

Capítulo VI

LA USURPACIÓN O SUPLANTACIÓN DE IDENTIDAD: UNA APROXIMACIÓN CONCEPTUAL Y LOS POSIBLES ELEMENTOS CONSTITUTIVOS DEL TIPO PENAL

Rodolfo Romero Flores¹

Julio Téllez Valdes²

SUMARIO:

1. La usurpación o suplantación de identidad: una aproximación conceptual. 2. ¿Una conducta ilícita de carácter continuo? 3. Los posibles elementos constitutivos del tipo penal. 4. Los sujetos activos del tipo penal. 5. Los bienes jurídicos tutelados. 6. Las disposiciones penales en el ámbito local mexicano sobre la suplantación de identidad. 7. Las iniciativas sobre usurpación de identidad en la legislación penal federal en México. 8. Las acciones institucionales del Gobierno mexicano en

¹ Maestro en Derecho con mención honorífica por la Universidad Nacional Autónoma de México. Profesor de Informática Jurídica en la Facultad de Derecho de dicha Universidad y en el Instituto Internacional del Derecho y del Estado. Coautor del libro "Voto electrónico, derecho y otras implicaciones," editado por el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. Miembro de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI).

^{**} Doctor en Informática Jurídica y Derecho de la Informática por la Universidad de Montpellier, Francia. Investigador de tiempo completo del Instituto de Investigaciones Jurídicas de la UNAM. Miembro del Sistema Nacional de Investigadores SNI II, CONACYT. Profesor del Instituto Tecnológico de Monterrey y del Posgrado en Derecho de la UNAM, BUAP y otras.

² Doctor en Informática Jurídica y Derecho de la Informática por la Universidad de Montpellier, Francia. Investigador de tiempo completo del Instituto de Investigaciones Jurídicas de la UNAM. Miembro del Sistema Nacional de Investigadores SNI II, CONACYT. Profesor del Instituto Tecnológico de Monterrey y del Posgrado en Derecho de la UNAM, BUAP y otras.

torno a esta problemática. **9.** Las acciones de organismos internacionales en materia de robo o usurpación de identidad. **10.** La legislación federal norteamericana sobre suplantación de identidad y las ID-Theft State Law. **11.** La usurpación de identidad a través de certificados digitales. **12.** Una propuesta de acción legislativa para un tratamiento jurídico-penal en torno a la usurpación de identidad.

1. LA USURPACIÓN O SUPLANTACIÓN DE IDENTIDAD: UNA APROXIMACIÓN CONCEPTUAL

Recordemos que la identidad surgió como un creciente interés por la individualización del ser humano en la sociedad de masas. Ahora bien, desde el punto de vista del Derecho, la identidad hace referencia a un conjunto de características, datos o informaciones que permiten individualizar o referenciar a una persona³ de manera precisa u objetiva. Este conjunto de atributos de cada una de las singulares personas permiten el desarrollo de las relaciones sociales y de los efectos jurídicos que las mismas pudieran producir, mismos que se traducen en una serie de cualidades atributivo-informacionales inherentes a una persona en lo específico que permite su reconocimiento y capacidad para habilitarse en lo social.

En consecuencia, la atribución de una identidad permite establecer las posibles consecuencias de una conducta para su autor. La imputación de un hecho o conducta a una o varias personas determinadas mediante su identidad es el presupuesto necesario para que hacia ella o ellas se dirijan los efectos que pudieran derivarse, es decir, la identidad en el ámbito jurídico tiene una significación fundamentalmente vinculativa, relacional y atributiva.

Podríamos señalar de forma objetiva que la identidad de una persona se integra a partir de una especie de "*Status Iuris Singulare*"; es decir, se crea un estado a partir de una ficción jurídica que aísla o separa a un individuo como centro de imputación jurídica a partir de determinada información vinculante y que con base en referido *Status*, sus acciones desplegadas lo establecen como responsable directo, aislado o separado del acto jurídico producido.

Más aún, en la actualidad Internet ha propiciado el surgimiento de la identidad electrónica, identidad digital o identidad virtual, que fundamentalmente está constituida por datos personales sensibles que pueden incluir claves de acceso a cuentas bancarias o redes, mediante los cuales las personas se comunican u operan en redes informáticas o telemáticas y cuya circulación transfronteriza es potencialmente peligrosa ante su posi-

3 De Salvador, Carrasco Luis. *Casos de suplantación de identidad detectados en denuncias tramitadas por la Agencia Española de Protección de Datos*, citado por Mata y Martín, Ricardo en *El robo de identidad: ¿una figura necesaria?* Ed. Arazandi-Thomson Reuters-Agencia Española de Protección de Datos-Universidad de Castilla-La Mancha. Pamplona. 2010. p.200.

ble apropiamiento no autorizado. De igual forma, la identidad puede asumir distintas vertientes tales como: la identidad genética o biológica, la identidad sexual, la identidad cultural, entre otras. En palabras del académico Fabián Zambrano Viedma, *la identidad virtual la constituye el conjunto de de datos de identificación telemática sustentados sobre la propia identidad oficial informatizada*.⁴ En este orden de ideas, el profesor José Antonio del Cerró define a la identidad digital como toda *aquella información de un individuo para un uso no presencial en medios telemáticos*.⁵

En los últimos años en el plano nacional e internacional, se han multiplicado los sucesos⁶ en los que, especialmente por medios informáticos o telemáticos, se obtienen fraudulentamente datos personales para luego llevar a cabo ciertos hechos u operaciones con tales datos, fundamentalmente en el ámbito económico, imputándose falsamente a los verdaderos titulares de los datos. Es lo que se conoce como "robo o usurpación de identidad, considerado en ocasiones como el crimen por excelencia del Siglo XXI".⁷

Es importante destacar que la mayoría de los organismos internacionales que han abordado el tema del hurto o suplantación de identidad, difícilmente han establecido un concepto en torno al mismo. Según la definición aportada por *Home Office Identity Fraud Steering Committee* del Reino Unido,⁸ *el hurto de identidad consiste en la recogida de información relativa a la identidad de una persona con el fin de obtener un fraude identitario, prescindiendo del hecho de que la víctima sea una persona viva o fallecida*.⁹ El robo de identidad consistiría por tanto en la apropiación indebida de la identidad o de cualesquiera otros datos personales (v.gr; fecha de nacimiento, domicilio, claves bancarias, contraseñas de acceso a redes, certificados digitales, etcétera). Sin embargo; referidas definiciones omiten el aspecto relacionado al apropiamiento no autorizado de datos

4 Agencia Española de Protección Datos- Societe Internationale de Defense Sociale Pour une Politique Criminelle Humaniste. *Robo de identidad y protección de datos*. Ed.Arazandi-Thomson Reuters-Agencia Española de Protección de Datos-Universidad de Castilla-La Mancha. Pamplona. 2010. p.244.

5 *Ibidem*.

6 Mata y Martín, Ricardo. *El robo de identidad: ¿una figura necesaria?* en *robo de identidad y protección de datos*. Ed.Arazandi-Thomson Reuters-Agencia Española de Protección de Datos-Universidad de Castilla-La Mancha. Pamplona. 2010. p. 200.

7 Disponible en http://www.priv.gc.ca/id/primer_f.cfm, consultada en octubre 10 de 2010.

8 Disponible en <http://www.identitytheft.org.uk>, consultada en octubre 10 de 2010.

9 *Ibidem*

personales con el objeto de cometer otros delitos, situación que también debiere tener un oportuno marco jurídico en el plano penal.

Al respecto, la suplantación de identidad obliga a acciones legislativas que permitan establecer normativamente una serie de conductas típicas, antijurídicas y sancionables en las legislaciones sustantivas penales; en virtud de que con los instrumentos jurídico-penales vigentes en la mayor parte de los países incluyendo a México, no es factible abordar un tratamiento jurídico-penal de las conductas vinculadas a la suplantación de identidad y por ende, no existe seguridad jurídica.

Ahora bien, ante esta problemática creciente, resulta obligado establecer un marco legislativo *ad hoc*, frente al uso de Internet como medio común creciente utilizado por la ciudadanía para realizar compras y el pago de impuestos y servicios locales, en transacciones donde se puede ver comprometida su identidad. En este orden ideas, el tratamiento jurídico-penal de la identidad mediante una base legislativa adecuada en la materia, tendría como efecto inmediato la implementación de mecanismos de cooperación a nivel internacional sobre este creciente problema, incluyendo la homologación de las legislaciones nacionales sobre esta problemática.

En efecto, el también denominado "robo de identidad", "usurpación de identidad", "suplantación de identidad", "falsificación de la identidad y su uso indebido"; de acuerdo con investigaciones internacionales realizadas por el Consejo Económico y Social (ECOSOC) de la Organización de las Naciones Unidas, la Unión Europea y la Organización para la Cooperación y el Desarrollo Económicos (OCDE), es el delito de más rápido crecimiento en el mundo sin que existan acciones legislativas concretas y políticas públicas acertadas para sancionar esta conducta atípica en el plano penal.

Para la OCDE, el denominado robo de identidad constituye una actividad ilícita con múltiples facetas que generalmente incluye una larga cadena de acciones criminales complejas y que en cada país tiene una categorización o estatus legal distinto. Sin embargo, para esta organización el *ID Theft* o robo de identidad *"ocurre cuando se transfiere, adquiere, posee o se utiliza información personal de una persona natural o legal de manera no autorizada con el intento de cometer o generar un fraude u otros crímenes"*.¹⁰

¹⁰ Organisation for Economic Co-operation and Development (OECD). *Online Identity Theft*. Ed. OECD, 2009. p. 16.

En este orden de ideas, la evolución de los delitos relacionados con la aplicación de las nuevas Tecnologías de la Información y Comunicación (TIC), se orientan en la actualidad a sistematizar normativamente atentados contra los datos personales y la eventual invasión de la intimidad por medios informáticos.

Es innegable que una nueva forma de entender la intimidad, resulta equiparable a la capacidad de disposición sobre las bases de datos automatizadas o convencionales que contienen información respecto de nuestras identidades. Sin embargo, objetivamente la ampliación punitiva en materia informática en la mayor parte de las legislaciones, se limita a castigar el simple acceso a las bases de datos personales, sea cual fuere su contenido, no obstante, se está omitiendo la punibilidad a la "capacidad de disposición sobre dichas bases de datos o información que no solamente generan una efectiva lesión sobre nuestra intimidad, sino que adicionalmente su apoderamiento podría producir la usurpación o suplantación de nuestra identidad con todo y sus catastróficos efectos inherentes.

Es cierto que en la actualidad resulta muy importante en el contexto legislativo, la criminalización del acceso a los datos personales informatizados cuando se realiza de manera no autorizada, pero resulta trascendental también, criminalizar cuando se afecta la facultad de disposición o de ejercer la titularidad de nuestra información personal, es decir, del poder de controlar la información sobre uno mismo, lo cual resulta aún más grave.¹¹

En este contexto, el binomio tecnología-usurpación de identidad demuestra que la utilización cada vez más extendida de dispositivos tecnológicos de telecomunicación genera la ausencia o presencia directa de las personas que puede ser aprovechada para suplantar la identidad. En este sentido, se cuenta actualmente con un manejo suficiente de los instrumentos tecnológicos que presentan mayores oportunidades de fraude, es decir, a mayores posibilidades técnicas y distancia entre los sujetos, se da lugar en muchos de los casos a una falta de control de la identidad.

Razón por la que ante esta novedad tecnológica-delincuencial y la incertidumbre que se genera en torno a su tratamiento jurídico-penal, cabe plantear la relevancia penal de estas conductas, y en su caso determinar legislativamente los hechos punibles vinculados al robo o usurpación de identidad. Es cierto también que por sí sola, la acción legislativa cuyo efecto sería de tipo correctivo-punitivo tendría que acompañarse de políticas públicas de carácter preventivo dirigidas también a corresponsabilizar y advertir a la ciudadanía sobre el problema que enfrentamos.

11 *Ibidem.*

En esta primera parte, una aproximación conceptual de esta creciente actividad ilícita la podríamos conceptualizar jurídicamente como “el despliegue de conductas u omisiones dirigidas al apoderamiento, utilización, disposición o cesión de cualquier tipo de datos personales, informaciones o documentos sin la autorización de quien o quienes legítimamente les pertenezcan; mismos que les permiten individualizarlos en un contexto social y que le permite a una persona física o jurídica ser identificada o identificable, cuya finalidad estriba en hacerse pasar por el titular de dichos datos personales”.

Ahora bien, esta primera aproximación conceptual no inhibe de formular algunas conductas equiparables que deberían tener una sanción penal; por ejemplo: a quienes cedan o vendan datos personales, sin consentimiento de quien deba autorizarlo; otorguen el consentimiento para llevar a cabo la usurpación de su identidad; y en todo caso a quienes se valgan de la homonimia para cometer algún ilícito.

2. ¿UNA CONDUCTA ILÍCITA DE CARÁCTER CONTINUO?

- a) *Modalidades de tipos penales como consecuencia de la acción ilícita primigenia.*

La conducta ilícita primigenia de robo o suplantación de identidad podríamos señalar que tendría efectos de tracto sucesivo o continuados —explícitamente efectos derivados— para la comisión de nuevos tipos penales tales como los delitos económicos vinculados a la informática, por ejemplo: estafa informática, espionaje industrial, sabotaje informático, apropiación de servicios, acceso no autorizado a los sistemas informáticos (hacking informático) e inclusive el fraude fiscal informático.¹² Sin embargo, la conducta inicial también podría derivarse hacia delitos cometidos en contra de menores de edad, particularmente en cuestiones de pornografía infantil, incluso de delitos como la violación derivados de la suplantación de identidad.¹³ Merece especial atención reflexionar en torno a si el tipo penal de robo de identidad, constituiría un posible concurso real o material de delitos, cuando la mayoría de la veces representan varias conductas que producen una pluralidad de resultados. También que como operadores jurídicos tendríamos que reflexionar que conductas tan complejas

12 Gutiérrez Francés M. *Notas sobre la delincuencia informática: atentados contra la información como valor económico de la empresa en: Mazuelos Coello, J. (comp.). Derecho penal económico y de la empresa.* Ed. San Marcos, Lima, 1997. p.60.

13 No resulta un tema menor, la suplantación de identidad en el plano estrictamente comercial, cuando precisamente a través de las redes sociales, es algo cotidiano, la utilización de identidades con el objeto de denigrar o calumniar a algunas empresas con fines estrictamente de competencia desleal a través de los agentes comerciales autorizados pero no reconocidos públicamente a quienes se les denomina como embajadores.

propiciarán en un momento dado, un conflicto de leyes o de concurrencia de normas aplicables entre sí, mismas que derivarían en la aplicación de los principios de especialidad y subsidiaridad en materia penal.

La idea central sobre la posible tipología de este tipo penal es clasificarlos como delitos de carácter continuo o permanente; esto es, la conducta ilícita sigue teniendo efectos de tracto sucesivo, consumándose a cada momento. En realidad, la apropiación de datos personales con fines de fraudes identitarios, la propia actividad de apoderamiento no autorizado de información personal, cuando se ceden e inclusive se venden, el uso a cada momento de la información personal que determina la identidad de un sujeto constituye en sí la realización permanente del delito. Brevemente, siempre que se siga detentando o utilizando la información personal no autorizada se sigue cometiendo el delito.

Recapitulando sobre el concurso real de delitos en torno a la suplantación de identidad, señalaríamos que pueden existir o concurrir varias acciones o diversos hechos autónomos que derivarían en una serie de delitos independientes, cuyo punto de partida es la usurpación o suplantación de identidad y que con posterioridad puede derivar en fraudes comerciales o financieros. En este sentido, continuando con la postura de algunos *ius penalistas* sobre las clases de concurso real de delitos, en la suplantación de identidad podríamos señalarle como de tipo heterogéneo, en la que el autor realizare distintos tipos penales en diversas oportunidades. No obstante, de ahí su complejidad como tipo penal no necesariamente un solo sujeto activo despliega la totalidad de las conductas en diversas oportunidades; ya que suele suceder que un sujeto activo se apropia de la información personal de manera no autorizada quien a su vez la cede ilícitamente a otro sujeto y tal vez, alguien más asuma la identidad; siendo este último un sujeto activo completamente distinto a quien despliega la conducta ilícita primigenia.

3. LOS POSIBLES ELEMENTOS CONSTITUTIVOS DEL TIPO PENAL

Es un hecho que incorporar en la legislación sustantiva penal, una serie de conductas vinculadas a la suplantación de identidad requeriría distinguir en el tipo penal al menos tres elementos básicos, mismos que tendrían interés o incidencia en la calificación jurídica-penal de los mismos hechos. Estos posibles elementos del tipo penal serían: la apropiación de datos personales por medios convencionales o informáticos (inclusive telemáticos); y un segundo elemento, la transferencia o cesión de los datos personales; y un tercer elemento, su posterior utilización o facultad arrogada de manera indebida para su utilización sobre dichos datos personales.

- a) El primer elemento, supondría la realización de cierta actividad por medios convencionales o informáticos con un carácter externo en el sujeto activo del delito cuyo objeto se enfocaría al apropiamiento indebido o ilícito de datos personales en soportes lógicos o materiales. En este orden de ideas, surge una primera cuestión; el apropiamiento de soportes lógicos que son elementos intangibles que si bien es cierto pueden tener un soporte material, lo cual es motivo de discusión en torno al apropiamiento de datos de carácter personal que en la actualidad se encuentran casi en su mayoría en bases de datos automatizadas y que tienen un carácter incorpóreo. Sin embargo, algo que matiza a las operaciones fraudulentas es también la usurpación de bienes incorpóreos, v.gr; los derechos patrimoniales ajenos.

Cabe citar que el apropiamiento no autorizado de datos adquiere un carácter telemático, cuando a través de redes digitales públicas o privadas de forma remota existe la posibilidad de que se adquieran mediante *cracking* referidos datos. Más aun, en el lenguaje técnico penal, la palabra "apoderamiento", tiene un significado jurídico especial, particularmente en tipos penales como el robo y el rapto. En el robo, el apoderamiento consiste en no sólo hacerse de la cosa, sino en realizarlo sin derecho y sin consentimiento de la persona que pueda disponer de ella con arreglo a la Ley.¹⁴ En síntesis, siguiendo al *ius penalista* mexicano Francisco González de la Vega, el apropiamiento implicaría la aprehensión de las cosas en ausencia de todo consentimiento del sujeto pasivo.

Ahora bien, la aprehensión de los datos personales por medios convencionales o telemáticos estaría fundamentalmente encaminada también a obtener un lucro indebido, es decir, un posible ilícito-beneficio para el sujeto activo mediante el cual obtiene ganancias de índole económicas, en detrimento del patrimonio de la víctima cuando la utilización de los datos personales derivan en una serie de modalidades delictivas, mismas que en ulteriores párrafos señalaremos.

Es importante señalar que el apropiamiento de datos personales constituye en esencia; una conducta de acción del sujeto(s) activo(s), no obstante, también podría constituir una conducta de omisión respecto a los titulares de ficheros que ante una negligencia o desatención de su responsabilidad de resguardar información de carácter personal puedan comprometerla en cuanto a su seguridad jurídica, técnica u organizacional.

¹⁴ González de la Vega, Francisco, *Derecho penal mexicano, los delitos*. Vigésima segunda edición. México, Editorial Porrúa, 1988.p.251.

- b) El *segundo elemento*, lo podría constituir la transferencia o cesión de datos personales obtenidos de manera ilícita. Específicamente este posible elemento implicaría una relación de causalidad con el primer elemento, cuando el sujeto activo se apropia de datos personales en soportes lógicos o materiales cuya intención radica en transferir o ceder los datos obtenidos mediante una retribución o compensación económica que también tendría un carácter indebido. En este contexto, es un hecho innegable que la mayor parte de las veces, los datos personales obtenidos ilícitamente acaban en manos de terceros o grupos de delincuencia organizada que precisamente tienen como origen en la realización de sus acciones ilegales; la comercialización previa de grandes bases de datos automatizadas de personas físicas o colectivas.
- c) El *tercer elemento*, es una condición *sine qua non* para determinar si nos encontramos frente al tipo penal de robo o usurpación de identidad o en alguna modalidad de delitos penales, consecuencia de la acción ilegítima primigenia. Este elemento consistiría en la facultad arrogada de manera ilícita para utilizar los datos personales con fines de suplantación de identidad, es decir, las calidades atributivas y relacionales con el ente de imputación jurídica, son derivadas a un nuevo ente para producir actos o consecuencias legales para ser atribuidas al ente jurídico original sobre del cual se obtuvieron datos personales.

4. LOS SUJETOS ACTIVOS DEL TIPO DE PENAL

Se refiere que el sujeto activo constituye la persona física que comete la conducta típica, antijurídica y culpable, no obstante, en la teoría penal, se asume que las personas jurídicas o colectivas nunca podrían tener el carácter de sujetos activos del delito, toda vez que siempre la persona física que pertenece al ente colectivo, se constituyó en el autor material o intelectual del delito, esto es, la persona física materializó o planeó el delito y los efectos jurídicos son imputables no a la persona moral sino al ente físico. En nuestra perspectiva, resulta cuestionable que en materia de robo o suplantación de identidad, las consecuencias penales recaigan solo en los operadores del delito, cuando actualmente existen un cúmulo importante de empresas a nivel mundial que lo que comercializan exclusivamente son bases automatizadas de datos personales; incluso muchas de ellas no solo alientan, sino que propician mediante sus políticas comerciales,¹⁵ la adquisición por medios ilícitos de información personal o existen simulaciones en cuanto a su adquisición por medios legales. En razón de lo anterior, ¿los responsables del Consejo de Administración de una

15 Recordemos el Programa Safe Harbor en Europa respecto de la protección de datos personales de ciudadanos europeos en posesión de empresas norteamericanas.

persona jurídica de una forma solidaria y subsidiaria que propician el apropiamiento ilícito de datos personales tendrían algún grado de responsabilidad penal? A nuestro juicio, sí, por lo que sancionar a la totalidad de miembros representativos y ejecutivos de una persona jurídica implicaría asignarle un grado de responsabilidad penal.

Podríamos señalar inicialmente que los sujetos activos que actualizan la posible hipótesis penal de suplantación de identidad, poseen importantes conocimientos en materia informática o bien, como señala el tratadista Luis Azaola Calderón, ocupan un lugar estratégico en los centros de trabajo. No obstante, la pericia informática no constituye tampoco una condición *sine qua non* respecto del agente delictivo. Es también, un tipo penal realizado por sujetos activos que no necesariamente tienen formación respecto de la aplicación de las nuevas Tecnologías de la Información y Comunicación y que más bien constituyen delincuentes del orden común con un nivel de especialización criminal que se orienta a la comisión de fraudes.¹⁶

Es importante mencionar que uno de los posibles sujetos activos que realizan este tipo de conductas ilícitas serían precisamente con la intención de apropiarse de datos para obtener un beneficio económico. Cabe señalar que distintas y sofisticadas técnicas son empleadas por los *crackers* para obtener información de carácter personal, tales como: el *pharming*, el *vishing*, el *phishing*, el *dumpster diving* y el *smishing*; destacando entre ellas, una de las técnicas más antiguas empleadas como lo es la *ingeniería social*; entre otras.¹⁷

Tampoco debemos de omitir en este punto, el vínculo entre *crackers* y delincuencia organizada. La criminalidad organizada, en los últimos años ha tenido un crecimiento exponencial de sus actividades delictivas, afectando a toda la comunidad internacional y abarcando una gran cantidad de sectores de la actividad económica y social;¹⁸ desde luego, dañando

16 Hace algunos años en el Estado de Aguascalientes, un módulo del Registro Federal de Electores del Instituto Federal Electoral detectó la suplantación de identidad de una persona que residía en el Estado de Zacatecas (entidad federativa contigua), misma que tenía también domicilio en Aguascalientes. El hecho delictivo, lo constituyó el delito de fraude, donde el sujeto activo por medios convencionales, en este caso, hurgando en la basura y correspondencia abandonada de la víctima que sólo ocasionalmente visitaba su domicilio en esta última Ciudad, se apropió de datos personales, número de seguridad social y relación de propiedades respecto de la víctima, mismos que utilizó para suplantar su identidad y que pretendió validarla con una Credencial para Votar con Fotografía.

17 También existen disponibles en Internet programas utilizados para la captación de datos personales fundamentalmente aplicados para obtener claves de acceso o *passwords* como p.ej. el *sniffer* (programa rastreador), *Keylogger* y *Trojan Horse*. También referido como *Spyware*.

sensiblemente la transferencia o el flujo internacional de datos mediante la apoderación ilegal de datos personales por grupos criminales perfectamente organizados y altamente especializados.

5. LOS BIENES JURÍDICOS TUTELADOS

En consecuencia, ante estas inéditas conductas desarrolladas por la delincuencia de alta tecnología e inclusive realizadas por ladrones convencionales, no resulta un tema menor las graves consecuencias para los ciudadanos que son víctimas del robo de identidad. Los efectos directos generados por la suplantación de identidad son en principio daños fundamentalmente económicos, tales como la imputación de ciertos gastos y operaciones comerciales a quien aparece falsamente como titular de los datos contractuales,¹⁹ que inclusive puede derivarse en la negación al pago de una operación que realmente no ha llevado a cabo y la inevitable producción de efectos sobre su reputación financiera, estos es, el ciudadano suplantado tiene inicialmente un daño patrimonial, sin embargo, a la usurpación de identidad le suceden una cascada de perjuicios de distinta naturaleza que podrían incluir ataques a la privacidad o intimidad de las personas y daños de tipo psicológico.

Por otra parte, el posible tipo penal buscaría proteger una serie de intereses jurídicos en el contexto de la suplantación de identidad, tales como: los intereses patrimoniales de la persona cuya identidad se suplanta, la privacidad de las personas a quienes sus datos personales les han sido sustraídos o apropiados e inclusive podríamos extender su tutela al ámbito de interés colectivos para garantizar la veracidad en las relaciones sociales a partir de Internet, en particular de las que se emprenden a través de las Redes Sociales.

En particular, conforme lo señala Ángeles Jareño Leal y la extensión del propio concepto de intimidad, la información proveniente de bancos u otras entidades financieras que suministran información económica o patrimonial del sujeto²⁰ constituirían una especie de intimidad económica de la cual se buscaría obtener una protección desde el ámbito penal.

Vale la pena señalar que la frecuencia en la afectación de la intimidad mediante los atentados de carácter informático y el acceso ilícito

18 Delgado Martín, J. *La criminalidad organizada*. Editorial J.M. Bosch, Barcelona, 2001. p.22.

19 En este sentido, véase Mata y Martín, Ricardo, *op. cit.* p.207.

20 Jareño, Leal Ángeles. *Intimidad e imagen: los límites de la protección penal*. Editorial iustel, Madrid, 2008. p.33.

o no autorizado a los datos personales informatizados, ha motivado que el concepto de intimididad se haya ido perfilando de forma distinta inclusive que el concepto se vaya amplificando o extendiendo.²¹ Ante esta situación, la intimididad jurídicamente se extiende a otros límites en los que el derecho a controlar y autodeterminar sobre nuestra información personal es una cuestión sustantiva y positivamente establece un derecho de control sobre sí mismos.

6. LAS DISPOSICIONES PENALES EN EL ÁMBITO LOCAL MEXICANO SOBRE LA SUPLANTACIÓN DE IDENTIDAD

Por lo que respecta a otras entidades federativas que han comenzado a regular este tipo de conductas antijurídicas, destaca el Estado de Colima, entidad que reformó mediante el decreto 525, del 29 de abril de 2009, el artículo 234, fracción VII de su legislación sustantiva penal, mismo que considera como delito de fraude, la suplantación de identidades por medios informáticos, telemáticos o electrónicos que tienen como consecuencia la obtención de un lucro indebido.

Por otra parte, el Código Penal para el Distrito federal, fue reformado el 29 de junio de 2010, para crear el Capítulo III denominado de la "usurpación de identidad o personalidad" del Título XII, mediante el cual se adicionó el artículo 211 bis. La Asamblea Legislativa del Distrito Federal, al adicionar este precepto penal, indicó que la iniciativa se orientaba a buscar la protección en la intimididad de las personas, así como la certeza jurídica en sus posesiones cuando alguien vulnerare su identidad con fines delictivos. En este sentido, Nuevo León mediante el artículo 245, fracción X de su Código Penal, mismo que fue reformado el 3 de octubre de 2009, norma lo relativo a la atribución de la identidad de una persona mediante la utilización de documentos falsos.

Por su parte, el Código Penal de Sonora en su artículo 201, fracción V, también sanciona lo relacionado a la falsificación de documentos mediante los cuales se pretende atribuir la identidad de una persona.

Cabe citar que en el Estado de México, se expidió el Decreto número 235 por el que se reformó la denominación del Capítulo V, del Subtítulo III del Título III del Libro Segundo del Código Penal de dicha entidad por el se adicionaron los artículos 264 y 265, en los términos siguientes:

"Artículo 264.- Se le impondrán de uno a cuatro años de prisión y de cien a quinientos días multa, a quien ejerza con fines ilícitos

21 *Ibidem.*

un derecho o use cualquier tipo de datos, informaciones o documentos que legítimamente pertenezcan a otro, que lo individualiza ante la sociedad y que le permite a una persona física o jurídica colectiva ser identificada o identificable, para hacerse pasar por él.

Se equiparan a la usurpación de identidad y se impondrán las mismas penas previstas en el párrafo que precede prevista en el presente artículo a quienes:

I. Cometan un hecho ilícito previsto en las disposiciones legales con motivo de la usurpación de la identidad;

II. Utilicen datos personales, sin consentimiento de quien deba otorgarlo;

III. Otorguen el consentimiento para llevar a cabo la usurpación de su identidad; y

IV. Se valgan de la homonimia para cometer algún ilícito.

Las sanciones previstas en este artículo se impondrán con independencia de las que correspondan por la comisión de otro u otros delitos."

"Artículo 265.- Las penas señaladas en el artículo anterior se incrementarán hasta en una mitad, cuando el ilícito sea cometido por un servidor público aprovechándose de sus funciones, o por quien sin serlo, se valga de su profesión o empleo para ello."

Hay que destacar que esta disposición legislativa introducida recientemente a la legislación sustantiva penal en el Estado de México, ha integrado una serie de conductas equiparables a la usurpación de identidad.

Por su parte, la Ley para el Uso de Medios Electrónicos del Estado de México dispone específicamente en su artículo 53 lo siguiente:

"Artículo 53.- Comete el delito de apropiación de certificado y sustitución de identidad, el que por cualquier medio obtenga, reproduzca, se apodere, administre, utilice o de cualquier forma dé un uso indebido a un certificado, a una firma electrónica y/o a un sello electrónico, sin que medie el consentimiento o autorización expresa de su titular o de quien se encuentre facultado para otorgarlos.

Por la comisión de este delito se impondrá una pena de tres a ocho años de prisión y una multa de ochocientos a mil quinientos días de salario mínimo general vigente en la zona de que se trate, independientemente de las sanciones administrativas o penales que puedan corresponder a la conducta realizada."

7. LAS INICIATIVAS SOBRE USURPACIÓN DE IDENTIDAD EN LA LEGISLACIÓN PENAL FEDERAL EN MÉXICO

Por lo que respecta al plano legislativo federal, no existe tipo penal específico en el Código Penal Federal que regule estas conductas ilícitas, sólo el artículo 249, fracción I, de dicho ordenamiento legal, dispone una norma penal relacionada con la variación del nombre o apellido, asumiendo el de otra persona al declarar ante una autoridad judicial.

Sin embargo, existen algunas iniciativas legales en materia de robo o usurpación de identidad en el ámbito legislativo federal, entre las que destaca la iniciativa de Ley por la que se adiciona la fracción XXII al artículo 387 del código penal federal, relativa al robo de identidad con fines defraudatorios, presentada por el Diputado Federal Arturo Zamora Jiménez, durante diciembre de 2009. Al respecto, la hipótesis legal propuesta se vincula al delito de fraude.

En este punto destaca la propuesta del Senador Federico Dóring respecto a la iniciativa que tipificar la usurpación de identidad en las redes sociales como un delito de carácter federal y que adicionalmente los ISP o Proveedores de Servicios de Acceso a Internet sean regulados por una ley de la materia.

8. LAS ACCIONES INSTITUCIONALES DEL GOBIERNO MEXICANO EN TORNO A ESTA PROBLEMÁTICA

En consecuencia, dada la importancia del tema, el Gobierno Federal mexicano también ha emprendido una serie de acciones institucionales que buscan evitar la usurpación de identidad en detrimento de los consumidores. Específicamente, la Procuraduría Federal del Consumidor en 2006, asumió diversas acciones preventivas dirigidas a alertar al consumidor sobre el robo de identidad para obtener créditos.

En el mismo sentido, mediante acciones preventivas conjuntas la Comisión Nacional de Usuarios de Servicios Financieros y el Buró de Crédito, establecieron desde el año 2006, un servicio de alerta para

detectar cuando se consulta el historial de crédito de una persona, así el sistema denominado “alertas buró”, notifica cualquier cambio en el historial crediticio ante una posible suplantación de identidad con fines de carácter financiero.

Desde luego, ante las crecientes conductas relacionadas con el “robo de identidad” en nuestro país y que nos alertan sobre la importancia del tema, también han surgido una serie de iniciativas en el sector privado mexicano, particularmente la Asociación Mexicana de Internet (AMIPCI), creó el website <http://www.navegaprotegido.com.mx>, mismo que contiene información que educa y auxilia a los consumidores sobre los riesgos del robo de identidad digital.

9. LAS ACCIONES DE ORGANISMOS INTERNACIONALES EN MATERIA DE ROBO O USURPACIÓN DE IDENTIDAD

En función de lo que precede, en el plano legislativo internacional existen diversas iniciativas en materia de “robo de identidad”. En Argentina, durante el año en curso, se presentó el proyecto de Ley Expediente 4643-D-2010, mejor conocida como “Ley sobre el robo de identidad digital”, proyecto que propone la incorporación del artículo 139 ter, al código penal argentino”, presentado por la Diputada Natalia Gambaro. Cabe señalar que este constituye el primer proyecto legislativo de esta naturaleza que se presenta en Latinoamérica, y que busca sancionar al que adoptare, creare, apropiare o utilizare, a través de Internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca. Adicionalmente, el proyecto, aumenta la punibilidad cuando el autor asuma la identidad de un menor de edad o tuviese contacto con una persona menor de dieciséis años, aunque mediere su consentimiento o sea funcionario público en ejercicio de sus funciones.

En lo que concierne a la regulación jurídica y acciones en materia de robo de identidad emprendidas por organismos internacionales, destaca a continuación lo emprendido por la Organización de las Naciones Unidas:

Informe 2010 de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) denominado “*the globalization of crime, a transnational organized crime threat assessment*”; en donde el capítulo 10 se relaciona con el cybercrimen y particularmente el apartado 10.1 se vincula al robo de identidad;

12° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, realizado en Salvador, Brasil, durante abril de 2010, organizado por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), mismo que analizó la falta de cooperación internacional en materia de justicia penal, situación que propicia una vía de escape a los delinquentes cibernéticos, así como los vínculos entre la delincuencia organizada y la delincuencia cibernética;

Informe 2007 de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), mismo que un apartado se dedica al análisis del robo de identidad;

Consejo Económico y Social de la Organización de las Naciones Unidas, a través de la Comisión de Prevención del Delito y Justicia Penal, durante su 18° período de sesiones, celebrado en Viena del 16 al 24 de abril de 2009, se realizó un debate temático sobre el fraude económico y los delitos relacionados con la identidad;

Consejo Económico y Social de la Organización de las Naciones Unidas, a través de su Comisión de Prevención del Delito y Justicia Penal, durante su 14° período de sesiones, realizado en Viena del 23 al 27 de mayo de 2005, el tema 6, se orientó a la cooperación internacional en la lucha contra la delincuencia transnacional; el fraude y la falsificación de identidad y su uso indebido con fines delictivos. Al respecto, se presentaron los avances realizados por el grupo intergubernamental de expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos;

Consejo Económico y Social de la Organización de las Naciones Unidas, mediante la Comisión de Prevención del Delito y Justicia Penal, durante su 13° período de sesiones, celebrado en 2004, examinó el problema desde una perspectiva de derecho penal y público, incluyendo el fraude comercial y otros tipos de fraude. También analizó el problema de la falsificación de identidad y su uso indebido con fines delictivos, que consistía en un problema conexo, y decidió solicitar que se efectuara un estudio combinado de ambos fenómenos, de modo que incluyera las relaciones entre el fraude y la falsificación de identidad y su uso indebido con fines delictivos y otros delitos, así como la prevención y control de referidos problemas recurriendo al derecho mercantil y al derecho penal;

Consejo Económico y Social de la Organización de las Naciones Unidas, mediante la Resolución 2004/26, estableció directrices respecto de los elementos del estudio relacionados a la gama de delitos que suponen la falsificación de identidad;

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, misma que constituye la base jurídica aplicable en materia de cooperación en los casos de fraude transnacional vinculados en materia de robo de identidad;

Por lo que respecta a las acciones que ha generado la Organización para la Cooperación y el Desarrollo Económicos (OCDE), destaca en 2009, la publicación de un estudio sobre el robo de identidad en línea y la emisión de las "Directrices sobre el robo de identidad en línea que datan de 2008, así como una serie de guías y recomendaciones en materia de fraude transfronterizo, seguridad sobre sistemas de información y redes, y protección de la privacidad sobre la circulación de datos personales transfronterizos.

En el ámbito de la Unión Europea, sobresalen ante esta problemática las conclusiones 2009/C 62/05, del Consejo de Europa, relativas a una estrategia de trabajo concertada y a medidas concretas contra la delincuencia informática, mismas que proponen a corto plazo la creación de instrumentos operativos que permita una mejor descripción de lo que se entiende por usurpación de identidad en Internet. En este sentido, también destaca del propio Consejo, la Convención sobre Cybercrimen (Budapest 2001, modificada en 2004) y la Directiva 95/46 sobre la Protección de los Individuos con Observación hacia el Procesamiento de Datos Personales.

Destaca en el ámbito de la Unión Europea también, la Decisión Marco UE 2005/222/JAI sobre ataques a los sistemas de información²²

Por su parte, la Organización para la Cooperación Económica Asia-Pacífico (APEC), en su oportunidad propuso la integración de un grupo de expertos para analizar el tema denominado "Computers Emergency Response Teams CERT's".

22 Diario Oficial de la Unión Europea del 16 de marzo de 2005.

10. LA LEGISLACIÓN FEDERAL NORTEAMERICANA SOBRE SUPLANTACIÓN DE IDENTIDAD Y LAS ID-THEFT STATE LAW

En este tenor, los Estados Unidos de Norteamérica en su legislación de orden federal, han decretado la "*Identity Theft and Assumption Deterrence Act*",²³ misma que trata sobre la disuasión de robo y asunción de identidad, promulgada por el Congreso en 1998, la cual fue codificada; en parte, en la Sección & 1028 (a), Título 18 del *United States Criminal Code*, la cual constituye la ley federal que hace del robo de identidad un delito. La norma penal decretada en este país, se orienta a sancionar a quien transfiera, posea o utilice sin mediar autorización, los datos identificativos de una persona con el objeto de cometer, intentar o favorecer cualquier actividad ilícita. Así también, prácticamente la totalidad de los Estados de la Unión Americana, han promulgado leyes relacionadas al delito de robo de identidad.²⁴ Recordemos que la Agencia Federal de Investigaciones, ha señalado que el robo de identidad es uno de los delitos de mayor crecimiento en los Estados Unidos de Norteamérica y estima que cada año, entre 500,000 y 700,000 norteamericanos son víctimas del robo de identidad. Sin embargo, según un Informe sobre Robo de Identidad, presentado por la Comisión Federal de Comercio de este país en 2007, señala que las cifras resultan aún más preocupantes, reportándose que durante 2005, un total de 8.3 millones de ciudadanos norteamericanos fueron víctimas de alguna forma de robo de identidad.²⁵

En este orden de ideas, el análisis expuesto buscaría colmar un vacío normativo en la legislación penal mexicana, mediante la incorporación de un tipo penal de naturaleza compleja y que complementaría también los delitos contra la fe pública, particularmente los delitos relativos a la falsificación de documentos; así como de aquellos tipos penales vinculados al uso de objetos o documentos falsos alterados y de las normas penales relacionadas con la variación del nombre, domicilio o nacionalidad.

Desde este punto de vista, en 2006, según datos de una encuesta realizada por la empresa especializada para la protección y seguridad de la información UNISYS; México ocupaba el cuarto lugar mundial en casos de fraude por robo de identidad.²⁶ No obstante, en la actualidad no se tiene certeza sobre las cifras ante este tipo de conductas ilícitas.

23 Federal Trade Commission. *Identity Theft*. November 2005, p.28.

24 También referidas como ID-Theft State Law.

25 Federal Trade Commission: *2006 Identity Theft Survey Report: prepared for the Commission by Synovate*, November 2007.

26 Disponible en <http://www.jornada.unam.mx>, consultada en octubre 11 de 2010.

11. LA USURPACIÓN DE IDENTIDAD A TRAVÉS DE CERTIFICADOS DIGITALES

Resulta con mayor frecuencia que validar la identidad de una persona través de Certificados Digitales y el otorgamiento de llaves privadas mediante técnicas de encriptación asimétrica; establezca siempre la posibilidad real de que algún sujeto activo intente apropiarse de manera no autorizada de los certificados digitales. En este caso, resulta oportuno establecer un tipo penal especial que sancione esta conducta y que adicionalmente se tomen medidas específicas dirigidas a revocar certificados digitales como medida precautoria o inclusive de carácter correctivo cuando exista el riesgo potencial de apropiación indebida de certificados digitales y se proceda por el agente certificador o la agencia certificadora a la cancelación de claves.

12. UNA PROPUESTA DE ACCIÓN LEGISLATIVA PARA UN TRATAMIENTO JURÍDICO-PENAL EN TORNO A LA USURPACIÓN DE IDENTIDAD

En razón del breve análisis planteado de este tipo de conductas ilícitas desplegadas, mismas que son nocivas para nuestras sociedades postmodernas; las cuales a nuestro juicio debieran tener un tratamiento jurídico-penal. Para tal efecto, desde el plano académico proponemos tipificar las siguientes conductas dentro de un Capítulo específico en la legislación sustantiva penal de orden federal o local que contemple el delito de "usurpación o suplantación de identidad", siendo estas posibles hipótesis penales, las siguientes:

CAPÍTULO... USURPACIÓN O SUPLANTACIÓN DE IDENTIDAD

Artículo...

Comete el delito de usurpación o suplantación de identidad a quien por cualquier medio incluyendo el informático o telemático despliegue conductas u omisiones dirigidas al apoderamiento, tenencia, utilización, disposición o cesión de cualquier tipo de datos personales, informaciones o documentos sin la autorización de quien o quienes legítimamente les pertenezcan; mismos que les permiten individualizarlos en un contexto social y que le permite a una persona física o jurídica ser identificada o identificable, cuya finalidad estriba en hacerse pasar por el titular de dichos datos personales, se le impondrá una pena de

uno a cinco años de prisión y de cuatrocientos a seiscientos días multa.

Serán equiparables al delito de usurpación de identidad y se impondrán las mismas penas previstas en el párrafo que precede, las siguientes conductas:

I.- Al que por algún uso de los medios telemáticos o electrónicos, genere un daño patrimonial y obtenga un lucro indebido para sí o para otro valiéndose de alguna manipulación informática o intercepción de datos de envío, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a bases de datos automatizadas para suplantar identidades;

II.- A quien transfiera, posea o utilice, sin autorización, datos identificativos de otra persona con la intención de cometer, intentar o favorecer cualquier actividad ilícita, y

II.- Al que asuma, suplante, se apropie o utilice a través de Internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca.

Se aumentarán en una mitad las penas previstas en el presente artículo y suspensión del derecho de ejercer la actividad profesional por un lapso de seis meses a dos años, en el supuesto que el sujeto activo tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática o telemática, la pena se aumentará hasta dos años más de prisión en caso de reincidencia y privación definitiva en el ejercicio de la actividad profesional.

Por último, cabría destacar la pertinencia de integrar este capítulo en el apartado correspondiente a los delitos patrimoniales o bien, resultaría prudente integrarlo al rubro de los delitos cometidos contra la seguridad de las personas. Esta última, sería una decisión que correspondería asumirla a nuestros legisladores federales o locales, a la brevedad posible o ignorarla con las inevitables consecuencias catastróficas para la ciudadanía respecto a la protección penal de su patrimonio y de su privacidad.

FUENTES DE CONSULTA

AZAOLA, CALDERÓN Luis, *Delitos informáticos y derecho penal*, México, Editorial UBIJUS, 2010.

GONZÁLEZ DE LA VEGA, Francisco, *Derecho penal mexicano, los delitos*. Vigésima segunda edición. México, Editorial Porrúa, 1988

JAREÑO, LEAL Ángeles, *Intimidación e imagen: los límites de la protección penal*. Madrid. Ed. IUSTEL, 2008.

RALLO, LOMBARTE ARTEMI et alius (comps.), *Robo de identidad y protección de datos*. Pamplona, Ed. Arazandi-Thomson Reuters-Agencia Española de Protección de Datos-Universidad de Castilla-La Mancha, 2010.

TÉLLEZ, VALDÉS Julio Alejandro. *Derecho informático*, cuarta edición, México, Mc Graw Hill/Interamericana Editores, 2008.

LEGISGRAFÍA

Código Penal Federal, edición electrónica de la Cámara de Diputados del H. Congreso de la Unión, México, 2010.

Código Penal del Estado de Colima, edición electrónica de la Cámara de Diputados del Estado de Colima, México, 2010.

Código Penal del Distrito Federal, edición electrónica de la Asamblea Legislativa del Distrito Federal, México, 2010.

Código Penal del Estado de México, edición electrónica de la LVII Legislatura del Estado de México, 2011.

Identity Theft and Assumption Deterrence Act of 1998, Public Law 105-318, October 30, 1998. 105th Congress, Senate and House of Representatives of the United States of America.

INFORME:

Federal Trade Commission: 2006 Identity Theft Survey Report: prepared for the Commission by Synovate, November 2007.