ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

115/2013 22 noviembre de 2013

*José María Molina Mateos**

CYBERDILEMMA

Visitar la WEB Recibir BOLETÍN ELECTRÓNICO

CYBERDILEMMA

Resumen:

Las periódicas apariciones de acontecimientos relacionados con la pugna entre la libertad y la seguridad, han adquirido mayor virulencia con la llegada de la era digital, cuyos ejemplos más paradigmáticos son los casos Wikileaks y Snowden. La abrumadora magnitud con la que se presentan no debe ocultar que bajo su aparente novedad subyace un dilema clásico, cuya solución requiere prestar especial atención a las nuevas y complejas circunstancias que lo rodean, que no todas son de naturaleza digital, y en cuya base está la toma de conciencia de la necesidad de protegerse en un nuevo entorno.
Para contribuir a situar las variables del ciberdilema se propone un modelo de referencia basado en su relación con las magnitudes más representativas.

Abstract:

The periodic occurrences of events related to the conflict between freedom and security, have become more virulent with the advent of the digital age, whose clearest examples are the cases Wikileaks and Snowden. The overwhelming magnitude that occur should not hide that under his apparent novelty lies a classic dilemma, whose solution requires special attention to the new and complex surrounding circumstances, not all are digital in nature, and whose base is the awareness of the need for protection in a new environment.
To help place cyber-dilemma variables proposes a reference model based on its relationship with the more representative magnitudes.

Palabras clave: Dilema digital, ciber-dilema, ciberseguridad, ciberespacio, derechos y libertades en la Red, modelo ideal ciber-dilema.

Keywords: Digital dilemma, cyber-dilemma, cyber-security, cyberspace, rights and freedoms on the Network, ideal model cyber-dilemma.

"Vos, Sancho, iréis vestidos parte de letrado y parte de capitán, porque en la Ínsula que os doy tanto son menester las armas como las letras, y las letras como las armas".

(El Quijote)

INTRODUCCIÓN

Las noticias que han inundado los medios de comunicación de todo el mundo relacionadas con las revelaciones de Edward Snowden, independientemente de la dimensión humana del caso, la calificación moral y legal que merezca su conducta y las consecuencias que tenga, han situado a la sociedad internacional ante unos hechos que, de ser ciertos, además del escándalo político consiguiente, no serían otra cosa que la expresión de un viejo dilema puesto de manifiesto en el mundo digital en su versión más actualizada, que ha sacudido las opiniones públicas del planeta como ninguno otro de naturaleza análoga lo había hecho anteriormente, y que ya tuvo un precedente el caso Wikileaks.

El ideal de cualquier organización, sea pública o privada, civil o militar, nacional o internacional, industrial o financiera, es saber todo de sus competidores y, simultáneamente, evitar que estos tengan acceso a sus activos de información. Del modo en que logren ambas cosas dependerá su éxito y reputación.

En ese marco actúan las agencias de inteligencia al servicio de los Estados, en la doble función de adquirir y proteger la información, con el mayor secreto y sigilo posibles como forma de no perjudicar sus logros.

Que estos servicios traten de obtener información… parece lo obvio. Que la protejan… es también su responsabilidad. Que lo hagan sin darlo a conocer… es un requisito de eficacia. Que realicen su tarea de acuerdo a la ley… es una exigencia ineludible.

Según los datos publicados en el caso Snowden, al parecer, se habría cumplido al menos con la legalidad formal, pero a juzgar por las filtraciones producidas, lo que no parece que se haya cumplido plenamente es con la protección eficaz de su información, tanto por los sujetos pasivos de las observaciones como por las propias agencias responsables de realizarlas.

Los servicios de inteligencia desde el momento en que existen, hemos de presumir que realizan las actividades que le son propias y que, a mayor potencia y prestigio tanto suyo como del país al que pertenecen, lo harán de una forma más eficiente. Pero por muy secretos que sean, la historia demuestra que sus actividades, antes o después, son conocidas, con las consecuencias –de todo orden− que ello comporta.

El hombre convive con esta realidad desde sus orígenes, por algo el espionaje es calificado como la segunda profesión más antigua del mundo y desde siempre ha suscitado conflictos que en cada época se han ido solucionando de una u otra forma. Siempre ha sido un asunto delicado.

GLOBALIDAD

La globalización digital es un fenómeno que ha llegado de la mano de las TICs y es paralelo al surgimiento del ciberespacio, adalid de la misma. Se caracteriza por la inmensidad de los espacios comunes y el debilitamiento de las fronteras en todos los aspectos de la vida de relación tanto territoriales, económicos o sociales, como políticos, jurídicos o securitarios, entre otros.

Todo ello ha generado grandes ventajas de naturaleza global, que comportan inconvenientes de la misma dimensión, necesitados de respuestas que también tengan el mismo alcance, lo que requiere, de forma muy especial un alto nivel de coordinación de todos los actores implicados, atendiendo fundamentalmente a las dimensiones informacionales, securitarias, tecnológicas, económicas, jurídicas y políticas.

El carácter global y alta complejidad del ciberespacio requiere de una estrategia internacional para su utilización y desarrollo que armonice los distintos componentes que entran en juego, por lo que alcanzan una dimensión de efectos inconmensurables y requiere de su acotación intelectual precisa como paso previo a su solución.

El carácter global del ciberespacio conlleva que los riesgos derivados del mismo también son globales -y consiguientemente su defensa- aunque bien es cierto que el carácter silente de muchas de sus manifestaciones impide que sea percibido por las opiniones públicas en toda su plenitud, lo que incide negativamente a la hora de movilizar la adopción de acciones políticas.

En todo caso, la toma de conciencia de los riesgos cibernéticos cuya materialización en determinado grado puede llegar a producir una auténtica catástrofe mundial, requiere un actor poderoso que tenga verdadero interés en que se tome conciencia política de este riesgo y, a la vez, sea capaz de propiciar la toma de decisiones para neutralizarlo. La clara limitación de los Estados nacionales para enfrentarse a procesos globales como es el que nos ocupa, requiere que los llamados a realizar esta magna tarea sea el Estado-nación junto a las organizaciones supranacionales, en el marco de la Organización de Naciones Unidas, acompañados de las grandes corporaciones digitales.

Pero incluso con la triple implicación de los actores indicados, esta opción sería incompleta si las opiniones públicas en general y los individuos en particular, no los perciben como garantes de su seguridad y, en última instancia, de su libertad, lo que vuelve a situar el debate en el clásico dilema de seguridad vs libertad, ya viejo conocido en el mundo no cibernético, y pone de relieve la necesidad de disponer de conceptos y categorías que den una respuesta clara a la pregunta: ¿cuál es la libertad posible y la seguridad necesaria en un mundo digital?, y requiere de instrumentos políticos, jurídicos y tecnológicos que hagan efectiva la respuesta.

Para ello resulta indispensable entender que la seguridad tiene un carácter instrumental al servicio de la libertad, ya sea de la humanidad, de las naciones, de los Estados o de los individuos, y que esto requiere tener un concepto y alcance, claro y compartido de la libertad.

Los supuestos actos de libertad realizados en el ciberespacio en nombre de la utopía ácrata y libertaria, en muchos casos, no son otra cosa que actos efectuados en fraude de libertad, toda vez que son actos realizados al amparo de una interpretación de la misma que persiguen resultados contrarios a la propia libertad o prohibidos por ella, y por consiguiente no han de impedir la aplicación de la interpretación que hubieran tratado de eludir.

DERECHO

La sociedad internacional está compuesta por Estados soberanos lo que, en puridad, implica la facultad de dictar normas no condicionadas y el derecho a no recibir órdenes de nadie, al no existir un poder superior internacional que cumpla funciones análogas a las del Estado de Derecho interno, esto es, que legisle, juzgue y aplique coactivamente el Derecho, en este caso, el derecho internacional.

Las organizaciones internacionales no son superestados, sino un entramado de relaciones y cauce de coordinación y discusión entre los diversos Estados que las componen. Sus resoluciones y normas, son consecuencia de acuerdos de los Estados que la integran, que ejercen su soberanía perteneciendo a las mismas y dictando normas a través de ellas.

La falta de un poder supraestatal hace que la eficacia de las normas jurídicas internacionales sea inferior a la que es habitual en el seno de un Estado. Las consecuencias de su violación están más difusas y son mayores las posibilidades que su contravención quede sin sanción, permaneciendo el recurso a la fuerza como última ratio en las relaciones internacionales.

La obligatoriedad de las normas entre Estados permite albergar la esperanza que en un futuro sea posible conferir a las normas internacionales la misma fuerza que tienen en los Derechos internos. Pero hoy no es así y esta situación no resulta indiferente para la seguridad en el ciberespacio.

En todo caso, en el panorama internacional, se aprecian pasos sólidos en el sentido de una mayor eficacia de las normas de derecho internacional lo que resulta ser, sin duda, una buena noticia para el ciberespacio, ámbito especialmente necesitado de ordenación e impregnado de internacionalismo y globalidad.

La Red no cuenta con una autoridad y control central y, a diferencia de otras instituciones sociales, se ha desarrollado de forma autónoma siguiendo pautas tecnológicas y sociológicas sin que, hasta ahora, haya encontrado su correlativo jurídico.

Para abordar la respuesta legal a las amenazas cibernéticas y su eventual inserción en una estrategia de ciberseguridad, es preciso analizar los elementos esenciales que la determinan, el entorno en el que operan y la realidad sociopolítica en la que se desarrolla, así como el grado de evolución del sistema legal actuante, considerando que en ciberseguridad, la magnitud de la dimensión legal es similar a la integrada por los elementos tecnológicos y de seguridad tradicionales y todos, conjuntamente, conforman un concepto securitario propio, específico del orden digital, considerado como el resultado de un equilibrio armónico y estable del ciberespacio.

En última instancia la respuesta legal de un ente en el ámbito cibersecuritario, está constituida por el conjunto de acciones encaminadas a crear, modificar, derogar e imponer las normas jurídicas necesarias para el logro efectivo de su seguridad cibernética, en lo referido tanto a la individualidad como a su campo de relaciones, lo que requiere comprender el alcance de la función del Derecho frente a las amenazas y riesgos cibernéticos en un proceso de constante evolución.

A esta evolución del ciberespacio como ente, se le une la expansión del concepto de seguridad derivado de los grandes cambios experimentados en el mundo actual, que ha devenido pluridisciplinar, con una directa incidencia en la configuración de la categoría jurídica de seguridad nacional necesitada de una precisa delimitación, que sirva como criterio central para la gestión de las necesidades estratégicas actuales en conexión con las exigencias de respeto a los derechos y libertades fundamentales. [1]

En esta nueva situación los instrumentos clásicos han sufrido una modificación en su idoneidad para garantizar el sistema de convivencia: las fuerzas armadas han dejado de ser el aparato estatal exclusivo encargado de garantizar la supervivencia, la diplomacia ha dejado de ser instrumento exclusivo para llevar a cabo la acción exterior y la administración de justicia resulta insuficiente para hacer frente al debilitamiento del sistema estatal, el crimen organizado o el terrorismo. Lo que comporta una expansión del espectro de sujetos, instituciones y organizaciones implicados en la seguridad nacional.

El desarrollo del ciberespacio ha potenciado toda clase de actividades tanto gubernamentales, como comerciales o sociales y muchos procesos mundiales son controlados a través del mismo; se configura como un bien de alto valor que requiere seguridad como elemento imprescindible y necesita protección jurídica.

El alto grado de sofisticación de las tecnologías utilizadas y el uso masivo de las mismas, dibujan un escenario global del ciberespacio en el que ni los organismos de seguridad ni el Derecho, han logrado dar una respuesta satisfactoria a las amenazas provenientes de su utilización con fines delictivos o como instrumento de agresión internacional.

La nueva situación demanda una respuesta adecuada de los ordenamientos jurídicos y de la normativa internacional, en un marco cívico, en el que se ha desarrollado exponencialmente toda clase de actividades, con una alta repercusión en todas las ramas del Derecho, de las que demanda su adecuación a la nueva realidad para hacer frente, especialmente, a las dimensiones informacionales, tecnológicas y securitarias incorporadas a las materias de su ámbito de ordenación, atendiendo al alcance global de los efectos de las nuevas tecnologías, su valor patrimonial, político y estratégico, su alto potencial como instrumento comisivo y en la internacionalización de la vida en general.

Esta adecuación de ordenamientos jurídicos y normas internacionales requeriría, además de la regulación de numerosos supuestos típicos derivados de la nueva situación, con la configuración incluso de nuevos ilícitos penales, una explícita consideración del

[1] "Estrategias legales frente a las ciberamenazas", José L. González Cussac, Cuadernos de Estrategia nº 149, Ministerio de Defensa, Madrid, 2010.

ciberespacio y los recursos de información como ámbitos de oportunidades y riesgos para el individuo, la sociedad y el Estado, y de la ciberseguridad como bien jurídico protegido.

Se da la circunstancia que en la realidad digital, cuando se produce una fuga de datos, el daño es irreversible, lo que unido a la dificultad probatoria para determinar su autoría y a que la acción jurisdiccional opera a posteriori, pone en evidencia que para lograr su protección se requiere el uso de medidas de prevención que impidan materialmente y de forma eficaz (a priori) que el hecho se produzca, lo que se logra mediante la aplicación de seguridad de la información, entre cuyas medidas están las organizativas, físicas, lógicas, electromagnéticas y, muy especialmente, las criptológicas.

Estos ámbitos han de ser protegidos de forma real y efectiva, de manera proporcional; de lo contrario, la alta función de servicio a la libertad que los legitima, resultaría inútil.

TECNOLOGÍA Y SEGURIDAD

El elemento físico, básico, posibilitador del ciberespacio es de naturaleza tecnológica. Tanto su naturaleza, como la amenaza y defensa de su existencia y funcionamiento están impregnadas de tecnología; de ella y de su aplicación derivan, en última instancia, las principales fortalezas y debilidades.

En el ámbito tecnológico es donde se produce, la gran confrontación cibernética, amplificada o atenuada por factores concurrentes de naturaleza política, jurídica, económica o de seguridad, entre otros, cuya interrelación da origen al núcleo esencial de su complejidad y configura el ámbito donde se ha de buscar la solución.

Al déficit social, político y jurídico de la Red, se le une un déficit de seguridad –dentro de la que juega un papel preponderante la Criptología- imprescindible para poder gestionar un sistema tecnológico de esa magnitud y que llega a adquirir en el ciberespacio el carácter de instrumento de ordenación al servicio de la eficacia del Derecho.

Su proliferación y uso, en paralelo al negocio que conlleva asociado, ha venido acompañada de un incremento exponencial de empresas, servicios, aplicaciones, equipos y sistemas que, desde la perspectiva del alto rigor matemático, tecnológico y de seguridad que esta disciplina requiere, podría haber provocado una eventual banalización de los niveles criptográficos requeridos, con las consecuencias que ello comporta para el cumplimiento de su finalidad, que no es otra, que la seguridad de la información y las comunicaciones. Y, en consecuencia, el logro de una protección real y efectiva, de intereses, derechos y libertades, requerimiento ineludible para la propia existencia del ciberespacio mismo y de un entorno digital humano política y económicamente viable.

El legítimo y lucrativo negocio que la eclosión de los desarrollos criptográficos comporta, no siempre ha tenido en cuenta el umbral mínimo de fortaleza criptológica requerida -determinado por los niveles de las capacidades internacionales más avanzadas en criptoanálisis- para evitar que esta protección pudiera ser una mera apariencia, lo que genera, a su propia escala, otro dilema nada baladí: el “criptoconflicto”, que por su

especificidad, importancia, alcance, e incidencia en el gran dilema cibernético y en el mundo digital en su conjunto, requiere ser tratarlo de forma monográfica y separada.

Figura 1

LA NUEZ DEL DILEMA DIGITAL (DI+DI)

Dicho todo lo anterior y por mera responsabilidad intelectual y cívica, nos aproximamos al nudo gordiano de este dilema desde una perspectiva realista con la finalidad de contribuir, si es posible, a proyectar algo de luz sobre una cuestión, sin duda compleja, que tiene en ascuas a las sociedad mundial.

Como primera consideración, a la altura del siglo en el que nos encontramos, ya no estamos para simplificaciones de atrincheramientos en ocultismos u opacidades propio de otras épocas, ni para transparencias incondicionadas de las proclamas libertarias, y menos aún para ingenuidades como las de creer que las redes per se están protegidas.

Ha llegado el momento para que las sociedades, los gobiernos y las organizaciones internacionales, realicen el esfuerzo de reconfiguración necesario para determinar el punto crítico de equilibrio entre la transparencia necesaria y el sigilo imprescindible, de los asuntos datos y objetos, que la sociedad actual, fuertemente digitalizada, demanda. Y, en consecuencia, actuar de forma que la protección necesaria en cada caso sea una realidad efectiva.

No parece que el problema esté en la obtención de información derivada de la falta de seguridad de las redes, hábilmente aprovechada por unas agencias de inteligencia que existen -no se ha de olvidar- porque las sociedades a las que sirven las crean y legitiman, proporcionándoles el marco legal de actuación. Las normas por las que se guían responden a la forma en que la sociedad que le dio origen, ha resuelto el permanente dilema de libertad y seguridad de las variables que intervienen e inciden directamente en el ciberespacio, entre las que están la seguridad del Estado, la intimidad personal, el secreto de las comunicaciones, la prevención y persecución del delito, el secreto profesional, o el secreto comercial e industrial, entre otras, que en la era digital se tornan de mayor complejidad y requiere una reformulación realista con base en sólidos argumentos éticos, políticos y jurídicos, así como el pronunciamiento decidido sobre aspectos que suelen generar controversia en la opinión pública, pero que la realidad digital demanda, de forma perentoria, por ser un elemento sustancial de su propia existencia.

Siguiendo un orden racional lógico, tal vez, lo que se necesite en primer lugar sea un reajuste en la delimitación clara de los ámbitos de confidencialidad y su adecuada valoración en el mundo digital, tarea que resulta ser esencialmente política, porque política es determinar hasta donde debe extenderse la transparencia de los asuntos públicos como norma general y donde se ha de limitar, como excepción, por exigencias de la libertad. Y, de igual modo, determinar hasta donde debe llegar el grado de reserva y secreto de los asuntos privados como principio, y donde está el punto crítico en el que esta reserva ha de ceder por razones del funcionamiento del Estado de Derecho, de forma excepcional y con garantía judicial.

En ambos casos, tanto la transparencia de los asuntos públicos como la reserva de los privados inciden directamente en la libertad, y su limitación solo es justificable en la medida que resulte estrictamente necesaria para garantizarla.

La delimitación de estos ámbitos resulta tan rigurosamente crítica que el sustrato cognitivo para su configuración, en los Estados democráticos, ha de proceder de la sociedad misma, que se ha de pronunciar sobre cuál es el límite de la transparencia de sus asuntos públicos y hasta donde llega el nivel de reserva de los privados, siendo consciente de la transcendencia que tienen estas decisiones tanto para su seguridad como para su independencia política, progreso económico y libertades ciudadanas.

La complejidad de esta tarea ha de convocar a los más idóneos para su realización a través de un enfoque multidisciplinar al modo de cómo lo entendió el juez Warren, en la década de los sesenta del siglo pasado, que sugería que debían ser periodistas, sociólogos, políticos y juristas quienes abordasen esta alta responsabilidad, de consecuencias políticas trascendentales. A los que hoy, tal vez, habría que añadir politólogos, tecnólogos, criptólogos y economistas, para hacerlo efectivo en la sociedad digital en la que vivimos.

En segundo lugar es tarea de las administraciones y formaciones políticas convertir esos posicionamientos sociales y políticos en proyectos que los legisladores transformarán en normas jurídicas, claras y precisas, conscientes de su importancia para seguridad, independencia, progreso social y bienestar económico de la Sociedad, el Estado y los Individuos.

En tercer lugar la tecnología y la criptología, proporcionarán las herramientas necesarias para hacer efectivo lo indicado en los dos puntos anteriores.

La complejidad para determinar el nudo gordiano del dilema digital es debida, entre otras razones, a que las variables que intervienen en la determinación del punto crítico de equilibrio tienen elementos comunes, responden a principios distintos, operan bajo coordenadas diferentes e, incluso, defienden intereses que en algunos casos pueden llegar a ser contrapuestos.

Y ello, en unos momentos en que los Estados no son ya entes territorialmente bloqueados, sino espacios fluctuantes de poder económico, político, tecnológico, cognitivo y científico; que operan en un entorno internacional en el que el aliado militar, puede ser, a la vez, socio y competidor económico, e incluso, adversario político; con unos requerimientos ineludibles para la eficacia de las resoluciones judiciales; y con ciudadanos que demandan conocer las cuestiones públicas y han desarrollado un fuerte sentimiento de privacidad.

El alto grado de dificultad que comporta la determinación de ese punto crítico de equilibrio, no excluye la posibilidad de su elaboración teórica mediante el correspondiente modelo matemático -reto colosal para los "ciber-metras"- que sin duda resultaría un referente de gran utilidad y, consideramos, sería idóneo para analizar el comportamiento de este sistema complejo ante situaciones que resulta difíciles de observar en la realidad.

El modelo como arquetipo para imitar o reproducir, sería la representación teórica de esta realidad compleja que permitiría generar una representación abstracta, conceptual, gráfica o visual para analizar, describir, explicar, simular y predecir el fenómeno que nos ocupa. Expresaría relaciones, proposiciones sustantivas de hechos, variables, parámetros, entidades y relaciones entre variable y entidades u operaciones.

A todo este complejo entramado de relaciones y a la controversia que se suscita en el ciberespacio, nos atrevemos a denominar "ciberdilema", que encontrará solución mediante un balanceo ponderado de los distintos intereses en juego, lo que supone que ellos mismos se contrarrestan e impiden "escoras" superiores a las toleradas por el sistema.

APROXIMACIÓN A UN MODELO

Mientras que los modelos conceptuales no tienen otra intención que ayudar a la comprensión de sistemas complejos mediante analogía con otros modelos más simples, los modelos matemáticos, en cuanto que reducen sistemas complejos a formulaciones concretas, tienen más pretensiones y, también, más limitaciones.

El modelo propuesto consiste en establecer el posicionamiento de las variables jurídico-políticas (políticas, normativas y de seguridad) que de forma más significativa, influyen en un sistema cibernético en relación con referentes estables de la misma naturaleza, de forma que proporcione la posición ideal que han de ocupar en el ciberespacio y, por comparación, determinar el desvío y, en su caso, el sentido que ha de tener la corrección de la variable comparada.

1. Del estudio de los artículos 18 y 20 de la Constitución Española, y los homólogos de las constituciones iberoamericanas y de algunos otros países del resto del mundo, así como de normas internacionales, se pueden deducir los referentes cualitativos básicos con respecto a los que se puede determinar un posicionamiento político y jurídico –que estimamos coherente- con respecto al ciberdilema.

De este análisis se derivan una serie de conclusiones válidas para sociedades y estados democráticos:

a. Transparencia de lo público y secreto de lo privado, como norma general.
b. Secreto de lo público y transparencia de lo privado, como excepción.
c. Secreto público poco extenso y muy intenso con el nivel que requiera la seguridad del Estado en el contexto del orden global internacional.
d. Secreto privado muy extenso y con la intensidad que requiera la acción de la Justicia.
e. Adecuación de la seguridad de la información y las comunicaciones a los requerimientos de puntos a, b, c y d.

De lo indicado se derivan una serie de referencias que, agrupadas por pares opuestos, resultan ser: Transparencia-Secreto, Información pública-Información privada, y Libertad-Seguridad.

Considerando que el punto crítico de equilibrio de estas referencias en un cibersistema se situaría en la equidistancia de las indicadas (salvo la de su par opuesto), las situamos en la superficie de una esfera, de forma que el valor de la equidistancia entre ellas sería $R\sqrt{2}$ y la distancia a su par opuesto 2R. Siendo R el radio de la esfera.

Estos seis puntos, así dispuestos, son los vértices de un octaedro regular inscrito en una esfera, que representaría el equilibrio perfecto de las referencias señaladas y sus relaciones, en el ciberespacio, cuyo centro de simetría coincide con el centro de la esfera circunscrita, a la que denominaremos ciberesfera.

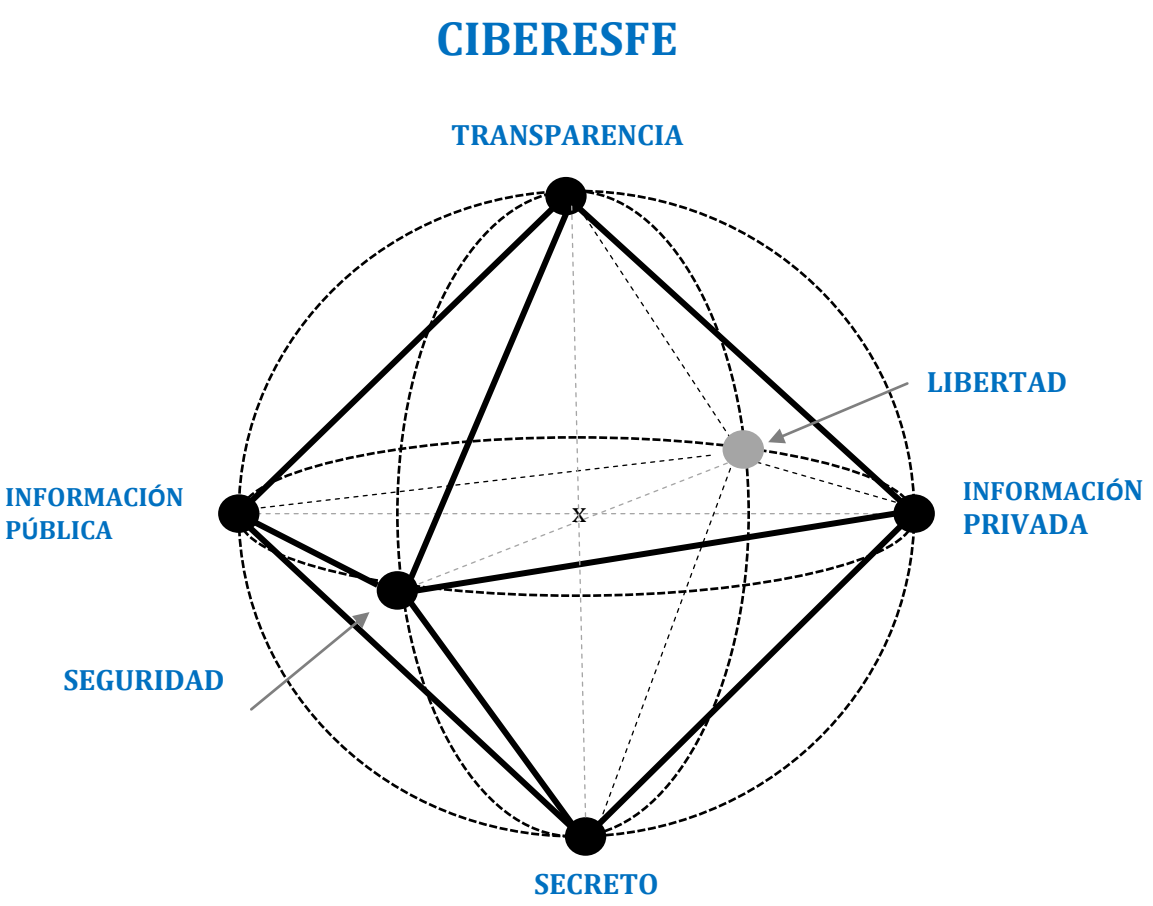

Figura 2

2. Como medio para posicionar las variables respecto a los referentes indicados, se recurre a una cuadrícula rectangular (coordenada cartesiana), que convenimos sea de 20x10, representativa de la superficie de la ciberesfera obtenida mediante el desarrollo del cilindro circunscrito, sobre la que se sitúan los puntos de las seis referencias permanentes obteniendo una plasmación gráfica de la posición relativa de unos respecto de otros que adopta la forma de cruz latina. Situando el punto 0 en el centro de la cuadrícula.

Sobre esta cuadrícula también se sitúan las variables más significativas de la ciberseguridad obtenidas del análisis del sistema jurídico-político que se pretenda analizar tales como Libertad de expresión, Privacidad, Secreto de las comunicaciones, Seguridad del Estado, Prevención y persecución del delito, Secreto comercial e industrial, etc.

Para ello, y tras el correspondiente análisis, sometemos estas variables a una valoración con respecto al grado de proximidad a cada una de las referencias permanentes, lo que nos dará su posición en la cuadrícula anteriormente indicada y, con ello, el modelo ideal.

La posición de las variables de una sociedad real en la cuadrícula no es estática, sino que está sujeta a desplazamientos (lentos pero desplazamientos) a consecuencia de su evolución política, jurídica (tanto normativas como jurisprudenciales) o tecnológica, que hacen que se aproxime o aleje de la referencia.

3. Debido a la interrelación de las variables, para determinar el sentido de la corrección se ha de tener en cuenta los efectos de las demás lo que eventualmente nos llevaría a requerir de cálculos cinemáticos, atendiendo al sentido y valor de los vectores representativos de todas ellas respecto al punto de referencia de que se trate.

Este modelo podrá ser perfeccionado hasta el infinitivo, aumentando tanto las referencias, como las variables-móviles, haciendo más pequeñas las cuadrículas del desarrollo esférico o intensificando el análisis normativo y jurisprudencial, entre otras formas de lograrlo.

Como convención inicial y con la precisión que permiten los datos disponibles en un trabajo de esta naturaleza que requeriría de una compleja investigación en profundidad, se determina un entorno de proximidad a los puntos críticos de las referencias, que permite establecer un criterio para considerar que si una variable-móvil entra en el mismo, se considere que cumple con el máximo nivel de proximidad a la referencia.

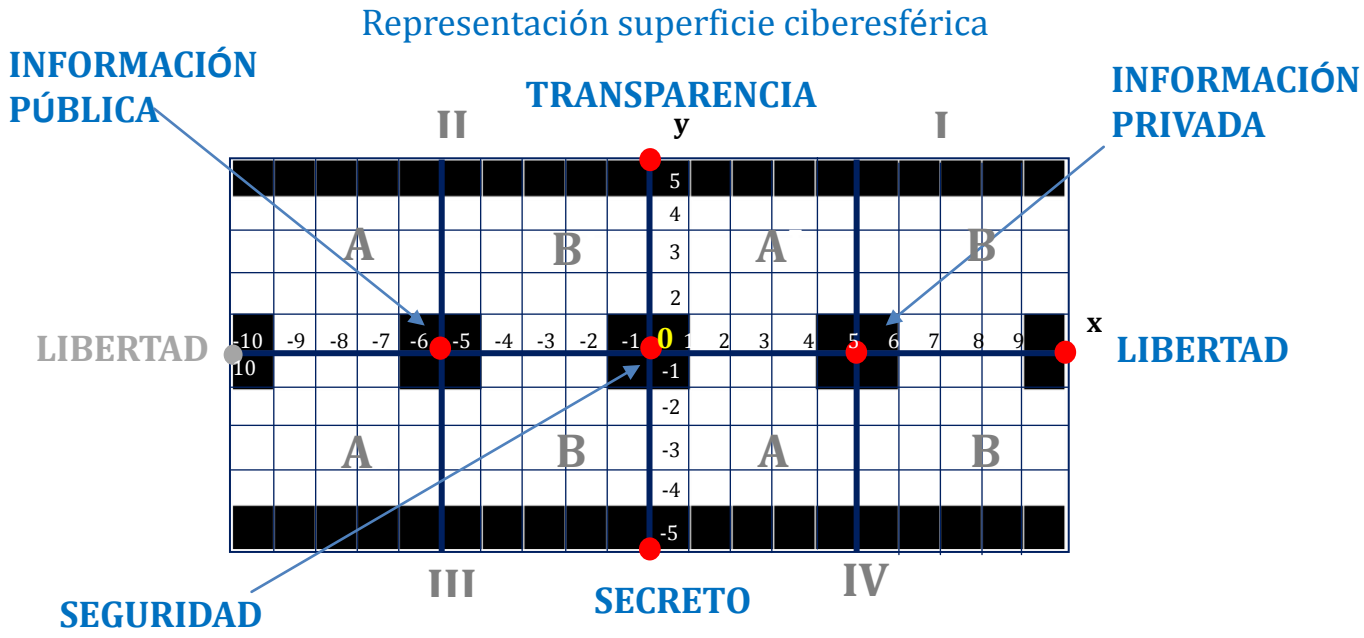

Figura 3

4. A modo de ejemplo, tratamos de situar en la cuadrícula una serie de variables y su posición cualitativa con respecto a cada una de las referencias, consistiendo la primera operación en situarlas en uno de los campos de los pares opuestos según su naturaleza jurídico política.

a) Determinación de las variables eligiendo una entre los pares opuestos de referencias:

▪ Libertad de expresión (a):

Información pública/Información privada= I. Pública.
Transparencia/Secreto= Transparencia.
Libertad/Seguridad= Libertad.*[2]

▪ Intimidad (b):

Información pública/Información privada= I. Privada.
Transparencia/Secreto= Secreto.*
Libertad/Seguridad= Seguridad y Libertad.

▪ Secreto de las comunicaciones (c):

Información pública/Información privada= I. Privada.
Transparencia/Secreto= Secreto.*
Libertad/Seguridad= Seguridad.

▪ Seguridad del Estado (d):

Información pública/Información privada= I. Pública.

[2] * = dominante.

Transparencia/Secreto= Secreto.
Libertad/Seguridad= Seguridad.*

▪ Prevención y persecución del delito (e):
Información pública/Información privada= I. Pública.
Transparencia/Secreto= Secreto.
Libertad/Seguridad= Seguridad.*

▪ Secreto comercial e industrial (f):
Información pública/Información privada= I. Privada.
Transparencia/Secreto= Secreto.*
Libertad/Seguridad= Libertad.

▪ Transparencia administrativa (g):
Información pública/Información privada= I. Privada.
Transparencia/Secreto= Transparencia.*
Libertad/Seguridad= Libertad.

▪ Datos personales (h):
Información pública/Información privada= I. Privada.
Transparencia/Secreto= Secreto.*
Libertad/Seguridad= Seguridad

▪ Secreto profesional (i):
Información pública/Información privada= I. Privada.
Transparencia/Secreto= Secreto.*
Libertad/Seguridad= Seguridad
▪ Secreto estadístico (j):
Información pública/Información privada= I. Pública.
Transparencia/Secreto= Secreto.*
Libertad/Seguridad= Seguridad.

▪ Información clasificada (k):
Información pública/Información privada= I. Pública.
Transparencia/Secreto= Secreto.*
Libertad/Seguridad= Seguridad

▪ Información administrativa (l):
Información pública/Información privada= I. Pública.
Transparencia/Secreto= Transparencia.*
Libertad/Seguridad= Libertad.

▪ Régimen electoral (m):
Información pública/Información privada= I. Pública.
Transparencia/Secreto= Secreto

Libertad/Seguridad= Seguridad.*

b) Para determinar la interrelación entre variables –con alta complejidad- se sitúa cada una en un punto de la cuadrícula con respecto a los seis referentes de los tres pares opuestos: Secreto- Transparencia, Información pública-privada, Libertad-Seguridad y, posteriormente, verificar y ajustar atendiendo a la dominante.

Situando las variables en la cuadrícula, teniendo en cuenta la dominante, tendríamos la representación gráfica del punto crítico de equilibrio de las variables contempladas. Uniendo los puntos entre sí resulta una línea quebrada que sería la representación del punto crítico del sistema. Haciendo lo propio con las variables de la organización real analizada, se podrá comparar sus posiciones respecto a las del modelo.

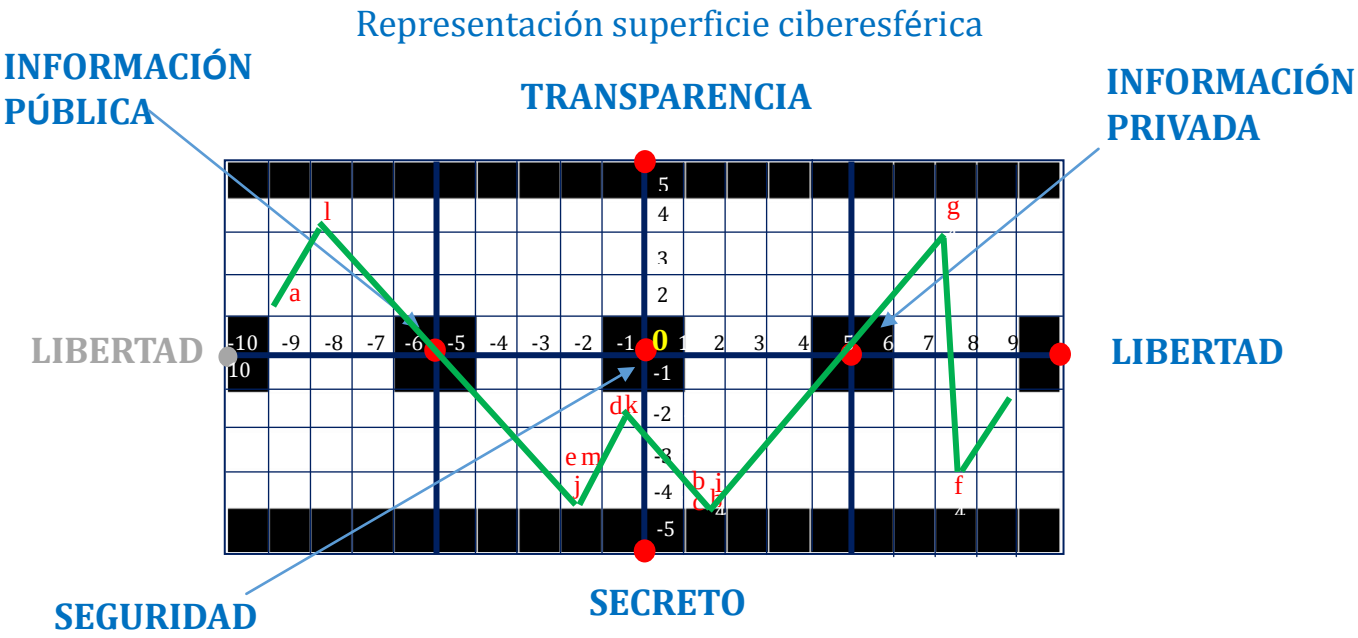

Figura 4

El ejemplo realizado con las seis referencias y las trece variables, indicadas, proporciona como resultado una figura que vista sobre la semiesfera que ofrece el punto 0 de los ejes cartesianos se asemeja, en su forma, a la de una w.

W

La coincidencia de las variables indicadas pertenecientes a un país, organización o sistema de que se trate, con las variables del modelo, permitiría determinar que cumple con los requerimientos básicos de una solución adecuada del ciberdilema y, en su caso, el grado de desvío para su eventual corrección.

CONCLUSIÓN

El ciberespacio, al igual que los ámbitos de tierra, mar, aire y espacio, es un Global Commons[3], pero a diferencia de estos, es el único que ha sido construido artificialmente; en su esencia están, como elementos constitutivos, la Tecnología, la Seguridad –especialmente en su dimensión criptológica-, el Derecho, así como la Globalidad.

Esta circunstancia condiciona cualquier estrategia para lograr su viabilidad y defensa efectiva frente a las amenazas. Asimismo, determina la ineludible necesidad de una intensa cooperación internacional para lograrlo, cuya máxima expresión estaría en una eventual entidad supranacional de naturaleza digital y carácter mundial, bajo el estricto cumplimiento de las normas que rigen el Estado de Derecho.

Esta entidad, conviviría con las organizaciones digitales territorializadas, derivadas de los Estados nacionales y de los organismos internacionales, bajo los auspicios de unas Naciones Unidas adecuadas al nuevo paradigma.

En todo caso, y parafraseando a Marcel Merle[4], hasta hoy, ni la cultura, ni la ideología, ni la economía han sido palancas suficientes para romper la resistencia de las soberanías nacionales. Tras ella se oculta una solidaridad de intereses y el temor de una pérdida de identidad nacional.

Lo cierto hasta ahora es que por débil que haya sido el consenso en el interior de muchos Estados nacionales, aún es más fuerte que la solidaridad internacional y está por ver si la nueva sociedad que emerge en torno al ciberespacio lo logrará; por lo que mientras no se encuentre un punto de apoyo para implantar nuevas estructuras, el mundo permanecerá dividido en Estados-Naciones.

En estas circunstancias, y para hacer frente al reto digital, cada Estado ha de diseñar sus estrategias conscientes del carácter global del ciberespacio, de la amenaza procedente del mismo y de la defensa para su protección, así como para garantizar su propia existencia y la protección efectiva de los intereses, derechos y libertades de sus ciudadanos. Y permanecer en esta tarea con rumbo sostenido hacia una convergencia internacional que fructifique en una entidad digital supranacional creíble, transparente y eficaz, donde el ciudadano de cualquier Estado perciba con nitidez el carácter instrumental de la seguridad requerida al servicio del progreso, del bienestar y de la libertad, como forma de aspirar al logro de una paz digital justa, estable y duradera.

[3] Ángel Gómez de Agreda, "El Ciberespacio como escenario de conflictos. Identificación de las amenazas", Centro Superior de Estudios de la Defensa Nacional, Monografía CESEDEN nº 126, febrero 2012.
[4] "Sociología de las relaciones internacionales", Alianza Universidad, Madrid 1984.

Una política sensata y realista, complementada con una elaborada estrategia de información en las que se aborde el fenómeno desde una perspectiva integral, que contemple conjuntamente la dimensión política, la jurídica, tecnológica y de seguridad −de la adquisición, procesamiento, clasificación, protección, almacenamiento y distribución de la información− proporcionarán el punto crítico de equilibrio de todas las variables intervinientes y aportará el sustrato cognitivo necesario para reformular el dilema clásico y adecuarlo a la era digital, base imprescindible para arbitrar una solución, con posterior plasmación en las correspondientes normas, y su implementación tecnológica en redes, sistemas, servicios y equipos.

En todo caso, independientemente del ruido que está generando por el reciente caso Snowden, y no hace mucho, Wikileaks, y que los servicios de inteligencia no son los únicos en la realización de una tarea que ha existido, existe y existirá; una posición realista para todos –gobiernos, empresas y ciudadanos− pasa ineludiblemente por tomar seria conciencia de los riesgos que comporta el uso de las tecnologías de la información y las amenazas globales a las que está sometido el entorno digital, cuyo corolario es la necesidad perentoria de protegerse al nivel de seguridad adecuado.

*José María Molina Mateos**
Doctor en Derecho,
Máster Universitario en Estudios sobre Paz, Seguridad y Defensa
Especialista en Criptología
Profesor visitante de la Universidad Camilo José Cela