DELITO EN EL COMERCIO ELECTRÓNICO[1]

MARTÍN PECOY TAQUE[2]

1. INTRODUCCIÓN.

La compra y venta de productos o de servicios a través de medios electrónicos, ha sido desarrollado tremendamente en la última década, al punto de que principalmente se concentra en las ventas a través de Internet.

Mucho ha recorrido esta metodología desde aquellas primeras ventas por catálogo del siglo XIX, disminuyéndose los costos y prescindiéndose de intermediarios.

Acompañando estos avances técnicos, la delincuencia ha adoptado esta herramienta tecnológica, utilizándola como medio y objeto de actos ilícitos. Así, son básicamente cuatro conductas las que los Estados pretenden punir a nivel comparado: 1) estafa informática, 2) falsificación de documentos electrónicos, 3) publicidad engañosa, y 4) sustracción de datos personales.

2. ESTAFA INFORMÁTICA.

2.1. Incumplimientos contractuales y delito de estafa.

Cuando transcurren los plazos razonables, luego de que el consumidor pagó el precio, pero no recibió producto que compró, entonces se comienza a pensar en el ámbito penal.

Si se utilizan artilugios informáticos como herramientas para inducir en error a los internautas, cómodamente estos artificios se pueden interpretar como estratagemas, usados para inducir en error al usuario, y de esa manera el reato se percibe como estafa.

Los ejemplos más frecuentes en la red son los siguientes:

- Felicitaciones usted es el visitante 1.000.000. Haga click aquí para cobrar su premio.
- Usted ha ganado el nuevo Iphone 4 en nuestro sorteo mensual. Haga click aquí para cobrar su premio.

Pero existen modalidades en que el engaño no recae sobre la persona física, por lo que la estafa es inaplicable. Tal es el caso de la Denegación de Servicio de Nombres de Dominio, porque es al sistema al que se le hace caer en error. El sujeto ha modificado de tal manera los códigos del sitio web, que logra desviar al internauta a un sitio web distinto de aquel que tecleó.

Pero atención en este punto, porque nos ponemos de acuerdo en castigar estos engaños en páginas web, y, sin embargo, ni se nos pasa por la cabeza cómo calificaremos la conducta de las empresas que con ataques de saturación bloquean un sitio web, como supuesta defensa válida ante aquellas páginas donde se publican obras protegidas por derechos de autor.

¿Allí no hay afectación de bien jurídico? ¿No se asemeja esa conducta a una justicia por la propia mano[3] porque "puede recurrir a la autoridad"? El Uruguay se debe este debate.

---

1 Fragmento de la Ponencia presentada en las 12as. Jornadas Académicas del Instituto de Derecho Informático, "Comercio Electrónico", el día 16 de junio de 2011, en el Salón de Actos Torre Ejecutiva, Presidencia de la República, Plaza Independencia, con el apoyo de la Fundación de Cultura Universitaria.

2 Profesor de Derecho Penal en la Universidad de Montevideo. Profesor de Postgrado en Derecho Penal Económico en la Universidad de Montevideo.

3 Artículo 198 Código Penal: "El que, con el fin de ejercitar un derecho real o presunto, se hiciera justicia por su mano, con violencia en las personas o las cosas, en los casos en que puede recurrir a la autoridad, será castigado con 20 U.R. (veinte unidades reajustables) a 800 U.R. (ochocientas unidades reajustables) de multa.
Concurre la violencia en las cosas, cuando se daña, se transforma o se cambia su destino."

2.2. Phishing o simulación de identidad online.

Se trata de adquirir información confidencial en forma fraudulenta, duplicando la apariencia de sitios web para hacerse pasar por una entidad de confianza, y así solicitar al cliente la actualización de su información.

Se han observado tres formas de phishing que podrían describirse de esta manera:

1. Copia idéntica de un sitio web y solicitud de autenticación o actualización de datos (cambio de nombres del sitio original para que sean similares, o uso de rutinas de *javascript* para que se apliquen al abrir el sitio original, sobrescribiendo la dirección real en la del sitio web simulado).
2. *Spoofing* o ataque homógrafo (el nombre de dominio es muy similar al original, por ejemplo cambiando la letra "I" por el número "1", una diferencia casi imperceptible para el usuario).
3. Lavado de dinero a través de ofertas de trabajo en casa con alta rentabilidad (se ofrece en Internet grandes sumas de dinero a quien identifique su número de cuenta para el pago).

Muchas de estas conductas pueden ser perfeccionadas utilizando virus informáticos, que generen ventanas de autenticación ficticias, a partir de las cuales se engaña al usuario para que revele su información.

Nótese aquí que resultaría aplicable en parte el tipo del artículo 297 del Código Penal uruguayo[4], siempre que se obstruya una comunicación vía mail[5], con la utilización de los virus (o incluso spam), en cuyo caso se habrá incurrido en el delito por utilizar los virus como "artificio" (todo lo cual es un desarrollo en aplicación de la interpretación extensiva del tipo[6]).

Doctrina, doctrina y más doctrina, pero el castigo penal sólo se justifica cuando una ley previa, estricta y escrita prevé la conducta como delito.

La tipificación de estas conductas es necesaria para algunos, y de hecho varias jurisdicciones proceden en tal sentido, pero preferimos mantener una postura restrictiva, conforme la cual ello no es recomendable, porque contar con la información sin hacer uso de ella es un acto preparatorio, o, según el caso, un acto ilícito pero completamente atípico para el Derecho Penal (no delictivo).

3. FALSIFICACIÓN DE DOCUMENTOS ELECTRÓNICOS.

La doctrina comparada entiende que existen hipótesis de falsificación que se traducen en suplantación de identidad, aún cuando ni siquiera se han presentado físicamente los documentos, ya que alcanza con la mera introducción de números en un formulario, y se destaca que, por ejemplo, la utilización -en Estados Unidos- del número de seguro social como documento de identificación, dá lugar a que quien tenga ese número y el nombre de la persona a que corresponde, entonces podría conseguir un provecho económico en perjuicio ajeno.[7] En buen romance, eso significa que comprar por Internet indicando el número de seguro social ajeno, sería una falsificación.

4 "Artículo 297 (Interceptación de noticia, telegráfica o telefónica). El que, valiéndose de artificios, intercepta una comunicación telegráfica o telefónica, la impide o la interrumpe, será castigado con multa de 20 U.R. (veinte unidades reajustables) a 400 U.R. (cuatrocientas unidades reajustables)."

5 Así lo ha entendido LANGON. Ver LANGON CUÑARRO, Miguel *"Código Penal y Leyes penales complementarias de la República Oriental del Uruguay"*, Tomo II, volumen II, Editorial Universidad de Montevideo, Montevideo, Uruguay, año 2005, página 191.

6 Que según CAIROLI "permite extender la palabra de la ley a situaciones que en principio parecen no estar comprendidas. Se trata de ampliar la palabra de la ley para captar su sentido, pero teniendo precaución de no franquear los límites y penetrar en la analogía, lo que sí estaría prohibido." Ver CAIROLI MARTINEZ, Milton. «*Es posible proteger penalmente el software*». Publicado en *"Protección jurídica del Software" Ciclo de conferencias organizado por el Instituto de Investigación jurídica "Centro Interamericano de Estudios Miradores"*. Fundación de Cultura Universitaria, Montevideo, 1992, página 31.

7 Ver FARALDO CABANA, Patricia. *"Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico"*. Publicado en la Revista de Derecho Penal y Criminología, 3ª. Época, Nº 3 (2010). Ver página 75: "el hecho de que en los Estados Unidos se utilice como dato identificativo fundamental el número de la seguridad social (SSN, Social Security number), que no nació con dicho propósito, sino para mantener un adecuado registro de las ganancias, careciendo de sistemas de seguridad adecuados, da lugar a que sea relativamente fácil hacerse pasar por otro simplemente contando con ese número. Por ej., acompañado de la fecha de nacimiento propia y de la madre basta para abrir una cuenta bancaria que se puede usar para blanquear cheques."

En nuestro país, y dado que el documento electrónico tiene la misma validez que el formato papel (ver Ley 18.600 y el reenvío que realiza el inciso segundo de su artículo 48), se puede aplicar sin inconvenientes a los casos de falsedades cometidas en el comercio electrónico, los tipos penales de falsificación de documentos regulados en el Código Penal uruguayo, en sus artículos 236 a 245.

Ahora bien, al igual que sucede en otros países, "La presentación de un documento de identidad, sea material o electrónico, auténtico pero perteneciente a otra persona para hacerse pasar por ella en el tráfico jurídico-económico no recibe sanción en nuestro Ordenamiento jurídico."[9]

El Código Penal uruguayo cuenta con la figura de Uso de un documento o de un certificado falso, público o privado (artículo 243[10]), pero se trata de un delito que resulta aplicable cuando se verifica el presupuesto de la falsificación, por lo que no es una conducta delictiva introducir el número de documento de identidad ajeno en un formulario web, puesto que no es un actuar precedido de una contrafacción.

4. PUBLICIDAD ENGAÑOSA.

Existen jurisdicciones que punen algunas formas de publicidad engañosa como una modalidad de competencia desleal, tal es el caso de la Ley federal contra la competencia desleal en Suiza, que en su artículo 23 castiga con pena de reclusión o de multa a quien realiza alegaciones falsas o susceptibles a inducir a error sobre su empresa, denominación comercial, artículos, productos o prestaciones, la cantidad disponible o sus relaciones comerciales, o favorece de modo análogo a terceros en la competencia.[11]

Países como Brasil[12] y Japón[13], o Argentina[14] y Canadá[15], castigan los actos anticompetitivos incluso con penas de reclusión. Otros, como Estados Unidos[16], castigan a las empresas con multa y a las personas físicas con prisión

¿Qué es la publicidad engañosa? Para poner negro sobre blanco podemos decir que es hablar mal de la competencia, injuriarla. Hablar mal de la competencia no es, entre nosotros, un nuevo delito informático si se lo hace en la página web desde la que se desarrolla el comercio electrónico, sino que se trata de injurias, puras y simples injurias, castigadas por el artículo 334[17] del Código Penal uruguayo.

Uruguay no prevé un delito de publicidad engañosa, rigiendo la disposición del artículo 24 de la Ley 17.250 que prohíbe la publicidad engañosa, pero no establece un delito para su persecución, dejándose en manos del Área Defensa del Consumidor la potestad sancionatoria en esta materia (artículo 45).

---

8 "Artículo 4. (Efectos legales de los documentos electrónicos).- Los documentos electrónicos satisfacen el requerimiento de escritura y tendrán el mismo valor y efectos jurídicos que los documentos escritos, salvo las excepciones legalmente consagradas.
El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento electrónico, incurrirá en los delitos previstos por los artículos 236 a 245 del Código Penal, según corresponda."

9 FARALDO CABANA, Patricia. Ob. Cit. *"Suplantación de identidad..."* página 38.

10 Artículo 243 (*Uso de un documento o de un certificado falso, público o privado*). "El que, sin haber participado en la falsificación, hiciere uso de un documento o de un certificado, público o privado, será castigado con la cuarta parte a la mitad de la pena establecida para el respectivo delito."

11 JAVATO MARTÍN, Antonio Ma. "La tutela penal del consumidor en el comercio electrónico en el derecho suizo." Publicado en la Revista Electrónica de Ciencia Penal y Criminología, 2005, página 5.

12 Ley 8884/1994 prevé sanciones de multa (artículos 20, 21, 23 y 24). Ver el texto de la ley en el sitio web del Sistema de Información sobre Comercio Exterior de OEA: http://www.sice.oas.org/compol/natleg/Brazil/8884.asp.

13 Ley 47/1993 y 116/1994 (artículo 13), que establece el castigo con multas y prisión con máximo tres años de reclusión. Ver el texto de la ley en el sitio web de la Organización Mundial de la Propiedad Intelectual: http://www.wipo.int/wipolex/es/text.jsp?file_id=128343.

14 Ley 25.156/1999 determina penas de multa e inhabilitación para ejercer el comercio (artículos 46 a 51). Ver el texto de la ley en el sitio web del Sistema de Información sobre Comercio Exterior de OEA: http://www.sice.oas.org/compol/natleg/Argent/25156.asp.

15 Competition Act de 1985 (Capítulo 34 Parte VI), que establece el castigo con prisión desde un año hasta cinco de reclusión, para una gran gama de conductas que van desde conspiración hasta doble facturación. Ver el texto de la ley en el sitio web del Sistema de Información sobre Comercio Exterior de OEA: http://www.sice.oas.org/compol/natleg/Canada/cpact4.asp#PART VI.

16 **Ley Sherman Antitrust Act (15 U.S.C. Secciones 1-7), modificada por la Antitrust Criminal Penalty Enhancement** and Reform Act de 2004.

17 Artículo 334 (Injurias). "El que fuera de los casos previstos en el artículo precedente, ofendiere de cualquier manera, con palabras, escritos o hechos, el honor, la rectitud o el decoro de una persona, será castigado con pena de tres a dieciocho meses de prisión o multa de 60 U.R. (sesenta unidades reajustables) a 400 U.R. (cuatrocientas unidades reajustables)."

No obstante, en nuestro país, al igual que en otros regímenes jurídicos[18], la protección del consumidor respecto de la publicidad engañosa, se traduce en normas que reprimen el uso fraudulento de las marcas registradas (tal como ocurre con el artículo 83 de la Ley 17.011, que castiga la fabricación, almacenamiento, distribución o comercialización de mercaderías con marcas falsificadas).

5. SUSTRACCIÓN DE DATOS PERSONALES.

En este punto, podemos decir que el descuido de los usuarios propicia gran parte de las conductas reprobadas, ya que los usuarios de Internet no suelen utilizar prácticas de navegación segura, como el bloqueo "*in private*", o la verificación de que siempre acceden a direcciones precedidas de las letras "http".

Aquí, la brecha digital resulta una gran fuente de vulnerabilidad en el comercio electrónico, porque ha sido explosiva la generación de nuevas tecnologías, y exponencial el desarrollo de las prestaciones que brinda la electrónica.

No resulta extraño entonces que la conducta más común, en cuanto a la protección de datos en el comercio electrónico, sea el robo de identidad.

Para la doctrina comparada no resulta dificultoso el encuadre de esa conducta como delito de estafa, ya que luego de obtenidos los datos personales de un individuo, se procede a realizar toda clase de operaciones para provecho del victimario, fingiendo ser la persona a la que se le extrajo su información sensible.

Sin embargo, otra es la consideración jurisprudencial que se observa en Derecho comparado, aún en los regímenes jurídicos que cuentan con una tipificación específica de la estafa informática. Tal es el caso de España, el artículo 248-2 de su Código Penal y la Sentencia del Juez del Juzgado de Lo Penal número 3 de Málaga (19 de diciembre de 2005),[19] en que se absuelve a quienes realizaron una compra por Internet indicando, como medio de pago, un número de tarjeta de crédito ajena, porque no se verifica una "alteración, supresión u ocultación de datos existentes en el sistema", ni tampoco "manipulaciones efectuadas no en los datos sino en la configuración del programa", y principalmente porque "al ser inidóneo el engaño no cabe hablar de delito de estafa."

Ahora bien, si el actuar del sujeto activo comporta dar a conocer datos personales ajenos contenidos en bases de datos a las que por su empleo tiene acceso, entonces por expreso mandato legal la figura aplicable es la revelación de secreto profesional (artículo 11 inciso 2º[20] de la Ley 18.331).

Las nuevas tecnologías aplicadas a Internet permiten hoy, en 2011, que pequeños archivos, llamados *cookies* o galletas informáticas, guarden información temporal sobre los sitios web que un determinado usuario del computador ha visitado, y, en algunos casos, existen empresas que comercializan estos archivos, ya que constituyen información muy codiciada sobre la popularidad de los emprendimientos comerciales.[21]

Esto significa una clara vulneración a la intimidad de las personas, que ningún Estado se encuentra en condiciones de perseguir, dada la globalizada economía que gobierna estas cuestiones.

Pero cuidado: esta situación de emergencia no habilita a ampliar el poder punitivo porque ello equivale a volver a soluciones del medioevo (ampliar las facultades investigativas, facilitar el proceso penal a costo de garantías del imputado).

---

18 Ver MUSCO, Enzo. "Perfiles penales de la publicidad engañosa", página 4, artículo publicado en el sitio http://www.cienciaspenales.net (descarga efectuada el día 24 de mayo de 2011).

19 Publicada en el sitio web http://www.bufetalmeida.com/155/compra-por-internet-mediante-tarjeta-de-credito-ajena-inexistencia-de-delito.html (descarga efectuada el día 2 de mayo de 2010).

20 "Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no será de aplicación en los casos de orden de la Justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular.".

21 Ver RUIZ MIGUEL, Carlos. "Protección de datos personales y comercio electrónico", página 4, publicado en el sitio http://www.estig.ipbeja.pt/~ac_direito/e~com.pdf de la Universidad de Santiago de Compostela. Al respecto el autor señala: "En efecto, la utilización de la red para la realización de una operación de comercio electrónico permite obtener ciertas informaciones del sujeto sin su consentimiento y sin que esté acreditada su necesidad y proporcionalidad. Me estoy refiriendo, por ejemplo, a la posibilidad de introducir unos archivos llamados "cookies" o gallegas informáticas al visitar un determinado sitio. La función de estos archivos es registrar cada visita a un determinado sitio en la red; si una misma empresa se encarga de transferir "cookies" a los visitantes de las páginas de diversas empresas, la misma puede recolectar una información valiosa acerca de qué páginas son más visitadas por ese usuario, dándose la posibilidad de crear perfiles de los usuarios de la red."

Simples conductas del internauta pueden invalidar todo intento de robo de datos, verbigracia la acción de borrar los *cookies* y archivos temporales del navegador o programa informático que se utilice para acceder a Internet.

Por tanto, este es otro terreno en el que no resulta necesaria la creación de nuevos delitos, porque con adecuada prevención e información se logran evitar las conductas reprochadas.

6. CONCLUSIONES.

Nadie explica la realidad en palabras simples, nadie muestra cómo prevenirse. A nadie parece serle rentable aclarar que existen programas informáticos gratuitos disponibles, para prevenirse de casi todos los abusos en Internet (en el portal español INTECO[22] -Instituto Nacional de Tecnologías de la Comunicación S.A.- se pueden descargar -sin costo- herramientas Antiespías, Anti-Keylogger, Antiphising, Anti-spam, Antivirus, de Control Parental, Cortafuegos y Gestor de contraseñas, entre otros).

Vencer los ataques cibernéticos es un trabajo del ciudadano, antes que un asunto necesitado de modificaciones legales o jurídico-penales.

Uno de los principales motivos para ello, entiendo que es la enorme cifra negra de la criminalidad informática, porque las estadísticas usualmente son equívocas, y los estudios existentes carecen de rigor científico[23]:

- No se conoce la frecuencia real de delitos, porque no interesa y no se mide (los números que se comunican provienen de integrantes del sistema penal, y por tanto tienen una visión compartimentada de la realidad a la que le falta objetividad).
- No existen muchos estudios criminológicos serios en este sentido, sino datos de agencias que intentan justificar las tendencias del momento, pero cuidándose de no afectar los intereses de las poderosas empresas, las cuales, a su vez, temen denunciar los delitos porque se perjudicaría su buen nombre al conocerse que fueron víctimas.
- La mayoría de los números provienen de empresas privadas que se dedican al negocio del monitoreo e investigación digital.

Estoy convencido de que el fundamento del Derecho Penal es constitucional.

Entonces debemos tener siempre en mente las disposiciones constitucionales para interpretar los casos, porque el modelo de país que pautaron los constituyentes es el de una nación liberal. No en vano, el artículo 10 de la Carta Magna expresa que "Las acciones privadas de las personas que de ningún modo atacan el orden público ni perjudican a un tercero, están exentas de la autoridad de los magistrados. Ningún habitante de la República será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe."

La situación concreta del Comercio Electrónico exige revisar la Constitución, para controlar que no existan supuestos prohibidos de prisión por deudas (artículo 52 inc. 2 de la Constitución[24]), o hipótesis de prisión por incumplimiento de obligación contractual (artículo 11[25] del Pacto Internacional de Derechos Civiles y Políticos, ratificado por Ley 13.751/1969, y artículo 7 N° 7[26] del Pacto de San José de Costa Rica, ratificado por Ley 15.737/1985).

22 Sitio web www.inteco.es.

23 Ver SAN JUAN, César; VOZMEDIANO, Laura y VERGARA, Anabel, "*Miedo al delito en contextos digitales: un estudio con población urbana*", publicado en la revista del Instituto Vasco de Criminología, http://www.ivac.ehu.es (descarga efectuada el día 19 de abril de 2011). En la página 13 los autores expresan a este respecto que "pocos investigadores se han ocupado del estudio científico del temor a los ciber-delitos. Sí se han realizado trabajos sobre las estimaciones de riesgo de ser víctimas de un delito al realizar compras por Internet, que principalmente han visto la luz en revistas de comunicaciones y tecnologías de la información. Trabajos similares, orientados a cuantificar los efectos de las percepciones de los usuarios en los negocios realizados a través de Internet, han sido llevados a cabo por parte de empresas consultoras o bien por empresas que trabajan directamente en la venta on-line. Los resultados de estos trabajos se divulgan principalmente en prensa o portales especializados, pero a menudo no es posible acceder al trabajo completo para conocer los detalles del estudio, como podríamos hacer en una publicación científica."

24 "Nadie podrá ser privado de su libertad por deudas."

25 "Nadie será encarcelado por el solo hecho de no poder cumplir una obligación contractual."

26 "Nadie será detenido por deudas. Este principio no limita los mandatos de autoridad judicial competente dictados por incumplimientos de deberes alimentarios."

BIBLIOGRAFÍA:

CAIROLI MARTINEZ, Milton. "Es posible proteger penalmente el software". Publicado en "Protección jurídica del Software" Ciclo de conferencias organizado por el Instituto de Investigación jurídica "Centro Interamericano de Estudios Miradores". Fundación de Cultura Universitaria, Montevideo, 1992.

FARALDO CABANA, Patricia. "Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico". Publicado en la Revista de Derecho Penal y Criminología, 3ª. Época, Nº 3, 2010.

JAVATO MARTÍN, Antonio Ma. "La tutela penal del consumidor en el comercio electrónico en el derecho suizo." Publicado en la Revista Electrónica de Ciencia Penal y Criminología, 2005.

LANGON CUÑARRO, Miguel "Código Penal y Leyes penales complementarias de la República Oriental del Uruguay", Tomo II, volumen II, Editorial Universidad de Montevideo, Montevideo, Uruguay, 2005.

MONTANO, Pedro. "Documento Informático. ¿Falsificaciones electrónicas?". Publicado en Revista del INUDEP, año VIII, Nº 10, editorial Amario Fernández AMF, 1989.

MUSCO, Enzo. "Perfiles penales de la publicidad engañosa", artículo publicado en el sitio http://www.cienciaspenales.net, Revista Nº 12, 2009 (descarga efectuada el día 24 de mayo de 2011).

RUIZ MIGUEL, Carlos. "Protección de datos personales y comercio electrónico", artículo publicado en el sitio http://www.estig.ipbeja.pt/~ac_direito/e~com.pdf de la Universidad de Santiago de Compostela (descarga efectuada el día 15 de junio de 2011).

SAN JUAN, César; VOZMEDIANO, Laura y VERGARA, Anabel, "Miedo al delito en contextos digitales: un estudio con población urbana", publicado en la revista del Instituto Vasco de Criminología, Eguzkilore: Cuaderno del Instituto Vasco de Criminología, ISSN 0210-9700, Nº. 23, 2009, http://www.ivac.ehu.es (descarga efectuada el día 19 de abril de 2011).