VIII Congreso Nacional de Topografía y Cartografía
TOPCART 2004

Madrid, 19-22 Octubre 2004

Un protocolo para protección contra piratería de mapas digitales utilizando marcas de agua

Carlos López[(1)]
[(1)] The Digital Map Ltda., carlos.lopez@thedigitalmap.com

RESUMEN

En muchos países la financiación del mantenimiento y creación de la cartografía digital se realiza en base a los ingresos por venta. Esta estrategia está hoy amenazada por la facilidad de copia disponible en equipos PC domésticos y por inadecuados medios de protección técnico-legal. Este trabajo analiza algunos aspectos asociados a la protección usando marcas de agua, técnica que consiste en insertar información invisible en un mapa identificando así al primer comprador legítimo. En particular, se describe una propuesta para el procedimiento que debe seguirse para generar pruebas válidas a ser presentadas en un reclamo ante los tribunales cualquiera sea la técnica de inserción de la marca utilizada.

1. INTRODUCCION.

La cartografía en formato digital (así como cualquier otro dato digital, geográfico o no) ha representado un salto significativo en muchos aspectos. Es fácil de mantener, editar, etc. así como conservar, todo lo cual es bien conocido. En particular, una vez producido el primer ejemplar con gran esfuerzo e inversión, es posible generar copias perfectas en cuestión de minutos, lo que desde el punto de vista del productor es un gran avance ya que baja drásticamente los costos de producción y distribución. No es necesario imprimir ni conservar por años ejemplares en papel, ni se está limitado para producir una versión actualizada al agotamiento del stock preexistente.

En medios analógicos, la costosa inversión inicial estaba indirectamente protegida contra copia por razones técnicas. Era harto difícil que un usuario individual tuviera acceso a imprentas apropiadas y mecanismos de copia de calidad suficiente para generar ejemplares piratas aceptables. Quien dispusiera de esos equipos, a lo sumo intentaría generar ejemplares nuevos para su venta al público general haciéndolo aparecer como propios. Se dice que en este caso se trata de una piratería de *Autoría*. La mayor parte de la legislación de derechos de autor considera (implícitamente) este problema como el principal a atender.

Los avances tecnológicos (en particular, el PC doméstico, la Internet y el copiador de CD) hacen hoy viable la piratería de *Propiedad.* En este caso, el poseedor del ejemplar pirata no niega ni oculta al creador original del dato, pero como no vende el ejemplar que posee no infringe automáticamente muchas de las leyes existentes. Es más: en muchos países y también en tratados internacionales la mera posesión de un ejemplar ilegal no constituye un delito, ya que está amparada por conceptos diseñados para atender el caso de organismos educativos, investigadores, etc. Desde un punto de vista legal, es una zona con muchos grises a la hora de intentar hacer un juicio al *poseedor* del ejemplar ilegal.

La solución (legal) que existe al respecto es señalarle explícitamente a los compradores que no deben permitir la realización de copias del dato recibido más allá de lo acordado en el contrato firmado al momento de la transacción. Este procedimiento es estándar, y a diferencia de lo mencionado anteriormente, su valor no reside en el derecho de autor sino en el derecho comercial común como cualquier otro contrato. A diferencia del derecho de autor, este cuerpo legal es bastante más homogéneo entre los diferentes países, y ello explica lo popular de su adopción por los organismos cartográficos y productores de datos en particular.

Lo que los contratos no logran resolver es cómo, una vez identificado que el pirata Pedro tiene un ejemplar que (se sospecha) fue vendido por la productora del dato Alicia originalmente al cliente legítimo Benito, sea posible recurrir a los tribunales y lograr que haya una sentencia que le obligue a compensar al productor. El dilema al que se enfrenta el juez Juan (y que por cierto, Luis el abogado de Benito se ha encargado de señalar) es que el ejemplar en manos de Pedro pudo haber venido de su cliente, pero también de cualquier otro de los clientes que el productor ha tenido para ese mapa. En la medida que el procedimiento productivo y de distribución hace que todos sean idénticos, no es posible probar (ni presumir) la culpabilidad de Benito, aunque Pedro sea un ex-empleado despedido en malos términos por Benito. En términos legales, el contrato es, a estos efectos, *letra muerta*. Siguiendo la práctica corriente en criptografía se utilizarán en lo sucesivo nombres propios (Alicia, Benito, Luis, etc.) para cada rol.

La tecnología de las marcas de agua digitales intenta resolver este problema. En esencia, lo que logra es insertar una marca o número de serie invisible en el archivo digital, de forma que sobreviva en las copias que del mismo se hacen. Cada cliente legítimo recibe un ejemplar único, aunque indistinguible de otros para muchos efectos, derivado

VIII Congreso Nacional de Topografía y Cartografía
TOPCART 2004

Madrid, 19-22 Octubre 2004

del mismo juego de datos. Una vez encontrado un ejemplar pirata en manos de Pedro, se analiza el archivo buscando la presencia de ese número de serie que, ahora *inequívocamente*, identificaría a Benito como la fuente de ese ejemplar. Este trabajo apunta a describir qué debe hacerse para lograr efectivamente agregar el adjetivo *inequívocamente* a la frase anterior.

Existe una relación entre tres aspectos cruciales del problema de la protección que se denominarán *tecnología*, *leyes* y *protocolos* que es ilustrada en la *Figura 1*. Con esto se espera enfatizar que, si bien interesante para los tecnólogos, la tecnología del *cómo* se inserta la marca de agua es sólo un aspecto del problema. Para ponerlo más claro: si la ley no persigue al infractor, poco podrá hacerse con esta tecnología. El otro aspecto que aparece indicado con la torre defensiva se ha denominado como protocolo, y ése es el tópico de este trabajo. Protocolo es el nombre técnico que se le da a las diferentes etapas del procedimiento de inserción, independientemente de la técnica de marcas de agua que se utilice. Un pirata decidido e informado necesitará violar alguno de los aspectos; se basará en la ausencia de legislación o en la imposibilidad práctica de aplicarla, en fallas del protocolo o en fallas de la tecnología. A estas acciones se las denomina colectivamente *Ataques*, y los más frecuentes son ataques puros a la tecnología (intentar borrar o alterar la marca) y puros al protocolo (generar una duda razonable). Además, hay ataques compuestos al protocolo que sólo son exitosos cuando se inserta la marca con ciertas tecnologías, y no con otras.

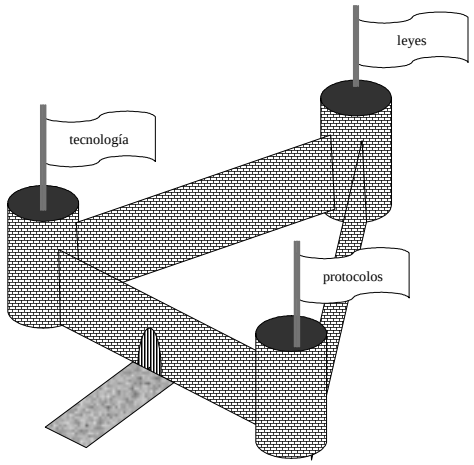

Figura 1.- Esquema ilustrativo de la relación entre leyes, tecnología y protocolos a los efectos de la protección.

En el capítulo 2 se tratará brevemente la tecnología; en el 3 se verán los aspectos legales, viéndose cómo la legislación de derechos de autor limita las posibles acciones a tomar en estos casos. El tema de Protocolos será tratado al detalle en el capítulo 4, presentándose una propuesta al respecto. Para finalizar, se encuentran las conclusiones y referencias

2. LA TÉCNICA DE LAS MARCAS DE AGUA.

La ciencia que estudia el cómo transmitir información secreta sin levantar sospechas se denomina Esteganografía. No es una ciencia nueva; pueden rastrearse antecedentes incluso entre los antiguos griegos. Cox y Miller, (2002) recogen aplicaciones de los últimos 50 años, aunque la mayor parte de las aplicaciones digitales son posteriores a 1994. La abrumadora mayoría de los trabajos se centran en imágenes (i.e. archivos raster), audio, video y luego en mucho menor medida se abordan los casos de los textos, bases de datos, software etc. En lo que a mapas digitales se refiere existen muy pocos trabajos; el de López, (2002) trata el tema en forma general para el caso vectorial y sería el punto de arranque recomendado para quien quiera comenzar con el tema. Para mapas en formato raster hay técnicas especiales curiosamente también utilizadas para dibujos animados ya que ambos casos se caracterizan por tener regiones de coloración uniforme separadas por fronteras nítidas. No es la única posibilidad; por ejemplo Barni *et al.* (2001) modifican detalles del producto cartográfico mismo (textos, etc.) para codificar la marca misma.

Las diferentes posibilidades y técnicas que se abren son ilimitadas en principio. Para los fines que se persiguen, las técnicas a utilizar deben tener algunas propiedades:

- no alterar en forma perceptible el mapa original.
- resistir a manipulaciones legítimas de los usuarios normales, como cambio de proyección, cambio de formato, ediciones menores, etc.
- permitir insertar varias marcas simultánea o sucesivamente
- ser independiente del formato (DXF, DGN, TIFF, etc.) en que se representen los datos

También serían útiles algunas otras propiedades:

- sobrevivir en la versión impresa
- no ser necesario acceder al archivo original, sin marcas, para detectar la misma

La lista de requerimientos puede por cierto ampliarse. Estas propiedades limitan sensiblemente las posibles soluciones. En el pasado, y para la protección de la *Autoría,* se ha recurrido también al truco de insertar deliberadamente errores en el mapa. Si alguien reimprime y vende el mapa como propio ese error estará aún incluído en el ejemplar. Esta solución es viable pero limitada al caso en que todos los ejemplares son idénticos; parece poco práctico generar errores diferentes para cada cliente. Además el producir información deliberadamente errónea puede tener otras consecuencias no deseadas para el productor (incluso legales).

Nótese que ningún mapa digital tiene, en principio, un mercado de miles o millones de compradores. Es por ello que es factible solicitar una identificación completa a cada uno de ellos al momento de la compra (así como la firma de un contrato de adhesión) y generar instancias diferentes para cada uno de ellos. Esto no es posible en otros problemas de piratería, como ser la música o los videos, en los que el comprador original rara vez será identificado.

La técnica de las marcas de agua podría utilizarse en principio para otros fines, como por ejemplo, probar la integridad de los datos. Dado que este trabajo no tiene por objetivo abundar en la técnica misma, se remite al lector a las referencias citadas.

3. EL MARCO LEGAL PARA LA PROTECCIÓN CONTRA LA PIRATERÍA.

La legislación aplicable en un país es, en ese orden, la legislación internacional refrendada por el estado y luego la legislación propia. En el ámbito internacional, y en lo que a derecho de propiedad intelectual se refiere, están vigentes desde 1886 la convención de Berna y las sucesivas revisiones que le siguieron (Convenciones de París, Roma, etc.). Hoy ello se coordina y concentra en la Organización Mundial de Propiedad Intelectual (http://www.wipo.int) que es una fuente oficial de información sobre el tema.

La legislación internacional contempla el caso de mapas como un ejemplo más de obra artística, pero también permite excepciones a determinar por las legislaciones nacionales. En Argentina, por ejemplo, la ley de derechos de autor no menciona a los mapas explícitamente, lo que obliga al demandante en cada caso a gestionar ante el juez la inclusión por analogía con una obra artística.

Según algunos autores (Karjala, 1995) los mapas en particular y los SIG en general son un ejemplo de tensión entre conceptos legales. Los mapas tradicionales tienen una fuerte componente artística en la elección de colores, diseños, formas de interpretar la realidad, localización y orientación de los textos, etc. Eso hace único cada mapa, por lo que corresponde calificar al producto completo como una *obra artística.* Por otra parte, en el mapa en esencia están recogidos elementos que deberían existir en el terreno, y que (especialmente en ambientes SIG) deben ser representados de forma tal que sean geométricamente compatibles con otros mapas para la misma localización. Los elementos así incluídos en los mapas son *hechos* constatables en la realidad, y que (y aquí viene el problema) deberían ser los mismos que detectaría cualquier otro productor de un mapa para la misma zona. Los *hechos* están explícitamente excluídos de la protección de derechos de autor, ya que no hay aporte creativo en su recopilación.

En la legislación europea se ha introducido recientemente (**Directiva 1996/9/CE)** un concepto *sui generis* que, si bien similar en su aplicación al de derecho de autor, tiene una base diferente. La Directiva reconoce por primera vez la importancia de proteger las bases de datos en términos del esfuerzo no creativo requerido para su compilación, evitándole a los jueces malabarismos para aplicar conceptos concebidos para obras artísticas a productos que no lo son. Bajo esta legislación, los mapas (como colecciones de hechos) tienen una protección en muchos aspectos equivalente a la de una obra artística, lo que lo protege fundamentalmente contra la venta de ejemplares piratas. Desafortunadamente, esto no es suficiente, ya que hay rendijas por la que pueden colarse otros argumentos.

Un concepto legal relevante en el problema de la piratería es el conocido en inglés como *fair use* (sobre cuya traducción no hay un gran acuerdo; buscando en Internet se ha encontrado “uso justo”, “uso leal” e incluso “uso de buena fe”). En http://www.bibliotecasvirtuales.com/biblioteca/derechosdeautor/usoleal.asp hay una definición que dice:

La Legislación Estadounidense sobre Propiedad Intelectual (Title 17) introduce una cláusula (Fair Use Act: Title 17, Chapter 1, Section 107) sobre el uso adecuado o leal de material protegido que permite su reproducción para los fines de críticas, comentarios, reportajes noticiosos, educación o investigación sin que ello sea una violación del derecho de autor. Para determinar la aplicación de dicha cláusula se definen los cuatro criterios siguientes:

- *Propósito y carácter del uso, incluyendo si dicho uso es de naturaleza comercial o para fines educativos no lucrativos;*
- *La naturaleza del trabajo protegido que se reproduce;*
- *La cantidad y substancialidad de la porción reproducida en relación al trabajo protegido como un todo; y*
- *El efecto del uso sobre el valor o valor potencial de mercado del trabajo protegido*

Si bien aquí se cita en relación a la legislación estadounidense, el concepto es un paraguas que existe en otras legislaciones. Bajo el mismo es posible incluir una gran cantidad de situaciones que, violando el derecho de propiedad, inhiben o minimizan el reclamo que Alicia puede plantear ante Juan, pues se está a su criterio en relación al uso que le da Benito al producto. En opinión del autor, esto demuestra que la legislación está concebida para proteger al autor

contra la piratería de *autoría*, ya que contempla (bastantes) excepciones a los derechos de Alicia en el caso de *fair use*. Esto atenta directamente contra las aspiraciones de Alicia de perseguir exitosamente al pirata Pedro, restándole únicamente la posibilidad de reclamar frente a Benito por su desidia (si es que permitió que sus datos fueran copiados) o mala fe (ya que vendió o regaló aquello a lo que no estaba autorizado). Ése es el mecanismo propuesto en este trabajo.

4. PROTOCOLOS.

En este contexto se entiende por protocolo el conjunto de procedimientos que hacen posible la generación de conclusiones irrefutables. El hecho que se desea probar es que, dado un ejemplar pirata, el mismo es total o parcialmente derivado del original entregado a un cliente legítimo original que se denominará Benito. Se denominará como Alicia al productor de datos, y como Luis al abogado de Benito.

La literatura sobre protocolos es significativamente más escasa que sobre la tecnología. Como excepciones pueden citarse los trabajos de Gopalakrishnan et al. (1999), Lintian y Nahrstedt (1998) y Memon y Wong (1998). En el primero, los autores presentan un protocolo que actúa en la etapa de extracción de la marca. Usualmente, Nelson (quien es neutral entre Alicia y Benito y es quien inserta y conoce de marcas de agua) tendría que exhibir información suficiente para que un tercero pueda detectar la marca. Si bien ese tercero puede ser confiable, podría también ponerse de acuerdo con Benito y eliminar definitivamente la marca del mapa, quedando en condiciones de realizar copias ulteriores impunemente. La solución que plantean utiliza técnicas criptográficas para evitarlo, pero es válida sólo para técnicas de inserción de marcas que sean *aditivas* e *invertibles*, conceptos cuya descripción excede los objetivos de este trabajo.

Lintian y Nahrstedt (1998) señalan que la mayor parte de la literatura apunta a proteger los derechos de Alicia, pero no consideran los derechos que tiene David como legítimo comprador. En particular, David debería recibir garantías en relación a que su ejemplar no pudo haber sido entregado también a otro cliente (Benito), y luego ser acusado injustamente por las malas prácticas de Benito. Este aspecto está contemplado (al menos parcialmente) en el protocolo que se propone.

Memon y Wong (1998) proponen un protocolo para insertar la marca de forma tal que Alicia no pueda generar por sí sola el ejemplar que Benito recibió. Este aspecto está también contemplado en el protocolo que se describirá.

Luis el abogado es inteligente y conoce algo de tecnologías. La primer pregunta que Luis le formula al juez Juan es quién ha suministrado la prueba. Aunque parezca obvio, algunas instituciones cartográficas han comenzado a aplicar este tipo de tecnologías de marcas de agua para proteger sus datos, siendo ellas mismas quienes insertan las marcas de agua y quienes por lo tanto generan la prueba. En esos casos, y llegado a una corte, Luis argumentará que, disponiendo del mapa original, la tecnología y sabiendo que Benito ha comprado un ejemplar de ese mapa en particular, es trivial para Alicia acusar injustamente a su cliente como el pirata. El juez Juan no tiene más alternativa que aceptar ese sólido argumento, y por lo tanto desestimar cualquier reclamo de Alicia contra Benito (¡y contra cualquier otro!).

Nótese que no es necesario probar que Alicia miente; alcanza con que Luis logre introducir una duda razonable en Juan para que la demanda no se pueda sostener. De hecho, la duda razonable es lo que impide al presente iniciar un juicio por estos temas, ya que todos los ejemplares distribuidos por Alicia son (en principio) idénticos entre sí, por lo que cualquier cliente pudo haber sido el traidor. Incluso si sólo se ha vendido un único ejemplar de ese mapa (el que fue entregado a Benito), Luis puede argumentar que los empleados de Alicia estaban en condiciones de ser los piratas. Esta posibilidad debe ser evitada por el protocolo mismo, quizá en coordinación con la tecnología de inserción de marcas.

5. DESCRIPCIÓN DE UN POSIBLE PROTOCOLO.

Habiendo descrito aspectos generales del problema, corresponde ahora presentar la propuesta. Esta es sólo una posible; la solución de este problema no es única.

En esta propuesta, quien coloca la marca de agua no es Alicia sino Nelson. Cuando Benito se presenta en las oficinas de Alicia solicitando y pagando un ejemplar del mapa, Alicia se pone en contacto con Nelson y le comunica mediante una transacción segura:

1. El nombre del comprador (Benito), así como otros datos filiatorios
2. El nombre del mapa, su localización física en los servidores de Alicia y su firma digital
3. Datos de la transacción comercial (número de factura, fecha de compra, etc.)
4. Claves públicas de Alicia y Benito

Por clave pública se entiende un número (muy grande) que es solicitado a un proveedor especializado (público o privado) que entrega junto con ella otro número (también muy grande) que se denomina clave privada. Este sistema (conocido como PKI, Public Key Infrastructure) es usado extensivamente en comercio electrónico para muchos fines. Se remite al lector a Schneier (1995) por una referencia muy completa, aunque más adelante se mencionarán algunas propiedades del PKI relevantes para este protocolo.

Nótese que el mapa no es enviado a Nelson, sino sólo información sobre la transacción. Nelson recibe de Alicia un paquete firmado y encriptado por ella. Con el concurso de la clave pública de Alicia, él comprueba que el envío es legítimo y procede a abrirlo. Con la información incluída genera un número de serie que será inserto en el mapa a entregar a Benito, y que NO comunicará a Alicia. Le prepara entonces a Alicia un paquete firmado digitalmente que contiene una clave de activación para un software capaz de insertar únicamente ESE número de serie en ESE mapa que Alicia especificó. El software (que opera en los servidores de Alice) va al directorio señalado, comprueba que es el mapa correcto (ya que su firma coincide con la recibida de Nelson) y lo procesa insertando la marca. El archivo con marca es encriptado por ese programa con la clave pública de Benito, y firmado con la clave privada de Alicia. El resultado encriptado es enviado en forma segura a Benito.

Benito recibe entonces ese archivo, y con el concurso de la clave pública de Alicia confirma que es legítimo. Con su propia clave privada es capaz de abrirlo y recién en ese momento el archivo toma la forma familiar de un mapa digital con extensión DGN, DWG, etc. La marca de agua invisible está inserta en él, aunque Benito no lo note.

Nótese que Alicia nunca tuvo acceso al archivo DGN, DWG, etc. que Benito finalmente obtuvo ya que el software de inserción escribe un archivo encriptado. Tampoco conoce el número de serie insertado por Nelson, por lo que en caso de encontrarse un ejemplar pirata ella o sus empleados están libres de sospecha. Nelson nunca recibió el archivo completo, sino sólo la firma digital del mismo.

El protocolo también tiene que tener previsto qué se hace cuando se encuentra un ejemplar pirata. Alicia consigue un ejemplar digital (o, dependiendo de la tecnología, un ejemplar impreso o quizá localiza un servidor WEB que lo despliega) y se lo transmite a Nelson. Nelson procede a analizarlo, y comparar los números de serie de que dispone en su servidor contra los que contiene el mapa. Asúmase que se comprueba que el que está presente es el de Benito. Hasta este momento, la operación de rastreo e identificación transcurre sin conocimiento de Benito ni participación de Juan. Nelson le comunica sus hallazgos a Alicia, y ella se presenta ante Juan reclamando daños y perjuicios en base al contrato firmado entre ellos el cual fue debidamente registrado en su momento. La ley aplicable es la del derecho comercial en la sede de Alicia, y no la genérica de derechos de autor. Juan convoca a Nelson y a Benito, quien se presenta junto con Luis. En este caso, el carácter de independiente de Nelson (en relación a Alicia) lo habilitan para operar como perito. A pedido de Juan, Nelson repite el análisis sobre el ejemplar en cuestión y si confirma lo obtenido entonces Juan le pregunta a Luis si tiene objeciones en que falle a favor de Alicia en su litigio con Benito.

Las *Figuras 2 y 3* ilustran el proceso. En la *Figura 2* se ilustran con rectángulos las tres partes involucradas en el proceso de inserción. Tanto Alicia, como Benito y Nelson disponen de parejas de claves públicas y privadas, las que se ilustran como dos piezas de un rompecabezas. Ambas están en relación entre sí, y una de ellas permanece en el interior de la empresa mientras que otra está a la vista del público. El pedido se origina en Benito, quien envía a Alicia sus datos comerciales y especifica el mapa solicitado.

Alicia, con un software apropiado, envía el pedido a Nelson, quien recibe empaquetada la información de las claves públicas de Alicia y Benito, un texto conteniendo el nombre y datos del cliente, así como el nombre y la firma digital del mapa solicitado. Todo ello va firmado digitalmente por Alicia, lo que se omite en la figura ya que la caja se muestra abierta.

Nelson dispone de un banco de datos de clientes en el que guardará la información de la transacción. En particular, se guardará la marca o número de serie que insertará en el mapa de Benito. Ese no es realmente un número secuencial, sino sólo se requiere que sea único.

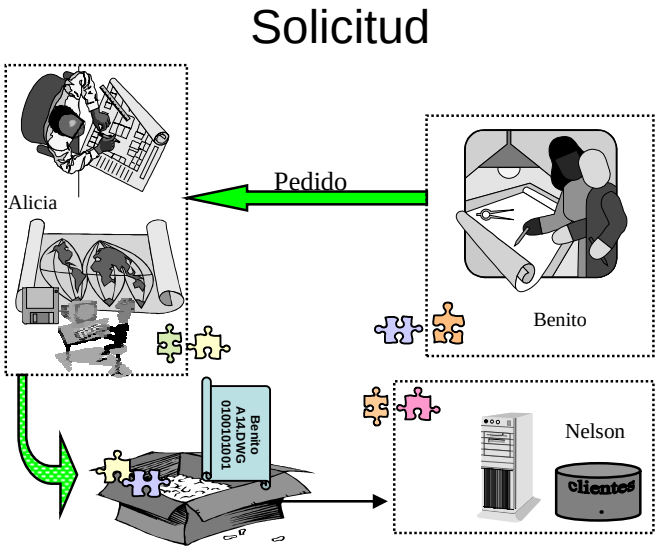

Figura 2.- Esquema de flujo de la solicitud. Con las dos piezas del rompecabezas fuera y dentro de la empresa se ha indicado el par clave pública/privada. La caja se muestra abierta, aunque en realidad está encriptada con la clave privada de Alicia.

VIII Congreso Nacional de Topografía y Cartografía
TOPCART 2004

Madrid, 19-22 Octubre 2004

La *Figura 3* ilustra las acciones posteriores. Nelson emite una clave de activación que es recibida por el programa que se está ejecutando en los servidores de Alicia. Ese programa verifica que el archivo a marcar coincide con el esperado, inserta la marca y con la clave pública de Benito genera un paquete encriptado y firmado por Alicia. El programa debe ser suministrado por Nelson, ya que tiene los algoritmos de inserción de la marca.

En el análisis del protocolo usualmente se excluyen hipótesis como la destrucción del banco de datos de Nelson, acuerdo entre Alicia y Nelson para perjudicar a Benito, etc. También se excluyen los ataques a la marca misma (en otras palabras, intentar borrarla o sustituirla por otra, etc.).

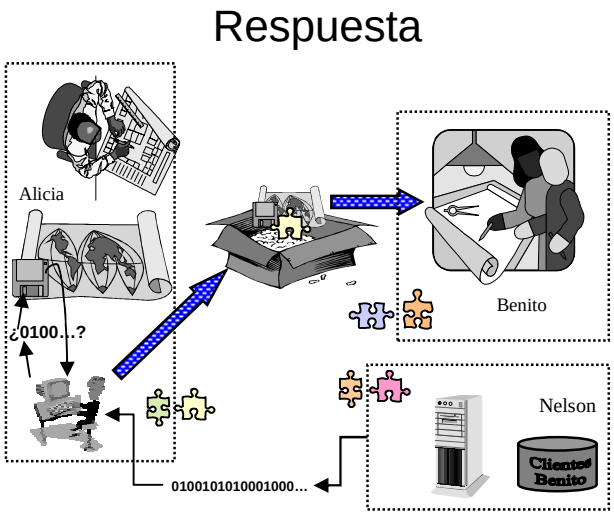

Figura 3.- Esquema de flujo de la respuesta. La caja se muestra abierta, pero está encriptada con la clave privada de Alicia. El mensaje binario está encriptado con la clave privada de Nelson.

6. ¿PORQUÉ ES ESTO TAN COMPLICADO?.

Los protocolos, la tecnología y las leyes apropiadas serán los que en definitiva protejan la inversión. Hay que contemplar por lo tanto todos los riesgos y posibilidades, ya sea para intentar mejorar la defensa como para estar al tanto de las limitaciones de la misma. No está de más señalar que todo sistema siempre tiene un punto débil, y sólo en unos pocos casos se puede demostrar (en criptografía) que un sistema es absolutamente seguro.

Si la intención es generar evidencia para Juan, deben contemplarse por adelantado las objeciones que pueda plantear Luis. Este artículo describe el protocolo en uso en The Digital Map Ltda. el cual se aplica con cualquiera de las tecnologías de marca de agua que se disponen (Bacci y López, 2003). Incluso podría continuar aplicándose con tecnologías nuevas que surjan en el futuro.

Las comunicaciones entre las partes se realizan utilizando la PKI, lográndose así dos propiedades importantes: a) la comunicación sólo puede ser leída por el destinatario correcto y b) el origen y autenticidad de la comunicación no puede ser repudiado.

Alicia no puede utilizar de nuevo la clave generada para Benito por Nelson con otro archivo que no sea el original; de eso se encarga el software que se le suministró. Si Alicia intenta cambiar el archivo por otro, la firma digital (función de hash) del nuevo no coincidirá con la del viejo y el software no funcionará. Si Alicia intenta generar una clave aleatoria el software notará que no fue generada por Nelson y tampoco funcionará. Si Alicia o un empleado infiel de ella logra información sobre el algoritmo de inserción de la marca podría hacer un programa que la inserte y presentarle a Benito el archivo resultante. Benito no puede notar nada raro ya que el mapa le viene legítimamente enviado por Alicia. Sin embargo, Alicia no puede lograr con este mecanismo que Benito figure en el banco de datos de Nelson por lo que éste deberá declarar que la marca no es conocida, liberando así a Benito de toda culpa y perjudicando obviamente a Alicia.

El archivo se entrega encriptado a Benito. La razón de ser de eso es eliminar la posibilidad que un empleado infiel de Alicia entregue otro ejemplar a Pedro el pirata. Ni Alicia ni su empleado tienen acceso a la clave privada de Benito, por lo que no podrán abrir el paquete encriptado para utilizar el archivo. En cambio, cualquier empleado infiel de Benito puede ver el archivo en la red interna de su empresa. Será en todo caso responsabilidad de Benito controlar esta posibilidad, por lo que siguen siendo válidos los términos del contrato que firmó con Alicia.

7. CONCLUSIONES.

La protección de la propiedad intelectual de la cartografía digital en particular, y de los datos geográficos en general, puede realizarse con una variedad de técnicas. Algunas intentan *impedir* la operación de copia, o el uso de los datos copiados. Otra estrategia es la de *inhibir* o *disuadir* a los legítimos propietarios de permitir la copia, por la vía de insertar información secreta en los archivos que hacen que los mismos sean únicos. Cada comprador recibe así un ejemplar diferente. Por razones obvias, las diferencias no deberían llevar a que un comprador genere un conjunto de datos derivados y que éste sea incompatible geométricamente para otro comprador. Los mapas y datos deberán ser por

lo tanto modificados en forma *imperceptible*, donde lo que se entiende por imperceptible puede depender del fin declarado al momento de la compra del plano.

El objetivo de la marca de agua es, por lo tanto, habilitar técnicamente a discernir entre diferentes orígenes de un mapa identificando así al cliente legítimo original. Sin embargo, la mera presencia de una marca de agua no alcanza para generar una prueba, ya que para ello debe seguirse un protocolo (procedimiento) que asocie inequívocamente el mapa con la marca con el cliente legítimo que lo recibió en primera instancia. Aunque parezca sorprendente, se sabe de algunos intentos de aplicar esta tecnología por parte de productores de datos insertando ellos mismos la marca de agua. En esos casos, el cliente acusado de piratería puede argumentar que el productor pudo (deliberada o accidentalmente) haber insertado la misma marca en el dato entregado otro cliente, argumento válido que será aceptado por un juez eximiéndole de culpa.

La aplicación del protocolo requiere la participación de autoridades emisoras de certificados (claves públicas y privadas). Eso es obligatorio para *todos* los compradores de datos, así como también para el productor. Es muy probable que muchos de esos clientes jamás hayan sentido hablar de esos certificados, y los consideren como una arbitrariedad del productor de datos. Si bien la solución de ese tipo de problemas de la vida real no es parte del protocolo, el plantear exigencias de este tipo tiene un obvio impacto en el comprador en relación a que los controles asociados a la copia ilegítima de esos datos ya no son lo que eran antes, y por lo tanto, funcionará desalentando a potenciales piratas. Que por cierto, es el objetivo último de todo el sistema.

8. AGRADECIMIENTOS.

La asistencia del autor a este evento ha sido financiada por el programa INFODEV del Banco Mundial en el marco del apoyo brindado a The Digital Map por INGENIO Incubadora de empresas LATU-ORT (www.ingenio.org.uy) lo cual se agradece.

9. REFERENCIAS.

Cox, I. J. and Miller, M. L. (2002): "The First 50 Years of Electronic Watermarking". EURASIP J. of Applied Signal Processing, 2, 126-132

López, C. (2002): "Watermarking of Digital Geospatial datasets: a review of Technical, Legal and Copyright issues", International Journal of Geographic Information Science, 16, 6, 589-607.

Bacci, A. and López, C. (2003): "Evaluation tests performed over a proposed anti-piracy system for digital vector datasets". Cambridge Conference, Cambridge, UK, 21-25th july

López, C. (2003): "Digital Rights Managements of Geo-Datasets: Protection against Map Piracy in the Digital Era". GIM International, 17, 2, 51-53

Barni, M.; Bartolini, F.; Piva, A. and Salucco, F. (2001): "Cartographic image watermarking using text-based normalization" Workshop on Multimedia Signal Processing, October 3-5, CANNES – FRANCE

Karjala, Dennis S. (1995): "Copyright in Electronic Maps". 35 Jurimetrics J. 395-415

Schneier, B. (1995): "Applied Cryptography: Protocols, Algorithms and Source Code in C". Juan Wiley & Sons, ISBN: 0471117099

Gopalakrishnan, K., Memon, N. and Vora, P. (1999): "Protocols for Watermark Verification". In Proceedings of the Multimedia and Security Workshop, GMD Report No. 85, Dec. 1999, 91—94

Lintian, Q. and Nahrstedt, K. (1998): "Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Rights. Journal of Visual Communication and Image Representation

Memon, N. and Wong, P. W. (1998): "A buyer-seller watermarking protocol". IEEE Signal Processing Society 1998 Workshop on Multimedia Signal Processing, December 7-9, Los Angeles, California, USA