PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Escuela de Posgrado

La responsabilidad de las entidades financieras ante la comisión de delitos informáticos

Trabajo de Investigación para obtener el grado académico de Maestro en Derecho Bancario y Financiero

que presenta:

Carlos Arturo Flores Jiménez

Asesor:

Ricardo Nicanor Elías Puelles

Lima, 2023

Informe de Similitud

Yo, ELÍAS PUELLES, RICARDO NICANOR, docente de la Escuela de Posgrado de la Pontificia Universidad Católica del Perú, asesor(a) de la tesis/el trabajo de investigación titulado LA RESPONSABILIDAD DE LAS ENTIDADES FINANCIERAS ANTE LA COMISIÓN DE DELITOS INFORMÁTICOS, del autor FLORES JIMENEZ, CARLOS ARTURO, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 26%. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el 21/08/2023.
- He revisado con detalle dicho reporte y la Tesis o Trabajo de Suficiencia Profesional, y no se advierte indicios de plagio.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha:

Lima, 5 de octubre de 2023

Apellidos y nombres del asesor / de la asesora: ELÍAS PUELLES, RICARDO NICANOR	
DNI: 4276970	Firma:
ORCID: 0000-0002-1257-1674	

RESUMEN EJECUTIVO

La presente investigación referente a la responsabilidad de las entidades financieras ante la comisión de delitos informáticos se justifica en primer lugar, ante el contexto en que nuestro país se ha visto desde hace años recientes, adecuándose al avance de la digitalización en muchos ámbitos, entre ellos en materia financiera. Estos cambios, acelerados por la Pandemia, implicó situaciones y consecuencias jurídicamente imprevistas y no reguladas, en especial las de naturaleza antijuridica, como lo son los delitos informáticos. Dichas falencias son advertidas e identificadas, planteándose respuestas en base al análisis del plano conceptual de la teoría del delito, al derecho nacional y comparado, así como el análisis de las figuras penales pertinentes y conexas, los actuales protocolos y metodologías que las entidades financieras puedan aplicar para la prevención de delitos informáticos. Así como definir el rol de las entidades financieras y su responsabilidad en un contexto de delito informáticos, y el impacto de estos en el ámbito financiero, nos permitirá contar con un marco normativo más consolidado. Estas respuestas por supuesto, sustentadas tanto desde el punto de vista jurídico, así como de otros factores empíricamente constatables sobre esta problemática. Por ello, teniéndose en cuenta los recientes acontecimientos sucedidos en especial en este año, los cuales son mencionados en este trabajo, y la constante evolución de estos delitos y sus modalidades aplicados al ámbito financiero, se pone en evidencia la relevancia y total vigencia sobre este tema.

Palabras Clave: Fraude informático; Normativa; Prevención; Suplantación de Identidad; Tráfico Ilegal de Datos Personales.

ÍNDICE

INTRODUCCIÓN:

La presente investigación versa sobre la búsqueda de respuestas a la responsabilidad de las entidades financieras ante la comisión de delitos informáticos. Primeramente, dentro del plan de trabajo se desarrollará el contexto por el cual se plantea la relevancia y justificación del tema de estudio, esto en base a la evidencia empírica obtenida de las instituciones correspondientes, en donde se pone de manifiesto que los delitos informáticos, siendo suplantación de identidad y fraude informático entre los más relevantes en materia financiera han ido en aumento paulatinamente en años recientes debido a diversos factores relevantes, como la realidad nacional y la conjunción de otros delitos que paulatinamente han ido favoreciendo a la criminalidad informática. Siendo que su crecimiento se agudizo durante la etapa inicial de la cuarentena, lo cual se dio por producto de la pandemia iniciada en el Perú y el mundo a principios del año 2021. De otro lado, tenemos al planteamiento de las hipótesis, la presentación del problema de investigación central y la búsqueda de sus respuestas en virtud de todo lo investigado, así como también tomando de insumo lo que la literatura especializada nos ha podido ofrecer.

Ya en el primer capítulo en el marco teórico propiamente dicho se estudiará y analizará las características propias tanto del delito base. Nos apoyaremos en las definiciones propias de los distintos autores sobre la materia, así como también se explorarán los conceptos de dolo y culpa, el bien jurídico protegido, etc. De otro lado se hará énfasis en la premisa de la responsabilidad que debe tener entidad financiera en su rol como institución que busco prevenir y combatir esta clase de delitos dentro de su competencia, en base a la toma de todas las debidas diligencias, garantizando la máxima seguridad informática, en beneficio de sus usuarios. De otro lado, se analiza si es posible considerar jurídicamente reprochable el actuar negligente de una entidad financiera en materia de ciber seguridad en perjuicio de sus clientes, en base a las denuncias, quejas de los usuarios, así como lo demostrara la evidencia empírica obtenida por fuentes oficiales. Todo ello buscará definir la necesidad de la existencia de un marco legal de carácter sancionatorio que enfatice y obligue a las entidades financieras a garantizar la ciberseguridad dentro de su actividad en el mercado peruano.

En el segundo capítulo se verá el desarrollo normativo sobre este delito en la legislación nacional desde sus inicios hasta lo más actual. Estudiando las modificaciones normativas y la relevancia de las mismas, a su vez en el apartado del enfoque metodológico me enfocare en el mismo estudio para la legislación chilena para posteriormente hacer la adecuada comparación entre ambas legislaciones, respecto de políticas, criterios, doctrina, y nivel de eficacia y contenido de ambas normativas. Comparando los Pro y contras y que aspectos positivos de la estrategia legal asumida por la legislación chilena podría replicarse en la legislación peruana en materia de prevención de los delitos informáticos, los que sean relevantes en materia financiera por supuesto.

Ya en el tercer capítulo se pasará a analizar los distintos criterios respecto a la responsabilidad de las entidades financieras ante los casos de delitos informáticos relevantes en materia financiera tales como suplantación de identidad, fraude informático, tráfico ilegal de datos. A su vez que doy mi opinión respecto de los casos que involucran en específico a los delitos de suplantación de identidad, fraude informático y tráfico ilegal de datos personales; en donde analizando en base a la ley penal, si es posible atribuir responsabilidad penal a una entidad financiera y/o que otros tipos de responsabilidad se podrían plantear. Se plantearán posibles soluciones a nivel normativo a estas interrogantes. Por un lado, tomando de ejemplo lo visto en la legislación chilena; así como considerando las características del contexto peruano en materia de ciberseguridad en el ámbito financiero y en general. Asimismo, justificar por qué la lucha contra de los delitos informáticos, debe ser asumida como una política de prevención, y de adecuada gestión de información y supervisión. Se planteará algunos mecanismos para la consolidación de la misma; destacando las ventajas de invertir y darle prioridad a dichas políticas. Finalmente cierro esta investigación con mis conclusiones que incluyen recomendaciones.

Tema y contexto:

El tema a investigar versa sobre la responsabilidad de las entidades financieras ante la comisión de delitos informáticos, los relevantes a nivel financiero, tales como suplantación de identidad, fraude informático y tráfico ilegal de datos. En principio considero este tema relevante, en vista del crecimiento y la demandante dependencia del uso de las tecnologías de la información en la gran mayoría de actividades que se dan hoy en nuestro país. En ese orden de ideas, el mundo financiero ya viene adoptando a la tecnología dentro de sus propios procedimientos y demás protocolos, puesto que las ventajas que tecnología nos ofrecen son innegables. Tanto desde el ahorro de trabajo humano, o el ahorro de tiempos en el procesamiento de datos, así como la seguridad entre otros. Todo lo antes mencionado son apenas algunos de los puntos más importantes que convalidan la necesidad de seguir impulsando el uso de la tecnología en materia financiera. Lo cual implica necesariamente seguridad; en ese sentido en materia ciberseguridad, son generalmente tres los principales recursos a evaluar: la integridad, la confidencialidad y la disponibilidad de los datos y sistemas informáticos. Ahora bien, actualmente vivimos en un contexto en el cual el proceso de digitalización de la banca ha pasado de ser un escenario futurista, sobretodo en el caso peruano, a una realidad palpable. Dicha realidad se ha visto impulsada aún más en estos años recientes, como consecuencia de lo vivido durante la Pandemia mundial por el virus Covid-19 surgida a principios del año 2020.Y si bien, ya muchos países contaban con un considerable uso de la tecnología, el caso del Perú no era similar, pues aún predominaba mayoritariamente la dependencia del uso del papel. Por ello la llegada de la pandemia al Perú, significo un cambio de realidad notable, puesto que se tuvo que adoptar, de la noche a la mañana, el uso masivo de la tecnología en muy poco tiempo en distintas áreas, entre ellas, la financiera y comercial, esto sobretodo como consecuencia del distanciamiento social, las restricciones en el libre tránsito debido a la entonces expansión del Virus antes mencionado, lo cual como es sabido, impactó a todo el mundo.

Por lo tanto, conceptos como la virtualidad, la tecnología móvil, el comercio electrónico, compras en línea, sistema de delivery, transacciones bancarias por internet, por aplicativos y demás actividades relacionadas se vieron ampliamente demandadas en el Perú, mucho más que en comparación con otros países, quienes ya tenían más años de experiencia con la transición

tecnológica. Por lo que, a día de hoy, año 2023, nos hemos adaptado a estos cambios; sin embargo, dentro de esta era de modernidad y mayor dependencia tecnológica, fruto de las tendencias internaciones y por la pandemia, existe un tema pendiente a resolver, el cual concierne al elemento más importante, mencionado anteriormente: La ciberseguridad. Y es que, ante cualquier cambio en una realidad, la normativa debe adaptarse a dichas nuevas realidades. Sin embargo, muchas veces la norma termina quedando rezagada por dicha realidad, esto es una característica de la cual adolece nuestro derecho peruano, siendo que, si nos centramos en materia financiera, no es la excepción. El crecimiento y dependencia tecnológica en el sistema financiero, ha hecho necesario el poder contar con medidas de seguridad, pues los delitos informáticos al igual que delincuencia común, se renuevan constantemente, y justamente respecto de la delincuencia común, veremos en el transcurso de este trabajo, de que existen determinados delitos y realidades sociales que agravan la situación de inseguridad informática en materia financiera en el Perú.

En ese orden de ideas, el aspecto de la seguridad no solamente debe entenderse dentro del punto de vista tecnológico sino también sobre la gestión interna de dicha seguridad y por supuesto a nivel normativo. Por lo tanto, habrá que preguntase si realmente existe claridad y plena seguridad jurídica respecto de la responsabilidad que lleguen a tener las entidades financieras en su rol garantista de prevención de los delitos informáticos, relevantes en materia financiera. Por otro lado, entender que tan bien está definida dicha responsabilidad, tanto de los agentes que incurran en actos antijuridicos, así como en las entidades financieras, las cuales si bien en principio, las podemos considerar como sujetos pasivos de la figura, estos a su vez como entidades autorizadas, cuentan con un deber de garantizar la seguridad no solamente de los bienes económicos, sino también de la información financiera que está a cargo de ellas. Y para ello la vinculación normativa con el deber de garantizar dicha seguridad lo considero fundamental.

Adicionalmente, siendo conscientes de que la seguridad tecnológica recientemente ha empezado a afianzarse en nuestro país. Así como los distintos paquetes normativos y reglamentos de distintas instituciones respecto a la seguridad y la regulación de los delitos informáticos, será importante buscar las fórmulas legales que aseguren que la prevención de cierto tipo de delitos que están teniendo un gran impacto en nuestra realidad, en el ámbito financiero. Esto implica por supuesto que se encuentre en la agenda nacional a nivel político y gubernamental. Para ello será importante ver qué tipo de norma será la más adecuada para garantizar la prevención en materia

de ciberseguridad a nivel de nuestra sociedad. Siendo importante precisar que los delitos informáticos afectan distintos bienes jurídicos dependiendo de cada caso y contexto. En ese sentido, nos interesan los delitos informáticos solamente relevantes en materia financiera para una protección en dicha área. Y parte de esa protección implica por supuesto de que haya mayor claridad y desarrollo conceptual sobre los mismos. Regulando sus impactos y consecuencias.

Justificación:

En la actualidad, la normativa peruana no cuenta con regulación ni desarrollo legal óptimo ni concreto respecto del impacto que tienen los delitos informáticos en materia financiera, es decir, todas aquellas formas de utilización fraudulenta de sistemas y recursos informáticos mediante los cuales se puedan afectar tanto a los usuarios como al sistema financiero en general. Pues como es sabido, los delitos informáticos son de naturaleza múltiple, afectan distintos tipos de derechos, como la identidad, la intimidad, etc. Sin embargo, La ley especial, Ley 30096 Ley de delitos informáticos. No desarrolla en ninguno de sus apartados respecto de la afectación al sistema financiero ni de sus consecuencias. En el sentido de que lo contenido en la norma versa sobre la descripción de la conducta delictiva del sujeto activo, es decir el que delinque, no desarrolla mucho respecto del sujeto pasivo, la víctima. Lo cual es una característica típica de la ley penal, de dar más descripción a la conducta típica que comete el sujeto activo. Pero en el caso de afectación a una entidad financiera el escenario es distinto, pues a diferencia de la mayoría de casos, en donde contamos 2 actores: un sujeto activo y un sujeto pasivo; cuando se trata de afectaciones al sistema financiero mediante un delito, contamos en principio con 3 actores, en principio el sujeto activo (el ciberdelincuente); y 2 sujetos pasivos: el usuario (cuyo patrimonio fue mermado ilícitamente) y la entidad financiera (cuyo sistema informático ha sido vulnerado ilícitamente para afectar a un tercero, el usuario). La norma no menciona nada respecto del rol de las entidades financieras. Es decir, por un lado, no se advierte un desarrollo respecto de las consecuencias que tiene para una entidad financiera, como sujeto pasivo ante la afectación que sufra por parte de las figuras delictivas de suplantación de identidad, fraude informático o tráfico ilegal de datos (las relevantes en materia financiera). La norma solamente hace alusión a la afectación de “sistemas informáticos” de manera genérica.

Por otro lado, en el supuesto de que una entidad financiera si tuviese cierto grado de responsabilidad, en la afectación, ya sea por negligencia o cuando el sujeto activo llegase a cometer tales actos en colaboración de un integrante de la entidad. Dicha responsabilidad tampoco está definida. Es decir, la norma ni siquiera contempla esa posibilidad, como una situación agravante. Lo que evidencia indudablemente falta de regulación y desarrollo al respecto.

Problema de investigación:

Dentro de los problemas advertidos en esta investigación tenemos una serie de puntos como se verán a continuación.

La evidencia empírica:

Tal como se mencionó al inicio de esta investigación, el contexto vivido en nuestro país con la pandemia y cuarentena incremento exponencialmente los casos de delitos informáticos, en especial los de suplantación de identidad. Esto se debe en parte debido a que justamente entre los años 2020 y el 2022[1], la emergencia sanitaria vivida en nuestro país, una de las más duras del mundo en su momento, significó un cambio sustancial y abrupto en la manera en la que se daban las interacciones comerciales y económicas en el Perú. Pasando del trabajo presencial y el predominio del papel, hacia el trabajo remoto tanto a nivel móvil como informático. Este cambio abrupto por el cual ni el país ni la sociedad estaba preparadas fue el caldo de cultivo perfecto para la comisión de este delito por muchos ciberdelincuentes inicialmente, pero que luego incluso se dio por personas no necesariamente expertas en informática, pero que aprovechando vulnerabilidades o falencias de sistemas informáticos o de identidad sacaron redito de ello. Por ello la suplantación de identidad tuvo un mayor auge, junto al delito de fraude informático. Esto por supuesto con el contexto de la permanente existencia del delito de robo de celulares, lo cual facilita a los delincuentes a información sensible, sobretodo porque la digitalización de la banca y el uso de Apps se ha vuelto una necesidad casi natural en estos tiempos.

[1] Datos según el Ministerio Público, SIDPOL y la DIVINDAT

Personal capacitado insuficiente:

Adicionalmente, el Sistema de Denuncias de la Policía (Sidpol), registraba aproximadamente ya a mediados del año pasado 2022 de más de 1.300 casos de suplantación de identidad, es importante mencionar que dicha cifra se ha ido superando año a año. Por su parte, División de Alta Tecnología (DIVINDAT), así como el sistema de Denuncias de la Policía y el Ministerio Público registraron un aumento de casos por suplantación de identidad en línea. Los índices de denuncian oscilan entre los 1000 y 2000. Respecto del número total de denuncias registradas por el delito de suplantación de identidad tenemos en nuestro sistema de justicia se cuenta con la siguiente información[2]:

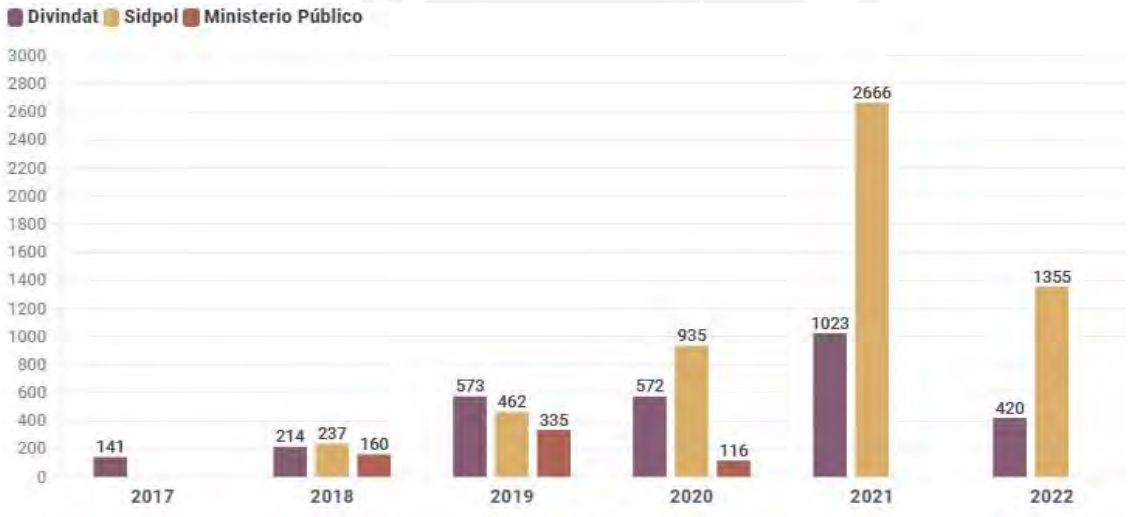

Figura 1. Denuncias por suplantación de identidad 2017-2022 (Morales Isla / Unidad LR Data, 2022)

De lo que se puede destacar del grafico presentado está definitivamente el hecho de que, si bien los delitos informáticos ya venían incrementando en su incidencia, estos tuvieron su pico más alto en el año 2021, en plena pandemia y en donde se normalizó hasta cierto punto la virtualidad tanto

[2] Morales, M (2022,7 de Julio): *Suplantación de identidad en línea: incrementan denuncias, pero no hay responsables.* DATA. La República. Véase en: **https://data.larepublica.pe/suplantacion-de-identidad-en-linea-incrementan-denuncias-pero-no-hay-responsables/**

en operaciones financieras, comerciales y económicas en general. De allí, se aprecia una sustancial disminución de los casos ya para el año 2022, pero esto es relativo, primeramente, porque las cifras oficiales procesadas en dicho año en curso sobre estas graficas son de casos contabilizados hasta mayo y Julio de ese año, no se contabilizan los casos de los meses subsiguientes por tratarse aun de casos en investigaciones en curso o a nivel preliminar. Ello se traduce en que posiblemente la cifra total oficial del año 2022 fue muy similar o hasta incluso superior al año 2021, y sin contar aún con los datos del año actual 2023.

El mismo panorama ha podido apreciarse si se acude al Ministerio Publico, que como se mencionó al inicio de esta investigación, recién ha comenzado a implementar personal capacitado para investigar esta clase de delitos, personal que es de un número muy reducido. Pues según cifras oficiales[3], se cuenta con solamente 25 fiscales especializados en ciberdelincuencia, de los cuales tres son superiores y los otros 22 son provinciales. A su vez a nivel policial se cuenta con solo dos dependencias policiales de la DIVINDAT[4]. En estas instalaciones, hay 150 efectivos en Lima y 23 en Arequipa, pero solo 70 de ellos están especializados en ciberdelincuencia. Lo cual evidencia una gran brecha entre denuncias recibidas y casos investigados, debido a la evidente falta de personal especializado. Por lo cual, si bien la denuncia es un acto importante, adolece de su falta de efectividad para dar respuestas y solución eficiente debido a la ausencia de más personal capacitado en la materia y esto incluye por supuesto a los magistrados, que muchas veces desconocen la naturaleza jurídica de estos delitos por no estar claramente delimitadas y terminan archivando desestimando muchos casos.

La suplantación y el fraude:

[3] Ministerio Publico. Anuario Estadístico 2021. Documento oficial disponible en: **https://cdn.www.gob.pe/uploads/document/file/2912946/Anuario%20Estadistico%202021.pdf.pdf?v=1647375523**

[4] CONACOP. Diagnóstico Situacional Multisectorial sobre Ciberdelincuencia en el Perú (2020). Primera edición Digital. Véase en: **https://cdn.www.gob.pe/uploads/document/file/1616607/Diagn%C3%B3stico%20Situacional%20Multisectorial%20sobre%20la%20Ciberdelincuencia%20%20en%20el%20Per%C3%BA.pdf?v=1611898656**

Dicho de tales cifras, se cuenta con que existen muchos casos en los cuales, emisiones de crédito se han dado en base a suplantación de identidad, así como de manera fraudulenta, tanto con la clonación de tarjetas de crédito, páginas web aparentemente oficiales, correos falsos, etc. Puesto que muchas denuncias de ciudadanos se han dado con un denominador común, que personas desconocidas o ajenas a ellos, lograron obtener la aprobación de préstamos por parte de una entidad bancaria, a su nombre. Luego estas personas obviamente se daban a la fuga, pero el daño ya estaba hecho, pues la victima ahora contaba con una deuda a su nombre que de no pagarla obviamente lo pone en una difícil situación que no solamente afecta su historial crediticio, o la dificultad para buscar un verdadero préstamo, sino incluso su tranquilidad, puesto que generalmente en estos casos de suplantación de identidad, la personas que cometió dicha acción obtuvo cantidades de dinero exorbitantes. En estos casos, los denunciantes acuden tanto a las entidades correspondientes, empezando las entidades financieras, ya sea bancos, cajas de ahorro o en última instancia, al Indecopi y Ministerio público, Pero la cancelación de la deuda depende sobre todo si se efectúa mediante vía de la conciliación con la empresa o por medio de Indecopi, en donde esta puede sancionar administrativamente a la entidad financiera, en base a multas en caso detectara indicios de poca rigurosidad en materia de seguridad. Sin embargo, este es un proceso que toma tiempo, hasta entonces la persona es registrada en Infocorp, su historial crediticio obviamente se ve afectado y hasta que no haya un pronunciamiento definitivo sobre el caso denunciado, la afectación de la víctima a su derecho se mantiene.

El tráfico ilegal de datos

Otro aspecto destacable dentro de la realidad problemática en este contexto, es el delito de Tráfico ilegal de datos. Que como su nombre lo indica, implica el tráfico de una base de datos sobre una persona natural o jurídica, con fines comerciales con terceras personas. Sobre este delito, existen actualmente en el Perú una grave situación de inseguridad desde el lado normativo y de campo, pues actualmente la justicia peruana ha tenido dificultades para prevenir y combatir este delito. Ya que a la fecha no cuenta con datos oficiales o estudios contundentes sobre esta

problemática, sin embargo, su existencia es de total conocimiento público, tal como lo revelan las distintas investigaciones periodísticas sobre el particular[5].

Como es sabido, en el centro de la ciudad de Lima, existe un grupo de personas, quienes operan dentro de distintas galerías dedicadas a la venta de computadoras, en donde directamente ofrecen venta de datos, así como otros datos ilegales, servicios y productos, bases de datos de entidades financieras o telefónicas, así como de instituciones públicas, como el Reniec. Todo ello desde el precio de S/.100 soles en adelante. En dicho lugar, estos traficantes de información directamente responden las dudas de sus clientes tales como: "¿De qué banco quieres? Tengo de cualquiera. En cada una [de las bases de datos] te vienen unas 50 mil personas. Viene nombre, dirección, teléfono, cargo, todo lo que necesitas", siendo esta la manera en la que estos sujetos lo ofrecen en dichas zonas e incluso en vía pública[6]. Una vez que acuerdan el precio, los traficantes de información conducen al comprador fuera de la vista del público, hasta un pequeño stand dentro de una galería cercana, donde pasarán los datos desde un USB a un CD que exigen comprar previamente.

Tal como lo menciona en una entrevista Erick Iriarte, abogado y experto en temas digitales: "Hay una gran cantidad de reportajes que han realizado diferentes medios de comunicación sobre las bases de datos que se vendían en la avenida Wilson, eso lleva años, el tema es que ahora se ha reflejado en la denuncia de Asbanc[7]. Además, han avanzado al consolidar estas diversas bases que estaban accesibles por diversas brechas en un solo producto"[8]. Es evidente que este ilícito negocio de información pone en riesgo a la población, tal como declara el experto: "En el mejor de los casos, son usadas con fines comerciales, para ofrecerte por teléfono productos. Por otro lado, también pueden ser aprovechados por criminales para cometer secuestros o extorsiones" y ello se

[5] Véase reportaje periodístico de Latina Noticias, emitida en mayo de 2023: **https://www.youtube.com/watch?v=WML4SH46mF4**

[6] Lara, J. (2019, 16 de noviembre) Privacidad a la venta: datos personales expuestos a la criminalidad*. En el Centro de Lima se venden ilícitamente nombres, teléfono y direcciones de miles de personas. Experto en delitos informáticos señala que en el país hace falta una ley sobre ciberseguridad.* Crónicas. El Comercio. Véase en: **https://elcomercio.pe/lima/seguridad/privacidad-a-la-venta-datos-personales-expuestos-a-la-criminalidad-noticia/?ref=ecr**

[7] Asociación de Bancos del Perú

[8] PERU 21. (2022, 21 de mayo) *Ministerio de Justicia investigará filtración y venta de datos personales de ciudadanos peruanos.* Véase en: **https://peru21.pe/politica/ministerio-de-justicia-investigara-filtracion-y-venta-de-datos-personales-de-ciudadanos-peruanos-noticia/**

agrava por la notoria falta de acción oportuna y coordinación por parte del Estado Peruano y el Congreso de la República respecto de las normativas pertinentes para tratar estos temas, esto se evidenciará al ver el contenido de las actuales normas respecto de los delitos de tráfico de datos y la demora en su implementación tal como advierte el experto, respecto de que la ley de ciberdefensa y la ley de ciberseguridad están entrampadas, puesto que la de ciberdefensa pasó al Ejecutivo, que la promulgó pero no la ha reglamentado, la cual la hace en buena práctica, inaplicable, mientras que la de ciberseguridad fue observada y el Congreso ni ha levantado las observaciones ni ha ido por la insistencia". De eso, agregó, han pasado ya tres años, desde 2019.

Así como preocupación respecto del personal calificado necesario para ver estos temas, técnicamente hablando, pues se necesitan unos 30 mil expertos en ciberseguridad. ¿Dónde se están formando? ¿Qué acciones está tomando el gobierno para trabajar desde las escuelas el tema de ciberseguridad y protección de datos? Son las preguntas que formula el experto respecto a este tema. Esto deja en evidencia de que normativa y reglamentariamente el Estado peruano no está a la par con la realidad de necesidad urgente de seguridad informática y de gestión de datos tanto a nivel público como privado.

Los robos en el Perú:

Por otro lado, si bien la problemática se entiende que está circunscrita a los delitos informáticos propiamente dicho tales como Suplantación de Identidad, Fraude informático y tráfico ilegal de datos, existe otro factor dentro de esta dinámica. Y si bien no es un delito de naturaleza informática propiamente dicho, lo considero relevante dentro de este contexto. Me refiero a uno de los delitos contra el patrimonio más común en el Perú, el delito de Robo. Como es sabido, el robo en el Perú representa todo un tema y problemática para el Estado Peruano. En general en el país, los delitos contra el patrimonio cuentan con el mayor número de denuncias como puede apreciarse en el siguiente cuadro:

Denuncias por comisión de delitos, según delito genérico (octubre, diciembre, 2020 – 2022)[9](Fuente: INEI. Gráfico: Boletín de Estadísticas Enero – noviembre 2022)

Delito genérico	2020 Oct - Dic	2021 Oct - Dic	2022 Oct - Dic	Variación Oct - Dic 2022 / Oct - Dic 2021	
				Absoluta	%
Total	89 723	114 394	131 654	17 260	15,1
Contra el patrimonio	52 725	71 560	87 395	15 835	22,1
Contra la seguridad pública	10 534	15 226	15 394	168	1,1
Contra la vida, el cuerpo y la salud	9 831	10 783	11 672	889	8,2
Contra la libertad	9 725	9 365	10 046	681	7,3
Contra la administración pública	4 227	4 030	3 533	-497	-12,3
Contra la fe pública	641	1 476	1 485	9	0,6
Contra la familia	1 266	1 192	1 027	-165	-13,8

Figura 2: Estadísticas de la criminalidad, seguridad ciudadana y violencia. Una visión de los registros administrativos (INEI,2022)

Como puede apreciarse en el cuadro, los delitos contra el patrimonio son los de mayor repercusión social, siendo el delito de robo (Art. 188 Código Penal[10]), su máximo representante, por su alta recurrencia en el país, siendo el robo de equipos de celulares, uno de los mayores problemas de nuestra sociedad hasta la actualidad. En ese sentido, el Organismo Supervisor de Inversión Privada en Telecomunicaciones, OSIPTEL, que es un organismo técnico especializado del Estado Peruano que regula y supervisa el mercado de servicios públicos de telecomunicaciones; y vela por los derechos del usuario ha llegado a contrastar datos oficiales respecto del robo de celulares en cifras, pudiéndose advertir que dicha cifra está en constante

[9] INEI: Informe Técnico Nº1- marzo 2023. *Estadísticas de la criminalidad, Seguridad Ciudadana y violencia.* Una visión de los registros administrativos. Enero-noviembre 2022. Pg. 5. Véase en:
https://m.inei.gob.pe/media/MenuRecursivo/boletines/boletin_estadisticas_criminiladad_ene_nov2022.pdf

[10] Artículo 188.- Robo
"El que se apodera ilegítimamente de un bien mueble total o parcialmente ajeno, para aprovecharse de él, sustrayéndolo del lugar en que se encuentra, empleando violencia contra la persona o amenazándola con un peligro inminente para su vida o integridad física…"

crecimiento, y más allá de que este delito está claramente tipificado, su aún vigente y excesiva comisión se debe a otros factores como la informalidad, la lentitud del sistema de justicia y sobretodo, la aparente falta de relevancia que la da la ley penal a los delitos menores, o cuando la cuantía del bien afectado no es tan excesivamente alto, lo cual no debería servir de excusa, pues la afectación económica y patrimonial no debería ser considerada relevante en función de su cuantía. Esto, sumado a la cultura de la informalidad y la compra de celulares de segunda mano hagan del delito de robo de celulares un mal vigente. Tal como se puede apreciar en el siguiente cuadro:

Celulares reportados como sustraídos o perdidos, según OSIPTEL (2015-2021)[11]

AÑO	Sustraídos (robados o hurtados)	Perdidos	Total
2015	2,277,469	988,580	3,266,049
2016	2,300,277	932,662	3,232,939
2017	2,356,262	700,320	3,056,582
2018	2,291,543	567,778	2,859,321
2019	2,174,750	444,046	2,618,796
2020	1,071,416	199,536	1,270,952
2021	1,350,352	235,365	1,585,717
TOTAL	13,822,069	4,068,287	17,890,356

Figura 3: ¿Cuánto nos cuesta el robo de un celular? (Zevallos Trigoso/Instituto de Criminología, 2022)

Si bien estamos ante un delito de naturaleza distinta, de orden estrictamente patrimonial, sus repercusiones en el mundo financiero son evidentes. Ya que teniendo en cuenta que la banca digital y los dispositivos móviles trabajan de manera conjunta, un simple robo de celular tiene el potencial de producir adicionalmente, una suplantación de identidad al momento de que el sujeto activo de este delito, acceda a correos, y sobretodo las aplicaciones oficiales ligadas a entidad financiera en la cual las víctimas resguardaban sus cuentas bancarias, tal como se ha evidenciado en las innumerables denuncias, reportes en donde generalmente las víctimas, se comunican con las compañía de telefonía y los bancos para bloquear tanto las líneas y servicios. Sin embargo, tal

[11] Zevallos, N. (2022, 29 de agosto). *¿Cuánto nos cuesta el robo de un celular?* Instituto de Criminología. Véase en: **https://www.ipe.org.pe/portal/cuanto-nos-cuesta-el-robo-de-un-celular-por-nicolas-zevallos/**

como menciona el investigador Nicolas Zevallos, muchas veces los ladrones logran acceder a algunas de sus cuentas y aplicaciones de sus víctimas, suplantándolos, haciendo pedidos a domicilio y hasta un consiguiendo préstamos bancarios.

Es por ello que considero al delito de robo de celulares en específico como parte de la problemática en este contexto y por lo tanto debe ser considerado relevante a la hora de establecer normativa referente a la lucha contra los delitos informáticos de relevancia financiera

Las preguntas claves:

Respecto de los delitos informáticos; nos planteamos las siguientes preguntas clave: ¿Qué responsabilidad tendría una entidad financiera ante los delitos financieros relevantes en materia financiera si se evidenciara un deficiente sistema ciberseguridad y de gestión del control de datos en general? ¿Qué soluciones se pueden formular normativamente?

Planteamiento de Hipótesis:

La evidente carencia de ciertos aspectos tales como; la carencia de recursos humanos calificados, entendiéndose como falta de mayor personal capacitado tanto a nivel policial, fiscal y judicial en materia de delitos informáticos; la carencia de recursos jurídicos idóneos, entendido como la poca claridad y ausencia de normativa y regulación más desarrollada y especifica respecto de aquellos delitos informáticos y toda practica ilícita, su impacto y consecuencias prácticas y jurídicas en el ámbito financiero; y la carencia de normativa, dispositivos legales más vinculantes que impulsen a las entidades financieras, respecto de su responsabilidad, y de adoptar modelos de prevención, ciberseguridad y gestión adecuada de datos más idóneos han permitido hasta ahora a que los delitos informáticos, en especial los relativos en materia financiera, tales como los delitos de Fraude informático, suplantación de identidad y tráfico ilegal de datos hayan aumentado de manera exponencial en estos años recientes, consolidándose a día de hoy como un serio problema de relevancia nacional, tal como la evidencia empírica a día de hoy nos lo demuestra.

Planteamiento de objetivos:

Lo que esta investigación primeramente busca es advertir la ausencia de claridad a nivel normativo respecto del rol de una entidad financiera ante los delitos informáticos relevantes (suplantación de identidad, fraude informático y tráfico ilegal de datos) y definir si es un sujeto pasivo o activo en dicha figura de acuerdo a su ámbito. Determinar el tipo de responsabilidad atribuible a una entidad financiera ante delitos informático tales como suplantación de identidad, fraude informático, tráfico ilegal de datos, en el supuesto de no contar un sistema control de identidad óptimo, protocolos de seguridad de gestión de información adecuada y en general un sistema de ciberseguridad integral. Buscar una solución normativa de carácter sancionatorio a nivel financiero que busque promover políticas preventivas en materia de delitos informáticos, los relevantes financieramente hablando.

Propuesta de enfoque metodológico:

El enfoque metodológico a utilizar será el método cualitativo, apoyándose en la literatura especializada en delitos informáticos en materia financiera, y analizando las leyes pertinentes. De otro lado también se recurrirá al método comparativo, para analizar y comparar, los tratamientos y cambios normativos dados en la legislación chilena y compararla con la peruana en busca de mejores alternativas de solución. El enfocarnos exclusivamente en la legislación chilena lo considero más factible el emular, seguir pasos de un solo sistema. De otro lado, tomar como ejemplo a una legislación de la región es mucho más idóneo por tratarse de una realidad más cercana a la peruana, siendo Chile por supuesto uno de los países referentes en la región. Finalmente se elige a la legislación chilena por haber utilizado una estrategia en base a la armonización de distintas normas para generar todo un paquete normativo a favor de la prevención de delitos informáticos como una política necesaria y obligatoria en el ámbito financiero, lo cual considero es uno de los caminos que el Perú puede replicar.

CAPÍTULO 1: MARCO TEÓRICO

1.1 Concepto de delito informático.

Sobre el concepto de delito informático se cuentan con distintas opiniones. Contándose con 2 vertientes. En la primera, en donde se considera al concepto de delito informático distinto al concepto de ciberdelito, o se lo entiende en un sentido más amplio, mientras que la segunda vertiente, algunos autores consideran a los delitos informáticos, la ciberdelincuencia y otros términos como conceptos similares.

Por ejemplo, para el profesor Felipe Villavicencio los delitos informáticos son todas aquellas conductas que en principio buscan vulnerar los sistemas de dispositivos de seguridad a nivel informático, esto incluiría tanto invasiones a computadoras, así como a correos o sistemas de datas completos mediante claves de acceso, siendo que dichas conductas típicas únicamente pueden ser cometidas a través del uso la tecnología. Por lo tanto, para este autor, en los delitos informáticos las Tecnologías de la Información (TIC) pueden ser tanto el objetivo, como también el medio o incluso el lugar de ejecución del delito, no olvidando que estos afectan bienes jurídicos diversos en función de su finalidad. (Villavicencio, 2014)

En ese mismo sentido tenemos al Dr. Santiago Acurio del Pino quien considera que, debido al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamientos impensables y en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad. Para este autor la doctrina ha denominado a este grupo de comportamientos, de manera genérica, «delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática» (Acurio del Pino, 2020)

Sin embargo, del otro lado tenemos la opinión del profesor español Romeo Casabona, quien nos señala que la expresión de “delito informático” se ha dado dentro de la literatura de la lengua española en base a que dicho concepto tiene la ventaja de su plasticidad, pues puede relacionarse directamente con la tecnología sobre o a través de la que actúa. Sin embargo, en un sentido estricto no puede hablarse de un delito informático de manera singular, sino de una pluralidad de ellos,

siendo que todos aquellos actos distintos tienen como denominador común el uso de los computadores, pero que ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características semejantes. Pues en ocasiones el computador es el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por lo que lo más correcto sería hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información. (Romeo Casabona, 1987)

En ese orden de ideas, nos orientamos más por la postura de considerar al concepto de delitos informáticos, como un concepto más amplio, es decir, entendiéndolo como un conjunto de conductas diversas. Pues enfocarnos solamente en ciberdelitos implicaría fijar solo los actos cometidos única y exclusivamente con un computador. Y como veremos más adelante, los delitos informáticos, dentro del ámbito financiero, pueden darse no solamente mediante el uso de una computadora, sino que estos actos delictivos pueden darse también mediante el uso de otras fuentes tales como dispositivos móviles, llamadas telefónicas, tarjetas de crédito, etc. Por lo tanto, el concepto más adecuado para esta investigación será el de "Delitos Informáticos", ya que esta englobaría tanto a los ciberdelitos, es decir aquellas conductas cuyo objeto o medio es un computador, así como las conductas cometidas sin necesidad del uso o vulneración de un computador.

1.2 Características principales.

Si bien los delitos informáticos son de naturaleza amplia y variada, así como compleja, la gran mayoría de estos guardan determinas características en común.

1.2.1. Tipificación en constante evolución

Una de sus características más destacables y que los diferencian un poco de otra de delitos no es solamente su dificultad para combatir y hallar a sus responsables, sino que también hay

dificultad para tipificarlos idóneamente en una ley penal, y esta situación de complejidad en su tipificación no solamente sucede en el Perú sino también en otras legislaciones. Por ellos, si bien se tienen tipificados algunas figuras delictivas, muchas nuevas modalidades aún continúan sin tipificación.

Bajo esa línea tenemos la recomendación (89) del Comité de ministros del Consejo de Europa[12] en donde se consideró que la delincuencia informática suele tener carácter transfronterizo que exige una respuesta adecuada y rápida y, por tanto, es necesario llevar a cabo una armonización más intensa de la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el computador. Es decir, desde hace varias décadas, distintos países ya advertían de la necesidad de lograr tipificar adecuadamente dichas nuevas figuras penales.

1.2.2 Afectación de distintos bienes jurídicos

De otro lado tenemos al autor Gómez Perals, quien considera a estos delitos como un conjunto de conductas de relevancia penal en donde tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta. Siendo que dichas afectaciones pueden darse de maneras múltiples, afectando distintos bienes jurídicos. (Los cuales varían dependiendo de la modalidad de dichos delitos, así como su finalidad. (Gómez, 1994). Evidentemente el estudio de estas conductas y sus finalidades puede reducirse sustantivamente al enfocarnos solamente en el ámbito financiero.

1.2.3 Los Sujetos del delito informático

Otra característica importante en los delitos informáticos, es que respecto de la doctrina de la clásica relación binomio o duplicidad víctima – delincuente en los delitos comunes, esta varia en

[12] Council of Europe. (Traducción: A. Cristina López). Head of Scope on Electoral Co-operation. Véase en **https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/E-votingRec_Spanish.asp**

el ámbito financiero. Pues en los casos delitos informáticos en el ámbito financiero, contamos con 3 actores, no 2 como se ha mencionado inicialmente. Primeramente, entenderemos como sujetos pasivos a dos actores, al cliente, quien es el principal agraviado, y en segundo lugar a la entidad financiera, cuando los estándares de confidencialidad, integridad y disponibilidad de su información financiera en su sistema se ha visto afectado, lo cual se traduce en una afectación y menoscabo patrimonial para el primero, su cliente. Y el sujeto activo es obviamente el agente que mediante el uso de tecnologías de la información vulneró el sistema de seguridad que salvaguardaba la información del sujeto pasivo (cliente). Ahora respecto de los sujetos pasivos en este delito, considero que la entidad financiera como sujeto pasivo mantiene mayores deberes de cuidado que el sujeto pasivo primigenio (cliente). Sin embargo, pueden existir supuestos en que la entidad financiera podría ser considerada responsable en cierto grado del delito, aun siendo teóricamente el sujeto pasivo. Este punto se desarrollará más adelante.

1.3 El dolo

Estos son elementos fundamentales en la estructura de todo delito, como es sabido dentro del derecho penal[13], se cuenta con los elementos importantes: Dolo y culpa, respecto de su distribución sabemos que dentro del dolo se reconocen actualmente tres formas. Para el abogado Guillermo Bringas, el dolo directo de **primer grado** se da cuando el autor conoce y quiere la realización de los elementos del tipo penal. En esta forma de dolo, se afirma pues que, si bien existe el elemento cognitivo y el elemento volitivo, predomina este último, es decir, la voluntad o intención.

Asimismo, el dolo directo de **segundo grado** se da cuando el autor conoce que con su conducta lesionará bienes jurídicos de terceros, aunque no tenga el propósito de producirlos. En esta forma de dolo, a diferencia del dolo en primer grado, se aprecia un predominio del elemento de conocimiento frente al elemento de voluntad o intención. Finalmente, la tercera forma de dolo, el **dolo eventual** se da cuando quien comete la conducta conoce el riesgo concreto que genera su acción y a pesar de ello, no desiste de su accionar sino por el contrario, continua. Se evidencia que

[13] Jescheck, H. y Weigend, T. (2002). Tratado de derecho penal. Parte general. Granada: Comare. P. 437

el elemento primordial en esta clase de dolo es también el conocimiento, mientras que el elemento de la voluntad o intención es difuso. (Guillermo, 2019)

1.4 La culpa

Respecto del concepto de culpa, este tiene infinidad de definiciones sin embargo nos apoyaremos nuevamente en el profesor Villavicencio, quien considera a la culpa como un componente psicomental vinculado al autor en el momento de ejecutar una conducta que produzca una infracción delictiva, basando el reproche de la sociedad en la ausencia de un resultado querido y en el incumplimiento de los deberes de cuidado. (Villavicencio, 2007)

Adicionalmente, para Hurtado Pozo, la culpa es un concepto abierto, el cual debe ser completado en su contenido por la autoridad judicial; y para que se pueda dar dicha operación, el juez deberá analizar el deber objetivo de cuidado que debía tener el sujeto activo (Hurtado, 2005)

Mientras que, para Almanza, la culpa está basada en resultado típico, teniendo como mayor relevancia la infracción de un deber de cuidado. Es decir, el concepto de culpa se entiende de que para este se configure, no es necesario imputarle un conocimiento pleno al autor, sino más que todo un conocimiento en menor grado que, unido a deberes de cuidado objetivamente establecidos, habría llevado a evitar la realización del tipo penal ((Almanza y Peña, 2014).

Ahora bien, respecto del concepto de culpa se pueden desprender las siguientes modalidades:

i) Imprudencia: Afrontar un riesgo de manera innecesaria pudiendo evitarse

ii) Negligencia: Implica la activa o inactividad que produce un daño, no hacer lo debido o hacer lo indebido

iii) Impericia: Actividades que para su desarrollo requieran conocimientos técnicos especiales

iv) Infracción al deber de cuidado: También entendida como una inobservancia a un reglamento, en omisión impropia, cuando se vulneren las normas a título de imprudencia o no se apliquen por negligencia.

Estos últimos puntos los considero relevantes financieramente, pues en determinados cabe pregunta. ¿Qué hacer cuando la conducta negligente o de infracción al deber de cuidado no se haya dado por parte de la víctima (cliente), sino por parte de una entidad financiera? En los supuestos en que una entidad financiera no hizo lo suficiente por remediar una situación de riesgo previamente advertida o denunciada o en un tiempo posterior, respecto de la ciberseguridad y de la gestión de datos en general.

1.4.1 La culpa Consciente

En este primer tipo de culpa, está presente el conocimiento, no está presente la voluntad o intención, mientras que la conducta está en función al hecho de que el agente confía en que no dé a lugar la producción de un resultado que es consciente de que podría afectar a un tercero (Chang, 2015). Es decir, a pesar de conocer la posibilidad, confía en que no se produzca. Este concepto de culpa lo considero más cercano a ser atribuible a una entidad financiera, ante casos en que esta confié en que su sistema informático de datos es infalible aun cuando quizás no haya hecho lo necesario para realmente tener esa plena convicción, o incluso, sea consciente de la infalibilidad de su sistema informático, pero aun así no tome, medidas, confiado en que dichas posibles falencias son mínimas o que difícilmente se produzcan vulneraciones.

En ese orden de ideas, se podría plantear en determinados escenarios, como en los casos de emisión de créditos mediante suplantación de identidad, descritos en muchas denuncias, en el sistema financiero. Que una entidad financiera tiene la responsabilidad y el deber de evitar que se dé un escenario desfavorable para su cliente, es decir. Una entidad financiera no espera que su cliente sea victimade un delito informático que afecte su patrimonio, sin embargo, el hecho de que dicha entidad no tome las medidas de seguridad necesarias para ello, implicaría que la entidad en cuestión confía o espera que dichos peligros potenciales, no se den, aunque es consciente de que estos podrían darse. Por lo cual podríamos estar hablando de un carácter de culpabilidad respecto de su rol como garante de la seguridad del patrimonio de su cliente. Y si bien la ley penal establece que, salvo mención distinta expresa, las conductas que se sancionan son únicamente dolosas, el elemento de culpa está presente, y en ese orden de ideas la normativa debería establecer un

mecanismo para en base a esa culpa, plantear una obligatoriedad a las entidades financieras para la prevención de delitos informáticos en perjuicio de las víctimas.

1.4.2 La ignorancia deliberada

En este segundo tipo de culpa, la ignorancia deliberada implica toda conducta que pudiendo y debiendo conocer determinadas circunstancias penalmente relevantes de su conducta, el agente toma deliberada o conscientemente la decisión de mantenerse en la ignorancia de dichas circunstancias. (Ragúes, 2007). Entendiéndose como la indiferencia ante la puesta en peligro de un bien jurídico protegido, que diera como desenlace un lesivo en perjuicio del titular de dicho bien jurídico. Siendo así se podría considerar dicha conducta, jurídicamente reprochable e incluso equiparable al dolo, aunque ello es una discusión aun no finalizada, que aún no ha se ha desarrollado lo suficiente en el Perú, pero está presente en la realidad.

Pues ya centrándonos a la problemática de esta investigación, este concepto de ignorancia deliberada no podría ser atribuible directamente a las entidades financieras como tal. Pero si sobre los integrantes de una entidad financiera. Esto cuando el daño producido a personas agraviadas por los delitos de suplantación de identidad, fraude informático, tráfico ilegal de datos u otros se diera por acción negligente, u omisión en el cumplimento de sus deberes y funciones internas. Lo cual implicaría por supuesto que dichos actos no se dieron en concordancia a las políticas propias de toda entidad financiera las cuales se entienden que buscar garantizar ciertos estándares de seguridad informática de su información, así como la gestión responsable de dichos datos en salvaguarda del interés de sus clientes. Por lo tanto, estos trabajadores y/o funcionarios responderían de nombre propio. Algo que como se advierte en la normativa actual, no ha sido contemplado como una situación agravante dentro de la estructura de estos delitos informáticos relevantes. Por lo tanto, el hecho de que se considere que la conducta típica no incluya a miembros de un sistema financiera en caso de participación como autores o coautores, implica un vacío. Lo cual se traduce en una eventual situación de inseguridad del patrimonio de los clientes, algo grave, que por supuesto es un defecto de la norma.

Este tipo de situaciones sería importante a analizar, más aun teniéndose en cuenta que tanto los clientes como las entidades financieras representan a los sujetos pasivos en la estructura del delito informático dentro de un contexto financiero. En ese orden de ideas, soy de la opinión de que la

entidad financiera por su propia naturaleza debe mantener un rol de salvaguarda del patrimonio que su cliente le ha confiado en sus arcas, y esto implica no solo el dinero, sino también su información personal.

En ese orden de ideas, si bien la ignorancia deliberada como elemento conductual no alcanza a la entidad financiera como tal, pero si a sus trabajadores como personas naturales, si considero que la entidad financiera tiene un deber de protección. Por ello es fundamental que dicho deber de protección, de prevención respecto de todas aquellas prácticas antijurídicas ya descritas, este plasmado de manera más categórica en una norma.

1.5 El bien jurídico protegido

Sobre este punto, existen también distintas opiniones, ya que el autor Bramont Arias, si bien considera que el bien jurídico protegido es punto de referencia obligado para la determinación del tipo penal del delito informático, puesto que determina el marco dentro del cual pueden realizarse las conductas delictivas. Sin embargo, nos advierte que no existe unanimidad sobre este punto respecto de los delitos informáticos. Agregando además que si bien la mayoría de legislaciones establecen que estos delitos afectan al patrimonio, hay autores que afirman que el bien jurídico protegido es bien el orden económico, o también la intimidad de las personas. (Bramont, 1997)

De otro lado tenemos a Claudio Magliona quien establece que los delitos informáticos tienen el carácter de pluriofensivos o complejos ya que simultáneamente afectan varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo de figura penal. Adicionalmente también nos menciona que el aspecto más importante de la informática radica en que la información ha pasado a convertirse en un valor económico de primera magnitud. Desde siempre el hombre ha buscado guardar información relevante para usarla después. (Magliona, 1999)

Sin embargo, para el Dr. Santiago Acurio del Pino, considera que en vista que en vista de la emergente Sociedad de Información en la que se vive, se hace totalmente necesaria para la doctrina

de la incorporación de valores inmateriales y de la información[14] misma como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible. (Acurio del Pino, 2020)

De lo visto podemos sintetizar que el bien jurídico protegido en el delito informático es múltiple. Esto en función del delito informático en específico de acuerdo a cada caso.

1.6 El delito de suplantación de identidad:

Entendemos que, en el caso del delito de Suplantación de identidad, el bien jurídico afectado es la fe pública, puesto que dicha suplantación vulnera la facultad del sujeto pasivo de relacionarse con otra persona natural o jurídica, afectando aspectos de su derecho civil. Sin embargo, desde la óptica financiera considero que también se da una afectación de orden económico. Pues es mediante el acto de suplantar la identidad de alguien en el ámbito financiero, que se busca obtener beneficios indebidos a costa de generar un evidentemente perjuicio tanto patrimonial como extra patrimonialmente a las víctimas, las cuales son tanto la entidad bancaria como su cliente. Adicionalmente a ello tenemos también otra figura delictiva que va siempre ligada a la suplantación de identidad, y esta es el fraude informático.

Respecto del concepto de este delito, en nuestro país lo tenemos definido, como ya se ha visto, en la Ley de delitos informáticos N.º 30096:

CAPÍTULO VI:

"DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA"

Art. 9: Suplantación de identidad:

[14] Si bien Budapest recoge como objetos de protección los datos y sistemas informáticos. Por ejemplo, la información está almacenada en sistemas o se desarrolla a través de datos concretos. Si bien esta información está en principio contenida en datos y sistemas en determinados casos, como en los casos de suplantación, dicha información puede ser obtenida también de otras fuentes, menos sofisticadas.

"El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años"

Si bien este no es el único tipo de delito informático, si es importante mencionar que en estos últimos años se ha vuelto uno de los más recurrentes en base a la evidencia empírica recolectada por las autoridades competentes tanto a nivel de denuncias recibidas e investigaciones realizadas por el Ministerio Publico y la Policía Nacional. El modo de operar este delito consiste en suplantar a otra persona, siendo este el medio, y la finalidad de este delito es justamente utilizar dicha identidad suplantada realizar una afectación económica sobre las personas que han suplantado.

Adicionalmente, dentro de los autores, no existe unanimidad sobre esta figura, tanto en su concepto como en la configuración de la comisión de este delito, lo cual es abordado de distintas maneras. Por ejemplo, contamos con el autor Ricardo Posada, quien destacada que en la legislación de Colombia existe en su Código Penal la figura de la "Transferencia no consentida de activos no consentida de activos y la fabricación, posesión, introducción y facilitación de software defraudatorio", la cual estaba incorporada en su art 269 de su Ley Penal. Esta figura autónoma de defraudación informática económica está definida como: "El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero (…)". Entendiéndose que, dentro de dicha manipulación, en esta figura penal colombiana, implicaría por supuesto el acto de la suplantación de identidad. Como puede apreciarse, la suplantación de identidad como figura penal, es tratada y desarrollada de manera muy variada entre los autores y legislaciones, en algunos casos, siendo relacionado con otras figuras jurídicas como la estafa, o de manera autónoma, o siendo incluso considerado simplemente una modalidad de delito los delitos antes mencionados. Sobre este punto, el precitado autor comenta también que, existen muchas otras posturas doctrinales que afirman que, por ejemplo, esta transferencia no consentida, es una modalidad asimilada al tipo básico de estafa o un tipo especial de estafa[15], o incluso de naturaleza peculiar. Por otro lado, es importante destacar que las transferencias no consentidas, o no autorizadas pueden darse tanto mediante suplantación de identidad que implica una suplantación, como por fraude informático, que es

[15] Posada Maya, Ricardo (2012). "El delito de transferencia no consentida de activos", Revista de Derecho, comunicaciones y Nuevas Tecnologías. Universidad de los Andes. P. 8.

cuando la persona es inducida a error, por ejemplo, ante la clonación de una cuenta o página oficial de un banco. Es importante hacer esta distinción, pues ambas, la suplantación de identidad y el fraude informático son figuras penales independientes dentro de los delitos informáticos, pero que muchas veces comparten la misma incidencia en los casos como se ha mencionado en el punto anterior.

Ahora bien, es importante mencionar también que independientemente de la denominación utilizada por estas figuras penales, los actos de transferencias bancarias no consentidas, no autorizadas implican necesariamente la participación de las figuras delictivas de fraude informático, suplantación de identidad y tráfico ilegal de datos para su comisión, puesto que la transferencia en sí, es el objetivo final. Por ello en ese sentido considero idónea y acertada la fórmula jurídica establecida por la legislación chilena, como se verá más adelante, respecto de los delitos informáticos relevantes a nivel financiero. Pues así podrá consolidarse de manera más articulada, políticas de mayor seguridad, prevención y gestión de datos.

1.7. El delito de fraude informático.

Este delito guarda ciertas similitudes con la suplantación de identidad. Aunque es claro que esta más circunscrito y centrado respecto del bien jurídico afectado, que es de orden patrimonial como se puede ver a continuación en la Ley de delitos informáticos N.º 30096:

CAPÍTULO V

DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 8. Fraude informático

"El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa

cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social"

Como puede apreciarse de la figura penal, en estos casos, los sujetos activos del delito dan con información de las cuentas bancarias y tarjetas de diversas personas para finalmente, hacer compras de distintos productos y servicios, trasladar dinero a cuentas benefactoras que son parte de una banda criminal o realizar préstamos en línea de sumas exorbitantes de manera no reconocida por parte de los verdaderos titulares al percatarse posteriormente del fraude. Este delito ha aumentado su incidencia en los últimos años. Pues a lo largo del año pasado 2022, según datos de la DIVINDAT[16] se denunciaron 2,382 casos de fraude informático, consolidándolo como el delito informático más denunciado en el Perú durante el año pasado.

1.8. Similitudes y diferencias entre ambos delitos

Como ha podido apreciarse en la estructura del delito de fraude informático, el bien jurídico afectado está mucho más delimitado en comparación a la suplantación de identidad. De otro lado, la evidencia empírica nos dice que muchas veces la suplantación de identidad es un acto un medio para concretar el fraude informático. Sin embargo, esto va más allá que simplemente establecer una relación de género y especie entre ambos delitos. Pues si bien en ambos casos se afectan los sistemas informáticos de una entidad financiera para obtener un beneficio indebido en perjuicio de terceros y de las mismas entidades, la diferenciación que se puede apreciar es que en la suplantación no es indispensable un conocimiento medianamente técnico de las tecnologías de la información. Mientras que en el fraude informático el sujeto activo elabora todo un escenario de engaño para inducir a error a las víctimas, en el caso de la suplantación de identidad este requisito no será indispensable, pues basta con tener determinado acceso a información sensible para cometer el mismo daño. En ese orden de ideas, el fraude informático como delito informático

[16] Pichihua, S (2023, 12 de febrero) *¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú*. Agencia Andina. Véase en: **https://andina.pe/agencia/noticia-cuidado-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-peru-928425.aspx%22#:~:text=En%20el%20Per%C3%BA%20se%20registran,de%20celulares%20robados%20para%20ciberdelitos.**

implica una mayor elaboración para su ejecución, por ejemplo: clonar una página web, utilizar softwares maliciosos, interferencias, manipulaciones, etc. En la suplantación de identidad propiamente dicha puede darse con el acceso indebido, ya sea también de manera técnica o ante el aprovechamiento de sistemas de control de reconocimiento poco eficientes.

Por otro lado, generalmente el Fraude informático es totalmente premeditado tanto en sus actos preparatorios como en su ejecución, mientras que en el delito de suplantación de identidad este puede darse incluso de manera espontánea, circunstancial o por medio otros delitos tales como en el robo, que como se ha mencionado anteriormente el caso de robo de celulares, es por excelencia el delito patrimonial con mayor incidencia en el Perú, ya que, según cifras oficiales del año pasado, en promedio se roban cerca de 7 mil celulares al día en el país[17]. La suplantación de identidad por lo tanto puede ser un delito producto del delito previo de robo de celulares, algo que no necesariamente se de en el caso de fraude informático. Sin embargo, más allá de las similitudes y diferencias advertidas, ambos delitos pueden verse favorecidas en su comisión, no solamente por el contexto del delito de robo, sino también por otro factor, en este caso de la ausencia de una real política de seguridad de datos informáticos en el Perú y en ese sentido entra a tallar otro delito financiero como se verá a continuación

1.9. El delito de tráfico ilegal de datos

Si bien este delito, actualmente ya no forma parte de los denominados delitos informáticos en su ley especial, es de suma relevancia a día de hoy. Puesto que su comisión afecta directamente una serie de ámbitos en nuestra sociedad, siendo entre ellos por supuesto, los datos de naturaleza financiera.

Este delito, que implica la venta ilegal de información de un sistema de datos. Actualmente está contemplado en el artículo 154-A del Código Penal:

[17] DPL News (2022, 31 de agosto): Perú | *"Siete mil celulares se pierden o se roban al día en el Perú, según datos de Osiptel", advierte exviceministro de Seguridad Pública.* Véase en: **https://dplnews.com/peru-siete-mil-celulares-se-pierden-o-se-roban-al-dia-en-el-peru-segun-datos-de-osiptel-advierte-exviceministro-de-seguridad-publica/**

Artículo 154-A.- Tráfico ilegal de datos personales

"El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior"

Como puede apreciarse, el delito está definido como tráfico ilegal de datos personales, esto obviamente en virtud a normativa específica respecto del uso de los datos personales en el Perú[18]. En este delito el bien jurídico tutelado es la Intimidad de la persona. Sin embargo, pese a que la realidad de este delito en particular, el Estado peruano en su conjunto no le ha dado la suficiente relevancia del mismo. Pues si bien el reglamento de la ley de datos personales ha significado avances, es necesario la conjunción de más cuerpos legales complementarios. Esto pese, como se mencionó inicialmente en el apartado de problemática de la investigación, en donde pese al conocimiento público y periodístico respecto de cómo los datos de las personas son comercializados impunemente, el Estado Peruano no toma medidas concretas o definitivas. Tanto a nivel operativo como a nivel normativo, ya que la normativa actual por si sola es insuficiente. No olvidar que, en el tráfico ilegal de datos personales, el sujeto activo tiene como una única agravante de si pertenece a una organización criminal, lo cual me parece hasta redundante, ya que la mayoría de estos delitos implica pluralidad criminal y por lo general división de roles. Este delito no contempla que sucedería si el sujeto activo formase para de una misma entidad bancaria, y sirviese de cómplice para la filtración y posterior venta de datos personales de clientes a terceros. Es un supuesto valido a ser contemplado en este delito que sin embargo no lo está. Ya que un aspecto clave en la comisión del delito es que quien trafica con la información necesita necesariamente de alguien que le provea de dicha información, quien en teoría es una persona o grupo de personas, que trabajan dentro de entidades que manejan y custodian información no publica de la esfera privada de personas naturales. Por lo tanto, el delito de tráfico de datos

[18] La Ley de protección de datos personales (Ley Nº 29733) y su Reglamento (Decreto Supremo Nº 003-2013-JUS) tienen por objeto proteger los datos personales regulando el uso que las entidades públicas y privadas hagan de sus bancos de datos

personales, no contempla a mi criterio como situación agravante si quien proporciona la información formara parte de la misma entidad afectada. Estaríamos hablando de un cómplice dentro de la misma entidad cuyo sistema de datos ha sido afectado. Esto nos demuestra que respecto del delito de tráfico de datos en general, la norma penal también es insuficiente y no nos aclara que responsabilidad tendría una entidad financiera o personal subordinado, en estos casos de comprobarse su directa o indirecta participación por acción u omisión.

1.10. Postura del autor

Respecto de los conceptos hasta ahora estudiados, puedo mencionar que a nivel de definición de lo que es un delito informático (dentro del ámbito financiero) podemos puntualizarlo en que consiste en toda conducta hecha por el agente activo que en principio buscan vulnerar los sistemas de seguridad de un sistema informático de una entidad financiera, y esto puede darse en base al uso de material especializado, tales como software, hardware, u otros dispositivos informáticos, móviles, etc. De otro lado, la ejecución de todo ello puede darse mediante a invasiones a computadoras, así como a correos o sistemas de datas completos mediante claves de acceso. Sin embargo, considero que el delito informático ha ido cambiando en estos últimos tiempos, especialmente en la fase de la ejecución y en el perfil del sujeto activo. Es decir, ya no en todos los casos será indispensable el uso de un computador para vulnerar un sistema de seguridad a una entidad financiera, esto se dará en función del grado de sofisticación de un sistema de seguridad, es decir cuanto más vulnerable o poco eficiente sea un sistema o protocolo de seguridad el sujeto activo del delito necesitara menos recursos para vulnerarlo. Esto lo menciono en el sentido de que hoy en día es sabido de la existencia de tráficos de datos, los cuales se comercializan en determinados lugares y en teoría es muy sencillo obtener datos masivos en bruto de muchísimas personas, y este acceso de información no implica ya necesariamente una sofisticación para su disposición, sumado además el caso de robos de dispositivos móviles

Quizás dicha sofisticación y conocimiento informático avanzado si sea necesario para quienes tengan acceso a nuestros sistemas de registro, que como sabemos son vulnerables y poco seguros, con la intención de vender dicha información a un público interesado en dicha información, la cual como sabemos es el insumo principal en los casos de suplantación de identidad. Tanto entidades

estatales como RENIEC, MIGRACIONES, entre muchas otras que manejan información y datos de los ciudadanos, adolecen de estas vulnerabilidades, sumado a las mafias interesadas en lucrar con estos datos y la poca prolijidad del Estado peruano de proteger estos datos como debería ser, son factores que a mi consideración permiten la mayor proliferación de los delitos informáticos, pues todos van ligados justamente a la información a los datos de personas. En ese orden de ideas el sistema financiero en sí debe buscar anticiparse a esto y que cuente con un sistema seguro y armónico entre todas sus instituciones, y esto implica toda una política que debe ser obligatoria. Ya que como se puede apreciar el sistema de identidad en el país no es del todo fiable. Nuestro Documento Nacional de Identidad (DNI), es un documento insuficiente para garantizar autenticidad en determinados supuestos. El hecho por ejemplo de que a las personas muy aparte de presentar su DNI, deba presentar declaraciones juradas, recibos por servicios como agua, luz, cable, etc. Son señales sutiles de que el DNI por sí solo no es suficiente, puesto que es sabido que muchas veces la información consignada en el DNI, no siempre estará actualizada, y ello depende de la disponibilidad de actualización de cada usuario.

Por ello teniendo en consideración de que nuestro sistema de identificación no es el más convincente y completo, ya que necesitamos documentación adicional para generar certera para acceder a ciertos servicios financieros, y sumado la alta incidencia de robo de celulares, y el enorme mercado de celulares “de segunda mano”, es evidente que el sistema financiero como tal debe tener unos altos estándares de reconocimiento de identidad. Por tal motivo es indispensable que exista una vinculación entre el deber de cuidado normativamente hablando, como políticas de prevención.

Sobre el bien protegido he de decir que este es múltiple en función al delito en sí. Por lo que, centrándonos en el delito de suplantación de identidad, si bien hay una afectación a la fe pública, es importante no olvidar que la razón de ser de este delito es que basa en usar una información esencial (la identidad, los datos de una persona) para generalmente realizar operaciones no autorizadas. En ese sentido considero fundamente centrar esfuerzos en salvaguardar el patrimonio de los usuarios y esto va de la mano con contar con un adecuado sistema de reconocimiento de los clientes.

Es evidente que el abrupto cambio social y la falta de previsión y anticipación de esta situación dieron como resultado tantos casos denunciados. Justamente en dicho año 2021, fue en donde el

ministerio público creo una división especializada en estos delitos. Por lo tanto, el problema no ha mejorado, más allá de las medidas que ha tomado el gobierno del Perú, es evidente que el problema radica en mi opinión en el aspecto normativo, esto no quiere decir que tampoco ignoremos otros factores de segundo orden, como lo son la precariedad de personal especializado disponible para esta materia en nuestro sistema de justicia, así como la ya conocida carga procesal, lo cual son datos no menores. Asimismo, los contabilizados oficialmente en nuestras distintas instituciones de justicia nos dice que el delito de suplantación de identidad ha sido por excelencia el que más agraviados ha generado, de allí la importancia en enfocar a esta figura, sin que esto por supuesto signifique ignorar los otros tipos de delito informático que como sabemos son variados y están en constante cambio.

Adicionalmente, considero que es importante destacar el hecho de que el delito de suplantación de identidad no debería solamente entenderse en el ámbito de delito informático contra la fe pública, sino también contra el patrimonio como se mencionó anteriormente, pues es lo que se ha visto a raíz de la gran mayoría de denuncias en los últimos 3 años, según datos del ministerio público. Y justamente el problema a investigar está enfocado en este delito. Pues, se han reportado muchos casos de otorgamiento de créditos, ampliaciones u otros servicios, de manera no autorizada por los titulares. Es decir, personas que se enteran que tienen deudas en el sistema financiero, evidenciándose que dichas deudas u aprobaciones de crédito se dieron sin su conocimiento, pero que finalmente fueron autorizadas por las entidades financieras, en virtud de que otra persona suplantó dichas identidades, para tener acceso a dicho producto, lo cual sígnica un perjuicio económico para la persona suplantada, pues esta termina con una gran deuda a su nombre. Por lo cual entra a tallar interrogante de como sucedió aquello, y si los controles de identidad utilizadas por las entidades financieras fueron los idóneos antes de otorgar o ampliar un crédito a los suplantadores. Sobretodo teniendo en cuenta la gran incidencia que tiene el delito de robo (Art 188. C.P.) de celulares en el país, lo cual da acceso a apps integradas, correos, de índole financiero. Tal como se ha visto en la evidencia empírica.

Por su parte en el delito de fraude informático es evidente que entra las diferencias que podemos encontrarle con la suplantación de identidad es que se necesita de mayor pericia y recursos tecnológicos para su realización, mientras que la suplantación puede darse de manera circunstancial o por el resultado de delitos previos tales como el robo de celulares los cuales tienen

alta comisión en el país, debido entre otras cosas a la cultura de la informalidad, la existencia y demanda del mercado de segunda mano de celulares robados y la conocida lentitud del sistema de justicia.

Finalmente respecto del delito de tráfico ilegal de datos en general su proliferación e impunidad en la actualidad en la cual los traficantes de información han podido y continúan delinquiendo a plena luz del día con la información de todos los peruanos se debe en primer lugar a la falta de coordinación de los distintos poderes del estado de poner el tema de la seguridad de los datos personales en la agenda nacional, y en segundo lugar al hecho de que son personas dentro de las instituciones que resguardan información privada no publica las que sin lugar a dudas filtran y proveen dicha información a estos traficantes. En ese sentido, en el ámbito financiero, las entidades financieras deben no solo velar por un sistema de ciberseguridad óptimo sino también sobre una adecuada gestión de la información que sus empleados manejan, ya que este delito en especial entra en concordancia con muchos otros delitos, este punto se profundizará más adelante.

CAPÍTULO 2: DESARROLLO NORMATIVO

2.1. Los delitos informáticos en la ley penal peruana

El primer antecedente que se tiene de los delitos informáticos es que esta figura penal se encontraba inicialmente en el artículo N.º 186, inciso 3 del código penal del año 1991. Es decir, esta figura se desprendía inicialmente como una modalidad dentro del delito de Hurto, por lo que aún no era una figura penal independiente. Sin embargo, posteriormente la figura de delito informático adquirido autonomía propia, esto en base a la Ley N° 27309: "Ley que incorpora los delitos informáticos al código penal[19]", siendo una ley de artículo único cuyo objetivo fundamental era Modificar el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo N° 635. El contenido de esta ley era lo siguiente:

Artículo 207°-A.-

"El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas. Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de la libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas"

Como puede apreciarse en este inciso, la definición base del delito informático está basada en el acceso no autorizado de un sistema de información informatizada. Es decir se hace énfasis solo en el acto de acceder a dicha información, es interesante apreciar que como circunstancia agravante está el hecho de si dicho acceso no autorizado a información se diese con finalidades de índole económica, es decir desde la óptica de nuestro derecho penal peruano, el delito informático no persigue un beneficio económico exclusivamente, si no que esta puede ser una de sus finalidades, lo cual tiene sentido, puesto que dentro del abanico de posibilidades de delitos informáticos, están las afectaciones por razones, tanto económicas, como de índole de comunicaciones, privacidad, información sensible, etc. El hecho de que la finalidad del delito informático fuese económica

[19] Ley promulgada el 17 de julio del año 2000 por el Diario Oficial "El Peruano"

definiera una pena más gravosa era un primer paso en el reconocimiento de que el mayor blanco de estos delitos era de orden económico, lo cual implicaba obviamente un impacto a nivel financiero. Si bien no estaba plasmado en la normal original, se puede presumir por qué se le da mayor relevancia a la finalidad económica del delito informático.

Artículo 207°-B.-

"El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multas"

Aquí en este inciso se enfoca en el acto del acceso no autorizado con el objetivo de generar perjuicio en los titulares de dicha información sistematizados, es decir, no se considera el acceso no autorizado que persiga un beneficio sino exclusivamente un perjuicio. Lo cual en cuestiones prácticas es posible, pero en el ámbito financiero por ejemplo esta premisa no sería realista, pues todo acceso no autorizado mediante lo comisión de delitos informativos, al menos en el ámbito financiero siempre perseguirá el beneficio económico.

Artículo 207°-C.-

"En los casos de los Artículos 207°-A y 207°-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.

2. El agente pone en peligro la seguridad nacional"

Sobre este inciso, se hacía énfasis en la circunstancia agravante que implicaba el uso de tecnología, dispositivos o conocimiento de información privilegiada en virtud de determinados cargos de gobierno. Era pues un apartado más enfocado en funcionarios públicos, aquellos que tenían mayor acceso a determinadas informaciones en comparaciones con el ciudadano común, obviamente este inciso iba más enfocado con finalidades de prevención de tráfico de datos, sobre datos gubernamentales, siendo el rubro de seguridad nacional el más relevante.

Como resumen se puede mencionar que en general esta modificación en estos artículos 207-A (interferencia, acceso o copia ilícita contenida en base de datos), 207-B (alteración, daño o destrucción de base de datos), 207-C (circunstancias agravantes); le daban mayor autonomía al delito informático, que como se mencionó anteriormente, surgió de una modalidad del delito de hurto. Asimismo, se puede mencionar como relevante al 207-D (tráfico ilegal de datos).

2.1.1. La Ley especial y sus modificaciones

Ahora bien, dentro de esta fase de consolidación de esta figura penal, el 22 de octubre del año 2013 se publicó la Ley Especial N.º 30096: "Ley de delitos informáticos", siendo que esta norma buscaba inicialmente prevenir y sancionar todas las conductas ilícitas que afectaran los sistemas y datos informáticos, en distintas modalidades y fines, en los cuales los delincuentes apoyaban su accionar con el uso la tecnología actual para cometer dichos actos ilícitos. El contenido de esta ley especial era la siguiente:

Capítulo I: Finalidad y objeto de la ley

Capitulo II: Delitos contra datos y sistemas informáticos

Capitulo III: Delitos informáticos contra la indemnidad y libertad sexual

Capitulo IV: Delitos informáticos contra la intimidad y el secreto de las comunicaciones

Capitulo V: Delitos informáticos contra el patrimonio

Capítulo VI: Delitos informáticos contra la fe pública

Capitulo VII: Disposiciones comunes

Posteriormente el 10 de marzo del año 2014, se publicó la Ley 30171: Ley que modifica la Ley 30096(Ley de Delitos Informáticos), siendo el claro objetivo de esta ley la modificación y adecuación de nuestra Ley especial en delitos informáticos a los estándares legales internacionales contenidos en el Convenio sobre cibercriminalidad (Convenio de Budapest). en la cual se agregaron a dichos tipos penales acceso ilícito (artículo 2º), atentado a la integridad de datos informáticos y sistemas informáticos (artículos 3º y 4º), interceptación de datos informáticos

(artículo 7º), fraude informático (artículo 8º), y abuso de mecanismos y dispositivos informáticos (artículo 10º) las palabras "deliberada e ilegítimamente", reafirmando que dichos tipos penales se cometen de forma dolosa, y se derogó el artículo 6º que tipificaba el tráfico ilegal de datos.

Como se mencionó en el párrafo anterior, esta modificación de nuestra ley especial se basó en gran medida al "El convenio sobre la Ciberdelincuencia" conocido internacionalmente como el "Convenio de Budapest"[20]. Ya que dicho convenio significó un hito en materia de seguridad a nivel informático, pues tal como lo menciona el investigador Carlos Guerrero Argote, dicho tratado se dio en un contexto en el cual el mundo empezaba a reaccionar, buscando hacerles frente a los delitos informáticos debido al crecimiento geométrico del uso de las TDI a través de mecanismos de homologación de normas de derecho penal sustantivo, estandarización de procesos penales y en base a la cooperación internacional (Guerrero, 2018)

Ahora bien, respecto del contenido de esta última modificación, su contenido (relevante en materia financiera) quedó definida de la siguiente manera:

Art 2: Acceso ilícito:

"El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa"

"Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado"

Este artículo, describe el primer acto del delito informático, el acceso, independientemente de la finalidad de este, de si se busca beneficio propio, perjuicio a tercero, o ambos. En ese sentido, en el ámbito financiero, este artículo estaría configurado en la gran mayoría de casos, pero también hay que considerar que no en todos los casos se necesita el uso de tecnologías para acceder o vulnerar sistemas de seguridad, es decir, también dichas vulneraciones pueden darse cuando estos sistemas no son lo suficientemente seguros. Pues con la era de la tecnología actual, cambiante todo

[20] Dicho Convenio se firmó en el año 2001, entrando en vigencia en la mayoría de países del Consejo de Europa en el año 2004

el tiempo, los mecanismos y sistemas de seguridad deben también periódicamente revisarse y renovarse justamente para evitar toda clase de accesos ilícitos.

Art 3: Atentado contra la integridad de datos informáticos:

"El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa"

En este artículo se sanciona el acto de afectar irremediablemente determinada información, ya sea de manera temporal o permanente. Esto configura como lo que se conoce como "Rasomware" o "Secuestro informático", los cuales han tenido mucha incidencia en estos años recientes[21] con el auge de las cripto monedas, o dinero electrónico, en donde mediante el uso de software malicioso, determinada información es cifrada, es decir, bloqueada e inaccesible para el usuario titular, y solamente puede ser recuperada mediante el depósito de considerables sumas de dinero o de lo contrario esta es diezmada o hasta destruida, similar a la figura penal del secuestro.

Art.4: Atentado contra la integridad de sistemas informáticos:

"El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa"

En este artículo, la descripción de la conducta ilícita es similar al artículo anterior, siendo la única diferencia el blanco a ser vulnerado, siendo en este caso no solamente información específica, sino todo un sistema informático, lo cual por supuesto lo vuelve una situación mucho más grave y perjudicial para quienes la sufren. En ese sentido, el "Rasomware" o "Secuestro informático" operan de la misma manera.

Art. 8: Fraude informático:

---

[21] INFOBAE (2022, 15 de noviembre) *Nuevos casos de ransomware o secuestro de datos donde piden rescate con Bitcoin:* Los ataques revelados están enfocados en víctimas de habla hispana que usan Windows.
Véase en: **https://www.infobae.com/america/tecno/2022/11/15/nuevos-casos-de-ransomware-o-secuestro-de-datos-donde-piden-rescato-con-bitcoin/**

“El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa”

“La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social”

En este delito en particular, los sujetos activos, inducen a error a las víctimas. Por ejemplo, en las transferencias financieras, ya sea a un destinatario no deseado, mediante el engaño, o como menciona el mismo artículo, clonación de datos, por ejemplo, clonación de tarjetas de crédito, páginas web oficiales de bancos, etc. Su naturaleza de afectación mediante la inducción al error, es similar al delito de estafa, obviamente en el contexto financiero mediante el uso de tecnologías informáticas. Es importante mencionar que tal como se ha visto en la evidencia empírica obtenida, el delito de Fraude informático por su manera de operar, es uno de los delitos informáticos con mayor incidencia a nivel financiero en nuestro país, esta condición la comparte con el siguiente delito que se verá a continuación.

Art. 9: Suplantación de identidad:

“El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años”

Este delito es otro de los que tienen mayor incidencia en el sistema financiero peruano, junto al delito de fraude informático. En el caso de la suplantación de identidad, esta puede darse tanto mediante el uso de recursos tecnológicos sofisticados como mediante formas poco sofisticadas, y esta última situación puede darse cuando los sistemas de seguridad de una entidad financiera no son lo suficientemente seguros, en especial cuando el acceso a estos sistemas se dé en base a celulares robados, por medio de las apps oficiales, correos, etc.

Como puede apreciarse, estos son los artículos más relevantes, y es interesante acortar que algunos de estos artículos, en los cuales se describen determinadas modalidades, se encuentran en

capítulos distintos. Por ejemplo: En el capítulo de delitos contra datos y sistemas informáticos se incluyen a los artículos 2, 3, 4, mientras que en el capítulo sobre delitos informáticos contra el patrimonio se encuentra el artículo 8, y finalmente en el capítulo sobre delitos informáticos contra la fe pública se incluye únicamente en el artículo 9.

Una mención aparte tiene el delito de tráfico ilegal de datos, el cual existió inicialmente en la ley especial en su artículo 6:

"El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años"

Sin embargo, este Artículo fue derogado por la Única Disposición Complementaria Derogatoria de la Ley N°30171, publicada el 10 marzo 2014. Y lo que se hizo en su lugar fue que este delito, reformularlo como Tráfico ilegal de datos personales y ubicarlo en el Articulo 154- A del Código Penal, en el capítulo correspondiente de delitos contra la intimidad, quedando definido de la siguiente manera:

Artículo 154-A.- Tráfico ilegal de datos personales

"El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años. Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior"

Estos cambios respecto del delito de tráfico de datos (ahora personales), respondieron a la Ley de protección de datos personales (Ley Nº 29733) y su Reglamento (Decreto Supremo Nº003-2013-JUS) tienen por objeto proteger los datos personales regulando el uso que las entidades públicas y privadas hagan de sus bancos de datos.

La línea de tiempo en los antecedentes y cambios recientes a nivel normativo demuestran que el tema de los delitos informáticos no ha sido una materia prioritaria para el Estado hasta años

recientes, tal como lo advierte el destacado abogado Oscar Zevallos Prado quien subraya el hecho de que la aprobación del Convenio de Budapest dentro de nuestra legislación nacional dio a lugar recién en el año 2019, siendo que el Poder Legislativo lo aprobó por Resolución Legislativa N.º 30913, en fecha 12 de febrero de 2019, y con fecha 10 de marzo de ese mismo año el Poder Ejecutivo lo ratificó mediante Decreto Supremo N.º 010-2019-RE; llamándole la atención el hecho de que nuestra ley especial sobre delitos informáticos databa del año 2013 y donde hubiera sido de mucha utilidad para que los operadores de justicia pudiesen haber tomado mayor consciencia sobre la protección de la seguridad informática y la cultura digital que debía existir en el país si dicho convenio hubiese sido aprobado con mayor antelación.(Prado 2020). De mi parte, me suscribo a esta opinión, y a la cual puedo agregar que indudablemente esta demora del Estado peruano se debió al extenso y profundo debate sobre el tema, pues era necesario adecuar nuestra legislación sustantiva previamente para la adhesión del convenio, sin embargo, dicha demora en aquella adecuación indudablemente ha puesto en riesgo a la seguridad informática de los usuarios, especialmente en materia financiera. Justamente por ello recién en el año 2021 en junio, se creó la Primera Unidad Fiscal Especializada en Ciberdelincuencia, la cual brinda acompañamiento técnico de los fiscales a través del uso de recursos tecnológicos. Esta unidad que ya viene operando en su primer año, trabajando con 34 distritos fiscales, y en lo que va del año A escala nacional, entre enero y abril de 2022, el Ministerio Público ha recibido 7,297 denuncias, siendo que de estas que son investigadas a nivel de fiscalía, quienes recurren al uso de mecanismos tecnológicos para rastrear las evidencias digitales.

Si bien estamos ante una reacción un tanto tardía del Estado peruano, posiblemente las recientes políticas a favor de la lucha contra los delitos informáticos se han concretado más como consecuencia de la Pandemia a principios del año 2020, que por una política de Estado. Pues fue durante la pandemia en donde el comercio electrónico y los servicios digitales expandieron su uso y llegada a la gran mayoría de usuarios y como consecuencia de todo crecimiento, empezaron a darse muchos casos de delitos de naturaleza informática, afectando a distintos sectores, sobre todo la banca.

Por lo tanto, que el Estado Peruano reaccione tarde es un claro indicio de la preocupación planteada inicialmente en esta investigación. Ya que a nuestro país le tomo cerca de 13 años para poder contar con una ley especial (Ley de delitos financieros); la cual dicho sea de paso fue fruto

de diversos proyectos de ley muy interesantes. Ahora bien, la legislación nacional apenas se está implementando y hay varios aspectos que a nivel normativo todavía no están definidos, sobretodo concerniente a las responsabilidades ante la comisión de estos delitos. No se evidencia claridad en la normativa sobre qué tipo de responsabilidad tendría una entidad financiera en caso de delitos informáticos. Ya que como es sabido, el derecho penal en general le dedica un mayor desarrollo al Sujeto activo en las figuras penal, al describir las conductas atribuibles de tipicidad. Sin embargo, como se mencionó inicialmente, las entidades financieras son sujetos pasivos, dentro de la estructura de los delitos informáticos, por ende, la ley penal no nos puede definir el rol que asume en este esquema. Por ello, una norma de otra naturaleza, como la administrativa por ejemplo podría definirnos de mejor manera, el rol y la responsabilidad que las entidades financieras tienen en estos casos. Definiéndose los límites y responsabilidades.

2.2. Legislación Chilena sobre Delitos Informáticos

En el caso de Chile, respecto de la figura de los delitos informáticos en la ley penal chilena se cuenta con la siguiente información[22]:

El 7 de junio de 1993 entró en vigencia en Chile la Ley N°19 223, "Ley sobre delitos informáticos". Esta ley tenía como finalidad proteger a un nuevo bien jurídico como es: "la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan".

Es decir, se buscaba que se preservase ante todo la intangibilidad de la información en sistemas informáticos. Respecto de su contenido, la Ley N°19 223, como ley especial, constaba de 4 artículos, que enunciaban lo siguiente:

-Artículo 1.

"El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Como consecuencia de estas conductas se afectaren

[22] MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile.

los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

Es interesante ver que, desde principios de los años 90, la legislación chilena ya desarrollaba en su normativa parte de las características propias del "Rasomware" o "Secuestro informático", aunque claro, en esta normal, no se considera ningún fin económico, sino simplemente el prejuicio de generar el daño

-Artículo 2.

"El que, con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".

El sentido de articulo, dado dicho contexto de esos años, esta posiblemente mas orientado a la prevención del espionaje, tanto para personas naturales como instituciones, empresas.

-Artículo 3.

"El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio".

El contexto de este articulo esta posiblemente orientado a la figura del sabotaje, es decir, no se trata de una destrucción de información aleatoria, sino de toda una estrategia de afectación informática, posiblemente las víctimas potenciales de este de delito eran instituciones, tanto públicas o privadas y no tanto personas en particular.

-Artículo 4.

"El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

En este artículo en particular, se sanciona con mayor rigor a quienes teniendo cargos de confianza a información sensible, los difunden. Evidentemente este tipo de artículos en ese entonces, estaban más destinados a las instituciones. Tanto públicas como privadas, esto por supuesto incluía a las entidades bancarias.

Como puede apreciarse, esta ley especial de principios de los años 90, buscaba catalogar de manera armónica, una serie de situaciones acorde a las posibilidades tecnológicas de ese país en esos años. Adicionalmente a ello, se contemplaría los delitos informáticos de sabotaje y espionaje informáticos, aunque las definiciones de dichas conductas no estaban del todo desarrolladas, es decir adolecían de una aparente ambigüedad o de interpretación más abierta. De otro lado, no se incluyeron muchas otras modalidades de delito informático, quizás por la postura de no catalogar los posibles actos delictivos y solo mencionar sus alcances de manera general quizás apuntan al hecho de que en virtud de las tecnologías de la información se van renovando constantemente, sucederá lo mismo con los delitos informáticos y sus modos de proceder.

Ello justificaría dicha postura para evitar que dicha norma quedase obsoleta. Mas allá de las razones, es destacable que Chile fue un país pionero en la Región en poner en agenda nacional a los delitos informáticos y su regulación. De otro lado la doctrina chilena, también consideraba desde ese entonces a los delitos informáticos como pluriofensivos. También la doctrina chilena solía clasificar los tipos penales de su ley especial en: a) delitos de espionaje informático y b) delitos de sabotaje informático (Huerta y otros, 1996)

2.2.1 La nueva ley chilena de delitos informáticos

Justamente el 20 junio del año 2022, se publicó la Ley Nº21459, cual estableció normas sobre delitos informáticos, derogando la precitada Ley 19913 y modifica otros cuerpos legales, con el objeto de adecuarlos a las exigencias del Convenio sobre la Ciberdelincuencia de Budapest[23]. Esto significa una segunda gran reforma sobre los delitos informáticos. Entre los artículos más relevantes tenemos los siguientes:

-Art. 1: Ataque a la integridad de un sistema informático: El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en sus grados medio a máximo.

[23] Ley Nº21459, disponible en: **https://www.bcn.cl/leychile/navegar?idNorma=1177743**

En ese artículo se entiende que se sanciona afectaciones de naturaleza sumamente sofisticada, posiblemente mediante el uso de software especializado.

-Art 2: Acceso ilícito: El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimos a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por este (…)

En este artículo, el acceso ilícito Chile lo considera tanto el que acceda sin permiso a determinada información, como también, cuando determinados agentes, teniendo autorización para acceder a terminada información, terminen excediendo dicho umbral, esto en el ámbito financiero es sumamente relevante, puesto que si por ejemplo determinados funcionarios estuvieren investigando financieramente a un sujeto por sospechas corrupción o lavados de activos, dicho accionar de "seguimiento" no podría tocar la información de otros usuarios, así fuese por error, estos funcionarios estarían cometiendo dicho delito, ya que el acceso licito es permitido siempre y cuando esté autorizado y desarrollado estrictamente en los límites pre establecidos, generalmente por un juez.

-Art 3: Interceptación ilícita: El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio. El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en sus grados medio a máximo

Este articulo y su accionar está más ligado a las telecomunicaciones, pero teniendo en cuenta que muchas operaciones bancarias se realizan hoy en día mediante teléfonos móviles, se considera relevante a tener en consideración. Pues generalmente las emisiones electromagnéticas utilizadas para el acceso a determinadas informaciones de telecomunicaciones se dan mediante equipos especializados, consolas que generalmente están a cargo de la Policía, y del Ejército. Cuando se da una orden judicial de interceptación en base a una investigación fiscal, mediante la consola se

ubica y triangula la posición del objetivo a ser rastreado y seguido, por ejemplo, un teléfono. Pero dicha actividad no es milimétrica, y tiene un umbral de acción de muchísimos metros, incluso kilómetros, de allí a que sin buscarlo se pueda tener acceso a información colateral no buscada inicialmente. De allí que considero importante que la norma establezca y advierta de estos límites.

-Art 4: Ataque a la integridad de los datos informáticos: El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos.

Este artículo define hasta cierto punto lo visto con el uso de los ransomware, aunque sin especificación de si se busca un beneficio económico o solamente el perjuicio de los titulares.

-Art 5: Falsificación informática: El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo. (…)

En este artículo, Chile busca penar aquellas que implican el uso de documentos físicos falsos que posteriormente son digitalizados y presentados como verdaderos. No confundirlo necesariamente con el fraude informático. Aquí la falsificación puede darse tanto de manera sofisticada como de manera convencional. Puesto que hoy en día, la dependencia del papel se ha reducido, y muchos papeles físicos son digitalizados, escaneados. Por ello es importante interesante tomar en cuenta este tipo de modalidad a considerar en la normatividad peruana.

-Art 6: Receptación de datos informáticos: El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado.

Básicamente, se sanciona el comercio de información, que de por si es un acto ilegal, porque la información solamente puede ser publica, por ende, gratuita, e información privada. Obviamente lo que se comercializa es información privada. Este tipo de delitos deben ser fuertemente combatidos, pues justamente el comercio ilegal de información es uno de los mayores insumos que les permiten a los distintos estafadores y clonadores de tarjetas de crédito, páginas web entre otros; el poder concretar sus actos delictivos. De allí a la importancia de la seguridad de la

información, puesto que, sin información, el accionar de los cibercriminales se vería sustancialmente disminuido. En ese sentido considero fundamente que esta sea una de las prioridades en la ley penal peruana, pues como sabe, actualmente en nuestro país, hay una cultura del comercio de información sin ningún tipo de limitación ni sanción.

-Art 7: Fraude informático: El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado:

1) Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales.

2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales.

3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales.

(…) Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito.

Tal como se puede apreciar en este artículo, y similar a la figura en la ley peruana, el fraude informático se basa en el engaño en la inducción a error, similar a la figura de la estafa, solo que esto mediante recursos digitales. Lo que me parece interesante de esta versión del fraude informático en chile es que en su último apartado vemos claramente que considerara como autor a aquel que de una forma u otra facilite la comisión de dicho delito, por lo tanto dentro de esa premisa cabria perfectamente la figura de la negligencia, y si lo trasladamos esto al ámbito financiero en estricto, si una entidad financiera tuviese un sistema de seguridad deficiente, y a sabiendas de las debilidades de dicho sistema, no lo mejorase, y esto terminaría permitiendo que se dieran casos de fraude informático u otro delito informático relevante, esta entidad podría tener responsabilidad, por omisión, por no hacer lo necesario para evitar dichas situaciones. Esto es muy importante, pues de manera indirecta si lo trasladamos al ámbito financiero traslada un deber de responsabilidad a

una entidad bancaria a hacer todo lo que esté en su alcance, dentro de lo razonable por supuesto, ha contribuir mediante un sistema de seguridad optimo, de la prevención de estos delitos informáticos hacia sus usuarios. En la legislación chilena ya vemos esta obligación de cumplimento de las entidades financieras chilenas en pro de la prevención de estos delitos, mas no en el caso peruano. Por ello, dicho deber de prevención debe estar establecido en el Perú, claramente en las normas vigentes como ya lo viene haciendo Chile, como se verá posteriormente. Además, no olvidar que en Perú hoy en día hay muchos casos de fraude informático, como la creación de páginas webs oficiales falsas, entradas a conciertos falsos, facturas falsas, préstamos falsos, entre otros.

-Art 8: Abuso de los dispositivos: El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 7° de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales

Este artículo en particular se refiere a los casos en los que, por medio del robo de equipos móviles, el delincuente acceda a otra información ligada a dichos teléfonos. Como sabemos, hoy en día, la gran mayoría de usuarios, no solamente en Chile y Perú, sino a nivel global utilizan el teléfono para todo, y muchas tarjetas, y credenciales están ligadas a los teléfonos móviles de sus titulares. De allí la importancia que las entidades financieras gocen de los mecanismos adecuados para una rápida acción ante casos de pérdida de dispositivos móviles por robo principalmente. Otro aspecto relevante de esta ley es que se modifican otros cuerpos legales tales como:

-Código Procesal Penal: Incorporación del art. 218, estableciendo una obligación de preservación provisoria de datos informáticos. Lo cual permite al Ministerio Público de ese país a requerir a cualquier proveedor de servicio “la conservación o protección de datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición hasta que se obtenga la respectiva autorización judicial para su entrega”. Lo cual es muy relevante para agilizar la obtención de información relevante en estos casos a los operadores de justicia.

-Ley 19913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos, en la cual se incorporan los delitos tipificados por esta nueva ley dentro del artículo 27 inciso a) de la Ley 19913, en donde se sanciona la ocultación o disimulo del origen ilícito de determinados bienes, a sabiendas que provienen de la perpetración de hechos constitutivos de alguno de los delitos que se indican.

-Ley 18168, Ley General de Telecomunicaciones: Sobre esta norma, se crea un nuevo delito de acción pública, por lo que en caso de que se vulnere el secreto durante una investigación penal, contemplado en los artículos 218, que regula la preservación provisoria de datos informáticos; el 219, que regula la copia de comunicaciones o transmisiones; y 222, que regula la interceptación de comunicaciones telefónicas.

Esto otorga mayor hermetismo y confidencialidad y reserva de las investigaciones, evitando potenciales filtraciones ya sea por motivos de corrupción.

2.2.2.: La responsabilidad penal de las personas jurídicas en Chile. Ley 20393

Esta norma versa sobre la responsabilidad penal de personas jurídicas, es una ley que fue promulgada inicialmente en fecha 25 de noviembre del año 2009, y publicada el 02 de diciembre de ese mismo año.[24] Esta norma establece desde su artículo primero una serie de delitos contemplados dentro de la responsabilidad jurídica de las personas jurídicas. Siendo inicialmente contemplados los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho. Así como el procedimiento para la investigación y establecimiento de dicha responsabilidad penal, la determinación de las sanciones procedentes y la ejecución de éstas en base a su código penal, código procesal penal y leyes especiales.

En ese sentido su artículo 3 establece que de responsabilidad penal de las personas jurídicas estará establecido en función de los delitos señalados en el artículo 1° que fueren cometidos directa e inmediatamente en su interés o para su provecho, por sus dueños, controladores, responsables, ejecutivos principales, representantes o quienes realicen actividades de administración y

[24] Véase en: **https://www.bcn.cl/leychile/navegar?idNorma=1008668**

supervisión, siempre que la comisión del delito fuere consecuencia del incumplimiento, por parte de ésta, de los deberes de dirección y supervisión. Es decir, en esta norma se sanciona no solo el acto doloso sino también la omisión o falta de prevención

Así mismo, el artículo establece que serán también responsables las personas jurídicas por los delitos cometidos por personas naturales que estén bajo la dirección o supervisión directa de alguno de los sujetos mencionados en el inciso anterior. Esto lo podemos entender en el sentido de que la persona jurídica esté al tanto de lo sucedido y no reaccionen oportunamente o peor aún, dirección los actos a favor de la comisión de los delitos previamente contemplados en la norma.

De otro lado el mismo artículo establece que las personas jurídicas no serán responsables en los casos que las personas naturales indicadas en los incisos anteriores, hubieren cometido el delito exclusivamente en ventaja propia o a favor de un tercero. Esto considero sumamente relevante, sobre todo en los casos en que un trabajador de una persona jurídica, actúan a espaldas de las directrices y políticas ya establecidas de sus empleadores y responsables funcionales.

Finalmente destacamos el artículo 4, en donde se establece la necesidad de la implementación de un modelo de prevención de los delitos ya contemplados, en base a un encargo de estas políticas de prevención. Destacándose dicho encargado cuenta con total autonomía respecto de la Administración de la Persona Jurídica, de sus dueños, de sus socios, de sus accionistas o de sus controladores. No obstante, podrá ejercer labores de contraloría o auditoría interna.

En mi opinión, la estructura de esta normativa de responsabilidad de la persona jurídica, de contar con un sistema de prevención de delitos previamente contemplados es un marco legal idóneo para justamente combatir a los delitos informáticos. Lo cual evidentemente se concretó en el caso chileno posteriormente

2.2.3.: La incorporación de los delitos informáticos en la Ley 20393

En la actualidad la Ley N.º 20.393 contempla 16 delitos por los cuales se puede establecer responsabilidad penal de las personas jurídicas en el caso de delitos informáticos. A partir de la vigencia de esta nueva Ley, la Nº21459, es decir desde el 20 de diciembre de 2022 se agregaron al catálogo de delitos ya existentes los 8 delitos informáticos ya enunciados anteriormente en la

nueva ley de delitos informáticos. En cual se incorpora dentro del listado de delitos establecidos en el art. 1° los delitos contemplados en el título I de la ley de delitos informáticos. Esto obviamente a implicado para la administración de las personas jurídicas que los modelos de prevención de los delitos previamente contemplados que estén vigentes o que estén certificados, deberán actualizarse incluyendo el nuevo catálogo de ilícitos, los delitos informáticos ya mencionados, con la finalidad de acceder a los beneficios propios de la Ley Nº20.393.

Esta última modificación la considero sumamente relevante y creo firmemente que es la vía normativa más idónea para garantizar una mejor política preventiva de las personas jurídicas, en especial las entidades financieras, en garantizar mejores estándares de seguridad informática. De otro lado, el hecho de que los delitos informáticos sean tratados y prevenidos en el caso de entidades financieras mediante este cuerpo legal trae ventajas significativas, normativamente hablando tanto para la mejor individualización de las conductas ilícitas en el curso de la investigación, ya que la misma norma de Responsabilidad de personas jurídicas en su última modificación incorpora circunstancias modificatorias de responsabilidad penal, en particular, como atenuante, la cooperación eficaz, y como agravantes, a modo ejemplar, cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función. Lo cual entra total sinergia respecto de la naturaleza de una entidad financiera, su rol como salvaguarda de la información no pública y la necesidad de establecerse correctamente las responsabilidades entre un sistema jerárquico de roles y funciones dentro de una persona jurídica.

2.3. Normativa administrativa peruana. La Ley N. º 30424

Como es sabido, la Ley N° 30424 que regula la responsabilidad administrativa de las personas jurídicas y modificatorias, se dio mediante Decreto Supremo N° 003-2019-EF, estableció que una persona jurídica estará exenta de responsabilidad administrativa, siempre que haya adoptado e implementado en su organización, con anterioridad a la comisión del delito, un modelo de prevención adecuado a su naturaleza, riesgos, necesidades y características. Dicho reglamento además establece los elementos mínimos que debe contener dicho modelo de prevención para

justamente prevenir la comisión de los siguientes delitos: Cohecho, Lavado de Activos, Financiamiento del terrorismo, Colusión y Tráfico de influencias.

Como puede apreciarse, de los delitos a considerar relevantes a prevenir, no se encuentra a los delitos informáticos, lo cual me parece algo que debe agregarse en nuestra normativa, es decir, replicar en ese sentido lo establecido recientemente por la legislación chilena. Puesto que su sistema de políticas de prevención y delimitación de las responsabilidades en base a funciones y jerarquías en una entidad financiera tales como directivos, responsables, ejecutivos principales, representantes o quienes realicen actividades de administración y supervisión, y trabajadores en general siempre que la comisión del delito fuere consecuencia del incumplimiento, por parte de ésta, de los deberes de dirección y supervisión. Y creo que dicha medida estaría ampliamente justificada en nuestra norma administrativa, pues los delitos informáticos representan una problemática de importante relevancia actual, en especial en el ámbito financiero, más aun teniendo en cuenta que nuestra propia normativa penal respecto de los delitos informáticos no ha desarrollado nada respecto del rol que asume una entidad financiera en este de delito, tal como lo demostrado la evidencia empírica registrada por nuestros operadores de justicia.

CAPÍTULO 3. DISCUSIÓN

3.1. Los delitos y su ejecución

Como se ha podido apreciar a lo largo de esta investigación, la proliferación de estos casos se debe principalmente a los factores tanto de orden socioeconómico como normativos. En ese sentido es importante vislumbrar que la ejecución de estas prácticas antijurídicas (Fraude informático, suplantación de identidad y tráfico ilegal de datos personales) entran en consonancia con las ya mencionadas carencias tanto logísticas como normativas para poder tanto prevenir como regular y sobre todo reducir su impacto en el ámbito financiero. Si bien estos delitos por su propia naturaleza se apoyan en el uso de las tecnologías, no son el único recurso, pues determinadas circunstancias de naturaleza distinta también pueden contribuir a la consumación de estas, tales como la participación de otros delitos, contar con normas poco desarrolladas sobre estos casos y una mala gestión respecto del control y salvaguarda de los datos, sistemas de seguridad ineficientes, negligencias por parte de trabajadores, etc. Esto es algo que puede aquejar no solo al sistema financiero, sino incluso en general en cualquier entidad que maneje información no pública. En ese sentido la forma como se ejecutan estas 3 figuras, las más relevantes por ahora en el ámbito financiero a mi criterio, se dan en menor o mayor medida de la siguiente manera.

3.1.1 El fraude informático

Este delito se consolida en base a varias modalidades, incluso pudiendo entrar en conjunción con otros delitos tales como el robo, la suplantación de identidad en algunos casos y por supuesto con el tráfico ilegal de datos personales.

3.1.1.1. Modalidades. Entre las modalidades más denunciadas según la Policía nacional en el año 2022[25] tenemos las siguientes:

a). Phishing

En esta modalidad los ciberdelincuentes clonan sitios web oficiales, en la mayoría de los especialmente de entidades bancarias, para engañar a los usuarios y obtener sus datos personales, como nombres, números de teléfono, DNI y claves de servicios financieros. Una vez obtenidas los datos, los ciberdelincuentes realizan una llamada telefónica a la víctima, haciéndose pasar por una supuesta entidad financiera en la que le advierten de un ingreso fallido a su cuenta y le piden que le entreguen el token de seguridad que llegará a su celular para verificar su identidad. Con esta información, los estafadores realizan transferencias bancarias ilegales y cometen el fraude informático, tal como lo menciona la autoridad policial[26]. Esta modalidad también se aplica para el delito de suplantación de identidad. Esta fue la modalidad más denunciada durante todo el año 2022 con 720 registros.

b). Carding

Esta modalidad versa sobre las compras ilegales en línea. Los ciberdelincuentes acceden de forma ilegal a las tarjetas bancarias de las víctimas para realizar compras de pequeños montos, con el objetivo de no despertar sospechas rápidamente. Generalmente siendo blancos las personas con buen historial crediticio y fondos disponibles, utilizando sus tarjetas para compras de gran valor, principalmente en sitios web de comercio electrónico internacional. Esta modalidad es compatible con la suplantación de identidad. De otro lado esta fue la modalidad más denunciada durante todo el año 2022 con 472 registros.

c). SIM Swapping

En esta modalidad, los ciberdelincuentes que hayan podido obtener los datos personales de sus víctimas, mediante por ejemplo tráfico ilegal de datos, proceden posteriormente a bloquear la tarjeta SIM (chip) del teléfono celular de la víctima mediante el contacto con las empresas de telefonía móvil. Luego, de aprobada dicha solicitud, los delincuentes duplican la tarjeta SIM y utilizan los datos capturados previamente para acceder a la banca digital de las víctimas, realizando

[25] Véase en: **https://infogram.com/delitos-informaticos-en-el-peru-1h7k2305y89xv2x**
[26] El coronel PNP Luis Huamán Santamaría, jefe de la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía Nacional del Perú

transferencias, solicitudes de préstamos y giros. Todo esto sin que la víctima haya perdido su celular en ningún momento de su poder. Esto posible por supuesto con la conjunción de otro delito, el de tráfico ilegal de datos personales.

Por otro lado, esta modalidad es una de las más difícil de rastrear y sobretodo prevenir, por lo que, en caso de problemas con la operadora de telefonía móvil, es crucial que los usuarios informen de inmediato a su proveedor de telecomunicaciones. Siendo una de las señales más relevantes es cuando la señal del equipo celular se corta de manera inesperada, en esos casos, las autoridades recomiendan buscar comunicación de cualquier otro por otro medio con sus proveedores de telefonía para reportar dicho incidente y así evitar convertirse en nuevas víctimas de fraudes informáticos. En el caso de esta modalidad, durante todo el año 2022 obtuvo 238 registros de denuncias.

d). Thief Transfer

La cuarta modalidad más frecuente se basa en el uso de teléfonos móviles robados o extraviados para cometer fraudes informáticos. Es decir, implica la participación de un delito previo, el robo de celulares. En estos casos, los delincuentes retiran la tarjeta SIM del celular que ya ha sido bloqueado por robo o pérdida por parte de la víctima; y la colocan en otro dispositivo para acceder a toda la información y cometer el fraude informático. Esta modalidad conto en el año 2022 con un total de 210 denuncias registradas.

e). Vishing

Finalmente, otra modalidad importante a mencionar es el Vishing, en donde los ciberdelincuentes engañan a sus víctimas a través de llamadas fraudulentas en las que se suplanta la identidad de una empresa, organización o persona de confianza para obtener información personal y confidencial de los receptores de estas llamadas fraudulentas.

Es importante mencionar que en esta modalidad en específica operan ciberdelincuentes de mayor especialización y recursos, puesto que según lo menciona la DIVINDAT, estos en su mayoría son de origen peruano, mientras que las cuentas receptoras de las transferencias ilegales suelen estar a nombre de ciudadanos extranjeros. Asimismo, la policía ha detectado la colaboración de cómplices en diferentes ciudades del país y la participación de hombres y mujeres en estos delitos, con los hackers principalmente hombres entre 25 y 30 años de edad. Asimismo, respecto

de sus zonas de operaciones, estas se encuentran fuera de Lima, sobre todo en la selva del Perú, Iquitos y otras ciudades de la zona oriente del país, siendo desde dichas zonas en donde realizan coordinaciones con cómplices en Lima Sur o Lima Norte para su accionar delictivo. Esta modalidad cuesta con 181 denuncias registradas en todo el 2022.

3.1.2. La suplantación de identidad

Tal como se ha visto tanto desde el punto de vista jurídico como practico, este delito guarda relación con el delito predecesor, representando muchas veces, la siguiente etapa del acto fraudulento en perjuicio de la víctima y del sistema financiero. Sin embargo, tal como se mencionó en pasajes anteriores este delito puede darse como resultado de delitos previos, como también por vulneración de los filtros de seguridad, los cuales puede implicar o no, el uso de recursos informáticos, asi como el aprovechamiento por parte de los delincuentes de determinadas circunstancias que exponen a la víctima a dicha situación.

3.1.2.1. Modalidades

En ese sentido las modalidades más usuales en que los delincuentes pueden llevar a cabo la suplantación son:

-Sustracción y perdida del DNI: De allí la importancia de reportar a la brevedad el extravío o robo.

-Falsificación de Firma: Esto va de la mano con de la perdida y robo de DNI, sumado también a que las firmas de muchas personas ya están digitalizadas, en documentos escaneados, etc. El tráfico ilegal de datos por lo general tiene repercusiones en este ámbito.

-Perfil falso en Redes sociales: Esto apunta tanto para suplantar como para obtener informaciones importantes del entorno de las víctimas, así como muchas veces validar datos accesorios como el correo electrónico registrado, el número de celular registrado, los cuales son elementos esenciales para la suplantación en materia financiera.

-Contratación de Servicios: Siendo estos más las consecuencias de la suplantación en donde generalmente la víctima se percata de manera tardía de que está asumiendo contrataciones, o prestaciones, aprobaciones de crédito o cualquier movimiento financiero no aprobado.

- Phishing y el Carding: Estas modalidades ya descritas en el Fraude informático, también están presentes en la suplantación

-El robo de celulares: El acceso a celulares robados, o sus Chips permiten a los delincuentes acceder a la información financiera alojadas en dichos equipos.

-El tráfico ilegal de datos personales: Si bien se trata de otro delito, este es de los mayores proveedores de información que permiten a los delincuentes, perpetrar, consumar, como dar inicio a las actividades delictivas que apuntan a las entidades financieras en materia de delitos informáticos. Tal como se verá a continuación

3.1.3 El tráfico ilegal de datos personales

Como mencione en el párrafo anterior. Este delito es de suma relevancia, pues si bien, no ostenta tanto número de denuncias, como los otros dos delitos estudiados; su impacto en la sociedad es más que evidente. Pues permite la consolidación de los otros dos delitos antes mencionados e incluso del resto de delitos informáticos en general. Así como la consolidación de otras figuras penales tales como el robo, extorsión, sicariato, acoso, entre otros. En tiempos recientes, las autoridades del país están aprendiendo a reconocer el peligro que implica este delito, no solo a nivel financiero, sino a nivel social. Los siguientes casos que se describirán a continuación solo reflejan la relevancia de este delito y por qué a día de hoy están en la agenda nacional, de las entidades financiera, policía, fiscalía y gobierno central en general.

En principio esta problemática de las filtraciones y venta de información es un problema cultural, se da en todos los estamentos de nuestra sociedad. Tanto a nivel de RENIEC, entidad encargada del registro civil, ha habido denuncias respecto de la venta de información, así como a nivel de MIGRACIONES, entidad encargada de registrar el registro migratorio de los peruanos. Muchas veces se han dado denuncias respecto a la venta indiscriminada del movimiento migratorio

de las personas por parte de empleados, esto es un tema que siempre se vio por ejemplo a nivel de la farándula, en donde siempre la prensa de espectáculos siempre tenía acceso exclusivo sobre el destino de muchos personajes públicos, conducta obviamente ilegal, aunque por muchos años sin ser tipificado oportunamente y sobretodo normalizado por nuestra sociedad.

3.1.3.1 Filtración masiva de datos: Casos emblemáticos y de actualidad

En nuestra sociedad, la problemática de la trafica ilegal de datos adquirió una relevancia y gravedad nunca antes vista. El punto de quiebre se dio justamente por a mediados del año 2022. Uno de estos casos ha sido el de la ya desaparecida Plataforma "Zorrito Run Run", la cual significó uno de los mayores escándalos de filtración de datos personales en el Perú, pues llevó la problemática de la venta ilegal de datos de nuestra capital a otro nivel. Esta plataforma era operada por una red de ciberdelincuentes, quienes se habían hecho de manera ilícita por supuesto con los datos personales de millones de peruanos, obtenidos de instituciones tanto públicas como privadas, con la cual lucraban. En su momento La Asociación de Bancos del Perú (Asbanc) advirtió mediante una carta enviada a la Presidencia del Consejo de ministros (PCM) y al Ministerio de Justicia y Derechos Humanos (Minjusdh), sobre la filtración de datos personales[27].

La manera en la que operaban estos sujetos era que, mediante su WEB, ofrecían nombres, apellidos, DNI, huella digital y dirección, a partir de esta información podían realizar estafas virtuales, fraudes y suplantación de identidad, según explicó el fiscal Juan Francisco Silva a la agencia Andina[28]. Este caso por supuesto implicó un pronunciamiento del Gobierno peruano, que en colaboración con Asbanc y otras instituciones llevaron a cabo determinadas medidas correctivas para intentar frenar el daño causado por la ciberdelincuencia. La plataforma en cuestión fue dada de baja rápidamente. Sin embargo, si bien dicha plataforma quedo inoperativa, actualmente este grupo organizado continúa operando esta vez por otras plataformas tales Whatsapp y Telegram, mediante el uso de bots, y mensajes automatizados. Esto se ha dado debido a que la información

[27] Infobae- PERU (2022, 24 de mayo) 'Zorrito Run Run': Esta es la plataforma que filtró y ofertó los datos personales de los peruanos. Véase en:
https://www.infobae.com/america/peru/2022/05/20/zorrito-run-run-la-plataforma-que-filtra-y-oferta-los-datos-personales-de-los-peruanos/
[28] IBID

ilícitamente obtenida sigue actualmente en poder de este grupo criminal, que como se ha constatado también contaban con información financiera, tributaria, etc.

Reciente a finales de mayo de este año 2023, la DIVINDAT ha podido capturar a dos de los presuntos implicados en estos delitos[29], siendo estos rápidamente procesados por los delitos de acceso ilícito y tráfico ilegal de datos personales por la creación de dicha plataforma "Zorrito Run Run" purgando actualmente 15 meses de prisión preventiva mientras continúan las investigaciones[30]; ya que la DIVINDAT está detrás del resto de integrantes, puesto que según información policial, el grupo delictivo que continua operando en la plataforma Telegram contaría con más de 350 integrantes.

A este preocupante caso también podemos mencionar el caso reciente del nuevo Bot de Telegram conocido como: "Himiko Data"[31], descubierto a finales de marzo del presente año 2023, el cual ha surgido como una suerte de clon de "Zorrito Run Run". Se presume que este nuevo Bot, haya adquirido una copia del archivo de información original sustraído por la plataforma anterior. Lo más desconcertante sobre este nuevo Bot es que a diferencia del anterior, este otorga a cualquier usuario que lo requiera información personal de cualquier peruano, completamente gratis.

A este catálogo de casos conocidos podemos agregar también conocidos casos de TRANDING, las comúnmente llamadas Ofertas de trabajo Fraudulentas, La estafa de los Likes, entre otros. Esta modalidad que esta de "moda" actualmente por los ciberdelincuentes lleva hasta fines de junio del presente año 143 denuncias de estafas virtuales, principalmente en Lima Metropolitana, con más de 270 agravados por un monto de 2.1. Millones de soles según datos de la policía. La forma de operar consiste en que un número desconocido, contacta con la victima por Whatsapp, Facebook ,Telegram y se presentan como representantes de una empresa, posteriormente ofrecer trabajos

[29] TV PERÚ (2023, 26 de mayo). "*DIVIAT ALLANAN VIVIENDAS Y CAPTURAN A DOS CIBERDELINCUENTES*" Véase en reportaje periodístico en: **https://www.youtube.com/watch?v=7IpuEGi514g**

[30] Simón, G (2023, 07 de junio). *Zorrito Run Run: dictan 15 meses de prisión preventiva contra hackers que vendían datos personales.* La República. Véase en: **https://larepublica.pe/sociedad/2023/06/07/zorrito-run-run-dictan-15-meses-de-prision-preventiva-contra-hackers-que-vendian-datos-personales-307440**

[31] Veliz, J. (2023, 24 de marzo). *Datos peruanos expuestos y gratis: nuevo bot de Telegram entrega DNI, dirección, foto, firma y huellas.* RPP. Véase en: **https://rpp.pe/tecnologia/mas-tecnologia/telegram-bot-himiko-data-expone-datos-personales-de-peruanos-noticia-1474670?ref=rpp**

tales como dar " Likes" (Boton Me gusta) a diversas paginas ya sea en Youtube, Facebook u otras redes sociales, una vez "completada la tarea" proceden a solicitad datos de la víctima, nombre, ubicación, número de cuenta a la cual se "pagara", entre otros datos relevantes, siendo que efectivamente realizan el pago, principalmente monto menores como S/.30 o S/.50 soles generando "confianza" en la victima. Sin embargo, ya dado el momento, y con la información financiera otorgada estos ciberdelincuentes acceden a dichas cuentas y realizan transferencias no autorizadas a cuentas receptoras de terceras personas para perjuicio de la víctima. Existen otras variantes en esta modalidad que implica pedir un dinero a cambio de facilitarles a las víctimas el cobro de un premio que supuestamente "han ganado". Todos estos casos están siendo actualmente preocupación de las autoridades[32].

Por ello quiero incidir en mi punto anterior. ¿Cómo surge todo esto? Con la comunicación inicial entre los ciberdelincuentes y las víctimas. Y esto es gracias al haber tenido previamente acceso a información básica, como el número telefónico para empezar. Por ello el tráfico ilegal de datos personales es actualmente el delito fuente, mediante el cual todas estas otras prácticas fraudulentas pueden prosperar.

Este panorama actual es de relevancia y actualidad nacional, en ese sentido la magnitud e impacto que tiene el delito de tráfico ilegal de datos personales tanto en el sistema financiero como en la sociedad en general es colosal. En ese orden de ideas si bien ya se ha establecido que jurídicamente respecto de lo penal, una entidad financiera por definición no puede ser penalmente responsable de esta clase de delitos, sin embargo, dicha responsabilidad si puede ser atribuida naturalmente a algún integrante, directivo, empleado que este filtrando estas informaciones. Pues es evidente que estos grupos delincuenciales no se basan solo en su tecnología, sino sobre todo en la colaboración de trabajadores, como es presumiblemente en el caso de las entidades financieras y otro tipo de entidades. La imputación fiscal atribuida recientemente a los primeros sujetos capturados de estos escándalos de información lo demuestra claramente. Los delitos de acceso ilícito como se ha visto en la norma correspondiente, implican el acceder a información mediante vulneración de mecanismos de seguridad ya establecidos, mientras que el delito de tráfico ilegal de datos personales como se ha visto no implica necesariamente del uso de recursos informáticos sofisticados y su realización está directamente vinculado a quien le provee dicha información

[32] Véase reportaje en: **https://www.youtube.com/watch?v=8JSErzh4Dks**

desde dentro de la organización afectada. Por lo tanto, en el caso de las entidades financieras, su sistema de seguridad informático, de reconocimiento de identidad y protocolos de prevención deben también ir en sinergia con un adecuado control en la gestión de los datos no públicos que los trabajadores manejan diariamente. El traficante de información verá mermada su accionar delictivo si les quitamos a sus proveedores de información. Es importante asumir que dichos proveedores se encuentran dentro y el sistema financiero debe buscar la manera integral de forjar políticas y protocolos de gestión de datos de manera mucho más controlada y supervisada para con sus integrantes.

3.2. La responsabilidad de las entidades financieras ante los delitos informáticos

En principio, las entidades financieras tienen un rol definido en el mercado como intermediarios y estos son regulados por la SBS, la cual, mediante la Constitución como norma fundamental, la faculta a tener una serie de atribuciones sobre la entidad financiera que aprueba y supervisa, siendo que sus objetivos, funciones y atribuciones están establecidos en la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca, Seguros y AFP, Ley N° 26702. En ese orden de ideas, todas las responsabilidades de las entidades financieras deben entrar en conjunción con los mandatos SBS, los cuales son la estabilidad financiera, la integridad financiera, la adecuada conducta de mercado, y el adecuado desempeño del SPP.

Ahora bien, respecto del tema de la seguridad de la información en materia de prevención de delitos informáticos, la SBS emite una serie de reglamentos y recomendaciones. Que toda entidad financiera debe seguir, puesto que si bien, dentro de la ecuación del delito, su rol principal sería el de sujeto pasivo (como uno de los agraviado), su situación puede cambiar en caso este no haya hecho todo lo posible para salvaguardar la información del otro sujeto pasivo (su cliente), pudiendo ser incluso considerado el sujeto activo (en un grado menor de responsabilidad) pero con una responsabilidad, a fin de cuentas. Sobre este punto existen distintas posturas, por ejemplo para algunos autores, la falta de cuidado en su información financiera y su seguridad por parte del propio cliente lo haría único responsable o el mayor responsable de contribuir a la comisión del acto ilícito en su propio perjuicio, tal como la menciona la investigadora Carmen Leyva Serrano quien a su criterio destaca el hecho de existen autores que pretenden encontrar en el

comportamiento de la víctima, una categoría de carácter formativo que actué como un principio a tenerse en cuenta dentro de la sistemática del delito, el cual se entendería como autorresponsabilidad.(Leyva, 2021)

En esa misma línea, el autor Juan José Blossiers, agrega que, en la autorresponsabilidad, implica que la víctima ha de tomar todas las precauciones que sean necesarias para evitar que sea su comportamiento la causa del delito. En otras palabras, quien no toma las precauciones correspondientes a su responsabilidad respecto de sus bienes jurídicos carecerá de protección frente a estos. Por lo que la negligencia de uno de los sujetos pasivos (el cliente) en principio exime de total responsabilidad a una entidad financiera. (Blossiers, 2000) Otra opinión la tenemos por parte de la autora Michel Martínez quien considera que las entidades bancarias al igual que los usuarios se ven perjudicados en la comisión de estos delitos, puesto que gran parte de ellos es cometido por terceros sin vínculo a la entidad financiera. Sin embargo, reconoce también que las entidades financieras se encuentran en el deber de brindar a sus clientes la máxima protección en base al uso de tecnología adecuada para el ingreso a sus plataformas vía online. (Martínez, 2015)

Es decir, para la autora, las entidades financieras son sujetos pasivos sin embargo haciendo el matiz que estos tienen cierta responsabilidad con su cliente. Si bien no habla de obligatoriedad, si está presente el concepto de deber.

Por otro lado, para Rodríguez, las entidades financieras están obligadas a dar seguridad en las transiciones electrónicas con mayor grado de certeza y eficacia, indudablemente excluyéndose esa responsabilidad subjetiva cuando se verifique la negligencia del cliente. (Rodríguez, 2014)

Finalmente, para Salas, respecto de la responsabilidad de una entidad financiera, la finalidad será siempre el reparar el daño causado por el delito informático que permanecía fuera de la esfera de responsabilidad civil subjetiva. Por ello se debe buscar la ampliación de protección legal para todas las situaciones en las que se genere afectación y requiera reparación. (Salas, 2017).

3.3. Postura del autor

De las distintas opiniones de los autores, respecto de la responsabilidad que debe tener una entidad financiera ante la comisión de un delito informático que afecte principalmente a sus

clientes, puedo destacar el hecho que primeramente no hay criterios unánimes, pero que dentro de dichos razonamientos hay como denominador común, y es que se hace énfasis en la necesidad de contar con una norma de amplia aplicación, de un rango protección alto, por lo cual considero dicha característica de amplitud, es algo que actualmente adolece nuestra normativa peruana sobre delitos informáticos es limitada y necesita mayor trabajo y contenido. Pues jurídicamente hablando no hay norma que obligue o vincule un deber de prevención de la comisión de delitos informáticos en el sistema financiero. Puesto que las normas sobre delitos informáticos que tenemos en la Ley Penal, ningún momento nos establecen claramente el rol que debe asumir una entidad financiera ante un caso de delito informático.

Por ello coincido en especial con la última opinión citada, del autor Salas, en el sentido de que es necesario que las normas peruanas referentes a delito informático deben ampliar su espectro de aplicación para ser más eficientes y proteger jurídicamente de manera más idónea a los sujetos pasivos en este delito. Por ello el carácter preventivo debe ser prioritario, por ser la forma más eficiente de combatir estos actos ilícitos. Adicionalmente a ello se sobreentiende que de tratarse del supuesto en donde se comprueba que la afectación y vulneración al sistema de seguridad de una entidad bancaria se dio debido a la negligencia del cliente, la entidad financiera queda por supueste libre de cualquier responsabilidad, siempre y cuando esta haya garantizado haber provisto del mecanismo de seguridad adecuados y de conocimiento del cliente.

Sumado a ello, actualmente en el país, como se ha mencionado en repetidas ocasiones no se cuenta con una ley o disposición que obligue a las entidades financieras a otorgar información relevante a solicitud del Ministerio público en materia de delitos informáticos. Teniendo en cuenta que no hay suficientes expertos en la materia, su desconocimiento calificado a nivel financiero o tecnológico, hace que no necesariamente soliciten la información más relevante en un determinado caso, lo cual se traduce en demora en la judicialización de un caso, al basar parte de la investigación en elementos de prueba y documentales no necesariamente relevantes, útiles, conducentes, pertinentes. O que incluso, documentales de relevancia, utilidad, conducencia, pertinencia, no necesariamente lo sean para el juez que lleve a cargo los casos al haber desconocimiento, o falta de especialización en dicha materia. Por lo tanto, teniendo en cuenta que nuestra misma fiscalía, policía y poder judicial tiene sus propias dificultades para procesar estos casos, considero que lo ideal sería que los esfuerzos se direcciones más en el apartado de la prevención. En ese orden de

ideas, las entidades financieras deberían tener la obligación de prevenir de manera más eficaz, la comisión de estos delitos dentro de sus sistemas informáticos, y no esperar a llegar a una vía conciliatoria, o incluso ser sancionada con multas por la entidad reguladora del Indecopi. O peor aún, por la lenta y tediosa vía judicial.

Por ello el problema radica en que la ley especial de delitos informáticos, la ley Nº 30096, por sí sola no nos da todas las respuestas, en el ámbito financiero. Pues no encontramos ningún apartado que nos hable de los supuestos, en el ámbito financiero, o que tipo de responsabilidad les correspondería. Ya que como se mencionó anteriormente, la ley penal suele describir más el accionar del sujeto activo del delito. Lo mismo sucede con el artículo 154 -A del Código penal referente al tráfico ilegal de datos personales. Sin embargo, como sabemos las entidades financieras en los delitos informáticos, representan a unos de los sujetos pasivos, siendo el otro su cliente, pero esto no los vuelve simplemente en victimas por definición, pues a diferencia del cliente, considero que una entidad financiera tiene el deber de garantizar cierto grado de seguridad respecto del patrimonio de sus clientes. Y pueden ser considerados responsables hasta cierto punto.

Si bien no se le puede atribuir directamente responsabilidad penal a una entidad financiera, ya que en el supuesto de que un integrante de la persona jurídica, en este caso una entidad financiera, este integrante estaría actuando por su cuenta, estaría cometiendo una conducta de manera individual. Es por ello que por ejemplo el maestro en derecho penal Jakobs siempre que ha tenido oportunidad se ha expresado en estar totalmente en contra de establecer responsabilidad de naturaleza penal a una persona jurídica, y cualquier empresa en general. En virtud que la persona que comete una conducta penalmente relevante lo hace en su calidad de persona individual. O por el contrario podría hacerlo en "representación" de una persona jurídica, pero esto necesariamente implicaría que dicho acto este "acorde" a la naturaleza y actividad de dicha persona jurídica. Ninguna persona jurídica es establecida para tener una naturaleza de ilegalidad, salvo que esta misma se haya concebido como tal.

En ese orden de ideas tenemos lo dicho por el autor alemán Lampen, quien, según su planteamiento, la culpabilidad de la empresa se sustentaría en haber creado, favorecido o mantenido una filosofía corporativa criminógena o ciertas deficiencias organizativas, Sin embargo, la manera en que se estructura esta culpabilidad de la empresa dependerá evidentemente del contenido del injusto en tanto culpabilidad realizada. En ese sentido el autor es muy claro al señalar

que la responsabilidad de una empresa no puede apoyarse en el injusto de acción ajeno, sino más bien en el injusto del sistema propio. (Lampe, 2003). Esto quiere decir que un acto individual de un empleado o directivo, que vaya en contra de las propias directrices de una entidad económica como las entidades financieras no es concebible, dentro de la teoría del derecho penal moderno, que dicha conducta individual sea reprochable penalmente para dicha entidad. Salvo por supuesto si se hablase de organizaciones netamente criminales y claro está que una entidad financiera goza de una naturaleza dentro de la legalidad. Puesto que su actividad financiera y cumple un rol socioeconómico importante en la sociedad como intermediador financiero, y con reconocimiento constitucional; entendiéndose por supuesto de entidades financieras reguladas por la SBS.

Por lo tanto, si bien la imputación penal aparentemente no posible de atribuir directamente a una entidad financiera, no por ello esta va a quedarse de brazos ante la comisión de delitos relevantes para su ámbito (suplantación de identidad, fraude informático, tráfico de datos), más aún en los supuestos parte de la consolidación de delito pueda darse por participación y contribución de algún integrante o trabajador.

Es decir, la entidad financiera debe garantizar siempre la debida diligencia para salvaguardar la seguridad de sus sistemas que pueda evitar un perjuicio económico a sus clientes respecto de los delitos informáticos relevantes a su actividad. Ya que las consecuencias de ellas son jurídicamente reprochables, aun cuando se ha evidenciado que no están totalmente desarrolladas normativamente hablando. Es necesario pues el cumplimiento de una norma de manera obligatoria, y que vaya por supuesto más allá de los compromisos ya asumidos con la SBS, como entidad supervisada. Ya que como sabemos la SBS no tiene un carácter coercitivo ni de naturaleza obligatoria en materia de seguridad.

Esta obligación de combatir y prevenir los delitos informáticos relevantes en pro de los intereses patrimoniales de sus clientes está más que justificado. Considero pues que una formula a seguir seria en base a una norma sancionatoria para las entidades financieras, que engloba una serie de delitos graves que es combatida por una sociedad desde distintos frentes; tal como sucede con el lavado de activos, financiamiento de terrorismo, corrupción, entre otros. El camino a seguir seria por lo tanto incluir en dicho compilado de delitos graves a los delitos informáticos relevantes a nivel financiero, como indudablemente lo son: La suplantación de identidad, el Fraude informático y el Tráfico ilegal de datos personales.

3.5.: La incorporación de los delitos informáticos relevantes en el reglamento de la Ley 30424

Como es sabido, dentro de la ley administrativa, el reglamento de la Ley 30424[33] que regula la responsabilidad administrativa de las personas jurídicas, incluye una relación de serios delitos, lo cuales son: los delitos de delitos de cohecho, lavado y financiamiento del terrorismo, colusión y tráfico de influencias. Siendo que toda persona jurídica, entre ellos las entidades financieras, deben adoptar e implementar en su organización, con anterioridad a la comisión de los delitos que regula, un modelo de prevención adecuado a su naturaleza, riesgos, necesidades y características. Dicho reglamento debe contar con elementos fundamentales mínimos que todo modelo de prevención debe seguir, independientemente de otros modelos, estándares, instrumentos internacionales que la persona jurídica adopte. Es evidente que el espíritu de esta norma en principio es que la implementación "voluntaria y anticipada" de este modelo se da bajo el principio de autorregulación de las empresas, siendo tal como se mencionó, reforzar el rol de prevención, detección, mitigación y reducción significativa de los riesgos de comisión de delitos, así como también la promoción de la integridad y la transparencia en la gestión de las personas jurídicas. En ese sentido incluir dentro de ese compilado a los delitos de Suplantación de Identidad, Fraude informático sería lo más óptimo.

3.6.: El tráfico ilegal de datos personales en la ley administrativa

Respecto de este delito, Art 155 -A del Código Penal, considero que este delito también debe ser también incluido en el reglamente de la Ley 30424, una formula seria que este delito vuelva a ser incorporado en dentro de la ley de delitos informáticos, lo cual normativamente sería más armónico, o en su defecto, que sea agregada como delito independiente. Más allá de la fórmula legal que se llegue a aplicar, la incorporación de esta figura penal es más que necesaria debido a la naturaleza de este delito, su potencial impacto no solo a nivel financiero sino a nivel social en la seguridad de las personas en general. Sobretodo teniéndose en cuenta que el Estado Peruano no ha podido todavía ejecutar acciones concretas respecto de esta problemática que goza en la actualidad casi de total impunidad.

[33] Aprobado mediante Decreto Supremo N° 003-2019-EF

3.7. Formando un marco normativo más sólido

Pues como parte de la solución, propongo como se ha desarrollado a lo largo de esta investigación que a la fórmula de los delitos contemplados a prevenir en la Ley 30424 se agreguen a los delitos informáticos relevantes para el ámbito financiero, los cuales son la suplantación de identidad, fraude informático; así como al delito de tráfico ilegal de datos personales. Dejando por supuesto la puerta abierta para posibles futuras incorporación porque tal como se evidencia, los delitos informáticos están en constante evolución, más aquellos que apuntan siempre al sistema financiero.

Por otro lado, como se ha visto, la ley penal no nos habla nada respecto del rol que la entidad financiera en estos delitos, y no tiene porque, puesto que las entidades financieras son sujetos pasivos, victimas ante estos casos. Sin embargo, es importante que se establezcan sus responsabilidades respecto de su deber como garantes, para con sus clientes. Por ello considero la norma administrativa como la más idónea jurídicamente hablando, tal como lo estableció en su momento la legislación chilena. Pues la responsabilidad administrativa daría sin duda mejore resultados ante la ausencia de una idónea prevención de estos delitos en el ámbito financiero, y los delitos informáticos a día de hoy cuentan con abundante reincidencia, tal como se podido constatar en la evidencia empírica.

Por ello en virtud a lo antes mencionado considero como indispensable que se agregue a dicha normativa a los delitos informáticos relevantes financieramente hablando: Suplantación de identidad, Fraude informático y tráfico ilegal de datos personales dentro del compilado de delitos a combatir y buscar prevenir como persona jurídica, esto por supuesto significara mayor estabilidad, uniformidad de criterios y en un conjunto una protección más integral respecto de la seguridad y en especial de los datos personales, que como se ha visto en la evidencia empírica, el tráfico ilegal de datos personales tiene una incidencia e impacto muy grande, no solo a las entidades financieras, sino también públicas y de actividades diferentes.

Quiero incidir en este punto. La entidad financiera si bien no puede ser directamente sindicado como responsable por la comisión de estos delitos informáticos en su contra, si tiene el deber de prevenirlos y sobretodo gestionar los riesgos que implica el manejo de información sensible y no pública; en especial con la realidad actual que vive el Perú, de constantes filtraciones de

información no pública. Y la mejor manera será mediante la incorporación de estas figuras ilícitas en dicha norma, puesto que tal como lo menciona la misma en su reglamento la adopción de todo modelo de prevención de delitos se constituyen en herramientas de gestión en materia de integridad corporativa, lo que implica la implementación de un sistema ordenado de normas, mecanismos y procedimientos de vigilancia y control, destinados a neutralizar o reducir significativamente los riesgos de comisión de delitos y a promover la integridad y transparencia en la gestión de las personas jurídicas; los que son adoptados e implementados de modo voluntario, bajo el principio de autorregulación de las personas jurídicas. Adicionalmente considero que también podrían agregarse y desarrollarse dichos conceptos en algún apartado de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros LEY Nº 26702.

3.8.: El doble factor de reconocimiento en el control de identidad

Otro punto que considero importante, en concordancia con esta eventual modificación de nuestra ley 30424, sería que se estandarice los criterios y mecanismos de control de identidad, pues este es el factor clave, la primera y más importante barrera de protección en los delitos de suplantación de identidad, sin embargo, no debe ser la única. Respecto de este apartado el control de identidad que una entidad financiera está obligada a tomar para evitar casos de suplantación de identidad tanto en las modalidades presenciales o digitales. Es decir, ante una gestión en oficinas de manera presencial, se sobre entiende que las entidades financieras cuenten con mecanismos para una correcta identificación de la persona que se acredite ante ellos, uno de los mecanismos más utilizados es el lector biométrico de huella digital. De otro lado entre los mecanismos de seguridad a nivel digital, informático se cuentan tantos las Aplicaciones oficiales de cada entidad financiera como claves digitales, mensajes de texto, tokens digitales, códigos de confirmación, etc. Muchas de estas modalidades son super útiles, pero pueden ser vulneradas si por ejemplo el teléfono móvil del titular fuese robado y un tercero tuviese acceso a todo ello. Por lo que un mecanismo adicional de seguridad podría ser un sistema de reconocimiento facial.

En ese orden de ideas el contar con una segunda barrera de protección complementaria a la primera, tal como lo podemos ver por ejemplo en nuestras cuentas de correo electrónico al

momento de activarse en direcciones IP diferentes a la usual, el doble factor de reconocimiento asegura la mayor protección en tiempo real. Así como otras formas de identificación tales como videollamada grabada con el usuario, mostrar una fotografía en tiempo real, ubicación en tiempo real, lo cual permitiría una correcta validación del titular. Hoy en día la tecnología ofrece muchas herramientas en este apartado, así como empresas especializadas en este rubro.

3.9.: La gestión responsable de los datos personales.

Sobre este punto quiero incidir específicamente en el delito de Tráfico ilegal de datos personales (Art. 155-A del Código Penal), que como se ha podido comprobar no solo en la evidencia empírica sino sobre todo en la realidad actual que viven todos los peruanos en el País. El problema del tráfico de información personal se debe no solamente a que existe una vigente demanda de tal información, si no a que la raíz del problema nace de las propias instituciones, tanto públicas como privadas. Siendo que los traficantes de información pueden hacer sus actos delincuenciales gracias a la colaboración de personas dentro de las entidades afectadas, por lo tanto, determinados integrantes, trabajadores quienes filtran y venden esta información sensible de los clientes y que en principio es de naturaleza no pública. No es necesario tener pruebas fehacientes para afirmar categóricamente que existen trabajadores dentro de todas las instituciones tanto públicas y privadas que están siendo cómplices del delito de tráfico ilegal de datos personales. Es por ello que el sistema financiero debe ser más hermético y enfatizar con más energía sus políticas de la correcta gestión de datos responsables, pues los traficantes de información pueden traficar con la información que determinados "proveedores" les otorgan en diferentes tipos de instituciones tales como RENIEC, MIGRACIONES y los sistemas financieros por supuesto. En ese sentido la vinculación normativa respecto de una adecuada gestión de los datos personales esta más que justificada, pues es importante que dichas políticas estén plasmadas y claras, no solo para la entidad financiera en sí, sino sobretodo para sus trabajadores. Ya que son ellos quienes manejan dichos datos todos los días.

3.10.: La prevención como el mejor incentivo

En principio muchas entidades financieras podrían considerar que invertir en mayor ciberseguridad, con los más altos estándares de eficacia implicaría una inversión considerable que quizás podría hasta cierto encarecer el costo de sus actividades, sin embargo, he decir que es todo lo contrario.

Considero que el hecho de una entidad financiera invierta en una mejor seguridad en sus sistemas informáticos, prácticamente está "ahorrando" dinero. Esto en el sentido de que en vista que los casos de delitos informáticos específicos (Suplantación de identidad, fraude informático, tráfico ilegal de datos personales, entre otros a futuro) continúan en auge, tal como se ha evidenciado en las denuncias reportadas hasta ahora.

Pues debido a que contexto actual de nuestro lo favorece, los potenciales litigios estarán siempre a la vuelta de la esquina, y todo ello implica costos adicionales no previstos, el recurrir a una consultaría de abogados, independientemente del área legal que se tenga, tanto para presentación de documentación, que los operadores de justicia requieran, la realización de declaraciones rigurosas, con sustento técnico, financiero, especifico. Ser parte de un expediente judicial, ya sea que la entidad sea parte del proceso como parte agraviada, o testigo, o hasta incluso tercero civilmente responsable, etc. Todos estos escenarios posibles evidentemente se van a contabilizar como costos.

Además, como es sabido el hecho de estar dentro de una investigación fiscal, si bien no necesariamente significa una mala señal, mientras no haya sentencia, si podría afectar en cierto modo el aspecto reputacional de una entidad financiera. Sumado al hecho de que nuestros de justicia es lento por gran carga procesal, no veo como algo favorable para una entidad financiera estar dentro de una investigación fiscal o caso judicializado por un tiempo por general excesivamente prolongado.

En ese sentido el adoptar las medidas y establecer los modelos de prevención más idóneos para garantizar la seguridad en base a una normativa vinculante será un gran incentivo para estar más protegidos, puesto que la evidencia empírica a día de hoy nos demuestra cuán expuesta esta las informaciones de los peruanos debido al tráfico ilegal de datos personales y la constante evolución de los mecanismos fraudulentos. Como puede apreciarse en el siguiente cuadro en estos años:

Relación de denuncias sobre delitos informáticos (2013-2020) a nivel procesal[34]

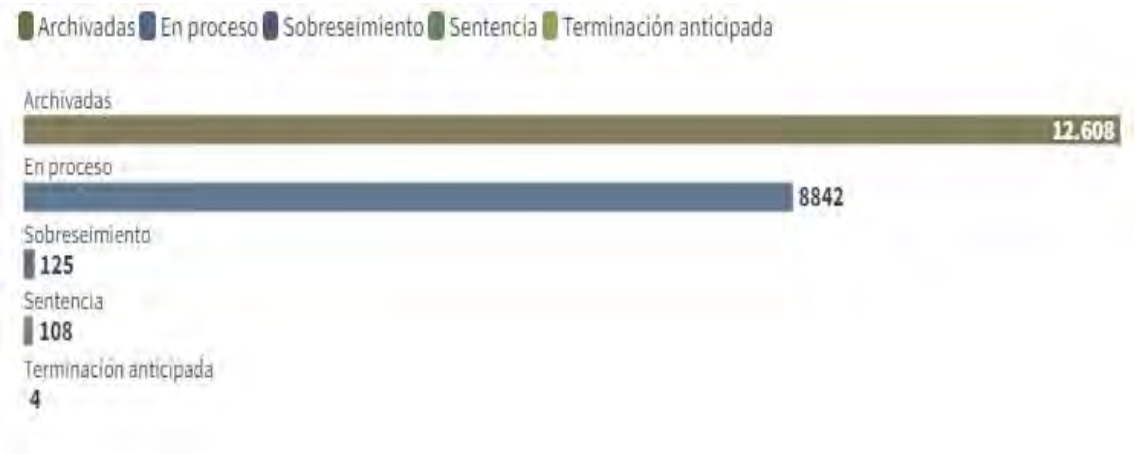

Figura 4: Denuncias de delitos informáticos 2013-2020, según estado procesal (Tercer Gráfico) (Morales Isla / Unidad LR Data, 2022)

Como puede apreciarse, los casos denunciados son de un índice alto, y si bien muchos casos son archivados, esto es por lo general ante la imposibilidad del Ministerio público y la DIVINDAT, de encontrar a los responsables, pues no se cuenta con suficiente personal especializado, por lo que muchas veces, estos casos en proceso son constante Ampliados, así como los archivados que pueden ser reabiertos en instancias superiores, y ampliados en su fase de investigación, para en muchos casos "ganar tiempo" a la fiscalía. Pero como es sabido, el Ministerio Publico, Dindat y Sidpol, tienen problemas para procesar con celeridad estos casos por le poco recurso humano especializado en esta materia.

Siendo evidente que llegar a un caso fiscal o judicial seria lo menos recomendable para una entidad financiera, debido a los altos costes no solo a nivel reputacional, sino que como es sabido en nuestro país los procesos fiscales y judiciales adolecen de una notoria lentitud en el todo el

[34] Fuente: Ministerio Público (2020) • Gráfico: LR Data. Véase en: **https://data.larepublica.pe/suplantacion-de-identidad-en-linea-incrementan-denuncias-pero-no-hay-responsables/**

proceso, curso de sus investigaciones y decisiones judiciales. Situación que, por supuesto se agrava debido a lentitud del Estado Peruano no solo en la toma de medidas concretas sino en la aprobación de normativa especializada o armónica sobre esta problemática, como el aprobar reglamentos, modificaciones. Así como la ausencia de especialistas para justamente ver, estudiar, y procesar de manera inequívoca y con el conocimiento pertinente de estos casos que están en constante reincidencia respecto de su comisión y el uso de las tecnologías de la información, en permanente evolución.

Por su parte tenemos a las consecuencias a nivel administrativo por parte del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) que como sabemos sanciona a nivel administrativo como se ve a continuación:

Entidades financieras sancionadas por operaciones no reconocidas (2019-2022)[35]

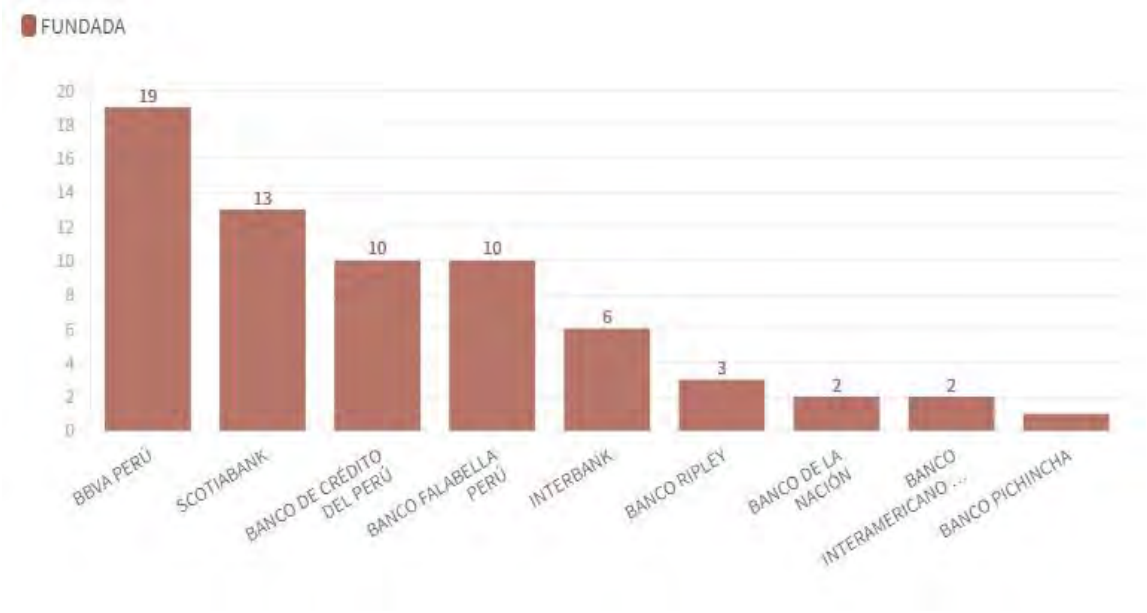

Figura 5: Entidades financieras sancionadas por operaciones no reconocidas 2019-2022 (Cuarto Gráfico) (Morales Isla / Unidad LR Data, 2022)

Como puede apreciarse, independientemente de los casos denunciados y que sean llevados a nivel fiscal, el INDECOPI en base a sus propias investigaciones ejecuta sus sanciones y multas a las distintas entidades financieras. Los casos están presentes, por las abundantes denuncias,

[35] IBID

prácticamente casi todas las entidades financieras más importante del país están incluidas, lo cual implica por supuesto costos tanto a nivel económico como a nivel reputacional dentro del mercado, lo cuales por supuesto no son temas menores. Como es sabido cada año las entidades financieras son noticia y no necesariamente noticias positivas, entre los casos mas recientes en este año 2023 tenemos por ejemplo la intervención de la SBS en reconocidas cajas de ahorro[36] o lo acontecido con un reconocido banco y las fallas con su App oficial[37]

De allí la importancia de buscar evitar incidir en esta clase de situaciones que implican sanción y llamada de atención sobretodo por parte de las entidades reguladoras, en especial ante denuncias hechas por los usuarios. Muchas veces, la notoriedad y viralización de determinas situaciones o denuncias hechas por redes sociales pueden tener un impacto más que significativo en la reputación de una entidad financiera. Ya que, en la actual, la imagen de una institución dentro del mercado es sumamente relevante

[36] SILVA, C (2023, 12 de agosto) *SBS interviene Caja Raíz: ¿Qué factores se han dado y qué ocurrirá con sus ahorristas?* Economía/Noticias. El Comercio: Véase en: **https://elcomercio.pe/economia/sbs-interviene-caja-raiz-que-factores-se-han-dado-y-que-ocurrira-con-sus-ahorristas-y-deudores-superintendencia-de-banca-seguros-y-afp-sistema-financiero-cooperativas-de-ahorro-y-credito-mypes-noticia/**

[37] ANCAJIMA, L (2023, 17 de Setiembre). *Interbank responde ante fallas en su aplicación: el saldo de muchos usuarios apareció en cero*. Radio Programas del Perú (RPP). Véase en: **https://rpp.pe/peru/actualidad/interbank-responde-ante-fallas-en-su-aplicacion-el-saldo-de-muchos-usuarios-aparecio-en-cero-noticia-1505939**

CONCLUSIONES:

1) Los delitos informáticos han tenido un crecimiento exponencial en estos últimos años. En especial los relevantes en materia financiera los cuales son Fraude Informático, Suplantación de Identidad y Tráfico Ilegal de datos personales. Este crecimiento se ha dado en un contexto en que el Perú y el mundo se vio azota por la Pandemia, lo cual implicó un cambio en la manera de trabajar y llevarse a cabo diversas actividades; pero adoptando la modernización y uso de la tecnología de manera masiva y abrupta, en comparación con otros países. Ya que, por muchos años, el Perú ha sido más dependiente del papel que del uso de la tecnología, situación que ya ha cambiado en la actualidad. Estos cambios abruptos por motivos de fuerza mayor. No le dieron al Estado peruano el tiempo suficiente como para adecuar sus políticas y leyes respecto del uso de las tecnologías, su regulación e impacto cuando se cometan actividad de naturaleza ilícita mediante el uso de estas tecnologías en distintas áreas, tales como la financiera.

2) Como ha podido apreciarse a lo largo de esta investigación, el auge de los delitos informáticos relevantes en materia financiera, se han visto beneficiados gracias a determinaras carencias que adolece nuestro País. Dentro de estas carencias tenemos en primer lugar las correspondientes a nivel de recurso humano. Es decir, todo personal calificado necesario para afrontar esta clase de delitos a nivel judicial, pericial, y fiscal. Como es bien sabido, nuestro sistema de justicia ya de por si cuenta con recursos muy limitados, es decir, cerca de 8000 fiscales y 3500 jueces aproximadamente a nivel nacional, según datos oficiales del año 2022. Esto para un universo de cerca de casi 34 millones de habitantes aproximadamente en el país, según datos en 2021, es bajísimo. Y a ello ahondamos que no se cuenta con suficientes fiscales especializados en los delitos financieros, lo mismo a nivel judicial, no se cuenta con juzgados ni salas especializadas para esta clase de delitos. En donde si se ha advertido una mayor presencia de recursos humanos calificados es en la policía nacional, con su visión DIVINDAT, División de Investigación de Delitos de Alta Tecnología. Estas unidades sumadas a las fiscales se han incrementado

progresivamente a partir del año 2021. Esto faltaría ser replicado a nivel judicial. Si bien son avances significativos, aún queda mucho por avanzar en materia de personal calificado. Por ello se ha apreciado en los casos de delitos informáticos con repercusión en el ámbito financiero reportados y la situación actual de su procesamiento a nivel de investigación policial, fiscal y judicial la primera carencia respecto de personal calificado insuficiente ha quedado demostrado.

3) Como segunda carencia advertida, la referente a la carencia de recursos jurídicos idóneos para afrontar los delitos informáticos relevantes en materia financiera se ha advertido que las normas actuales son insuficientes. Tanto la Ley de Delitos Informáticos. Ley 30096 la cual contiene al Delito de Fraude Informático (Art 8) y el Delito de Suplantación de Identidad (Art 9), no nos habla nada respecto del rol de la entidad financiera en estos casos, tampoco regula ni contempla como circunstancia agravante cuando uno de los sujetos activos es un integrante de una entidad financiera. Lo mismo sucede con el Delito de tráfico ilegal de datos personas (Art 154-A Código Penal), el cual inicialmente estaba incluido dentro de la Ley 30096, pero que Decreto Supremo Nº 003-2013-JUS. Fue reubicado en la ley penal. Este cambio a la luz de los hechos, tampoco ha significado grandes cambios o mejoras respecto de la lucha contra los delitos informáticos en materia financiera. Y eso es dado la naturaleza especial que tienen estos delitos dentro del ámbito financiero. Pues como se ha visto en esta investigación, a diferencia de la gran mayoría de delitos en donde contamos con 2 participantes, 1 sujeto activo (el que comete el delito, y un sujeto pasivo (el agraviado del derecho vulnerado); en cambio en los delitos informáticos relevantes a nivel financiero contamos con 3 participantes: dos sujetos pasivos (la entidad bancaria y su cliente), y como sujeto activo (el ciberdelincuente). Así que en principio la norma penal no nos hablara nada respecto de la entidad financiera, pues su enfoque va más ligado a la conducta del sujeto activo, sin siquiera contemplar la posibilidad de considerar a este segundo sujeto pasivo como agraviado, testigo, de oficio; más aún en los eventuales casos en que un trabajador participara en la contribución del accionar delictivo, como en los casos de tráfico ilegal de datos personales por ejemplo, en donde el traficante de información puede desarrollar su actividad ilícita gracias a su proveedor. Este análisis desde la misma teoría del delito hecho en esta investigación nos demuestra que desde el plano conceptual los recursos jurídicos que disponemos, las normas penales pertinentes a delitos informáticos en materia financiera son insuficientes y poco claros.

4) Como tercera carencia que se ha advertido en esta investigación es el hecho de que nuestra normativa a nivel de prevención, gestión de datos adecuada de datos y ciberseguridad en la actualidad no es del todo vinculante en el sentido de que no tiene un carácter de obligación de cumplimiento. Esta carencia de obligación de implementación y dejarlo todo a suerte de la autorregulación de las entidades financieras respecto de la ciberseguridad, políticas de prevención de los delitos informáticos y adecuada gestión de datos no es lo más recomendable. Ya que dada la complejidad del panorama que se vive hoy en día en el País, por las otras carencias antes descritas, sumado a la presencia de otras figuras delictivas como el robo, así como la informalidad, la inseguridad, entre otros aspectos que las entidades financieras deben lidiar diariamente; nos hace inferir que el camino más adecuado es el de contar con una política preventiva. Ya que nuestro propio estado peruano ha descuidado la figura de la prevención en distintos apartados. Por ello las entidades financieras deben adoptar la prevención, sumado a la adecuada gestión de datos y la ciberseguridad como elementos fundamentales en su agenda para su adecuada operación de actividades. Esto beneficiara a todos el sistema en general si se aplica de manera armónica, integral y en un mismo sentido. Por ello la necesidad de contar con una normativa vinculante que impulse a las entidades financieras a adoptar todo lo antes mencionados. En la actualidad normas de ese tipo son carentes tal como lo demuestra la evidencia empírica y el análisis de nuestros dispositivos legales actuales de allí que se proponga Ley N° 30424 y sus modificaciones es una alternativa válida, tal como en su momento lo ha implementado la legislación chilena.

5) Como se ha podido apreciar, los delitos vistos que tienen una incidencia directa en el mundo financiero, son 3. Por un lado, tenemos a los delitos informáticos propiamente dichos en su ley especial, como lo es la Suplantación de Identidad en su Artículo Nº9, tiene una especial relevancia debido a las abundantes denuncias de usuarios que advirtieron ser titulares de préstamos que jamás solicitaron, en ese sentido considero que la afectación no solamente es la fe pública sino, que el caso del ámbito financiero también se aprecia una afectación de naturaleza económica. Por su parte el delito de Fraude Informático, contenido en el artículo Nº8, también tiene un amplio número de denuncias, las cuales se han visto sobretodo incrementadas en el contexto de la pandemia que se vivió en estos años recientes. Este delito guarda similitudes y conexiones con el delito anterior,

siendo su diferencia que la primera necesita de más recursos y conocimientos informáticos para su ejecución. Mientras que la suplantación de identidad puede darse también de manera circunstancias o por resultado de otros delitos previos, tales como el tráfico de datos personales y el robo de celulares. Y respecto del delito de tráfico ilegal de datos personales, su relevancia a quedado más que demostrado, por la evidencia obtenida a base de las recientes y presentes investigaciones, capturas, y demás diligencias fiscales, policiales dado su potencial impacto no solo a nivel financiero sino en general, en la seguridad de las personas y sus datos. Y este delito tiene mucho más impacto que el delito de acceso ilícito en el sentido que este delito implica mayores conocimientos y vulnerar sistemas de seguridad ya existentes para la obtención de datos en un sistema, sin embargo, como se ha podido apreciar en la evidencia tanto empírica como sobretodo periodística y documental, el tráfico ilegal de datos se apoya en los proveedores de información no publica de las personas. Debido al aspecto cultural y la histórica normalización de la compra de información en distintos ámbitos del país, sumado a las dificultades de las instituciones, sobretodo las públicas, para gestionar adecuadamente sus datos. Por ello mientras no se trabaje y se fiscalice adecuadamente sobre quienes proveen la información a los traficantes, este delito continuara en auge. Ya que soy de la opinión de que el tráfico ilegal de datos personales es el delito fuente, no solo de los otros dos delitos antes mencionados, sino incluso de otra clase de delitos tales como secuestro, sicariato, extorsión, etc. Inicialmente los focos se dirigían más al Fraude Informático y Suplantación de Identidad por su mayor número de denuncias reportadas; sin embargo, esta investigación ha demostrado que el Delito de tráfico ilegal de datos es igual o incluso más urgente a tratar, tal como se ha apreciado en los casos denunciados más actuales.

6)La evidencia empírica que reportan nuestros operadores de justicia tanto a nivel de denuncias de entidades publica, privadas y de la población en general, las investigaciones tanto a nivel policial, fiscal y periodístico, así como sanciones de entes reguladores como el Indecopi, y directivas dictadas por PCM, entre otros; nos demuestra que la lucha contra los delitos informáticos en materia financiera aún adolece de resultados satisfactorios y es necesario mejorar la normativa vigente en esta materia. Independientemente del desarrollo normativo de esta materia en nuestra ley penal, la ciberseguridad y una adecuada gestión de datos, han sido temas que el Estado Peruano no ha priorizado hasta tiempos recientes por el impacto de la pandemia, a diferencia de otros países que ya venían trabajando en estos delitos, como es el caso chileno, el cual en su momento articulo e integró sus distintas normas, sumado a normativa nuevas, todas orientas hacia el mismo objetivo,

prevenir y combatir los delitos dentro de las personas jurídicas, lo cual evidentemente alcanzó a su sistema financiero. Siendo claro su más reciente modificatoria, en donde entre otras cosas, incorporó a los delitos informáticos dentro de su ley de responsabilidad administrativa de personas jurídicas, como uno de los delitos a combatir preventiva y obligatoriamente. Siendo ello el camino que debe replicar nuestra legislación. Que básicamente implicara el incluir en la lista de delitos contemplado por el reglamento de la Ley Nº 30424 a los delitos de Fraude informático, suplantación de identidad, Tráfico ilegal de datos personales; por ser las más relevantes a nivel financiero e incluso a nivel general. Teniendo a su vez la perspectiva de que dicha lista podría ampliarse, sobretodo por el hecho que los delitos informáticos y sus modalidades puedan variar, tanto empíricamente como jurídicamente, como es el caso de la inicial Tráfico Ilegal de datos que inicialmente estaba dentro de los delitos informáticos y paso a ser un delito independiente, más allá de que su contenido descrito en la ley penal es prácticamente el mismo. El ceñirse a lo dispuesto por el reglamento de Ley Nº 30424, permitirá definitivamente que se consoliden modelos de prevención sobre estas prácticas fraudulentas que hoy en día representan un gran problema de relevancia en la agenda nacional. En ese orden de ideas, mi propuesta de apoyarnos en la normativa administrativa sancionatoria para garantizar la prevención de los delitos informáticos en las personas jurídicas, influenciara positivamente en materia financiera para una mejor adecuación con políticas de prevención, ciberseguridad y adecuada gestión de datos no públicos.

7)Respecto de la responsabilidad que tienen las entidades financieras ante la comisión de delitos informativos, relevantes para su ámbito de actividad, podemos concluir que existe, en el sentido de que tanto las responsabilidades y deberes de prevención que debe tener la entidad financiera tienen que ser contempladas por nuestro ordenamiento legal, ya que por más que sea uno de los sujetos pasivos en este delito, considero que tiene el deber garantizar la seguridad del patrimonio de su cliente de la manera más óptima posible, y ello va de la mano con un adecuado sistema informático, de reconocimiento de identidad y protocolos de supervisión y fiscalización respecto del uso adecuado y correcto de la información personal de los clientes. En ese orden de ideas, en base a lo que nos dice el derecho penal moderno, sería muy difícil de sostener responsabilidad penal directa sobre una entidad financiera, toda vez que la naturaleza de esta, como persona jurídica, es financiera, lo cual tiene un rol socio económico relevante, dentro de la legalidad y amparado a nivel constitucional como intermediario financiero. Que un integrante de una entidad financiera, independientemente de su rango, director, supervisor, accionista, empleado, cometiera

un acto directamente delictivo orientado a los delitos informáticos, este acto serio considerado de naturaleza individual y por lo tanto respondería como tal. Ya que ese acto perpetraría en contra de las directrices internas y naturales que tiene una entidad financiera conforme a ley, salvo que dichas directrices de la entidad financiera fueran originalmente orientadas a la criminalidad. Lo cual evidentemente en ese supuesto iría en contra de la propia naturaleza legal que tiene una entidad financiera, refiriéndome por supuesto de las que están debidamente reguladas. Esta dificultad por no decir imposibilidad de imputación directa no le exígeme a una entidad financiera a asumir otro tipo de responsabilidades, como la administrativa en los casos en que no llego a hacer lo suficiente, dentro de lo razonable, a reducir al mínimo la exposición al riesgo tanto el patrimonio como los datos personales de sus clientes. Por lo que el reproche legal puede sustentarse en ese sentido, de allí la importancia de que la normativa sobre delitos informáticos cuente necesariamente con supuestos agravantes, cuando el sujeto activo en estos delitos sea un propio miembro de la entidad afectada.

8) Que las entidades cuenten de manera obligatoria en base al cumplimiento de una normal de políticas de prevención está más que justificado y esta investigación lo ha demostrado. Esto en virtud de lo visto por la experiencia chilena y en consideración del contexto peruano, el cumplimiento por parte de las entidades financieras de aplicar los adecuados estándares de seguridad, prevención y gestión responsable de los datos, representaran el mejor incentivo. Ya que todo ello reduciría notablemente la afluencia de casos denunciados y, por ende, permitirían a nuestro precario y reducido número de especialistas en sede fiscal y policial a responder de manera más breve los casos ya vistos. Sobretodo porque que toda esta prevención ayudaría a evitar largas esperas por una investigación fiscal o solución al problema de manera judicial, así como a la imposición de reiteradas multas por parte de Indecopi a las entidades financieras, que como somos conscientes no siempre basa sus resoluciones en criterios financieros. Todo ello representando el mejor incentivo, el de evitar litigios y costos innecesarios o que pueden ser minimizados. Para beneficio de las entidades financieras y sobretodo de sus clientes al reducirse sobrecostos futuros en base a la prevención.

9) Entre los estándares en control de identidad que podrían adoptar las entidades financieras muy aparte del lector biométrico, pueden ser el uso de apps oficiales. Viviendo hoy en día en una era digital, podría plantearse de necesidad urgente que toda entidad financiera tenga una aplicación oficial para teléfonos móviles, dada a la realidad actual, las cuales han demostrado los útiles que son para la prevención de las suplantaciones. Otros criterios que deben tomarse para proteger a los clientes son por ejemplo en los casos de la aprobación de emisión de créditos, es no solamente basarse en la identificación física o digital, sino también saber "identificar" los patrones de conducta de los clientes en materia financiera. Por ejemplo, si una persona que tiene una determinada forma de manejar su dinero, cantidades pequeñas, y un día se presenta solicitando una cantidad de dinero considerablemente alta para sus ingresos o el dinero que acostumbra mover diariamente; por más que este "califique" no debería aprobarse inmediatamente sino asegurar que la persona que está allí, ya sea presencial o por teléfono, para garantizar la validación de la identidad del titular. Esto puede hacerse mediante mecanismos adicionales de identificación, como tokens digitales, códigos de seguridad autogenerados en tiempo real con minutos de vigencia, etc. Pues la delincuencia está en constante renovación, en especial teniendo en cuenta que reciente se ha evidenciado la vulnerabilidad y poca fiabilidad que a veces puede tener nuestro propio registro nacional de Identificación y el problema reciente de la filtración de información. La obligatoriedad de la aplicación de este tipo de metodologías y tecnología impulsaría a las demás entidades que no tengan estas herramientas a implementarlas.

10) Respecto de un adecuado control responsable de la gestión de datos personales, elemento clave en la lucha contra el delito de tráfico ilegal de datos personales que cuenta una entidad financiera en su sistema esta necesita una mayor supervisión para detener las filtraciones, una posible solución podría ser por ejemplo emulando lo que supervisa el ministerio público a nivel de la función fiscal. En el ministerio público, en una fiscalía especializada en criminalidad organizada, por ejemplo, los fiscales tienen acceso a un sistema que trabaja con data de RENIEC mediante el cual, pueden visualizar y revisar la ficha RENIEC de dicha persona, antecedentes judiciales, penales de cualquier persona. Sin embargo, toda aquella búsqueda queda registrada en el historial y puede ser revisada por los órganos de control. Si en dichos controles se evidencia que un fiscal busco información de una persona sin ninguna razón objetiva de peso, como que está investigando a esta persona de manera formal, o es una de las partes, denunciante o denunciado de algo caso fiscal enumerado en específico; podría ser amonestado y hasta sancionado en su legajo

personal o administrativamente por revisar información personal de una persona de manera injustificada.

11) Entre otras recomendaciones podríamos contemplar el hecho de que las de que las entidades financieras relancen o en su defecto, inicien alianzas o estrategias comunicaciones para con sus clientes, sugerencias, publicidad respecto de la seguridad, tales como, por ejemplo: “Cambiar el PIN de seguridad del chip, evitara que cualquier persona pueda usar el mismo chip en otro dispositivo”. “Si tu dispositivo celular se queda sin señal de manera inesperada comunícate con tu proveedor de telefonía y con nosotros”. Así como promover con mayor énfasis el uso de apps oficiales, pues muchas veces los fraudes informáticos sobretodo, se dan por caer en páginas web falsas. Mostrar por videos o publicidades cortas per concisas las virtudes de la app tales como, “control de tus movimientos en tiempo real”, “límites a los movimientos diarios”, “tú tienes el control”. Entre otros mensajes y consejos útiles, los cuales están presentes en las políticas de la mayoría de entidades financieras, pero dada la coyuntura actual, en especial con el delito de tráfico de datos, es importante reforzar y darles mayor impulso a dichos consejos y sugerencias a los usuarios en general.

BIBLIOGRAFÍA:

Acuario del Pino, S. Profesor de Derecho Informático de la PUCE. *Delitos informáticos: Generalidades*. 2020 Lima – Perú p.7,9,20 Véase en: **https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf**

Almanza Altamirano, F. y Peña González, O. *Teoría del delito. Manual práctico para su aplicación en la teoría del caso*.: APECC. Lima – Perú. 2014 p.184, 185

ANCAJIMA, L (2023, 17 de Setiembre). *Interbank responde ante fallas en su aplicación: el saldo de muchos usuarios apareció en cero*. Radio Programas del Perú (RPP). Véase en: **https://rpp.pe/peru/actualidad/interbank-responde-ante-fallas-en-su-aplicacion-el-saldo-de-muchos-usuarios-aparecio-en-cero-noticia-1505939**

BCN (Biblioteca Nacional del Congreso de Chile) Ley Chile. *Normas sobre delitos informáticos*: Véase en: **https://www.bcn.cl/leychile/navegar?idNorma=1177743**

Y también en: **https://www.bcn.cl/leychile/navegar?idNorma=1008668**

Blossiers Mazzini, J. y Calderón García, S. *Los Delitos Informáticos en la Banca: El delito del milenio. Informática y Derecho Bancario*. Editora RAO S.R.L. Lima – Perú. 2000. p. 367

Bramont – Arias Torres, L. *El delito Informático en el Código Penal Peruano. Biblioteca de Derecho Contemporáneo*. Volumen 6. Pontificia Universidad Católica del Perú. Fondo Editorial. Lima – Perú. 1997. p. 51

Chang Kcomt, Rommy. Teoría General del Delito Imputación objetiva y subjetiva. Escuela del Ministerio Publico. 2015. Véase en: **https://www.mpfn.gob.pe/escuela/contenido/actividades/docs/3762_1_chang.pdf**

Council of Europe. (Traducción: A. Cristina López). Head of Scope on Electoral Co-operation. Véase en: **https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/E-votingRec_Spanish.asp**

CONAPOC (Consejo Nacional de Política Criminal): *Diagnóstico Situacional Multisectorial sobre Ciberdelincuencia en el Perú.* Presidencia del Consejo de ministros. Lima- Perú 2020.

Primera Edición digital. Véase en: **https://cdn.www.gob.pe/uploads/document/file/1487798/01%20Diagno%CC%81stico%20Situacional%20Multisectorial%20sobre%20la%20Ciberdelincuencia%20en%20el%20Peru%CC%81%20%281%29.pdf.pdf?v=1608385058**

DPL News (2022, 31 de agosto): Perú | *"Siete mil celulares se pierden o se roban al día en el Perú, según datos de Osiptel", advierte exviceministro de Seguridad Pública.* Véase en: **https://dplnews.com/peru-siete-mil-celulares-se-pierden-o-se-roban-al-dia-en-el-peru-segun-datos-de-osiptel-advierte-exviceministro-de-seguridad-publica/**

Gómez Perals, M. "Los Delitos Informáticos en el Derecho Español", Informática y Derecho Nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi. Como se citó en Acuario del Pino, 2020

Guerrero Argote, C. *De Budapest al Perú: Análisis sobre el proceso de implementación del Convenio de Ciberdelincuencia. Impacto en el corto, mediano y largo plazo*. Editorial: Derechos Digitales América Latina, 2018, p.4. Véase en: **https://www.derechosdigitales.org/wp-content/uploads/minuta_hiperderecho.pdf**

Guillermo Bringas, L. Análisis sobre el contenido y temporalidad del dolo como elementos de imputación subjetiva en el Código Penal peruano. Revista Ciencia Tecnología. 15(4): 229 - 237, (2019) Trujillo – Perú

Huerta M., M. y Líbano M., C. Delitos Informáticos, Ed. Cono Sur Ltda., 1996, p. 285.

Hurtado Pozo, J. Manual del Derecho Penal, Parte General I, Editora Jurídica Grijley E.I.R.L. Perú. 3 edición 2005, pp. 709,710

INFOBAE (2022, 15 de noviembre) *Nuevos casos de ransomware o secuestro de datos donde piden rescate con Bitcoin: Los ataques revelados están enfocados en víctimas de habla hispana que usan Windows.* Véase en: **https://www.infobae.com/america/tecno/2022/11/15/nuevos-casos-de-ransomware-o-secuestro-de-datos-donde-piden-rescato-con-bitcoin/**

Infobae- PERU (2022, 24 de mayo) *'Zorrito Run Run': Esta es la plataforma que filtró y ofertó los datos personales de los peruanos.* Véase en:

https://www.infobae.com/america/peru/2022/05/20/zorrito-run-run-la-plataforma-que-filtra-y-oferta-los-datos-personales-de-los-peruanos/

INEI (Instituto Nacional de Estadística e Informática): Informe Técnico Nº1- marzo 2023. *Estadísticas de la criminalidad, Seguridad Ciudadana y violencia.* Una visión de los registros administrativos. Enero-noviembre 2022. Pg. 5. Véase en: **https://m.inei.gob.pe/media/MenuRecursivo/boletines/boletin_estadisticas_criminiladad_ene_nov2022.pdf**

Lara, J. (2019, 16 de noviembre) Privacidad a la venta: datos personales expuestos a la criminalidad*. En el Centro de Lima se venden ilícitamente nombres, teléfono y direcciones de miles de personas. Experto en delitos informáticos señala que en el país hace falta una ley sobre ciberseguridad.* Crónicas. El Comercio. Véase en: **https://elcomercio.pe/lima/seguridad/privacidad-a-la-venta-datos-personales-expuestos-a-la-criminalidad-noticia/?ref=ecr**

Latina Noticias. Reportaje Periodístico emitido el 22 de mayo de 2023. Véase en: **https://www.youtube.com/watch?v=WML4SH46mF4** ; Reportaje Periodístico emitido el 28 de junio de 2023. Véase en: **https://www.youtube.com/watch?v=8JSErzh4Dks**

Leyva Serrano, C. *Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales*. Investigación de la Facultad de Derecho y Ciencia Política de la Universidad Nacional Mayor de San Marcos. Lucerna Iuris Et. Lima 2021. p. 41

Magliona Markovicth, C., López Medel, M. *Delincuencia y Fraude Informático*, Editorial Jurídica de Chile. 1999

Martínez Padilla, M. *La responsabilidad bancaria frente a los delitos informáticos*. Universidad Andina Simón Bolívar. Ecuador. 2015

MINISTERIO PÚBLICO. FISCALIA DE LA NACIÓN: Boletín Estadístico. Lima Perú. 2021

Morales, M (2022,7 de Julio): *Suplantación de identidad en línea: incrementan denuncias, pero no hay responsables.* DATA. La República. Véase en: **https://data.larepublica.pe/suplantacion-de-identidad-en-linea-incrementan-denuncias-pero-no-hay-responsables/**

Muñoz Conde, F. *Derecho penal. Parte general*. Valencia: Tirant lo Blanch. España – Valencia. 2002

Paez Rivadeneyra, J. y Acurio del Pino, S. *Derecho y Nuevas Tecnologías*, p.211.

PERU 21. (2022, 21 de mayo) *Ministerio de Justicia investigará filtración y venta de datos personales de ciudadanos peruanos.* Véase en: **https://peru21.pe/politica/ministerio-de-justicia-investigara-filtracion-y-venta-de-datos-personales-de-ciudadanos-peruanos-noticia/**

Pichihua, S (2023, 12 de febrero) ¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú. Agencia Andina. Véase en: **https://andina.pe/agencia/noticia-cuidado-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-peru-928425.aspx%22#:~:text=En%20el%20Per%C3%BA%20se%20registran,de%20celulares%20robados%20para%20ciberdelitos.**

Posada Maya, Ricardo (2012). "El delito de transferencia no consentida de activos", Revista de Derecho, comunicaciones y Nuevas Tecnologías. Universidad de los Andes. P. 8.

Ragués, R. *La Ignorancia Deliberada en el Derecho Penal*. Barcelona: Atelier, 2007. p. 158

Rodríguez Zarate, A. *Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos: El riesgo provecho, el riesgo creado y el riesgo profesional*. Bogotá D.C.: Javeriana. 2014

Romeo Casabona, C. *"Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la información"*, FUNDESCO, Colección impactos, Madrid. 1987

Salas Peña, D. *Responsabilidad civil bancaria frente al cliente por delitos informáticos*. Universidad de Costa Rica. 2017

SILVA, C (2023, 12 de agosto) *SBS interviene Caja Raíz: ¿Qué factores se han dado y qué ocurrirá con sus ahorristas?* Economía/Noticias. El Comercio: Véase en: **https://elcomercio.pe/economia/sbs-interviene-caja-raiz-que-factores-se-han-dado-y-que-ocurrira-con-sus-ahorristas-y-deudores-superintendencia-de-banca-seguros-y-afp-sistema-financiero-cooperativas-de-ahorro-y-credito-mypes-noticia/**

Simón, G (2023, 07 de junio). Zorrito Run Run*: Dictan 15 meses de prisión preventiva contra hackers que vendían datos personales.* La República. Véase en: **https://larepublica.pe/sociedad/2023/06/07/zorrito-run-run-dictan-15-meses-de-prision-preventiva-contra-hackers-que-vendian-datos-personales-307440**

TV PERÚ (2023, 26 de mayo). *"DIVIAT ALLANAN VIVIENDAS Y CAPTURAN A DOS CIBERDELINCUENTES"* Véase en: **https://www.youtube.com/watch?v=7IpuEGi514g**

Veliz, J. (2023, 24 de marzo). Datos peruanos expuestos y gratis*: Nuevo bot de Telegram entrega DNI, dirección, foto, firma y huellas.* RPP. Véase en: **https://rpp.pe/tecnologia/mas-tecnologia/telegram-bot-himiko-data-expone-datos-personales-de-peruanos-noticia-1474670?ref=rpp**

Villavicencio Terreros, F. *Derecho penal. Parte general*. Editorial: Grijley. Lima – Perú. 2006

Villavicencio Terreros, F. Derecho Penal Parte General, Grijley, Lima 2007, pp. 381-384

Villavicencio Terreros, F. Delitos informáticos. Ius et Veritas, 24(49), 284-304. Lima - 2014

Zevallos Prado, O. *Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce?* 2020. Véase en: **https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/#:~:text=En%20el%20a%C3%B1o%202013%20se,y%20la%20fe%20p%C3%BAblica%2C%20en**

Zevallos, N. (2022, 29 de agosto). *¿Cuánto nos cuesta el robo de un celular?* Instituto de Criminología. Véase en: **https://www.ipe.org.pe/portal/cuanto-nos-cuesta-el-robo-de-un-celular-por-nicolas-zevallos/**