

Ambiente legal

Ricardo Posada Maya

¿Es integral la protección jurídico penal por intrusión informática para titulares de información reservada?

Cuando se aborda el estudio de la responsabilidad penal por intrusión informática, desde la perspectiva de la legislación vigente, se advierte que el Código Penal colombiano (Ley 599 de 2000) se aproxima de manera parcial a dicha fenomenología criminal.

En efecto, si se observan las diversas conductas que consagra el artículo 195 del estatuto punitivo, que regula el tipo penal doloso de *'acceso abusivo a sistema informático protegido con medida de seguridad'*, queda el amargo sinsabor, no solo que se regula una figura muy imperfecta desde el punto de vista de la técnica científica, sino también de la ausencia de criminalización de ciertos comportamientos que, en principio,

se deberían sancionar por la vía de la omisión propia, bajo supuestos especiales en el mundo de la era digital.

Para ilustrar dicha afirmación, es válido preguntar si debería quedar sin sanción jurídicopenal, aquella hipótesis en la que el médico, que previamente ha decidido almacenar toda la información confidencial de sus pacientes en un ordenador personal, no impide a terceros extraños el acceso a dicho sistema informático, precisamente, por omitir disponer de forma dolosa o imprudente (Art. 21 y ss.) las medidas de seguridad informáticas básicas necesarias para evitar dicha intrusión y la probable afectación, no sólo de la información sino también de la intimidad de sus pacientes; o por disponerlas de manera insufi-

ciente, inadecuada o inidónea para proteger dicho sistema informático y los datos o la información informatizada contenida en él.

Si se analiza con detenimiento el caso anterior, todo indica que dicha situación de intrusión resulta impune. No solo porque los terceros intrusos no responden por el supuesto típico vertido en el artículo 195 *ibidem*, sino también porque el galeno no resulta penalmente responsable, atendidas las restricciones derivadas del principio de legalidad (Arts. 9, 10 y 25), que exige consagrar de forma expresa los delitos de omisión propia o de pura omisión.

Ello, con independencia de que las conductas posteriores de los intrusos sean susceptibles de adecuación a otras tipicidades -*incluso subsidiarias*- referidas, por ejemplo, a la divulgación o al empleo comisivo doloso en provecho propio o ajeno del contenido de documentos -electrónicos- reservados (Art. 194²), que precisamente se han obtenido mediante el acceso abusivo, o a tipicidades similares a ésta, aunque orientadas a proteger bienes jurídicos diferentes a la intimidad personal, como el orden económico social o la seguridad y existencia del Estado.

En cualquier caso, dicha afirmación implica verificar, en concreto, algunos matices que entraña el caso propuesto.

Responsabilidad por intrusismo informático activo

Para nadie es un secreto que el fundamento material de incriminación de la conducta de acceso abusivo a sistema informático protegido, reside en que dicha conducta dolosa pone en peligro las condiciones de privacidad de los datos o la información contenida en el sistema informático o en la red de comunicación electrónica de datos, al carecer del consentimiento del titular o administrador del sistema para la lograr una conexión normal (Art. 32).

Situación que genera -en concreto- un peligro próximo para la confiabilidad, la disponibilidad e integridad de la información, y en el caso específico propuesto, un peligro mediato para la intimidad de los pacientes, que ven en riesgo de exposición -*con infracción al principio de confianza*- información personal de naturaleza sensible y reservada. Es decir, información que claramente los pacientes se han reservado a su esfera íntima de conocimiento³, desde la perspectiva del bien jurídico más general de la libertad individual

(Capítulo séptimo del Título III, Libro II del Código Penal; y Constitución Política, art. 16). Y, que solo por razones evidentes y limitadas está en posesión de un tercero, que legalmente tiene el deber de proteger la confidencialidad de la información, y garantizar que no se presenten riesgos de intrusión indebidos que puedan lesionar los derechos fundamentales o que desemboquen en lesiones penales típicas.

Así las cosas, el tipo penal de peligro en abstracto⁴ bajo análisis consagra desde un punto de vista estructural, dos conductas de naturaleza alternativa⁵ que, claramente, no exigen que el intruso: i) acceda abusivamente al sistema informático protegido con medida de seguridad, con alguna finalidad ilícita concreta y, ii) que el sujeto alcance algún grado de disponibilidad sobre datos o informaciones informatizadas, para realizar actividades delictivas posteriores.

Desde luego, el tipo penal del art. 195 cuenta con fallas importantes frente al bien jurídico tutelado, que no pueden ser desconocidas, pues el mero acceso en sentido jurídico, no parece afectar directamente a la intimidad, sin que dicha conducta implique otras actuaciones y finalidades ilícitas adicionales (escarbar información, obtener

datos, etc.) que indiquen *-objetivamente- el peligro en la órbita que cada persona se ha reservado*; y no simplemente una infracción contra la seguridad de la información.

Ahora bien, en el caso concreto propuesto, el sistema dispuesto por el médico para efectos de almacenar la información carece de cualquier clase de medida de seguridad.

En este orden de ideas, lo que desde el punto de vista ordinario implicaría una intromisión inaceptable a la intimidad y a la libertad por parte de terceros; desde la perspectiva del Derecho penal se descarta como una hipótesis de acceso abusivo al no quedar cobijado por el ámbito de protección del tipo delictivo vertido en el artículo 195 del Código penal, toda vez que el legislador penal exige, de manera acertada, que el objeto sobre el cual recae la acción del sujeto (el sistema informático), deba estar protegido con medidas de seguridad.

Para el Derecho Penal colombiano, entonces, no basta una mera intrusión, pues es necesario *-en el contexto típico-*, que los intrusos realicen manipulaciones dolosas orientadas a quebrantar o a superar dichas medidas de seguridad informáticas, para

luego 'ingresar' o acceder sin obstáculos al sistema, programa, módulo informático o base de datos, con lo cual se disminuye la posibilidad de defensa de los titulares del sistema y de la información en sí misma considerada.

En este punto, es importante abordar tres preguntas fundamentales.

¿Por qué el legislador condiciona la conducta delictiva a sistemas informáticos protegidos?

De manera muy breve, se puede afirmar que tal exigencia típica se puede explicar, de manera más o menos satisfactoria, desde el punto de vista legal. En efecto, la información es un bien inmaterial que, salvo previsión legal expresa en contrario, es de libre disposición por parte de su titular. Naturalmente, cuando le concierne a su propia personalidad o cuando el sujeto tenga autorización legal para su divulgación. AQUIAQUIAQUI

Con ello se quiere indicar, que será la misma persona natural o jurídica quien deba decidir *-asumiendo las consecuencias derivadas de ello-*, si desea o no que la información informatizada constituya un secreto, sea información de conocimiento restringido o privilegiado, o sea información de conocimiento público

o general. Desde luego, considerada la naturaleza misma del contenido de la información, pues en algunos eventos -por razones de interés general- la ley prescribe la calidad que debe poseer la información pública (como sucede en los casos de información informatizada que concierne a la seguridad nacional, a operaciones de inteligencia militar o policial del Estado, entre otras).

Así mismo, de conformidad con la naturaleza asignada a la información informatizada privada, será el mismo titular de derechos quien deba *-en principio-* asegurarse desde una perspectiva objetiva, que se cumpla con la calidad otorgada a la información informatizada frente a terceros. Y entiende el legislador penal, que ello se logra con medidas de autoprotección informática que limiten *-de manera efectiva-* el acceso de intrusos a los sistemas informáticos o a las redes electrónicas de datos. Se trata, pues, de un adelantamiento en las barreras de protección a los datos o a la información informatizada, que colateralmente protege bienes jurídicos tradicionales, cuya efectividad real depende del titular de derechos.

De otro lado, la libertad de protección objetiva sobre la infor-

mación, naturalmente tiene excepciones como bien inmateria de libre disposición, cuando la información informatizada o los datos no se encuentren en el ámbito de dominio específico de su titular. En estos casos, es decir, cuando la información que los sujetos entienden como reservada o privilegiada (según el caso) se encuentra en posesión de terceros (como el médico), el deber de protección material se traslada a ellos, con la obligación de adoptar las medidas de seguridad que, desde una perspectiva razonable, hubiese tomado su titular para garantizar la eficacia del ámbito de custodia y vigilancia de dichos intereses inmateriales.

¿Qué clase de medidas de seguridad informáticas deben adoptar los titulares de la información, para entender que se trata de un sistema informático realmente protegido?

En este punto la ley penal guarda silencio. Sin embargo, una interpretación literal de la norma resultaría irrazonable, pues bastaría entender que el sistema informático que cuenta con un simple *login* y un *password* o con simples advertencias referidas a la prohibición genérica de acceder sin la observancia de ciertas condiciones⁶, para calificar el sistema informático como realmente protegido; cuestión

que la técnica informática no considera actualmente como medidas de seguridad suficientes, para proporcionar una seguridad integral (para ello existen los firewell, los antivirus y otros programas informáticos adicionales).

En este orden de ideas, las medidas adoptadas por el titular o por el administrador del sistema informático, desde un punto de vista material, deben ser idóneas, adecuadas, explícitas y equivalentes como mínimo, a las medidas de seguridad sugeridas como consecuencia de la aplicación de los estándares nacionales e internacionales de gestión en seguridad informática '*lex informática*'; o a aquellas medidas o programas de seguridad empleados en el tráfico informático ordinario por los técnicos expertos en la materia⁷, atendida, desde luego, la importancia de la información almacenada, transmitida o procesada en el caso concreto.

Y ello es así, pues sería ilógico pensar que el legislador se conforma, para proceder al castigo del acceso abusivo, con que el titular disponga medidas de seguridad ineficaces u obsoletas, precisamente, porque ello implicaría lo contrario a la norma, proteger sistemas informáticos

desprotegidos dolosamente por su titular. En efecto, mientras más sensible sea la información, mayores deben ser las medidas de seguridad dispuestas para su 'protección' real, todavía más, cuando jurídicamente se esté obligado a ello.

¿Cuál es la consecuencia jurídica de no tomar medidas de seguridad informáticas eficaces para proteger el sistema?

La respuesta, de cara al caso propuesto, es evidente: Los terceros que 'acceden' al sistema informático del médico no responden jurídico penalmente, aun cuando hayan colocado en peligro efectivo la información y, de manera remota, la intimidad de los pacientes. Y ello es así, pues el médico -titular del sistema informático y tenedor legítimo de la información- al omitir dichas medidas de seguridad, ha autopuesto en riesgo el sistema y la información de sus pacientes (suicidio informático), con infracción dolosa (o imprudente en su caso) del cuidado legal debido a la reserva y confidencialidad que ha debido tener. Ello implica que el riesgo para la intimidad de los pacientes quede impune, por atipicidad de la conducta frente al Art. 195 *ibidem*.

Así las cosas, el médico mismo ha descalificado objetivamente la naturaleza reservada de la

información almacenada (su integridad, confiabilidad y disponibilidad), violando la confianza de sus pacientes, pues, para el legislador penal el acceso de terceros en dichas condiciones, bien o mal, tiene la misma trascendencia jurídica que un 'ingreso' a un sistema informático de acceso público. Discutible o no, esa es la consecuencia que se desprende de la infracción de las normas de cuidado informático.

Hacia una protección integral de los titulares de información privada sensible

Del caso propuesto queda algo claro: en términos absolutamente pragmáticos, el responsable directo de la desprotección de la información informatizada confidencial de los pacientes, ha sido el propio titular del sistema informático. Si los terceros conocen indebidamente la información, no serán responsables penalmente.

De otro lado, el médico tampoco responderá penalmente, pues dicha omisión no es punible y el delito de divulgación de secreto es de naturaleza comisiva o activa y no de naturaleza omisiva o pasiva (Art. 194 y Arts. 10 y 25). Sólo será autor de este último hecho, en tanto y en cuanto dolosamente le divulgue directamen-

te a los terceros la información confidencial de sus pacientes.

De ello se desprenden las siguientes preguntas: Si el médico, al no disponer de salvaguardas, ha sido quien ha infringido de forma dolosa o imprudente el deber de protección y de confidencialidad de la información informatizada de naturaleza sensible de los pacientes, que adicionalmente ven en peligro su intimidad por la conducta impune de terceros: *¿Debe quedar el médico exento de toda responsabilidad penal por el peligro que ha generado frente a la información y la intimidad? ¿Sí los intrusos posteriormente divulgan la información, el médico será una simple víctima desde la perspectiva del Derecho penal?*

La respuesta a dicha cuestión no es sencilla. En principio, si se tiene en cuenta que la sola tenencia legítima de datos o de información de terceros (bancos de datos financieros, contables, etc.) constituye una modalidad de 'actividad peligrosa'⁸, no parece descabellado desde el punto de vista político criminal, que la doctrina penal comience a prever la posibilidad jurídica de configurar -en el futuro- tipos penales de peligro, bien por la omisión del control debido en la gestión de seguridad informática referi-

da a las actividades de almacenamiento, procesamiento o transmisión de datos o información de naturaleza sensible de terceros; o por la adopción de medidas de seguridad y sistemas de salvaguarda irrisorios o inapropiados para proteger la seguridad, integridad, confiabilidad y disponibilidad de datos o informaciones sensibles de regulación controlada legalmente.

Ello, para evitar claramente la completa indefensión de terceros que carecen de la custodia y vigilancia de su información sensible (o de población protegida), castigando los atentados claros contra la *seguridad colectiva o pública de la información*'.

Finalmente, es necesario advertir que esta clase de modalidades delictivas ya existen en el ordenamiento punitivo colombiano, por la vía del castigo de la omisión de control en materia de lavado de activos⁹. Con lo cual, de forma preliminar, no existiría ningún impedimento estrictamente técnico-dogmático para configurarlas en su modalidad dolosa; sin que ello signifique que estén dadas -necesariamente- las condiciones político-criminales para hacerlo en su modalidad imprudente, pues en estos casos parece suficiente la

responsabilidad civil y ética del titular del sistema informático.

En conclusión, se ha hecho evidente que la protección jurídico penal en materia de intrusión informática no es integral, de cara a la protección del derecho fundamental a la intimidad, cuando terceros poseen o administran información de naturaleza sensible, almacenada en sistemas informáticos que carecen de medidas de salvaguarda, precisamente, por omisión dolosa de los titulares o administradores del sistema informático intrusado.

NOTAS

¹Art. 195: "El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa". Dicha conducta tiene referente en el CP. español, art. 197.2, apt. 2º, cuando indica que se impondrán las penas previstas en el art. 197.1, "...a quien, sin estar autorizado, acceda por cualquier medio a los mismos...", es decir, cuando se acceda sin autorización en ficheros o soportes

informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado que contenga datos reservados de carácter personal o familiar. De otro lado, el CP. Federal de México regula los delitos de acceso ilegal a los sistemas informáticos en los arts. 211 Bis 1 al 211 bis 7 y en la Ley 2002-67 de Comercio electrónico, firmas electrónicas y mensajes de datos (Registro Oficial 557-S, 17-IV-2002), arts. 58 a 64; La ley 19223 de 1993 de Chile, art. 2º, consagra como delito el acceso, con ánimo de usar o conocer de forma indebida la información contenida en un sistema de tratamiento de información (con lo cual congloba las posibles afectaciones generales a la intimidad o confidencialidad de la información oficial); el CP. Suizo castiga dicha conducta en el art. 146bis.; el CP. francés, mod. Ley 92-683 de 1994, la sanciona en el art. 323-1; el StGB. alemán en el § 202a; el CP italiano en el art. 615-tercero. De otro lado, dicha conducta tiene referente en la Convención de Budapest del 23.22.2001, ob. cit., Cáp. II, Sección I, art. 2º "Acceso ilegal" que, entre otras cosas, demanda el propósito (elemento subjetivo especial distinto del dolo) de obtener datos del computador o realizar cualquier otro intento deshonesto.

En www.acis.org.co aparecen completas las notas de pie de página y la bibliografía.

Ricardo Posada Maya. Abogado de la Universidad Pontificia Bolivariana (Medellín). Especialista en Derecho penal de la Universidad de Antioquía. Magíster (DEA) en Derecho penal por la Universidad de Salamanca -España. Candidato a Doctor por la misma Universidad. Actualmente, se desempeña como Profesor de Planta de la Universidad de los Andes, y regenta las cátedras de Constitución & Democracia, Derecho penal general y especial.