§ 14
DELITOS DE FALSIFICACIÓN DE DOCUMENTOS

I
Delitos de falsificación de documentos y delitos informáticos*

Sumario: **1.** Introducción. **2.** Delito informático. **3.** Sucesión temporal de normas. **4.** Delito de fraude informático. **5.** Delito de falsificación de documentos privados. **6.** Delito de falsedad genérica.

1. Introducción

La realidad supera con frecuencia la imaginación. Por lo que resulta de mucho interés el analizar algunas situaciones desde la perspectiva del derecho penal. Son hechos que quizás nunca sean objeto de un pronunciamiento judicial, pero no dejan de tener consecuencias en el contexto en el que se presentan. Habiendo tenido ocasión de pronunciarnos sobre un caso parecido al que describimos en seguida, nos parece provechoso compartir algunas de las consideraciones que tratamos. Claro está, sin la pretensión de creer que las interpretaciones realizadas son siempre correctas o las únicas posibles.

* Versión elaborada en base de un informe jurídico relativo a: Informe sobre delito informático, falsedad documental, administración fraudulenta de personas jurídicas, defraudación genérica, Lima, octubre 2014.

Los hechos pueden ser resumidos, aunque de manera incompleta, como sigue: por la lectura de una serie de mensajes electrónicos, se constató que uno de los técnicos de la sección Informática ingresó, utilizando una clave perteneciente a un tercero, en la base de datos de la compañía y eliminó un documento digitalizado concerniente a un contrato de trabajo, reemplazándolo por otro en el que se había insertado cláusulas de penalidad inexistentes en el documento destruido.

En base del nuevo documento incorporado, se solicitó el pago de las penalidades indebidas. Las mismas que fueron canceladas por la compañía agraviada. Los representantes de esta al enterarse de la falsificación de documentos, debido a una copia fotostática simple del documento reemplazado, y de la manipulación de la base de datos informáticos denunciaron los hechos.

Estos hechos aparecen como una operación organizada y planeada por quienes se favorecerían económicamente. En la que intervinieron quienes elaboraron el documento digitalizado con las cláusulas de penalidad, penetraron en la base de datos y manipularon los documentos informatizados, así como quienes exigieron el pago de dichas penalidades en su favor.

Mediante este procedimiento global y fraudulento, comprende, de esta manera, diversas acciones parciales de relevancia penal: la elaboración de contratos de locación de servicios falsos; el acceso indebido a una base de datos informática; la alteración de esta base de datos mediante la supresión de datos informáticos y la inserción de otros nuevos, y los requerimientos maliciosos de que se hagan efectivas las cláusulas de penalidad.

2. Delito informático

Para comprender mejor en qué consisten los delitos informáticos de acuerdo con nuestra legislación, conviene tener en cuenta la evolución legislativa de su regulación en nuestro país. De acuerdo con el texto original del artículo 207-A, se reprimía a quien:

> "[U]tiliza o **ingresa** indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, **acceder** o copiar **información** en tránsito o **contenida en una base de datos**, será reprimido con pena privativa de libertad no mayor de 2 años o con prestación de servicios comunitarios de 52 a 104 jornadas".

El hecho de introducirse en una base de datos, utilizando una clave que no está autorizado a emplear, realiza el tipo legal objetivo y es de índole contraria al

orden jurídico (por actuar contra la voluntad del derechohabiente). El término "acceder" no debe ser comprendido en el sentido de "entrar en un lugar", ya que implicaría entenderlo como si expresara lo mismo que "ingresar" (que es el verbo utilizado para indicar una de las formas del comportamiento delictuoso, "[e]l que [...] ingresa indebidamente a una base de datos"). "Acceder" debe, entonces, ser interpretado en el sentido de "llegar o alcanzar a conocer información"[1], contenida en datos informáticos. El autor se introduce en el sistema, penetra burlando las seguridades previstas por el titular del sistema. El comportamiento delictuoso es realizado cuando no existen más barreras informáticas que podrían seriamente impedirle tomar conocimiento de los datos informáticos[2].

Lo mismo hace con el tipo legal subjetivo, en la medida en que obra con dolo y la finalidad de suprimir y substituir datos informáticos, que debió ubicar y reconocer en la base de datos. Por lo que, necesariamente, tenía el propósito de "acceder" a la información, uno de los objetivos indicados en el artículo 207-A (propósito de "interferir, interceptar, **acceder** o copiar información en tránsito o contenida en una base de datos").

Si el autor obra "con el fin de obtener un beneficio económico", incurre en la agravante del segundo párrafo del artículo 207-A:

> "Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de 3 años o con prestación de servicios comunitarios no menor de 104 jornadas".

De conformidad con el artículo 207-B:

> "El que utiliza, **ingresa** o interfiere indebidamente una **base de datos**, sistema, red o programa de computadoras o cualquier parte de la misma **con el fin de alterarlos**, dañarlos o **destruirlos**, será reprimido con pena privativa de libertad no menor de 3 ni mayor de 5 años y con 70 a 90 días multa".

---

1 Ver: Suárez-Mira Rodríguez, Carlos; Judel Prieto, Ángel y José Ramón Piñol Rodríguez, *Delincuencia informática. Tiempos de cautela y amparo*, Aranzadi, Navarra, 2012, pp. 170 y 171. Ver: Meek Neira, Michael, *Delito informático y cadena de custodia,* Universidad Sergio Arboleda, Bogotá, 2013, p. 80. Son interesantes los comentarios de este autor, pues trata de la legislación colombiana (artículo 269 CP) en la que el delito de acceso abusivo es descrito utilizando el verbo "acceder" y no ingresar.

2 Hurtado Pozo, José, *Droit pénal. Partie spéciale*, Schulthess, Zurich, § 36, N.º 1062, p. 319. Cfr. Meek Neira, Michael, *Delito informático y cadena de custodia,* cit., p. 81.

El tipo legal es realizado cuando: (i) se ejecuta uno de los comportamientos mencionados en el tipo legal; (ii) el objeto sobre el que se actúa es "una base de datos" y (iii) se tiene el propósito específico de alterar, dañar o destruir los datos (dice el texto legal, con el "fin de alterarlos, dañarlos o destruirlos [...]"). El móvil puede ser doble, por un lado, "acceder a la información" (artículo 207-A) y, por otro, "alterar la base de datos suprimiendo datos informáticos" (artículo 207-B). El hecho que estas sean efectivamente suprimidas (en el contexto determinado por la ley entonces vigente) solo hubiera implicado que hubiera incurrido en una circunstancia que debería tenerse en cuenta al individualizar la pena, pero no para tipificar el comportamiento.

Así mismo, puede considerarse que incurrió, en la medida en que aprovechó la situación que tenía en la empresa para obtener la clave o usuario electrónico de un tercero, en la circunstancia agravante prevista en el artículo 207-C, inciso 1:

> "En los casos de los artículos 207-A y 207-B, la pena será privativa de libertad no menor de 5 ni mayor de 7 años, cuando:
>
> 1) El agente accede a una base de datos, sistema o red de computadora, haciendo **uso de información privilegiada, obtenida en función a su cargo**".

Sea que se consideren las formas simples o agravadas, debería por tanto aplicarse el artículo 207-B por presentarse, en principio, un concurso aparente, en el que la forma más grave del comportamiento consume la más leve (prevista en el artículo 207-A), de acuerdo con las penas estatuidas en estas disposiciones.

3. Sucesión temporal de normas

Los artículos 207-A, 207-B y 207-C, incorporados en el Código Penal mediante la Ley N.º 27309 (del 17 de julio de 2000), fueron derogados por la Ley de Delitos Informáticos, Ley N.º 30096 (del 22 de octubre de 2013), por lo que corresponde evaluar si, para efectos del presente caso, esta modificación legislativa constituye una descriminalización de los comportamientos típicos previstos en los artículos derogados.

Al respecto es de considerar que, al mismo tiempo, la Ley N.º 30096, en su artículo 2, prescribió:

> "El que accede sin autorización a todo o parte de un **sistema informático**, siempre que se realice con vulneración de medidas de seguridad

> establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de 1 ni mayor de 4 años y con 30 a 90 días multa.
>
> Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado."

Esta disposición reprime el hecho de acceder o ingresar a un sistema informático, el mismo que comprende siempre una base de datos. Si bien difiere formalmente del texto del artículo 207-A, para los efectos del presente caso, las diferencias carecen de significación esencial en la medida en que, por un lado, el verbo "acceder" comprende el hecho de "ingresar" previsto en la disposición derogada y que la expresión "sistema informático" abarca la de "base de datos"[3] (así como las otras mencionadas en el artículo 207-A). Y, por otro, que la referencia, contenida en el artículo 2, a que el agente obre "sin autorización" corresponde a la de "indebidamente" empleada en el artículo derogado.

El artículo 2 fue luego modificado por la Ley N.º 30171. La nueva versión de esta disposición, dice:

> "El que **deliberada e ilegítimamente** accede sin autorización a todo o parte de un **sistema informático**, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.
>
> Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado".

El único cambio es que se introduce la expresión: el que "deliberada e ilegítimamente accede". El término "ilegítimamente" debe ser interpretado en el sentido de que, al menos de manera estricta, el autor actúe "indebidamente", "sin autorización", como se decía en las dos versiones modificadas, respectivamente. La expresión "deliberada" precisa el elemento esencial del tipo legal subjetivo, pues en dos de las disposiciones no se hacía expresamente referencia al dolo, en función de que el artículo 14 CP prevé que se reprimen solo las infracciones

3 La Convención del Consejo de Europa sobre Delincuencia Informática o Convención de Budapest (del 23 de noviembre de 2001) señala que "datos informáticos son toda representación de hechos, informaciones o conceptos expresados bajo una forma tratable informáticamente, incluido el programa destinado a hacer que un sistema informático ejecute una función". Cfr. Morales García, Óscar, "Delincuencia informática. Problemas de responsabilidad", en *Cuadernos de Derecho Judicial*, IX, CGPJ, Madrid, 2002, p. 307.

dolosas (salvo que la ley disponga expresamente también la represión a título de culpa). Por tanto, con el término "deliberadamente" solo se excluye la posibilidad de admitir el dolo eventual, que no entra en consideración en este caso.

Para completar el análisis, se debe tomar en cuenta que en la Ley N.º 30096 se preveía un artículo 3. Según esta disposición:

> "El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de 3 ni mayor de 6 años y con 80 a 120 días-multa".

Esta regla fue modificada mediante la Ley N.º 30171, en el sentido siguiente:

> "El que deliberada e ilegítimamente, daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de la libertad no menor de 3 ni mayor de 6 años y con 80 a 120 días multa".

La interpretación de esta disposición, en relación con los hechos resumidos en la introducción de este análisis, es bastante complicada. Se presentan, por lo menos, dos posibles maneras de comprender su sentido.

Mediante la primera, se puede considerar que el comportamiento también se subsumiría dentro de este tipo legal debido a que, "borró" o "suprimió" el contrato de trabajo ("datos informáticos"). Con este fin accedió a la base de datos en la cual estos fueron tratados o salvaguardados (objetos del delito). Debido a la imprecisión del texto legal, cabría comprender que es indiferente que el agente esté autorizado a acceder a la base de datos o que se introduzca de manera indebida. Sin embargo, en consideración a que se fija el medio que debe utilizar ("a través de las tecnologías de la información o de la comunicación"), debe ser interpretada restrictivamente en el sentido que el acceso tiene que ser indebido, sea porque el agente se excede en el uso de la autorización que detenta o recurre a medios y procedimientos indebidos.

En este sentido, se podría argumentar que las diferencias formales que distinguen este dispositivo del artículo 207-B, para los efectos del presente caso, no son tampoco de significación esencial. Por un lado, porque el verbo típico "alterar" de la nueva ley supone tanto la conducta típica "ingresar" y "el fin de alterarlos" que es el propósito con el que debe actuar el agente, previstos en la disposición derogada.

Por otro, la expresión "a través de tecnologías de la información o de la comunicación" abarca la de "base de datos" (así como el sistema, red o programa de computadoras, mencionadas en el artículo 207-B). Tal es así que la doctrina especializada sostiene que las tecnologías de la información o de la comunicación (TIC) son "los modernos desarrollos que tienen por objeto el tratamiento de información en forma automatizada, tanto en su recolección como en su acceso, uso, consulta o difusión"[4], y que estas permiten "el tratamiento, procesamiento, almacenamiento y transferencia de la información y los datos que la representan, tanto desde la perspectiva de los soportes físicos (*hardware*) como lógicos (*software*)"[5]. Es patente que el concepto de TIC incorporado en la Ley N.º 30096 abarca sin duda la referencia a "base de datos" que previó la norma derogada.

Además, se puede también alegar que el citado artículo 3 hace referencia a la expresión "datos informáticos" no utilizada en el artículo 207-B, de acuerdo con la definición contenida en la Convención de Budapest, citada anteriormente[6]. Definición que abarca el concepto "base de datos" al que se refiere el artículo 207-B. En suma, la conducta imputada al procesado podría subsumirse en el artículo 3 de la Ley N.º 30096 por lo que la derogación del artículo 207-B no implica la descriminalización de los hechos imputados contra esta persona.

En relación con la modificatoria del artículo 3 (llevada a cabo mediante la Ley N.º 30171) se podría afirmar, *mutatis mutandis* lo mismo en relación con la expresión "datos informáticos" (definidos por la Convención de Budapest) prevista en la Ley N.º 30096. Así mismo, el que la frase "a través de tecnologías de la información o de la comunicación" no exista más en el texto modificado, no tiene relevancia para la subsunción.

---

4 Palazzi, Pablo, *Delitos informáticos*, Ad Hoc, Buenos Aires, 2000, p. 235.

5 Rovira del Canto, Enrique, "Tratamiento penal sustantivo de la falsificación informática", en López Ortega, Juan (dir.), *Internet y derecho penal,* Cuadernos de Derecho Judicial, N.º X, CGPJ, Madrid, 2001, p. 477. En el mismo sentido sostiene Romeo Casabona: "Las nuevas tecnologías de la información y de la comunicación (TIC) han ido incorporándose a lo largo de las últimas décadas en la vida social con el efecto de favorecer un más eficaz tratamiento y gestión de la información" (Romeo Casabona, Carlos, *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Comares, Granada, 2006, p. XI); así también, Francisco Pinochet: "Las tecnologías de la información, al permitir un manejo rápido y eficiente de gran cantidad de datos, facilitan el almacenamiento automático de estos" (Pinochet Cantwell, Francisco, *El derecho de internet,* Editorial de Derecho de Chile, Santiago, 2006, p. 305).

6 Ver, n. 3.

El término "ilegítimamente" del artículo 3 (conforme a lo expuesto con relación al artículo 2 de la Ley N.º 30171) abarca sin duda una actuación efectuada "indebidamente", como la calificaba el derogado artículo 207-B. Lo mismo se predica de la expresión "sin autorización" que se encuentra comprendida, a su vez, por el término "indebido" que se utilizó en la ley derogada. Así mismo, con la palabra "deliberada" del texto modificatorio, no contenida ni en el artículo 207-B ni en la Ley N.º 30096, el legislador se ha referido al tipo subjetivo. De forma tal que con dicha expresión, conforme a lo ya sostenido, solo se precisa la exclusión de admitirse la tipicidad subjetiva de dolo eventual.

Finalmente, el elemento que diferencia al artículo 207-B, vigente en el momento de los hechos, en relación con las dos versiones del artículo 3 de la Ley de Delitos Informáticos es el del propósito con el que debe actuar el agente. En el texto derogado, se establecía "con el fin de alterarlos, dañarlos o destruirlos". Con lo que se restringía su campo de aplicación. En el artículo 3, por el contrario, la conducta reprimida es el hecho de quien "deliberada e ilegítimamente [...] altera [...] datos informáticos". Por lo que debería comprenderse que este comportamiento equivale al de "ingresar indebidamente a una base de datos con el fin de alterarla". Lo que permitiría afirmar que el comportamiento imputado es conforme a esta disposición, en la medida en que ingresó a la base de datos y alteró datos informáticos suprimiendo los documentos PDF de los contratos de locación de servicios.

Mediante la segunda posibilidad de comprender los hechos y el texto legal, aún admitiendo en gran parte lo afirmado respecto a la primera posible interpretación, se puede contraargumentar objetando, justamente, lo sostenido en el párrafo precedente. La argumentación allí desarrollada es incorrecta por ser analógica, por lo que va más allá del posible sentido del lenguaje utilizado para describir los comportamientos incriminados. No es lo mismo o análogo decir que se actúa con "el propósito de alterar" que afirmar que se debe "alterar" (hecho y no simple deseo o móvil).

De modo que la diferencia, últimamente indicada, entre el artículo 207-B con las dos versiones del artículo 3 es sustancial debido a que se refiere al comportamiento mismo que es tipificado. En el primero, se trata de un delito formal o de pura actividad consistente en "acceder" y, subjetivamente, caracterizado por el propósito con el que debe actuar el agente: "con el fin de alterarlos, dañarlos o destruirlos". Mientras que en el artículo 3, se trata de un delito de resultado. El agente no solo debe introducirse en el sistema informático con dicha finalidad, sino que debe realmente dañar, introducir, borrar, deteriorar, suprimir o hacer inaccesibles datos informáticos.

Esto no solo implica que se restringe el campo de aplicación del artículo 207-B, sino que el artículo 3 estatuiría un nuevo tipo legal, al describir un comportamiento que no estaba previsto en el momento en el que se cometió el hecho delictivo. Entonces se sancionaba solo el acceso indebido a una base de datos informáticos.

Debe preferirse la segunda interpretación por ser más favorable a todo posible procesado. Por lo que el hecho de haber suprimido e introducido datos informáticos constituye un hecho ilícito (contrario al orden jurídico) pero atípico respecto al artículo 3 y, por tanto, penalmente irrelevante. Esta deficiencia legislativa no debía ser corregida mediante el razonamiento analógico o cualquier otro medio interpretativo incompatible con el principio de la legalidad. Para reprimir ese comportamiento (alterar datos informáticos) era necesario que se dictara un nuevo tipo legal, como se hizo con el artículo 3 comentado.

En todo caso, si se compara los márgenes de pena establecidos en las disposiciones en conflicto, hay que admitir que la aplicación de los artículos 2 y 3 es menos favorable que la de los artículos 207-A y 207-B (pena privativa de libertad no mayor de 2 años o con prestación de servicios comunitarios de 52 a 104 jornadas). Esto aun cuando se aplique la circunstancia agravante prevista en el segundo párrafo del artículo 270-A: "Si el agente actuó con el fin de obtener un beneficio económico" (pena privativa de libertad no mayor de 3 años o con prestación de servicios comunitarios no menor de 104 jornadas).

4. Delito de fraude informático

En la Ley N.º 30096, se integró una nueva disposición (artículo 8) para reprimir ciertos casos que la doctrina, generalmente, denomina fraude informático. Comete este delito:

> "El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de 3 ni mayor de 8 años y con 120 días-multa".

El legislador precisó esta disposición mediante la Ley N.º 30171 incorporando, por un lado, el elemento subjetivo "deliberadamente", que califica la intencionalidad con la que debe actuar al agente (requisito que se presuponía en el texto original, de acuerdo con el artículo 12 CP) y, por otro, la referencia a la ilicitud del comportamiento. Así, se dispone:

> "El que **deliberada e ilegítimamente** procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de 3 ni mayor de 8 años y con 120 días-multa".

La previsión de esta disposición fue indispensable ante la imposibilidad de reprimir el comportamiento descrito aplicando los artículos referentes a los fraudes y, en especial, a la estafa (artículo 196 CP). De esta manera, el legislador prefirió, en lugar de ampliar simplemente el artículo 196, elaborar una nueva figura delictiva para tener en cuenta las peculiaridades de las nuevas formas del comportamiento delictuoso[7].

El fraude informático tiene, debido a sus orígenes, relaciones estrechas con la estafa, en la medida en que consiste en procurar para sí o para terceros un provecho ilícito. Se diferencian respecto a los recursos fraudulentos utilizados. En la estafa, por ejemplo, el engaño, la astucia, el ardid, mientras que en el fraude informático se trata de manipulación del sistema informático. Aunque se asemejan nuevamente en que los actos fraudulentos deben causar el acto de disposición patrimonial de parte de la víctima y el perjuicio correlativo[8].

La supresión de los datos correspondientes al contrato de trabajo original y su reemplazo por la versión informática del contrato falsificado (escaneados y tratados en el sistema informático), implica haber introducido, borrado y suprimido "datos informáticos". Comportamiento comprendido en el artículo 8. Esto se habría realizado "a través de las tecnologías de la información o de la comunicación".

Sin embargo, esta acción es tan solo el medio por el cual el agente debe realizar la acción indicada por el verbo típico principal. En este caso, el **procurar** "para sí o para otro un provecho ilícito en perjuicio de tercero". Este enriquecimiento indebido debe ser originado, provocado por el hecho de manipular los datos informáticos de la manera indicada en el tipo legal. Lo que debe comportar que el agente cree o aumente un riesgo indebido y que el resultado, obtener para sí o para otro un enriquecimiento indebido, sea la concretización de ese riesgo no autorizado o tolerado.

---

7 Pica, Giorgio, *Diritto penale delle tecnologie informatiche*, UTET, Torino, 1999, pp. 139 y s.

8 Cfr. Pecorella, Giorgio, *Diritto penale delle tecnologie informatiche*, UTET, Torino, 1999, pp. 49 y s. Pica, *Diritto penale delle tecnologie informatiche,* cit., p. 144.

En consideración de la diferencia destacada entre el artículo 8 y el artículo 196, hay que subrayar, en consecuencia, que el provecho ilícito con que se benefician les resulta de la exigencia formal que hicieron para que se hagan efectivas las penalidades establecidas en los contratos fraudulentos y que no figuraban en los contratos originales. De modo que se trataría más bien de una estafa. Pues, dicha ventaja patrimonial no se debe a las manipulaciones de los datos informáticos. Por lo que no procede imputárseles objetivamente la realización del tipo legal previsto en el artículo 8.

En cuanto a la imputación subjetiva, si bien es evidente que se ha obrado con consciencia y voluntad, en grado de dolo directo ("deliberadamente", excluyente del dolo eventual), la intencionalidad estaba dirigida solo a vulnerar y alterar los datos informáticos de modo ilícito. Al mismo tiempo, se sabía que el comportamiento no era apropiado para producir directamente un beneficio patrimonial a favor de sí mismo o de Dyer, en el sentido del tipo legal.

5. Delito de falsificación de documentos privados

Para calificar los hechos descritos es de recurrir, en principio, al artículo 427 CP:

> "El que hace, en todo o en parte, un documento falso o adultera uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho, con el propósito de utilizar el documento, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de 2 ni mayor de 10 años y con 30 a 90 días-multa si se trata de un documento público, registro público, título auténtico o cualquier otro trasmisible por endoso o al portador y con pena privativa de libertad no menor de 2 ni mayor de 4 años, y con 180 a 365 días-multa, si se trata de un documento privado".

El hacer en todo o en parte un documento[9] es el comportamiento típico que debe tomarse en consideración. El autor, mediante la creación de un documento, comete una falsedad material o una falsedad ideológica (reprimida de

9 Según el Tribunal Constitucional, en "líneas generales un documento puede ser definido como aquel escrito en el que constan datos o se recoge información de tipo fidedigna, la cual puede ser utilizada con la intención de probar algún hecho", STC EXP. N.º 03742-2007-PHC/TC PUNO.

manera agravada, en caso tratarse de un documento público). Para esto, imita un documento preexistente o elabora uno conforme a su propia imaginación.

Se crea un documento falso cuando una persona fabrica un documento cuyo autor real no coincide con el autor aparente. La falsedad intelectual consiste en el establecimiento de un documento por parte de su autor aparente, pero que es engañoso debido a que su contenido no corresponde a la realidad[10].

Si se toma como referencia el contrato original, en nuestro caso, este no es alterado ni mutilado en su contenido. Más bien se crea uno a su semejanza y en el que se inserta una nueva cláusula conteniendo la penalidad. Documento adulterado que luego es utilizado, una vez informatizado, para reemplazar la versión original en la base de datos.

Debido a que el nuevo contrato es firmado por las mismas personas que suscribieron la primera versión, podría considerarse que no se altera el "origen del documento", pues se aparenta que procede de quien lo había establecido. Sin embargo, la modificación de la presentación de la realidad radica en que quien suscribe y asume las obligaciones del contrato original son los representantes de la compañía, mientras que el documento creado con posterioridad es firmado por personas naturales sin actuar en el nombre de la empresa. Esta diferencia normativa no cambia por el hecho de que los firmantes sean físicamente las mismas personas. Además, se falsea también el contenido o sentido de los documentos, al alterarse, al hacerse pasar por verdadero, lo estatuido en las cláusulas penales que no figuraban en los contratos originales.

Justamente, respecto a las personas jurídicas y debido a que la voluntad de estas se manifiesta mediante sus órganos, es indispensable tener en cuenta que si personas (por ejemplo, empleados) no autorizados a comprometerla establecen y suscriben un documento falso como si emanara de la persona jurídica, crean un documento falso[11].

El documento creado por los imputados dio origen a pretensiones jurídicas indebidas, sirvió para probar un hecho y fue realizado con el propósito de utilizarlo (para probar la exigencia de que se pague como penalidad un monto por el cambio de propietario de la empresa). De esta manera, se vulneraba la expectativa de los participantes en el sistema del tráfico jurídico de bienes y servicios de que los documentos sirvan de prueba de la existencia de obligaciones y

10 Schubarth, Martin, "Zur Auslegung der Urkundendelikte", en *RPS*, N.º 113, 1995, pp. 387 y ss.

11 Lackner, Karl, *Strafgesetzbuch*, 21ª ed., Munich, 1995, § 267, N.º 19.

derechos. El procedimiento recuerda al hecho de suplantar o completar datos en un documento original "para que aparezcan en una fotocopia a ser legalizada"[12]. En el caso analizado, se hace aparecer una cláusula inexistente en el original para presentarla como verdadera, al insertar el documento falsificado como dato informatizado en la base de datos violada indebidamente.

6. Delito de falsedad genérica

La argumentación precedente parte de la hipótesis que existen físicamente tanto los documentos originales como los adulterados. De modo que, al compararlos directamente, sería posible establecer sus diferencias y semejanzas. Así, se constataría que no solo se imitó la versión original sino que se falseó su contenido. Vulnerándose, al mismo tiempo, la autenticidad y la veracidad de los documentos.

Sin embargo, el problema que se plantea es que solo existen copias de las versiones informatizadas del contrato, de modo que la comprobación del falseamiento realizado se realizaría utilizando solo las trazas informáticas de la manipulación de la base de datos, la versión digitalizada del documento falseado y las copias de los documentos originales.

En esta perspectiva, resulta difícil determinar cómo se procedió a "hacer los documentos falsos", pero queda en evidencia que de alguna manera se manipuló la base de datos donde habían sido archivados electrónicamente. Esto es, como "documentos informáticos", los cuales pueden ser definidos como representaciones "de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenado en un medio idóneo para permitir su uso posterior"[13]. Datos que pueden ser vistos y leídos con la ayuda de equipos especiales y reproducidos en copias impresas, esencialmente iguales al documento original. Respecto a los cuales se admite, en general, que solo se diferencian de los documentos en papel en cuanto a la corporeidad de los mismos[14]. Su valor ha sido reconocido de manera fragmentaria en diversos ámbitos mediante diversas

12 Cfr. SCS Exp. 253-95 Lima.

13 Pinochet Cantwell, *El derecho de internet,* cit., p. 423; Canelo, Carola; Raúl Arrieta; Rodrigo Moya y Rodrigo Romo, "El documento electrónico. Aspectos procesales", en *Revista Chilena de Derecho Informático*, N.º 4, Universidad de Chile, Santiago, pp. 85 y ss. Cfr. Bramont-Arias Torres, Luis, *El delito informático en el Código Penal peruano*, Fondo editorial PUCP, Lima, 1997, pp. 427, 429 y ss.

14 Aguilar Cabrera, Daniel, *Valor probatorio y efectos legales del documento informático*. Versión en línea: http://bit.ly/1EV3QlG.

disposiciones legales[15]. Una referencia importante es el artículo 234 del Código Procesal Civil, según el cual:

> "Son documentos los escritos públicos o privados, los impresos, fotocopias, fascímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de **soportes informáticos**, y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho, o una actividad humana o su resultado".

Documentos que si bien no caen del todo en la noción de documento implícita en el artículo 427, sí pueden sin embargo ser utilizados para cometer falsedad "simulando, suponiendo, alterando la verdad". Comportamiento previsto en el artículo 438 CP:

> "El que de cualquier otro modo que no esté especificado en los Capítulos precedentes, comete falsedad simulando, suponiendo, alterando la verdad intencionalmente y con perjuicio de terceros, por palabras, hechos o usurpando nombre, calidad o empleo que no le corresponde, suponiendo viva a una persona fallecida o que no ha existido o viceversa, será reprimido con pena privativa de libertad no menor de 2 ni mayor de 4 años [...]"[16].

15 La Ley de Títulos Valores (Ley N.º 27287), en su artículo 2 en su inciso 2.1, regula los valores desmaterializados. El Decreto Legislativo N.º 681, valida el uso de tecnologías avanzadas en materia de micrograbación. Además, en su capítulo V, artículo 14, prevé que las empresas de derecho privado pueden organizar sus archivos mediante las tecnologías de las microformas. El Decreto Legislativo N.º 702 y el Decreto Ley N.º 26095 (y su Reglamento) incluyen dentro de la legislación de telecomunicaciones los documentos electrónicos. El Decreto Legislativo N.º 773 (que aprueba el Nuevo Código Tributario), reconoce expresamente las normas vigentes sobre efectos legales y valor probatorio de las microformas que incluyen documentos informáticos.

16 Disposición que, con ciertas variaciones de redacción, reproduce lo dispuesto en el artículo 227 CP de 1863. Respecto al cual, José Viterbo Arias, después de indicar que "nuestro Código y el argentino, entre los que estudiamos, son los únicos que contienen esta disposición subsidiaria", enumeraba a título de ejemplo una serie de casos en los que era aplicable. Además, justificaba la manera en que el legislador buscaba evitar "vacíos", diciendo que lo había hecho "por ser imposible prever la multitud de formas que la mala fe puede tomar". Su mantenimiento en el Código vigente se explica mejor si se considera que permite abarcar las nuevas y modernas formas de describir y constatar hechos en diversos tipos de documentos.

La penetración indebida en la base de datos, la manipulación de los documentos informáticos (hechos comprobados con las "huellas" constatadas) y la existencia de una versión de los contratos originales (sin cláusula de penalidad), muestran que se ha buscado presentar una versión de la realidad que no es la "verdadera". Esta falsedad no es una simple mentira inocua, sino que tiene efectos jurídicos y patrimoniales semejantes a los que se producen mediante la falsedad de documentos previstos en el artículo 427 CP.

El documento verdadero, en su versión electrónica, ha sido sustraído, destruido y no imitado o alterado. De esta manera, se ha impedido "la prueba de la verdad que puede ser verificada por el propio documento, cuya presencia hubiera llevado a distinta conclusión"[17]. Se provoca una apreciación, un juicio, equivocados "de la situación de hecho que el documento probaría"[18]. Esta manera de falsear la verdad (delito de falsedad genérica) constituye una forma especial de falsedad situada entre la falsedad material y la ideológica[19].

Debido a que no es comprendida por ninguna de las disposiciones que reprimen la "falsificación de documentos en general" (Título XIX Delitos contra la fe pública del Libro Segundo del CP), se debe afirmar que los investigados han incurrido en "falsedad genérica", debido a que han recurrido a "otro modo" para falsear la representación de la "verdad" (artículo 438 CP).

Esta disposición prevé un tipo legal "residual" de los delitos contra la fe pública, denominado en la doctrina como tipo legal "de recuperación" (*Auffangtatbestand o Aufgreiftatbestand*)[20]. Se trata de una disposición subsidiaria, cuyas condiciones son simplificadas, y que son aplicadas cuando el comportamiento del autor no está comprendido por la disposición penal principal. Las dificultades de prueba que implica la complejidad de esta última son aligeradas por la restricción de los elementos típicos del tipo legal de recuperación.

17 Donna, Edgardo Alberto, *Derecho penal. Parte especial*, Rubinzal Culzoni, Buenos Aires, 2004, t. IV, p. 245.

18 Molinario-Aguirre Obarrio, Alfredo, *Los delitos*, preparado y actualizado por Eduardo Aguirre Obarrio, Tea, Buenos Aires, 1999, t. III, p. 518.

19 Soler, Sebastian, *Derecho penal argentino*, cit., t. V, p. 155.

20 Tiedemann, Klaus, *Wirtschaftsstrafrecht* - EAT, 2014, pp. 190 y ss.