FRAUDE ELECTRÒNICO Y CULTURA CORPORATIVA[1]

Luis Gerardo Gabaldón

EL FRAUDE Y LAS NUEVAS TECNOLOGÍAS EN LA ERA INFORMÁTICA

El fraude, vinculado a la idea de engaño con fines lucrativos, tiene larga historia como conducta penalizada. El Código de Hammurabí (c.1750 a.c.) contempla varias formas, tales como la entrega en préstamos de granos y plata en distinta medida de lo acordado, castigada con la pérdida total de lo prestado (art. 94), la apropiación de granos o forrajes cedidos para siembra o cría, castigada con la pérdida de la mano (art. 253) y la alteración de marcas o disposición de ganado cedido para apacentar, castigadas con multa de diez veces el valor del importe (art. 265) (Lara Peinado, 1986, p. 18,39,40). En el derecho romano, la acción originalmente concedida para perseguir los fraudes era de naturaleza privada y auxiliar al procedimiento civil, aunque mediante la práctica de los tribunales se extendió como auxiliar al procedimiento acusatorio, revistiendo entonces carácter penal (Mommsen, 1976, p. 426). El *stellionatus*, nombre genérico para la estafa, fue precedido en la criminalización por la adulteración de testamentos y de monedas, y por la corrupción de funcionarios y, aun antes, desde la Ley de las XII Tablas, por el falso testimonio, el cohecho de jurados y la compra de votos (1976, p. 419-420). Todos estos delitos implican alguna forma de engaño mediante inducción a error, si bien el interés tutelado no constituye, salvo en los casos fraude, el patrimonio individual.

En las legislaciones modernas se describen las conductas fraudulentas, bien como estafa (inducción explícita al error para obtener un provecho indebido a costa de otro) o como formas de enriquecimiento o apropiación de bienes o derechos patrimoniales que suponen la cesión, renuncia o inactivación del titular o de quien tiene

[1] Este artículo ha utilizado como base de datos mi Informe *El fraude electrónico en Venezuela: una aproximación a sus tendencias y modalidades*, Caracas, Universidad Católica Andrés Bello, Núcleo de Estudios sobre Delincuencia Económica, Sección de Investigación, Caracas, julio de 2003, p. 58. Agradezco a mi asistente de investigación, María Teresa Moreno, la colaboración en el desarrollo de los grupos de discusión, en el análisis de contenido y en la identificación de fuentes bibliográficas para la legislación comparada y las tendencias recientes. José Luis Cartaya, del Centro de Documentación del NEDE colaboró también en la identificación y acceso a dichas fuentes.

una expectativa legítima debido a una falsa representación de la realidad, generada por el defraudador, o no develada cuando se tiene la obligación jurídica de hacerlo. Este concepto amplio incluye ilícitos penales de reciente creación legislativa, como la defraudación tributaria en materia fiscal, los abusos de posición y privilegio en materia bancaria y el uso de información privilegiada (*insider trading*, en la terminología jurídica anglosajona) en materia de mercado de capitales.

El fraude conforma también un aspecto fundamental de la reflexión criminológica sobre el delito. Garófalo (1888, p. 18 ss.), quien acuñó el término que designa a esta disciplina de la modernidad e incluyó, en su definición de delito natural, la violación de los sentimientos altruistas de probidad que repercuten en daños patrimoniales o en violación de la confianza en perjuicio ajeno. Cien años después, Gottfredson y Hirschi (1990, p. 15) han definido el delito como actos de fuerza o fraude cometidos en búsqueda de satisfacción de un interés propio, bajo el supuesto de que la persecución del interés egoísta es una disposición natural de obrar el ser humano. Salvo que se desarrollen mecanismos de autocontrol, los seres humanos procurarán la utilización de cualquier medio disponible para la satisfacción de dicho interés. En ambos conceptos subyace el fraude como una forma de apropiación y ganancia- que ignora o atropella una expectativa individual o colectiva socialmente reconocida.

¿Qué tiene de nuevo, entonces, esto que llamamos *fraude electrónico*? Se podría sostener que es *el medio de comisión*, favorecido por el desarrollo de la tecnología de la información. Este desarrollo implica la revolución más importante del siglo XX, quizás la única que marcará un cambio irreversible en nuestro modo de ver y de actuar, que ha operado en forma silenciosa, universal, cotidiana y ha incorporado en forma asombrosa a una gran cantidad de personas a redes extensas de comunicación. Estas redes se encuentran vinculadas a agentes institucionales de liquidación y pago, que conforman el sistema bancario, de modo que son los bancos quienes en definitiva saldan las cuentas cuando se opera por vía electrónica. Por ello, podemos entender, en el contexto actual, el fraude electrónico como *toda conducta dirigida a la obtención de un provecho económico indebido, mediante la apropiación, la falsificación, la interferencia y la reproducción de códigos, instrucciones o programas, tanto sobre instrumentos portables como sobre programas incorporados a sistemas de procesamiento de datos, que permiten el acceso a dinero en efectivo o a bienes y servicios con cargo diferido a cuentas bancarias*.

Este es el concepto de fraude a que se refiere el art. 14 de la Ley Especial contra Delitos Informáticos de Venezuela, del 30 de octubre de 2001, al tipificarlo, como delito de peligro, cuando lo define como *manipulación de sistemas de información o datos, mediante la inserción de instrucciones falsas o fraudulentas* ***que permitan*** *obtener un provecho injusto en perjuicio ajeno*. La tipificación básica del fraude como intervención de códigos y datos, independientemente del provecho patrimonial específico, confunde la tutela de la seguridad informática con la tutela patrimonial, a pesar de que la modificación de instrucciones ha sido prevista por la misma ley como sabotaje o daño a sistemas por el art. 7.

El fraude propiamente dicho se define en otras legislaciones, como la alemana, como "estafa informática", caracterizándose, en relación al tipo básico de estafa, por la interferencia con la tecnología informática que produce el perjuicio económico a través de la sustitución de la conducta del titular del derecho, antes que como una cesión de éste último al defraudador, y que, al igual que el tipo básico de estafa, requiere para su consumación de la producción del daño patrimonial, cualquiera sea la modalidad que asuma la interferencia con los códigos, instrucciones y programas (Kindhäuser, 2002, p. 665).

La legislación venezolana también penaliza subtipos de fraude superpuestos al delito base o formas de colaboración, como delitos autónomos, e incluso actos preparatorios. Tales son la obtención indebida de bienes y servicios mediante la utilización de cualquier instrumento de pago

electrónico (art. 15), la preparación de instrumental de defraudación, definida como crear, capturar, grabar, copiar, duplicar o eliminar la información contenida en un instrumento de pago (art. 16), la detentación y comercialización de estos instrumentos (art. 16, ap. único), la apropiación de los mismos con la finalidad de uso, venta o transferencia a un tercero (art. 17), la provisión indebida de bienes o servicios contra presentación de instrumentos indebidamente obtenidos, falsificados, alterados, retenidos, revocados o vencidos (art. 18), y la posesión, venta y custodia de equipos para realizar las falsificaciones (art. 19). Esta tendencia a la criminalización expansiva de casos que podrían ser resueltos conforme a los principios generales sobre la participación y la tentativa, ilustra bien la proactividad del control penal en la era informática.

El desarrollo de las tecnologías de la información puede favorecer de varios modos el desarrollo de los fraudes, como una actividad colateral de la expansión de la movilización del dinero. La migración hacia plataformas de gestión electrónica y automatizada de procesos permite la reducción de costos y la expansión de todo tipo de negocios en cuanto a la clientela y las operaciones. El desarrollo del protocolo de Internet, caracterizado por la apertura, la interfase, y la capacidad de expansión en el medio virtual (Mc Knight, 2001, p. 43), abre la posibilidad de negocios y de fraudes a una escala inimaginable hace dos décadas. La fusión de tecnologías comunicacionales en formas cada vez más poderosas expone a tipos más solapados e inteligentes de fraude y engaño (Cerf, 1999, p. 371). Castells (2001b, p. 331) sostiene que la tecnología comunicacional permite el acopio de información sobre individuos por parte de organizaciones de todo tipo y la creación del correspondiente mercado; la tarjeta de crédito es el instrumento mediante el cual se puede clasificar, analizar y seleccionar las vidas de la gente con fines de mercadotecnia.

La información en un mercado puede tener usos lícitos e ilícitos, aunque muchas veces la definición de uno y otro dependa de la percepción de quien se siente victimizado. Según datos aportados por la Comisión Federal de Comercio de Estados Unidos, el número de quejas por fraude pasó de 220.000 a 380.000 y el monto de las pérdidas reportadas creció de USD 160 millones a USD 343 millones entre 2001 y 2002, con la usurpación de identidad encabezando el tipo de denuncia, en un 43% de los casos (delitos informaticos.com, 2002 c). Estos datos sugieren una expansión considerable de la percepción de lesividad económica y la redefinición de tipos legales de falsificación previstos en la etapa preinformática.

Algunas de las modalidades recurrentes del fraude en la era informática ya están descritas en la literatura. Muchas de las conductas comprenden la distracción y aprovechamiento directo de fondos provenientes de la vulneración externa o interna de los códigos y procedimientos de seguridad para el manejo de cuentas, como ilustra el caso de los hackers que, en 1994, transfirieron desde Rusia fondos de Citibank a cuentas finlandesas, alemanas, holandesas, suizas e israelíes (Grabosky; Smith, 2001, p. 34) o el desvío de fondos de 21 cuentas de clientes en un banco de Singapur por montos variables entre USD 113 y 2.837 (delitos informáticos.com, 2002b). Sin embargo, también incluye la obtención de datos sobre perfiles y tarjetas de crédito, por parte de intrusos (delitosinformaticos.com, 2003b), o el acceso a bases de datos, por parte de empleados de compañías de servicio, cuya información es vendida a bandas especializadas que continúan una cadena de defraudación (delitosinformaticos.com, 2002a). La participación de personal interno en los fraudes parece tener gran importancia, aunque podría haber disminuido con la apertura de las comunicaciones y las redes. Un estudio adelantado entre 1986 y 1989 para empresarios en Inglaterra determinó que la intervención de extraños a la empresa en los fraudes computacionales era virtualmente inexistente (Levi, 2001, p. 52-53), lo que demuestra el peso de la participación interna. Sin embargo, la colaboración con extraños podría haber aumentado significativamente: una estimación muy reciente para el caso de España sugiere que hasta el 50% de los casos de fraude electrónico podrían

contar con la participación de empleados descontentos de la propia empresa (Medina, 2003). Más adelante me referiré a las implicaciones de la lealtad y la cultura corporativas en el desarrollo de estas nuevas modalidades de fraude.

Podemos afirmar, pues, que la expansión de la tecnología comunicacional parece haber multiplicado la escala cuantitativa de los fraudes mediante el incremento de las oportunidades que se ofrecen para acceder cómodamente, incluso sin contacto directo con la víctima, a blancos atractivos para esta actividad delictiva. Probablemente el fraude vinculado estrictamente a lo que se conoce como banca electrónica (operaciones a través de Internet) constituye, entre nosotros, un área de criminalidad todavía relativamente limitada, si bien en perspectivas de expansión, considerando el grado de incorporación de usuarios a la red. Para 1998, la tasa de conexión a la red por cada mil habitantes fluctuaba, en los países industrializados de Europa, Asia y Norteamérica, entre 6,22 y 107,51, mientras, para América Latina, fluctuaba entre 2,03 y 0,54, con Venezuela muy cerca del tope inferior, con una tasa de 0,61 (Iesa, 2000, p. 31). Estas nuevas y variadas posibilidades pueden tener algún efecto en las explicaciones sobre el fraude. Por otro lado, el desarrollo legislativo, cada vez más estandarizado a nivel internacional, indica la tendencia de una criminalización legal anticipatoria, que no requiere en el tipo legal la consumación del perjuicio económico, sino la creación de la situación de riesgo. Este rasgo, que no es particular a la materia del fraude (véase. Hernández Basualto, 2004, en este mismo volumen, para el lavado de dinero), tiene implicaciones importantes con relación a los límites entre control social formal e informal, que discutiré más adelante.

PROPOSICIONES TEÓRICAS PARA LA EXPLICACIÓN DEL FRAUDE ELECTRÓNICO

No hay una teoría para explicar el fraude electrónico y ni siquiera la delincuencia informática en general. Aunque probablemente tampoco es necesaria su formulación, es conveniente revisar algunas proposiciones desarrolladas dentro de la criminología, cuya pertinencia, en esta materia, caracterizada por el recurso a tecnología sofisticada y por el acceso a redes de comunicación extensas y fundamentalmente despersonalizadas, puede resultar de particular interés.

El criminólogo norteamericano Edwin H. Sutherland postuló nueve proposiciones teóricas para la explicación de la delincuencia. Cuatro de ellas tienen que ver con los mecanismos de incorporación al repertorio conductual del sujeto: el comportamiento criminal se aprende; dicho aprendizaje se produce en comunicación con otras personas; lo más importante en el aprendizaje es el contacto con grupos íntimos; y el aprendizaje incluye tanto técnicas como motivos, impulsos, racionalizaciones y actitudes. Otras tres guardan relación con la dinámica del aprendizaje: se aprende a través de definiciones favorables o desfavorables sobre las leyes; cuando hay un exceso de exposición a definiciones favorables a la violación de la ley es más probable la delincuencia; y la exposición a estas definiciones favorables a la violación a la ley varían en frecuencia, duración, prioridad e intensidad. Hay otras dos proposiciones vinculadas a lo inespecífico del aprendizaje del comportamiento criminal frente al no criminal: uno y otro implican mecanismos equivalentes, como imitación o identificación, y no existen motivos específicamente criminales frente a los no criminales, pues motivaciones como el lucro, la búsqueda de la felicidad, la persecución del estatus social o la frustración son comunes a la conducta ilícita y a la lícita (Sutherland, 1996, p. 160). Es pertinente discutir, en el contexto del fraude electrónico, las proposiciones relativas a los grupos íntimos y a la asociación diferencial con definiciones favorables a la violación de la ley.

Aunque pareciera un contrasentido hablar de grupos íntimos en la red, considerando la virtualidad de la comunicación, nada hay que obste al establecimiento de grupos de interés selectivos y al logro de una "intimidad a distancia", que a los efectos del aprendizaje equivale a la situación des-

crita por Sutherland sesenta años atrás; lo íntimo ahora guarda relación con un contacto sin contigüidad física, que, sin embargo, podría ser estrecho, a los efectos del aprendizaje. Las técnicas de hackeo pueden difundirse por la red, incluso a través de "grupos íntimos" de acceso restringido, y los motivos y racionalizaciones pueden ser encontrados dentro de grupos de discusión que tematizan y discurren sobre apertura, liberalidad, monopolio, enriquecimiento, exclusividad, democratización, transparencia y propiedad privada. Estas consideraciones tocan el aspecto de la asociación diferencial con definiciones favorables a la violación de la ley. Probablemente hay, en la actualidad, más ambigüedad que antes sobre lo que es legal e ilegal, en cuanto a propiedad intelectual, beneficios, especulación, arbitraje y oportunidades, y en este sentido las "definiciones desfavorables a la violación de la ley" son más imprecisas. Ello no implica, sin embargo, que no se sigan aplicando principios como la frecuencia, duración, prioridad e intensidad de las asociaciones. La exposición desde temprana edad a los multimedia y sobre todo a la navegación virtual está compitiendo cada vez más con la interacción personalizada en el medio familiar (descontando aquella anécdota de la pareja de investigadores que, en el lecho, se comunicaban a través de sus laptops), y el prestigio de la fuente del comportamiento criminal y el refuerzo de la reacción emocional vinculados a la asociación diferencial no tienen que provenir, necesariamente, de un contacto físico inmediato. Así como la frecuencia y duración de los contactos con grupos íntimos se verificaba antaño mediante el tiempo y el desplazamiento físico hacia áreas de "organización social diferencial" espacialmente distantes, dicha frecuencia y duración puede verificarse hoy día mediante el tiempo de permanencia de la conexión con determinados sitios de la red por parte de los usuarios, en particular los niños y los jóvenes. Que estos contactos sean menos determinantes que otros de naturaleza física podría, incluso, ser discutible. Uno de los rasgos de la nueva era informática es la permutabilidad entre lo virtual y lo real, y el tema ya ha sido tratado en la cinematografía, recientemente en las películas Kill Bill, de Quentin Tarantino.

Otra consideración merece la teoría del control de la delincuencia de Travis Hirschi. En su formulación original de la teoría del control, denominada del vínculo social, Hirschi (1969, en español, 2003) destacó como elementos fundamentales de contención del delito el apego (*attachment)*, el compromiso *(commitment)*, la participación *(involvement)* y la creencia *(belief)*. El apego supone el tomar en cuenta los deseos y expectativas de los demás; como violar una norma supone actuar en forma contraria a esos deseos y expectativas, a medida que exista menor apego mayor será la probabilidad de incurrir en actos delictivos; el compromiso supone que una persona que se encuentra inserta dentro de líneas de acción convencionales vería amenazados sus propios intereses y expectativas laborales y de vida, entregándose a conductas delictivas; la participación implica que a un individuo que pasa la mayor parte de su tiempo en actividades rutinarias propias de su trabajo le queda muy poco tiempo para cometer actos delictivos; y la creencia implica que a medida que la gente piensa que debe obedecer las reglas sociales, menos propensa se encuentra a la delincuencia. Esta teoría fue formulada inicialmente con miras a explicar la delincuencia juvenil, callejera, convencional, inmediatista y poco remunerativa en términos económicos. Más recientemente, Gottfredson y Hirschi (1990, p. 190, 198-200) han extendido la teoría a los "delitos de cuello blanco", sosteniendo que delitos como la apropiación indebida, el fraude y la falsificación, si bien pueden tener causas diversas, no hay razón para pensar que sus autores obedezcan a diversas motivaciones que las que corresponden a delitos convencionales: todos requieren de la oportunidad y están asociados al castigo si se descubren, así como todos se ejecutan en interés propio y egoísta del delincuente. Y dado que la diferencia fundamental con los delitos convencionales es que los delitos de cuello blanco lesionan los intereses de la organización para la

cual se trabaja (pues los fraudes hacen más onerosos y menos eficientes los negocios), la diferencia entre "delitos de la calle" y "delitos de oficina" es el tipo de hecho, pero no la motivación ni las características del delincuente.

Aunque existan muchas modalidades de fraude con tecnologías de la información, y aunque el escenario de una clonación de tarjeta o engaño en un cajero automático o un punto de venta es distinto al de una transferencia electrónica ilegítima por un empleado bancario, todos estos delitos, en la medida en que se encuentran mayormente vinculados al "sitio de trabajo" que otros delitos contra la propiedad (véase, abajo, la discusión sobre "delito ocupacional") sugieren una revisión del elemento "participación" propuesto por Hirschi para la explicación de la delincuencia. En estos casos, no es que el delincuente deba buscar tiempo extra al de su trabajo convencional para cometer el delito, sino que lo ejecuta mientras está ocupado en dicho trabajo, o en una tarea muy vinculada con él, muchas veces difícil de distinguir del trabajo mismo (véase Manning, 2004, en este volumen). Por otro lado, el valor del "compromiso" en casos de fraudes, podría ser menos determinante como factor preventivo que en otros delitos convencionales contra la propiedad; en efecto, en materia de fraudes electrónicos la conducta delictiva puede ser más fácilmente disimulada, la víctima puede ser más distante o anónima, los signos externos de conformidad del infractor, tales como atuendo, maneras, gustos y nivel de vida, son más notorios que en otras formas de delincuencia convencional y, probablemente, la respuesta social, formal e informal, frente a este tipo de delincuencia, es menos intensa que frente a delitos convencionales. Todo ello podría implicar que quien incurre en fraudes con uso de tecnología electrónica se expone a menores riesgos y costos que un delincuente convencional, y por ello no necesitaría estar "tan comprometido" con la conformidad, como sugiere Hirschi.

Finalmente, en cuanto a las teorías de las oportunidades del delito, resulta pertinente tomar en consideración los conceptos de magnitud y valor de la oportunidad, así como de exposición, conceptos fundamentales para la perspectiva situacional del delito. Una oportunidad delictiva se define como cualquier situación en la cual los recursos del delincuente para cometer el delito superan los recursos para la protección de determinado objeto (Birkbeck, 1984/85, p. 58). La oportunidad es mayor (magnitud de la oportunidad) en la medida en que aumenta la disparidad entre recursos para el delito y protección del objeto, a favor de los primeros; una oportunidad tiene mayor valor en la medida en que aumenta el valor del objeto sobre el cual versa el delito, es decir, en la medida en que aumenta la perspectiva del beneficio económico del delincuente como consecuencia de su consumación (1984/85, p. 58-59). Estas teorías asumen que el delincuente es un ser racional capaz de calcular costos y beneficios al momento de cometer el delito; considerando que, en principio, la motivación para cometer el delito es invariable, esto es, constante en todos los sujetos, la decisión de cometer el hecho depende, en primer término, del valor de la oportunidad, bajo el supuesto de que el delincuente se encuentra atraído, en un primer momento, por la perspectiva del beneficio económico a ser obtenido y, mediante una segunda selección, por la magnitud de la oportunidad, esto es, por la disparidad, a su favor, de los recursos dispuestos para proteger un determinado objeto, en presencia de objetos de igual valor (Birkbeck, 1984/85, p. 65). Si estos supuestos son correctos, podríamos esperar que, en materia de estos fraudes, el acceso a información relevante sobre el valor del objeto, en este caso, montos disponibles en cuentas bancarias o límites autorizados de crédito, es crucial para la decisión de seleccionar un blanco para la defraudación. El nivel de protección entraría a ser considerado en una segunda fase, como opción para victimizar con mayor frecuencia a quien se encuentra en desventaja para oponer resistencia o para, de otro modo, neutralizar el ataque. Esta condición podría representar mayor variabilidad para las defraudaciones "cara a cara" sobre víctimas desprevenidas en cajeros y puntos de venta, que para

situaciones de mayor distancia y automatización, donde se supone que los procesos de seguridad se encuentran estandarizados y revisten menor variabilidad. En ambos casos, tanto en lo que se refiere al valor del objeto del delito como a la protección del blanco seleccionado, la variable determinante podría ser la personal, antes que la tecnológica, por las mismas razones: hay mayor variabilidad en la primera, sea que se refiera a filtración de información confidencial como a falta de cuidado frente a una aproximación física, que en la segunda, que estandariza procesos.

Un aspecto importante dentro de estas teorías es la exposición del blanco que resulta atractivo. Birkbeck y Lafree (1989, p.19) han sugerido que no es la reducción de la distancia física entre grupos delincuentes y víctimas, a través del contacto directo, lo que aumenta el riesgo de estas últimas, como sugerían las primeras teorías sobre la victimización interpersonal, sino el incremento de la frecuencia con la cual un delincuente evalúa a una víctima como blanco potencial, la cual aumenta con la proximidad espacial. Estas consideraciones se han hecho tomando en consideración la delincuencia convencional contra la propiedad, que requiere algún tipo de proximidad fìsica, en casos de hurto, robo o estafa, pero también resultan aplicables a la defraudación por medios electrónicos, tanto en los casos que implican contacto físico inmediato, tales como clonación de tarjetas y retiros en cajeros mediante sustitución de titularidad, como en los que no lo requieren, como manipulación de bases de datos en computadoras. En efecto, no solo a través de la observación reiterada de posibles víctimas es posible inferir sobre su estilo de vida, perfil económico o tipo de cuidado empleado en sus operaciones cotidianas, sino que, a través de la supervisión incrementada de determinados titulares, puede evaluarse mejor su perfil y conducta, tanto en términos del valor de la oportunidad (monto de transacciones y movilizaciones) como de la magnitud de la oportunidad (medidas de seguridad adoptadas, uso de claves, encriptación, acceso).

UN MARCO METODOLÓGICO PARA EL ANÁLISIS DEL FRAUDE ELECTRÓNICO EN VENEZUELA

Abordar el tema del fraude electrónico en Venezuela, en una perspectiva que rebase el análisis normativo y que procure incorporar datos confiables sobre sus manifestaciones y tendencias, requiere un trabajo fundamentalmente exploratorio y cualitativo. Por una parte, estas conductas no son convencionales, en el sentido que obedezcan a una práctica bien sedimentada, sobre la que existan datos cuantitativos, registros oficiales, rutinas y prácticas policiales y judiciales bien establecidas y, en general, un acervo documental consistente. Por otro lado, el medio bancario constituye un ambiente de negocios de acceso restringido, debido a la confidencialidad requerida por la clientela y a las estrategias de negocios que implican el mantenimiento de ventajas competitivas. Por todo ello se requiere un abordaje no intrusivo y de perfil fundamentalmente cualitativo. Ello permite tanto el acceso cómodo al ambiente de negocios bajo estudio como la elaboración de categorías y registros que permitan la identificación de las modalidades operativas y tendencias generales del fraude. Es por ello que hemos adoptado, como método de acceso a la información el grupo de discusión (o grupo focal) y como técnica de procesamiento de la información el análisis de contenido.

El grupo focal es una forma de investigación cualitativa basada en una conversación con un grupo preseleccionado y orientada por temas suministrados por el investigador, que funge como moderador del grupo. Es mediante el uso de esta interacción grupal que se obtienen datos y sugerencias a los cuales resultaría difícil acceder sin la interacción que proporciona la actividad grupal (Morgan, 1997, p. 2). El grupo focal se sitúa, como método de recolección de información, entre la observación participante, que supone la presencia no intrusiva del observador en el ambiente a ser estudiado, y la entrevista, abierta o cerrada, que supone la proposición de preguntas por parte

de un observador externo, a los sujetos de la investigación. Como ventaja se destaca la posibilidad de obtener concentración de información sobre el tema propuesto, enriquecida por el intercambio de opiniones y experiencias entre los participantes, en condiciones de relativa rapidez y facilidad; como desventaja hay que destacar la relativa indiscriminación entre lo que el miembro individual y el colectivo podrían aportar, la dificultad que pueden tener algunas personas de expresarse libremente frente a otros y la polarización de las opiniones en cuestiones sensibles (Morgan, 1997, p. 13-15). El grupo focal ha sido ampliamente utilizado desde la década de 1950 en estudios de mercadeo y preferencias de consumidores, y se considera apropiado como método cualitativo que puede complementar otros métodos de investigación social, tales como la entrevista, el sondeo de opinión, la observación participante y el experimento (1997, p. 22-30).

El análisis de contenido se ha definido como *una técnica de investigación destinada a formular, a partir de ciertos datos, inferencias reproducibles y válidas que puedan aplicarse a su contexto* (Krippendorff, 1990, p. 28). Dado que la información que se recoge a través del grupo de discusión proviene de una comunicación colectiva orientada por una guía temática flexible, la técnica del análisis de contenido resulta particularmente apropiada para estudiar las percepciones, opiniones y particularidades del fraude electrónico, tal como es percibido por los participantes calificados para intervenir en un grupo de discusión.

Decidimos convocar a dos grandes bancos a designar participantes en cuatro grupos focales de discusión, dos de ellos con intervención de funcionarios policiales y fiscales del Ministerio Público. Las sesiones se realizaron los días 6 y 20 de noviembre de 2002 y 5 y 26 de marzo de 2003, con la asistencia de 12 funcionarios de uno de los bancos y 13 funcionarios del otro, 4 fiscales y un auxiliar de fiscal del Ministerio Público y 3 funcionarios del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas. Los funcionarios del primer banco provienen, dos de ellos de la Unidad de Monitoreo de Alertas, dos de la Unidad de Investigaciones de tarjetas y uno de las Unidades de Prevención de Fraudes, Administración y Seguridad de la Informática, Soporte Tecnológico de la Red Física, Auditoría de Sistemas, Investigaciones Regional, Metropolitana e Internacional y Comercio Electrónico y Cajeros Automáticos. Los funcionarios del segundo banco provienen, cinco de ellos de la Unidad de Seguridad Operativa, tres de la Unidad de Medios de Pago, dos de la Unidad de Desarrollo de Sistemas, dos de la Unidad de Calidad Informática, y uno de la Unidad de Banca Electrónica. Los fiscales del Ministerio Público tienen competencia plena en el área Metropolitana de Caracas, y uno de ellos ha trabajado con cierta especialidad en materia de delitos informáticos. Los funcionarios policiales pertenecen a las Brigadas de Delitos Telemáticos, de Falsificación y Bancaria, de la División Nacional contra Delitos Financieros e Informáticos de CICPC. Como se puede apreciar, se trata de funcionarios con experticia y experiencia en el área del fraude electrónico, provenientes del medio bancario y del sistema de administración de justicia penal.

Cada sesión, de una duración aproximada de 135 minutos, fue adelantada con un director de debate como moderador y un asistente de debate, quien tomó apuntes puntuales para facilitar la identificación del orden de intervenciones. Se exploraron temas como características, modalidades, motivaciones, vulnerabilidad sistémica, y organización del fraude electrónico, mediante la incorporación y desarrollo de temas sucesivos, en cada nueva sesión, de acuerdo a los aspectos resaltantes identificados en la sesión inmediatamente precedente. De este modo, las guías temáticas incorporaron aspectos surgidos en sesiones previas, acumulando y organizando información calificada a medida que avanzaba el proceso de la investigación. Se procuró incrementar la participación de funcionarios con mayor capacidad de decisión en las últimas sesiones, así como la incorporación explícita de los temas de detección, investigación y persecución penal del fraude electrónico en las sesiones tercera y cuarta, a fin

de tener una aproximación al sistema de justicia penal.

Las sesiones fueron grabadas mediante un registro magnetofónico con cuatro canales, a fin de preservar la discriminación de todas las intervenciones, y fueron transcritas y analizadas en cuanto a contenidos temáticos en función de criterios de relevancia y recurrencia. Se garantizó la salvaguarda de la identidad de cada participante al momento de presentar los resultados del análisis temático correspondiente, a fin de favorecer la participación y libre expresión de ideas y experiencias, en un ambiente de diálogo abierto y constructivo.

La discusión de los temas que se desarrolla a continuación incorpora, junto a las consideraciones generales de la bibliografía disponible, algunos aspectos surgidos en los grupos de discusión y que constituyen la base de datos de esta investigación.

DIVISIÓN DEL TRABAJO, DESARROLLO TECNOLÓGICO Y ORGANIZACIÓN DELICTIVA

El fenómeno del fraude a través de medios electrónicos no ha generado aun suficiente información para describir patrones consistentes de división del trabajo y organización delictiva. Castells (2001c, p.201 ss.), refiriéndose a la globalización y la criminalidad, menciona como ejemplos paradigmáticos de esta última el tráfico de drogas, el blanqueo de activos y el tráfico de personas, órganos, armas y materiales nucleares. Levi (2004) sugiere que la organización delictiva podría concentrarse en actividades fraudulentas que requieren especialización e inversión de capital, como el forjamiento y la reproducción de tarjetas de crédito o de débito, aunque es cauteloso sobre la posibilidad de que existan organizaciones criminales en torno a las actividades fraudulentas en sus diversas modalidades. Dado que la utilización del medio informático para defraudar es relativamente reciente, probablemente no existen aún estructuras estables que hayan "ocupado" este sector de la economía en perspectiva global.

Esta cuestión sobre la delincuencia organizada en materia de fraude electrónico, su perfil y desempeño, no ha arrojado suficiente información en los grupos de discusión que adelantamos en Caracas. Los participantes hablan de "bandas" y "organizaciones" en varios contextos, aunque no en forma inequívoca. Dos representantes bancarios y un fiscal comentaron que hay una proliferación de estas agrupaciones y, en comentarios separados, igual número de representantes se refirieron a bandas a nivel internacional, es decir, que operan más allá de las fronteras del país. En dos comentarios adicionales se aborda la especialización y la división del trabajo, con implicación internacional, y en uno más se habla explícitamente de la planificación de actividades y el entrenamiento de delincuentes en el área del fraude electrónico. Un funcionario policial reconoce la existencia de áreas comerciales ocupadas por bandas y un representante bancario admite que la falsificación y uso de tarjetas es producto de bandas organizadas. Otro sugiere que esta forma es la que permite penetrar y captar colaboradores entre empresas proveedoras de servicios o entidades bancarias, con experiencia previa en el área de trabajo. Otro comentario refiere que los cabecillas están muy bien preparados, aunque quienes trabajan "en la calle" no requieren dicha preparación. En tres oportunidades se habló de trabajo fácil con acceso a mucho dinero. Un funcionario policial llegó a comentar que es la delincuencia organizada la que afecta "verdaderamente" a las entidades financieras, y un funcionario bancario consideró que, si bien los hechos no son de ordinario violentos, se puede llegar a adoptar represalias contra el personal de seguridad de los bancos que identifica a las bandas. Esta utilización de la violencia ha sido vinculada, tanto en análisis nacionales (Block; Chambliss, 1981) como internacionales (Castells, 2001c) a la delincuencia organizada, en general, como un mecanismo para lograr sometimiento, defensa de espacio y mercado en materia de actividades ilícitas.

Un representante bancario brindó la descripción de un caso en el cual fue aproximado por una supuesta organización delictiva en un restaurante del Este de Caracas, a través de un conocido suyo:

> ...nosotros somos una banda que fregamos a bancos... le clonamos una tarjeta y le robamos no sé cuántos millones de dólares al banco y queremos darte tanto para que tú nos des la información y nosotros estamos agradecidos y no sabemos más nada de ti... ahorita no tienes que hacer nada, y lo único que quiero es que tú me digas que sí o no para estar dispuesto... el domingo que viene nos vamos a encontrar otra vez aquí, pero vas a hablar con otra persona... una de las cosas que me dijo el tipo es que sabía dónde yo vivía, a qué hora salía del banco, dónde almorzaba, sabían todos mis movimientos... le cuento a(...) y me dice... eso es una banda, no sé qué cosa, ustedes conocen esos términos... al poco tiempo me enteré que habían agarrado en ese mismo restaurante, porque salió publicado en el periódico, a una banda de clonadores y de estafadores de maquinitas y de prostitución...

Sin embargo, en otros comentarios no queda claro el proceso de la organización delictiva, y se sugiere, más bien, la existencia de un amplio escenario en el que se mueven muy variados actores, si bien de alguna manera vinculados, no necesariamente a través de una organización específica. Así, un representante bancario menciona que las tarjetas clonadas son "vendidas a bandas de delincuentes", como si éstos últimos formasen un grupo aparte de los clonadores mismos. En dos comentarios, de un representante bancario y de un fiscal, se indicó el uso de "intermediarios" que impiden identificar a los cabecillas en el proceso de distribución de las tarjetas clonadas, lo que sugiere una escasa integración entre las fases de preparación del instrumento del fraude y su utilización. Por otro lado, uno de los fiscales se refiere a un *pacto sceleris* en estos delitos, lo que sugiere una asociación oportunista para determinados hechos, antes una organización estable. En dos comentarios de un policía y un fiscal se habló de reclutamiento de informantes entre bandas, aunque la mención de la banda, en este contexto, no especifica grado de participación o compromiso con la actividad delictiva.

Pensamos que el tema de la organización criminal en materia de fraude electrónico es todavía un área relativamente inexplorada que requiere mayor investigación e información.

CULTURA CORPORATIVA Y LEALTAD EMPRESARIAL

Las organizaciones, entendidas como sistemas, suponen la integración de estructuras y funciones para la obtención de una finalidad común. Así, han podido ser definidas como *sistemas humanos de cooperación y coordinación integrados dentro de límites definidos con el fin de alcanzar metas compartidas* (Hodge; Anthony; Gales, 1998, p. 13). Dos conceptos estrechamente vinculados al concepto de organización son el de *cultura* y el de *compromiso*. La cultura ha sido concebida como *conjunto de reglas tácitamente asumidas que dicen a los empleados lo que deben hacer en una gran variedad de circunstancias*, mientras el compromiso ha sido entendido como *una situación en la que los miembros de un grupo aportan sus esfuerzos, habilidades y lealtades a la organización y a la consecución de las metas, para obtener a cambio satisfacción* (Hodge; Anthony; Gales, 1998, p. 251, 265; véase también, Manning, 2004, para una distinción entre compromiso, adhesión y lealtad). Dado que las actividades de fraude suponen conductas desarrolladas en el proceso de interacción de la organización con el medio exterior, mediante participación de propios y extraños, hemos querido incorporar los temas de la lealtad empresarial y la cultura corporativa al análisis de esta materia, lo cual permite explorar y analizar variables vinculadas a la explicación y predicción de estas conductas. Considerando, por otro lado, que el medio en el cual se desarrolla este tipo de defraudación es el de una actividad económica lícita, como la bancaria, y que la actividad se desarrolla con el soporte de nuevas tecnologías, podríamos considerar que el fraude electrónico encuadra dentro de lo que algunos han denominado *delito ocupacional*, entendido como *cualquier acto punible que se comete a través de oportunida-*

des creadas en el curso de alguna ocupación que es legal (Green, 1990, p. 12-13). Estas oportunidades deben entenderse como creadas, no solo para quienes trabajan dentro de una empresa sino para quienes, desde afuera, utilizan operaciones y transacciones generadas en el curso de actividades usuales e incluso rutinarias de la organización, para obtener ventajas indebidas.

La cultura organizacional venezolana ha sido descrita, según un estudio adelantado hace 10 años en 40 organizaciones públicas y privadas, mediante 2.192 cuestionarios y 50 entrevistas, como defensiva de la jerarquía para definir la autoridad, requirente de vigilancia y control a todos los niveles de la gerencia, con fuerte motivación para el poder, como medio de implantar planes y obtener resultados, de aceptación de la distancia frente a los superiores pero, a su vez, de recurrencia necesaria a las vías informales a través de relaciones personalizadas, para atenuar la distancia y lograr la fluidez de los procesos (Granell: Garaway: Malpica, 1997, p. 25-26). Los rasgos descritos permiten identificar una organización donde, a la par de la vigilancia y la desconfianza, subsiste la informalidad y el amiguismo y donde probablemente los procesos de supervisión no son, después de todo, tan estrictos como parecen.

En nuestra investigación a través de los grupos focales, pudimos identificar algunos resultados compatibles con estos rasgos, que pueden ayudar a explicar la laxitud y flexibilidad de ciertos procesos.

En cuanto a los procesos de toma de decisiones y jerarquía, hemos recogido nueve comentarios entre representantes de ambos bancos en los cuales se enfatiza la adopción de decisiones y la imposición de criterios sin mayor participación de los empleados. Algunos de ellos mencionan la aplicación de medidas de presión y el establecimiento de cuotas de productividad, si bien un representante bancario destacó que las unidades administrativas preguntan a los empleados el nivel de capacitación que requieren y facilitan dicha capacitación, mientras otros dos de ellos mencionaron como positivo el aplanamiento de la estructura jerárquica del banco y la asignación de responsabilidades a especialistas, en la base, lo que permitiría un flujo más eficiente de la información. Otro representante bancario mencionó, en dos oportunidades, la responsabilidad del líder en la calidad de la comunicación, las relaciones interpersonales y el flujo de información.

En cuanto al ambiente de trabajo, fue descrito con cierta ambigüedad. Algunos hablan de buen compañerismo y de la necesidad de sentirse cómodo en el sitio de trabajo para evitar el malestar físico; dos representantes bancarios indicaron satisfacción por la adecuada división del trabajo y el buen trato. Sin embargo, surgieron varios comentarios sobre las fallas en la ubicación del personal según su nivel de capacitación o merecimiento. Esta situación genera incomodidad al momento de supervisar el trabajo de los subordinados, según una representante bancaria, si bien otras reconocen que la exigencia de rendimiento es indispensable e inevitable a pesar de estas situaciones. Otro representante bancario recomienda aceptar una situación transitoria de desventaja en espera de una mejor oportunidad.

Por lo que se refiere a manuales y procedimientos, dos temas importantes son la falta de control sobre el acceso a información sensible por parte de antiguos empleados de la institución y la inexistencia o ambigüedad de normativa explícita sobre comunicación, lo que produce una flexibilización de hecho. El escaso control sobre acceso y retención de información generó comentarios por parte de tres representantes bancarios. Unos indican que las auditorías revelan retención acumulada de claves por parte de ex empleados, o por empleados que son desplazados a otras áreas donde ya no las requieren. La conexión de este problema con la seguridad de la información es puesta de manifiesto por el siguiente comentario de otro representante bancario:

> ...si las instituciones fueran constantes, fueran totalmente auditoras, los riesgos fueran menos... es imposible que cada seis meses que yo audito el sistema me dice que hay mil personas con la misma clave, de los cuales 500 se han ido y 500 están en otras áreas donde no debería existir esa

> clave... podemos estar totalmente encima de los proyectos, encima de los sistemas, encima de las revisiones, pero si no somos efectivos estamos en lo mismo, seguirá siendo el mismo fraude.

La carencia de normativa explícita comunicacional y la sustitución por mecanismos informales es bien descrita por una representante bancaria en los siguientes términos:

> Pienso que no hay algo que haya establecido el Banco a través de un manual o un correo o algo... todo el mundo busca sacar su trabajo y eso es la comunicación que tienes tú con los demás departamentos... existe esa interacción y todos buscamos la manera de ayudarnos. Yo pienso que en las organizaciones, actualmente, todo eso es debido a la necesidad... tengo un muchacho a mi cargo y él me está pidiendo algo y lo tiene que sacar. Y entonces le digo, mira, vamos a sentarnos de contingencia, se hace el trabajo de grupo con el personal, pero no es algo que vino del jefe; no, es algo muy espontáneo, mira tenemos que sacar esta trabajo y existe esa comunicación... qué ideas aportas tú para sacar el trabajo y yo escucho a mis analistas... de repente yo pongo el camino más largo y ellos pueden establecerme a mí el camino más corto... puedo decir que la gerente se dirige a mí y mi jefe no se aprieta.

Esta cuestión de la comunicación informal permite conectar con el tema de la comunicación con otras entidades bancarias, que fue mencionada como importante para la resolución de todo tipo de problemas por representantes de ambos bancos y de la policía en cuatro oportunidades, aunque en otras seis se indicaron sus dificultades, debidas, fundamentalmente, a la competencia y al celo comercial. Un representante bancario, discutiendo el tema de la información cruzada sobre fraudes, lo expresa en los siguientes términos:

> ...hay un celo por parte de muchas áreas de los bancos, sobre todo la de toma de decisiones... cada banco hace su política de publicidad por separado, pero sentarnos todos y decir: vamos a sacar una propaganda y educar al cliente sobre todo lo que está pasando, eso no se ha logrado. Por eso, porque hay ese recelo de cómo lo va a tomar el cliente a la hora de ver esa propaganda que diga: mira, el fraude se comete de esta forma y entonces el cliente puede tomar una decisión: si mi dinero no está seguro aquí, yo voy a retirarlo.

El proceso de comunicación con los clientes puede resultar afectado por esta visión restrictiva, si bien la inducción y facilitación de información a la clientela fueron mencionadas en ocho oportunidades y en tres de los grupos de discusión como importantes para prevenir los fraudes, especialmente a través de instrucciones sobre activación de las tarjetas de crédito o débito, reserva sobre las claves y utilización de los cajeros automáticos. Sin embargo, los límites entre información oportuna e inconveniente y las referencias a la necesidad de las estipulaciones contractuales para determinar las responsabilidades del banco frente a sus clientes, en materia de fraudes, ilustran bien la tensión entre la seguridad y el riesgo implícito en toda expansión de los negocios. La pertinencia de la información selectiva a los clientes queda manifiesta en el siguiente comentario de un representante bancario:

> A nivel comercial la información tiene que ser filtrada, o sea, yo no puedo decirle a un cliente la forma cómo se atraca o cómo se roba o cómo se comete un delito... esos son los puntos más delicados, cuando legalmente son establecidas todas las actuaciones nuestras, yo hago un contrato con un usuario que es un cliente, y le indico: usted no puede darle la tarjeta a terceros, no puede traspasar la clave, no puede escribir la clave detrás de la tarjeta... lo mismo cuando yo le digo a un cliente a través de un contrato que el cliente es como un padre con esa chequera, entonces ese cliente cuando nos hace un reclamo yo le demuestro que efectivamente su paternidad no se demostró o fue deficiente... pero yo no puedo decirle a él, los ladrones llegan y abren los carros y se llevan las chequeras, sacan los cheques, te falsifican la firma. Yo les digo que tienen que cuidar sus chequeras, hasta ahí llega la información.

La preservación de la imagen del banco ante la clientela, por otra parte, queda expresada en el siguiente comentario de este representante bancario:

> ...ya nosotros tenemos un seguro de veinte millones de dólares en caso que ocurra un robo (sic). Ok, muy bueno este seguro, ¿pero tú vas a pagar con veinte millones de dólares el prestigio de un banco? Si llega a ocurrir algo así, algo de envergadura, porque esto es algo grande, el banco ¿se va a recuperar? ¿va a pagar el prestigio ante sus clientes y el cliente nuevamente va a creer en el banco? Jamás.

El riesgo implícito en la expansión de las oportunidades de negocios queda manifiesto en el siguiente comentario de otra representante bancaria:

> ...si nosotros vemos atrás, la cultura o la visión de los bancos, los que llevaban aquel entonces la visión del banco, fue que siempre querían ser los primeros en ofrecer servicios, primeros en ofrecer el producto y por eso siempre las áreas de desarrollo trabajaban como casi a la carrera porque el banco quería ser el primero en prestar este servicio... esa fue la cultura que tuvo la banca nacional en estos últimos años. Ahora, producto de eso es que tenemos sistemas abiertos, sistemas con atribuciones claras, nunca se habló de medidas de revisión de datos, de transferencia segura de datos, ninguna de esas políticas se tomaron nunca en cuenta hasta que comenzamos a tener estos niveles de fraude... hacíamos sistemas apurados, desarrollos, porque el gerente quería ser el primero en ofrecer este producto...

En estos comentarios se aprecia una clara tensión entre apertura y reserva, entre riesgo y oportunidad y entre información y desinformación, que evidentemente requiere mayor reflexión para entender apropiadamente los patrones que gobiernan el flujo de información extrabancaria. Esta tensión se manifiesta, por supuesto, en el flujo de la información hacia el sistema de justicia, sobre la cual es pertinente mencionar la ambivalencia percibida en las conexiones con la policía. Buena parte del personal de seguridad de la banca proviene de la policía, y los funcionarios policiales participantes en el tercer grupo de discusión reconocieron, en una oportunidad, que la información entre los departamentos de seguridad bancaria y la policía fluye adecuadamente, y en otra, que ha habido trabas para dicho flujo, en un caso en el cual hubo implicados de la alta gerencia. La aparente contradicción desaparece si se pone en contexto el continuo formalidad e informalidad en el flujo de la información. La información a través de canales formales conduce a procesos legales, mientras la operada a través de canales informales podría servir para reforzar la seguridad y detección sin recurrir al sistema de justicia, con o sin participación de la policía. Una y otra cumplen diversos propósitos. El siguiente comentario de un representante bancario puede ilustrar esta antinomia, si se busca reconstruir en el texto un discurso que no llega a ser totalmente explícito:

> ...en este ambiente, más que con las autoridades yo creo que entre las unidades de seguridad de los diferentes bancos hay muy buena comunicación... pareciera mentira pero hay menos comunicación muchas veces, quizás, por políticas internas de los propios bancos entre entidades... todos nos conocemos en este ámbito de seguridad... y quizás yo puedo tener una información extra oficial como amistad pero él me la da como amistad porque existen políticas establecidas dentro de esa institución que no te permiten dar ese tipo de información, yo la tengo extraoficialmente pero oficialmente no puedo y por fidelidad a esa persona tampoco.

Evidentemente que un tema importante de investigación, en el futuro, es la relación entre las exigencias de seguridad, espacio de negocios, riesgos, comunicación selectiva y relaciones con instancias ajenas a la organización bancaria, que permitan aclarar la racionalidad, propósito y resultados de los esfuerzos combinados para enfrentar la problemática del fraude electrónico.

En cuanto al tema de la lealtad a la empresa, entendida como la adhesión a sus prácticas y honestidad laboral, antes que la disposición del sobre tiempo de trabajo (véase Manning, 2004), resaltan varios temas, como son: a) las motivaciones para la fidelidad y el compromiso con la empresa; b) las manifestaciones de la infidelidad en cuanto a las conductas fraudulentas; y c) los riesgos de la infidelidad en cuanto a la cuestión más amplia y general del acceso a la información y la seguridad de las bases de datos en la empresa.

Por lo que se refiere a las motivaciones para la infidelidad, un tema recurrente es la percepción de escasa remuneración, que mereció siete comentarios directos, incluyendo la percepción de subpago en función de la calificación que se posee o del tiempo extra requerido por los bancos. La dificultad de obtener otro trabajo fue presentada como un motivo para permanecer en la empresa en otras dos oportunidades. Sin embargo, no emerge una vinculación directa entre insatisfacción laboral e infidelidad, si bien es posible inferir que la frustración que esta situación genera podría influir, por vía indirecta, en el apego y la lealtad en el trabajo. Los participantes reconocen, también, que otras motivaciones como la perspectiva de carrera en la institución bancaria, los beneficios adicionales al sueldo (que no fueron explicados) y el desarrollo profesional, pueden constituir

alicientes para permanecer empleados en los bancos, aunque esta dimensión tampoco puede vincularse directamente a conductas de lealtad en el trabajo. Un comentario de un representante bancario, no obstante, establece una relación explícita entre las dimensiones de remuneración, desarrollo profesional y la lealtad a la empresa:

> Yo no puedo mantener a un empleado que tenga 14 años trabajando ganando un sueldo de 230.000 bolívares mensuales. Hoy en día ese es un delincuente en potencia y esa puede ser una falla del empleador... yo empleador necesito darle a él la confianza total o el apoyo total para que ese empleado se desarrolle... esa es una situación que lo que está creando es un foco de delincuentes... hoy en día de cien empleados que se meten en problemas, ochenta son de ese tipo de empleados...

En algunos comentarios de los participantes la cuestión de la ganancia fácil es destacada como la principal motivación para el fraude, antes que una frustración acumulada por la percepción de una remuneración inadecuada. Esto se aplicaría, fundamentalmente, a empleados muy jóvenes que, careciendo de otros factores de contención, como lazos familiares y compromisos de vida, se hacen particularmente vulnerables a esta situación. Un representante bancario lo expresa de esta forma:

> ...no es la generación nuestra, es la generación nueva, estos muchachos que están naciendo y que están aprendiendo a trabajar ahorita, son los que se meten en esos problemas... hoy en día los muchachos no saben lo que es la identidad y viven de otra forma... en muchos casos se descubrieron (sic) a los muchachos y ellos decían, no mira, vale, me ofrecieron medio millón de bolívares y yo necesito esos reales, porque estoy enamorado de una chica, porque quiero un zapato de marca o quiero ir a la playa, entonces a mí no me interesa la información del banco, yo se la vendí y ya está. Si me quieres meter preso, méteme.

La infidelidad se puede manifestar, a juicio de los participantes, como suministro de información confidencial, tanto internamente, entre los propios empleados dispuestos a defraudar por su cuenta y riesgo, como externamente, hacia personas ajenas al banco que conforman una red de defraudación con los empleados. Sin embargo, del contexto de las discusiones, pareciera desprenderse que la conexión externa es más frecuente, en muchos casos mediante la captación de empleados retirados y descontentos que pueden suministrar información calificada para acceder a datos, lo cual no sería una particularidad venezolana ni algo exclusivo del sistema bancario, pudiendo producirse también entre compañías que suministran programas de computación por vía de outsourcing. Dos comentarios expresos fueron realizados sobre este particular.

Las anteriores consideraciones llevan a poner un tercer aspecto vinculado con el tema, esto es, la cuestión de los riesgos asociados a la infidelidad en cuanto al acceso a la información y la seguridad de las bases de datos en la empresa. En siete comentarios provenientes de tres grupos de discusión se hizo manifiesta la estrecha conexión entre acceso a información sensible e infidelidad y riesgo de fraude, y en cuatro comentarios más, incluyendo dos de fiscales del Ministerio Público y uno de la policía, se planteó con convicción el hecho de que la infidelidad permite rebasar cualquier control de seguridad existente. Un representante bancario insistió en que el nivel de sofisticación de ciertas estafas revela con claridad un conocimiento superior y la sustracción de información interna; otro representante bancario resume su percepción sobre la relación entre infidelidad y vulnerabilidad de la seguridad de la siguiente manera:

> Existiendo los sistemas que son netamente manejados por el hombre, necesitamos de una característica particular que es la infidelidad... yo no puedo obtener información siendo un agente externo, de las transacciones, de las operaciones, de los proyectos que se están generando en la institución, a menos que tenga un infiel.

La cuestión de la fidelidad a la empresa cobra particular importancia cuando se trata de personal de alta jerarquía, debido a los niveles de información, creatividad y dominio que posee. Un representante bancario indicó que, pese a lo infrecuente de esta situación a nivel de alta gerencia, sus efectos son muy dañinos debido a la ascendencia de estas personas sobre los subalter-

nos y a la información que poseen. Dos representantes de los fiscales mencionaron a un gerente y un vicepresidente de operaciones en casos de deslealtad vinculada al fraude. Por otra parte, la posibilidad de destruir o disimular evidencias una vez cometido el fraude, por parte de empleados infieles, añade un componente adicional de impunidad, según mencionó un representante policial en el tercer grupo de discusión. Pensamos, sin embargo, que la relación entre la fidelidad, como conducta de compromiso y lealtad con el desempeño funcional, y la satisfacción laboral derivada de los estímulos salariales o profesionales, no está todavía claramente establecida, y constituye un tema de interés y relevancia para una investigación ulterior. Como lo ha expresado un representante bancario, el cumplimiento leal de los compromisos asumidos puede implicar valores de diverso tipo, lo cual requiere una visión que va más allá de los incentivos materiales.

CONTROL SOCIAL FORMAL E INFORMAL DEL FRAUDE

El control social puede ser entendido como el conjunto de instancias y acciones, públicas o privadas, genéricas o específicas, encargadas de definir, individualizar, detectar, restringir y (o) suprimir conductas delictivas o desviadas (Gabaldón, 1987, p. 11). Hablamos de control formal cuando se trata de instancias y acciones públicas y específicas, dentro de las cuales, en materia delictiva, destaca el sistema de justicia penal con todos sus actores: jueces, fiscales, policías, defensores y funcionarios de ejecución penal. El control informal está representado por instancias y acciones privadas o, en caso de ser públicas, no específicamente dispuestas o autorizadas para lidiar con el problema. El control formal es legalista y rígido, mientras el informal es moralista y flexible; en ambos siempre está implícita la coerción como último recurso, aunque con diversos perfiles de intensidad y probabilidad.

El desarrollo de la red, que pasó de un sistema de información estratégica gubernamental norteamericana a un sistema de comunicación abierto e irrestricto hace algo más de una década, ha producido el fenómeno de un espacio no regulado, sometido al avance tecnológico y a la disciplina que puedan disponer sus propios usuarios (Castells, 2001a, p.78). Por otro lado, ha determinado que la definición situacional de un delito quede librada a una multiplicidad de actores dispersos antes que a determinados órganos de control social formal con base territorial (Wall, 2001, p. 11). Esto representa desafíos importantes a nuestros conceptos tradicionales sobre el control y la prevención de la criminalidad. Dado que la materia del fraude electrónico es novedosa y constituye un área de reciente intervención para el sistema penal, es pertinente resaltar algunos de los temas que emergieron en nuestros grupos de discusión en relación a su control formal e informal.

Lo primero que pudimos observar fue que la persecución a través del sistema de justicia penal constituye un tema complejo, por cuanto involucra cuestiones de legalidad formal, oportunidad, conveniencia y optimización de recursos. Las cuestiones abordadas dentro de esta temática pueden ser divididas en dos grandes grupos: a) percepciones y comentarios sobre activación del sistema de justicia formal, que comprende todo lo relativo a la investigación, documentación, preservación de evidencias e incorporación a un proceso que debería culminar, bien con una sanción, bien con la exoneración de responsabilidad o con el archivo de las actuaciones; b) percepciones y comentarios sobre el sistema informal de tratamiento de los casos, que comprende la búsqueda de alternativas al sistema legal existente. A continuación se presentan los temas discutidos y se reportan los comentarios específicos que realizaron los fiscales del Ministerio Público, por separado, dado que, con la reforma de la legislación procesal de 1998, corresponde a ellos la dirección formal de la investigación y las decisiones sobre persecución o archivo de los casos en sede judicial.

Pese a que la captura y procesamiento de clonadores o "pescadores" de bandas magnéticas

fueron mencionados en dos oportunidades como indicadores de activación del sistema de justicia formal, mayor número de comentarios, tanto por parte de los representantes bancarios como de la policía, generó la falta de recursos para adelantar la investigación policial y la impunidad y falta de procesamiento de los casos, incluyendo el grupo de infractores entre 16 y 17 años, lo que, a juicio de un representante bancario, estimula la reincidencia y la formación de bandas. También se destacó el otorgamiento de beneficios penales y procesales, lo cual es percibido como un estímulo para el delito. El trabajo conjunto entre bancos y policía fue destacado expresamente como importante en nueve comentarios a lo largo de los grupos de discusión, incluyendo dos de ellos donde se destacó, por parte de un representante bancario, la asesoría brindada a la policía sobre cómo adelantar la investigación. En dos comentarios de funcionarios policiales, fue mencionada la oportunidad de la intervención policial proactiva para detener la comisión de un fraude mediante tarjetas de crédito, así como en otro se destacó la aplicación de técnicas policiales, independientemente de los bancos afectados, para el rastreo y la investigación de los fraudes. En todo caso, los funcionarios policiales reconocen la primacía de la intervención de las entidades bancarias, mediante comentarios relacionados con la participación policial luego que han sido violados los sistemas de seguridad, sin que ello excluya las alertas a los bancos, por parte de la propia policía, una vez adelantado el proceso de la investigación policial. La colaboración descrita por los representantes bancarios incluye mecanismos de instrucción e inducción a las autoridades policiales sobre modalidades y novedades tecnológicas, llegando a describir, uno de los representantes bancarios, esta perspectiva como "una nueva filosofía en la aproximación al sistema de justicia penal".

Los fiscales del Ministerio Público son reconocidos como quienes llevan la responsabilidad legal de la investigación y quienes están facultados para solicitar evidencias con valor probatorio, aunque en varios comentarios, de funcionarios bancarios y policiales, se sugiere que no comprenden bien lo que se pretende castigar y que requieren mayor formación. Uno de los funcionarios policiales comentó:

> ...tenemos que mantener comunicación directa con los fiscales del Ministerio Público, ponerlos en conocimiento a ellos del modus operandi, tenemos que instruirlos en esta materia ya que tenemos muchísimo desconocimiento de ella... tenemos que unirnos por completo para poder llegar a un juicio bien basado, en manos de todos, porque si ellos (los bancos) hacen, nosotros hacemos y la Fiscalía no tiene conocimiento de ello a la hora de un juicio, todo se cae y no sirve absolutamente de nada... porque mientras ellos (los fiscales) no lo sepan exponer en una sala de juicio, podrá haber un expediente muy bien sustanciado pero no va a haber enjuiciado porque ellos no tienen el conocimiento, y nosotros, mientras más nos desarrollemos en esto y podamos ayudarlos, podemos avanzar en que no exista más impunidad.

Vinculado con ello está el tema de la información relevante y la comprensión de los mecanismos del fraude por parte de los fiscales. Un representante bancario sostuvo la conveniencia de que la institución financiera instruya a los fiscales sobre el ciclo de la defraudación, mencionando una experiencia positiva directa con una representante del Ministerio Público, así como el seguimiento de las actuaciones de los fiscales mediante abogados internos especializados y la necesidad de que las pruebas e informes suministrados sean "amigables", es decir, comprensibles tanto para los fiscales como para los jueces.

Un tema importante de la discusión fue el de la selectividad bancaria para denunciar los casos a la policía y las alternativas a la persecución penal, con lo cual se abre el tema del control informal de los fraudes. Parece haber varios factores que inciden en la disposición a denunciar. Uno de ellos es la aparición de una nueva modalidad delictiva, según mencionaron dos representantes bancarios y un funcionario policial. Otro es la identificación de un nuevo grupo criminal o de formas de delincuencia organizada según indicaron dos representantes bancarios y un funcionario policial. La magnitud o extensión del fraude fue

indicada como otro factor por un representante policial y la exigencia legal de la denuncia para el pago de la suma asegurada por un representante bancario. La relevancia social del particular defraudado fue señalada por dos funcionarios policiales como una variable que predice la activación policial en la apertura y seguimiento de las investigaciones, con lo cual surge la cuestión sobre quién es la auténtica víctima de estos hechos, si el particular titular de la cuenta indebidamente cargada o el banco al cual pertenece la cuenta afectada. Esta cuestión tiene implicaciones para las decisiones sobre los acuerdos reparatorios previstos en el Código Orgánico Procesal Penal como una alternativa a la persecución penal.

A través de la conversación surgió la cuestión de las alternativas a la persecución penal, o control informal. Dos representantes bancarios mencionaron la posibilidad de retener a infractores para obtener información complementaria sobre el hecho fraudulento, sin denunciar el hecho a la policía, y otros tres admitieron que la amenaza de la detención provisional, que realizaba la policía de conformidad con el régimen procesal anterior, constituía una forma efectiva para obtener información y (o) restitución por parte de los defraudadores identificados. Estas posibilidades operaban con buen efecto intimidativo sin tener que afrontar la incertidumbre de un proceso penal, que, en general, tiende a ser percibido como favorecedor de la impunidad.

Por lo que se refiere a los fiscales del Ministerio Público, los comentarios registrados en la cuarta sesión de discusión tienen que ver con tres temas fundamentales: a) los recursos técnicos y la asesoría para adelantar la investigación penal (cuestiones sustantivas sobre la materialidad del delito); b) los aspectos procesales vinculados a la incorporación de las evidencias y su valor probatorio; c) el conflicto de intereses y de objetivos entre el sistema penal y el sistema bancario.

La cuestión de los recursos técnicos y la asesoría fue mencionada ocho veces por los cinco fiscales participantes en el cuarto grupo de discusión. Se manifestó que el procesamiento de estos delitos requiere preparación técnica y recursos humanos de los cuales no se dispone, que la banca debe "acompañar" a los fiscales en la investigación interna, que se carece de la suficiente especialización en materia de fraudes y estafas, que en alguna oportunidad un banco obstaculizó una investigación de la Fiscalía, que la policía cuenta con mayor preparación que los fiscales, por lo cual debe marcharse juntos en el proceso de investigación, que el trabajo en equipo es fundamental y que hay un plan del Ministerio Público para especializar algunos despachos en esta materia.

Por lo que se refiere a los aspectos sobre incorporación de la prueba al proceso penal, se mencionó que la eficiencia policial, por sí misma, no es garantía del éxito por las cuestiones de la legalidad procesal y el debido proceso, que la evidencia en esta materia debe hacerse tangible y comprensible para quienes deciden en los juicios, incluyendo los escabinos, así como se habló de las dificultades para establecer la autoría material en la delincuencia informática, los problemas derivados de la inspección, registro y preservación de trazas en las unidades de procesamiento central de los computadores y la necesidad de documentar la secuencia de los fraudes a los efectos probatorios.

Por lo que toca a los conflictos de intereses entre sistema de justicia penal y sistema bancario, se indicó la contraposición entre castigo e indemnización como objetivos en conflicto, los problemas derivados de delitos que, siendo de acción pública, permiten poco espacio de maniobra, una vez que son conocidos, la conveniencia de mantener archivos sobre empleados para, mediante un control de antecedentes, mejorar la posición de negociación de acuerdos reparatorios (aunque un fiscal manifestó que el objetivo de la Fiscalía sería llegar a cualquier acto conclusivo del proceso, descartando los acuerdos reparatorios), la falta de políticas a nivel de la Fiscalía sobre el valor de la delación y el arrepentimiento como casos del principio de oportunidad en esta materia, incluyendo la dificultad de incentivos cuando el monto de la ganancia ilícita es grande y puede ser mantenido bajo resguardo, así como la necesidad

de satisfacer las expectativas de los bancos, como víctimas, dentro del proceso penal. Estos comentarios reflejan la tensión entre los fines de indemnización e intimidación en la percepción de las funciones del control social formal.

Uno de los fiscales resume su percepción sobre las principales fallas en la persecución penal de estos delitos mediante el siguiente comentario:

> ...de la experiencia que tengo en esto veo que en la gran mayoría de estos casos... nosotros procuramos que algunos puedan salir de manera selectiva; pero no avanzan en cuanto a las medidas y entonces intervienen tres cosas ahí: una es la carencia de recursos para la intervención. Es recurso humano o tecnológico. El segundo asunto, falta de proactividad en la investigación... proactividad de la Fiscalía y proactividad del órgano judicial, porque no ve por dónde entrar en el asunto, porque es un problema también de falta de conocimientos técnicos. Y el tercer elemento que veo es que no hay credibilidad de que ese proceso investigativo le vaya a traer una reflexión satisfactoria a la víctima... en el caso de las organizaciones mercantiles, que es lo más importante, porque tal vez no le interesa que metan preso a Pedro Pablo, sino que le resarza y le devuelva el daño que le causó y se lo reponga.

De los anteriores comentarios se desprende que, independientemente de los mecanismos alternativos al sistema penal, los representantes del Ministerio Público coinciden en las dificultades que representa esta novedosa forma de criminalidad para las instancias del control social formal, tanto por la tecnología que implica su comisión y persecución como por la necesidad de familiarizarse con algo que, como la evidencia material de estos fraudes, es percibida por los operadores del sistema de justicia y por los ciudadanos como intangible y difícil de documentar.

¿QUÉ HAY DE IDIOSINCRÁTICO EN EL FRAUDE DENTRO DE LA GLOBALIZACIÓN?

En su discusión sobre la economía criminal global, Castells (2001c, p.238-243) sugiere el desarrollo de una extensión mundial de redes criminales que, a su vez, contarían con identidades culturales ancladas en sus sitios de origen, y que les permitirían adaptarse a cambios en los patrones de persecución a nivel internacional. Aunque ese tema está planteado para las formas de delincuencia organizada mejor descritas, como el tráfico de drogas, armas, personas y materiales radioactivos, podría pensarse en una tendencia equivalente para otras formas de criminalidad, como los fraudes. Pero ¿qué de particularmente cultural e idiosincrático tiene el fraude electrónico, o cuál es el impacto de la localidad en sus manifestaciones? En su ensayo sobre el fraude telemático, Stangeland (2004) sugiere un desarrollo futuro estratificado de las transacciones con tecnologías de la información: un nivel estará representado por el comercio e intercambio seguros, con protocolos y claves estandarizados, supervisados y reforzados, con primas por el acceso, y otro nivel inseguro y devaluado, sin supervisión, con intercambio azaroso y de libre acceso. Ambos niveles diferenciarán a los pudientes de los no pudientes en la era informática, una distinción que hasta ahora es algo borrosa. Esto podría equivaler a la distinción entre la economía formal e informal, o entre ricos y pobres, o entre urbanizaciones y barrios en una ciudad. ¿Cómo se manifestará el fraude entre estos dos mundos y qué espacio quedará para lo regional y lo local? Si los patrones de desarrollo planetario persisten y si la transferencia de bienes y servicios se generaliza mediante medios de pago electrónicos, habrá mucho que aprender de la diversidad y la estratificación, en cuanto a vulnerabilidad, modalidades, racionalizaciones y controles sobre los sistemas informáticos. Así como geográficamente han existido, y aún las hay, zonas más seguras y más peligrosas para el desplazamiento terrestre o marítimo, podrán desarrollarse, a nivel virtual, tales áreas diferenciadas, dependiendo de autocontrol o de controles externos, como sucede con la criminalidad en general. El espacio para estudiar la diversidad y la riqueza de la desviación podría expandirse, antes de contraerse debido a la estandarización. Nuevas identidades podrían manifestarse. El campo de la investigación comparada, en términos de motivaciones delictivas, habilidades, adhesión normativa y vulnerabilidad de

sistemas luce prometedor en un área donde el control anticipado de las contingencias toma abierta primacía sobre la corrección y enmienda de los errores.

(Recebido para publicação em maio 2006)
(Aceito em agosto de 2006)

REFERÊNCIAS

BIRKBECK, Christopher. El concepto de oportunidades para el delito: su definición y consecuencias, *Revista Cenipec, 9*, Mérida, p. 43-81, 1984/1985.

_____; LAFREE, Gary. Una revisión crítica de las teorías de las oportunidades para el delito", *Revista Cenipec, 12*, Mérida, p. 11-34, 1989.

BLOCK, Alan A.; CHAMBLISS, William J. *Organizing crime*. New York: Elsevier. 1981.

CASTELLS, Manuel. *La era de la información:* la sociedad red. Madrid: Alianza Editorial, 2001a. v. 1

_____. *La era de la información:* el poder de la identidad. Madrid: Alianza Editorial. 2001b. v. 2.

_____. *La era de la información*: fin de milenio. Madrid. Alianza Editorial, 2001c. v. 3.

CERF, Vinton G. Ás extraño que la verdad o la ficción: fraude, engaño e internet. En: TAPSCOTT Don; LOWY Alex; TICOLL, David (Eds.). *La era de los negocios electrónicos.* Bogotá: Mc Graw Hill, 2000. p. 371-383.

DELITOS informáticos.com. Boletín Informativo n.6, 8 jul. 2002a en <http://delitosinformaticos.com/noticias/10256857468084.shtml>

_____. Boletín Informativo n.4, 26 jan. 2002b en <http://delitosinformaticos.com/estafas/fraudes-FTC2002.shtml>

_____. Novedades y noticias 26 nov. 2002c en <http://delitosinformaticos/proteccion datos/103830785417388.shtml>

GABALDÓN, Luis Gerardo. *Control social y criminología*. Caracas: Editorial Jurídica Venezolana, 1987.

GAROFALO, Rafael. *La criminologie*. Paris: Alcan, 1888.

GOTTFREDSON, Michael R.; HIRSCHI, Travis. *A general theory of crime*. Standford: Standford University Press, 1990.

GRABOSKY, Peter; SMITH, Russell. Telecommunicaton fraud in the digital age. En WALL David S. (Ed.) *Crime and the internet.* Londres: Routledge, 2001.p. 29-43.

GRANELL, Elena; GARAWAY, David; MALPICA, Claudia. *Éxito gerencial y cultura*: retos y oportunidades en Venezuela. Caracas: Ediciones Iesa, 1997.

GREEN, Gary S. *Occupational crime*. Chicago: Nelson Hall, 1990.

HERNÁNDEZ BASUALTO, Héctor. Límites del tipo objetivo de lavado de dinero. En: GABALDÓN, Luis Gerardo (Ed.). *Delincuencia económica y tecnologías de la información*. Caracas: Universidad Católica Andrés Bello, 2004. p. 77-105.

HIRSCHI, Travis. Una teoría de la delincuencia, *Capítulo Criminológico*, v. 31, n. 4, p. 5-31oct,/dic., 2003.

HODGE, B.J.; ANTHONY, W.P.; GALES, L.M. *Teoría de la organización*. Madrid: Prentice Hall, 1998.

IESA. La brecha informática en Negocio Electrónico, *Debates Iesa*, v. 4, p. 31, 2000.

KINDHÄUSER, Urs. La estafa mediante computadoras en el Código Penal alemán (art. 263 A, Stgb). En: PUIG, S. Mir J.L. *et al. Estudios de derecho penal económico*. Caracas: Livrosca, 2002. p. 649-674.

KRIPPENDORFF, Klaus *Metodología de análisis de contenido*. Barcelona: Piados, 1990.

LARA PEINADO, Federico *Código de Hammurabí* (Estudio preliminar, traducción y comentarios). Madrid: Tecnos, 1986.

LEVI, Michael. La organización y regulación comercial del pago fraudulento con tarjetas de crédito. En: GABALDÓN, Luis Gerardo (Ed.). *Delincuencia económica y tecnologías de la información*. Caracas: Universidad Católica Andrés Bello, 2004. p. 41-61.

_____. Between the risk and the reality falls the shadow. En: WALL, David S. (Ed.). *Crime and the Internet.* Londres: Routledge, 2001. p. 44-58.

LEY especial contra delitos informáticos. Gaceta Oficial de la República Bolivariana de Venezuela, Caracas, n. 37.313, 30 oct. 2001b.

MANNING, Peter K. Lealtad de los empleados en la era de la información: observaciones sobre las relaciones entre lealtad y organización. En: GABALDÓN, Luis Gerardo (Ed.). *Delincuencia económica y tecnologías de la información*. Caracas: Universidad Católica Andrés Bello, 2004. p. 15-40.

MCKNIGHT, Lee W. Internet business models: creative destruction as usual. En: _____; VAALER, Paul M.; KATZ, Raul L. (Ed.). *Creative Destruction:* business survival strategies in the global internet economy, Cambridge: MIT Press, 2001. p. 39-59.

MEDINA, Elvira. *Uno de cada tres usuarios de la Red ha sufrido algún ataque informático*, en Diario en la web, 23 nov. 2003 en <http://www.diariomalaga.com/noticias/articulo.php.id=25520>

MOMMSEN, Theodor. *Derecho penal romano*. Bogotá. Temis, 1976.

MORGAN, David L. *Focus Groups as Qualitative Research*. Thousand Oaks: Sage, 1997.

STANGELAND, Per. El fraude telemático: proposiciones para su explicación y control. En: GABALDÓN, Luis Gerardo (Ed.). *Delincuencia económica y tecnologías de la infrmación*. Caracas: Universidad Católica Andrés Bello, 2004. p. 63-76.

SUTHERLAND, Edwin H. Differential association. En: PONTELL Henry N. (Ed.). *Social Deviance:* readings in theory and research. New Jersey, Prentice Hall, 1996.

WALL, David. S. Cybercrimes and the Internet. En: WALL, David. S. (Ed.). *Crime and the Internet*. Londres: Routledge, 2001, p. 1-17.