Cripto-conflicto:

una cuestión esencial de naturaleza política, jurídica y estratégica

José María Molina Mateos

Doctor en Derecho

Resumen: La criptología como medio para proteger la información y las comunicaciones, encierra en sí misma un conflicto político y jurídico de difícil solución dada sus implicaciones geopolíticas, estratégicas, tecnológicas o económicas y, simultáneamente, resulta esencial para la protección de intereses, derechos y libertades, especialmente el 'derecho a la intimidad' y el 'derecho a la seguridad', en sus múltiples variables y relaciones con el 'derecho al secreto de las comunicaciones' y con la 'libertad de expresión'. Lo que exige a la criptología, además de efectividad técnica para dar cumplimiento del 'derecho al secreto criptológico', su sometimiento al resto del ordenamiento jurídico, dando lugar a debates como el de 'privacidad vs. seguridad' o el menos explícito de 'seguridad vs. seguridad', en el marco del más genérico y amplio de 'seguridad vs. libertad'.

Todo ello comporta un enfrentamiento de diversos intereses y derechos que tienen consecuencias distintas según la naturaleza de la información cifrada, el tipo de criptología utilizada, el tratamiento legal que dé a la criptografía el ordenamiento jurídico de aplicación y, los eventuales condicionantes que puedan contribuir a configurar el grado de independencia operativa posible derivados de los alineamientos internacionales.

Palabras claves:

cripto-conflicto, cripto-dilema, cripto-controversia, criptología, criptografía, criptoanálisis, cifrado, seguridad de la información, seguridad nacional, seguridad internacional, seguridad informática, ciberseguridad.

Crypto-conflict:

an essential issue of political, legal and strategic nature

Abstract:

Cryptology as a means to protect information and communications, itself contains a political and legal conflict difficult to solve given its geopolitical, strategic, technological or economic implications and, simultaneously, is essential for the protection of interests, rights and freedoms, especially the 'right to privacy' and the 'right to security', in its multiple variables and relations with the 'right to secrecy of communications' and with 'freedom of expression'. What requires cryptology, in addition to technical effectiveness to comply with the 'right to cryptological secrecy', its submission to the rest of the legal system, leading to debates such as' privacy vs. security 'or the least explicit of' security vs. security ', in the framework of the more generic and comprehensive' security vs. freedom'.

All this entails a confrontation of diverse interests and rights that have different consequences according to the nature of the encrypted information, the type of cryptology used, the legal treatment that gives the cryptography the legal system of application and, the eventual conditions that may contribute to set the degree of possible operational independence derived from international alignments.

Keywords:

crypto-conflict, crypto-dilemma, crypto-controversy, cryptology, cryptography, cryptanalysis, encryption, information security, national security, international security, computer security, cybersecurity.

*

La infalibilidad del mecanismo para la codificación segura de los protocolos criptográficos resulta ser imposible, porque imposible es una criptografía infalible. Y no tanto por razones tecno-criptográficas, presentes y previsibles, que podrían permitirlo de forma periódica en virtud de los ciclos evolutivos de la criptografía y el criptoanálisis, sino por razones políticas, jurídicas o geoestratégicas en un mundo como el que conocemos.

La criptografía, en sí misma, es un problema político y jurídico global de difícil solución dada sus implicaciones geopolíticas, estratégicas y tecnológicas. Que se ha amplificado al unírsele la expansión de las necesidades de seguridad en el ámbito cibersecutirario o la dependencia que tienen de la criptografía los nuevos sistemas tecnológicos, como 'blockchain' (cadena de bloques) u otros de naturaleza análoga, de previsible fuerte influencia en la economía digital, la política, la estrategia y amplios aspectos de la vida social, empresarial y administrativa, de lo que deviene una subordinación de todos ellos a la misma, sus conflictos, problemas y limitaciones. De esta forma, el clásico 'cripto-conflicto' incrementa aún más su dimensión y, en consecuencia, la necesidad de su análisis.

Fig. 1. Nudo gordiano de Haken

https://culturacientifica.com/2017/12/13/la-artista-anni-albers-the-walking-dead-la-teoria-nudos/

Calificación de la información.

Como quiera que estamos en un tema de información, en este caso, relativo a su protección, que es una de las dimensiones de la estrategia de la misma y, la información en todos sus tipos y variantes siempre es un tema político esencial en cualquier sociedad, conviene distinguir en el seno de la gran controversia los dos tipos básicos de información: la 'información privada' y la 'información pública' y que, cada una, tiene un tratamiento jurídico-político diferente, producto de un ya largo debate, de efectos altamente significativos. Y que, dentro de la información pública y, en ocasiones, de la privada, está la información de naturaleza estratégica.

El resultado de este debate ha cristalizado en las constituciones de todos los países del mundo y en los textos internacionales sobre derechos humanos, de los cuales se deriva que, la regla general de toda información privada es el secreto y la de la información pública es la transparencia. Mientras que, en base a los mismos, debates y textos, la transparencia es la excepción en la información privada y el secreto es la excepción en la información pública.

Entre los instrumentos para una protección real y efectiva de la información y las comunicaciones, sean de uno u otro tipo, secularmente se ha venido utilizando la criptología. Uno de los elementos que más perturban el debate en torno a la protección criptográfica, tal vez sea la falta o insuficiente distinción, si no clara confusión, cuando esta se aplica a uno u otro tipo de información. Lo que sea información privada (datos personales, empresarial, comercial, industrial, profesional, etc.)[1] o información pública (económica, financiera, seguridad, defensa, administrativa, etc.) y, en ambos casos, cuando sea estratégica o de directa y significativa repercusión en los grandes intereses generales, no es irrelevante habida cuenta de que el ser de una u otra naturaleza tiene efectos diferentes.

En consecuencia, existe un primer requerimiento para el análisis y posterior debate, que necesita de una calificación de la información atendiendo a criterios políticos y jurídicos para, en base a ello, determinar la protección requerida a la luz de la normativa existente, sólo después es cuando entra en juego la criptología, como instrumento para lograr la protección real y efectiva de la misma (a modo de 'paraguas

[1] Para Hannah Arendt, filósofa política, lo social aparece como un espacio intermedio entre lo público y lo privado. Así lo social se expande absorbiendo tanto lo privado como lo público. La política se convierte en mera función de lo social, mientras que lo privado, ante la amenaza de lo social, se refugia en lo íntimo.

criptológico'), derivada del cumplimiento de un mandado jurídico previo que, indudablemente, entre otros, ha de tener en cuenta sus efectos sobre la libertad de expresión e información y la transparencia de lo público toda vez que la protección criptológica en sus máximos niveles puede llegar a crear reductos impenetrables.

Fig. 2

https://www.google.es/search?q=departamento+de+seguridad+nacional&biw=1366&bih=662&source=lnms&tbm=isch&sa=X&ved=0ahUKEwil17qfuJnRAhWBtxoKHfG3Aq4Q_AUIBigB&dpr=1#imgrc=3vni-VRBHFN1EM%3A

Cifrado

El cifrado como instrumento de seguridad de la información y las comunicaciones es el resultado de aplicar a las mismas uno o varios algoritmos de cifra utilizando técnicas criptográficas.

Por información cifrada se puede entender aquella que el mensaje se expresa y ocultan bajo estas técnicas y, la comunicación cifrada sería aquella que se realiza mediante señales que previamente han sido sometidas a técnicas criptográficas o bien señales no cifradas en las que el contenido de lo comunicado sí lo está.

El cifrado es un proceso material, real y efectivo que mediante un hecho consumado de naturaleza técnica, configura un ámbito de protección propiamente dicho que impide el acceso de terceros a la información o a la señal de comunicación antes de ser cifrada, a la que se aplica.

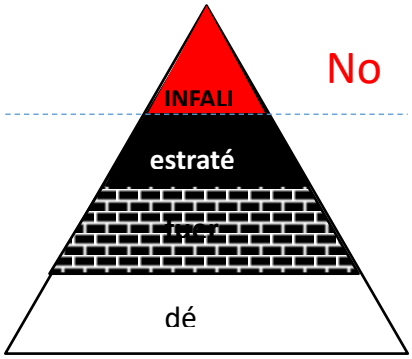
La utilización de técnicas criptográficas puede tener efectos antitéticos y estar amparadas y reguladas por el derecho, o no. Aún en los casos utilizados para el cumplimiento de derechos, se dan situaciones de conflictos entre estos.

Todos estos conflictos confluirían en un punto crítico de equilibrio de naturaleza jurídica, política, estratégica y técnica, donde la protección criptológica ha de ser efectiva respetando estas dimensiones y el derecho al secreto criptológico.

Categorías criptográficas básicas y regulación.

La criptología aunque como ciencia pueda ser considerada unitariamente, en su seno conviven multitud de tipos, sistemas, métodos, algoritmos…etc., que simplificando se pueden agrupar en tres grandes categorías: lo que se conoce como la *'criptología blanda'*, la *'criptología dura o fuerte'* y la *'criptología estratégica'.* La criptología 'infalible' de forma permanente como se ha indicado, no existe.

Al ser una clasificación técnica se refiere a la menor o mayor robustez y consiguiente consistencia protectora, en definitiva, mayor seguridad y eficacia en la protección, en lo que interviene muy especialmente, entre otros factores, el algoritmo de cifrado, siempre dentro de los mínimos y máximos a los que su naturaleza, tecnología y finalidad, obligan.



(*Fig. 3 Elaborada por el autor)*

De igual modo que la criptología desde el punto de vista técnico tiene tres referentes en torno a los que se forman las categorías indicadas, los ordenamientos jurídicos pueden contemplar o no su regulación o, en su caso, prohibir su uso. Dentro de los que optan por permitir la criptología, se pueden clasificar en 'permisivos' o 'restrictivos', en función de su mayor o menor tolerancia al uso de la misma y la mayor o menor fortaleza de la utilizada.

Un *ordenamiento criptológico permisivo*, es el que tolera la general utilización de criptología y que, a pesar de su consistencia, su aplicación está regulada de tal forma que no obstaculiza el normal funcionamiento del Estado de Derecho. Su umbral sería el nivel necesario para garantizar razonablemente desde el punto de vista técnico el secreto criptológico, su techo vendría determinado por la imposibilidad material de hacer efectivo el cumplimiento de una resolución judicial que ordenase la interceptación de la comunicación, la aprehensión del contenido del mensaje y el conocimiento de lo comunicado. De este modo se evita que se produzcan reductos impenetrables de información, incompatibles con la legalidad y la convivencia, que impedirían la prevención y persecución del delito y, sin duda, sería un ámbito idóneo, para el crimen organizado, narcotraficantes, terroristas y delincuencia en general. Esta modulación, en España, viene determinada por lo dispuesto en la Constitución, Ley de Telecomunicaciones y Ley de Enjuiciamiento Criminal, básicamente.

Por el contrario, un *ordenamiento criptológico restrictivo*, es aquel que aun permitiendo el uso de la criptología, limita sus capacidades técnicas. La criptología estratégica se reservaría para la protección de la información en los casos excepcionales en los que, por ley, quede excluida su transparencia y requiera ser fuertemente protegida por ser relevantes para la seguridad y la defensa nacional −elementos indispensables para una paz efectiva, la estabilidad, el progreso sostenible,

el bienestar y la garantía de derechos y libertades− al permitir neutralizar amenazas o agresiones que se realicen, incluso, sin respeto al derecho internacional. Su umbral vendría determinado por los niveles criptológicos y tecnológicos con potencia suficiente para resistir los envites de las capacidades criptoanalíticas internacionales más avanzadas y conocidas, sin que tenga otro techo que los límites tecnológicos y científicos, matizados por los condicionantes geopolíticos derivados de los alineamientos y compromisos internacionales que el país haya decidido aceptar en su política exterior, adoptado por los órganos correspondiente, dotados de capacidad jurídica, política y técnica, para ello.

Los componentes de este sistema generalmente conviven y solo desaparecerían, eventualmente, en el escenario de una globalización efectiva en un mundo regido internacionalmente por los principios del Estado de Derecho, circunstancia que, en principio, no se vislumbra en el horizonte de la política ni del Derecho Internacional.

En el caso de los ordenamientos 'prohibitivos', se limiten a no permitir el uso de la criptología o, al menos, no permitir su uso fuera de las aplicaciones tradicionales de inteligencia, seguridad y diplomacia, o economía y finanzas estratégicas.

Derecho al secreto criptológico.

De la posibilidad técnica de aplicar la criptología en general, y de su propia naturaleza, ha surgido el 'derecho al secreto criptológico' del que, a su vez, se deriva que el cifrado de información ha de realizarse con plena garantía técnica del secreto de su contenido.

Entendiendo por ello, que el cifrado sea ejecutado con el grado de seguridad y efectividad técnica necesaria para que solo pueda ser descifrado mediante la utilización de las claves asignadas a su destinatario.

El derecho al secreto criptológico en España, es de naturaleza infraconstitucional y no fundamental, aunque está intrínsecamente ligado al derecho a la intimidad del artículo 18.1 de la CE, del que es complementario y, en el caso de un proceso comunicativo está orientado a la protección 'de lo comunicado'.

Este derecho es diferente del ‘derecho al secreto de las comunicaciones’ que es un derecho fundamental regulado en el art. 18.3 de la CE y se predica de la comunicación en sí misma, del proceso, esto es del procedimiento de relación significante entre personas que está jurídicamente protegido frente a cualquier interceptación (ya sea retención, suspensión del curso, apoderamiento antes de que llegue a su destino o, incluso, acceso a su contenido), ambos suelen confundirse tal vez porque para acceder a “lo comunicado” en una comunicación es necesario acceder a la comunicación misma, acceder a su contenido y, si este estuviese cifrado, lograr su desciframiento. Solo en este último caso se estaría en presencia del ‘derecho al secreto criptológico’.

Lo que puede suponer que la violación del secreto criptológico sería un atentado a la intimidad y sólo se da cuando se está en presencia de una información cifrada. Además podría haber una violación al secreto de la comunicación, si para conseguir el texto cifrado se ha violentado un proceso comunicativo.

Casos que pueden ejemplificar uno y otro derecho serían las violaciones denunciadas por Edward Snowden, típico caso de violación del ‘derecho al secreto de las comunicaciones’ al producirse con metadatos de comunicaciones de los que se obtienen los ‘patrones personales’ sin necesidad de acceso a lo comunicado, bien estuviesen en claro o cifradas. O, la controversia surgida entre Apple y el F.B.I. (o en España el caso de Diana Quer) y, algún otro actualmente sub iudice, que serían casos en los que, además de acceder a la comunicación, típico caso de ‘secreto de las comunicaciones’, al pretenderse acceder a lo comunicado por estar cifrado, se estaría ante un supuesto de ‘derecho al secreto criptológico’.

Debates

En el marco del debate ‘seguridad vs. libertad’ el cripto-conficto aporta toda una serie de debates específicos entre los que, el más generalizado y conocido, está referido a la información privada en el que se da la clásica confrontación entre *privacidad vs. seguridad*. Junto a él, existen otros debates entre los que destaca el referido a la interceptación y acceso a la información pública que le han precedido y, sin duda, le seguirán, formando la otra parte, complementaria de la primera, entre los que

cabe destacar los relacionados con la confrontación que se da entre *seguridad vs. seguridad*, menos explícito en la sociedad, pero subyacente de forma permanente. A ellos se les une el debate de cómo afecta el uso de la criptología a la 'libertad de expresión' por cuanto aquella comporta la realización efectiva y material de una sustracción de la información al conocimiento público por lo que resulta imprescindible que tenga el soporte legal necesario.

Estos debates configuran sucintamente la gran controversia que se cierne en torno al 'derecho al secreto de las comunicaciones' y al del 'secreto criptológico', con todo lo que ello implica para el derecho a la intimidad y el derecho a la seguridad. Tanto la protección de la privacidad como de la seguridad, genéricamente consideradas y en el marco del Estado de Derecho, necesitan de una criptología de nivel 'suficiente', con el límite de estar sometida al control de la ley, en cuyo contexto, privacidad y seguridad, encontrarán el equilibrio requerido.

Todo cambia cuando la confrontación se da en entornos en los que no opera el Estado de Derecho, como es el entorno internacional o cuando la confrontación tiene lugar entre la *seguridad vs. seguridad*, que alcanza su máxima expresión cuando se produce al margen del derecho internacional. En estas circunstancias es cuando surgen, de una parte, los desarrollos criptológicos '*propios*' a niveles estratégicos −de quien puede hacerlo y tiene capacidad para ello− que pueden llegar a ser, incluso, desconocidos para el resto de la comunidad internacional (como ya ocurrió, en su momento, con la famosa ENIGMA hasta que su criptología fue rota por el equipo de Alan Turing), como medio de protección de sus activos críticos y, de otra, la utilización de la criptología fuerte, '*ajena*' (y con mayor motivo, la estratégica), desarrollada por países terceros, como una amenaza, por ser inmune a sus ataques u ocasionar graves dificultades a su criptoanálisis.

Esta confrontación, que ya sale del ámbito técnico y científico-criptológico para entrar en el de la inteligencia, toma una especial importancia y dimensión con la aparición del ciberespacio como quinta dimensión de los ámbitos de confrontación globales y de posicionamiento de poder a escala planetaria.

Estos fenómenos van más allá de cada uno de los países del mundo individualmente considerados, para alcanzar una dimensión global, teniendo por componentes esenciales las libertades individuales, los derechos fundamentales, las

soberanías nacionales, la tecnología y la criptología, la política y la geopolítica, la seguridad internacional e, incluso, la economía global, muy especialmente, la digital.

Qué duda cabe que la sociedad de la información y el conocimiento tiene consecuencias para la privacidad del individuo y la soberanía de los Estados tal como se venían entendiendo. Y que, ambas, requieren ser reconfiguradas a la luz de la nueva realidad. Precisamente por ello, se demanda un esfuerzo intelectual que permita apreciar en conjunto el marco en el que se inscriben, poder ver sus interrelaciones y, en su caso, abordar el diseño de soluciones, tanto desde las perspectivas político-jurídicas como tecno-securitarias subyacentes y, obviamente, las criptológicas.

Percepción global de los debates en torno a la criptología.

Solo un enfoque amplio de este sensible tema, arrojará la luz necesaria para abordar razonablemente los conflictos políticos y jurídicos que subyacen en la utilización del cifrado de información, comunicaciones y datos en una sociedad global hipercomunicada.

En todo caso, este asunto, al afectar a la intimidad, el secreto de las comunicaciones, a la libertad de expresión, derecho a la información, transparencia pública, en determinados casos a la seguridad nacional o internacional, etc., es un tema político esencial, al que hay que darle una solución adecuada a su naturaleza. Solo después, vendrá la respuesta jurídica y, finalmente, la tecnológica y la criptológica.

La cuestión se torna aún más compleja cuando hablamos de entornos tecnológicos amplios donde se dan comunicaciones, informaciones y tecnologías de todo tipo, como es el caso del ciberespacio o, simplemente, de Internet que son globales, en un mundo que política y jurídicamente no lo es.

Se suele hablar de un Internet abierto, seguro, confiable e inclusivo y, con respecto a su seguridad, que los gobiernos no deben buscar debilitar los estándares de encriptación y que se debe alentar a la comunidad técnica a incorporar soluciones de protección de la intimidad y la seguridad en todas las normas y protocolos de Internet. Así como que los fabricantes de dispositivos tecnológicos deben mejorar la privacidad y seguridad de sus productos tanto como sea tecnológicamente posible y que, la

competencia, debe hacer que los compradores opten por los productos TIC más seguros, en definitiva, que la estructura central de Internet sea estable y segura.[2]

Para poder dimensionar la realidad de la seguridad de la información y las comunicaciones y, específicamente, la que le proporciona la criptología en el entorno tecnológico, político y jurídico actual (superdesarrollo tecnológico vs. infradesarrollo social, político y jurídico), se requiere ir más allá de afirmaciones como las indicadas, realizando mayores precisiones y algunas matizaciones.

En la reconfiguración de la privacidad y la soberanías derivadas del superdesarrollo tecnológico, no hay que partir de cero, y tal vez sea conveniente releer la 4ª Enmienda a la Constitución de Estados Unidos[3], todas las constituciones del mundo y algunas normas internacionales sobre Derechos Humanos, especialmente el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, firmado en Roma en 1950, dónde en su artículo 8.2 tal vez encontremos las orientaciones suficientes que determinan lo que se puede, o no, hacer, al menos en el ámbito europeo, al prever que no puede haber injerencia de la autoridad pública sino en tanto en cuanto esté prevista por ley y constituya una medida que en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás, lo que en definitiva presupone que sí puede haber injerencia por parte de la autoridad pública en los demás casos.

Por cuanto se refiere a las soberanías de los Estados, igualmente conviene releer las constituciones nacionales y los textos internacionales, en este caso, sobre

---

[2] "Un momento crítico para el futuro de Internet", artículo publicado por Pablo Bello en la revista Política Exterior, número 172, julio/agosto 2016. Pablo Bello es miembro de la Global Comisión on Internet Governance. Ha sido Viceministro de Telecomunicaciones de Chile y es director ejecutivo de la Asociación Internamericana de Empresas de Telecomunicaciones.

[3] IV Enmienda de la Constitución de los EE.UU.: "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas".

‘libertad de expresión y derecho a la información’ y sus limitaciones[4], observar con realismo el escenario internacional, detectar los desafíos de un mundo incierto, los intereses geoestratégicos en juego y la seguridad internacional. Y tras reconfirmar el alineamiento internacional −en el caso español, señalado por las huellas de la historia, los valores, las formas, el estilo de vida de nuestra sociedad, las posiciones tradicionales en política internacional y nuestro anclaje en la civilización occidental−, fijar las posiciones en política exterior que permitan hacer frente a los retos imperantes.

De todo ello se derivan condicionantes que pueden contribuir a configurar el grado de independencia operativa posible, con eventuales efectos para los entornos tecnológicos, securitarios y criptológicos, vectores esenciales de nuestra posición internacional, especialmente en el marco de la globalidad electrónica en la que el mundo está inmerso.

Para tener una percepción global del debate en torno a la criptología y disponer de una visión estratégica de la misma, se ha de abordar el fenómeno en su conjunto, contemplando toda su gama de posibilidades tecnológicas, securitarias, jurídicas, políticas y estratégicas en sus aplicaciones, tanto a la protección de la información pública como a la privada, la defensa de intereses individuales y colectivos, en el marco jurídico nacional e internacional en el que se desenvuelve, en relación con el contexto geopolítico global proyectado en el ciberespacio y en la economía. Y, atendiendo a que es la propia criptología la que lleva en sí misma el conflicto, toda vez que en base a la misma ciencia se protege criptográficamente una comunicación o se la criptoanaliza para acceder a la comunicado, por lo que la solución de este dilema viene dada por la naturaleza de la información protegida y su tratamiento legal.

La criptología es un vector esencial de la ciberseguridad, considerada como la acción del Estado constituida por el conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, en el caso español configurada como uno de los ámbitos de especial interés[5] de la Seguridad Nacional. Que protege la libertad, los derechos y bienestar de los ciudadanos, garantiza la defensa de España y sus principios y valores constitucionales, así como contribuye junto a nuestros socios y

---

[4] En el caso español recogido en el artículo 20 de la Constitución de 1978.

[5] Artículo 10 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos, mediante la defensa de la infraestructura tecnológica, de los servicios que estas prestan y de la información que manejan.[6]

Precisamente en este último aspecto, la defensa de infraestructuras, servicios e información, la criptología resulta determinante.

Se ha de considerar que la criptología es una herramienta para hacer real y efectiva la protección material de determinados derechos, intereses y libertades, que son subyacentes y previos a la misma, que están perfectamente regulados y jerarquizados. Por ello, en estos y en sus relaciones recíprocas y eventuales conflictos es donde hay que buscar la solución a lo que se ha denominado 'cripto-conflicto' o 'cripto-controversia', (que sería un aspecto específico de la '*controversia securitaria*'), toda vez que la criptología es meramente instrumental, se ocupa solo de una parte, importante, sin duda, pero solo parte, y está al servicio de intereses, derechos y libertades. Y esta cumple su finalidad, simplemente si es efectiva en la protección del secreto criptológico, en función del nivel exigido en cada momento en el entorno de un marco tecnológico y regulatorio, adecuado, tanto nacional como internacional.

---

[6] Estrategia de Seguridad Nacional. http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017.

CRIPTO-CONFLICTO DIGITAL

(elementos básicos indicativos)

1. Políticos

a) Información pública

b) Información privada

c) Libertades de expresión, información y conciencia

d) Ámbitos de confidencialidad

2. Jurídicos

a) Secreto de las comunicaciones
b) Secreto criptográfico
c) Prevención y persecución del delito
d) Regulación legal de la criptología

3. Tecno-criptológicos

a) Criptografía fuerte
b) Criptografía débil
c) Criptografía estratégica
d) Criptoanálisis

4. Geoestratégicos

a) Soberanía de los Estados
b) Seguridad Nacional, Internacional y Defensa
c) Alineamientos políticos internacionales derivados de la política exterior

Conclusión.

El cripto-conflicto es el enfrentamiento de los distintos intereses y derechos, y de estos entre sí, surgido de la aplicación de la criptología para proteger información y las comunicaciones, atendiendo a la naturaleza de la información, a los derechos

concernidos, el tipo de criptología utilizada y su regulación en el ordenamiento jurídico de aplicación, así como a los eventuales condicionantes que puedan contribuir a configurar el grado de independencia operativa posible derivados de los alineamientos internacionales. En definitiva, el gran 'cripto-conflicto digital', sería un sumatorio de conflictos de naturaleza política, jurídica, geopolítica y tecno-criptológica, cuya solución final conjunta habría que buscarla en el balanceo ponderado de los puntos de solución de los distintos sub-conflictos intervinientes con sus intereses y derechos en juego, así como de los resultantes de sus interrelaciones.

El grado de complejidad es elevado dado que tanto en cada uno de los conflictos intervinientes, como en el resultante, los elementos en juego responden a principios distintos, operar bajo coordenadas diferentes y defienden intereses que pueden llegar a ser contrapuestos, por lo que, aunque tengan algunos elementos comunes, tiene un tratamiento y consecuencias, políticas, jurídicas y geoestratégicas, diferentes.

Un reto para los diseñadores de algoritmos tal vez sea el encontrar el algoritmo que dé respuesta a todo ello y, para politólogos y juristas, diseñar el marco regulatorio adecuado.

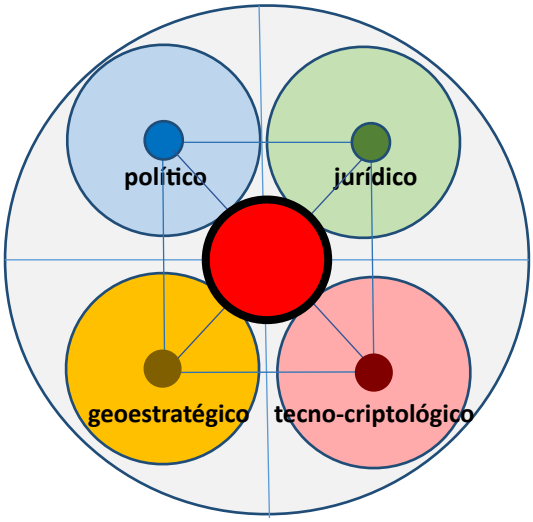


Fig. 4. Elaborada por el autor

NORMAS RELACIONADAS CON LA CRIPTOLOGÍA

1. Normas internacionales.

-Declaración Universal de Derechos Humanos.

-Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales.

-Pacto Internacional de Derechos Civiles y Políticos.

-Convenio de Viena sobre Relaciones Diplomáticas de 18 de abril de 1.961.

-Convenio de Viena sobre Relaciones Consulares de 24 de abril de 1.963

-Constituciones del mundo: https://www.constituteproject.org/

- http://www.cryptolaw.org/cls2.htm#sp

2. Normas nacionales.

-Constitución Española.
-Ley Orgánica 1/1982 de protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal
-Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
-Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
-Ley 11/2002, de 6 de mayo, del Centro Nacional de Inteligencia.
-Ley 9/2014, de 9 de mayo, de Telecomunicaciones.
-Ley 21/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica.
-Ley 20/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
-Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
-Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
-Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores,
-Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros automatizados que contengan datos de carácter personal.
-Real Decreto 421/2004, de 12 de marzo por el que se regula el Centro Criptológico Nacional.
-Real Decreto 3/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3. Normas europeas.

-Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos.

JURISPRUDENCIA DE INTERÉS PARA LA CRIPTOLOGÍA

-Sentencia del Tribunal Europeo de Derecho Humanos de 3 de abril de 2007.

-Sentencia del Tribunal Constitucional 114/1984, fundamento jurídico 7º.

-Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre.

-Sentencia del Tribunal Constitucional 96/2012, de 7 de mayo.
-Sentencia del Tribunal Constitucional 241/2012, de 17 de diciembre.
-Sentencia del Tribunal Constitucional 10/2002, de 17 de enero.
-Sentencia del Tribunal Constitucional 127/2003, de 30 de junio.
-Sentencia del Tribunal Constitucional 189/2004, de 2 de noviembre
-Sentencia del Tribunal Constitucional 173/2011, de 7 de noviembre.
-Sentencia del Tribunal Constitucional 115/2013, de 9 de mayo, Fundamento Jurídico 5. Fundamento Jurídico 6.
-Sentencia del Tribunal Constitucional 70/2002, de 3 de abril, Fundamento Jurídico 10.
-Sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre.
-Sentencia del Tribunal Constitucional 34/1996, de 11 de marzo.

-Sentencia 241/2012, de 17 de diciembre, Fundamento Jurídico 7.

-Sentencia del Tribunal Supremo 2844/2014, de 16 de junio.