



DELITOS INFORMÁTICOS: LA SUPLANTACIÓN DE IDENTIDAD

Miguel Zamora Acevedo¹

Fecha de recepción: 23 de enero de 2025

Fecha de aprobación: 24 de octubre de 2025

RESUMEN: La sociedad de la actualidad además de representar el progreso tecnológico también trae consigo nuevas adversidades, para lo que interesa en el presente artículo “*Delitos informativos: La suplantación de identidad*” busca investigar y analizar los nuevos tipos de delincuencia cibernética que han surgido con el progreso tecnológico. El autor analiza el *phishing* como forma delictiva de suplantación de identidad. Si bien, estas nuevas formas delictivas se han vuelto una problemática importante y una amenaza para los ciudadanos, no es posible prescindir del avance tecnológico y las nuevas oportunidades que con ellas trae. El objetivo es mostrar la aplicación teórica y práctica del delito, según la legislación penal costarricense.

PALABRAS CLAVES: Phishing, ciberdelincuencia, suplantación, identidad, delito.

ABSTRACT: Today's society, in addition to representing technological progress, also brings with it new adversities. This article, “Information Crimes: Identity Theft,” seeks to investigate and analyze the new types of cybercrime that have emerged with technological progress. The author analyzes phishing as a criminal form of identity theft. Although these new forms of crime have become a significant problem and a threat to citizens, it is not possible to ignore technological advances and the new opportunities they bring. The objective is to

¹ Abogado y notario graduado de la Universidad de Costa Rica, con estudios de doctorado y maestría en Derecho Penal por la Universidad de Costa Rica; máster en argumentación jurídica, máster en sociología jurídica y máster en razonamiento probatorio en universidades de España e Italia. Ha sido juez de apelación de sentencia penal; juez de juicio; abogado letrado de la Sala de Tercera de la Corte Suprema de Justicia, defensor público y facilitador. Autor de varios artículos y libros en derecho penal, procesal penal, criminología, ética y razonamiento probatorio. Docente universitario.



show the theoretical and practical application of the crime, according to Costa Rican criminal law.

KEYWORDS: Phishing, cybercrime, impersonation, identity, crime.

ÍNDICE: 1. El llamado ciberespacio y la ciberdelincuencia; 2. El *phishing*; 3. Breve esquema para la resolución de casos en materia penal; a. Primera etapa; b. Segunda etapa; 4. La suplantación de identidad;

1. EL LLAMADO CIBERESPACIO Y LA CIBERDELINCUENCIA

En la actual sociedad de la información, es muy común escuchar las nociones de ciberespacio y cibercriminalidad. Ambos conceptos se entremezclan y se presentan en la cotidianidad de las personas de varias formas expresivas muy heterogéneas y disímiles entre sí.

Empero, por lo general concurren en nuevas formas delictivas que se contraponen a la delincuencia tradicional, especialmente aquellas modalidades que se realizan a través de sistemas o redes informáticas, datos de Internet y cualquier otro medio telemático de información, cuya complejidad operativa generalmente conlleva mayores dificultades de persecución y, por ende, obstaculiza la obtención de las pruebas; en consecuencia, se elevan los niveles de lo que se denomina inmunidad.

En este sentido la palabra ciberespacio hace referencia al espacio artificial y virtual emergente donde se realizan las relaciones sociales entre personas, organizaciones y en general, máquinas computacionales, que no tienen existencia independiente de los equipos y programas informáticos que posibilitan dichas interacciones.

La primera referencia a la noción de ciberespacio nace de la literatura, específicamente en la novela neuromante de William Gibson (1996). Surge de la composición de los términos *neuro*, sea lo mental y *mante* sujeto o actor de *mancia* que significa adivinación y por extensión magia en consecuencia neuromante se traduciría como el neuromancer.



Como resulta fácil deducir, de las nociones antes indicadas, se refieren componentes de “autonomía y autorreferencia” (Santana Soriano & Báez Vizcaíno, 2022). Lo cual es coincidente con el desarrollo actual de las relaciones virtuales en el ciberespacio.

En consecuencia la ciberdelincuencia trata de un término que hace referencia a toda aquellas actividades ilícitas que se cometen en el ciberespacio o en el uso y abuso de las tecnologías de la información, comunicación y almacenamiento de datos, amenazando los bienes jurídicos individuales, colectivos y de seguridad de los sistemas informáticos; de hecho, algunos consideran que pronto, el comercio internacional, será absorbido por el comercio electrónico (Gudín Rodríguez Magariños, 2018, págs. 22-23).

Dentro de este punto cobra especial referencia todas las defraudaciones de la banca, la delincuencia electrónica que se comete a través de sistemas informáticos que afectan especialmente la integridad y con fidelidad confidencialidad de los datos personales.

Así las cosas, se debe reconocer que las relaciones sociales, económicas y en general de comunicación, no se puede realizar sin el uso masivo de la tecnología, pues se están ante la supremacía de la sociedad de la información, que no se concibe sin la utilidad de los medios tecnológicos que avanzan a un nivel vertiginoso, que incluso dificulta al Derecho regular apropiadamente sus manifestaciones.

Dentro de este escenario real y vigente, resulta fundamental dotar de seguridad a las personas y entidades que se interrelacionan en el ciberespacio, especialmente sobre sus datos personales que se alojan en redes informáticas, redes sociales y virtuales cómo sería, por ejemplo, el correo electrónico, para que puedan tener plena vigencia de identidad frente a terceros que conviven en ese universo alternativo “ciber”.

2. EL PHISHING



La etimología del término phishing deviene la palabra inglesa '*fishing*', que se traduce como pesca, lo cual hace referencia al acto de pescar, en este caso, se busca atrapar usuarios mediante el lanzamiento de anzuelos cada vez más sofisticados para obtener información sensible y que brinde acceso a los datos privados cómo serían las contraseñas, tokens y usuarios de las personas.

La forma más usual de realizar esta actividad es mediante el envío masivo de correos electrónicos para imponerse de información financiera, sin embargo, la diversidad de formas delictivas actuales es innumerables, aunque lo propio de la figura es y será, la masificación de información tendiente a que las personas brinden sus datos.

El modo más común es la de utilizar técnicas de engaño por medio de formas y contenidos de los correos electrónicos que simulan ser de entidades del destinatario, enlaces hacia páginas equivalentes de las entidades bancarias o financieras, con lo que se pretende ser lo más parecido posible de la organización por la cual se pretenden hacerse pasar.

En este caso, la calidad del engaño, la suplantación de la forma del sitio web o del correo, dependerá del *phiser*, lo que sirve a su vez, para determinar el grado de ejecución del delito; ello, porque, en asocio a los delitos de estafa, en esta forma delictiva, también contribuye el exceso de confianza de los sujetos pasivos y muchas veces, algún nivel de ignorancia en el manejo de los sistemas informáticos.

Aunque lo común es que se realice mediante correos electrónicos, nada obsta para que ejecute por otras formas tecnológicas como mensajes de texto, *whatsapp*, *telegram*, *signal*, ventanas emergentes, etc. Pero siempre, la finalidad es la misma: la obtención de información restringida de las personas usuarias.

La idea del delito se puede relacionar análogamente a las formas de estafas, que se trasladan al ámbito telemático, por medio de lo cual, se busca que las víctimas sean conducidas a sitios web con apariencia a la entidad real, con el objetivo de obtener la información básica que permita el acceso o bien, o



bien, al correo electrónico que permita la recuperación de los datos de acceso al sitio financiero, el cual es fraudulento.

Una vez con la información de entrada, se puede acceder a los sitios bancarios o financieros (conocido como *e-banking*) y poder apoderarse del patrimonio ajeno, mediante transferencias, o simplemente tener una cuenta puente donde transferir patrimonio ajeno.

Ahora bien, en forma general, este delito se configura en las interacciones que se realizan en la internet, con las caracterizaciones que se han apuntado, propio de la llamada técnica de ingeniería social. Esto se entiende como la manipulación para obtener la información confidencial del usuario, basado en la falta de información y la inocencia de las personas.

Por general, la ingeniería social está ligada a las técnicas de engaño, como la captación de datos en redes sociales en lugares públicos y algunas más avanzadas como la utilización del *texting* (la suplantación del ciber delincuente para obtener información financiera de la empresa o del empleado).

Como forma de ingeniería social, la más común es el modo de hacerse pasar por otras personas, en sitios webs o correos de las entidades bancarias. En razón de ello, interesa acá, analizar la figura delictiva que castigaría tales acciones, sea el delito de suplantación de identidad en el artículo 230 (Código Penal de Costa Rica, 2003), el cual establece que, “será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información”.

Ahora bien, de seguido se brinda un breve esquema de análisis de los hechos delictivos, para mostrar la manera que se va a examinar el tipo penal en estudio; dicho esbozo, sigue la clásica tesis del finalismo y su versión de la teoría el delito.



3. BREVE ESQUEMA PARA LA RESOLUCIÓN DE CASOS EN MATERIA PENAL

De seguido se indica en forma esquemática y breve, una guía de cómo analizar un caso penal y poder aplicar la teoría del delito para darle una resolución (Pawlik, 2023, pág. 61 y ss).

En lo particular, se desarrolla la guía de Maqueda Abreu y Copello (2011, pág. 253) la cual señala que existen diversas etapas, las cuales serán explicadas a continuación.

a. Primera etapa

En este apartado, lo que lo primero que se debe realizar es la comprensión del supuesto fáctico y el planteamiento de hipótesis (o teoría del caso, según la parte).

En este primer momento, para resolver un caso práctico de derecho penal, es necesario la comprensión del supuesto de hecho que se propone al análisis, para lo cual:

1. Se tiene que realizar lectura cuidadosa y detenida del supuesto fáctico. El tiempo que se invierte, se traduce en una mejor comprensión del caso, al tener la posibilidad de ver detalles, máxime en tipologías delictivas modernas y de desarrollo tecnológico.
2. De seguido, deben seleccionarse aquellos elementos tácticos que, desde el primer punto evidencian principio, se muestran primordiales para el ulterior análisis jurídico. Con relación a esto, debe tenerse claro que los antecedentes o datos que plasman en el caso, en evidencia probada y cierta; En concordancia con lo anterior, no se deben alterar ni suponer hipótesis alternativas. En lo posible, se debe evitar todo subjetivismo de quien escogió el caso.
3. Posteriormente, se tienen que ordenar todas las situaciones o circunstancias que se presenten en el caso, como puede ser: personas



implicadas (sujetos activos o pasivos, etc.), lugar, tiempo, modo, delito, etc. En el caso de intervenir una pluralidad de personas en el caso, se debe determinar a cada uno el papel que representa; sea en calidad de autoría y modo de participación (instigador o cómplice), etc.

b. Segunda etapa

En este apartado se debe analizar y evaluar jurídicamente el supuesto de hecho. Ahora bien, para el análisis del caso y para su examen posterior, se deber contar con las herramientas jurídicas necesarias que faciliten su estudio y resolución, por ejemplo:

1. La normativa aplicable al supuesto fáctico.
2. Jurisprudencia supuestos semejantes o similares
3. Doctrina que estudie el tema o que se haya problematizado.

Teniendo los instrumentos jurídicos al alcance, se debe proceder al estudio del caso, para lograr, primeramente, la identificación de la problemática del caso y posteriormente determinar las soluciones jurídicos penales que se presentan.

Como primer criterio, es recomendable iniciar con la realización del estudio guiado por la referencia la acción de quien se consideraría el autor del hecho (o autores co-autores, según correspondan).

Subsiguientemente se debe analizar el papel desempeñado por los demás participantes del hecho – si los hay– como serían los instigadores y cómplices, pues su posible responsabilidad penal, es accesoria a la autoría.

Una vez determinada esta primera diferenciación, debe analizarse y establecer lo siguiente:

1. La existencia de un comportamiento humano penalmente relevante, de parte del autor o autores;
2. De ser afirmativo lo anterior, se debe determinar si esa conducta es típica de delito. En este caso, se tiene que analizar de forma separada el tipo



- objetivo (elementos descriptivos, normativos, sujeto activo, modo, bien jurídico, nexo de causalidad, etc.) y el tipo subjetivo (dolo, culpa o preterintencional);
3. Igual que lo anterior, en un supuesto que confirme el hecho típico, se pasaría a determinar si esa conducta típica, es también antijurídica, por no presentarse alguna causa de justificación y si existe una grave afectación al bien jurídico tutelado;
 4. A su vez, si se confirma este punto, sea que la conducta es típica y antijurídica, habría que comprobar si ese injusto penal es también culpable, pues si se constata la presencia de algún estado de inimputabilidad, no habría culpabilidad (aun en estos casos, se valoraría la *actio libera in causa*).
 5. Por último, y siguiendo la teoría del delito, se debe analizar la existencia de condiciones objetivas de punibilidad o la existencia de alguna excusa absolutoria que elimine la punibilidad, lo cual es excepcional y rara avis, en el derecho penal costarricense).
 6. Es esencial que los anteriores pasos de raciocinio no deben variarse o alterarse. Lógicamente, si se concluye que en el caso, no existe acción penalmente relevante, por la presencia de alguna causal de no acción; el estudio de la etapa concluye, una etapa es una condición necesaria para proseguir al estudio de la siguiente; en igual sentido, si se determina acción es atípica, no podría proseguir y así continuamente.

Finalizado lo anterior análisis, se debe establecer y justificar el grado de imputación del sujeto que ha realizado la conducta (autor) o bien, ha favorecido el hecho por medio de su participación (instigador o cómplice). Sumado a ello, también debe estudiarse y determinar las formas imperfectas de ejecución del delito sea el *iter criminis*.

Posteriormente, es necesario considerar la aplicación de más de un tipo penal, en cuyo supuesto, debe determinar las reglas del concurso, sea aparente



(de normas), o bien de delitos de delitos: ideal o real), y se procede a establecer las penalidades correspondientes.

Por último, se aclara que, muchas veces, los supuestos de análisis jurídico penal no tienen sola solución. Existen diversas orientaciones de la teoría de delito que conllevan a distintas soluciones alternativas. Así, dependiendo de la escogencia de una concepción causalista, finalista, normativista o funcionalista, se determinará respuestas diversas o fundamentaciones diferentes.

De ahí que, la solución que se exponga no es lo más significativo en sí mismo, sino la fundamentación, coherencia y fuerza argumentativa por la que se adopta dicho resultado.

Lo anterior, obliga a exponer con total claridad y desde antes de mostrar el resultado, cuál es el enfoque que se toma en el análisis, para así poder ponderar la coherencia de la solución brindada.

4. LA SUPLANTACIÓN DE IDENTIDAD

El delito de suplantación de identidad es una figura sumamente reciente. Data del año 2012. Antes de dicho tipo penal, las acciones de suplantación se aplicaban otros tipos penales, como por ejemplo el delito de “violación de datos personales” (Código Penal, 2003, artículo 196 bis). Por su parte, en la esfera internacional, España, por ejemplo, se utilizaban los tipos penales de “usurpación del estado civil”, “falsedad en documento privado”, “revelación de datos personales”, etc. (Asociación Profesional de Expertos Contables y Tributarios de España, 2013).

En nuestro ordenamiento jurídico, el tipo penal en cuestión establece que: “será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información” (Código Penal, 2003, artículo 230).



En este delito, el bien jurídico tutelado es la intimidad, la confianza pública de la sociedad o la garantía (fe pública) en la identificación de las personas, debido a que, al hacerse pasar por otro (suplantar la identidad de la persona) se transgrede la fe pública y se causa desconfianza en las identidades digitales de las instituciones y organizaciones financieras, la de las personas en diversas redes sociales, etc., es un delito pluriofensivo.

Respecto a la tipicidad objetiva (Roxin, 1997, pág. 110 y ss), el delito como acción humana invariablemente la realiza un autor, quien precisamente es el que realiza la acción prohibida y solo puede ser una persona física. Así vemos como algunos tipos penales utilizan las frases “El que...”, “quien...”, para hacer referencia a la persona que lleva a cabo la acción.

Existen tipos penales que para su configuración requieren la presencia de dos o más personas, como, por ejemplo, el robo agravado llevado a cabo por ese número de sujetos. En igual sentido, existen varios tipos penales que exigen condiciones especiales en el sujeto activo, como los delitos contra la Administración de Justicia, o ciertos delitos de homicidio que se agravan por el parentesco, sin embargo, la mayoría de los delitos son comunes, porque no requieren alguna condición del sujeto, como es el caso de la suplantación.

Por su parte, el sujeto pasivo es el destinatario de la protección del bien jurídico, distinta del sujeto pasivo de la acción que es solo la persona sobre la que recae la acción típica pero no necesariamente el destinatario de la protección del bien jurídico (González Castro, 2008, pág. 16). Por ejemplo, el hurto del bolso de la madre al niño. En el caso, anterior la víctima es el niño pues sobre él recae la acción, pero el sujeto pasivo es la madre pues es la titular del bien jurídico.

Una cosa distinta a lo que suceden con el sujeto activo, el pasivo puede ser una persona física como jurídica, e incluso el conglomerado social, como los delitos que afectan la salud pública. De igual manera existen ciertos sujetos pasivos que la ley exige ciertas características para la configuración del delito,



como el tiempo de nacido del menor para efecto de configurar el homicidio especialmente atenuado.

En este sentido, en cuanto a los sujetos participantes de la suplantación de identidad, se establece que, el sujeto activo y el pasivo son comunes, pues no requieren de una característica especial; sin embargo, se aclara que el sujeto activo, para realizar la tipicidad objetiva, requiere algún conocimiento especial en temas informáticos para acceder a simular la identidad de las páginas o los remitentes de los correos anzuelos.

Respecto al acto, la norma dice que es la acción de suplantar. Para entender el término, al recurrir al diccionario de la Real Academia Española (s.f, definición 1 y 2), éste establece la palabra suplantar como,

1. tr. Falsificar un escrito con palabras o cláusulas que alteren el sentido que antes tenía. Y en su segundo significado, sostiene que:
2. tr. Ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba.

En cuando a la acción, la suplantación de identidad reside en exclusivamente en apropiarse del nombre o de alguna pertenencia que simule al titular, no requiere mayores acciones para configurar el delito, ya que, si bien se busca hacer actos delictivos lesionando el buen nombre de la persona la cual están suplantando, el resultado no es un requisito del tipo penal; si se realiza, cometería otro delito.

Ahora bien, lo que se suplanta es la identidad, pero específicamente para el delito en cuestión, la identidad digital. Es decir, al conjunto de la información sobre una persona sea física o jurídica, o bien de una organización que se expone en la Internet o redes sociales, como serían datos personales, imágenes, registros, noticias, comentarios, etc., que conforman la descripción de dicha persona en el ciber espacio.



Ahora bien, como se señala, dicha información es la que se encuentra en las bases de datos, algunas públicas y otras privadas o de acceso limitado, y son las que permiten al sujeto acceder a diversos lugares en el ciberespacio como sería la entrada a la banca en línea, redes sociales, correo electrónico, páginas de sitios de compra, *delivery*, etc. Lo que se busca con la suplantación es la obtención sin consentimiento del usuario, clave o token que permita el acceso; de lograrse, se infringe otra figura penal.

Es decir, se suplanta para poder acceder a la identidad digital, sea, a los datos que le permiten interactuar con el plano digital. Datos que son precisamente los que se registran en las bases de información de la internet y que identifican a la persona o entidad.

Ahora, la idea es que tal información, sea solo utilizada con el objetivo para la cual fue proporcionada y registrada en la base de datos; empero, dicha información registrada en la web no siempre queda protegida frente al ataque de terceros, es común que se registre y quede como predeterminada en alguna máquina o sistema de almacenamiento de contraseñas.

En consecuencia, este delito busca suplantar la identidad de una persona física o jurídica o incluso de una marca comercial, para acceder a dicha información, para la cual, según el artículo 2 de la Ley 7978 (2003), la marca comercial sería todo “signo denominativo o mixto que identifica y distingue una empresa o un establecimiento comercial determinado”.

En el caso de personas físicas, tiene que existir la persona a suplantar, caso contrario el delito no existe. Así, es irrelevante que la persona haya fallecido. Pero no habría delito si la persona es ficticia, por ejemplo, hacerse pasar por Sherlock Holmes.

Lo que busca este tipo penal es que el autor utilice la información para “ocupar el lugar de otra persona”, esto es, utilizar la identidad digital de otro sujeto para realizar acciones a nombre del suplantado, específicamente, imponerse de su información privada.



De esta forma la suplantación de identidad tiende a cumplir dos objetivos; primero, ocultar la propia identidad del autor y consecuentemente, como segundo objetivo, causar un perjuicio a la intimidad de la víctima suplantada que es la titular de la identidad utilizada, o bien, de un tercero que beneficia al autor.

Finalmente, en cuanto a la tipicidad subjetiva, la suplantación es un delito doloso, donde solo cabe su realización con dolo directo, pues se presenta la intención de hacerse pasar por otro.

Respecto al *iter criminis* o camino del delito, esta figura penal no admite formas imperfectas de ejecución, ya que no admite tentativa; con la simple suplantación se consuma el tipo penal. La norma no exige ningún resultado, tampoco afectación patrimonial efectiva, aunque en la práctica, esto es lo que se busca.

La conducta delictiva se perfecciona con la realización de la actividad suplantada y cesa cuando concluye la suplantación. Debe darse la permanencia, o sea, que se tenga la totalidad de las circunstancias que componen la identificación suplantada, de modo tal, que el suplantador se haga pasar por el suplantado a todos los efectos como si se tratara de esa persona, pero en la esfera digital.

5. CONCLUSIONES

En resumen, se puede concluir que el delito de suplantación de identidad es una figura novedosa en las formas delictivas actuales, sin embargo, su aplicación práctica y compleja constituirán un verdadero reto al operador jurídico. De ahí que, en las presentes líneas de investigación se haya realizado un breve bosquejo que facilite su aplicación práctica.

A su vez, se ha identificado los elementos básicos de la tipicidad objetiva y subjetiva y sus particularidades, también las diferencias que identifican la figura y a su vez sirven para distinguirlo con representaciones semejantes.



Para su análisis, se ha seguido la teoría jurídica del delito y el tipo complejo, lo cual facilita su estudio y orientación; en este sentido, no se ha realizado referencia alguna a la escasa jurisprudencia patria que compara el delito con otros tipos penales, por carecer de referencia directa al tipo penal estudiado.

6. BIBLIOGRAFÍA

AECE. (2010). Asociación Profesional de Expertos Contables y Tributarios de España. La suplantación de una identidad digital. Madrid: Cont4bl3, 45, 38.

Código Penal. Ley no. 4573.(2003) San José: Investigaciones Jurídicas

Gibson, W. (1996). Neuromante. Barcelona, España: Planeta

González Castro, J. A. (2008) Teoría del delito. San José, Costa Rica: Programa de Formación Inicial de la Defensa Pública.

Gudín Rodríguez Magariños, F. (2018). Nuevo Reglamento europeo de protección de datos vs big data. Valencia: Tirant lo Blanch.

Ley de Marcas y Otros Signos Distintivos, ley no. 7978. (2003). San José: Investigaciones Jurídicas.

Maqueda Abreu, M. L y Copello, P. (2011). El derecho penal en casos: parte general. Teoría y práctica. Valencia, España: Tirant lo Blanch

Pawlik, M. (2023). El injusto del ciudadano. Bogotá, Colombia: Externado

Santana Soriano, E. y Báez Vizcaíno, K. (2022). Ciberespacio y ciber mundo: delimitaciones conceptuales desde el materialismo sistémico. Ciencia y Sociedad, 47(1), 45-57.



Rodriguez Magariños, F. (2019). Universidad de Alicante. Obtenido de Sitio Web de la Universidad de Alicante-Sociología del Derecho: www.ua.ed.cr

Roxin, C. (1997). Derecho Penal. Parte General. Tomo I. Barcelona, España: Civitas.

Real Academia Española. (s.f.). Suplantar. En diccionario de la Real Academia Española. Recuperado de: <https://dle.rae.es/suplantar>