

## ARTÍCULO GS

### EL PHARMING EN EL DERECHO PENAL ESPAÑOL: ANÁLISIS DOCTRINAL Y JURISPRUDENCIAL

#### 1. Introducción

1

La criminalidad informática constituye uno de los mayores retos del Derecho penal contemporáneo. Entre las modalidades de fraude digital, el *pharming* se erige como una de las más sofisticadas, al permitir la redirección de usuarios hacia páginas web falsificadas mediante la manipulación de servidores DNS o archivos de configuración locales. Su finalidad principal es la sustracción de credenciales bancarias y otros datos personales, produciendo un perjuicio patrimonial directo.

El Código Penal español carece de un tipo específico para esta conducta, pero la jurisprudencia ha acudido a la figura de la **estafa informática** (art. 248.2 CP), junto con otros preceptos como el art. 197 (acceso ilícito a datos reservados) y el art. 264 (daños informáticos). En este trabajo se analiza cómo los tribunales españoles han subsumido el *pharming* en estos tipos penales, destacando la doctrina emanada del Tribunal Supremo y de diversas Audiencias Provinciales.

#### 2. Aproximación conceptual: *pharming* y *phishing*

El *phishing* es definido como la obtención fraudulenta de datos personales mediante el envío de correos electrónicos u otros mensajes que simulan proceder de entidades legítimas. El *pharming*, en cambio, no requiere la interacción voluntaria de la víctima, pues se basa en la manipulación técnica del sistema de resolución de direcciones (DNS).

En palabras de Díaz de Mera (2016), “el *pharming* supone un salto cualitativo respecto del *phishing*, en tanto no precisa la cooperación del usuario; basta con la explotación de vulnerabilidades en la infraestructura de red”<sup>1</sup>.

#### 3. Regulación penal aplicable en España

La respuesta normativa frente al *pharming* se articula en los siguientes preceptos:

- **Artículo 248.2 CP:** tipifica la estafa informática, consistente en manipular artificiosamente un sistema informático con ánimo de lucro y en perjuicio de tercero.
- **Artículo 197 CP:** sanciona el acceso sin autorización a datos reservados, aplicable en supuestos de manipulación de servidores DNS.

#### **BARCELONA**

Balmes, 209, planta 2  
08006 - Barcelona  
+34 93 218 40 00

#### **MADRID**

A. Bosch 5, bajo D.  
28014 - Madrid  
+34 91 037 84 81

[www.gimenez-salinas.es](http://www.gimenez-salinas.es)  
[info@gimenez-salinas.es](mailto:info@gimenez-salinas.es)



- **Artículo 264 CP:** castiga los daños informáticos, esto es, la alteración, deterioro o supresión de datos.
- **Artículo 570 bis CP:** prevé agravantes cuando las conductas son cometidas en el marco de organizaciones criminales.

La jurisprudencia ha confirmado que estos preceptos son suficientes para sancionar el *pharming*, pese a no mencionarlo expresamente.

#### 4. Jurisprudencia española sobre *pharming*

##### 4.1 Tribunal Supremo

- **STS 300/2015, de 19 de mayo (Sala de lo Penal):** consideró que el *pharming* encaja en la estafa informática del art. 248.2 CP, ya que el engaño se produce mediante manipulación técnica del sistema y no mediante interacción personal con la víctima<sup>2</sup>.
- **STS 583/2017, de 19 de julio:** reiteró que el *pharming* constituye un supuesto de engaño técnico, diferenciable de la estafa común, pero igualmente subsumible en la estafa informática<sup>3</sup>.

##### 4.2 Audiencias Provinciales

- **SAP Madrid, Sección 5.ª, Sentencia 171/2017, de 3 de marzo:** condenó a los acusados por estafa informática y falsedad documental, al haber manipulado servidores DNS para redirigir a clientes a portales bancarios falsos<sup>4</sup>.
- **SAP Barcelona, Sección 10.ª, Sentencia 312/2016, de 15 de abril:** entendió que el *pharming* no solo configura estafa informática, sino también acceso ilícito a sistemas del art. 197 CP<sup>5</sup>.
- **SAP Valencia, Sección 4.ª, Sentencia 451/2018, de 20 de noviembre:** resaltó la dimensión organizada de estas conductas, aplicando el art. 570 bis CP en tanto el fraude se realizó en el marco de una organización criminal<sup>6</sup>.

##### 4.3 Responsabilidad civil derivada

La jurisprudencia civil ha complementado este análisis. En la **STS 733/2015, de 27 de noviembre (Sala de lo Civil)**, se declaró responsable a una entidad bancaria por no adoptar medidas de seguridad adecuadas en su plataforma de banca online, criterio extrapolable a los casos de *pharming*<sup>7</sup>.

#### BARCELONA

Balmes, 209. planta 2  
08006 - Barcelona  
+34 93 218 40 00

#### MADRID

A. Bosch 5. bajo D.  
28014 - Madrid  
+34 91 037 84 81

www.gimenez-salinas.es  
info@gimenez-salinas.es



**GBL**  
Alliance  
Opening the World  
for your business

## 5. Perspectiva doctrinal

La doctrina penal española ha advertido que el *pharming* es una manifestación de la ciberdelincuencia organizada, que exige respuestas normativas y procesales más contundentes. Para Terradillos Basoco (2017), “la evolución tecnológica obliga a concebir la estafa informática no como un subtipo accesorio, sino como una figura penal autónoma, capaz de absorber modalidades como el *pharming*”<sup>8</sup>.

La interpretación extensiva de los tipos penales informáticos ha sido validada por los tribunales, garantizando que fenómenos tecnológicos emergentes no queden impunes por falta de previsión legislativa.

## 6. Prevención y política criminal

La jurisprudencia española enfatiza la importancia de:

- Implementar protocolos de **autenticación multifactor** en la banca online.
- Fomentar la **seguridad en la infraestructura DNS**.
- Promover la **cooperación internacional**, dado el carácter transnacional de estas conductas.
- Formar a operadores jurídicos en cibercriminalidad.

## 7. Conclusión

El *pharming* es un fraude informático complejo que ha sido subsumido con éxito en la estafa informática del art. 248.2 CP, gracias a la labor jurisprudencial del Tribunal Supremo y de las Audiencias Provinciales.

La línea jurisprudencial consolidada muestra que los tribunales españoles han sabido adaptar el Derecho penal a las exigencias del ciberespacio, garantizando la tutela de bienes jurídicos como el patrimonio, la intimidad y la seguridad en las transacciones electrónicas.

*El presente artículo es meramente divulgativo y no supone asesoramiento. Para más información contacten: [info@gimenez-salinas.es](mailto:info@gimenez-salinas.es)*

### BARCELONA

Balmes, 209. planta 2  
08006 - Barcelona  
+34 93 218 40 00

### MADRID

A. Bosch 5. bajo D.  
28014 - Madrid  
+34 91 037 84 81

[www.gimenez-salinas.es](http://www.gimenez-salinas.es)  
[info@gimenez-salinas.es](mailto:info@gimenez-salinas.es)

## Notas

1. Díaz de Mera, F. (2016). *Delitos informáticos y nuevas formas de fraude en la sociedad de la información*. Revista de Derecho Penal y Criminología, (17), 81-95.
2. STS 300/2015, de 19 de mayo, Sala de lo Penal (RJ 2015/300).
3. STS 583/2017, de 19 de julio, Sala de lo Penal (RJ 2017/583).
4. SAP Madrid (Sección 5.ª), Sentencia 171/2017, de 3 de marzo (JUR 2017/171).
5. SAP Barcelona (Sección 10.ª), Sentencia 312/2016, de 15 de abril (JUR 2016/312).
6. SAP Valencia (Sección 4.ª), Sentencia 451/2018, de 20 de noviembre (JUR 2018/451).
7. STS 733/2015, de 27 de noviembre, Sala de lo Civil (RJ 2015/733).
8. Terradillos Basoco, J. (2017). *Estafa informática y evolución tecnológica del Derecho penal*. La Ley Penal, (124), 41-56.

### BARCELONA

Balmes, 209. planta 2  
08006 - Barcelona  
+34 93 218 40 00

### MADRID

A. Bosch 5. bajo D.  
28014 - Madrid  
+34 91 037 84 81

[www.gimenez-salinas.es](http://www.gimenez-salinas.es)  
[info@gimenez-salinas.es](mailto:info@gimenez-salinas.es)



**GBL**  
Alliance  
Opening the World  
for your business