UNA CALIFICACIÓN JURÍDICA EXIGUA

María Milagros Roibón

Correo electrónico**:** milagrosroibon@gmail.com

1.- Introducción

El presente trabajo tiene por objeto analizar la calificación jurídica adoptada en la causa caratulada: "**Ranieli Germán Walter s/ recurso de casación**", Expte. N° FSM 32224/2014/CFC1, la que -desde mi opinión- resulta exigua para el objeto procesal sobre el que versan los autos citados. Pero además se abordan, en forma sucinta, algunas cuestiones sobre el acceso ilegítimo a un sistema o dato informático (contemplado en el artículo 153 bis del Código Penal) y el daño informático (sancionado por el artículo 183, segundo párrafo del mismo código): delitos incorporados por la Ley 26.388 al Derecho Penal argentino. Por último, se ofrece una valoración personal sobre la importancia de este tipo de fallos, y la necesidad de contar con fuerzas policiales y operadores judiciales que persigan con eficacia y eficiencia uno de los flagelos criminales más recientes: el ciberdelito, el que trasciende todas las fronteras y estamentos sociales.

2.- Síntesis del fallo "Ranieli Germán Walter s/ recurso de casación", Expte. N° FSM 32224/2014/CFC1

El 30/3/2017 la Sala I de la Cámara Federal de Casación Penal, integrada por los jueces Ana María Figueroa, Mariano Hernán Borinsky y Gustavo M. Hornos, confirmó la sentencia dictada por el Juzgado en lo Criminal y Correccional Federal N° 2 de San Isidro, por el que se condenó a German Walter Ranieli a la pena de diez meses de prisión de ejecución condicional, por ser autor penalmente responsable del delito de acceso ilegítimo a un sistema o dato informático de acceso restringido (art. 153 bis, primer párrafo del CP) reiterado en dos ocasiones.

En la causa bajo análisis, caratulada “Ranieli Germán Walter s/ recurso de casación”, Expte. N° FSM 32224/2014/CFC1, el imputado que fue despedido de una cooperativa, en la que se desempeñó como contador, utilizó las claves fiscales de su ex empleadora sin autorización. En los autos, se demostró que Ranieli -luego de renunciar litigiosamente- ingresó desde un dispositivo apto para la navegación en Internet a la página web de la AFIP los días 29 y 30 de mayo y 2 de junio de 2014, específicamente a los datos informáticos de la cooperativa y del querellante, empleado para ello las claves fiscales asignadas a ambos sin su autorización.

Quedo probado que la conexión se llevó a cabo en la oficina del contador Ranieli, que éste disponía de una información relevante al conocer las claves fiscales. Asimismo, se determinó que el contador tenía conocimientos especiales, como consecuencia de su profesión, para realizar las operaciones impositivas cuestionadas que se efectuaron mediante los ingresos ilegales. Por otro lado, también se acreditó que el citado era el titular del servicio de Internet, al que correspondió la IP desde la que se realizaron las maniobras ilícitas y que las oficinas del contador coinciden con el lugar de instalación de dicha IP.

La Cámara Federal de Casación Penal consideró que los elementos probatorios obrantes en autos “*configuran el cuadro cargoso cuya valoración de conformidad con la sana crítica racional permitió a la sentenciante reconstruir históricamente las acciones atribuidas al imputado y colegir -en un adecuado razonamiento lógico- que los días 20 y 30 de mayo y 2 de junio del año 2014 desde un dispositivo apto para la navegación en internet, conectado a la red mediante el servicio “ARNET” y emplazado en la oficina de RANIELI (sita en la calle… de San Martín) se ingresó a la página web de la AFIP, a los datos informáticos allí contenidos del querellante Ariel Hernán Idoy y de la “Cooperativa de Vivienda, Crédito y Consumo Limitada” usando las claves fiscales asignadas a los nombrados y sin su autorización (pues a partir de su desvinculación en el año 2013 y en los malos términos en que ello ocurrió, ya no contaba con autorización para proseguir utilizando las mismas).*

Dicho corolario se encuentra en sintonía con las manifestaciones del querellante y es el fruto de la valoración racional de las pruebas colectadas, no existiendo resquicio alguno para albergar una hesitación razonable que haga plausible la operatividad del

principio in dubio pro reo (art. 3 el C.P.P.N.), como pretende la defensa y sin que se adviertan fisuras en el decurso del razonamiento desarrollado por la judicante para concluir como lo hizo".

La Cámara Federal de Casación Penal concluyó, en la sentencia, que *"...de conformidad con las probanzas valoradas, el agente llevó a cabo a sabiendas y sin la debida autorización los accesos a los datos informáticos restringidos de la cooperativa y de IDOY contenidos en el sitio web de la A.F.I.P. desarrollando así la acción típica prevista en la figura atribuida, es decir, con conocimiento y voluntad de vulnerar el ingreso a dichos datos, encontrándose de este modo configurado el doble aspecto que requiere el dolo como elemento subjetivo del tipo penal previsto en el art. 153 bis del CP, por lo que no podrá prosperar la pretensión de la defensa de que la conducta de su asistido sea reputada como atípica.*

De adverso a lo esgrimido por el impugnante, los hechos acreditados configuran el delito de acceso a un sistema o dato informático de acceso restringido reiterado en dos ocasiones que concurren en forma real entre sí (arts. 55 y 153, primer párrafo, del Código Penal), no mereciendo reparo alguno el juicio de tipicidad formulado por la judicante".

3.- Análisis de la calificación jurídica del caso bajo análisis

3.1.- Entiendo que la calificación jurídica adoptada por el fallo resulta exigua para los hechos por los que se condenó al contador German Water Ranieli a la pena de diez meses de prisión de ejecución condicional, por ser autor penalmente responsable del delito de acceso ilegítimo a un sistema o dato informático de acceso restringido (art. 153 bis, primer párrafo del CP) reiterado en dos ocasiones. A continuación, explicaré las razones por las que la calificación jurídica sostenida por el fallo no parece la mejor opción, siendo -desde mi punto de vista- desacertada. Adelanto mi opinión, en el sentido de que se debería haber condenado a Ranieli al delito de daño informático (artículo 183) agravado por aplicación del inciso 5 del artículo 184, ambos del Código Penal.

3.2.- El artículo 153 bis del Código Penal establece que: "*Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el*

que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o financieros".

Esta figura castiga la entrada por cualquier medio a un ordenador o sistema informático extraño o ajeno. Pablo Palazzi expresa que "*El sistema o dato informático es un ordenador o un conjunto de informaciones que no se encuentran fácilmente accesibles porque no están conectadas a una red, o porque se hallan amparadas con una clave de ingreso… El término "restringido" no debe entender como un elemento fáctico, sino como uno normativo del tipo penal… el término restringido está orientado a resultar la obligación de no ingresar en un ordenador extraño. No se tiene derecho a acceder a dicho sistema informático, y por eso se lo define como de acceso restringido".* (Pablo A. Palazzi. Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388, Editorial Abeledo Perrot, año 2009, página 103).

El acceso ilegítimo a un sistema o dato informático de acceso restringido se consuma cuando se entra o se accede sin autorización, ya sea violando las barreras de seguridad establecidas, sea por no estar autorizado a acceder o cuando se excede la autorización que el sujeto activo del delito posee. Es decir que este delito se consuma mediante el simple acceso a un dato o sistema restringido, sin que el autor del ilícito cuente con la autorización para ello.

Asimismo, este delito se caracteriza por ser de carácter subsidiario o residual. La figura del artículo 153 bis se aplica cuando "*no resulte un delito más severamente penado*". ¿Esto qué significa? Significa que el acceso ilegítimo a un sistema o dato informático se halla supeditado a que no se haya cometido un delito más severamente penado. La redacción de la norma excluye la comisión de un daño o la relevación de datos protegidos para la configuración del delito.

En síntesis, la simple intromisión informática sin autorización configura una conducta típica en el Derecho Penal argentino. El autor del delito sancionado por el artículo 153 bis no

debe modificar o alterar el sistema o los datos del sistema informático para que se consume el ilícito en cuestión.

3.3.- Ahora bien, de la lectura de la sentencia se desprende que Ranieli ingresó desde un dispositivo apto para la navegación en Internet a la página web de la AFIP los días 29 y 30 de mayo y 2 de junio de 2014, específicamente a los datos informáticos de la cooperativa y del querellante, empleado para ello las claves fiscales asignadas a ambos sin su autorización. Sin embargo, el fallo no tuvo en cuenta que Ranieli además de haber ingresado a los usuarios de la cooperativa y del querellante en la página de la AFIP, realizó operaciones impositivas. Esas operaciones tributarias fueron efectuadas mediante los ingresos ilegales perpetrados por el condenado. Por ende, los hechos referenciados no pueden encuadrarse en el delito del acceso no autorizado a un sistema informático, ya que el condenado modificó los datos de las cuentas de la cooperativa y del querellante en el portal del organismo fiscal, para lo que previamente debió ingresar ilegítimamente a la página web del Fisco nacional, empleando claves fiscales ajenas que no podía utilizar.

3.4.- Siguiendo con este razonamiento, estos hechos deberían haber sido encuadrados en el delito de daño informático (artículo 183, segundo párrafo del CP) agravado por el artículo 184, inciso 5 del mismo código. El artículo 183, segundo párrafo establece que será reprimido con prisión de quince días a un año "*el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños*" (el subrayado me pertenece).

La acción típica de este ilícito consiste en alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos. Palazzi expone que alterar "*implica modificar un archivo de datos o programas sin destruirlo completamente… alterar es cambiar la esencia o forma de algo… tanto el borrado como la alteración modifican la esencia de la cosa en sí, independientemente de que, por tratarse de objetos digitales, puedan restaurarse con cierta facilidad*" (Palazzi, obra citada, páginas 187/188).

Jorge Eduardo Buompadre aclara que la alteración "*supone una modificación de la información, la que puede llevarse a cabo por medio de múltiples modalidades (v.gr., borrando datos, introduciendo datos nuevos, cambiando una información por otra)"* (Jorge

Eduardo Buompadre. Manual de derecho penal. Parte especial. 3ª reimpresión, Editorial Astrea SRL, año 2017). Es decir que esta acción supone la desaparición definitiva de información, la que es reemplazada por otra, como sucedió en la causa caratulada: "Ranieli Germán Walter s/ recurso de casación".

El objeto del delito se refiere a los "*datos, documentos, programas o sistemas informáticos… Por datos se entiende cualquier información que tenga un significado, tanto para una persona como para el sistema informático o un programa de ordenador".* (Palazzi, obra citada, página 189).

El mismo autor agrega que la *"finalidad de este delito es penalizar al que daña la propiedad ajena con la intención de alterar datos o sistemas informáticos, por lo que se requiere un dolo específico de dañar"* (Palazzi, obra citada, página 199). Buompadre entiende que se trata de "*un delito doloso, en el que sólo es posible el dolo directo*". (Buompadre, obra citada, página 541). Diego Migliorisi añade que "*La finalidad de producir un daño informático en forma intencional puede tener diferentes motivos, desde la simple diversión de destruir, atacar o inutilizar un sistema informático, hasta intencionales comerciales*". (Diego F. Migliorisi. Crímenes en la web. Los delitos del siglo XXI. Del Nuevo extremo, año 2014, página 90).

3.5.- En este orden de ideas, la aplicación de la agravante del artículo 184, inciso 5 del Código penal (el que establece que: *"La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes… 5) Ejecutarlo en…datos, documentos, programas o sistemas informáticos públicos")* al caso comentado, resulta apropiada. Buompadre enseña que la figura agravada del daño informático importa "*una protección más intensa a datos, documentos, programas o sistemas informáticos de carácter públicos, de interés general y que interesa al Estado preservar de toda interrupción o daño, precisamente por los graves perjuicios que ello causaría a la comunidad social o al propio funcionamiento del Estado. De ahí la justificación de la mayor penalidad para esta clase de hechos*" (Buompadre, obra citada, página 542).

3.6.- En conclusión, y a raíz de las características de los hechos por los que German Ranieli fue condenado en los autos mencionados, sostengo que el encuadre jurídico correcto del caso consistía en condenarlo por el delito de daño informático (artículo 183, segundo

párrafo) agravado por la aplicación del inciso 5 del artículo 184 del Código Penal. El contador no sólo ingresó sin autorización a los datos informáticos de usuarios ajenos, sino que además modificó los datos informáticos de esos usuarios en la página del organismo fiscal.

4.- Consideraciones generales sobre el daño informático

Independientemente del análisis de la calificación jurídica del caso "Ranieli Germán Walter s/ recurso de casación", me referiré a la figura del daño informático, el que se encuentra consagrado en diversas legislaciones (Colombia, Chile, Estados Unidos, Alemania, Venezuela, Mozambique, Angola, Lituania, España, etc.). La Ley 26.388 que incorporó el daño informático en el Código Penal argentino, se basó en las disposiciones de la Convención sobre el cibercrimen, más conocida como el Convenio de Budapest del 23/11/2001.

¿Qué se entiende por daño informático? Diego Migliorisi sostiene que "*cuando hablamos de daño informático no nos referimos a una destrucción material mediante la violencia física, sino a que una persona autorizada, o no, ingrese a un ordenador o a través de la web desconfigure o borre intencionalmente elementos informáticos necesarios para su funcionamiento, páginas web o bien información almacenada en soportes electrónicos, propiedad de la víctima…*

En cuanto a la forma de configurar el delito, el autor puede lograrlo ya sea en forma directa, ingresando físicamente al ordenador y producir el daño en vivo y en directo, o bien mediante algún programa malicioso que se envíe camuflado en algún correo electrónico. Existen programas que se autoinstalan cuando el usuario intenta ver su contenido; su activación produce la ejecución del malware provocando la eliminación o el daño determinados.

El daño informático no solamente tiene por objeto la destrucción de información local, sino también los sitios web que estén alojados en algún lugar de datacenters y hostings, computadoras que no están exentas de ataques" (Migliorisi, obra citada, página 90).

5.- Valoración personal

Los vertiginosos cambios tecnológicos se han extendido a los más diversos campos de la vida en sociedad, incluido el criminal, dando lugar a lo que se conoce como "delitos informáticos". Y en esta dirección se pronuncia Carrión, quien define a estos delitos como *"aquellas acciones tipificadas, antijurídicas y culpables que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad como bien jurídico de naturaleza colectiva o macrosocial (abarcativo de otros intereses, v.gr.: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos, etc.), en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, trasmisión y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre lo que operan las maniobras dolosas".* (Carrión, "Presupuestos para la incriminación del hacking", ponencia presentada en las "Primeras Jornadas Latinoamericanas de Derecho Informático", Mar del Plata, 2001).

En la actualidad, algunos sustentan que los delitos informáticos generan más ganancias que el narcotráfico. Detrás de los delitos informáticos, existen poderosas organizaciones criminales -casi todas internacionales-, que además de poseer conocimientos sofisticados y complejos que dificultan su persecución, utilizan el anonimato que les ofrece Internet. El anonimato impide que, en muchos casos, se pueda identificar a los autores del crimen, o en muchas oportunidades el país en donde reside el delincuente no colabore con la nación en donde se efectúa la investigación. Asimismo, y al tratarse -en su mayoría- de delitos trasnacionales, cuyos alcances pueden esparcirse por toda la red, esto dificulta aún más su persecución por parte del Estado.

De esta forma, las estafas y los ataques informáticos están creciendo en forma exponencial, convirtiéndose en un flagelo mundial, lo que ha comenzado a generar una creciente preocupación en los gobiernos y en las empresas. En este contexto, debe destacarse el hecho de que la Argentina forme parte de la Convención de Budapest, el primer tratado internacional sobre ciberdelincuencia, que propone la cooperación mutua entre los países firmantes para obtener evidencia digital de usuarios, empresas y servidores que estén en otros países. Esta convención estandariza criterios, protocolos y legislaciones de los distintos

países que adhieren a la misma con el fin de avanzar en la lucha contra los delitos cometidos con la ayuda de las redes y sistemas informáticos.

Por ende, las fuerzas policiales y los operadores judiciales deben contar con los conocimientos necesarios y los medios suficientes para castigar el cibercrimen, que evoluciona en forma continua, afectando a todos los actores de la sociedad (gobiernos, multinacionales, pequeñas empresas, sanatorios, bancos, entidades financieras, particulares, etc.). Y que en nuestro país comiencen a conocerse condenas -como la del caso analizado- señalan el nuevo -aunque tímido- rumbo que la justicia argentina ha empezado a transitar: la persecución del ciberdelito, el que exige una capacitación de excelencia por parte de los encargados de combatirlo. He ahí, uno de los grandes desafíos que la tecnología y la sociedad de la información suponen para la justicia penal argentina, la que debe adecuarse con eficacia y eficiencia a los nuevos tiempos que corren.

Por último, entiendo que la creación de fiscalías especializadas en la investigación del cibercrimen en el interior del país (ya sea en los fueros penales de competencia ordinaria como en los fueros federales) permitiría que este tipo de causas cobren un gran impulso, mejorando los niveles de la persecución penal en este tipo de investigaciones que requieren por la naturaleza y características de los ilícitos a investigar, de personal altamente especializado y capacitado.