LA CRIPTOGRAFÍA Y LA PROTECCIÓN A LA INFORMACIÓN DIGITAL

JHONNY ANTONIO PABÓN CADAVID*

"Las tecnologías de la encriptación constituyen el avance tecnológico más importante de los últimos mil años. Ningún otro descubrimiento tecnológico - desde las armas nucleares (espero) hasta Internet- tendrá un impacto más significativo en la vida social y política de la humanidad. La criptografía va a cambiar absolutamente todo".

LAWRENCE LESSIG.

I. DEFINICIÓN

La criptografía es la técnica utilizada para cifrar mensajes que contienen información, palabra que proviene del griego *Kryptos* y *Graphein*, que significan "escondido" y "escritura", respectivamente[1]; ha sido denominada también escritura secreta, ya que el cifrado supone un grado de secretitud para evitar el descifrado por personas ajenas a los receptores originales del mensaje.

La criptografía es parte de la criptología (del griego *Kriptos* = oculto y *Logos* = ciencia o estudio); la otra parte de la criptología es el criptoanálisis, el cual tiene como objeto el descifrado de la información procesada por algún criptosistema, es decir, que se encuentre cifrada.

Para autores como GALENDE DÍAZ (1995: 15), la actividad de criptoanálisis puede denominarse de dos formas, dependiendo si el que realiza la actividad es un destinatario legítimo o no; la primera sería el destinatario que de forma legítima hace el criptoanálisis, en donde el proceso a realizar se denominaría "descifrar";

* Abogado de la Universidad Externado de Colombia. Derecho de Internet y Tecnologías de la Información, Universidad de los Andes. Especialista en Derecho de la Competencia y del Consumo, Universidad Externado de Colombia. Estudiante de la Maestría en Historia, Pontificia Universidad Javeriana. Investigador del Departamento de Propiedad Intelectual, Universidad Externado de Colombia. E-mail: j4207732@hotmail.com

1. "El objeto de la criptografía no es ocultar la existencia de un mensaje, sino más bien ocultar su significado, un proceso que se conoce como codificación" (SGARRO, 1990: 20).

y la segunda que correspondería a un ataque o intrusión por parte de un usuario no autorizado, en este caso se denomina "descriptar". Aunque este uso lingüístico solo aparece por el autor en mención, parece conveniente generar esa distinción con el fin de expresar de forma sencilla si estamos ante un criptoanÁlisis legal o ilegal, en el uso común y frecuente, el tÉrmino que se usa es decriptar.

Algunos han considerado la criptografía como un arte[2], otros como una ciencia aplicada[3] o simplemente como una técnica. La definición de criptografía que nos da el Diccionario de la Real Academia Española es la siguiente: "Arte de escribir con clave secreta o de un modo enigmático". No entraré a esta discusión filosófica sobre la clasificación de la criptografía como ciencia o como arte, pero sí quiero resaltar cómo los usos que se le den pueden llevar a que este objeto de estudio sea llevado a tan diversas interpretaciones, y afirmaría que no podemos encasillar la criptografía dentro de ninguno de estos aspectos sino que dependerá del uso que se le dé y del conocimiento de la persona para determinar si está ante algo bello o simplemente ante algo práctico: así, un anagrama[4], que es una forma de criptografía por permutación y a la vez un estilo literario bien definido que podría dar como resultado un escrito artístico, mientras que un criptosistema como el DES definitivamente carecería de característica alguna para clasificarse como arte para una persona que careciera de conocimientos matemáticos, pero la matemática subyacente a este sistema puede resultar artística para una persona versada en la materia.

Hasta el surgimiento de los ordenadores modernos y del uso de sistemas binarios para las telecomunicaciones, la criptografía se basaba en una matemática relativamente elemental, en el conocimiento de alfabetos y sistemas de comunicación lo más seguros posibles, pero esta seguridad en los sistemas de comunicación, más que el desarrollo tecnológico de éstos, buscaba ardides para ocultar los mensajes. Ahora, la relación de la criptografía con múltiples áreas del conocimiento, como la teoría de la información[5], teoría de conjuntos, informática, la importancia de los números primos, las telecomunicaciones, hace que sea necesario para el desa-

2. Charles Babbage en su autobiografía escribiría que "descifrar es, en mi opinión, una de las artes más fascinantes" (Sgarro, Ob. cit.: 76): Si descifrar es un arte, ¿podríamos excluir el hecho de cifrar de este calificativo?

3. "Fue considerada un arte, hasta que Shannon publicó en 1949 la teoría de las comunicaciones secretas…entonces la criptografía empezó a ser considerada una ciencia aplicada, debido a su relación con otras ciencias…" (Caballero Gil, 1997. Segunda edición 2003: 1).

4. La autora alemana Unica Zurn, de corriente surrealista se especializo en la creación de anagramas como fuente principal de su obra artística; en su obra *Hexentexte* (textos de hechicera) podemos encontrar poemas de esta naturaleza. En palabras de ella, "Los anagramas son palabras y frases que se forman intercambiando letras de una palabra o frase. Solo pueden utilizarse las letras dadas, y no se debe recurrir a otras". Muchos autores también han utilizado esta técnica como forma para crear sus seudónimos a la hora de firmar sus obras, ejemplo de esto es Francois Rabelais quien, al publicar su obra maestra, *Gargantua y Pantagruel,* apareció bajo el anagrama de su nombre, alcofribas nasier.

5. En esta se busca transmitir el mensaje lo mejor posible, es decir que el receptor logre un mensaje lo más fiel posible, para lo cual habrá que evaluar el canal de transmisión del mensaje. Para más información ver Shannon, 1949: 656-715. Citado por Pino).

rrollo de criptosistemas robustos un estudio interdisciplinario, que más que nada necesita capital humano para su desarrollo, tanto para el criptoanálisis como para la criptografía.

Debemos diferenciar entre proceso de cifrado y codificación: un criptosistema sirve para realizar el cifrado de cualquier mensaje dentro del alfabeto que este construido, mientras que los códigos establecen una relación limitada dentro de cada asignación, así cada código está restringido al significado que se le haya establecido, funciona como un diccionario. Un uso muy frecuente del sistema de códigos es el utilizado en operaciones militares, en las que a cada sujeto se le establece un *nickname* que sirve de código, además, a cada una de las acciones se le coloca un código, así como a los objetivos y a los lugares geográficos y desplazamientos a realizar dentro de la operación; de esta forma, así intercepten la comunicación, los intrusos no podrán entender ya que carecen del significado del código. Otro uso muy frecuente de la codificación es en el correo diplomático. Aunque este sistema es muy seguro, ya que cuando se utilizan los códigos, éstos se asignan para utilizarlos por una sola vez (en el caso militar, para cada misión se asignan códigos diferentes), sus usos son muy restringidos, ya que su efectividad está basada en usos de baja frecuencia, es decir que se use una sola vez o muy pocas veces, ya que al utilizarlo con frecuencias altas pierde la seguridad, también la extensión de los mensajes esta limitado a las palabras o frases o ideas que previamente hayan sido codificadas y sean de conocimiento de los intervinentes en la comunicación[6].

II. BREVE HISTORIA DE LA CRIPTOGRAFÍA

la necesidad de transmitir un mensaje preservando la confidencialidad hizo que los medios para ocultar información se desarrollaran desde hace milenios; ante las precarias formas de transmitir la información, los gobiernos y los ejércitos utilizaban formas de comunicación bastante vulnerables a ser descubiertas, los primeros métodos que se utilizaron para asegurar la transmisión de mensajes fueron a través de la esteganografía, que proviene de las palabras griegas *steganos* y *graphein*, que significan respectivamente "encubierto" y "escribir" (SGARRO, Ob. cit.: 19), es decir, encubrimiento de la información, la ocultación. De los relatos más antiguos de los que se tiene noticia en los que se cuenta la utilización de estos métodos, es el de HERODOTO, en *Las Historias* narra que DEMARATO envió un mensaje a los espartanos para advertir de los peligros que representaba el plan de invasión del rey persa JERJES; la técnica que utilizó DEMARATO fue la ocultación con cera en

6. "Las principales desventajas del código cuando se utiliza como cifrado son: 1. Sólo se pueden transmitir aquellas palabras que tengan traducción asignada en el diccionario del código. 2. El receptor debe tener el diccionario para poder decodificar; es decir, el código completo constituye la clave. 3. Su implementación, sobre todo a la hora de cambiar el código, es muy costosa. 4. El criptoanálisis se puede basar en un análisis de frecuencias" seguridad informática, Pág. 10.

tablillas donde estaba inscrito el mensaje[7]. Otro relato importante del que se tiene memoria es cuando Histaiaeo envía una información a Aristágoras de Mileto, lo hace afeitando la cabeza de su mensajero; allí escribió el mensaje, una vez que creció el cabello de su sirviente el mensaje quedó oculto. Otra forma de ocultación muy antigua la explicó Plinio el Viejo: con la "leche" de la planta *Thithymallus* se podía hacer tinta invisible (Ídem: 19).

La primera técnica criptográfica de la cual se tiene conocimiento es la del escitalo espartano, que data del siglo v a.c. El escitalo es una vara en la que se coloca un pergamino de forma que lo enrolle, el emisor escribe el mensaje a través del escitalo, después de esto desenrolla el pergamino de tal forma que las letras del mensaje quedan traspuestas; luego, para descifrar el mensaje, se enrolla nuevamente en un escitalo en donde se verá claramente el mensaje enviado[8]. Otra referencia bastante antigua de criptografía está en el *Kamasutra*, donde dentro de las 64 artes que deben saber las mujeres se encuentra mlecchita-vikalpa, el arte de la escritura secreta, donde se recomienda un método de sustitución para cifrar la información.

Una de las más famosas referencias de aplicación criptográfica para enviar información con propósitos militares, es la de Julio César, quien utilizó técnicas esteganograficas, criptográficas y de codificación para asegurar la confidencialidad de sus mensajes, los cuales fueron vitales para la consecución de la expansión de su imperio. El historiador Suetonio menciona lo que se ha denominado la *cifra del César*, un método de sustitución o desplazamiento de +3[9]. Otro sistema utilizado por Julio Cesar (*Guerra de las Galias*: 190), fue el de la codificación, al escribir los mensajes en griego[10], idioma que era desconocido por sus enemigos, así, aun en caso de ser interceptados los mensajes, resultaban indescifrables, por desconocer el idioma, el código.

Además de Occidente, en el mundo árabe y en la antigua China se desarrollaban métodos de cifrado y ocultación: en China se ocultaban los mensajes escribiéndolos en seda, luego la tela era aplastada y se recubría de cera, y en el mundo árabe, en lo que actualmente es Irak, lugar donde la matemática y la ciencia en general

7. "Como el peligro de que lo descubrieran era muy grande, sólo había una manera de en que podía contribuir a que pasara el mensaje: retirar la cera de un par de tablillas de madera, escribir en la madera lo que Jerjes planeaba hacer y luego volver a cubrir el mensaje con cera. De esta forma, las tablillas, al estar aparentemente en blanco, no ocasionarían problemas con los guardas del camino. Cuando el mensaje llegó a su destino, nadie fue capaz de adivinar el secreto, hasta que, según tengo entendido, la hija de Cleomenes, Gorgo, que era la esposa de Leónidas, lo vaticinó y les dijo a los demás que si quitaban la cera encontrarían algo escrito debajo, en la madera. Se hizo así; el mensaje quedó revelado y fue leído, y después fue comunicado a los demás griegos" (Citado en Scarro, Ob. cit.: 18).

8. Revista de Propiedad Inmaterial, comercio electrónico.

9. Cayo Suetonio Tranquilo (*Los Doce Cesares*: 37): " Para los negocios secretos utilizaba una manera de cifra que hacía el sentido ininteligible, estando ordenadas las letras de manera que no podía formarse ninguna palabra; para descifrarlas, tiene que cambiarse el orden de las letras, tomando la cuarta por la primera, esto es d por a, y así las demás."

10. Durante la Segunda Guerra Mundial, los Estados Unidos utilizaron como código el alfabeto navajo.

eran cultivadas al ser esta la sociedad más culta del mundo, a través de estudios teologales[11] se desarrolló el criptoanálisis de los métodos por sustitución; en el siglo IX, el erudito AL KINDI, mediante sus conocimientos en fonética, sintaxis, estadística, matemática, desarrolló un escrito titulado *Sobre el descifrado de mensajes criptográficos* (SGARRO, Ob. cit.: 29), donde describe la forma de descifrar los mensajes cifrados con métodos como el de la cifra del CÉSAR. Se ha encontrado que culturas mesoamericanas, como la azteca, también cifraban su información a través de ideogramas.

Hasta el siglo XIV, con el libro más antiguo del que se tenga noticia sobre criptografía, el *Liber Zifrorum* de GABRIEL DE LAVINDE (GALENDE DÍAZ, 1995: 78), se vuelve a tener noticia del interés por la materia, en ese entonces su estudio estuvo muy ligado a la alquimia. En el siglo XVI, el aporte más importante lo realiza BLAISE DE VIGENERE, quien diseñó criptosistemas polialfabéticos y, desde ese momento, se empiezan a usar los sistemas de alfabetos múltiples y los de transposición sencillas y múltiples, métodos que son la base de los actuales criptosistemas.

Desde el siglo XVIII se empezaron a desarrollar ideas para aprovechar los sistemas eléctricos para la transmisión de mensajes; fue hasta 1839 con el sistema Wheatstone-Cooke que se desarrolló el telégrafo, comunicando dos estaciones de tren que se encontraban a 29 Km. de distancia, luego con los progresos de MORSE, el sistema cobró total popularidad y se adoptó la implementación del telégrafo trasmitiendo mensajes con el Código Morse. Pero este avance tan importante presentaba una deficiente seguridad en lo que respecta a la confidencialidad[12], además con esta tecnología se empieza a dar un crecimiento notable en las comunicaciones, ya que la velocidad y la facilidad para transmitir mensajes hizo que las relaciones fueran más dinámicas.

A finales del siglo XIX, GUGLIELMO MARCONI realizó progresos en el área de las telecomunicaciones que cambiarían totalmente la forma de comunicarnos: inventó la radiotransmisión, pero si el telégrafo tenía problemas de confidencialidad, la comunicación por radio carecía de seguridad alguna, ya que la señal, una vez emitida, podría ser interceptada por cualquiera que dispusiera de un receptor, lo que implicaba un desequilibrio entre seguridad y capacidad de comunicación.

En 1914 comienza la Primera Guerra Mundial, y en menos de un siglo se han hecho avances en las telecomunicaciones que cambiarían no solamente el comercio

11. En la Biblia también se encuentran apartes cifrados con el atbash, que es un sistema de sustitución hebreo.

12. La revista inglesa *Quarterly Review,* en 1853, comentaría lo siguiente al respecto: "También deberían tomarse medidas para evitar una gran objeción que se presenta en estos momentos con respecto a enviar comunicaciones privadas por telégrafo –la violación del secreto- porque en cualquier caso media docena de personas deben tener conocimiento de cada una de las palabras dirigidas por una persona a otra. Los empleados de la Compañía Inglesa de Telégrafo están bajo juramento de guardar secreto, pero a menudo escribimos cosas que resulta intolerable ver cómo personas extrañas leen ante nuestros ojos. Ésta es una penosa falta del telégrafo, y debe ser remediada de un modo u otro" (Citado Por Simón Sigh: 73).

sino las estrategias de combate, ya que se podría contar con información neurálgica para la toma de decisiones en la batalla. Durante todas las guerras se ha buscado por cada uno de los participantes en éstas, transmitir información de forma segura, y para esto utilizar criptosistemas que permitan una comunicación confiable, y a la vez que se intenta comunicar de una forma segura, se realiza el mismo esfuerzo en atacar los sistemas de comunicación del oponente, interceptar las comunicaciones y, en caso de estar cifrada la información, descifrarla. Ese esfuerzo por descifrar los mensajes ha hecho evolucionar los sistemas criptográficos y a la vez impulsar el desarrollo de la matemática y la informática.

Después de la Segunda Guerra Mundial, no solamente aumentó el desarrollo y la investigación en criptografía, sino que además proliferó el interés en este tema dentro de la población en general; se volvió así un lugar común en obras literarias y cinematográficas, libros y películas, como *Criptonomicom* o *Beatiful Mind,* relatan historias en las que la criptografía es uno de los temas principales, o en otra película, como el *Dr. Strangelove,* de Stanley Kubrick, en la que el prefijo en la codificación de una comunicación puede salvar al mundo de una catástrofe atómica durante la guerra fría.

Es importante anotar que muchos de los desarrollos que se han realizado en los ordenadores modernos han sido generados para tener una aplicación primigenia en la criptografía: así tenemos el motor de diferencias realizado por Charles Babbage en la década de los treinta del siglo xix, la máquina desarrollada por el inventor británico que logró descifrar la cifra Vigenere tenía la capacidad de ser programable, poseer memoria y seguir instrucciones lógicas similares a las usadas actualmente en el desarrollo de *software* (Sgarro, Ob. cit.: 76), los avances que hizo Alan Turing creando las bombas de Turing, las cuales ayudaron a descifrar el sistema Enigma de los Alemanes durante la Segunda Guerra Mundial han llevado junto a los avances también para propósitos criptográficos de Max Newman a las bases de los ordenadores actuales. Por el mismo camino, los primeros ordenadores creados alrededor de la Segunda Guerra Mundial fueron herramientas de cifrado y descifrado de información para las agencias de seguridad de Estados Unidos. Tal vez si no hubiesen existido estos usos en los sistemas computacionales, la explosión de las tecnologías de la información hubiese sido muy diferente, ya que gran parte de los recursos que se invirtieron en un primer momento en estas tecnologías fue debido a las aplicaciones militares y más precisamente en la criptografía.

Desde la creación del primer computador moderno, el eniac[13], se empezaron a convertir los mensajes en códigos binarios, es decir en ceros y unos, utilizando protocolos[14], como el ascii[15]. Cada letra de cada palabra para su transmisión se convierte en series de ceros y unos, a los cuales para cifrar el mensaje se les aplica

13. Acrónimo de Electronic Numerical Integrator And Calculador.
14. "Los protocolos de comunicación son los procedimientos para realizar operaciones de comunicación…" (*Técnicas criptograficas de proteccion de datos*: 104).
15. Acrónimo de American Standard code for Information Interchange.

el criptosistema. Este uso estaba restringido a aquellos que tuviesen computadores, en la década de los cincuenta del siglo pasado, solamente el gobierno y el ejército los poseían. En 1947, AT&T creó el transistor, lo cual fue un paso para hacer ordenadores más económicos. En 1953, IBM ofreció su primer computador y en 1959 se desarrolló el circuito integrado, elemento que reemplazó al transistor y brindó la posibilidad de computadores más potentes, más pequeños y más económicos. De esta forma, los computadores dejaron de ser artículos exclusivos de agencias estatales para pasar a ser utilizados por empresas en actividades civiles de todo tipo: comerciales, estadísticas, comunicaciones, etc.

Con el advenimiento de sistemas computacionales cada vez más potentes y con el aumento del uso de estos equipos para procesar y transmitir información, se presentaron necesidades nuevas frente a la criptografía, mientras que antes de esta evolución, cuando el uso de la criptografía no era normal en las relaciones de la sociedad civil, cuando la información que se debía cifrar no era mucha, solamente se buscaba la confidencialidad. Surgió entonces la necesidad de estandarizar el uso de un sistema criptográfico para hacer transmisiones sin problemas de compatibilidad, además de incentivar el uso generalizado de este tipo de comunicaciones. Otro tipo de problemas que surgieron fueron el de la distribución de claves[16], la autenticidad, integridad[17], no repudio; es decir, que el destinatario y el emisor correspondan realmente a quienes deben ser, tener la certeza de que el mensaje no haya sufrido alteraciones o manipulaciones.

A. DES

En 1973, la oficina nacional de estándares de los Estados Unidos[18] abrió convocatoria para presentar un criptosistema que se convirtiera en el estándar comercial para la transmisión y archivo de información cifrada. En 1976 se escogió el sistema DES (Data Encryption Standard) creado por IBM[19], un criptosistema de cifrado por bloques que combina sustituciones y permutaciones[20]; la clave es de 56 bits y de clave simétrica, es decir que utiliza la misma clave tanto para el proceso de cifrado como para descifrar. La escogencia de este sistema se hizo bajo la supervisión de la NSA[21], que es la institución que más investiga e invierte en criptoanalisis y cripto-

16. Las principales dificultades que se presentan en el manejo de claves son "1. La gente tiende a utilizar estereotipos para recordar la clave (la fecha de nacimiento, sus iniciales, etc.), lo cual es una pista para quien desea averiguarlo. 2. El uso de las claves tiende a viciarse cuando los usuarios las comparten mutuamente. 3. Las personas acostumbran apuntar la clave para no olvidarla. 4. El cambio frecuente de claves tiende a crear un desorden en su administración" (*Criptografía, elemento indispensable en la seguridad de la banca electrónica*: 16).

17. (*Técnicas Criptográficas de protección de datos*: 3).

18. NBS, acrónimo de National Bureau of Standards.

19. El DES tiene como base el criptosistema denominado *Lucifer*, creado por HORST FEISTEL.

20. Este sistema aplica las teorías de CLAUDE SHANNON (s.f.: 18).

21. Acrónimo de Nacional Security Agency.

grafía, además es la agencia que más información intercepta en el ámbito mundial (Sgarro, Ob. cit.: 250). La selección de este sistema suscitó discusiones bastante álgidas, debido a que el grado de seguridad del sistema no es lo suficientemente fuerte, ya que la longitud de la clave es bastante corta; generó muchas sospechas el hecho de que el proyecto inicial del DES tenía una longitud de clave de 128 bits, lo cual lo hacía mucho más seguro. Aunque con 56 bits se crea un modelo bastante seguro, ya que para descifrarlo se necesita una fuerza bruta demasiado alta, cuyos recursos solamente poseen agencias como la NSA. En julio de 1979 se publicó un artículo[22] donde se pusieron de manifiesto los dos principales problemas del DES, el primero es que ante un análisis de búsqueda exhaustiva[23] el sistema es vulnerable, y el segundo inconveniente es la existencia de atajos que reducen el tiempo de búsqueda. Ante estas críticas se pone en evidencia un criterio político que indujo a la NSA a establecer este estándar: no podían seleccionar un criptosistema tan robusto que ellos no pudieran descifrar. Aunque una comisión del Senado de los Estados Unidos investigó la manipulación del estándar por parte de la NSA, se concluyó que IBM fue totalmente independiente en la construcción del DES y que se había comprobado su seguridad práctica de tal manera que hasta la NSA cifraría su información clasificada como secreta con este estándar[24]. El departamento de comercio implementó el estándar para las transacciones del gobierno en todas las EFT[25], pero la más notable ausencia en la implementación es la del departamento de defensa de los Estados Unidos (Shannon, s.f.: 31).

En mayo de 1998, la Electronic Frontier Foundation con una inversión de 210.000 dólares diseñó un computador capaz de realizar un criptoanálisis efectivo en un mensaje cifrado con sistema DES, el *DES Cracker*[26], mediante el sistema de búsqueda exhaustiva logró probar todas las claves en nueve días. Cualquier organización con los recursos suficientes puede diseñar una máquina que logre descubrir la clave. Cada vez con el desarrollo en los microprocesadores será más económico realizar esta máquina, además del aprovechamiento de recursos en red, por lo cual este sistema ya no es confiable. Otro punto a tener en cuenta es que la patente del DES expiró. Vale la pena anotar que el DES evolucionó al triple DES, el cual posee una longitud efectiva de clave de 112 bits, lo cual proporciona más seguridad, aunque aun así está expuesto a las mismas debilidades que su antecesor.

El DES dejó de ser el cifrado estándar en el año 2000, cuando el NIST[27]declaró como nuevo estándar el sistema AES, también conocido como Rijndael, por las iniciales de sus creadores, los belgas Rijmen y Daemen. Este criptosistema trabaja

22. "On foiling computer crimen" Spectrum del IEEE, Julio de 1979. citado por Querubín Londoño, p. 53.
23. Este tipo de ataque consiste en buscar todas las claves posibles hasta que encuentre la correcta, según la longitud de la clave se demorará el proceso de desciframiento.
24. Criptografía, elemento dd en la seguridad de la banca electrónica, p. 54.
25. Acrónimo de Electronic Funds Transfer.
26. *Técnicas Criptograficas de protección de datos*: 67.
27. Acrónimo de National Institute for Standards and Technology.

con longitudes de clave variable entre 128 y 256 bits, el descifrado de este sistema se realiza mediante el mismo algoritmo de cifrado aplicado de forma inversa[28]. Hasta el momento este algoritmo ha pasado todas las pruebas de seguridad a las que se ha sometido.

b. criptografía de clave pública

El problema fundamental de los sistemas de clave simétrica es la distribución de las claves. Un ejemplo notorio de esto es que en la Segunda Guerra Mundial el alto mando alemán tenía que distribuir un libro mensual de claves del día a todos los operadores del Enigma (Sgarro, Ob. cit.: 252), lo cual implicaba una vulnerabilidad muy alta. En ambientes de transmisión de datos, donde existe un flujo muy alto de información, un sistema de clave privada entorpecería las comunicaciones, ya que la inmediatez se perdería, además de costos demasiado altos para la transferencia de claves.

En 1976, Martin Hellman y Whitfield Diffie, este último denominado el primer *cypherpunk*, crearon el concepto de clave asimétrica, que se utiliza una clave para cifrar, que será de conocimiento público y otra para descifrar, que es de conocimiento privado, cuando se desee confidencialidad; al contrario, un mensaje cifrado con la clave privada, lo que busca es autenticidad, ya que solamente con la clave pública del mismo emisor se podrá descifrar el mensaje, dando así la certeza que quien envía el mensaje es el titular de esa clave pública: este es el principio de la firma digital.

Se busca entonces que el cifrado sea sencillo; en cambio, el descifrado sin la clave privada sea irresoluble. El inconveniente que poseen estos sistemas es que la velocidad de desciframiento es mayor que los de clave privada[29].

Uno de los criptosistemas de clave pública más usado es el rsa**,** desarrollado en 1978 por L. Rivest, A Shamir y L. Adleman, científicos del Departamento de Matemáticas y Ciencias de la Computación del mit, en su artículo titulado "A Method for Obtaining Digital Signatures and Public Key Criptosystems"[30]. A traves de números primos se realiza este cifrado, la seguridad depende de lo grande que sean estos números; así, con una clave de 10 a la 130 con un computador Intel Pentium de 100 Mhz con 8 Mb de memoria ram tardaría aproximadamente 50 años en factorizar el número y por tanto descifrar el mensaje (Sgarro, Ob. cit.: 277), aun así con la tecnología actual no sería tan demorado factorizar esta cifra, por lo que hay que escoger números primos mucho más altos para generar la clave.

28. *Introducción a la criptografía*: 40.
29. Ídem: 84.
30. Publicado en la revista "Communications of the acm" febrero de 1978. Citado por Querubín, Pág. 62.

c. PGP

El sistema RSA es deficiente bajo algunas necesidades, ya que el tiempo de descifrado no es el óptimo. El sistema PGP (Pretty Good Privacy) es una combinación de las ventajas del cifrado de clave pública y el de clave privada, ya que cifra con el sistema RSA la clave de un mensaje que está cifrado con clave simétrica[31]. En 1991, el autor de este método, PHIL ZIMMERMANN, por medio de un BBS (Bolletin Board System) de Usenet, puso a disposición el *software* de cifrado. Este *software*, con una interfaz versátil, logra que cualquier persona tenga a disposición una herramienta de cifrado supremamente poderosa y fácil de usar, por lo que se pueden generar firmas digitales, cifrar e-mail, y hasta telefonía digital con el PGPfone. El creador de este popular *software* tuvo bastantes problemas legales que, como veremos más adelante, dejan al descubierto la discusión política y jurídica que existe sobre este tema.

Actualmente, el desarrollo en técnicas criptográficas es bastante vertiginoso y en todo el mundo existen grandes inversiones en investigación para lograr cada vez criptosistemas más ágiles, más robustos y más novedosos. El estudio de números primos, de curvas elípticas y otros temas similares ocupan ahora un espacio importante en las facultades más importantes de Matemática e Ingeniería, además del puesto que ya ocupaban en las agencias de seguridad estatal. Como hemos observado, los avances de los últimos años se han concretado al esfuerzo de equipos de trabajo; desafortunadamente, en nuestro país y en toda América latina no existe la atención que merece este tema, ni por parte del gobierno ni por la academia, por lo que la mayoría sino todos los criptosistemas que se usen serán importados, y como veremos más adelante difícilmente se tendrá acceso a los sistemas más seguros de cifrado, ya que su exportación está bastante limitada; esto es preocupante en la medida que cada día el uso de estos métodos encuentra más aplicaciones.

III. NOCIONES GENERALES Y CARACTERÍSTICAS DE CRIPTOSISTEMAS

Cuando hablamos de criptografía se tienen en cuenta ciertos elementos:

1. Un mensaje que se desea transmitir.
2. Un sistema de comunicación por el cual se va a transmitir el mensaje.
3. Un protocolo o sistema que va a permitir el cifrado y descifrado del mensaje.

Para hablar de un sistema criptográfico o criptosistema tenemos que tener en cuenta los siguientes elementos:

1. Alfabeto.
2. Un conjunto de transformaciones de cifrado.
3. Conjunto de transformación de descifrado.
4. Conjunto de claves.[32]

31. Utiliza el sistema IDEA, que es un derivación del DES.
32. *Teoría de números para principiantes*: 195.

Las condiciones básicas de un criptosistema informático son cinco:

1. Conjunto finito de textos claros, es decir de unidades de mensaje que se deseen transmitir.

2. Conjunto finito de textos cifrados, unidades de mensaje que se reciban por parte del receptor.

3. Conjunto finito de claves: se busca que este conjunto sea lo más grande posible para que se demore la mayor cantidad de tiempo posible en hallar claves para cifrar o descifrar los textos.

4. Conjunto de funciones de cifrado: a cada texto claro se asigna una función de texto cifrado.

5. Conjunto de funciones de descifrado: a cada texto cifrado corresponde un texto claro (Moreno).

El ejemplo prototípico sobre el cual se establece la forma como va a operar el envío de un mensaje cifrado, es el de dos presos que se necesitan comunicar dentro del establecimiento penitenciario: cada uno se encuentra en diferentes áreas de reclusión, y la única forma de enviar el mensaje es a través de un guardián, así que codifican el mensaje, se lo dan al guardia para que se lo entregue al otro recluso; el guardia revisa el mensaje y no logra captar el mensaje que desean transmitir los reclusos, creyendo así que el mensaje contiene un significado muy diferente al que transmiten. El guardia entrega el mensaje al recluso receptor, éste logra descifrarlo y se realiza exitosamente la comunicación sin haberse revelado la información. Este es un principio básico de la criptografía: el poner a disposición el mensaje a cualquier sujeto pero que solamente pueda ser cifrado por el receptor que se desee.

También se han establecido unas reglas básicas que deben seguir los criptosistemas. El holandés August Kerckhoffs[33] publicó en 1883 una serie de elementos de cualquier criptosistema. El más importante de estos enunciados fue que el enemigo podía conocer el método de cifrado, lo importante era la privacidad de la clave. Recomendó las siguientes pautas que han de tenerse en cuenta:

1. No debe existir ninguna forma de recuperar mediante el criptograma el texto inicial o la clave.

2. Todo criptosistema debe estar compuesto por dos tipos de información:

a. Pública, como es la familia de algoritmos que lo definen.

b. Privada, como es la clave que se usa en cada cifrado particular. (En casos como los criptosistemas de clave pública, parte de la clave es información pública y otra parte, información privada).

3. La forma de escoger la clave debe ser fácil de recordar y modificar.

5. Debe ser factible la comunicación del criptograma con los medios de transmisión habituales.

33. En Journal Des Sciences Militaires, artículo titulado "La Cryptographie Militaire". Enero de 1883.

6. La complejidad del proceso de recuperación del texto original debe corresponderse con el beneficio obtenido.[34]

Debemos realizar una diferencia importante entre secreto teórico y secreto práctico[35], ya que lo más importante no es que el sistema teóricamente sea indescifrable sino que esté en la práctica, es decir que con los recursos que posee el oponente éste permanezca indemne.

Las funciones de cifrado y descifrado deben realizarse con algoritmos computacionales eficientes, lo cual significa que deben ser posibles de calcular.

Otra característica fundamental es que el cifrado o descifrado no puede ser ambiguo, es decir que sea unívoco el resultado[36], que no permita multiplicidad de resultados pues de suceder esto no se tendría certeza de cuál es el mensaje claro, o también permitiría equivocaciones de interpretación del mensaje cifrado.

Así, la forma para que un receptor no autorizado conozca un mensaje, es decir viole el cifrado para poder conocer el mensaje original, actividad realizada por una persona no autorizada para conocer el mensaje, éste tendrá dos formas para realizar el ataque:

1. Intervenir la comunicación

2. Atacar la forma de cifrado, intentar descifrar el criptosistema que se haya utilizado[37].

Si se logra este segundo punto, la situación de seguridad se complica bastante, ya que en caso de que logre descifrar el criptosistema, todos los mensajes que se transmitan serán vulnerables. Lo más usual es que una vez se conozca el protocolo de cifrado no se hace conocer a los transmisores y receptores sobre la violación para que éstos no se alerten de la vulneración de su criptosistema.

El sistema Enigma, utilizado por los alemanes durante la Segunda Guerra Mundial, presentó dos problemas principales; estos inconvenientes hicieron que se establecieran como puntos estratégicos actualmente dentro de los criptosistemas:

34. *Seguridad Informática, técnicas criptográficas*: 8. En el artículo original en francés aparece en el título II. Desiderata de la cryptographie militaire. 1º Le système doit être matériellement, sinon mathématiquement, indéchiffrable ; 2º Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ; 3º La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ; 4º Il faut qu'il soit applicable à la correspondance télégraphique ; 5º Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ; 6º Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

35. "Un criptosistema tiene secreto teórico, si es seguro contra cualquier enemigo que tenga recursos y tiempo ilimitados. Práctico, si es seguro contra aquellos enemigos que tengan menos de una cantidad de tiempo y/o recursos" (Caballero Gil, 1997: 9).

36. Ante la distribución de contenidos digitales por Internet, parece restar un poco la importancia de esta regla, un ejemplo de esto es el sistema DRM, Chameleon, el cual asigna una clave de desciframiento diferente para cada usuario ante un contenido cifrado: de esa forma, cada usuario descifrará de una manera ligeramente diferente (ver más información, *Avances en Criptología y seguridad de la Información*: 642).

37. De forma similar, el autor Pino denomina como amenazas contra un mensaje secreto, y establece dos: 1. Pasiva, siendo ésta el acceso no autorizado y Activa, como la alteración del mensaje (*Seguridad informática*: 3).

1. La velocidad de cifrado y descifrado de los mensajes.
2. La libertad de los agentes para usar claves.

El primer punto en la antigüedad no revestía mayor importancia. La velocidad de transmisión del mensaje en los sistemas de comunicación antiguos es bastante lenta aunque el descifrado es veloz; otro problema que se puede presentar es una transmisión veloz pero un descifrado lento.

El segundo punto incrementa las posibilidades de fuga de información, además de no establecer los controles necesarios para asegurar la confidencialidad. Vale la pena mencionar que el uso de *passwords*[38] tiene para el acceso, mas no son claves de cifrado. Así, cuando se nos solicita nuestro *password* o clave para algo, en la mayoría de casos simplemente estamos frente a una validación que permite el acceso a algo, mas no hay aplicación de cifrado, pues en esquemas de seguridad se combinan tanto las claves de acceso como las de cifrado.

Por razones de eficiencia, la clave que se genere se busca que sea lo más segura posible y que sirva para cifrar y descifrar el mayor número posible de mensajes, así que sea inversamente proporcional el número de claves a usar y el número de mensajes transmitidos, se debe pensar que aunque el mensaje sea interceptado sea lo más difícil posible descifrarlo, y pensar también que el atacante o persona que está interceptando tendrá recursos infinitos para vulnerar el criptosistema. Esto se debe analizar para medir el grado de seguridad del sistema que se este utilizando. El grado de mayor seguridad es el de secretitud perfecta[39], en donde por más que el atacante tenga recursos infinitos para descifrar el mensaje, no lo logra, y esto se consigue cambiando la clave para cada mensaje; este tipo de sistemas son los que se utilizan en los servicios diplomáticos. Cabe resaltar en este punto que la comunicación de cada clave se realiza por un canal privado absolutamente seguro.

Los sistemas clásicos de criptografía son los de traslación o desplazamiento y el de permutación; el de traslación ya se mencionó y corresponde al de la cifra del Cesar, un sistema que sustituye un dato por otro; el de permutación corresponde a un cambio de posición. Estos sistemas son la base de toda la criptografía.

Por último, las características de un sistema de clave pública son:

1. Cualquier usuario puede calcular sus propias, claves pública y privada.
2. El emisor puede cifrar su mensaje con la clave pública del receptor.
3. El receptor puede descifrar el criptograma con la clave privada.
4. El criptoanalista que intente averiguar la clave privada mediante la pública se encontrará con un problema intratable.
5. El criptoanalista que intente descifrar un criptograma teniendo la clave pública se encontrará con un problema intratable[40].

38. *Passwords*, o Palabra (*word*) de paso (*pass*).
39. El cifrado de Vernam posee esta cualidad, pero en la práctica es poco útil ya que la clave debe poseer la misma extensión que el mensaje. Para más información, ver Pino: 27.
40. *Introducción a la criptografía*: 52.

IV. IMPORTANCIA DE LA CRIPTOLOGÍA

con el desarrollo de la informática y las telecomunicaciones, la criptología ha tenido un avance vertiginoso; el constante enfrentamiento entre desarrolladores de criptosistemas cada vez más seguros y más sofisticados y los descifradores que a través de ataques cada vez más complejos logran vulnerar y notar las debilidades de los "seguros" sistemas, llevando así una carrera que cada día cuenta con más recursos económicos, tecnológicos y humanos.

Resulta relevante preguntarse: ¿por qué resulta tan importante la criptología? Sin tener plena conciencia de sus usos, la mayoría de los ciudadanos a diario están en permanente contacto con diferentes aplicaciones que tienen como fondo el uso de un criptosistema. "Es entonces cuando la criptografía pasa de ser una exigencia de minorías a convertirse en una necesidad del hombre de la calle."[41]. Todas las transmisiones de información a través de las redes telemáticas intentan ser lo más seguras posibles, y esto lo logran aplicando criptosistemas, ya sea en los contenidos que se transmiten o en los canales que comunican la información. En términos más gráficos, cada vez que entramos a Internet se usa criptografía, hoy en día que afirmaciones como éstas no parecen exageradas: "La codificación es la única manera de proteger nuestra privacidad y garantizar el éxito del mercado digital. El arte de la comunicación secreta, también conocido como criptografía, suministrará las cerraduras y las llaves de la era de la información" (Sgarro, Ob. cit.: 10).

Todo esto enmarcado dentro de la sociedad de la información, de un ambiente donde la información está almacenada en lenguaje binario y en donde se aplica la fórmula de Nicolas Negroponte (s.f.: 49), "la digitalización es el pasaporte al crecimiento".

Uno de los mayores retos que impone la sociedad de la información es consolidar la privacidad de los ciudadanos. El envío de información a través de Internet, por ejemplo, un correo electrónico, implica que éste pase por múltiples computadores hasta llegar al destinatario final. De esta forma, las comunicaciones de ahora son más sensibles a la interceptación y sus contenidos son mas vulnerables de ser descubiertos y observados de forma ilegítima. El simple hecho de conectarnos a una red de computadores sin las medidas de seguridad suficientes nos pone en una situación de desnudez, en donde cualquier persona con conocimientos básicos puede esculcar todos nuestros documentos, saber qué hacemos en la red, qué páginas visitamos, qué música escuchamos, qué fotos poseemos, en fin, puede tener total acceso a nuestro computador y ni siquiera surge la más mínima sospecha de esto. Frente a la cada vez más cercana posibilidad de perder la intimidad y privacidad, semejante a un mundo orwelliano donde el Big Brother puede ser cualquiera con conocimientos básicos de informática y un computador, se presenta la criptografía como una posibilidad de salvaguardar la privacidad.

41. *Técnicas criptográficas de protección de datos*: 2. Alfaomega.

Herramientas criptográficas simples integradas a procesadores de texto o *software* utilitario, que permiten cifrar nuestros documentos, tales como criptosistemas RC-4, RSA, DSS entre otros dispuestos en las opciones de seguridad de software como MS-Office, colocan al alcance de cualquier persona la posibilidad de brindar protección a sus documentos. Otro *software* de uso común es el Winzip, programa que se utiliza para la compresión y empaquetamiento de archivos, cuya última versión incorpora la posibilidad con dar un solo *click* de proteger la información con el criptosistema AES.

De igual forma, todas las herramientas que se encargan de brindar protección en los protocolos SMTP (Service Mail Transfer Protocol) o correos electrónicos, buscan la privacidad en los correos, herramientas como el PGP o el PEM (Privacy Enhanced Mail) generan autenticidad, privacidad e integridad.

Al mismo tiempo, un elemento crucial en la protección de la privacidad, es el anonimato. Desde hace décadas se han utilizado los Remailers, los cuales son servidores que realizan una "limpieza" de los mensajes, eliminando la posibilidad de identificar su recorrido y emisarios. Vale la pena citar sobre este punto las palabras de JOHN GILMORE, fundador de la EFF, que por estos años y sobre estos temas estaba muy de la mano con toda la industria del *software*; en 1991, en una conferencia titulada "Ordenadores, Libertad y Privacidad", decía: "¿Qué pasaría si construyéramos una sociedad en la que no se recabara la información? En la que pudiéramos alquilar un video sin tener que dejar el número de la tarjeta de crédito o el de la cuenta bancaria. En la que pudiéramos demostrar que tenemos carné de conducir sin tener que dar nuestro nombre. En la que pudiéramos enviar y recibir mensajes sin revelar nuestro paradero, como un buzón de correos electrónicos. Esta es la sociedad que yo quiero construir. Quiero garantizar mediante la física y las matemáticas, y no mediante las leyes, cosas tales como la privacidad real de comunicaciones personales, privacidad real de datos personales…" (SIMON, s.f.: 222), y tal como diría JOHN STUART MILL, "el anonimato es un escudo ante la tiranía de la mayoría".

V. PROTECCIÓN LEGAL DE ALGORITMOS CRIPTOGRÁFICOS

Para determinar qué tipo de protección se puede aplicar a un algoritmo, debemos definir lo que es; encontramos en el diccionario de la Real Academia que un algoritmo es un conjunto ordenado y finito de operaciones que permite hallar la solución de un problema.

Esta definición bastante amplia nos da indicios sobre la naturaleza de los algoritmos a los cuales nos estamos refiriendo, entonces agregaremos una cualidad a este tipo de algoritmos diciendo que son informáticos.

Antes de continuar conviene hacernos una pregunta: ¿existe creación cuando se desarrolla un algoritmo? La respuesta es afirmativa y por lo tanto sí deben tener protección legal.

El sistema de protección de la propiedad intelectual de los Estados Unidos permite que los algoritmos sean protegidos bajo la modalidad de propiedad industrial y más específicamente bajo las patentes de invención.

En países como Colombia se excluye de este tipo de protección a los algoritmos, tal como se deduce del artículo 15 de la Decisión 486 del 2000, la cual manifiesta que no se considerarán invenciones: c) Las obras literarias y artísticas o cualquier otra protegida por el derecho de autor, y en el literal e) Los programas de ordenadores o el soporte lógico, como tales. Los programas de ordenador están realizados mediante algoritmos informáticos, y aunque no siempre un algoritmo llegue a ser un *software*, todo *software* sí contiene algoritmos, así un *software* muy sencillo puede estar elaborado con tan solo un algoritmo, y uno muy complejo puede constar de miles de algoritmos.

De igual forma, se excluye la protección por vía de patentes al *software*[42] y a los algoritmos por el requisito de novedad y estado de la técnica que es indispensable para brindar este tipo de protección.

Igual que el *software* antes de ser protegido de forma explícita por el derecho de autor, se debe considerar que los algoritmos se protegen en los mismos términos que las obras literarias, y que son el resultado de una forma de expresión original. Por el momento y por no ser el objeto de este trabajo, dejo la discusión abierta sobre la posibilidad en nuestra legislación de este tipo de protección para este tipo de creaciones.

En los Estados Unidos, recién finalizada la Segunda Guerra Mundial y durante la Guerra Fría a través de la Invention Secrecy Act of 1952, por razones de seguridad, la NSA podría mantener como confidencial un desarrollo criptográfico y no permitir su publicación.

Hasta 1995, la protección de patentes en Estados Unidos era por un término de 17 años, pero con la ratificación de los acuerdos del GATT en junio de 1995 la protección de las patentes pasó a ser de 20 años.

Estas han sido algunas de las patentes de los criptosistemas más importantes:

Nombre del criptosistema	Npumero de la Patente	Fecha de la solicitud	Fecha de otorgamiento	Inventores	Titular
DES	3, 962,539	Febrero 24, 1975	Junio 8, 1976	Ehrsam et al.	IBM
Diffie-Hellman	4, 200,770	Septiembre 6, 1977	Abril 29, 1980	Hellman, Diffie, and Merkle	Stanford University[1]

42. El derecho de autor en la protección jurídica de los programas de ordenador- soporte lógico (*software*) y los bancos o bases de datos (Ríos, 2002).

43. Esta fue la primera patente de un criptosistemas de clave pública. Esta Patente ya expiró.

La patente de Diffie-Hellman pertenecía a Standford y la de RSA al MIT, se presentó entonces un problema de patentes, ya que la D-H era un concepto más amplio que abarcaba el sistema de clave pública, la patente RSA implicaba la de D-H, por lo cual Standford pretendía derechos sobre la de RSA. El caso terminó en una conciliación en la que Standford quedó como titular de las patentes y las sublicenciaba al MIT.

Public-key cryptosystems	4,218,582	Octubre 6, 1977	Agosto 19, 1980	Hellman and Merkle	Stanford University
RSA	4,405,829	Diciembre 14, 1977	Septiembre 20, 1983	Rivest, Shamir, and Adleman	MIT
Fiat-Shamir identification	4,748,668	Julio 9, 1986	Mayo 31, 1988	Shamir and Fiat	Yeda Research and Development (Israel)
Control vectors	4,850,017	Mayo 29, 1987	Julio 18, 1989	Matyas, Meyer, and Brachtl	IBM
CQ identification	5,140,634	Octubre 9, 1991	Agosto18, 1992	Guillou and Quisquater	U.S. Phillips Corporation
IDEA	5,214,703	Enero 7, 1992	Mayo 25, 1993	Lai and Massey	Ascom Tech AG (Switzerland)
DSA	5,231,668	Julio 26, 1991	Julio 27, 1993	Kravitz	United States of America
Fair cryptosystems	5,315,658	Abril 19, 1993	Mayo 24, 1994	Micali	

En 1994, el NIST estableció como estándar de firma digital el DSA, un criptosistema que la industria no estaba dispuesto a aceptar y que desde el principio tuvo inconvenientes, sobre todo por la intervención de la NSA en el proceso de adopción del estándar, el cual en un principio iba a ser de 512 bits, pero por presión de la industria pasó a ser de 1.024 bits. En 1991, el científico alemán Claus Schnorr patentó su sistema de firma digital, el cual, según su autor, estaba siendo violado por el sistema DSA; fue tan álgida la discusión que al decidir el estándar la NIST asumió la responsabilidad en caso de que algún usuario del DSA fuera demandado por violación de patentes.

VI. CRIPTOGRAFÍA E INVESTIGACIÓN JUDICIAL

Como se ha mencionado en la descripción realizada sobre las funciones de la criptografía en el ambiente digital, ésta presta una utilidad sumamente importante en el contexto de la evidencia digital. La autenticidad, el no repudio, el estampado de fecha y hora de forma digital, la integridad, son elementos que a la hora de analizar un documento o cualquier mensaje que sirva de prueba en un proceso, nos va a generar certeza sobre ciertas características que permitirán identificar la responsabilidad de los sujetos intervinentes en un proceso judicial.

Además, es necesario para todo el sistema nacional de información, para las agencias de seguridad y para todos los organismos estatales, tales como centros de estadística, juzgados, fiscalías, etcétera, estar protegidos por el uso de criptografía que provea la seguridad que amerita tan sensible información de toda la nación (Litt, 1998).

Pero, así como puede ayudar a esclarecer situaciones litigiosas, la criptografía puede generar anonimato y confidencialidad, a tal punto que logra cercenar las posibilidades de identificación del responsable de un acto. Pensemos en una amenaza o un fraude por medios electrónicos o simplemente el envío de una oferta

comercial en la que se usurpe la identidad del supuesto oferente, o la puesta en Internet de una noticia que no corresponda a la verdad y que se ajuste a una injuria o calumnia, o borrar las huellas del recorrido por Internet evitando ser rastreado, y miles de casos más en los que las autoridades de investigación podrán encontrarse con la imposibilidad de hallar los indicios necesarios para la determinación de los autores de actividades que impliquen violación a la ley. Uno de los casos más renombrados sobre este tema fue el del finlandés Johan "Julf" Helsingius, en el caso The Church of Scientology vs. anon.penet.fi, el operador y propietario de uno de los Remailers más usados en Europa, a quien, mediante orden judicial se le conmino a revelar la identidad de los emisarios de ciertos mensajes que estaban revelando secretos comerciales de la Iglesia de la Cienciología a través de su servicio de reenvío de correos electrónicos anónimos: planet.fi.

Solamente en 1996, año en que empiezan a debilitarse las restricciones de exportación de criptografía fuerte, al menos 250 casos en investigaciones criminales encontraron evidencia cifrada, y al menos 500 casos criminales más a nivel mundial, en el mismo año contenían información que se encontraba cifrada[44]. Se ha encontrado evidencia del uso de criptografía por redes terroristas; se ha descubierto, por ejemplo, que la Secta Aum Shinrikyo, responsables de los atentados con gas en el metro de Tokio en 1995, había utilizado rsa para cifrar sus documentos y mensajes (Sgarro, Op. cit.: 304), de igual forma en los atentados con bombas contra el World Trade Center, a uno de los terroristas involucrados, Ramsey Yousef, se le encontraron sus planes terroristas cifrados en su computador portátil[45]. Se cree que en los atentados del 11 de septiembre los terroristas utilizaron técnicas esteganográficas tanto digitales como análogas, que, como vimos están muy relacionadas con la criptografía, para la ocultación y ejecución de sus planes (Guerrero: s.f.: 115).

El acceso a criptosistemas seguros es muy fácil, y criminales de cualquier índole y latitud pueden tener acceso de forma muy sencilla a estas herramientas[46], según una investigación realizada por Dorothy E. Denning y por el grupo de trabajo contra el Crimen Organizado del Centro de Información de Estrategia Nacional de Estados Unidos, el número de casos en los cuales se encuentra información cifrada se duplicaría cada año.

44. Encryption Technology And Crimen, Educom Review, September - October 1997.

45. Litt (1998) Sgarro (Ob. cit.: 305) El computador fue decomisado en Filipinas y el terrorista fue capturado años después en Pakistán; la información que hay es que entre otros planes terroristas encontrados en este computador se encuentra el del 11 de septiembre a las torres gemelas; se cree que Yousef fue el autor intelectual del atentado del once de septiembre, el cual financió Osama Bin Laden (Documental Nacional Geographic, Inside 11/9).

46. "Pero una vez que el programa <criptografico> estaba en un servidor de archivos, cualquiera podía descargarlo: *hackers* paquistaníes, terroristas iraquíes, luchadores por la libertad búlgaros, adúlteros suizos, estudiantes japoneses, hombres de negocios franceses, pederastas daneses, fanáticos de la privacidad noruegos o narcotraficantes colombianos" (Galende Díaz, 1995: 211).

La discusión que se ha generado es hasta qué punto el gobierno puede tener acceso a los textos planos de la información cifrada. Es por esto que la NSA todavía continúa con su influencia en la adopción de estándares. El Acta de Seguridad Informática de 1987, trasladaba la competencia para la creación de los estándares de la NSA al NBU que más tarde se convertiría en NIST. El papel de la NSA en los estándares no desaparecería y seguiría como asesor en todos los temas relacionados con algoritmos criptográficos y las técnicas criptográficas.

Un ejemplo de las medidas que toma Estados Unidos para lograr decriptar mensajes en investigaciones, es a través de *backdoors*, las cuales comprometen la seguridad de los criptosistemas pero permiten la intrusión para hallar los textos planos; la compañía suiza Crypto AG había creado una *backdoor* en su herramienta criptográfica, y suministró al gobierno americano la información para aprovecharla; Estados Unidos tenía acceso a las comunicaciones de varios países que utilizaban este criptosistema. En 1991, gracias a la interceptación y decriptado de mensajes a través de esta puerta trasera, fueron capturados los asesinos del ex primer ministro iraní exiliado Sapur Bajtiar, criminales que utilizaban la herramienta de Crypto AG. Este tipo de alternativas son bastante dañinas para la confiabilidad en los sistemas de cifrado, además que como puede ser usado para develar información vital en una investigación criminal, también podría a través de estas *backdoors* violar la privacidad e intimidad de cualquier ciudadano sin ningún sustento legal, sería una abierta violación al artículo 12 de los Declaración Universal de los Derechos Humanos, pues en todo tipo de interceptaciones ilegales debe considerarse la prueba como ilegal y no tenerse en cuenta en un proceso.

La propuesta del Chip Clipper era una solución que buscaba el uso de criptografía fuerte por parte de todos los ciudadanos sin debilitar la capacidad de investigación de las agencias del estado. El sistema de depósito de claves, aunque presenta muchos puntos polémicos, como por ejemplo la confiabilidad de los sujetos que preservan las claves (TTP), sería una opción valida para preservar la seguridad nacional y posibilitar la recuperación de textos planos en evidencias cifradas siempre y cuando medie una orden judicial, tal como sucede en la interceptación de llamadas.

VII. RESTRICCIONES DE EXPORTACIÓN Y COMERCIO

TRATADO DE WASSENAAR

Ante la necesidad de los países intervinientes en la Segunda Guerra Mundial, y después de finalizada ésta, de regular el tráfico de armas, municiones y tecnologías de doble uso, es decir, aquellas que tienen tanto aplicaciones civiles como militares, entre las cuales se encuentra la criptografía y los sistemas de comunicación de alta potencia entre otros muchos mas elementos; ante esta necesidad se creó el COCOM, para el control de las exportaciones de estos instrumentos. Los 17 países miembros

observaron la necesidad de generar un nuevo tratado, denominado temporalmente "Nuevo Foro". La decisión final de crear un nuevo tratado se dio los días 29 y 30 de marzo de 1994, en Wassenaar, Holanda.

La plenaria inaugural de los países firmantes del tratado tuvo lugar en Viena, Austria, el 2 y 3 de abril de 1996, con la participación de los siguientes 33 países como fundadores: Argentina, Australia, Austria, Bélgica, Bulgaria, Canadá, República Checa, Dinamarca, Finlandia, Francia, Alemania, Grecia, Hungría, Irlanda, Italia, Japón, Luxemburgo, Holanda, Nueva Zelanda, Noruega, Polonia, Portugal, Corea, Rumania, Rusia, Eslovaquia, España, Suiza, Suecia, Turquía, Ucrania, Reino Unido, Estados Unidos de América.

El tratado fue diseñado para promover la transparencia, el intercambio de información y prevenir la acumulación de armamento, complementando el régimen para la cooperación para la paz y para evitar la proliferación de armas de destrucción masiva.

El tratado no impide las transacciones de buena fe entre civiles y no dirige las restricciones de forma directa a un Estado o sujetos en particular. Se busca que cada país regule de forma discrecional sus políticas de transferencia y exportación de estos elementos, manteniendo de forma efectiva restricciones sobre el listado que se encuentra en el tratado.

En la declaración interpretativa sobre transferencia de *software* y tecnología realizada en la plenaria del 2001, se establece que se incluirán controles para transferencia de material intangible, como toda transmisión de datos por redes, fax, medios electrónicos o teléfono.

En la declaración de la plenaria del 2004, se expresa que no habrá control para software que de forma general esté disponible al público para transacciones electrónicas, telefónicas, de correo o diseñadas para ser instaladas por el usuario sin el soporte esencial del proveedor, además de aquellas que se encuentren en el dominio publico.

El listado de elementos relacionados con criptografía que se encuentran bajo restricción, se hallan en la categoría 5 apartado 2, seguridad de la información.

RESTRICCIONES LEGALES EN ESTADOS UNIDOS

Estados Unidos presenta una regulación bastante estricta sobre la criptografía, evitando las exportaciones de productos de cifrado *fuerte.*

En la sección 38 de AECA[47], el gobierno contempla las restricciones para la exportación de este tipo de material, además que en la USML[48] en el apartado 121 y en el ITAR[49] podemos encontrar la criptografía enumerada como una munición; es preciso mencionar que según la sección 120.17 de ITAR, está prohibido el envío

47. Arms Export Control Act.
48. United States Munitions List.
49. International Traffic in Arms Regulations.

o recibo de material de defensa fuera de los Estados Unidos, de cualquier forma.

El Departamento de Estado controla la exportación de artículos de defensa, y mantuvo este control con la criptografía hasta 1996; en noviembre 15 de ese año, el presidente Clinton transfirió la competencia sobre los controles de las herramientas criptográficas del Departamento de Estado al Departamento de Comercio, mediante la orden ejecutiva número 13026[50], debido a la cada vez mayor utilización de estas herramientas para propósitos civiles.

Este cambio de competencia significó que ahora fueran reguladas estas herramientas no bajo ITAR a través de AECA sino que estuvieran en la lista de productos de comercio controlados (CCL)[51], a través de la Export Administration Act of 1969.

Para la exportación de los productos que se encuentren en la CCL se necesita un permiso previo de la BXA[52], oficina que en el año 2002 cambió de nombre y ahora es la BIS[53], que administra los controles de exportación.

Bajo la categoría de criptografía se crearon las siguientes tres nuevas subcategorías en la CCL: 1.Artículos de Cifrado. 2. *Software*. 3. Tecnologías que contienen características de cifrado.

La enmienda que sufrió la administración de exportación (EAR)[54], aunque flexibilizó las exportaciones de herramientas criptográficas, permitiendo que para las entidades financieras y transacciones bancarias se exporten cifrados[55] de 56 bits, de todas formas prohíbe aun el que cualquier persona sin la autorización previa proveyera de asistencia técnica, incluyendo entrenamiento a personas extranjeras o ayudar a personas extranjeras con la intención de desarrollar o manufacturar fuera de los Estados Unidos artículos y *software* que en los Estados Unidos estén controlados; se hace la aclaración que esta prohibición no aplica para enseñanza o discusión de información acerca de la criptografía, incluyendo por ejemplo ambientes académicos o en el trabajo de grupos encargados del desarrollo de estándares[56].

Se hizo entonces una división en productos criptográficos fuertes y débiles; se entiende por débiles aquellos de clave simétrica de hasta 56 bits, productos RSA de hasta 512 bits y productos desarrollados por teoría de curvas elípticas de hasta 112 bits[57].

En el suplemento 3 del apartado 740 de EAR se establece un listado de países para los cuales la exportación y las restricciones sobre herramientas criptográficas se flexibilizaran al máximo, estos países son: Austria, Australia, Bélgica, Chipre, República Checa, Estonia, Dinamarca, Finlandia, Francia, Alemania, Grecia, Hungría, Irlanda, Italia, Japón, Letonia, Lituania, Luxemburgo, Malta, Holanda, Nueva Zelanda, Noruega, Polonia, Portugal, Eslovaquia, Eslovenia, España, Suiza,

50. Privacy And Encryption Export Controls, Keith Aoki.
51. Commerce Control List.
52. Bureau of Export Administration.
53. Bureau of Industry and Security.
54. Export Administration Regulations, apartados 730 a 774.
55. Encryption Technology And Crime, Educom Review, Pag. 40.
56. Federal Register Doc 04-26992, December 9, 2004. Sección 744.9.
57. www.rsasecurity.com

Suecia, Reino Unido y demás países que hagan parte de la Unión Europea.

países con restricciones altas en el uso de criptografía[58]

Solamente unos pocos países tienen restricciones altas en el uso de la criptografía. Estas naciones están caracterizadas por no respetar y proteger las libertades individuales de sus ciudadanos, tienden a ser países con políticas severas de represión con tintes totalitarios y con la presencia de dictaduras en su historia más o menos reciente. En estos países existen controles fuertes para la exportación, importación y uso domestico de herramientas criptográficas:

belarus

La resolución número 217 de 1997 restringe la manufactura, tenencia y uso de productos criptográficos. Las licencias para realizar estas actividades de forma legítima son expedidas por el comité de seguridad estatal (la belorusian KGB).

china

El 15 de octubre de 1999, el gobierno chino promulgó la orden del consejo de estado número 273, la cual requiere que organizaciones o individuos extranjeros que utilicen productos o equipos de cifrado en China soliciten una autorización para la tenencia y uso de estos equipos. Prevé una excepción para misiones diplomáticas.

Las compañías interesadas en solicitar esta autorización deben identificar el uso que se le esté dando al *software* de cifrado, dar la ubicación de los computadores que usan estas herramientas, después de adquirir la autorización las empresas podrán importar *software* para cifrado para su propio uso. El gobierno prohibió la venta de productos criptográficos comerciales extranjeros.

Según noticias de la Agencia Reuters, la mayoría de compañías e individuos en China ignoran la reglamentación existente concerniente a productos criptográficos[59]. Durante las negociaciones para la entrada de China en la OMC, el gobierno de esta nación aclaró que las restricciones serían solamente aplicadas a *hardware* y *software* especializado cuyo propósito principal fuera el cifrado y que las restricciones no cubrirían sistemas operativos ni *browsers*.

En la lista de productos restringidos y prohibidos tanto para exportación e importación en la DES. 50-305, del 1º de noviembre de 1987, se restringe el comercio de dispositivos para el cifrado de voz.

58. Cryptography and Liberty 2000, An International Survey of Encryption Policy. Electronic Privacy Information Center. Washington, D.C.

59. Chinese Crypto Regs? 'Whatever', Reuters, enero 31, 2000.

KAZAKISTAN

Sus controles son fuertemente prohibitivos y restrictivos; el uso doméstico de herramientas criptográficas está controlado por el gobierno. Para la investigación, desarrollo, manufactura, mantenimiento, venta y publicidad de productos criptográficos es necesario contar con una licencia del Comité de Seguridad Nacional (KNB). Las licencias de exportación las otorga la KNB y las importaciones por la Comisión Técnica Nacional (CNS).

MONGOLIA

Existen controles de importación y uso doméstico; la criptografía solo puede ser usada por empresas bajo la autorización del consejo de seguridad nacional.

BIRMANIA

Con la expedición en 1996 de la ley para el desarrollo de computación, se prohibió el uso de la criptografía, excepto para el uso de las fuerzas amadas y agencias del gobierno. La ley exige que el ministro de Comunicaciones, con la aprobación del Consejo para el Desarrollo de la Computación, determine el tipo de computadores que podrán ser importados y ser usados. La ley también restringe el uso de Internet y cualquier clase de extranet. Las personas que sin la debida autorización posean equipos de comunicación de uso restringido podrían sufrir condenas de 7 a 15 años de prisión.

Grupos guerrilleros utilizan criptosistemas fuertes y débiles, especialmente para sus comunicaciones y almacenar su información de forma cifrada.

PAKISTÁN

Toda herramienta criptográfica, tanto en *hardware* como en *software* antes de su venta o su uso debe ser inspeccionada y autorizada por la autoridad de telecomunicaciones de Pakistán.

Pakistán posee las más estrictas restricciones para el uso de dispositivos de cifrado en sistemas de comunicación celular, por ejemplo una compañía de celulares tuvo que cancelar la prestación de sus servicios debido al uso de un criptosistema que utilizaba en la prestación de sus servicios y el gobierno al no poder decriptarlo, prohibió su implementación[60].

60. *Internet Cryptography*: 27.

RUSIA

La regulación sobre importación, exportación y uso doméstico de elementos criptográficos en Rusia es la siguiente:

En 1994, bajo el decreto 74 de febrero 11, fue promulgado el estatuto de controles para la exportación e importación de materia prima, material procesado, equipos, tecnología, información científica y técnica que se pueda usar en la producción de armas y equipos militares. El *hardware* y *software* criptográfico fue incluido en la lista de elementos que requieren licencias de exportación e importación por ser considerados de doble uso, con la expedición del Edicto número 334 de abril 3 de 1995 sección 5, en el cual se prohíbe la importación de productos criptográficos sin la respectiva autorización mediante licencia. En la sección 4 del mismo edicto, se prohíben las actividades de venta, uso y desarrollo de herramientas criptográficas sin la licencia de la agencia federal de comunicaciones e información, la cual es equivalente a la NSA norteamericana. En febrero del año 2000, debido a la intervención de la agencia federal de comunicaciones e información, Microsoft anunció la venta de su versión rusa del sistema operativo Windows sin la posibilidad del uso de cifrado fuerte.

TÚNEZ

Con el Decreto número 97-501 de mazo 14 de 1997, se reglamenta la prestación de servicios de telecomunicaciones que utilicen sistemas de cifrado, de tal forma que se requiere una autorización previa para tales servicios. Existe un sistema de depósito de claves. El ministro de Telecomunicaciones puede, en ciertos casos donde estén de por medio la seguridad nacional o el orden publico, revocar de forma total o parcial las autorizaciones para la prestación de servicios de telecomunicación que utilicen cifrado.

Otras naciones con fuertes restricciones son Irak, Irán, Turkmenistán, Uzbekistán y Vietnam.

VIII. CASOS RELACIONADOS CON LA CRIPTOGRAFÍA

CASO PHIL ZIMMERMANN

PHIL ZIMMERMANN, físico y experto en informática, desarrolló el sistema PGP, un producto de cifrado para las masas, capaz de funcionar en un computador personal, con un interfaz sencilla y fácil de usar, y con múltiples prestaciones, como confidencialidad a través del cifrado, autenticidad, brindando la posibilidad de firmar digitalmente los mensajes; todas las prestaciones se utilizaban solamente con dar click en ciertos botones, es decir de forma automática. La versión del PGP utilizaba el criptosistema suizo IDEA y se creaba el sistema de red de confianza para avalar las claves públicas.

Zimmermann pensaba distribuir su programa pgp como *shareware*, pero ante el proyecto legislativo 266 de 1991, el cual hacía obligatoria una forma de recuperación de mensajes cifrados, lanzó su *software* como *freeware*, con el inconveniente de que su programa utilizaba el algoritmo rsa, del cual el titular de los derechos era la compañía rsa Data, la cual no había licenciado a Zimmerman para usarlo en su *software*.

En junio de 1991, apareció en un *bulletin board* el programa pgp, cualquier persona desde cualquier lugar del mundo conectado a la red y a través de Usenet podría descargar el *software*.

Su proceder le generó dos problemas legales bastante disímiles. El primer problema al que se enfrentaba Zimmermann era la violación de la patente del criptosistema rsa, número 4, 405,829, y cuya licencia de forma infructuosa había intentado negociar, de tal forma que la rsa podía interponer una acción legal en contra del creador del pgp, por distribuir un producto que utilizaba un algoritmo propietario sin la respectiva licencia; sobre el otro algoritmo que utilizaba el pgp, la patente de idea fue solicitada apenas en 1992. Aunque no se llevó a los estrados, finalmente se llego a un acuerdo donde se le pagaría a rsa por cada copia del programa que se comercializara.

El segundo problema y el más grave para Zimmermann fue que se consideró que al colocar a disposición por medio de un bbs el programa criptográfico, estaría exportando armamento, lo cual estaba claramente prohibido por las normas itar (International Traffic in Arms Regulation).

En 1993, el fbi empezó a investigar a Zimmermann por exportación de municiones sin la autorización debida, fue investigado por un jurado en San José, California. Pero después de tres años de investigación el caso se derrumbó debido a que el *software* fue cargado a un servidor americano, por lo cual no estaba saliendo de la frontera, y el hecho de que alguien desde otras latitudes pudiera descargarlo hacía que no fuera muy clara la situación, además las restricciones estaban determinadas para aparatos criptográficos, y en ese momento también era muy confuso si se podía considerar el software como un aparato. En esta época, el mit estaba distribuyendo ya una versión digital del libro donde se describía el pgp, edición que se podía igualmente descargar desde cualquier lugar del mundo; lo más relevante para el desistimiento en la investigación fueron las represiones políticas del caso, ya que cobró tal relevancia la discusión sobre la criptografía, que organizaciones civiles, como la eff y otras, apoyaron la causa Zimmermann.

caso daniel j. bernstein vs. united states department of justice, 9th cir., may 6, 1999

Daniel Bernstein, científico de la Universidad de Berkeley, había desarrollado un sistema denominado Snuffle; basado en un artículo de Ralph Merkle publicado en 1990, el aporte que realizó Bernstein al desarrollo de Merkle fue hacer de la función reductora de Merkle un criptosistema.

Antes de publicar su artículo, y temiendo enfrentar problemas legales, aunque fuese netamente académico su ejercicio, procedió a averiguar la legalidad de publicar en Internet sus avances. Después de varias consultas terminó en la Oficina de Control de Comercio de Defensa, donde le informaron que necesitaría una Comodities Jurisdiction, que es un permiso especial para la exportación de elementos que tengan control de de exportación por la EAR (Export Administration Regulations) por ser material de defensa.

En septiembre de 1992, BERNSTEIN dividió su trabajo en cinco partes, para cada una de las cuales solicitó la Comodities Jurisdiction. En octubre de 1993, tras el estudio de cada una de las partes, el gobierno determinó que sus fórmulas matemáticas encajaban en las restricciones de exportación, y denegó las CJ. De tal forma que los avances académicos del profesor Bernstein no podían salir de Estados Unidos, y la publicación en Internet le había sido prohibida.

En 1995, BERNSTEIN, con la ayuda de la EFF, demandó al Departamento de Estado de Estados Unidos. La demanda se basaba en que las fórmulas matemáticas del criptosistema que había desarrollado Bernstein eran una forma de expresarse, protegida por la primera enmienda, por lo cual de forma directa se estaba atentando contra su libertad de expresión.

El caso en primera instancia se encontró en la Corte del Distrito de Northern, California. Ante esta situación, el gobierno se retractó en dos de las cinco denegaciones, argumentando que aquellas fórmulas matemáticas eran simples datos técnicos. La juez MARILYN PATEL determinó que el código fuente de un programa se podía considerar como una forma de expresión y por lo tanto le era aplicable la protección constitucional de libertad de expresión, de tal forma que prohibir la divulgación de su criptosistema era ilegal.

Antes, el 11 de mayo de 1978, la oficina del fiscal general había emitido su opinión sobre la constitucionalidad de ITAR "Es nuestra opinión que las existentes normas ITAR son inconstitucionales en tanto en cuanto establecen una restricción para la divulgación de la ideas criptográficas y de la información desarrollada por los matemáticos y científicos del sector privado" (GALENDE DÍAZ, Ob. cit.: 131).

La apelación del gobierno llegó a la Corte de Apelaciones del Noveno Circuito. Uno de los argumentos centrales del demandante fue que prohibiendo la publicación en Internet, se desconocía la decisión de la Corte Suprema que derogaba el acta de la decencia de las comunicaciones, la corte establecía que Internet era el paradigma de la democracia y merecía los niveles más altos de protección de la Primera Enmienda. En 1999 se confirmó la sentencia de la juez PATEL y se estableció que se protegía tanto la libertad de expresión de los criptógrafos como los derechos constitucionales de cada uno de los ciudadanos como potenciales beneficiados de la criptografía: se protegían, entonces, la intimidad y privacidad.

chip clipper

Con el uso cada vez más alto de Internet para comunicaciones y transacciones comerciales, y ante la necesidad de utilizar criptosistemas para proteger la información y las infraestructuras de información, a la par que se disponía en el mercado de *software* más potente para cifrar la información, el gobierno tenía que regular de forma directa (Lessig, s.f.: 99) la implementación de sistemas de cifrado en las comunicaciones, ya que era latente el problema de seguridad nacional que se avecinaba. De igual manera como cualquier ciudadano podía utilizar para usos honestos la criptografía, ésta podría ser herramienta para terroristas, narcotraficantes, traficantes de pornografía infantil y demás delincuentes, de tal forma que se planteó una solución para permitir que se usara de forma libre la criptografía dentro de Estados Unidos la solución fue el sistema Clipper.

Se propuso entonces como estándar de cifrado en comunicaciones el chip Clipper, el cual se basaba en el sistema de depósito de claves, que databa de 1989. Se buscaba en este sistema encontrar un punto de equilibrio, entre un método que permitiera la privacidad y confidencialidad en las comunicaciones, pero que brindara la posibilidad, en caso de ser necesario, de recuperar el texto plano por parte de las autoridades, ya que un método de cifrado inexpugnable por las agencias de seguridad e investigación judicial sería contraproducente para la seguridad nacional y la investigación judicial.

En 1990, ni siquiera el fbi era consciente de las dificultades que podrían tener por la criptografía. Una vez conocieron las vicisitudes que se les podrían presentar con el uso masivo de la criptografía plantearon que todo sistema criptográfico que no permitiera la recuperación del texto plano, fuera considerado ilegal (Galende Díaz, Ob. cit.: 257), pero esta propuesta se encontraba en un extremo de la discusión; en el otro extremo estaba la posición de la no regulación de la criptografía, es decir el uso irrestricto de estos sistemas, la liberalización en la exportaciones y la eliminación de patentes y limitaciones legales para el uso de la criptografía.

El sistema Clipper derivaba del Skipjack, un sistema de cifrado por bloques de longitud de clave de 80 bits, este sistema solo era una parte de Capstone. Este sistema de criptografía, al momento de comercializarlo, por razones de seguridad, decidieron empaquetarlo en un chip, ya que era mucho más vulnerable sacar una versión en *software*; la compañía Mykotronx sería la encargada de fabricar los chips.

En 1992, AT&T piensa lanzar al mercado el tsd (Telephone Security Device) 3600, el cual utilizaría el sistema des, las mayores ventajas de este teléfono son su portabilidad y facilidad de uso. El fbi y la nsa no estuvieron de acuerdo con este producto y después de una serie de negociaciones con AT&T, pensaron implementar el sistema Capstone al teléfono de AT&T.

El sistema de deposito de claves funcionaría de tal manera que la clave para el funcionamiento de cada uno de los aparatos con el chip Clipper estuviera consignada por terceros de confianza. La clave se dividiría en dos y para recuperarla

sería necesaria una orden judicial, de tal forma que sin los dos pedazos guardados por agentes diferentes no se podría descifrar la información.

El Clipper consta de un chip de 128 bits, los cuales están distribuidos en su funcionamiento de la siguiente manera: 32 bits, identificación del chip, 80 bits de longitud de clave, 16 bits de LEAF (Law Enforcement Access Field).

El 16 de abril de 1993, el presidente CLINTON dio a conocer la iniciativa del chip Clipper. "El chip es un paso importante en la solución del problema de doble filo de la criptografía: el cifrado de las comunicaciones ayuda a la privacidad y a la industria, pero también puede ayudar a los criminales y terroristas. Necesitamos el chip Clipper, además de otras soluciones, para proporcionar a los ciudadanos respetuosos con la ley el acceso a la encriptación que necesitan e impedir que los criminales la utilicen para ocultar sus actividades ilegales" (Ídem: 262)[61]

La primera dificultad por la que tuvo que enfrentarse Clipper fue un problema de patentes, pues un profesor del MIT, llamado SILVIO MICALI, había patentado en 1992 un protocolo matemático denominado Fair Cryptosystems, que se parecía al sistema de depósito de claves del gobierno, por lo que el gobierno no tuvo otro camino que pagarle un millón de dólares por la licencia de su patente (Ídem: 266).

El 4 de febrero de 1994, el presidente aprobó finalmente Clipper, conocido como Escrow Encryption Standard, estándar de cifrado que se adoptó para las comunicaciones federales.

La segunda gran dificultad que tuvo el sistema fue el descubrimiento de MATHEW BLAZE, quien desarrolló un sistema para comunicarse por medio del Clipper sin ser identificado y cambiando la clave LEAF, que era lo que permitía al gobierno tener acceso a la comunicación.

Con tan grave vulnerabilidad y bajo la sospecha por parte de los grupos de ciudadanos y de la industria en general de la existencia de más *backdoors*, y la intervención de la NSA en la adopción del estándar lo cual implicaba una carga aun mayor de desconfianza el proyecto fue un fracaso, y la industria no lo adoptó. Aunque al principio el gobierno había pensado en la obligatoriedad del mismo, por presiones comerciales y por evitar tensiones políticas se hizo de éste un sistema de adopción voluntaria.

A finales de 1994 a través de una de las primeras iniciativas políticas por Internet, se reunieron varias decenas de miles de firmas en contra de Clipper.

IX. SITUACIÓN DE COLOMBIA RESPECTO A LA CRIPTOGRAFÍA

intentando evitar la redundancia creo que no es necesario realizar una elucidación prominente sobre la importancia de la criptografía. Se ha realizado una aproximación al tema desde un enfoque técnico-legal que resalta la imprescindible atención del particular por parte de los diferentes sectores que están inmersos en las implicaciones del punto tratado, es decir toda la sociedad.

61. Statement by the press secretary, La Casa Blanca, 16 de abril de 1993.

En Colombia, la discusión sobre este tópico no ha sido exigua, es inexistente; ni el gobierno ni la sociedad civil y absolutamente ningún sector ha manifestado preocupación alguna por las ventajas o desventajas que pueden existir por la ausencia de regulación sobre la criptografía o por sus aplicaciones.

1. Siempre, en las discusiones internacionales sobre seguridad nacional discurren varias problemáticas colombianas como amenazas al orden mundial. Narcotráfico y terrorismo son estigmas que han marcado el nombre de nuestro país en el ámbito global y cuando se ha discutido en diferentes latitudes sobre criptografía se han expuesto a los narcotraficantes colombianos como asiduos consumidores de servicios criptográficos, más precisamente al cartel de Cali (Sigh, s.f.: 304). Además, no hay que olvidar que según la posición común 2004/309/ pesc del consejo de la Unión Europea de 2 de abril de 2004 dentro de los 36 grupos en el ámbito mundial considerados como terroristas, 3 de ellos pertenecen a Colombia, las farc, el eln y las auc; de igual forma, aparecen en la lista de organizaciones terroristas del Departamento de Estado de los Estados Unidos; debemos tener presente que estas organizaciones están inmersas en el trafico de drogas y se ha demostrado su vínculo con otros grupos terroristas, como el ira, Sendero Luminoso, grupos de medio oriente y mafias chinas, japonesas, italianas, rusas y del resto del planeta.

La capacidad técnica, legal y humana de los organismos de seguridad e investigación del Estado frente a evidencias que se encuentren cifradas es mínima, e inevitablemente el uso por estas organizaciones de todo tipo de comunicaciones cifradas, de gps con capacidad de cifrado para movilizarse sin dejar rastros, del uso de criptosistemas para salvaguardar los documentos con el propósito de evitar que sus contenidos se utilicen en procesos judiciales en caso de ser incautados por el gobierno, cada día aumentará.

2. Aunque el uso del comercio electrónico en Colombia no ha alcanzado un nivel de implementación y receptividad alto, desde 1999 con la Ley 527, se cuenta con una legislación que regula el tema y en la cual se encuentran las únicas normas relacionadas de forma implícita con criptografía dentro de nuestra legislación. Encontramos así, en su artículo segundo literal c) la definición de firma digital, también se halla en el literal e) del mismo artículo el concepto de edi, en el artículo 28 encontramos los atributos jurídicos que se le adjudican a una firma digital. El capítulo ii de la mencionada ley se refiere a las entidades de certificación que, como vimos, son un elemento esencial en las infraestructuras para el uso de firmas digitales. Reglamentando esta ley se expidió el Decreto 1747 del año 2000, el cual detalla sobre certificados digitales, responsabilidades y otros puntos de interés en el avance del comercio electrónico.

3. La fragilidad en las redes e infraestructuras telemáticas del Estado pone en riesgo la seguridad nacional, la inexistencia de estándares de seguridad para la protección de información neurálgica del gobierno y de los ciudadanos que está almacenada en computadores, la cual es cada día mayor, además la falta de políticas para la protección tecnológica eficaz de bases de datos, archivos judiciales

y estadísticos. Es importante recordar que en nuestro país la creación de infraestructuras tecnológicas de seguridad es realmente pobre, que la implementación de éstas se realiza mediante *software* y *hardware* que en la mayoría de ocasiones es extranjero, y que como hemos visto en los casos de algoritmos criptográficos que se pueden importar por ejemplo de los Estados Unidos son *débiles*, lo cual no brinda una real protección.

4. El cumplimiento de los compromisos adquiridos a través de los tratados OMPI de 1996, se ha realizado, a través de la tipificación de las conductas de elusión de las medidas tecnológicas de protección en el artículo 272 del Código Penal, el cual no creó excepciones, lo cual impide aprovechar de forma tajante la investigación de forma lícita en el campo criptológico por medio de los sistemas de DRM[62] y TRM implementados en los contenidos existentes en el mercado actual, lo cual genera una desventaja competitiva muy alta para la creación de este tipo de tecnologías, de forma que se está excluyendo al país de participar en este mercado.

Una interpretación exegética y estricta de este artículo también nos puede llevar a la conclusión de que un documento cifrado está protegido por una medida tecnológica de forma tal que ante un proceso judicial la autoridad no tendría la posibilidad de hallar el texto plano mediante la superación o elusión de la medida, ya que no cuenta con una habilitación legal que lo autorice y que, según la ley, la autoridad no tiene acceso a los elementos necesarios para realizar este tipo de labor; al contrario, sí existe una prohibición de tipo penal que le impide realizar tal actividad, de forma muy diferente sucede en las interceptación de comunicaciones, en donde sí existe la posibilidad mediante una orden judicial que lo habilita y que está expresamente consagrada en la ley.

5. La implementación de algoritmos criptográficos en el desarrollo de *software* es vital, y definitivamente se debe buscar la implementación de algoritmos *fuertes,* si se desea crear y consolidar una industria de creación de *software* fuerte, tal como ha sucedido en economías emergentes en este sector, como India o Corea: es necesario contar con tales algoritmos, además de realizar una discusión política sobre la conveniencia o no de la protección legal de los mismos.

6. Aunque el país parezca ir en retroceso en cuanto a sistemas de votación para la elección y participación ciudadana, es necesario que se impulse la votación electrónica como mecanismo de participación directa que ayude a formar una cultura democrática y de inclusión del pueblo en las decisiones políticas.

X. PROPUESTA

es necesaria una política estatal que les dé prioridad a los siguientes puntos:

1. Invertir en programas de investigación y desarrollo de criptosistemas. La mayor parte de recursos necesarios en este campo son en capital humano, lo cual no

62. Digital Right Management.

lo hace tan costoso y sí puede generar unos beneficios muy altos para lo sociedad. Además, siendo el Estado el que financie este tipo de investigaciones, la propiedad intelectual de los desarrollos resultantes quedará en manos de la nación.

2. Buscar cooperación internacional para la realización del punto primero, tanto en recursos económicos como en capacitación y asistencia, además de aunar esfuerzos regionales y con el sector privado; buscar que se creen ventajas y excepciones para la importación de tecnologías relacionadas con el tema, tal como ha sucedido con otros países.

3. Continuar con la posición neutral del libre uso, importación y exportación de sistemas criptográficos; de esta manera se permite y respeta la privacidad y la libertad de expresión.

4. Crear excepciones legales para la elusión de medidas tecnológicas que permitan la investigación criptográfica y que no impidan a las autoridades la investigación y el acceso a evidencias que se encuentran protegidas por medidas tecnológicas.

5. En casos en los que las autoridades no logren decriptar información cifrada, discutir un mecanismo legal que no viole derechos fundamentales (Díaz y Peraza, 2005: 10) para conminar a los implicados en casos donde se hallen posibles evidencias cifradas a que descifren la información. No se puede pensar en dar un valor probatorio a este tipo de información como indicio o crear una presunción ante tales circunstancias; es más, se debe velar porque el juez no contamine su juicio ante la incapacidad de descriptar información cifrada.

6. Crear un régimen especial de propiedad intelectual que permita la protección de algoritmos, ya que la protección de algoritmos por vía de derechos de autor no se ajusta a la finalidad de este tipo de regulación; de igual forma el *software*.

7. Crear unos estándares de protección de las infraestructuras de la información de las entidades del Estado y de aquellas organizaciones que contengan información sensible sobre los ciudadanos.

8. Estimular el comercio electrónico y exigir el cumplimiento de unas medidas mínimas en el tratamiento de información digital, para asegurar la autenticidad, el no repudio, la integridad, el sellado de lugar y datación digital, asegurando la fuerza probatoria de los documentos y mensajes digitales.

9. Garantizar la privacidad a través de la protección de datos personales de los colombianos[63] (*Habeas Data*), implementando medidas en las cuales se podrían considerar el uso de herramientas criptográficas como un elemento que disminuya la vulnerabilidad de información sensible.

63. Documento gecti 02 de 2004. Revista de Derecho, comunicaciones y nuevas tecnologías.

BIBLIOGRAFÍA

Caballero Gil, Pino (1997). *Seguridad Informática, Técnicas Criptográficas*. México: Alfaomega Grupo Editor.

Cayo Suetonio Tranquilo. *Los Doce Cesares*.

Cesar Cayo Julio. *Guerra de las Galias.*

Díaz, Carolina y Laura Peraza (2005). "La Criptografía: Una guerra de Piratas y Corsarios", en *Revista Alfa Redi*, Mayo 2005.

Documento gecti 02 de 2004. *Revista de Derecho, comunicaciones y nuevas tecnologías*.

Galende Díaz, Juan Carlos (1995). *Criptografía. Historia de la escritura cifrada*. Madrid: Editorial Complutense.

Guerrero, María Fernanda (s.f.). *La Ciberdelincuencia*.

Lessig, Lawrence (s.f.). *El código.*

Litt, Robert S. (1998). *Códigos Secretos*. Departamento de Justicia de Estados Unidos.

Moreno, Agustín (s.f.). *Clases de Criptografía.*

Negroponte, Nicolas (s.f.). *Ser digital*.

Ríos, Wilson Rafael (2002). *Revista Propiedad Inmaterial*.

Sgarro, Andrea (1990). *Códigos Secretos*. Madrid: Ediciones Pirámide.

Shannon, C.E. (1949). *Communication theory of secrecy systems*. Bell system technical journal, Vol.28.

Shannon, Claude (s.f.). *Mathematical Cryptology, for computer Scientists and Mathematicians.*

Sigh, Simon (s.f.) *Cripto*.