"El tipo penal de acceso abusivo a un sistema informático -art. 269 A del C.P.-, ha sido reconocida por la doctrina como *"hacking directo o mero intrusismo informático"*, es decir, *"conductas de meros accesos y/o permanencias perpetradas con el único fin de vulnerar un password o una puerta lógica que permite acceder a sistemas informáticos o redes de comunicación electrónica"*[1]*:*

En ese orden, el tipo penal está conformado i) por un sujeto activo que no es calificado por no necesitar de una condición especial para quien accede a un sistema informático *"sin autorización",* o que, teniéndola, decide conscientemente mantenerse conectado;

ii) por un sujeto pasivo, que es la persona natural o jurídica titular del sistema informático;

iii) por lesionar varios bienes jurídicos tutelados, entre ellos, la información, los datos y la intimidad, ha sido reconocido como un tipo penal pluriofensivo;

iv) solo admite el dolo en el actuar del ciberdelincuente;

v) es un delito de mera conducta, por cuanto, la sola intromisión en una red informática, en las condiciones establecidas en el tipo penal, afecta el bien jurídico tutelado;

vi) contempla dos verbos rectores, acceder o mantener;

vii) como ingrediente normativo, exige que el sujeto activo de la acción a) *acceda* en el sistema informático sin autorización, o, b) aun cuando, teniendo el permiso del titular legítimo del derecho, se *mantiene* dentro del mismo, excediendo las facultades otorgadas.

Respecto de la primera forma de actuar del ciber-delincuente, no reviste mayor complejidad, por cuanto, resulta suficiente la introducción ilegítima sin la voluntad del titular de la cuenta.

El problema surge con la segunda manera de actuar, en tanto, el ingrediente normativo que la contiene está enfocado a establecer cuáles serían los límites de esa autorización que desbordaría el tipo penal estudiado.

En las condiciones anotadas, se entrará a examinar si, en efecto, el acusado *accedió* al sistema informático del banco sin la debida autorización o si, teniendo el permiso del titular legítimo del derecho, se *mantuvo* dentro del mismo, excediendo las facultades otorgadas.

Lo primero que debe señalarse es que, conforme con el acuerdo de voluntades al que llegó el acusado con la organización, su aporte en la empresa delincuencial, consistió en acceder a las cuentas bancarias de los demás integrantes de la banda y verificar el momento en que los títulos valores hicieran canje, por lo que, una vez establecida la

liberación de cupos, procedían a realizar transacciones o a retirar el dinero.

De esa manera, se precisa que el acusado, como informador del banco, tenía la posibilidad de acceder a la cuenta de los usuarios siempre y cuando cumpliera con algunos de los requisitos establecidos en el manual de autenticación de clientes, entre los que se encontraba contar con la presencia del legítimo titular del derecho.

Para el efecto, cobran relevancia las declaraciones de los funcionarios del banco, al señalar que, en cumplimiento del manual de autenticación de los clientes, establecido en la entidad, los informadores sólo podían acceder a las cuentas de los usuarios en el horario de atención al cliente, cuando éstos se encontraran presen- tes en la entidad realizando sus transacciones.

En ese orden, resulta preciso establecer si cuando el acusado, entre enero de 2010 y enero de 2011, accedió más de trescientas veces a las cuentas bancarias de los integrantes de la organización criminal, como lo sostuvieron los investigadores, incurrió con su actuar en el delito de acceso abusivo a un sistema informático, con forme los hechos de la acusación.

De acuerdo con el señalamiento que estos últimos hicieron, las consultas realizadas por el acusado aunque ocurrieron cuando éste cumplía funciones de informador y en su horario de trabajo de 9 am., a 4 pm, no por

ello se descarta, como la defensa lo sugiere, la antijuridicidad de la conducta, dado que como el bien jurídico tutelado es la información y los datos, de igual manera puede éste resultar vulnerado, cuando a ellos se accede para cumplir propósitos ilícitos como en este caso.

De esta suerte que, aunque el funcionario se encontrara cumpliendo sus labores en su jornada laboral, es posible vulnerar bienes jurídicos protegidos por la norma, por cuanto el reproche punitivo se presenta en los dos eventos claramente establecidos, bien cuando el ciber-usuario accede a los sistemas sin estar autorizado o, estándolo, decide permanecer en ellos con fines delictuales.

En este caso, el acusado pretextando veladamente que no infringía el manual de autenticación del cliente, ingresó de manera reiterada a las cuentas bancarias de quiénes igualmente hacían parte de la organización criminal, con el objeto de cumplir la labor que el grupo delincuencial le había asignado, sin que para el trámite que le competía realizar al interior de la entidad se requiriera de la presencia del cliente, como la defensa lo esgrime.

Es lo cierto que según el acuerdo de voluntades que con el grupo delincuencial había llegado, el informador contaba con la anuencia explícita del cliente para acceder a las plataformas virtuales, aprovechando además que, poseía las claves que la propia entidad le había suministrado para a ellas ingresar solo en cumplimiento de su función, de tal suerte que, al utilizarlas para los intereses del grupo criminal, de entrada, vulneraba el bien jurídico de la información y los datos.

Bajo esos lineamientos, la Fiscalía sí logró acreditar que el acusado en atención al número de incursiones efectuadas en las cuentas de tres de los miembros de la banda, perfeccionó el delito de acceso abusivo a sistema informático, que tuvo como finalidad, como ya se ha venido indicando -en cumplimiento de los acuerdos de voluntades-, mantenerlos al tanto del momento en que la operación fraudulenta se podía realizar por la falla técnica en los sistemas.

No cabe duda que el actuar del acusado, al ingresar desmedidamente a la cuenta de uno de los mayores defraudadores del banco, no se corresponde con el normal desarrollo de su actividad como informador, sino con un actuar ostensiblemente doloso tendiente a favorecer a la banda de la que hacía parte, proceder éste que repercutió en los intereses de la entidad, al utilizar a su antojo la contraseña y el usuario que sólo le permitía ingresar a la base de datos con propósitos lícitos.

De esta manera, sin justificación alguna, vulneró la información y datos privilegiados que la entidad bancaria sometía a la respectiva reserva y confidencialidad".(Corte Suprema de Justicia, Sala de Casación Penal, Sentencia: SP-592 del 02 de Marzo de 2022, Referencia: Rad. 50621).