulnerar la libertad de actividad empresarial, aumentar la carga regulatoria, dificultar la actividad económica, carecer de proporcionalidad y no resolver el problema.

ENDESA

Esta medida podría tener un impacto en la reducción de llamadas fraudulentas, pero debe valorarse con cautela debido a su difícil implantación y puesta en practica

OCU, CECU, AUI

Les parece una medida adecuada. AUI considera que las llamadas deben bloquearse no anonimizarse.

IMDEA

Señalan que su investigación acredita que solo el 5,14% de los números involucrados en fraude resultan ser válidos.

1f)

¿Considera que esta lista DNO debería estar a disposición de cualquier entidad o debería limitarse a la numeración asignada a entidades públicas y entidades financieras en razón de su especial sensibilidad y/o riesgo de ser utilizados para fraudes de mayor impacto económico?

OPERADORES Y ASOCIACIONES DE OPERADORES

No hay un apoyo común a la medida, por lo que no hay una postura clara a este respecto. Si bien se podría decir que en términos generales se considera mejor centrarse en los sectores de riesgo para abrirla posteriormente al resto de sectores.

SUMINISTRADORES

HIYA, TCR y SOMOS INC consideran que debe estar actualizada y accesible a cualquier entidad.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En general se muestran a favor de extender la medida a otros sectores

AEECF

La lista tiene que ser accesible a cualquier operador, pues si no el fraude podría mutar a otros sectores.

AEERC/CEX

Rechazan la medida por vulnerar la libertad de actividad empresarial, aumentar la carga regulatoria, dificultar la actividad económica, carecer de proporcionalidad y no resolver el problema.

ENDESA

Esta medida debe analizarse con cautela, pero si se pusiera en marcha la lista debería estar a disposición de cualquier entidad.

OCU, CECU, AUI

Consideran que debe estar a disposición de cualquier entidad, pero AUI señala que el problema es que los defraudadores acabarían accediendo a la lista.

1g)

¿Qué opina del establecimiento de una lista de "numeraciones sin uso" que prohibiera el uso de las numeraciones en dicha lista como identificador de llamadas? Se trataría de rangos de numeración o numeraciones que no hubiesen sido asignados y, en consecuencia, cualquier llamada que utilizara estos números como CLI identificador de la llamada sería irregular (puesto que el CLI habría sido modificado) y con alta probabilidad, fraudulenta. Las llamadas que, a pesar de la prohibición, se generaran desde estas numeraciones podrían ser bloqueadas o anonimizadas (como "número desconocido"). ¿Qué ventajas o desventajas ve a estas alternativas?

OPERADORES Y ASOCIACIONES DE OPERADORES

En general se muestran favorables a bloquear cualquier llamada que no tuviese una estructura válida (numeración no asignada, numeración del propio operador, campo número vacío, …), salvo MASMOVIL que es completamente contrario a la medida, y VODAFONE que la encuentra desproporcionada por el coste que supondría. Otros operadores (DIGI, GAMMA) también advierten sobre el coste de las herramientas de análisis, por lo que se debería analizar el impacto económico de su implantación.

SUMINISTRADORES

F24 e HIYA consideran que podría reducir el fraude, pero este último apunta que se trata sólo del 0,1% de las llamadas fraudulentas.

TCR señala que con el registro habría un historial del número. Los números no registrados serían bloqueados.

POLICIA NACIONAL

Es evidente que estas llamadas son fraudulentas, pero la medida exige que los operadores compartan información sobre números no asignados.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En general, se muestran a favor de esta medida, prefiriendo el bloqueo a la anonimización

AEECF

Se valora positivamente prefiriendo el bloqueo

AEERC/CEX

Rechazan la medida por carecer de proporcionalidad y no resolver el problema.

ENDESA

Esta medida debe analizarse con cautela, pero si se pusiera en marcha la lista debería estar a disposición de cualquier entidad

OCU, CECU, AUI

Les parece una medida adecuada siempre que se bloquee. AUI recuerda la importancia de la rápida actualización, ya que estas numeraciones pueden ir asignándose y dice optar en cualquier caso por la firma digital de las llamadas.

IMDEA

Consideran que el bloqueo puede ser una medida adecuada, ya que los delincuentes usan en gran medida números no asignados.

2. Posibles medidas en el ámbito de la numeración y códigos alfanuméricos identificativos de mensajes (SMS2, MMS o RCS)

2a)

¿Qué consideración le merece la posible medida regulatoria que obligara a los operadores de mensajería y de reenvío y almacenamiento de comunicaciones interpersonales basados en numeración a bloquear los mensajes con origen internacional identificados por un CLI del plan nacional de numeración? Especifique si la extensión de la medida propuesta en el punto 1a) a los mensajes con origen internacional planteara cuestiones técnicas, comerciales o de otra índole diferentes de las que haya señalado en su respuesta a los diferentes apartados del punto 1a).

OPERADORES Y ASOCIACIONES DE OPERADORES

Las posturas van desde los abiertamente a favor, como Telefónica / DIGITALES (sólo se curse tráfico A2P nacional, y se proceda al bloqueo SMS internacional y CLI español si centro emisor no es del operador asignatario del CLI), pasando por posturas cautas como Orange y ALYSIS (se debe analizar pues es probable que empresas extranjeras envíen mensajes desde el extranjero), a ser contrario a la medida pues podría suponer el bloqueo de tráfico genuino de comerciantes hacia clientes extranjeros que ahora residen/utilizan un móvil español así como de tráficos genuinos generados fuera del territorio español con destino a clientes españoles (DIGI, LLEIDANET, MEF). Esta última postura es compartida por Vodafone, pero en este caso por la necesidad del desarrollo de una solución compleja y difícil de implementar, por lo que, al igual que con las llamadas, Vodafone pide que se habilite a los operadores a bloquear los SMS cuando se tenga constancia de que no se trata de un número en roaming.

SUMINISTRADORES

SINCH no aconseja este tipo de bloqueo en los canales habituales del A2P. Los agregadores de A2P han de conectarse de manera directa los servidores de los operadores móviles. Es necesario mantener la posibilidad de entregar SMS con senders de numeración nacional por estas vías dado que multitud de servicios ofrecidos a usuarios con numeración móvil nacional son gestionados por empresas internacionales (ej. Salesforce, Google, Microsoft, Banca internacional, etc). Además, hay empresas nacionales que soportan sus servicios sobre proveedores internacionales. Otro escenario diferente, en el que, si estan de acuerdo en dicho bloqueo, sería en el que el SMS alcanzara las redes móviles por las rutas de roaming internacional. En tal caso si se pondría coto a una fuente importante de fraude.

Por su parte, F24 es contrario pues obligaría a empresas internacionales como F24 a conseguir infraestructuras en España.

TCR recomienda proporcionar una solución que evite tener que tomar una decisión regulatoria como esa. El tráfico se registra como A2P (de aplicación a persona) o P2P (de persona a persona. El primero debe pasar por un registro donde se le aplican las normas definidas por el regulador. TCR les asocia un SenderID y registra sus campañas de SMS/MMS, a las que asigna un CampaignID. El código identificativo de marca único (BrandID) y el CampaignID. El firewall diferencia el tráfico registrado y el no registrado, siendo este último sometido a mayor control o bloqueado. La solución TCR no plantea problemas pero se requiere una integración técnica entre operadores

POLICIA NACIONAL

Todas las medidas propuestas para llamadas de voz en líneas generales son igualmente válidas para mensajes SMS.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En general se muestran a favor, con excepciones previamente comunicadas y para usuarios en roaming y teniendo en cuenta que para la emisión de sus SMS las empresas suelen usar servicios de terceros con diferentes orígenes o proveedores de agregación de mensajería.

AEECF

Se valora positivamente.

AEERC/CEX

Consideran que la medida no debe adoptarse hasta que no exista una solución técnica adecuada y viable, que debería estudiarse en un grupo de trabajo técnico formado por personal del Ministerio, la CNMC, los operadores y el sector del call center.

ENDESA

Esta medida debe analizarse con cautela, pero si se pusiera en marcha la lista debería puede suponer un perjuicio más que una mejora.

OCU, CECU, AUI

OCU Y CECU consideran que es una medida adecuada. AUI señala que el problema es que muchos agregadores de SMS son internacionales y transitan tráfico nacional, por lo que la medida afectaría a tráfico lícito.

2b)

¿Qué medidas considera necesario adoptar, a nivel de cooperación entre operadores móviles, para identificar el tráfico generado por usuarios en roaming internacional, evitando que los mensajes de texto, legítima y lícitamente enviados por estos usuarios, se vieran perjudicados por la medida del punto 2a)? Especifique si la extensión de la medida propuesta en el punto 1b) a los mensajes con origen internacional planteara cuestiones técnicas, comerciales o de otra índole diferentes de las que haya señalado en su respuesta a los diferentes apartados del punto 1b.

OPERADORES Y ASOCIACIONES DE OPERADORES

El principal aspecto es el de las rutas internacionales que sigan los SMS así como el problema para las multinacionales que emplean proveedores internacionales para sus campañas a través de SMS.

SUMINISTRADORES

TCR cree que el escenario ideal sería separar A2P de P2P, un registro como el TCR registra el quién y el qué, y por tanto también visibilidad sobre el origen de la comunicación.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

AEB señala que debe requerirse un identificador que el operador coteje y Abanca y CECA proponen incluir una marca de "SMS MMS RCS en roaming" o similar.

AEECF

Propone que haya un marco regulatorio con parámetros confidenciales

AEERC/CEX

Consideran que la medida no debe adoptarse hasta que no exista una solución técnica adecuada y viable, que debería estudiarse en un grupo de trabajo técnico formado por personal del Ministerio, la CNMC, los operadores y el sector del call center.

OCU, CECU, AUI

OCU considera que el problema es meno pues los usuarios en roaming casi no envían SMS ya que usan aplicaciones compo Whatsapp. AUI insiste en la firma digital de estos mensajes.

2d)

¿Qué beneficios asocia a la creación de una base de datos nacional única con lista exhaustiva de nombres y abreviaturas alfanuméricas a utilizar para identificar a las entidades emisoras de los mensajes?

OPERADORES Y ASOCIACIONES DE OPERADORES

Mientras que los operadores móviles con red (MASMOVIL, Orange, Telefónica y Vodafone) y DIGITALES son partidarios de la medida, si bien debería constituirse un grupo de trabajo para su análisis en detalle. DIGI, LLEIDANET y MEF no la consideran apropiada dada sus dificultades (disponibilidad limitada de identificadores, limitaciones de la prevención de fraude, complejidad técnica).

SUMINISTRADORES

SINCH considera que es un valor añadido, pero tiene una serie de inconvenientes (necesidad de analizar el remitente del mensaje, pérdida del secreto comercial, incremento de procesos de gestión, …). El tráfico no registrado se trasladaría de manera masiva a canales no autorizados como las rutas grises o las granjas de SIM. En este sentido se manifiesta Quobis. Sin embargo F24 no es partidario de la medida.

TCR cree que tener una base de datos nacional única con una lista exhaustiva de nombres y abreviaturas alfanuméricas (Alphanumeric senderID) es una medida beneficiosa siempre que haya una tecnología fiable y participen todos los agregadores y operadores de red. El registro TCR puede actuar como base de datos nacional Unica.

POLICIA NACIONAL

Si se emplea algún mecanismo robusto de identificación que asegure que la entidad que utiliza un alfanumérico de la base de datos está legitimada para ello, se evitaría el uso malicioso de alfanuméricos para suplantar a entidades legítimas y se facilitaría a los operadores el bloqueo, por tanto, se considera una medida efectiva.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

La consideran una medida adecuada. AEB propone añadir algún distintivo como oficial o verificado. RED6000 propone valorar la posibilidad de crear un Código único y privado para cada entidad emisora de SMS. Cuando el operador reciba la petición de envío de SMS deberá enviar un código hash dinámico (SHA256) a la entidad emisora, la cual deberá tomarlo y añadirle su código único y privado. Si la operadora obtiene el mismo resultado el SMS se enviará, en caso contrario se bloqueará. De este modo no es necesario entrar al contenido del mensaje.

AEECF

Se valora positivamente

AEERC/CEX

Rechazan la medida por vulnerar la libertad de actividad empresarial, aumentar la carga regulatoria, dificultar la actividad económica, carecer de proporcionalidad y no resolver el problema.

ENDESA

Comparten la visión de que se establezca dicha lista de empresas que ofrezcan y contraten números de teléfono con identificación de cada una de ellas. En el caso de que se contraten por terceros (para evitar aparecer), deben crearse mecanismos para la identificación obligatoria tanto del contratante directo como del que realiza el encargo, estableciendo un régimen de infracciones y sanciones.

OCU, CECU, AUI

CECU cree que la medida podría ayudar. OCU cree necesario identificar de algún modo a quien envía un SMS. AUI señala que la medida reduce las posibilidades de remitentes a utilizar por los defraudadores, pero que estos remitentes de la base de datos también podrían ser utilizados por los defraudadores.

2e)

¿Considera que esta base de datos debería cubrir los nombres y alfanuméricos utilizados por cualquier entidad o debería limitarse a los nombres y alfanuméricos de entidades públicas y entidades financieras en razón de su especial sensibilidad y/o riesgo de ser utilizados para fraudes de mayor impacto económico?

OPERADORES Y ASOCIACIONES DE OPERADORES

La clave más que restringirlo a determinados sectores es que se asigne a una empresa que posee el derecho o la marca para usar ese alfanumérico. Vodafone propone un protocolo de actuación similar al actual de asignación del dominio ".es" para inscribirse en la base de datos.

SUMINISTRADORES

SINCH considera que debería restringirse a sectores altamente sensibles al Smishing (banca, entrega paquetería, entidades públicas sensibles, empresas de recobros y todo lo relacionado con las OTP). Para Quobis también podría ser suficiente con que se incluyan organizaciones de determinados sectores.

TCR cree que debe aplicar a todas las marcas y comerciantes del país.

POLICIA NACIONAL

Debería aplicarse a cualquier entidad.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

Proponen abrir la medida a otros sectores

AEECF

Considera que la lista debe ser accesible a cualquier operador para que el fraude no mute hacia otros sectores.

OCU, CECU, AUI

Considera que debe cubrir el máximo de entidades, pero AUI insiste en que esta lista no mitiga el fraude.

2f)

¿Cuál sería el mecanismo adecuado para controlar y verificar el origen de los mensajes que utilizaran un alfanumérico registrado en la citada base de datos nacional como identificador de origen? ¿Sería necesario algún mecanismo de certificación cualificado para los emisores de estos mensajes?

OPERADORES Y ASOCIACIONES DE OPERADORES

En términos generales los operadores no son partidarios de la imposición de mecanismos de certificación por el coste y el plazo de su implantación, salvo que el operador haya desarrollado he implantado una solución, caso de LLEIDANET, en cuyo caso considera que es la única forma de evitar el fraude.

SUMINISTRADORES

TCR cree que es necesario un mecanismo de certificación y verificación como TCR.

POLICIA NACIONAL

La eficacia del control de los alfanuméricos va ligada a la fiabilidad del mecanismo de validación, todo se basa en que no haya dudas sobre que quien utiliza un alfanumérico para identificarse en un SMS está realmente legitimado para usarlo.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

Dejan el mecanismo de certificación en manos del operador señalando algunos que las certificaciones deben poder ser revocadas.

ENERGYA VM

Consideran adecuado que exista una numeración concreta que identifique actuaciones comerciales, pero no que dicha numeración de identifique con las empresas en cuyo nombre se contacta.

OCU, CECU, AUI

AUI insiste en que el mecanismo adecuado es el certificado digital con atributos, que sería validado por el operador.

2g)

¿Sería necesario acompañar esta medida de la prohibición de envío de mensajes haciendo uso de los nombres y alfanuméricos registrados en la base de datos sin la previa verificación del origen?

OPERADORES Y ASOCIACIONES DE OPERADORES

Los que apoyan la medida en términos generales sí, pero MASMOVIL considera que los clientes nacionales habilitados para enviar alfanuméricos podrían enviar remitentes dentro y fuera de la lista. Sin embargo, los generadores de mensajes internacionales sólo podrán enviar mensajes si el remitente no está registrado en la lista.

SUMINISTRADORES

TCR recomienda que se utilice el mismo registro de marca para esos códigos alfanuméricos asociando al proveedor de servicios con la marca. La campaña solo puede ponerse en marcha cuando el registro y la verificación sean exitosos

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

Sí

AEECF

Sí

OCU, CECU, AUI

CECU cree que sí. AUI considera que sin previa verificación del origen la prohibición no sería efectiva

2h)

¿Considera que la llevanza del registro citado en el punto 2d) debe realizarse por un organismo público, un organismo privado o vía cooperación entre los diferentes agentes en la cadena de transmisión de los mensajes?

OPERADORES Y ASOCIACIONES DE OPERADORES

Los que apoyan la medida en términos generales que la gestione la AAPP (Ministerio o CNMC).

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

La mayoría opta por un organismo público. AEB propone usar el Registro ya existente promovido por el sector financiero.

SUMINISTRADORES

TCR considera que debe atribuirse a una entidad completamente independiente como TCR.

AEECF

Sí, un organismo público dependiente del Ministerio.

OCU, CECU, AUI

Creen que la llevanza debe corresponder a un organismo público. OCU cree que además debe tener carácter público. CECU cree que si participan las empresas también deben participar los consumidores. AUI considera que puede haber cooperación entre varios agentes incluso utilizando blockchain, pero siempre vinculado a la previa identificación del origen mediante certificado digital.

2i)

¿Qué consideración le merece la prohibición de los mensajes no numéricos con origen internacional?

OPERADORES Y ASOCIACIONES DE OPERADORES

Las posturas van desde la abiertamente a favor de Telefónica y Vodafone, al considerar que es imprescindible, a la abiertamente en contra de DIGI que argumenta que no es posible la medida en el seno de la UE.

SUMINISTRADORES

TCR señala que podría asignar numeración nacional a clientes registrados cuando se necesitase.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En general, les merece una opinión favorable.

AEECF

Se valora positivamente

AEERC/CEX

Rechazan la medida por vulnerar la libertad de actividad empresarial, aumentar la carga regulatoria, dificultar la actividad económica, carecer de proporcionalidad y no resolver el problema.

OCU, CECU, AUI

CECU la considera una medida adecuada. OCU y AUI creen que le la prohibición por defecto podría impedir el envío de mensajes lícitos.

3. Posibles medidas para evitar que progresen las comunicaciones con manipulación de CLI.

3a)

¿Conoce de la existencia de alguna solución técnica suficientemente madura para ser adoptada regulatoriamente a nivel nacional? En caso afirmativo, aporte información detallada.

OPERADORES Y ASOCIACIONES DE OPERADORES

Las posturas van desde la idoneidad de las medidas de certificación, ya sean propietarias (LLEIDANET) o variantes del STIR/SHAKEN (MASMOVIL, ORANGE), a la valoración muy desfavorable de dichas medidas por el coste y tiempo que supondrían

su implantación, además de no ser necesarias en el escenario de red móvil VoLTE (ASTEL, DIGITALES, COLT, DIGI, TELEFÓNICA), pasando por el escepticismo de Vodafone al considerar que sería muy complicado dada la necesidad de su implantación por todos los operadores de forma coordinada.

SUMINISTRADORES

Hay unanimidad en cuanto a considerar que las soluciones de certificación son las idóneas para atajar el fraude.

AB HANDSHAKE CORPORATION, empresa americana con sede en Valencia, que comercializa tecnología para prevenir la suplantación de CLI a nivel nacional. Garantizan la validez del CLI de cualquier llamada entre los operadores en un país determinado, mediante un proceso consistente en crear una base de datos que valida la llamada y toma una decisión para permitirla o rechazarla, para lo que consulta la base de datos de MNP (Moblile number portability), si es necesario. La Decisión final se envía a los equipos de conmutación de los MNO que rechazan o continúan la sesión de llamada/aplican cualquier etiquetado de llamada necesario. Señalan que el mismo procedimiento se puede implementar para el tráfico de SMS.

NUMERACLE, empresa americana que promueve el objetivo de comunicaciones identificadas verificadas de extremo a extremo (KYC know your client). Consideran que el estándar RCD (Rich Call Data) que adjunta información de identidad como el nombre del llamante, el motivo de la llamada y un logotipo solo son confiables si han sido adjuntados a la llamada por parte de una entidad conocida y confiable. Solo en ese caso deberían los operadores de destino mostrar la información de los RCD. Asimismo, Numeracle advierte contra los motores de análisis (AE) que identifican llamadas ilegales y no deseadas a través de análisis de big data, ya que sus algoritmos basados en picos de tráfico impiden muchas veces que se cursen llamadas legales cuando cada vez más las personas que llaman ilegalmente distribuyen su tráfico entre muchos números y varios proveedores.

ASSECO GROUP, empresa que cotiza en la bolsa de valores de Varsovia con sede en Madrid, cuenta con un protector contra suplantación de identidad llamado Spoofing Protector, que garantiza una defensa en tiempo real contra llamadas y SMS falsos, mediante un backend para llamadas y una firma segura para SMS.

TCR señala que la mayoría de los actores que operan actualmente en España y están verificados y forman parte de su Registro en EEUU

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

La mayoría se refieren a STIR/SHAKEN y a la experiencia de Traficom (Finlandia) obligando a los operadores a controlar que se impide cambiar el número de la persona que llama para imitar un número finlandes. CECA se refiere también a la experiencia de OFCOM (UK).

AEB se refiere al uso de servicios de comunicación enriquecida (RCS)

AEECF

Existen diferentes iniciativas técnicas y operativas para impedir la manipulación del CLI, se trata de variantes del STIR/SHAKEN que comparten información entre el operador originante y el receptor de la llamada a través de una entidad verificadora.

AEERC/CEX

No

OCU, CECU, AUI

OCU y CECU no conocen. AUI se refiere a STIR SHAKEN

3b)

¿Existiría, en su opinión, la necesidad de crear un grupo de trabajo nacional específico para el desarrollo de esta solución y la necesaria coordinación internacional?

OPERADORES y ASOCIACIONES DE OPERADORES

Sí sería imprescindible el grupo de trabajo y la cooperación internacional.

SUMINISTRADORES

Sí, y la cooperación internacional.

AB HANDSHAKE propone la creación de un grupo de trabajo que incluya al personal relevante de los operadores nacionales para encontrar los parámetros de implementación óptimos.

NUMERACLE considera que debe crearse un grupo entre los operadores y partes interesadas para permitir la transmisión de información segura y verificada.

TCR cree que el proyecto necesita una estrecha cooperación y coordinación entre los participantes del ecosistema, que podría ser proporcionada por TCR, quien a su vez trabajaría con el regulador.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

Todos consideran que sí, refiriéndose también algunos a la necesidad de cooperar a nivel internacional.

AEB propone que el grupo se ampare en el Plan de Acción Financiera contra el Fraude (PAFF)

AEECF

Sí. Existen técnicas de IA de tratamiento de mensajes que generan un hash y permiten identificar el envío de SMS masivos potencialmente fraudulentos para un tratamiento posterior.

AEERC/CEX

Consideran adecuado crear un grupo de trabajo técnico formado por personal del Ministerio, la CNMC, los operadores y el sector del call center.

OCU, CECU, AUI

Sí

4. Posibles medidas de detección, a través de equipamiento y/o software en la operativa de red, de este tipo de estafas y consecuente bloqueo de comunicaciones electrónicas afectadas.

4a)

¿Considera que la adopción de medidas como la técnica de hash expuesta requiere de una modificación normativa para su implementación en España?

OPERADORES Y ASOCIACIONES DE OPERADORES

La postura general es la necesidad de dotar soporte jurídico al filtro de SMS (MASMOVIL indica la necesidad de Ley Orgánica) para el acceso al contenido de forma automatizada, salvo LLEIDANET que es más partidario de firmar el SMS evitando así entrar al contenido del mismo.

SUMINISTRADORES

Sí se precisaría de modificación normativa al vulnerar el secreto de las comunicaciones.

TCR cree que debe permitirse que los operadores de red móvil cuenten con un Registro que puedan imponer o implementar para las comunicaciones de mensajería. TCR no realiza hash, pero comprueba la autenticidad del mensaje por la vinculación de la entidad con las campañas registradas.

ASEE proporciona una técnica de hash para la detección de SMS falsos basándose en la firma segura proporcionada en cada mensaje. Si no tiene firma segura y se envía desde una entidad válida se trata como un mensaje falso.

POLICIA NACIONAL

Con independencia de si es necesario un cambio normativo o no, creen que la utilización de firmas digitales (hash) para identificar sms que responden a un patrón que se asocia al fraude es altamente efectiva y evita la propagación de la estafa. Pero tiene que ser una medida

dinámica que tenga en cuenta que con un mínimo cambio en el mensaje da lugar a un hash 2 que escapa al filtro aplicado al hash 1.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En términos generales consideran que debe adoptarse normativa que contemple y regule esta posibilidad, contemplando salvaguardas que protejan la privacidad.

AEB considera que estas medidas podrían ampararse en una Ley Orgánica y en la protección de la seguridad nacional constituyendo una medida necesaria en una sociedad democrática.

ABANCA alude al artículo 51.1 de la CE relativo a la defensa de los intereses de los consumidores y entiende que conforme al artículo 6.3 del RGPD debe usarse la la base jurídica del artículo 6.1.c y 6.1.e) del RGPD (tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento y tratamiento necesario para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al responsable) para obligar a los operadores por Ley a aplicar filtros y bloquear mensajes.

AEECF

Sí

ENDESA

ENDESA ya utiliza filtros para los procesos de contratación a través de mensajes cortos, por tanto, en caso de que se regulen estos filtros se deben tener en cuenta esos procesos y no perjudicarlos.

OCU, CECU, AUI

Sí

4b)

En caso afirmativo, ¿qué consideración le merece la posibilidad de excepcionar del secreto de las comunicaciones las situaciones de las estafas originadas por mensaje corto de texto, permitiendo a los operadores la aplicación de filtros y el bloqueo de los mensajes que, de acuerdo con la aplicación de determinados algoritmos, se identificaran como fraudulentos? ¿Considera necesaria la intervención pública en el diseño de los algoritmos a utilizar? Indique, en su caso, alternativas.

OPERADORES Y ASOCIACIONES DE OPERADORES

Se apunta a la dificultad de diseñar un algoritmo común (variabilidad de sistemas operadores y soluciones terceros), si bien podría solventarse a través de una supervisión de la AAPP en cuanto a los filtros que se podrían utilizar.

SUMINISTRADORES

F24 considera que la privacidad es más importante que luchar contra los spammers.

AB Handshake, en cuanto a las estafas originadas por mensajes cortos de texto considera que el operador debería tener acceso a todos los parámetros del mensaje, pudiendo realizar un análisis exhaustivo en tiempo real. El análisis en sí puede ser totalmente automatizado y realizado sin supervisión o intervención humana, pero es fundamental que estas herramientas de detección automatizada que utilizan tecnología de IA/ML tengan la capacidad de trabajar con el conjunto completo de datos, incluido el origen del mensaje, el texto y cualquier enlace contenido en él.

ASSECO GROUP señala que spoofing Protector consta de un SDK y un servicio de backend que se encarga de la verificación y filtrado de mensajes falsificados. La firma segura es el número MAC. Todos los mensajes que contengan una firma segura generada por nuestra solución se consideran válidos. No hace falta intervención pública, los algoritmos y mecanismos de seguridad son diseñados y desarrollados por la empresa ASEE.

TCR cree que si se necesita alguna regulación debe ser simple. Los mensajes son leídos por maquinas por lo que se preserva la intimidad. Con TCR no hay necesidad de intervención pública

POLICIA NACIONAL

Los mensajes que se utilizan en campañas de smishing no suelen incorporar datos personales, por tanto, si una aplicación IA previamente ha detectado como probablemente fraudulento un sms, el examen manual del mismo, probablemente. no supondrá una invasión grave del secreto de las comunicaciones pues no habrá datos personales.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

Todos consideran que debe permitirse la aplicación de filtros y bloqueos.

AEB propone que los filtros y bloqueos sean automatizados y se limiten a comprobar la inclusión de enlaces respecto a los que existan indicios vehementes de fraude. A su juicio debe articularse como una obligación para los operadores de telecomunicaciones y las empresas de mensajería y reenvio. AEB considera que deben comunicarse o autorizarse previamente los criterios y condiciones de aplicación de filtros de acuerdo a algoritmos predecibles sujetos a auditoría y control.

AEECF

Valora muy positivamente la medida como la más efectiva. Señala que esta medida ya está implantada en Belgica, UK y Alemania y entiende que la intervención pública debe limitarse a al marco regulatorio y al disño de parámetros.

ENDESA

La función pública debería fijar criterios regulatorios sin intervenir en el diseño de los algoritmos necesariamente.

OCU, CECU, AUI

OCU se opone a excepcionar el secreto. CECU cree que puede excepcionarse, ya que los particulares usan otras aplicaciones como Whatsapp pero creen que la intervención pública es imprescindible. AUI cree que debe excepcionarse el secreto y que la intervención pública debe limitarse a regular patrones básicos ya que el diseño de algoritmos no puede ser común.

4c)

¿Considera necesario o conveniente adoptar algún tipo de salvaguardas para que la excepción no interfiera con la protección de la privacidad y datos personales (p.ej. acceso automatizado, generación de identificadores de mensajes para el análisis del tráfico que, una vez generados no permita adquirir conocimiento del contenido, etc.)? Especifique, en su caso, qué salvaguardas, identificando – cuando sea posible- su coste, impacto y viabilidad.

OPERADORES Y ASOCIACIONES DE OPERADORES

Las salvaguardas vendrían dadas por la automatización del proceso, la anonimización o agrupación de los SMS a analizar, y por la aplicación de un hash.

SUMINISTRADORES

Asseco Group cree que solución no interfiere con la privacidad de los datos personales, ya que la seguridad radica en un a firma segura para SMS y un backend para llamadas que detecta si la llamada se origina en el Call center del cliente,

TCR cree que, en todo caso, podrían excluirse las comunicaciones P2P. Los mensajes son leídos por maquinas por lo que se preserva la intimidad.

POLICIA NACIONAL

Los mensajes que se utilizan en campañas de smishing no suelen incorporar datos personales, por tanto, si una aplicación IA previamente ha detectado como probablemente fraudulento un sms, el examen manual del mismo. Probablemente. no supondrá una invasión grave del secreto de las comunicaciones pues no habrá datos personales.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

Todos consideran que deberían adoptarse salvaguardas

AEB considera que debe tratarse de mecanismos totalmente automatizados que impidan que se viole el carácter reservado de las comunicaciones y que debe existir intervención pública o de un consorcio plural para garantizar el correcto diseño y aplicación de los algoritmos y su adaptación a los cambios en el comportamiento de los delincuentes.

AEECF

AEECF recuerda que se tiene que tratar de un software sin intervención humana

OCU, CECU, AUI

AUI señala que la opción de firmar la llamada o SMS evita tener que entrar en el contenido. Para el emisor implica un coste, pero el operador se limita a realizar una consulta para ver si existe un token como ya ocurre con las consultas de portabilidad. Adicionalmente se refiere a la integración de una plataforma analítica de comportamientos inusuales de llamadas en los sistemas de los operadores, como la ofrecida por TNS (Call Guardian).

5. Posibles medidas de retirada y bloqueo de páginas web

5a)

Para los casos en los que, al consumidor, vía SMS o e-mail, se le solicita el acceso a una página web que, al acceder, recaba sus datos y claves personales, ¿resultan eficaces, para combatir las estafas identificadas, los procedimientos y mecanismos actuales de retirada por propietarios y operadores de servicios de hosting; y de bloqueo de páginas web por prestadores de servicios de acceso a internet?

OPERADORES Y ASOCIACIONES DE OPERADORES

En términos generales se considera una medida de eficacia muy limitada, entre otras, por la posibilidad de reproducción en otras páginas, el empleo de acortadores, y que requeriría de recursos por parte de los operadores.

SUMINISTRADORES

En términos generales no se considera una medida eficaz.

Asseco Group dice que Spoofing Protector informa al usuario que está a punto de recibir SMS falsos. Además, podemos mover este mensaje a la carpeta basura.

TCR recomienda legitimar la comunicación de principio a fin con TCR, lo que evitara la mayoría de bloqueos. TCR además captura la URL de la marca, lo que en caso de fraude ayudará a bloquear.

POLICIA NACIONAL

Los mecanismos existentes son insuficientes e inoperativos porque se requiere autorización judicial que tarda en conseguirse o no se consigue y porque las operadoras no son ágiles e incluso porque existen mecanismos para saltarse el bloque, tratándose muchas veces de ciberdelincuencia de ámbito internacional lo que limita la efectividad de las medidas aplicadas. En todo caso no debe permitirse que una página que recaba ilícitamente credenciales de usuarios esté operativa.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En general, consideran que son necesarias pero que no son eficaces, especialmente porque tardan demasiado y, por tanto, solo acaban siendo útiles cuando los estafadores reutilizan el dominio para posteriores campañas fraudulentas.

AEECF

No

ENDESA

Considera que las medas de retirada y bloqueo existentes son eficaces, pero deberían ser ágiles y sencillas.

OCU, CECU, AUI

OCU cree que no resultan eficaces porque las webs de phishing desaparecen rápidamente. CECU cree que esta medida no se está adoptando para estos casos, aunque convendría adoptarla y AUI cree que exigir la firma de la llamada o mensaje es más eficaz.

5b)

¿Qué utilidad atribuiría a un mecanismo de lista negra de URLs para advertir a los usuarios que no es un sitio seguro?

OPERADORES Y ASOCIACIONES DE OPERADORES

En términos generales si bien podría ser una medida adecuada, se ve limitada su eficacia por tener que actualizarse constantemente.

SUMINISTRADORES

TCR señala que crear una lista negra es un enfoque reactivo en su lugar proponen establecer listas blancas a través de TCR

POLICIA NACIONAL

Lo crítico es que la información sobre una URL fraudulenta llegue al usuario en el momento adecuado, es decir, cuando está accediendo a ella. Si no es así no vale, pues nadie chequea si

la URL a la que quiere acceder está en una lista negra. El navegador debería chequear la URL introducida t advertir al usuario de que es un sitio de riesgo.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNAC Y FRAUDFENSE C)

En general consideran que es una medida útil y necesaria pero que debe adoptarse con cautelas (ABANCA, por ejemplo, recuerda que el phishing puede incluso encontrarse en una web legítima que ha sido comprometida, por lo que es importante delimitar quién valida esta lista. También insisten en que esta medida debe ir acompañada de otras, como acciones de bloqueo, educación y concienciación, etc.

FRAUDFENSE es una plataforma colaborativa a la que pertenecen Banco Santander, BBVA y CaixaBank, que contendrá una base de datos de listas negativas en la que podrían incluirse URL maliciosas que las entidades adheridas hayan identificado como fraudulentas.

AEECF

No.

ASSECO GROUP

Spoofing Protector informa al usuario que está a punto de recibir SMS falsos. Esta notificación se puede personalizar.

ENDESA

Lo consideran útil, proponiendo que el prestador de servicios de acceso a internet advierta a los usuarios a través de un pop up de que va a entrar en una zona no segura.

OCU, CECU, AUI

No lo ven muy efectivo, porque no se puede exigir que las personas consulten esta lista cada vez que navegan por internet. AUI además señala que los defraudadores al consultarla cambiaran de URL.

5c)

¿Acompañaría un mecanismo como el apuntado en el punto 5b) de una obligación a los prestadores de servicios de acceso a internet de bloquear esas páginas web?

OPERADORES Y ASOCIACIONES DE OPERADORES

Vodafone apunta que toda obligación en esta materia que recaiga sobre los prestadores de servicios de acceso a internet debe ser de carácter reactivo, en el cual por un proceso previo amparado legalmente se establezca el procedimiento tasado de actuación que se debe llevar a cabo.

SUMINISTRADORES

TCR cree que estas medidas son limitadas, porque los estafadores actúan muy rápido.

ASSECO cree que no aplica, que depende de la decisión del cliente.

POLICIA NACIONAL

Si es conocido que una URL es fraudulenta no puede permitirse el acceso a la misma, por tanto, hay que bloquear.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, , AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En general contestan que sí, aunque algunos como EURO6000 insisten en incorporar mecanismos agiles para revertir la situación ante posibles errores.

AEECF

Sí, pero es una medida que toma demasiado tiempo para ser adoptada

OCU, CECU, AUI

Sí, esas URL deben bloquearse, aunque OCU cree que debe notificarse al usuario de que la página se ha bloqueado debido a phishing.

5d)

¿Acompañaría un mecanismo como el apuntado en el punto 5b) de una obligación a los operadores de comunicaciones interpersonales basados en numeración de bloquear los mensajes que incluyan esas URLs?

OPERADORES y ASOCIACIONES DE OPERADORES

Debería dotarse de soporte jurídico para ello, pero no tiene por qué ser una obligación sino una posibilidad que sea de aplicación por los operadores. MASMOVIL indica que la SETID debe permitir el bloqueo de URL en e-mail y SMS al ser amenazas (Reglamento Neutralidad de Red 3.3b)).

SUMINISTRADORES

TCR cree que es una solución insuficiente que a veces genera bloqueo de tráfico legítimo y sensible.

ASSECO Group cree que no es necesario bloquear estos mensajes, solo si la URL está en el archivo SenderID. También existe una solución o inicio de sesión que puede verificar la validez de estas URL.

POLICIA NACIONAL

Si es conocido que una URL es fraudulenta no puede permitirse el acceso a la misma, por tanto, hay que bloquear.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

En general contestan que sí, pero algunos como RED6000 recuerdan que crear webs/URL es sencillo, por lo que los estafadores enseguida crean otras, por lo que creen que es mejor bloquear llamadas/mensajes.

AEECF

No

OCU, CECU, AUI

CECU y AUI consideran que debe bloquearse, ya que de esta manera el mensaje ni siquiera llega al usuario. OCU considera que eso exige entrar en el contenido del mensaje por lo que no está a favor.

IMDEA

Recomiendan que los operadores móviles identifiquen las URL maliciosas en los SMS y bloqueen estos dominios en sus redes. Estas listas de bloqueo deben compartirse con los ISP que operen en el país.

6. Otras posibles medidas

6a)

¿Existe alguna medida adicional que considerara necesario abordar por parte de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales?

OPERADORES Y ASOCIACIONES DE OPERADORES

ALYSIS:

- Esquema criptográfico basado en firmas compatible con SMS/MMS tanto numéricos como alfanuméricos.

LLEIDANET:

- IA discriminativa (tecnología que clasifica y predice datos) para la identificación y control de las actividades fraudulentas.

MEF (MOBILE ECOSYSTEM FORUM):

- Single click reporting (Informes de un solo click).
- Reducción conjunto caracteres en los identificadores de SMS.

ORANGE:

- Enriquecimiento de llamadas y validación extremo a extremo.
- Migración de los sectores más afectados por el SMS Smshing (ej. banca) a RCS.

TELEFÓNICA:

- Bloquear tráfico P2P mismo remitente si supera umbral en un determinado espacio de tiempo.

SUMINISTRADORES

HIYA INC:

- Las medidas propuestas ayudarían, pero no detendrían a estafadores, se necesita una medida holísitca como el producto Hiya PROTECT (BD que se alimenta a través de IA).

PROVENANT:

- La única solución es autenticar a los remitentes a través de credenciales o recibos verificables (VR) permite verificación sin revelar su identidad. (se haya comprobado se cumple ej. DNO, consentimiento campaña, …).

RIBBON COMUNICATIONS:

- Análisis de tráfico en tiempo real con múltiples parámetros configurables que asignen un valor de fraude a la llamada.
- Análisis del contenido de la llamada a través de generar una huella de la misma.

SINCH:

- El sistema de Protección de Remitentes Nórdicos (SenderID Protection) bloquea mensajes fraudulentos, salvaguardando a los consumidores de intentos de smishing y spoofing, protege la reputación de las entidades y aumenta la confianza del consumidor final. Este sistema consiste en acotar los orígenes de tráfico (mediante análisis de remitente) a los proveedores utilizados y autorizados por las entidades bancarias. Cualquier tráfico con origen distinto al autorizado es bloqueado, tanto por el operador como por Sinch. Se acompaña del uso de listas blancas y negras de proveedores de SMS, y la asignación a los proveedores de SMS de licencias.

ASSECO:

- Debería haber una lista pública donde el cliente pueda informar de un problema sobre llamadas falsas o falsificadas o SMS sospechosos.

FUNDACIÓN ESYS

- Señala que si no se aportan datos que justifiquen la necesidad de regular el fraude telefónico (por ser minoritario frente a otro tipo de fraudes financieros, especialmente vía Internet) parece que una nueva regulación no sería necesaria.
- Existe una vía clara para la adopción de medidas técnicas y/o regulatorias orientadas a reducir el fraude financiero: la adopción de medidas de mejora de la aplicación de la PSD2 en España mediante la identificación segura reforzada por parte de las entidades financieras.

- En definitiva, para poner freno al preocupante fenómeno de la suplantación de identidad en servicios financieros la vía adecuada es atacar el problema: que las entidades financieras adopten de manera diligente todas las medidas tecnológicas adecuadas para identificar correctamente a sus clientes, estableciendo medidas de compliance y gestión de riesgos que minimicen el riesgo de suplantación de identidad de sus clientes. En otras palabras, medidas relativas a la identidad digital segura, no a medidas regulatorias en materia de numeración telefónica.

POLICIA NACIONAL

No se debe obviar el impacto que otras vías como el correo electrónico en las estafas múltiples, por lo que deben adoptarse medidas para prevenir la obtención de información sensible por esta vía.

BANCOS Y ENTIDADES FINANCIERAS (ABANCA, AEB, AEFI, CECA, EURO6000, IBERCAJA, UNACC)

AEFI considera oportuno establecer mecanismos técnicos y operativos destinados a exigir a los portales web y redes sociales la verificación de identidad, endurecer las penas previstas en el Código Penal para la suplantación de identidad en el ámbito digital y crear un organismo gubernamental, al que entidades y particulares puedan elevar casos de suplantación de identidad en colaboración con las FFCCS.

RED6000 se refiere a medidas de educación del usuario, a la necesidad de testeo de vulnerabilidades y a la criptografía, proponiendo valorar la posibilidad de crear un Código único y privado para cada entidad emisora de SMS. Cuando el operador reciba na petición de envío de SMS deberá enviar un código hash dinámico (SHA256) a la entidad emisora, la cual deberá tomarlo y añadirle su código único y privado. Si la operadora obtiene el mismo resultado el SMS se enviará, en caso contrario se bloqueará. De este modo no es necesario entrar al contenido del mensaje.

AEECF

Evitar que solo el sector TELCO pague los costes y por ejemplo usar fondos europeos. Extender a Whatsapp y aplicaciones de mensajería.

FENIE

Señalan que FENIE no puede denunciar los fraudes que conoce ante la AEPD porque las directrices de la Agencia obligan a que lo haga el usuario afectado, que suele negarse a hacerlo, por lo que piden que se abran canales de comunicación entre el sector energético (y otros) y el Ministerio o la AEPD para denunciar estos casos.

Asimismo, propone crear un canal entre la CNMC y la AEPD para que estas conductas fraudulentas se castiguen.

OCU, CECU, AUI

AUI propone firmar digitalmente llamadas y mensajes desde el extremo origen y las llamadas entre operadores, estampar el logo en el terminal una vez validada la firma e implementar una plataforma en los operadores que actúe con mecanismos de IA y machine learning como la que ofrece TNS.

UCARAGON

Señala que, aunque la normativa permite ejercer ante el responsable del tratamiento los derechos relacionados con la protección de datos, en la práctica es muy difícil para el receptor de una llamada comercial identificar al responsable del tratamiento y ejercer estos derechos, por lo que debería habilitarse algún sistema para que el consumidor pueda hacer esta identificación de forma sencilla.

Asimismo, creen que debe limitarse el acceso a los datos del Registro de Distribuidores, Comercializadores y Consumidores de gas y electricidad (Real Decreto 1011/2009) ya que estos datos son utilizados para inducir al consumidor a engaño simulando ser la empresa que actualmente presta el servicio.

Por último, entienden que, por defecto, en la contratación con consumidores, se debería separar el momento de prestar el consentimiento para el tratamiento de datos personales del momento de la contratación.

IMDEA

Piden que se preste atención a las estafas de SMS que no utilizan URL como la estafa “hola mamá y papá”, para lo que recomiendan obligar a incluir metadatos en el protocolo de SMS.

TESORERO AYUNTAMIENTO NERJA

Solicita que para hacer transferencias bancarias sea necesario incluir el CIF del beneficiario y comprobar que la cuenta que recibe el pago es titularidad del beneficiario del pago. Asimismo, solicita que haya un servicio online de acceso público, por ejemplo, en la web del Banco de España, que permita la comprobación de la veracidad de los datos introducidos por el usuario. Dicha web debería ser accesible al menos para las Administraciones Publicas.

PARTICULARES

Álvaro Sanchez Rodríguez pide eliminar la autorización de transferencias y pagos por teléfono, bloquear los números utilizados para fraude, identificar a los titulares últimos de las líneas de empresas de call, establecer un canal telemático de denuncia, tipificar como estafa agravada la realizada por medios telefónicos o informáticos y permitir a los usuarios solicitar al operador que sus números sean de “uso privado”.

David Ch pide crear una lista negra dinámica de números usados para estafas y que los operadores implementen un sistema basado en IA que avise al usuario de la posible estafa

Ana Isabel Ramiz Considera imprescindible que la numeración de los centros de telemarketing difiera completamente de la de empresas y entidades y que las listas DNO a disposición de toda empresa de envergadura con alcance nacional. Asimismo, solicita prestar atención a las estafas a través de Whatsapp.

Jorge Jose Arboleda Romero solicita que se imponga a las entidades financieras t de otro tipo que operen en internet la prohibición de ofrecer servicios que no ofrezcan presencialmente,

conforme a Sentencias que adjunta. Asimismo, pide la clausura de las páginas web de compraventa de bienes de segunda mano por competencia desleal.

Jose Carlos González Viejo pide la creación de un organismo público que actue como centralita de todas las llamadas comerciales de información a clientes potenciales con cargo de costes a cada empresa por el servicio.

Jose Marcos Giménez Teruel propone crear una página web en la que los usuarios puedan denunciar números o URL y al llegar a determinado número de denuncias se emita una alarma u orden de bloqueo.

José Naranjo Flox presenta una propuesta de mecanismo técnico mediante la creación de una red P2P en la que cada usuario decide con quien quiere emparejarse para intercambiar comunicaciones seguras. Adjunta link a la patente.