Boletín N° 18.558-25

Proyecto de ley, iniciado en Moción de los Honorables Senadores señoras Vodanovic y Núñez, y señor Castro, que modifica diversos cuerpos legales, con el objeto de establecer la obligación de entrega o puesta en ejecución de claves de descifrado, y de sancionar penalmente su incumplimiento.

I. ANTECEDENTES

La utilización de dispositivos electrónicos y sistemas informáticos constituye actualmente una dimensión ordinaria de prácticamente todas las actividades humanas. Teléfonos móviles, computadores, servicios de almacenamiento remoto y otras tecnologías almacenan información que puede resultar determinante para establecer la existencia de un delito, identificar a sus responsables, reconstruir sus circunstancias o impedir la comisión de nuevos hechos delictivos. Paralelamente, el desarrollo de tecnologías de cifrado y de mecanismos avanzados de autenticación ha permitido incrementar considerablemente la protección de la información frente a accesos no autorizados. El cifrado constituye una herramienta legítima y necesaria para la protección de la privacidad, las comunicaciones y la seguridad de las personas, las empresas y las instituciones públicas.

Sin embargo, estas mismas tecnologías pueden impedir el acceso a información respecto de la cual los órganos de persecución penal han obtenido legítimamente facultades de investigación. En particular, es posible que un teléfono móvil, computador u otro soporte sea legalmente incautado y que, no obstante existir autorización para examinar su contenido, la información permanezca inaccesible debido a la utilización de contraseñas, códigos de acceso, claves criptográficas o mecanismos equivalentes.

Esta circunstancia genera una asimetría entre las facultades que el ordenamiento jurídico reconoce formalmente a los órganos encargados de la investigación penal y su posibilidad material de ejercerlas. La autorización judicial para registrar o examinar determinada información pierde eficacia cuando quien controla la clave que permite acceder a ella puede frustrar definitivamente la diligencia mediante su sola negativa a proporcionarla.

II. LEGISLACIÓN CHILENA

El Código Procesal Penal contempla actualmente diversas medidas destinadas a obtener evidencia digital. Su artículo 217 regula la incautación de objetos y documentos relacionados con el hecho investigado o que pudieren servir como medios de prueba.

Asimismo, el ordenamiento jurídico contempla reglas especiales relativas a la conservación de datos informáticos, interceptación de comunicaciones y registro remoto de equipos informáticos. En particular, el artículo 225 quinquies del Código Procesal Penal establece un deber de colaboración de determinados prestadores de servicios y responsables de sistemas informáticos respecto de la ejecución de medidas de acceso remoto y obliga a prestar la asistencia necesaria para que los contenidos obtenidos puedan ser examinados y visualizados.

No obstante dichos avances, la legislación chilena carece de una regla general que permita exigir a una persona que conoce la contraseña, clave o mecanismo de descifrado de determinados datos que lo entregue o lo ponga en ejecución, así como de una consecuencia penal específica para quien deliberadamente se niegue a cumplir dicho requerimiento.

III. EXPERIENCIA FRANCESA

El derecho francés contempla una solución particularmente clara a este problema.

El artículo 434-15-2 del Código Penal francés sanciona a quien, teniendo conocimiento de la convención secreta de descifrado de un medio de criptología susceptible de haber sido utilizado para preparar, facilitar o cometer un crimen o delito, se niegue a entregar dicha clave a las autoridades judiciales o a ponerla en ejecución cuando sea requerido por ellas.

La legislación francesa contempla además una hipótesis agravada cuando la entrega o utilización de la clave habría permitido evitar la comisión de un delito o limitar sus efectos.

La obligación no se limita a terceros. Conforme a la interpretación de los tribunales franceses, puede imponerse también a la propia persona sospechosa de haber participado en el delito investigado.

En 2018, el Consejo Constitucional francés declaró conforme con la Constitución esta disposición. Para ello consideró, entre otros elementos, que la obligación sólo puede imponerse cuando se encuentra establecido que la persona conoce la clave requerida; que su objeto no consiste en obtener una confesión; que la entrega de la clave no supone por sí misma un reconocimiento de culpabilidad; y que la información descifrada existe con independencia de la voluntad de la persona requerida.

Posteriormente, la Corte de Casación francesa precisó que el código utilizado para desbloquear un teléfono móvil puede constituir una clave de descifrado cuando su utilización permite poner en claro los datos cifrados contenidos en el dispositivo o aquellos a los cuales éste permite acceder.

El presente proyecto recoge dicha experiencia y adapta sus elementos esenciales al sistema

procesal penal chileno.

IV. DECISIÓN DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS EN MINTEH C. FRANCIA

El 19 de mayo de 2026, el Tribunal Europeo de Derechos Humanos resolvió el caso Minteh c. Francia (dec.), solicitud N°23624/20, relativo a la condena penal de una persona que, durante su detención policial por hechos vinculados al tráfico de drogas, se negó a comunicar los códigos de acceso de sus teléfonos móviles.

En relación con el artículo 6 del Convenio Europeo de Derechos Humanos y el derecho a guardar silencio, el Tribunal destacó que el artículo 434-15-2 del Código Penal francés no tiene por finalidad obtener una confesión ni establece una presunción de culpabilidad, sino permitir el descifrado de datos y facilitar la investigación de infracciones penales. Asimismo, consideró relevantes las garantías que rodean la aplicación de la norma: la intervención de una autoridad judicial, la información al requerido de que su negativa puede dar lugar a una persecución penal, la acreditación de la utilización del dispositivo en relación con la infracción investigada y la demostración de que la persona requerida conoce efectivamente la clave de descifrado. Sobre esa base, concluyó que no existía apariencia de vulneración del derecho a guardar silencio.

Respecto del derecho a no contribuir a la propia incriminación, el Tribunal reconoció expresamente que la amenaza de una sanción penal por negarse a entregar la clave constituye una medida de coerción. Sin embargo, estimó que, para determinar la aplicación de esta garantía, debía atenderse a la información que las autoridades pretendían obtener mediante dicha coerción. A juicio del Tribunal, el objeto último del requerimiento no era la clave de descifrado considerada aisladamente, sino los datos almacenados en los teléfonos.

El Tribunal observó que los dispositivos ya habían sido incautados y se encontraban en poder de la policía, y que los datos estaban previamente fijados en ellos y podían, al menos potencialmente, ser obtenidos mediante procedimientos técnicos aun sin la cooperación del requerido. Por consiguiente, concluyó que esos datos existían independientemente de la voluntad del imputado. De ello derivó que el privilegio contra la autoincriminación no resultaba aplicable a dichos datos y declaró este aspecto de la solicitud manifiestamente infundado.

En consecuencia, Minteh c. Francia constituye un antecedente especialmente relevante para la presente iniciativa. La decisión respalda, bajo el artículo 6 del Convenio Europeo, la posibilidad de sancionar al propio imputado por negarse a entregar o ejecutar una clave de descifrado cuando la medida persigue acceder a datos preexistentes e independientes de su

voluntad.

V. FUNDAMENTOS DE LA INICIATIVA

El proyecto se sustenta en una distinción fundamental entre obligar a una persona a declarar acerca de los hechos investigados y exigirle la realización de una actuación destinada a hacer accesible evidencia que existe con independencia de su voluntad.

El derecho a guardar silencio protege al imputado frente a la obligación de prestar declaraciones autoincriminatorias. No debe, sin embargo, transformarse en una facultad para impedir materialmente la ejecución de una diligencia de investigación legalmente autorizada respecto de información preexistente.

La contraseña o clave de descifrado cumple, para estos efectos, una función instrumental. Su entrega o puesta en ejecución no tiene por objeto obtener del imputado una explicación sobre los hechos, una confesión o una declaración acerca del contenido de la información. Su finalidad consiste exclusivamente en remover una barrera tecnológica que impide acceder a evidencia cuya obtención se encuentra jurídicamente autorizada.

Por esta razón, el proyecto establece expresamente que el cumplimiento de la orden de descifrado no constituirá declaración del imputado ni podrá ser utilizado, por sí mismo, para acreditar que éste es propietario del dispositivo, autor de los documentos o comunicaciones contenidos en él, o responsable de los hechos investigados. Lo anterior no impedirá, naturalmente, que la información legítimamente obtenida como consecuencia de la diligencia pueda ser utilizada como evidencia conforme a las reglas generales.

El proyecto contempla además que la obligación podrá satisfacerse tanto mediante la entrega de la clave como mediante su puesta en ejecución por la propia persona requerida. Esta segunda alternativa permite obtener el acceso a la información sin que necesariamente sea necesario incorporar permanentemente la contraseña o secreto criptográfico a los antecedentes de la investigación.

Asimismo, siguiendo directamente el modelo francés, se establece un delito autónomo de negativa a entregar o poner en ejecución una clave de descifrado. La figura será aplicable a cualquier persona, incluida aquella que tenga la calidad de imputado.

Finalmente, se contempla una hipótesis agravada cuando la colaboración requerida habría permitido impedir la comisión de un crimen o limitar sus consecuencias.

En mérito de lo anterior, venimos en presentar el siguiente:

PROYECTO DE LEY

Artículo primero. - Introdúcense las siguientes modificaciones en el Código Procesal Penal:

1. Incorporase, a continuación del artículo 217, el siguiente artículo 217 bis:

"Artículo 217 bis. - Entrega o puesta en ejecución de claves de descifrado. Cuando durante una investigación penal relativa a un crimen apareciere que datos contenidos en un dispositivo, computador, sistema informático, soporte de almacenamiento, cuenta, servicio informático o cualquier otro medio tecnológico se encuentran cifrados o protegidos mediante una contraseña, código, clave criptográfica, mecanismo de autenticación o cualquier otra medida tecnológica que impida acceder a ellos o comprender su contenido, el Ministerio Público podrá solicitar al juez de garantía que ordene su entrega o puesta en ejecución.

El juez podrá autorizar la medida cuando existieren antecedentes que permitan presumir fundadamente:

a) que los datos cuyo acceso se pretende guardan relación con el crimen investigado, con sus circunstancias o con la participación de una o más personas en él;
b) que la persona requerida conoce, posee o controla la contraseña, código, clave o mecanismo necesario para acceder a los datos, y
c) que el dispositivo, sistema, soporte o información respectiva ha sido legítimamente incautado, obtenido o sometido a una medida de investigación autorizada conforme a la ley.

La resolución podrá ordenar a cualquier persona, incluida aquella que tenga la calidad de imputado en la investigación, entregar la contraseña, código, clave criptográfica o mecanismo equivalente o, alternativamente, ponerlo directamente en ejecución de manera que permita obtener el acceso a la información o su versión inteligible.

La orden podrá comprender mecanismos de autenticación basados en conocimientos, elementos físicos, dispositivos de autenticación, características biométricas o cualquier otro procedimiento que permita obtener acceso a los datos protegidos.

La persona requerida será apercibida expresamente de las consecuencias penales establecidas en el artículo 269 quáter del Código Penal para el caso de negativa injustificada.

El cumplimiento de la orden no podrá ser utilizado, por sí solo, como reconocimiento o confesión acerca de la propiedad o posesión del dispositivo o sistema, de la autoría de los datos o comunicaciones contenidos en él, de su conocimiento por parte del requerido o de la participación de éste en el hecho investigado. Esta disposición no impedirá la utilización,

conforme a las reglas generales, de los datos, documentos, comunicaciones y demás antecedentes obtenidos como consecuencia del descifrado.

Cuando el requerido alegare desconocer la contraseña, código, clave o mecanismo correspondiente, corresponderá acreditar su conocimiento efectivo para efectos de establecer la responsabilidad penal prevista en el artículo 269 quáter del Código Penal.

2. Agrégase, en la letra g) del artículo 93, a continuación del punto final, que pasa a ser punto seguido, la siguiente oración:

"El derecho establecido en esta letra se entiende sin perjuicio del deber de cumplir la orden prevista en el artículo 217 bis, la que no tendrá el carácter de declaración para los efectos de este Código/'

3. Agregase, en el artículo 225 quinquies, el siguiente inciso final:

"Cuando la asistencia requerida para la ejecución de la medida suponga la utilización de una contraseña, código, clave criptográfica, convención secreta de descifrado o mecanismo equivalente que se encuentre en conocimiento, posesión o control de alguna de las personas señaladas en este artículo, podrá ordenarse su entrega o puesta en ejecución en conformidad al artículo 217 bis/'

Artículo segundo.- Incorporase en el § II bis del Título VI del Libro Segundo del Código Penal, a continuación del artículo 269 ter, el siguiente artículo 269 quáter:

"Artículo 269 quáter.- El que, teniendo conocimiento de una contraseña, código, clave criptográfica o cualquier otro mecanismo de acceso correspondiente a un medio de criptología o mecanismo de autenticación susceptible de haber sido utilizado para preparar, facilitar o cometer un crimen, se negare injustificadamente a entregarlo a la autoridad competente o a ponerlo en ejecución, habiendo sido requerido para ello en conformidad al artículo 217 bis del Código Procesal Penal, será castigado con presidio menor en su grado medio y multa de cincuenta a cien unidades tributarias mensuales.

La calidad de imputado por el crimen respecto del cual se hubiere formulado el requerimiento no eximirá de responsabilidad conforme al inciso precedente.

Si la negativa se produjere en circunstancias en que la entrega o puesta en ejecución de la contraseña, código, clave o mecanismo de acceso hubiere permitido evitar la comisión de un crimen o limitar sus efectos, la pena será de presidio menor en su grado máximo y multa de cien a doscientas unidades tributarias mensuales.

Incurrirá en las mismas penas del inciso primero quien, con conocimiento de la orden y con el propósito de impedir o dificultar su ejecución, proporcione una contraseña, clave o mecanismo falso o deliberadamente inoperante.

Si después de haber sido notificado del requerimiento el obligado destruyere, eliminare, alterare o hiciere inaccesibles los datos, claves o mecanismos comprendidos en la orden, la pena señalada en el inciso primero se aumentará en un grado, sin perjuicio de las penas que correspondieren por otros delitos."