

INVASIÓN DE RED WIFI: ACTUACIONES DELICTIVAS

Dentro de nuestra actividad de consultoría jurídica a empresas, observamos como cada día se produce con mayor frecuencia una actividad de invasión de redes wifi ajenas, situación que produce a las empresas y sobre todo particulares una gran inseguridad jurídica, al dejar en descubierto su información más reservada.

Esta invasión de las redes de conexión wifi supone en la mayoría de los casos la comisión de una actuación delictiva al faltar el consentimiento del titular de la red, señalando a continuación los diferentes tipos penales aplicables.

En primer lugar, la invasión de una red wifi ha de incardinarse dentro del delito de defraudaciones de fluido eléctrico previsto en el Artículo 255 C.P., que se refiere al uso no autorizado o abusivo de terminales de telecomunicaciones ocasionando un perjuicio superior a 400 Euros.

Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a 400 euros, utilizando energía eléctrica, gas, agua, telecomunicaciones (televisión, teléfono, etc.) u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1º Valiéndose de mecanismos instalados para realizar la defraudación.

2º Alterando maliciosamente las indicaciones o aparatos contadores.

3º Empleando cualesquiera otros medios clandestinos.

Tal y como se manifiesta en el precepto, es necesario que se ocasione un perjuicio superior a 400 Euros, si es inferior se reenvía al artículo 623 C.P. (faltas contra el patrimonio).

Por otra parte, si la defraudación se realiza a través de equipo terminal de comunicaciones, el tipo penal aplicable es el previsto en el Artículo 256 C.P.

El que hiciere uso de cualquier equipo terminal de comunicación, sin consentimiento de su titular, ocasionando a este un perjuicio superior a 400 euros, será castigado con la pena de multa de tres a 12 meses.

Por tanto el mero acceso no consentido, conocido como hacking directo (acceso indebido o no autorizado con el único ánimo de vulnerar el password sin ánimo delictivo adicional), únicamente podría incardinarse en el tipo penal de defraudaciones, necesitando en todo caso, que se haya producido un perjuicio económico, como consecuencia de ese intrusismo, superior a 400 euros.

En segundo lugar, si la invasión de la red wifi se realiza con el fin de invadir el/los equipo/s conectados a la misma, dicha conducta sería constitutiva de un delito de descubrimiento y revelación de secretos previsto en el Artículo 197 C.P.

El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.”

Hasta ahora en los procesos penales habidos se ha utilizado como defensa exculpatoria la falta de intención de descubrir los secretos, señalando que la mera presencia en un equipo no era con dicha intención, si acaso con la intención de hacer una broma, pero ante este argumento cabe aplicar el artículo 197.2 el cual señala que

Las mismas penas se impondrán al que sin estar autorizado, se apodere, utilice o modifique en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

En este sentido, ya está desarrollada una importante jurisprudencia indicando que se trata de un delito contra la intimidad, considerando la interceptación del correo electrónico asimilada a la violación de la correspondencia.

En tercer lugar, nos encontraríamos con el llamado hacking indirecto, el cual supone un acceso in consentido al ordenador o sistema informático, bien como vulneración de la intimidad de su propietario (artículo 197) o como medio para cometer diferentes conductas delictivas, en cuyo caso, se castigará por el delito finalmente cometido.

Dentro de las conductas delictivas que pueden cometerse a través del hacking indirecto, caben resaltar los siguientes tipos:

1) Espionaje informático empresarial – A. 278 C.P.

El que para descubrir un secreto de empresa se apodere por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos previstos en el apartado 1 del artículo 197, será castigado con la pena de dos a cuatro años y multa de doce a veinticuatro meses.

El bien jurídico protegido es el secreto empresarial, la información almacenada informáticamente que supone un valor económico para la empresa porque confiere al titular una posición ventajosa en el mercado.

2) Daños informáticos o sabotaje – A. 264.2 C.P.

La misma pena (prisión de uno a tres años y multa de doce a 24 meses) se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.”

3) Estafa informática – A. 248.2 CP

También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años, si la cuantía de lo defraudado excede de 400 €.

4) Delitos contra la propiedad intelectual – A. 270 y ss C.P

5) Delitos contra la propiedad industrial – A. 273 y ss C.P.

Firmado: Ana M^a López Trigueros
Alberto Picón Cintas

Abogada
Abogado