LA CIRCULAR DE LA FISCALÍA GENERAL DEL ESTADO RELATIVA A LOS DELITOS INFORMÁTICOS

I. Introducción

La Fiscalía General del Estado (**"FGE"**) publicó el pasado 21 de septiembre de 2017 su Circular 3/2017, sobre la reforma del Código Penal operada por la LO 1/2015 de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y delitos de daños informáticos (la **"Circular"**), dirigida a homogeneizar la actuación de las diferentes fiscalías de nuestro país en lo relativo a la persecución de determinados ciberdelitos.

La publicación de la Circular se produce como consecuencia de la entrada en vigor, el 1 de julio de 2015, de la última reforma del Código Penal (**"CP"**) por medio de la cual se modificó, entre otras cuestiones, el régimen previsto hasta la fecha para los delitos de descubrimiento y revelación de secretos y delitos de daños informáticos. En lo atinente a la lucha contra la ciberdelincuencia, la citada reforma tuvo por objeto la incorporación a nuestro Ordenamiento Jurídico de la Directiva 2013/40/UE, del Parlamento y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, actualizando de esa forma los tipos delictivos que rigen en una materia que destaca especialmente por su incipiente evolución.

II. Criterios de la FGE en la lucha contra la ciberdelincuencia

A continuación enumeraremos de manera sucinta los puntos más destacables de la Circular en lo que a la lucha contra la ciberdelincuencia se refiere:

(i) El delito de acceso ilegal a sistemas informáticos (artículo 197 bis 1º CP)

- El bien jurídico que se protege a través de la norma no es la intimidad personal, sino la propia seguridad de los sistemas de información como bien jurídico autónomo.

- El mero acceso no autorizado a un sistema informático (aunque no conlleve el apoderamiento de datos o información ajena) se considerará delictivo cuando se burle cualquier tipo de medida de seguridad que se encuentre operativa con la finalidad de impedir el acceso al sistema.

- La solidez de la medida de seguridad burlada o quebrada no es relevante como tampoco lo será si ésta ha sido establecida por el usuario, el administrador o el instalador del sistema.

(ii) El delito de abuso de dispositivos (artículo 197 ter CP)

- El delito de abuso de dispositivos sanciona a la persona que, sin estar debidamente autorizada, adquiera para su uso, importe o, de cualquier otro modo, facilite a terceros un medio informático para descubrir o revelar ilícitamente secretos.

- Los medios informáticos susceptibles de generar el perjuicio que protege la norma son programas informáticos o contraseñas de ordenador, códigos de acceso o datos similares que permitan el acceso a un sistema de información.

- Entre los programas informáticos que penaliza la norma deben entenderse incluidos los programas espía (*software maliciosos* o *malwares*).

- Quedan excluidos aquellos que no estén concebidos o adaptados principalmente para infiltrarse y/u obtener información de sistemas de información sin el consentimiento de su propietario.

- A efectos de determinar lo anterior será necesario generalmente un informe pericial.

- La mera posesión de un medio informático que reúna las características anteriores, con la intención de vulnerar la intimidad ajena, debe entenderse incluida dentro de la conducta penada, aunque dicho medio no llegue a usarse.

(iii) Legitimación activa para denunciar la comisión de los delitos anteriores

- Los delitos descritos en los apartados anteriores requieren para su persecución la denuncia de la persona agraviada o de su representante legal.

- El Ministerio Fiscal asumirá la legitimación activa para perseguir las anteriores conductas, sin necesidad de la denuncia previa del perjudicado, cuando el delito afecte a intereses generales o a una pluralidad de personas.

(iv) Delito de daños informáticos (artículo 264 CP)

- Se aplicará el tipo agravado a aquellos ataques que puedan realizarse contra servicios públicos esenciales o la provisión de bienes de primera necesidad.

- Deberán entenderse como servicios esenciales los relativos a la salud, seguridad, protección de derechos fundamentales y libertades públicas y el normal funcionamiento de las Instituciones del Estado.

- Entre los bienes de primera necesidad deben entenderse incluidos los alimentos, medicamentos y otros productos de consumo imprescindible para la subsistencia y salud de las personas.

- Las conductas de esta naturaleza podrían llegar a integrar delitos de terrorismo si se aprecian las finalidades previstas en el artículo 573 CP.

- Se reputará también como delictiva la adquisición, importación o facilitación a terceros –e incluso la mera posesión– de programas informáticos, contraseñas o códigos que tengan como finalidad producir daños en sistemas de información, aunque dichos medios informáticos no lleguen a usarse.

(v) El delito de obstaculización o interrupción del funcionamiento de sistemas informáticos (artículo 264 bis CP)

- No toda obstaculización o interrupción de un sistema será reprobable desde un punto de vista penal, sino únicamente aquellas que afecten significativamente a su funcionalidad.

- Dicha circunstancia deberá acreditarse a través de los correspondientes informes periciales.

III. Conclusiones

La Circular analizada establece los criterios que las diferentes fiscalías de nuestro país aplicarán en la persecución de los delitos de descubrimiento y revelación de secretos a través de medios tecnológicos y delitos de daños informáticos. Prácticas como las analizadas han copado la actualidad en los últimos tiempos en el panorama nacional e internacional, motivo por el cual cobra una especial relevancia que la Fiscalía haya publicado los criterios que dotarán de una mayor uniformidad la lucha contra este tipo de ciberdelitos.

Para más información,
pueden ponerse en contacto con:

Adriana de Buerba
Socia
Penal Económico e Investigaciones
adebuerba@perezllorca.com
Telf: + 34 91 423 67 29

Juan Palomino
Abogado
Penal Económico e Investigaciones
jpalomino@perezllorca.com
Telf: + 34 91 423 20 87