Chillán, veintiséis de agosto de dos mil veintiséis.

Visto:

En estos autos RUC 2201188569-5, RIT N°252-2024, el Tribunal de Juicio Oral en lo Penal de Chillán, por sentencia de treinta de junio de dos mil veintiséis, condenó a RODRIGO IGNACIO VALENZUELA PARRA, a la pena de quinientos cuarenta y un días de presidio menor en su grado medio, y a la accesoria legal de suspensión de cargo u oficio público durante el tiempo de la condena, en su calidad de autor del delito consumado de acceso ilícito a sistema informático con divulgación de la información contenida en éste, previsto y sancionado en el artículo 2 incisos 1° y 3° de la Ley N°21.459, perpetrado en la comuna de Chillán el 22 de noviembre de 2022.

Los sentenciadores sustituyeron el cumplimiento de la pena privativa de libertad por la de remisión condicional, por el mismo lapso de la condena, con arreglo a los artículos 4 y siguientes de la Ley N°18.216.

La decisión condenatoria fue adoptada por mayoría, con el voto en contra del juez don Juan Pablo Lagos Ortega, quien estuvo por absolver, por estimar que la conducta establecida en el juicio no satisface el tipo penal de acceso ilícito.

En contra de la referida sentencia, la Defensora Penal Pública doña María Daniela Carrasco Conejeros, en representación del condenado, dedujo recurso de nulidad fundado en la causal contemplada en el artículo 373 letra b) del Código Procesal Penal.

Declarado admisible el recurso, se procedió a su vista en la audiencia respectiva, con la asistencia de la parte recurrente y de la representante del Ministerio Público, fijándose para la comunicación de la sentencia el día de hoy.

Con lo relacionado y considerando

Primero: Que la defensa sostiene que la sentencia incurrió en una errónea aplicación del derecho al calificar los hechos como constitutivos del delito de acceso ilícito del artículo 2 incisos 1° y 3° de la Ley N°21.459.

Argumenta que la mayoría del tribunal efectuó una interpretación extensiva y analógica de la expresión "excediendo la autorización que posea",

sancionando en definitiva por la finalidad del acceso y no por la falta de poder técnico o jurídico para ingresar al sistema, en circunstancias que el tipo penal exige copulativamente que el acceso se verifique "superando barreras técnicas o medidas tecnológicas de seguridad". Habiéndose establecido en el juicio que el señor Valenzuela contaba con nombre de usuario y contraseña válidos, provistos por la propia institución, y que accedió al sistema precisamente facultado para ello, no existió superación de barrera alguna, sino a lo sumo un uso indebido de las facultades conferidas, reprochable en sede administrativa o disciplinaria, mas atípico en sede penal. Añade que, ausente el acceso ilícito, la divulgación sancionada en el inciso 3° tampoco resulta punible, por cuanto ésta presupone que la información se haya obtenido mediante un acceso ilícito. Adhiere expresamente a los fundamentos del voto disidente del juez Lagos Ortega. Concluye que el error influyó sustancialmente en lo dispositivo del fallo, pues de haberse aplicado correctamente el derecho la única decisión posible era la absolución, y pide anular la sentencia y dictar, sin nueva audiencia pero separadamente, sentencia de reemplazo que absuelva a su representado, conforme al artículo 385 del Código Procesal Penal.

Segundo: Que el artículo 373 letra b) del Código Procesal Penal dispone que procederá la declaración de nulidad del juicio oral y de la sentencia "cuando, en el pronunciamiento de la sentencia, se hubiere hecho una errónea aplicación del derecho que hubiere influido sustancialmente en lo dispositivo del fallo".

Tercero: Que el recurso de nulidad es un arbitrio de carácter extraordinario y de derecho estricto, instituido para invalidar el juicio oral y la sentencia definitiva, o solamente ésta, por las causales expresamente previstas en la ley. Tratándose de la causal invocada, ella importa necesariamente aceptar los hechos tal como fueron establecidos por el tribunal de la instancia, sin cuestionar su construcción ni los razonamientos valorativos que a ellos condujeron, de modo que el reproche sólo puede relacionarse con la correcta aplicación del derecho a ese sustrato fáctico. A diferencia de otros supuestos, en la especie la causal no se dirige a controvertir la ponderación de la prueba —facultad privativa de los jueces del fondo—, sino que plantea una cuestión estrictamente jurídica de subsunción o calificación típica, sobre hechos que no son objeto de disputa, materia respecto de la cual esta Corte se encuentra plenamente habilitada para pronunciarse.

Cuarto: Que, en tal orden, conviene precisar que el hecho que el tribunal a quo tuvo por acreditado consistió en que el día 22 de noviembre del año 2022, en la comuna de Chillán, el imputado RODRIGO IGNACIO VALENZUELA PARRA, quien a esa fecha se desempeñaba como Carabinero del Retén Bonilla, ingresó a la plataforma institucional de Carabineros denominada “Sistema de Información Operativa” con la finalidad de obtener antecedentes personales del ciudadano Matías Enrique Solís Vera, Rut 20.374.526-5, correspondientes a: su fotografía, RUN, nombre completo, género, fecha de nacimiento, edad y el domicilio, para posteriormente enviarle vía WhatsApp dicha información a su primo de nombre Cristopher Nicolás Muñoz Ortiz apodado “EL YIYO”, excediendo de esta manera la autorización que poseía en razón de su cargo como carabinero, para ingresar a dicha plataforma, entregando y revelando información reservada a un tercero a la que tiene acceso en razón de su cargo para fines institucionales.

Quinto: Que resulta conveniente dejar establecido que sobre los hechos acreditados no existe controversia, pues tanto el voto de mayoría como el disidente coinciden en que el acusado, funcionario activo de Carabineros, accedió al Sistema de Información Operativa valiéndose del dispositivo institucional en que la aplicación se hallaba instalada y del nombre de usuario y contraseña que le habían sido asignados, para obtener la información de un tercero a requerimiento de su primo y luego remitírsela. La discrepancia entre mayoría y disidencia es, por tanto, exclusivamente de calificación jurídica.

Sexto: Que, así delimitada, la controversia jurídica se reduce a determinar si la conducta descrita satisface el tipo del artículo 2 inciso 1° de la Ley N°21.459 y, en particular, si el funcionario que, contando con credenciales válidas, accede a un sistema informático al que se encuentra habilitado a ingresar, pero lo hace con una finalidad ajena a la institucional, "excede la autorización que posea" y "supera barreras técnicas o medidas tecnológicas de seguridad" en los términos que la norma exige.

Séptimo: Que el examen debe partir del tenor literal del precepto, y es así que el artículo 2 inciso 1° de la ley 21.459 sanciona a quien, "sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático".

La estructura del tipo revela dos exigencias copulativas, enlazadas por la conjunción "y": de un lado, que el acceso se realice sin autorización o excediendo la que se posea y, de otro, que el acceso se verifique superando barreras técnicas o medidas tecnológicas de seguridad. Ambas condiciones deben concurrir conjuntamente para la configuración del injusto.

Octavo: Que, sentado lo anterior, corresponde examinar por separado la concurrencia de cada una de las dos exigencias copulativas, comenzando por la primera, esto es, que el acceso se realice “sin autorización o excediendo la autorización que posea”. Este elemento, de carácter normativo, expresa la ajenidad o antinormatividad del acceso y se refiere al ámbito del ingreso: la hipótesis de “exceso” supone que el agente, hallándose autorizado para acceder a una parte o nivel del sistema, se interna en otro sector que le está vedado conforme a su perfil. Alude, pues, al ámbito o extensión de la habilitación de acceso, y no a los móviles o a la finalidad con que se utiliza aquello a lo que legítimamente se está facultado para ingresar. Cabe precisar, además, que la exigencia de “superar barreras técnicas o medidas tecnológicas de seguridad" no gobierna únicamente la hipótesis del extraño que accede “sin autorización”, sino también la del interno (intraneus) que lo hace “excediendo la autorización que posea”, desde que la conjunción copulativa “y” vincula ambas modalidades de acceso con el modo comisivo, sin establecer distinción entre ellas.

Noveno: Que, contrastada dicha exigencia con los hechos asentados, esta Corte concluye que ella no concurre en la especie. En efecto, quedó establecido que el acusado se encontraba habilitado para ingresar al Sistema de Información Operativa y que consultó datos comprendidos dentro del ámbito propio de su perfil funcionario, sin franquear sector, nivel o segmento alguno reservado a una habilitación diversa de la suya. Que la consulta se haya efectuado con un propósito ajeno al institucional configura una desviación en el uso de una facultad legítimamente conferida, reprochable, en su caso, en sede disciplinaria, mas no un “exceso” en la autorización de acceso en el sentido que el tipo reclama. Entender lo contrario importaría incorporar al tipo un elemento no previsto por el legislador, cual es la finalidad del acceso, con infracción del principio de legalidad. De esta manera, no concurriendo la primera de las exigencias del tipo, y según se dirá tampoco la segunda, la atipicidad de la conducta se sigue por doble motivo.

Décimo: Que, contrastado dicho estándar con los hechos, esta Corte advierte que no concurre, asimismo, la segunda de las exigencias señaladas, pues el acusado ingresó al Sistema de Información Operativa sirviéndose del dispositivo institucional en el que la aplicación se encontraba instalada y de las credenciales, usuario y contraseña, que la propia institución le había proporcionado.

El acusado no creó ni empleó credenciales ajenas, no franqueó un nivel o segmento del sistema vedado para su perfil, ni neutralizó mecanismo de protección alguno, ya que se limitó a utilizar la clave que legítimamente detentaba. Faltó, en consecuencia, la superación de barreras técnicas o medidas tecnológicas de seguridad que el tipo requiere como elemento copulativo.

En tal sentido el profesor Roberto Navarro Dolmestch ha sostenido que el que accede a un sistema informático, pero sin violar medidas de protección, configura una conducta atípica. (La autorización como causal de atipicidad en el delito de acceso ilícito a un sistema informático en la legislación chilena de delitos informáticos, Revista Chilena de Derecho y Tecnología, página 21).

En similar sentido se ha dicho que el acceso ha de realizarlo un sujeto que no cuenta en absoluto con autorización para ingresar al sistema informático en cuestión o bien que cuente con autorización, pero no respecto de la parte o del ámbito del sistema al cual esta accediendo. (Delitos informáticos y cibercriminalidad, aspectos sustantivos y procesales, Laura Mayer Lux y Jaime Vera Vega, página 187.)

Décimo primero: Que en palabras de los profesores Gonzalo Bascur y Rodrigo Peña (Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459. Primera parte Revista Estudios de la Justicia, NÚM. 37, 2022, página 13), *el tipo objetivo está constituido por i) la conducta de «acceso» a un sistema, mediante ii) la «superación» de «barreras técnicas» o «medidas tecnológicas de seguridad», ejecutada iii) «sin autorización» del titular o «excediendo» aquella concedida. De esta descripción, como también por lo dispuesto en el artículo 16, se desprende que necesariamente el sistema de referencia debe ser total o parcialmente ajeno, vale decir, encontrarse adscrito a la esfera de gestión y acceso de una persona distinta del autor. Asimismo relatan que en relación a los elementos*

normativos de carácter alternativo «sin autorización del titular» y «excediendo la autorización que se posea», estos reflejan con nitidez que los datos o el sistema informático no se encuentra destinado al autor de la intromisión. Bajo la expresión «sin autorización», se castiga a los denominados outsiders (o extraneus) del sistema, mientras que mediante la segunda redacción, «excediendo la autorización que se posea», a los insiders (o intraneus). Estas exigencias constituyen elementos de antinormatividad, vale decir, elementos normativos que expresan la contrariedad a derecho de la conducta de acceso, o según la nomenclatura más difundida, que determinan si el ingreso pertenece o no a la esfera de un riesgo permitido.

Décimo segundo: Que la interpretación sostenida por el voto de mayoría, conforme a la cual "excede la autorización" quien, estando facultado a ingresar, lo hace con una finalidad diversa, importa incorporar al tipo un elemento que el legislador no previó, cual es la finalidad del acceso y, a la vez, prescindir del requisito copulativo de superación de barreras técnicas, privándolo de todo contenido autónomo.

Así la doctrina ha sostenido que no es típico del delito de acceso ilícito el ingresar físicamente al sistema informático, como cuando se conoce información contenida en él mirando la pantalla de un computador que exhibe parte de esa información, o cuando el atacante conoce la información por medio de la revisión de registros impresos de la arquitectura del sistema o de sus datos. En estos dos casos no hay un acceso que haya implicado una violación de barreras técnicas al ingreso no autorizado. (Roberto Navarro Dolmestch, El concepto de delito informático según la nueva legislación chilena (Ley nº 21.459) Política Criminal, Volumen 18, N°36).

Décimo tercero: Que el legislador incorporó al tipo penal expresamente la exigencia de "superando barreras técnicas o medidas tecnológicas de seguridad", lo cual implica la necesidad de un quebrantamiento efectivo de las medidas de seguridad, pues como ha sostenido el profesor Gonzalo Medina Schulz, este es el requisito esencial para dar por realizado el tipo penal, pues la vulneración de mecanismos informáticos de protección en la exteriorización más nítida de la perpetración de una intromisión indebida en una esfera de resguardo de la privacidad, respecto de la cual se carece de la legitimación para acceder. (El delito de acceso a sistemas informáticos, Delitos informáticos,

análisis dogmáticos y comentarios a la ley 21.459 página 59) y que precisamente aquello que no se verificó en la especie.

Décimo cuarto: Que, en consecuencia, la conducta acreditada, el uso desviado, para un fin particular, de un acceso al que el funcionario se encontraba habilitado con credenciales válidas, podrá revestir gravedad y merecer reproche en sede administrativa o disciplinaria, pero no satisface los elementos objetivos del tipo de acceso ilícito previsto en el artículo 2 inciso 1° de la Ley N°21.459, tal como lo sostiene el voto disidente y cuyos fundamentos esta Corte comparte.

Décimo quinto: Que, descartada la tipicidad del acceso, tampoco puede configurarse la figura de divulgación del mismo artículo 2, cualquiera sea la modalidad que se considere. En efecto, tanto el inciso 3°, que sanciona a quien divulga información accedida ilícitamente cuando no fue obtenida por él, como el inciso 4°, que contempla el caso de ser una misma persona la que hubiere obtenido y divulgado la información, hipótesis esta última que corresponde a la del acusado, presuponen como antecedente necesario un acceso ilícito previo. Ausente éste, la posterior comunicación de los antecedentes a un tercero deviene igualmente atípica a la luz de los preceptos invocados en la acusación.

Décimo sexto: Que el error de derecho anotado influyó sustancialmente en lo dispositivo del fallo, pues de haberse aplicado correctamente el artículo 2 de la Ley N°21.459 a los hechos establecidos, la única decisión posible habría sido la absolución del acusado, razón por la cual el recurso debe necesariamente ser acogido.

Chillán, veintiséis de agosto de dos mil veintiséis.

Por estas consideraciones, normas citadas y lo dispuesto en los artículos 2 de la Ley N°21.459; 372, 373 letra b), 376, 378, 379, 380, 381, 383, 384 y 385 del Código Procesal Penal, **SE ACOGE** el recurso de nulidad deducido por la defensa del sentenciado Rodrigo Ignacio Valenzuela Parra en contra de la sentencia dictada el treinta de junio de dos mil veintiséis por el Tribunal de Juicio Oral en lo Penal de Chillán, en los autos RUC 2201188569-5, RIT N°252-2024, y, en consecuencia, se declara que dicha sentencia es **NULA**, procediéndose acto seguido y separadamente a dictar la correspondiente sentencia de reemplazo.

Redacción a cargo del fiscal judicial subrogante Gabriel Hernández Sotomayor, quien no firma por haber cesado en el cargo.

Regístrese y comuníquese lo resuelto.

Rol N°565-2026.- PENAL.

SENTENCIA DE REEMPLAZO

En cumplimiento con lo dispuesto en el artículo 385 del Código Procesal Penal, se procede a dictar la siguiente sentencia de reemplazo.

Chillán, veintiséis de agosto de dos mil veintiséis.

VISTO:

Se reproduce la sentencia recurrida dictada por el Tribunal de Juicio Oral de esta ciudad, con excepción de los motivos 8° a 20°, que se eliminan.

Y se tiene en su lugar, y además, presente:

Primero: Que se ha tenido por acreditado, que el día 22 de noviembre del año 2022, en la comuna de Chillán, el imputado RODRIGO IGNACIO VALENZUELA PARRA, quien a esa fecha se desempeñaba como Carabinero del Retén Bonilla, ingresó a la plataforma institucional de Carabineros denominada “Sistema de Información Operativa” con la finalidad de obtener antecedentes personales del ciudadano Matías Enrique Solís Vera, Rut 20.374.526-5, correspondientes a: su fotografía, RUN, nombre completo, género, fecha de nacimiento, edad y el domicilio, para posteriormente enviarle vía WhatsApp dicha información a su primo de nombre Cristopher Nicolás Muñoz Ortiz apodado “EL YIYO”, excediendo de esta manera la autorización que poseía en razón de su cargo como carabinero, para ingresar a dicha plataforma, entregando y revelando información reservada a un tercero a la que tiene acceso en razón de su cargo para fines institucionales.

Segundo: Que dicho hecho no es constitutivo del delito de acceso ilícito a sistema informático, con divulgación de la información contenida en éste, previsto y sancionado en el artículo 2 incisos 1° y 3° de la Ley N°21.459. En efecto, y según se razonó latamente en el fallo de nulidad que precede, el acceso al Sistema de Información Operativa se verificó mediante credenciales válidas asignadas al acusado, sin superación de barreras técnicas o medidas tecnológicas de seguridad y sin exceder el ámbito del sistema al que se hallaba habilitado a ingresar, constituyendo la finalidad del acceso un elemento ajeno a la descripción típica.

En consecuencia, la conducta es atípica; y la divulgación posterior de los antecedentes, carente de un acceso ilícito que la preceda y le sirva de presupuesto, tampoco resulta punible a la luz del precepto invocado.

Tercero: Que, por lo anterior, no configurándose el delito materia de la acusación ni ningún otro respecto del cual se hubiere formulado cargo en este juicio, procede dictar sentencia absolutoria en favor del acusado.

Por estas consideraciones y visto, además, lo dispuesto en los artículos 1 del Código Penal; 2 de la Ley N°21.459; y 45, 340, 341, 342, 347 y 385 del Código Procesal Penal, SE DECLARA:

I.- Que se ABSUELVE a RODRIGO IGNACIO VALENZUELA PARRA, ya individualizado, de la acusación que lo suponía autor del delito de acceso ilícito a sistema informático con divulgación de la información contenida en éste, previsto y sancionado en el artículo 2 incisos 1° y 3° de la Ley N°21.459, supuestamente perpetrado en la comuna de Chillán el 22 de noviembre de 2022.

II.- Que no se condena en costas al Ministerio Público, por haber tenido motivos plausibles para litigar.

Regístrese, comuníquese y, en su oportunidad, devuélvanse los antecedentes al tribunal de origen.

Redacción a cargo del fiscal judicial subrogante Gabriel Hernández Sotomayor, quien no firma por haber cesado en el cargo.

Rol N°565-2026.- PENAL.

Guillermo Alamiro Arcos Salinas
Ministro
Corte de Apelaciones
Veintiséis de agosto de dos mil veintiséis
11:39 UTC-4

Carolina Isabel Vásquez Epuñán
Ministro(S)
Corte de Apelaciones
Veintiséis de agosto de dos mil veintiséis
11:12 UTC-4

Pronunciado por la Segunda Sala de la C.A. de Chillan integrada por Ministro Guillermo Alamiro Arcos S. y Ministra Suplente Carolina Isabel Vasquez E. Chillan, veintiseis de agosto de dos mil veintiseis.

En Chillan, a veintiseis de agosto de dos mil veintiseis, notifiqué en Secretaría por el Estado Diario la resolución precedente.